Exchange 2010 SP1

Microsoft Operations guide

Prepared for

Microsoft Corporation

Tuesday, 30 August 2011

Version 3.0

Prepared by

PFE/MCS Exchange Ops Team

Project Team Leads/Editors

Jack Maye

Ed Grant

Contributors

Didier Akakpo

Maged Ezzat

Dale Hardin

Kent Tilger

Nikharge Amit Rajan

Varun Aggarwal

Kamaljit Mundi

Gordon MacAllister

Al Wolchesksy

Mauricio Tamayo Ortega

Kamal Abburi

Franck Nerot

Shashwat Mohapatra

Rob Brown

Jim Kuterbach

Patrick Murray

Brian Day

Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Author** | **Version** | **Change reference** |
| 2011/04/07 |  | 0.1 | Initial draft for review/discussion |
| 2011/04/11 | Didier Akakpo | 0.9 | Draft |
| 2011/04/22 | Didier Akakpo | 1.0 | For approval |
| 2011/07/19 | Jack Maye | 1.1 | Reviewed |
| 2011/07/20 | Jack Maye | 2.0 | Added Disaster Recovery Strategies Section |
| 2011/07/20 | Jack Maye | 2.0 | Added How To Guides Section |
| 2011/07/20 | Jack Maye | 2.0 | Added Backup/Recovery Process and Procedures |
| 2011/07/20 | Jack Maye | 2.1 | Added Operations Management and Framework |
| 2011/07/21 | Jack Maye | 2.2 | Added additional content for Operations Management- Mailbox |
| 2011/07/21 | Jack Maye | 2.3 | Added As Needed Tasks |
| 2011/07/22 | Jack Maye | 2.4 | Added Evolutions and Updates-Servicing |
| 2011/07/25 | Jack Maye | 2.5 | Removed Exchange install section |
| 2011/08/19 | Jack Maye | 3.1 | Sanitizing document for generic use |
| 2011/08/25 | Jack Maye | 3.2 | Adding Messaging Tracking Section to As Needed Tasks |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Version approved** | **Position** | **Date** |
|  |  |  |  |

Table of Contents

[1 Introduction 1](#_Toc301517891)

[1.1 Audience 1](#_Toc301517892)

[2 Operations Management and Monitoring of an Exchange 2010 Organization 1](#_Toc301517893)

[2.1 Microsoft Operations Framework 2](#_Toc301517894)

[3 Operations Management 2](#_Toc301517895)

[3.1 Standard Procedures 2](#_Toc301517896)

[4 Exchange 2010 Management 3](#_Toc301517897)

[4.1 Exchange Management Console 3](#_Toc301517898)

[4.2 Exchange Management Console Interoperability 4](#_Toc301517899)

[4.2.1 Interoperability with Exchange 2010 4](#_Toc301517900)

[4.2.2 Side-by-Side Management Console 6](#_Toc301517901)

[4.3 Exchange Management Shell 6](#_Toc301517902)

[4.4 Installation of the Exchange Management Tools 7](#_Toc301517903)

[4.4.1 Prerequisites 7](#_Toc301517904)

[4.5 Exchange Control Panel (ECP) 7](#_Toc301517905)

[5 Exchange 2010 permissions and delegations 9](#_Toc301517906)

[5.1 RBAC 9](#_Toc301517907)

[5.1.1 Management Role Group 10](#_Toc301517908)

[5.1.2 Built-in Management Roles 12](#_Toc301517909)

[5.2 RBAC model – needs to be sanitized and made generic 15](#_Toc301517910)

[5.2.1 Naming convention 15](#_Toc301517911)

[5.2.2 Role groups and scopes definition 16](#_Toc301517912)

[5.2.3 Scope creation 16](#_Toc301517913)

[5.2.4 Role group creation 17](#_Toc301517914)

[5.2.5 Add role group member 17](#_Toc301517915)

[5.2.6 Example 17](#_Toc301517916)

[6 Operations Management 18](#_Toc301517917)

[6.1 Managing Mailboxes 18](#_Toc301517918)

[6.1.1 Create a Mailbox for a New User 18](#_Toc301517919)

[6.1.2 Create a Mailbox for a SHARED Mailbox 21](#_Toc301517920)

[6.1.3 Viewing existing Mailbox access rights 22](#_Toc301517921)

[6.1.4 Add an E-mail address for a mailbox 23](#_Toc301517922)

[6.1.5 Disable a Mailbox 23](#_Toc301517923)

[6.1.6 Connect a Mailbox 24](#_Toc301517924)

[1.1.1 Create a Mailbox for an Existing User 26](#_Toc301517925)

[6.1.7 Enable a Personal Archive for a New mailbox 34](#_Toc301517926)

[6.1.8 Enable a Personal Archive for an Existing Mailbox 36](#_Toc301517927)

[6.1.9 Configure Personal Archive Quotas for a Mailbox 37](#_Toc301517928)

[6.1.10 Disable a Personal Archive for a Mailbox 38](#_Toc301517929)

[6.1.11 Connect a Disconnected Personal Archive 39](#_Toc301517930)

[6.1.12 Monitoring Exchange Database Information and Statistics 40](#_Toc301517931)

[6.1.13 Viewing Mailbox Statistics 40](#_Toc301517932)

[6.1.14 Monitoring Resource Usage 41](#_Toc301517933)

[6.1.15 Using Performance Monitor Counters 41](#_Toc301517934)

[6.1.16 Obtaining Information about Public Folder Databases 42](#_Toc301517935)

[6.1.17 Viewing Public Folder Statistics 43](#_Toc301517936)

[6.1.18 Moving a Mailbox 43](#_Toc301517937)

[6.2 Managing Contacts 49](#_Toc301517938)

[1.1.2 Create a Contact 49](#_Toc301517939)

[6.2.2 Change contact properties 50](#_Toc301517940)

[6.2.3 Remove a contact 50](#_Toc301517941)

[7 Daily Tasks 52](#_Toc301517942)

[7.1 Performing Physical Environmental Checks 52](#_Toc301517943)

[7.2 Performing and Monitoring Backups 53](#_Toc301517944)

[7.3 Checking Disk Usage 53](#_Toc301517945)

[7.4 Checking Disk Space 53](#_Toc301517946)

[7.5 Checking the Event Viewer 54](#_Toc301517947)

[7.6 Monitoring Server Performance 54](#_Toc301517948)

[7.7 Monitoring the Operating System 54](#_Toc301517949)

[7.7.1 System Monitor 54](#_Toc301517950)

[7.7.2 Performance Logs and Alerts 55](#_Toc301517951)

[7.7.3 Task Manager 55](#_Toc301517952)

[7.8 Monitoring Network Performance 55](#_Toc301517953)

[7.8.1 Network Monitor 55](#_Toc301517954)

[7.9 Verify MAPI Connectivity through system mailboxes 56](#_Toc301517955)

[7.10 Monitoring Mail Queues 56](#_Toc301517956)

[8 Weekly Tasks 58](#_Toc301517957)

[9 Monthly Tasks 58](#_Toc301517958)

[10 As Needed Tasks 58](#_Toc301517959)

[11 Evolutions and updates-Servicing 60](#_Toc301517960)

[11.1 Installing Updates (Rollups and all patches) on DAG Members 60](#_Toc301517961)

[11.1.1 Suspend activation for the database copies on the server being updated 60](#_Toc301517962)

[11.1.2 Perform a server switchover on the server being updated 61](#_Toc301517963)

[11.1.3 Install the updates rollup Exchange 61](#_Toc301517964)

[11.1.4 Resume activation for the databases on the updated server 62](#_Toc301517965)

[11.1.5 Perform database switchovers and re-balance the DAG 62](#_Toc301517966)

[11.2 Replace a hard disk failed in a database of a DAG member 62](#_Toc301517967)

[11.3 Suspend a Mailbox database copy 64](#_Toc301517968)

[11.4 Update a Mailbox database Copy 65](#_Toc301517969)

[12 Disaster Recovery Strategies 66](#_Toc301517970)

[12.1 Implement Best Practices 66](#_Toc301517971)

[12.2 Identify Data to Protect 66](#_Toc301517972)

[12.2.1 Mailbox Servers 67](#_Toc301517973)

[12.2.2 Hub Transport Server 67](#_Toc301517974)

[12.2.3 Edge Transport Server 68](#_Toc301517975)

[12.2.4 Client Access Server 69](#_Toc301517976)

[12.2.5 Active Directory Data 69](#_Toc301517977)

[12.2.6 Unified Messaging Server 70](#_Toc301517978)

[12.2.7 Other 71](#_Toc301517979)

[13 Backup Process and Procedures 71](#_Toc301517980)

[13.1 VSS-based backups of Exchange data 71](#_Toc301517981)

[13.1.1 Use Windows Server Backup to Perform a Backup of Exchange 73](#_Toc301517982)

[13.2 Exchange Native Data Protection 74](#_Toc301517983)

[13.2.1 Mailbox Resiliency 74](#_Toc301517984)

[13.2.2 Single Item Recovery 76](#_Toc301517985)

[13.2.3 Single Page Restore 76](#_Toc301517986)

[13.2.4 Calendar Repair 76](#_Toc301517987)

[13.2.5 Mailbox Moves 77](#_Toc301517988)

[13.2.6 New-MailboxRepairRequest 77](#_Toc301517989)

[13.2.7 Personal Archive 78](#_Toc301517990)

[14 Recovery Process and Procedures 78](#_Toc301517991)

[14.1 Client Access Server 78](#_Toc301517992)

[14.1.1 Server Failure: Hardware 78](#_Toc301517993)

[14.1.2 Server Failure: Software 78](#_Toc301517994)

[14.1.3 Non Recoverable Failure 79](#_Toc301517995)

[14.1.4 Site Failure 79](#_Toc301517996)

[14.2 Hub Transport Server 79](#_Toc301517997)

[14.2.1 Server Failure: Hardware 80](#_Toc301517998)

[14.2.2 Server Failure: Software 80](#_Toc301517999)

[14.2.3 Non Recoverable Failure 80](#_Toc301518000)

[14.2.4 Site Failure 80](#_Toc301518001)

[14.3 Edge Transport Server 81](#_Toc301518002)

[14.3.1 Server Failure: Hardware 81](#_Toc301518003)

[14.3.2 Server Failure: Software 81](#_Toc301518004)

[14.3.3 Non Recoverable Failure 81](#_Toc301518005)

[14.3.4 Site Failure 81](#_Toc301518006)

[14.4 Mailbox Server 82](#_Toc301518007)

[14.4.1 Lost Mail Item 82](#_Toc301518008)

[14.4.2 Lost Mailbox 85](#_Toc301518009)

[14.4.3 Lost Database or Logs 87](#_Toc301518010)

[14.4.4 Lost Server 87](#_Toc301518011)

[14.4.5 Lost Site 88](#_Toc301518012)

[15 How to Guides 92](#_Toc301518013)

[15.1 Recover an Exchange Server 92](#_Toc301518014)

[15.2 Recover a Database Availability Group Member Server 92](#_Toc301518015)

[15.3 Shadow Redundancy 94](#_Toc301518016)

[15.4 Working with the Queue Database on Transport Servers 94](#_Toc301518017)

[15.5 Edge Transport Server Cloned Configuration 95](#_Toc301518018)

[15.6 Disk Full on Exchange Log Drive 96](#_Toc301518019)

[15.7 Rebuild the Full-Text Index Catalog 96](#_Toc301518020)

[15.8 Restore Data Using a Recovery Database 96](#_Toc301518021)

[15.9 Database Portability 98](#_Toc301518022)

[15.10 Dial Tone Portability 99](#_Toc301518023)

[15.11 Use Windows Server Backup to Restore a Backup of Exchange 100](#_Toc301518024)

[15.12 Rebuild an Entire Database Availability Group 101](#_Toc301518025)

[15.13 Seeding a Mailbox Database Copy 104](#_Toc301518026)

[15.14 Restoring Service to the Primary Datacenter 106](#_Toc301518027)

[15.15 Database Availability Group, (DAG) Disaster Recovery 108](#_Toc301518028)

[1. Prepare Active Directory for the Introduction of Servers with the Same Name 109](#_Toc301518029)

[2. Prepare the DAG's Cluster Name Object 110](#_Toc301518030)

[3. Remove the Database Copies from the DAG 110](#_Toc301518031)

[4. Remove the Mailbox Servers from the DAG 110](#_Toc301518032)

[5. Build Replacement Mailbox Servers 111](#_Toc301518033)

[6. Recover each DAG Member 111](#_Toc301518034)

[7. Restore and/or Mount Mailbox Databases 112](#_Toc301518035)

[8. Add Mailbox Servers to the DAG 112](#_Toc301518036)

[9. Add Mailbox Database Copies to the DAG 112](#_Toc301518037)

[2. Disaster Recovery procedure for Standalone server 114](#_Toc301518038)

[15. Server and Database Operations 116](#_Toc301518039)

[1. Databases 116](#_Toc301518040)

[1. Check the database copies status 116](#_Toc301518041)

[2. Activate the initial database copies 116](#_Toc301518042)

[3. Failback – Resume database copy 117](#_Toc301518043)

[4. Log Truncation 118](#_Toc301518044)

[5. Dismount a database 119](#_Toc301518045)

[6. Mount a database 119](#_Toc301518046)

[2. Maintenance 120](#_Toc301518047)

[1. Activate Maintenance mode 120](#_Toc301518048)

[2. Back from maintenance 120](#_Toc301518049)

[3. Suspend a DAG node 121](#_Toc301518050)

[4. Witness Server 121](#_Toc301518051)

[3. Transport 122](#_Toc301518052)

[1. Disable Receive connectors 122](#_Toc301518053)

[2. Enable Receive connectors 122](#_Toc301518054)

[3. Check HUB queues 122](#_Toc301518055)

[16. Monitoring Exchange Database Information and Statistics 122](#_Toc301518056)

[1. Viewing Mailbox Statistics 122](#_Toc301518057)

[2. Monitoring Resource Usage 123](#_Toc301518058)

[3. Using Performance Monitor Counters 124](#_Toc301518059)

[4. Obtaining Information about Public Folder Databases 125](#_Toc301518060)

[5. Viewing Public Folder Statistics 125](#_Toc301518061)

[6. Viewing Mailbox Database Replication Health 126](#_Toc301518062)

[7. Verifying Success of Database Backups 127](#_Toc301518063)

[8. Monitoring Background Database Maintenance 128](#_Toc301518064)

[17. Unified Messaging 129](#_Toc301518065)

[1. Standard Procedures 129](#_Toc301518066)

[2. Unified Messaging Availability 130](#_Toc301518067)

[1. Load Balancing and Redundancy; How does UM failover work? 130](#_Toc301518068)

[3. Unified Messaging Redundancy and Timeouts (EXUMROUTING) 135](#_Toc301518069)

[Exumrouting.exe.config File 136](#_Toc301518070)

[4. Network Traffic 138](#_Toc301518071)

[5. Monitoring Server Performance 140](#_Toc301518072)

[1. Using Performance Monitor Counters 140](#_Toc301518073)

[6. Synthetic Transactions 141](#_Toc301518074)

[18. Edge Transport Server 141](#_Toc301518075)

[1. Create a new Edge Subscription 141](#_Toc301518076)

[2. Retrieve the properties of existing Edge Subscriptions 142](#_Toc301518077)

[3. Remove an Edge Subscription 143](#_Toc301518078)

[4. Starting synchronization through an Edge Subscription 143](#_Toc301518079)

[5. Testing the Edge Synchronization 144](#_Toc301518080)

[6. Creating the configuration for the EdgeSync service 144](#_Toc301518081)

[7. Setting the configuration for the EdgeSync service 145](#_Toc301518082)

[8. Retrieve the configurations created for the EdgeSync service 146](#_Toc301518083)

[19. Public Folders 146](#_Toc301518084)

[20. Appendix – Operations Checklists for Unified Messaging 150](#_Toc301518085)

[1. Daily Operations Checklist for Unified Messaging 150](#_Toc301518086)

[2. Weekly Operations Checklist 151](#_Toc301518087)

[3. Monthly Operations Checklist for Unified Messaging 152](#_Toc301518088)

[21. Appendix - Operations Checklists 153](#_Toc301518089)

[1. Daily Operations Checklist 153](#_Toc301518090)

[2. Weekly Operations Checklist 155](#_Toc301518091)

[3. Monthly Operations Checklist 155](#_Toc301518092)

[4. Summary Checklist 156](#_Toc301518093)

[5. Exchange permissions 157](#_Toc301518094)

[1. Mailbox Permission 157](#_Toc301518095)

[2. Calendar and Sharing Permissions 158](#_Toc301518096)

[3. Resource Mailbox Configuration Permissions 158](#_Toc301518097)

[4. Address List Permissions 158](#_Toc301518098)

[5. Mailbox Database Permissions 158](#_Toc301518099)

[6. Recipient Provisioning Permissions 159](#_Toc301518100)

[7. Transport Permissions 160](#_Toc301518101)

[8. Client Access Server Permissions 161](#_Toc301518102)

[9. Exchange ActiveSync Permissions 162](#_Toc301518103)

[10. Exchange Web services permissions 162](#_Toc301518104)

[11. Outlook Web App Permissions 162](#_Toc301518105)

[12. Database Availability Group Permissions 163](#_Toc301518106)

[13. Mailbox Database Copy Permissions 163](#_Toc301518107)

[22. Operation Powershell Scripts 164](#_Toc301518108)

[TechNet Script Center Repository - Exchange 2010 164](#_Toc301518109)

# Introduction

This document describes in details how to manage and operate Exchange 2010 SP1 infrastructure deployed in XYZ Company. It also describes about the day-to-day exploitation of the Exchange servers in production. This document will be used for the administration, management for XYZ’s<company> platform.

## Audience

This document has been prepared for a technical audience and is intended for personnel associated with <Company> IT operation team that are involved in the Microsoft Exchange Server 2010 deployment, day-to-day operation and periodic maintenance and main principal administration tasks.

The administrator should have working knowledge of Windows Server 2008 R2 concepts, Exchange 2010 SP1 concepts, the Exchange Management Console and Exchange Management Shell, the command line, and various system utilities. This document does not elaborate on the details of any system utility except as necessary to complete the tasks within.

# Operations Management and Monitoring of an Exchange 2010 Organization

This document details the operational processes, tasks, and tools that are required to maintain an Exchange 2010 environment. It explains how the management of Exchange 2010 fits in with the overall Microsoft Operations Framework (MOF) model. It will help you design your operational management environment and give you the means to implement processes and procedures to keep your environment running smoothly.

Within a Microsoft Exchange Server 2010 organization, the procedures, roles, and responsibilities that are involved in operations should be formalized. You can use the Microsoft Operations Framework to help model your organization's formalization efforts. Implementing Exchange Server 2007 operations procedures according to the MOF processes requires:

 Understanding MOF   MOF is a collection of best practices, principles, and models that give you technical guidance about the management of IT projects such as daily Exchange Server 2010 operations. Following MOF guidelines will help you achieve mission-critical production system reliability, availability, supportability, and manageability for Microsoft products.

 Learning about best practices for Exchange organizations   It is recommended that you implement proven and practical procedures to manage an Exchange 2010 organization. Using the tried, tested, and documented methods of managing operations in your organization may be more efficient than developing your own methods.

 Separating operations into daily, weekly, and monthly processes   Document the operations tasks performed regularly in your company. Documenting how and when tasks are performed ensures that the information is preserved when operations staff change jobs or leave the company. New employees also benefit from this documentation because it helps them quickly learn how your IT department conducts its Exchange operations.

 Deploying the tools required for operating an Exchange 2010 organization   Many tools are available to help troubleshoot problems, automate tasks, and aid in the monitoring and maintenance of your Exchange 2010 environment. You can define a standard set of tools for your organization so the tasks performed by your operations team are performed accurately, efficiently, consistently, and in a controlled manner. You should also implement processes to track incidents and major configuration changes.

For more information, see the following sections:

 [Microsoft Operations Framework](#_Microsoft_Operations_Framework)

 [Operations Management](#_Operations_Management)

## Microsoft Operations Framework

The Microsoft Operations Framework (MOF) is a collection of process best practices from which you can design the procedures, controls, and roles required for the efficient operation of your IT infrastructure. MOF is based on the IT Infrastructure Library (ITIL), and it adds specificity for the Microsoft platform.

For additional information on MOF- <http://technet.microsoft.com/en-us/solutionaccelerators/dd320379.aspx>, and <http://technet.microsoft.com/en-us/library/cc506049.aspx>

# 

# Operations Management

Operations management involves the administration of an organization's infrastructure components and includes the day-to-day administrative tasks, both planned and on-demand, that are required to keep an IT system operating smoothly. Typically, operations management tasks are covered by written procedures. These procedures provide all support staff with the same standard tools and methods.

In a Microsoft Exchange Server 2010 environment, typical system administration tasks include creating mailboxes, backing up and archiving mailbox and public folder data, monitoring logs, maintaining and recovering mailboxes, and updating antivirus scanners.

## Standard Procedures

Several resources can help you define what standard procedures are required in your organization and how to perform them. For more information about how to administer your Exchange organization, see [Operations](http://technet.microsoft.com/en-us/library/bb124558.aspx). Because each organization is unique, you will have to customize and adapt these resources to suit your requirements.

Standard procedures will change, and documentation will occasionally need to be revised. As changes are made, your change management process should identify how each change is likely to affect how and when administrative tasks are performed. Use the change management function to update and control the documentation.

The tasks that need to be performed can generally be separated into the following general categories:

 [Daily Tasks](#_Daily_Tasks)

 [Weekly Tasks](#_Weekly_Tasks)

 [Monthly Tasks](#_Monthly_Tasks)

 [As Needed Tasks](#_As_Needed_Tasks)

When preparing documentation for operations management, checklists are useful to help make sure that the required tasks are performed at the appropriate time. For detailed information about preparing operations checklists, see the sample checklists located in [Operations Checklists](#_Appendix_-_Operations).

Frequently, change management takes over where system administration finishes. If a task is covered by a standard procedure, it is part of the system administration function. If there is no standard procedure for a task, it should be handled using the change management function.

# Exchange 2010 Management

## Exchange Management Console

The ADUC (Active Directory Users and Computers) extensions have been removed since Exchange 2010 and with Exchange 2010 also to consolidate recipient management into a single, updated management interface. This was done for a number of reasons:

* Reduce time and complexity to manage users (add/delete/modify/move) by introducing automation. Since the Exchange 2010 recipient management tools are built on top of PowerShell cmdlets, Microsoft was able to introduce automation and a powerful bulk management solution.
* Truly supporting the split-permissions model where an Exchange Administrator can do everything relevant to Exchange within one console.
* Simplify the management of the GAL and recipient types from the Exchange console - only the objects and attributes that pertain to Exchange are shown.
* Make recipient types explicit, rather than implicit. Exchange 2010 has 13 different explicit recipient types and having these types differentiated makes it easier to manage recipients.

Note:

Exchange 2010 Administrators should use this tool to configure any Exchange specific functions like creating mailbox, creating DL, deleting mailbox and etc.

The following figure shows the main components of the Exchange 2010 Management Console:

**Console** **Result Pane** **Action Pane**

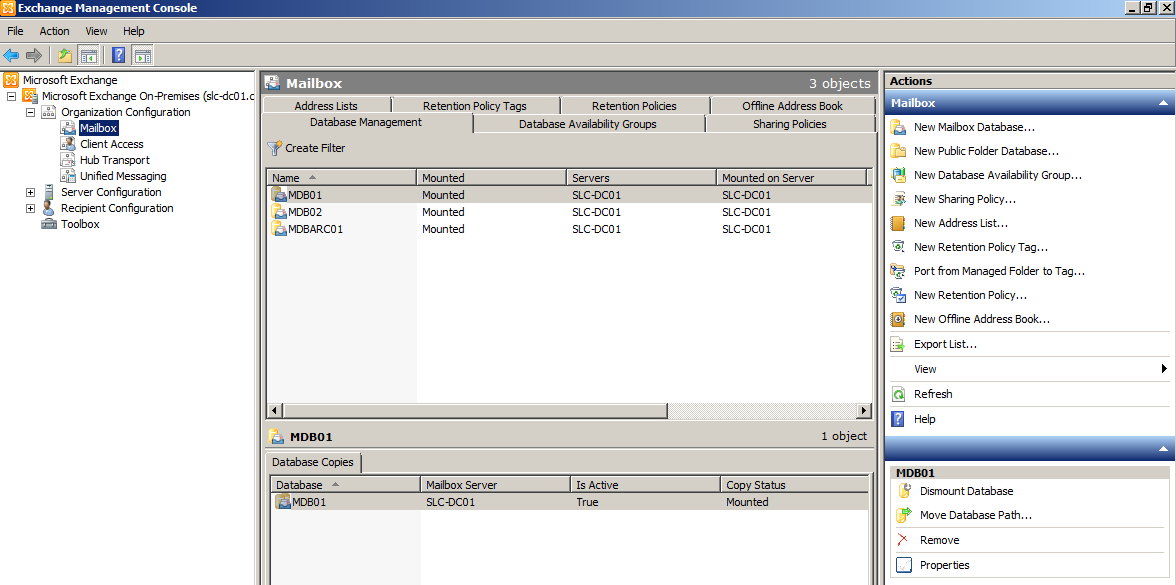


Figure 1 : Exchange 2010 Management Console

## Exchange Management Console Interoperability

The Exchange Management Console (EMC) is a Microsoft Management Console-(MMC) based tool that provides Exchange administrators with a GUI to manage the configuration of Exchange organizations. You can also add the Exchange Management Console snap-in to custom MMC-based tools. This topic discusses interoperability between the EMC in Exchange Server 2010 and earlier versions of Exchange, specifically Exchange Server 2003 and Exchange Server 2007.

For more information about the improvements to the Exchange Management Console, see [New Administrative Functionality in the Exchange Management Console](mk:@MSITStore:D:\My%20Documents\1MyDoc\Help_\Exchange%202010\Exch2010Help.chm::/html/18cc52a3-6d86-4384-b700-f6a209808cdf.htm).

### Interoperability with Exchange 2010

The Exchange Management Console (EMC) is available in both Exchange Server 2010 and Exchange Server 2007. The following lists the tasks and actions that can be performed using the EMC in either Exchange 2007 or Exchange 2010:

* Actions that create objects, such as new mailboxes or a new offline address book (OAB), can only be performed on a version of the EMC that's the same as the target object. For example, creating a mailbox on an Exchange 2010 Mailbox server must be performed with the EMC in Exchange 2010. The following applies:
  + Exchange 2010 Mailbox databases can't be managed from the EMC in Exchange 2007, although these databases can be viewed.
  + The EMC in Exchange 2007 can't enable or disable Exchange 2010 Unified Messaging mailboxes.
  + The EMC in Exchange 2007 can't manage Exchange 2010 mobile devices.
* Actions that require viewing of objects can be performed from any version of the EMC to any version of Exchange objects, with a few exceptions:
  + Exchange 2010 and Exchange 2007 transport rule objects can only be viewed from their corresponding version of the EMC.
  + Exchange 2010 and Exchange 2007 servers can only be viewed from their corresponding version of the EMC.
  + The Queue Viewer tool in the EMC in Exchange 2010 can't connect to an Exchange 2007 server to view queues or messages.

**Note**: If an Exchange 2007 object (such as a storage group) is no longer present in Exchange 2010, there's no interoperability expected or provided because Exchange 2010 isn't aware of the feature.

* You can't use message tracking configuration tasks between Exchange 2010 and Exchange 2007. You must use Exchange 2007 messaging tracking tools within your Exchange 2007 servers, and Exchange 2010 messaging tracking tools within your Exchange 2010 servers.

The following is a list of Exchange 2010-only and Exchange 2007-only objects. These objects are available for viewing, managing, and creating only in the corresponding version of the EMC.

**Note:** Be aware that managing an object in the Exchange 2010 Exchange Control Panel can upgrade the object. As a result, it can't be managed by the Exchange 2007 management tools (EMC, Shell) that created the object.

Exchange 2007 objects no longer present in Exchange 2010:

* Storage groups
* Exchange Administrators
* WebDAV

Exchange 2010 Management Console-only objects:

* Database availability group
* Certificate creation
* Database copies
* Federation trust
* Sharing relationships
* Sharing policies
* Microsoft Office Outlook Web App mailbox policies
* Customer Experience Program properties

### Side-by-Side Management Console

To use the side-by-side EMC feature, the Exchange 2007 EMC must first be installed on a non-Exchange administrative machine. After the Exchange 2007 EMC is installed, you can then install the Exchange 2010 EMC to run in a side-by-side scenario.

**Note:** Exchange 2010 EMC can only be administered from a 64-bit machine. Therefore, for side-by-side management, the Exchange 2007 EMC must be installed on a 64-bit machine. However, you can use 32-bit Windows PowerShell 2.0 and remotely access your Exchange 2010 environment.

For more information, see [Install the Exchange 2010 Management Tools](mk:@MSITStore:D:\My%20Documents\1MyDoc\Help_\Exchange%202010\Exch2010Help.chm::/html/71fcbe4c-783b-4f77-aabb-a21aa7a4ef23.htm).

## Exchange Management Shell

The Exchange Management Shell, built on Microsoft Windows PowerShell technology, formerly codenamed "Monad", provides a command-line interface and associated command-line plug-ins for Exchange Server that enable automation of administrative tasks. With the Exchange Management Shell, you can manage every part of Microsoft Exchange 2010. You can enable new e-mail accounts and configure SMTP connectors, store database properties, transport agents, and much more.

The Exchange Management Shell also provides a robust and flexible scripting platform that can reduce the complexity of current Microsoft Visual Basic scripts. Tasks that previously required many lines in Visual Basic scripts can now be done by using one line of code in the Exchange Management Shell.

The Exchange Management Shell provides this flexibility because it does not use text as the basis for interaction with the system, but uses an object model that is based on the Microsoft .NET platform. This object model enables the Exchange Management Shell cmdlets to apply the output from one command to subsequent commands when they are run. The below figure show the screen shot of the Exchange management shell

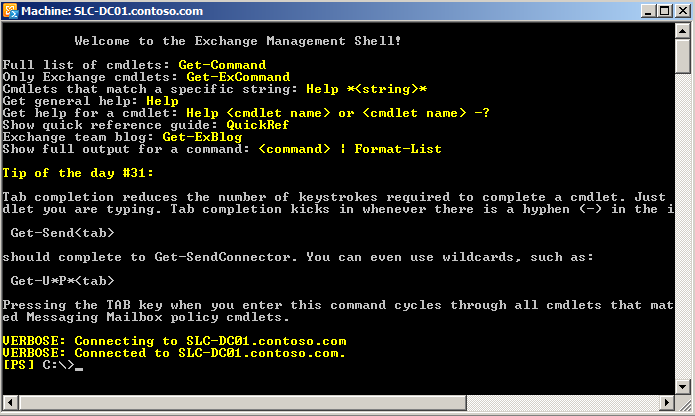


Figure 2 : Exchange Management Shell

Note:

The Exchange Management Shell can perform every task that can be performed by Exchange Management Console in addition to tasks that cannot be performed in Exchange Management Console.

When a task is performed in the Exchange Management Console, the same command is made available to the Exchange Management Shell. Exchange team can copy the command and modify further if they wanted to run through shell.

## Installation of the Exchange Management Tools

To have the most up to date information, please refer to <http://technet.microsoft.com/en-us/library/bb691354.aspx>

### Prerequisites

|  |  |
| --- | --- |
| **Operating System Requirement** |  |
| **Component** | **Requirement** |
| **Operating system (on a computer with 64bit processor)** | * 64-bit edition of Windows Server 2008 Standard or Enterprise with SP2. * 64-bit edition of Windows Server 2008 R2 Standard or Enterprise. |
| **Operating system for Management Tools (on a computer with 64bit processor)** | * Windows Vista with Service Pack 2 or later. * Windows 7. |

## Exchange Control Panel (ECP)

Microsoft Exchange 2010 provides new tools and management approaches to reduce help desk costs and to empower users. Role-based access control (RBAC) enables delegation based on job function. This allows administrators to provide users the ability to perform common tasks such as allowing compliance officers to perform multi-mailbox searches without granting full administrative privileges and without giving them access to the entire Exchange management interface.

Exchange 2010 also introduces the Web-based Exchange Control Panel (ECP). ECP gives users the power to manage distribution lists, track messages, and edit personal information tasks that represent a significant percentage of help desk calls in many organizations.

The improved Exchange Management Console (EMC) is based on Windows PowerShell 2.0, also known as Remote PowerShell, which allows administrators to run commands and cmdlets on remote computers.

All the Exchange management tools are RBAC-aware, so users have access only to features that are appropriate to their defined roles.

# Exchange 2010 permissions and delegations

Exchange 2010 includes a large set of predefined permissions, based on the Role Based Access Control (RBAC) permissions model, which you can use right away to easily grant permissions to your administrators and users. You can use the permissions features in Exchange 2010 so that you can get your new organization up and running quickly.

RBAC grants permissions to manage the Mailbox, Hub Transport, Client Access, and Unified Messaging server roles.

## RBAC

Role Based Access Control (RBAC) is the new permissions model in Exchange 2010. With RBAC, you don't need to modify and manage access control lists (ACLs), which was done in Exchange Server 2007. ACLs created several challenges in Exchange 2007, such as modifying ACLs without causing unintended consequences, maintaining ACL modifications through upgrades, and troubleshooting problems that occurred due to using ACLs in a nonstandard way.

RBAC enables you to control, at both broad and granular levels, what administrators and end-users can do. RBAC also enables you to more closely align the roles you assign users and administrators to the actual roles they hold within your organization. In Exchange 2007, the server permissions model applied only to the administrators who managed the Exchange 2007 infrastructure. In Exchange 2010, RBAC now controls both the administrative tasks that can be performed and the extent to which users can now administer their own mailbox and distribution groups.

RBAC has two primary ways of assigning permissions to users in your organization, depending on whether the user is an administrator or specialist user, or an end-user: management role groups and management role assignment policies. Each method associates users with the permissions they need to perform their jobs. A third, more advanced method, direct user role assignment, can also be used.

The following figure shows the components in RBAC and how they fit together:

* Role groups:
  + One or more administrators can be members of a role group. They can also be members of more than one role group.
  + The role group is assigned one or more role assignments. These link the role group with one or more administrative roles that define what tasks can be performed.
  + The role assignments can contain management scopes that define where the users of the role group can perform actions. The scopes determine where the users of the role group can modify configuration.
* Role assignment policies:
  + One or more users can be associated with a role assignment policy.
  + The role assignment policy is assigned one or more role assignments. These link the role assignment policy with one or more end-user roles. The end-user roles define what the user can configure on his or her mailbox.
  + The role assignments between role assignment policies and roles have built-in scopes that restrict the scope of assignments to the user's own mailbox or distribution groups.
* Direct role assignment (advanced):
  + A role assignment can be created directly between a user or USG and one or more roles. The role defines what tasks the user or USG can perform.
  + The role assignments can contain management scopes that define where the user or USG can perform actions. The scopes determine where the user or USG can modify configuration.

**RBAC overview**

As shown in the preceding figure, many components in RBAC are related to each other. It's how each component is put together that defines the permissions applied to each administrator or user.

### Management Role Group

A management role group is a universal security group (USG) used in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. A management role group simplifies the assignment of management roles to a group of users. All members of a role group are assigned the same set of roles. Role groups are assigned administrator and specialist roles that define major administrative tasks in Exchange 2010 such as organization management, recipient management, and other tasks. Role groups enable you to more easily assign a set of permissions to a group of administrators or specialist users.

The following are the layers that make up the role group model:

* **Role holder** A *role holder* is a mailbox that can be added as a member of a role group. When a mailbox is added as a member of a role group, the assignments that have been made between management roles and a role group are applied to the mailbox. This grants the mailbox all of the permissions provided by the management roles.
* **Management role group** The *management role group* is a special USG that contains mailboxes that are members of the role group. This is where you add and remove members, and it's also what management roles are assigned to. The combination of all the roles on a role group defines everything that users added to a role group can manage in the Exchange organization.
* **Management role assignment** A *management role assignment* links a management role and a role group. Assigning a management role to a role group grants members of the role group the ability to use the cmdlets and parameters defined in the management role. Role assignments can use management scopes to control where the assignment can be used.
* **Management role scope** A *management role scope* is the scope of influence or impact on a role assignment. When a role is assigned with a scope to a role group, the management scope targets specifically what objects that assignment is allowed to manage. The assignments, and its scope, are then given to the members of the role group, which restricts what those members can manage. A scope can be made up of lists of servers or databases, organizational units, or filters on server, database or recipient objects.
* **Management role** A *management role* is a container for a grouping of management role entries. Roles are used to define the specific tasks that can be performed by the members of a role group assigned the role.
* **Management role entries** *Management role entries* are the individual entries on a management role that provide access to cmdlets, scripts, and other special permissions that enable access to perform a specific task. Most often, role entries consist of a single cmdlet and the parameters that can be accessed by the management role, and therefore the role group to which the role is assigned.

The following figure shows each of the role group layers in the preceding list and how each of the layers relates to the other:

#### Built-in Role Groups

Exchange 2010 includes several management role groups by default. The following built-in role groups provide you with a preconfigured set of roles that you can assign to various administrator and specialist users in your organization:

|  |  |
| --- | --- |
| **Role group** | **Description** |
| [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) | Administrators who are members of the Organization Management role group have administrative access to the entire Exchange 2010 organization and can perform almost any task against any Exchange 2010 object. |
| [View-Only Organization Management](http://technet.microsoft.com/en-us/library/dd351130.aspx) | Administrators who are members of the View Only Organization Management role group can view the properties of any object in the Exchange organization. |
| [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) | Administrators who are members of the Recipient Management role group have administrative access to create or modify Exchange 2010 recipients within the Exchange 2010 organization. |
| [UM Management](http://technet.microsoft.com/en-us/library/dd351142.aspx) | Administrators who are members of the UM Management role group can manage the Unified Messaging (UM) features in the Exchange organization such as Unified Messaging server configuration, UM properties on mailboxes, UM prompts, and UM auto attendant configuration. |
| [Discovery Management](http://technet.microsoft.com/en-us/library/dd351080.aspx) | Administrators or users who are members of the Discovery Management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria. |
| [Records Management](http://technet.microsoft.com/en-us/library/dd633492.aspx) | Users who are members of the Records Management role group can configure compliance features, such as retention policy tags, message classifications, transport rules, and more. |
| [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) | Administrators who are members of the Server Management role group have administrative access to Exchange 2010 server configuration. They don't have access to administer Exchange 2010 recipient configuration. |
| [Help Desk](http://technet.microsoft.com/en-us/library/dd876949.aspx) | Users who are members of the Help Desk role group can perform limited recipient management of Exchange 2010 recipients. |
| [Hygiene Management](http://technet.microsoft.com/en-us/library/dd776125.aspx) | Administrators who are members of the Hygiene Management role group can configure the antivirus and anti-spam features of Exchange 2010. Third-party programs that integrate with Exchange 2010 can add service accounts to this role group to grant those programs access to the cmdlets required to retrieve and configure the Exchange configuration. |
| [Public Folder Management](http://technet.microsoft.com/en-us/library/dd876947.aspx) | Administrators who are members of the Public Folder Management role group can manage public folders and databases on Exchange 2010 servers. |
| [Delegated Setup](http://technet.microsoft.com/en-us/library/dd876881.aspx) | Administrators who are members of the Delegated Setup role group can deploy previously provisioned Exchange 2010 servers. |

### Built-in Management Roles

Exchange 2010 includes many management roles by default. The following roles are assigned to management role groups or management role assignment policies in various combinations that grant permissions to manage and use the features provided by Exchange 2010:

|  |  |
| --- | --- |
| **Built-in Management Roles** |  |
| Active Directory Permissions | MyDistributionGroupMembership |
| Address Lists | MyDistributionGroups |
| ApplicationImpersonation | MyMobileInformation |
| Audit Logs | MyName |
| Cmdlet Extension Agents | MyPersonalInformation |
| Database Availability Groups | MyProfileInformation |
| Database Copies | MyRetentionPolicies |
| Databases | MyTextMessaging |
| Disaster Recovery | MyVoiceMail |
| Distribution Groups | Organization Client Access |
| Edge Subscriptions | Organization Configuration |
| E-Mail Address Policies | Organization Transport Settings |
| Exchange Connectors | POP3 and IMAP4 Protocols |
| Exchange Server Certificates | Public Folder Replication |
| Exchange Servers | Public Folders |
| Exchange Virtual Directories | Receive Connectors |
| Federated Sharing | Recipient Policies |
| Information Rights Management | Remote and Accepted Domains |
| Journaling | Retention Management |
| Legal Hold | Role Management |
| Mail Enabled Public Folders | Security Group Creation and Membership |
| Mail Recipient Creation | Send Connectors |
| Mail Recipients | Support Diagnostics |
| Mail Tips | Transport Agents |
| Mailbox Import Export | Transport Hygiene |
| Mailbox Search | Transport Queues |
| Message Tracking | Transport Rules |
| Migration | UM Mailboxes |
| Monitoring | UM Prompts |
| Move Mailboxes | Unified Messaging |
| MyAddressInformation | Unscoped Management |
| MyBaseOptions | User Options |
| MyContactInformation | View-Only Audit Logs |
| MyDiagnostics | View-Only Configuration |
| MyDisplayName | View-Only Recipients |

Exchange 2010 uses the Role Based Access Control (RBAC) permissions model. This model consists of management role groups that are assigned one of a number of management roles. Management roles contain permissions that enable administrators to perform tasks in the Exchange organization. Administrators are added as members of the role groups and are granted all the permissions the roles provide. The following table provides an example of the role groups, some of the roles that they're assigned, and a description of the type of user who might be a member of the role group.

**Examples of role groups and roles in Exchange 2010:**

|  |  |  |
| --- | --- | --- |
| **Management role group** | **Management roles** | **Members of this role group** |
| **Organization Management** | The following are some of the roles assigned to this role group:   * Address Lists * Exchange Servers * Journaling * Mail Recipients * Public Folders | Users who need to manage the entire Exchange 2010 organization should be members of this role group. With some exceptions, members of this role group can manage nearly any aspect of the Exchange 2010 organization.  By default, the user account used to prepare Active Directory for Exchange 2010 is a member of this role group.  For more information about this role group, and for a complete list of roles assigned to this role group, see [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx). |
| **View Only Organization Management** | The following are the roles assigned to this role group:   * Monitoring * View-Only Configuration * View-Only Recipients | Users who need to view the configuration of the entire Exchange 2010 organization should be members of this role group. These users need to be able to view server configuration, recipient information, and be able to perform monitoring functions without the ability to change organization or recipient configuration.  For more information about this role group, see [View-Only Organization Management](http://technet.microsoft.com/en-us/library/dd351130.aspx). |
| **Recipient Management** | The following are the roles assigned to this role group:   * Distribution Groups * Mail Enabled Public Folders * Mail Recipient Creation * Mail Recipients * Message Tracking * Migration * Move Mailboxes * Recipient Policies | Users who need to manage recipients, such as mailboxes, contacts, and distribution groups in the Exchange 2010 organization, should be members of this role group. These users can create recipients, modify or delete existing recipients, or move mailboxes.  For more information about this role group, and for a complete list of roles assigned to this role group, see [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx). |
| **Server Management** | The following are some of the roles assigned to this role group:   * Databases * Exchange Connectors * Exchange Servers * Receive Connectors * Transport Queues | Users who need to manage Exchange server configuration, such as Receive connectors, certificates, databases, and virtual directories, should be members of this role group. These users can modify Exchange server configuration, create databases, and restart and manipulate transport queues.  For more information about this role group, and for a complete list of roles assigned to this role group, see [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx). |
| **Discovery Management** | The following are the roles assigned to this role group:   * Legal Hold * Mailbox Search | Users who need to perform searches of mailboxes to support legal proceedings or configure legal holds should be members of this role group.  This is an example of a role group that might contain non-Exchange administrators, such as personnel in your legal department. This allows legal personnel to perform their tasks without intervention from Exchange administrators.  For more information about this role group, and for a complete list of roles assigned to this role group, see [Discovery Management](http://technet.microsoft.com/en-us/library/dd351080.aspx). |

As shown in the previous table, Exchange 2010 provides a granular level of control over the permissions you grant to your administrators. You can choose from 11 role groups in Exchange 2010. For a complete list of role groups and the permissions they provide, see [Built-in Role Groups](http://technet.microsoft.com/en-us/library/dd351266.aspx).

Because of the number of role groups Exchange 2010 provides, and because further customization is possible by creating role groups with different role combinations, manipulating access control lists (ACLs) on Active Directory objects is no longer necessary and won't have any effect. ACLs are no longer used to apply permissions to individual administrators or groups in Exchange 2010. All tasks, such as an administrator creating a mailbox or a user accessing a mailbox, are managed by RBAC. RBAC authorizes the task and if it's allowed, Exchange performs the task on behalf of the user in the Exchange Trusted Subsystem universal security group. With some exceptions, all of the ACLs on objects in Active Directory that Exchange 2010 needs to access are granted to the Exchange Trusted Subsystem USG.

The permissions granted to a user in Active Directory are separate from the permissions granted to the user by RBAC when that user is using the Exchange 2010 management tools.

## RBAC model – needs to be sanitized and made generic

This chapter will describe the RBAC model and how to implement it.

### Naming convention

|  |  |  |
| --- | --- | --- |
| **Itemp** | **Defintion** | **Note** |
| **Role Group** | *ROLE-<GROUPNAMINGCONVENTION>* | *Role Group are special Universal Security Group dedicated for Exchange 2010 administration* |
| **Scope** | *SCOPE<OBJECT>-<ROLEGROUP>* | Scope defines the area in Active Directory and/or Exchange organization:  <OBJECT>= ***DB*** for database list scope or ***SRV*** for server list definition |

### Role groups and scopes definition

**Note**: The company’s central IT team must be member of “***Organization Management Role group***”. Apply this procedure to add member: <http://technet.microsoft.com/en-us/library/dd638143.aspx>

This table defines the role groups and scopes for CGGVeritas Exchange 2010 administration:

|  |  |  |  |
| --- | --- | --- | --- |
| **Role definition** | **<USG>(1)** | **<ROLES>** | **<SCOPE>** |
| **Company server Management** | ***<Company\_SRV-MGMT>*** | “Exchange Servers”  “Delegated Setup”  “Monitoring”  “Disaster Recovery”  “Receive Connectors”  “Mailbox Import Export”  “Mailbox Search”  “Message Tracking”  “Transport Queues” | All Exchange 2010 servers |
| **Company Recipient Management** | ***<Company-USER-MGMT>*** | “Mail Recipient Creation”  “Mail Recipients” | All Exchange 2010 server databases |

* + - 1. Universal Security Group must follow the Company’s naming convention.

<USG> and scope name are strings limited to 64 characters.

### Scope creation

**Important: The management scope will be created only for scope other than the *Organization***

1. Connect to an Exchange 2010 server with an account that is member of ***Organization Management role group***.
2. Launch an ***Exchange Management Shell*** console with *Run as administrator* privileges.
3. Execute these commands:

Set-ADServerSettings –ViewEntireForest $true

1. Create a custom scope with one of this command:
   1. Scope for ***databases***:

New-ManagementScope -Name *<SCOPEDB>* -DatabaseList *<DBLIST>*

Ignore warning about Exchange 2010 RTM.

***<DBLIST>***: list of databases separate by comma (*Ex: “EDV-DB01”, “EDV-DB02”, “EDV-AR01”*)

* 1. Scope for ***servers***:

New-ManagementScope -Name *<SCOPESRV>* -ServerList *<SRVLIST>*

***<SRVLIST>***: list of databases separate by comma (*Ex: “DB01”, “DB02”, “DB03”*)

### Role group creation

1. Connect to an Exchange 2010 server with an account that is member of ***Organization Management role group***.
2. Launch an ***Exchange Management Shell*** console with *Run as administrator* privileges.
3. Create Role group with this command:

New-RoleGroup -Name <USG> -Roles <ROLES> -CustomConfigWriteScope <SCOPE> - RecipientOrganizationalUnitScope “*internal.company.com/OU/OU*”

### Add role group member

1. Connect to an Exchange 2010 server with an account that is member of ***Organization Management role group***.
2. Launch an ***Exchange Management Shell*** console with *Run as administrator* privileges.
3. Execute these commands:

Add-RoleGroupMember "*<ROLEGROUP>*" -Member “*<USERLOGIN or UNIVERSALGROUP>”*

For more detail, refer to <http://technet.microsoft.com/en-us/library/dd638143.aspx>

### Example

1 – Create Company database scope:

New-ManagementScope –Name *SCOPE*-*Compnay-EXCHDB*-DatabaseList “*DB01”,* “*DB02”, ”DB03”, etc*

2 - Create Company server scope:

New-ManagementScope –Name *SCOPE*-*=Company-EXCHDB* -ServerList “*Servername”, ”Servername2”,* “*Servername3”, ” ServerName4”*

3 – Create role group for Company Helpdesk:

New-RoleGroup –Name *-Company-Provisioning* -Roles *“Mail Recipients”, “Mail Recipient Creation”, …,”Transport Queues”* -RecipientOrganizationalUnitScope “*int.company.com/org”* – CustomConfigWriteScope *SCOPE*-*Org-EXCHDB*

4 – Create role group for Company IT Support:

New-RoleGroup -Name *Company-ITSupport* -Roles “*Exchange Server*”*, “Delegated Setup”* -RecipientOrganizationalUnitScope *int.company.com/Org* – CustomConfigWriteScope *SCOPE-ORG-EXCHSRV*

5 – Add member in role groups:

Add-RoleGroupMember *Company-ITSupport* –Member *<USERLOGIN>*

Add-RoleGroupMember *Company-Helpdesk-Provisioning* –Member *<USERLOGIN>*

# Operations Management

Operations management involves the administration of an organization's infrastructure components and includes the day-to-day administrative tasks, both planned and on-demand, that are required to keep an IT system operating smoothly. Typically, operations management tasks are covered by written procedures. These procedures provide all support staff with the same standard tools and methods.

In an Exchange 2010 environment, typical system administration tasks include creating mailboxes, Deleting mailboxes, Creating DL, monitoring logs, maintaining and recovering mailboxes, updating antivirus scanners and etc.

## Managing Mailboxes

Use the Recipient Configuration node for a variety of recipient management tasks. Specifically, for the recipients in Exchange 2010 organization, create new recipients and manage existing mailboxes, mail contacts, mail users and distribution groups.

In Exchange 2010, recipients are comprised of mailbox users, mail-enabled users, mail contacts, distribution groups, mail enabled security groups and dynamic distribution groups.

In Exchange 2010, to perform these management tasks in both the Exchange Management Console and the Exchange Management Shell.

To perform any recipient’s operations tasks, the account must be delegated to the following group by using RBAC tool: https://mail<site>.Company.com/ECP

* Exchange Recipient Management

The Recipient Configuration node contains the following sub-nodes:

* ***Mailbox***: Use the Mailbox node to manage mailbox users and resource mailboxes. Resource mailboxes include room and equipment mailboxes. To create new mailboxes and remove, disable, or move existing mailboxes.
* ***Distribution Group***: Use the Distribution Group node to manage mail-enabled distribution groups (which include security groups) and dynamic distribution groups. To create new distribution groups, and remove, disable, or configure existing distribution groups.
* ***Mail Contact***: Use the Mail Contact node to manage mail contacts. To create new mail contacts and delete or configure existing mail contacts.
* ***Disconnected Mailbox***: Use the Disconnected Mailbox node to view and connect disabled mailboxes. Disconnected mailboxes are retained based on the configured mailbox database limits. Note that only the mailboxes that have been disconnected within the retention period that is specified for the mailbox database.

### Create a Mailbox for a New User

|  |  |
| --- | --- |
| **Prerequisites**: |  |
| **Built-in Exchange 2010 Role required** | Mail Recipient Creation Role |
| **Scope** | Target Organizational Unit, target Mailbox database |
| **Execute on** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup) or an Exchange Server 2010 SP1 |
| **Domain** | Domain in which the mailbox account will be hosted |

#### Using Exchange Management Console

Refer to <http://technet.microsoft.com/en-us/library/bb123809.aspx>

1. Connect to an Exchange 2010 server or from workstation with Exchange Management Tools.
2. Launch an ***Exchange Management Console*** with *Run as administrator* privileges.
3. In the console tree, click **Recipient Configuration**.
4. Right-click on it or use the Action pane and click **New Mailbox**.
5. On the **Introduction** page, select one of the following option:
   * **User Mailbox**
6. On the **User Type** page, select one of the following options:
   * **New User** Click this button to simultaneously create a new user in Active Directory and mail-enable the user.   
     If you click this button, you'll need to provide the required user account information on the **User Information** page of this wizard.
   * **Existing users** Click this button to mail-enable one or more existing users.  
     Click **Add** to open the **Select User** dialog box. This dialog box displays a list of user accounts in the forest that aren't mail-enabled or don't have Exchange mailboxes. Select the user accounts you want to mail-enable, and then click **OK** to return to the wizard.  
     To remove a user from the list, select the user name, and then click Remove icon.
7. If you selected **New User** in previous step, complete the following fields on the **User Information** page. Otherwise skip to next step:
   * **Specify the organizational unit rather than using a default one**: select this check box and click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**. The target organizational unit (OU) must be on the recipient scope defined by your role.
   * **First name** Use this box to type the first name of the user. This field is optional.
   * **Initials** Use this box to type the initials of the user. This field is optional.
   * **Last name** Use this box to type the last name of the user. This field is optional.
   * **Name**: type a name for the user with the format “***<Lastname>, <Firstname>***”.

**Note:** In Exchange 2010, the mailbox's alias is generated based on the Name property. Invalid characters in the name will be replaced with a question mark (?) when the alias is generated.

* + **User logon name (User Principal Name):** type the user login with the format “***<firstnameLetter><lastname>***”. This is the name that the user will use to log on to the mailbox.
  + **User logon name (pre-Windows 2000):** type the same as UPN (User Principal Name)field.
  + **Password:** type the password.
  + **Confirm password**: confirm the password
  + **User must change password at next logon**: check this box.

1. On the **Mailbox Settings** page, complete the following fields:
   * **Alias**: type the same string as the user login
   * **Specify the mailbox database rather than using a database automatically selected**: click **Browse** to open the **Select Mailbox Database** dialog box and select the target database and then click **OK**
   * **Retention policy** Select this check box to specify a retention policy for the mailbox. Based on the CGGVeritas policies, click **Browse** to open the **Select Retention Policy** dialog box and select the policy that must be apply to the user mailbox
   * **Exchange ActiveSync mailbox policy:** do not check
2. On the **Archive Settings** page, complete the following fields:
   * **Don't create an archive** Click this button if you don't want to create an archive for the mailbox.
   * **Create a local archive** Click this button if you want to add an archive mailbox for the mailbox. **Select a specific mailbox database rather than having one selected automatically** Select this check box and then click **Browse** to select a database that resides in the local forest.
3. On the **New Mailbox** page, review your configuration settings. To make any configuration changes, click **Back**. To create the new mailbox, click **New**.
4. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   * A status of **Completed** indicates that the wizard completed the task successfully.
   * A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

#### Using Exchange Management Shell Console

Launch ***Exchange Management Shell*** Console with Run as administrator privilege.

* ***Create a new user account with a new user account***

**New-Mailbox -Name '<LASTNAME>, <Firstname>' -Alias '<ALIAS>' -OrganizationalUnit '<OU>' -UserPrincipalName '<UPN>@int.cggveritas.com' -SamAccountName '<SAMACCOUNT>' -FirstName '<FIRSTNAME>' -LastName '<LASTNAME>' -Password (Get-Credential).Password -ResetPasswordOnNextLogon $true -Database '<DATABASE>'**

* ***Create a Mailbox for an Existing User***

**Enable-Mailbox -Identity '<LOGIN>' -Alias '<LOGIN>' -Database '<DATABASE>'**

### Create a Mailbox for a SHARED Mailbox

A shared mailbox is a mailbox to which multiple users can log on. This mailbox isn't associated with any of the users that can log on. It's associated with a disabled user account.

|  |  |
| --- | --- |
| Prerequisites: |  |
| **Built-in Exchange 2010 Role required** | [Mail](http://technet.microsoft.com/en-us/library/dd298028.aspx) Recipient Creation Role |
| **Scope** | Target Organizational Unit, target Mailbox database |
| **Execute on** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup) or an Exchange Server 2010 SP1 |
| **Domain** | Domain in which the mailbox account will be hosted |

**Note**: there is no option in the Management Console to directly create a Shared mailbox. The work around is to create a standard user mailbox and then disables account through Active Directory User and Computers console (dsa.msc).

Launch ***Exchange Management Shell*** Console with Run as administrator privilege:

***Step 1: Create the mailbox***

**New-Mailbox -Name ‘<LASTNAME>, <Firstname>’ *-Shared* -Alias <ALIAS> -DisplayName “<DISPLAYNAME>” [-ManagedFolderMailboxPolicy <MAILBOXPOLICYNAME>] -PrimarySmtpAddress *<SERVICENAME>@company.com* -OrganizationalUnit '<OU>' -UserPrincipalName '<UPN>@int.company.com' -SamAccountName '<SAMACCOUNT>' -FirstName '<FIRSTNAME>' -LastName '<LASTNAME>' -Password (Get-Credential).Password -ResetPasswordOnNextLogon $true -Database '<DATABASE>'**

**Note**: Parameters between “[ ]” are optional.

***Step 2: Allow Full mailbox access***

Important: In Exchange 2010 Service Pack 1 (SP1), Outlook 2007 and Outlook 2010 clients automatically map to any mailbox to which a user has Full Access permissions. If a user is granted Full Access permissions to another user's mailbox or to a shared mailbox, Autodiscover automatically loads all mailboxes to which the user has full access. If the user has full access to a large number of mailboxes, performance issues may occur when starting Outlook. For example, in some Exchange organizations, administrators have full access to all the mailboxes in the organization. In this case, upon starting, Outlook attempts to open all mailboxes in the organization. Users can’t control this behavior and have no way to turn it off.

Execute this command for each user (<LOGIN>) that you want to allow access:

Add-MailboxPermission "*<SHAREDMAILBOX\_ALIAS>*" -User "*<LOGIN>*" -AccessRights FullAccess

**Note**: Full Access or Receive As permissions aren't granted until the *Microsoft Exchange Information Store* service caches the permissions and updates the cache.

### Viewing existing Mailbox access rights

|  |  |
| --- | --- |
| Prerequisites: |  |
| **Built-in Exchange 2010 Role required** | [Mail](http://technet.microsoft.com/en-us/library/dd298028.aspx) Recipients Role |
| **Scope** | Organization or Organizational Unit |
| **Execute on** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup) or an Exchange Server 2010 SP1 |
| **Domain** | Domain in which the mailbox account is hosted |

Note: If you are connected on an Exchange 2010 server that is not on the same domain as the mailbox, you need to change the scope of search. By default, an Exchange server has its AD domain as scope.

To expand the scope executes this command:

Set-AdServerSetting –ViewEntireForest $True

To check the permission on a mailbox

**Get-MailboxPermission –Identity “*<IDENTITY>*” |FT user, accessrights**

### Add an E-mail address for a mailbox

|  |  |
| --- | --- |
| Prerequisites: |  |
| **Built-in Exchange 2010 Role required** | [Mail](http://technet.microsoft.com/en-us/library/dd298028.aspx) Recipients Role |
| **Scope** | Target Organizational Unit, target Mailbox database |
| **Execute on** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup) or an Exchange Server 2010 SP1 |
| **Domain** | Domain in which the mailbox account is hosted |

***Use Exchange Management Console***

1. Connect to an Exchange 2010 server or from workstation with Exchange Management Tools.
2. Launch an ***Exchange Management Console*** with *Run as administrator* privileges.
3. In the console tree, click **Recipient Configuration** 🡪 **Mailbox**
4. In the result pane, select the mailbox for which you want to add an e-mail address.
5. In the action pane, under the mailbox name, click **Properties**.
6. In **<MAILBOX> Properties**, click the **E-Mail Addresses** tab.
7. To create an e-mail address, under **E-mail Addresses**, click the arrow next to **Add** and select from the following address types:
   * **SMTP Address** This is the default address type. Click this button and use the corresponding dialog box to add an SMTP address.
   * **Custom Address** Click this button and use the corresponding dialog box to add a custom address (for example, fax or X500)

***User Exchange Management Shell console***

Launch ***Exchange Management Shell*** Console with Run as administrator privilege:

$Temp = Get-Mailbox -Identity *<SMTP>*

$Temp.EmailAddresses += ("*smtp:<SMTP@ADDRESS>*")

Set-Mailbox -Identity *<SMTP>* -EmailAddresses *$Temp.EmailAddresses*

### Disable a Mailbox

|  |  |
| --- | --- |
| Prerequisites: |  |
| **Built-in Exchange 2010 Role required** | [Mail](http://technet.microsoft.com/en-us/library/dd298028.aspx) Recipients Role |
| **Scope** | Target Organizational Unit, target Mailbox database |
| **Execute on** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup) or an Exchange Server 2010 SP1 |
| **Domain** | Domain in which the mailbox account is hosted |

***Using Exchange Management Console***

1. Connect to an Exchange 2010 server or from workstation with Exchange Management Tools.
2. Launch an **Exchange Management Console** with Run as administrator privileges.
3. In the EMC console, expand **Recipient Configuration**, and then click **Mailbox**.
4. In the result pane, select the mailbox user
5. In the action pane, click **Disable** option
6. On the warning that appears in the panel, click “Yes” and finish this task.

***Using Exchange Management Shell console***

Launch ***Exchange Management Shell*** Console with Run as administrator privilege:

**Get-Mailbox *<ACCOUNT>* | Disable-Mailbox**

Press [ENTER] to confirm with “Y” or choose another option

**WARNING**: **Do not** use the command ***Remove-Mailbox*** to disable mailbox because this command will also remove the Active Directory user account!

### Connect a Mailbox

|  |  |
| --- | --- |
| Prerequisites: |  |
| **Built-in Exchange 2010 Role required** | [Mail](http://technet.microsoft.com/en-us/library/dd298028.aspx) Recipient Creation Role |
| **Scope** | Target Organizational Unit, target Mailbox database |
| **Execute on** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup) or an Exchange Server 2010 SP1 |
| **Domain** | Domain in which the mailbox account will be hosted |

A disconnected mailbox is a mailbox object in the Microsoft Exchange store that is not associated with an Active Directory service user account.

Refer to <http://technet.microsoft.com/en-us/library/bb123490.aspx> to choose the best case that match to your situation.

#### Use Exchange Management Console

1. Connect to an Exchange 2010 server or from workstation with Exchange Management Tools.Launch an ***Exchange Management Console*** with Run as administrator privileges.
2. In the console tree, navigate to **Recipient Configuration** > **Disconnected Mailbox**.
3. In the result pane, select the disabled mailbox that you want to reconnect.
4. In the action pane, click **Connect**.
5. On the **Introduction** page, select the following type for the mailbox you're connecting:
   * **User Mailbox** Click this button to connect the mailbox as a mailbox owned by a user to send and receive e-mail messages.
6. On the **Mailbox Settings** page, configure the following settings:
   * **Matching User** Click this button to have Exchange locate a matching user object in Active Directory. Click **Browse** to open the **Select User** dialog box. If Exchange locates a matching user, it will appear in this dialog box. Select the user, and then click **OK**.   
     If Exchange can't find a matching user, you must click **Existing User**. To locate a user account that matches the mailbox object, Exchange uses the **LegacyExchangeDN** and **DisplayName** attributes of the Exchange store mailbox object.
   * **Existing User** Click this button if you want to connect the mailbox to a user other than the matching user. Click **Browse** to see a list of users available in Active Directory. The list contains only users that don't have an associated mailbox.
   * **Alias** Use this box to type an alias for the mailbox.
   * **Retention policy** Select this check box to specify a retention policy for the mailbox. Based on the CGGVeritas policies, click **Browse** to open the **Select Retention Policy** dialog box and select the policy that must be apply to the user mailbox
   * **Exchange ActiveSync mailbox policy:** do not check
7. On the **Connect Mailbox** page, review your configuration settings. Click **Connect** to associate the disconnected mailbox with the Active Directory user that you selected on the **Mailbox Settings** page. Click **Back** to make configuration changes.
8. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   * A status of **Completed** indicates that the wizard completed the task successfully.
   * A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

#### Use Exchange Management Shell Console

Launch ***Exchange Management Shell*** Console with Run as administrator privilege.

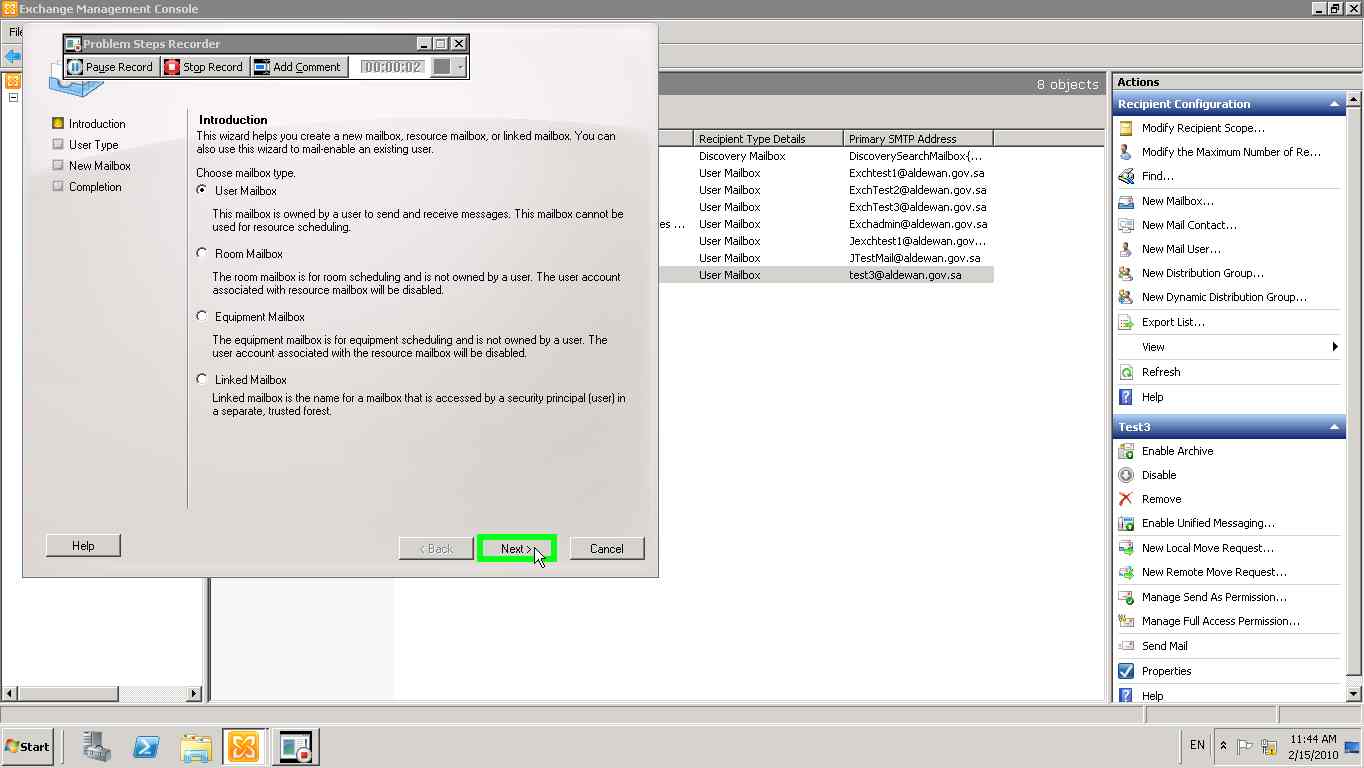
Connect-Mailbox -Identity "*<MAILBOX-NAME>*" -Database "*<TARGET-DB>*" -User "*<NEWOWNER-LOGIN>*"

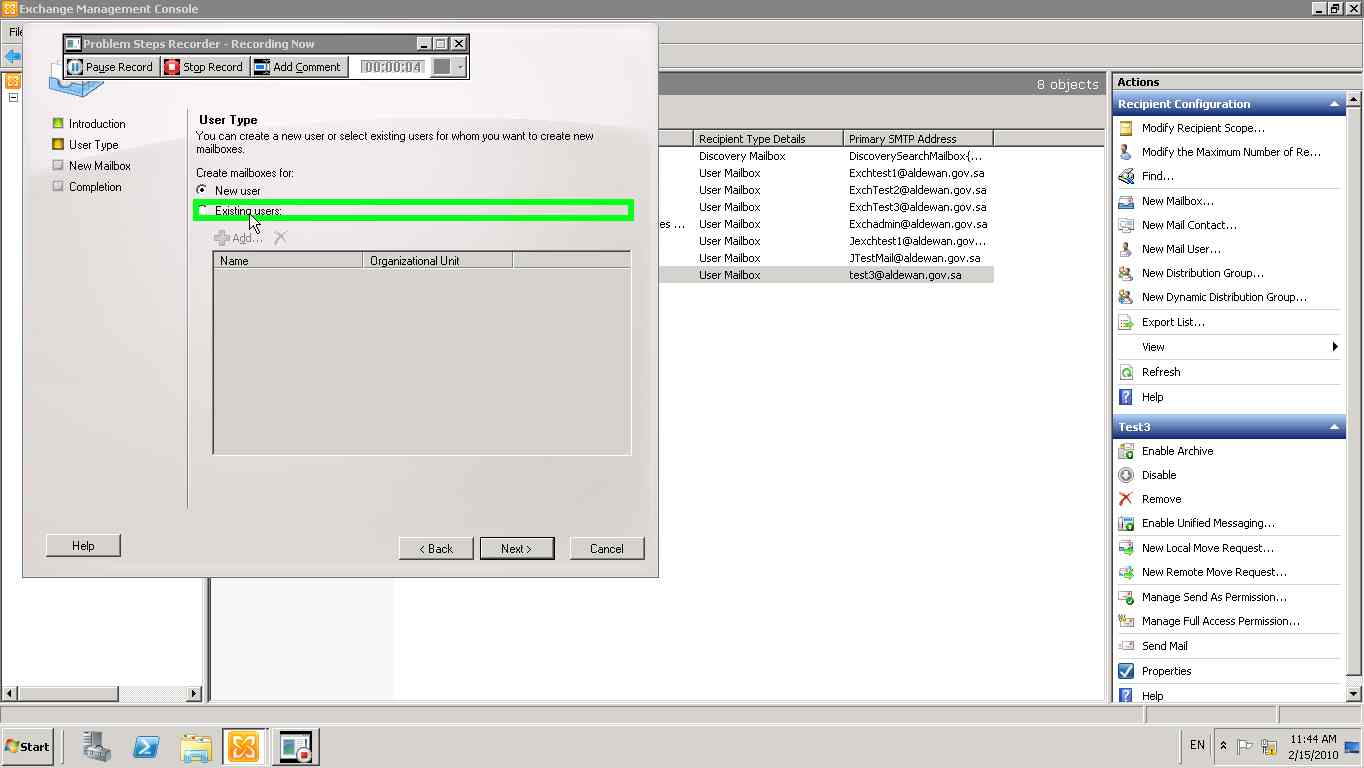
* + 1. Create a Mailbox for an Existing User

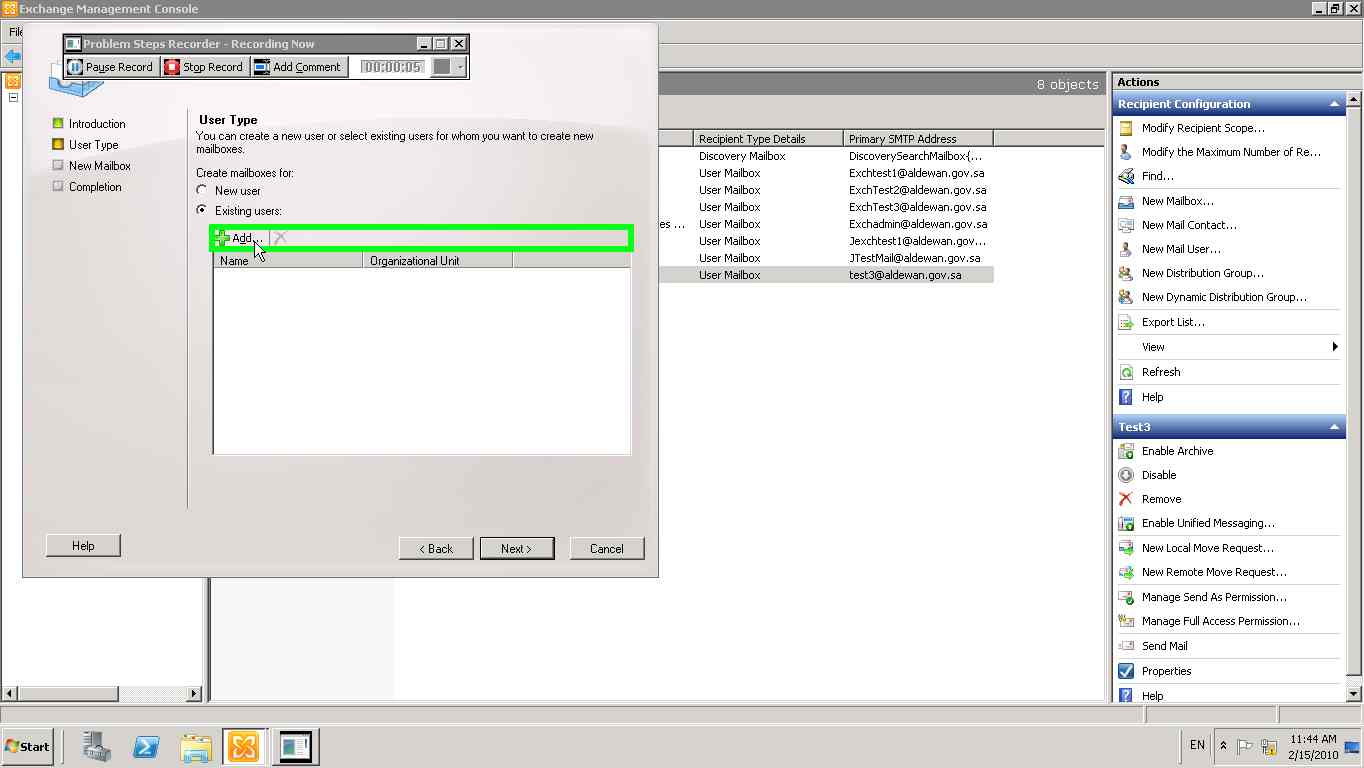
1. In the Exchange Management Console, click Recipient Configuration.
2. In the action pane, click New Mailbox. The New Mailbox wizard appears.
3. On the Introduction page, click User Mailbox, and then click Next.
4. On the User Type page, click Existing user, and then click Browse.
5. In the Select User dialog box, select the user that you want to create a new mailbox for, and then click OK.
6. On the User Type page, click Next.
7. On the Mailbox Settings page, complete the following fields:
   1. Alias: Type the User logon name (User Principal Name) of the user, the alias cannot exceed 64 characters and must be unique in the forest.
   2. Mailbox database: check the box “Specify the mailbox database rather than using database automatically selected” Click Browse to open the Select Mailbox Database dialog box. This dialog box lists all the mailbox databases in your Exchange organization. By default, the mailbox databases are sorted by name. You can also click the title of the corresponding column to sort the databases by storage group name or server name. Select the mailbox database you want to use, and then click OK.
   3. (Optional) Managed folder mailbox policy: To specify a messaging records management (MRM) policy, select this check box, and then click Browse to select the MRM mailbox policy to be associated with this mailbox. For example, use this option if you want this mailbox to adhere to an MRM policy such as the retention period for the mailbox data.
   4. (Optional) Exchange ActiveSync mailbox policy: To specify an Exchange ActiveSync mailbox policy, select this check box, and then click Browse to select the Exchange ActiveSync mailbox policy to be associated with this mailbox.
   5. (Optional) Archive Settings: To specify Archive mailbox and this is not planned for Contoso
8. On the New Mailbox page, review the Configuration Summary. This summary contains information about the options you have selected for the mailbox. To create the new mailbox, click New.
9. On the completion page, the summary states whether the mailbox was successfully created and displays the Exchange Management Shell command that was used to create the mailbox.
10. Click Finish to create the mailbox for the user.

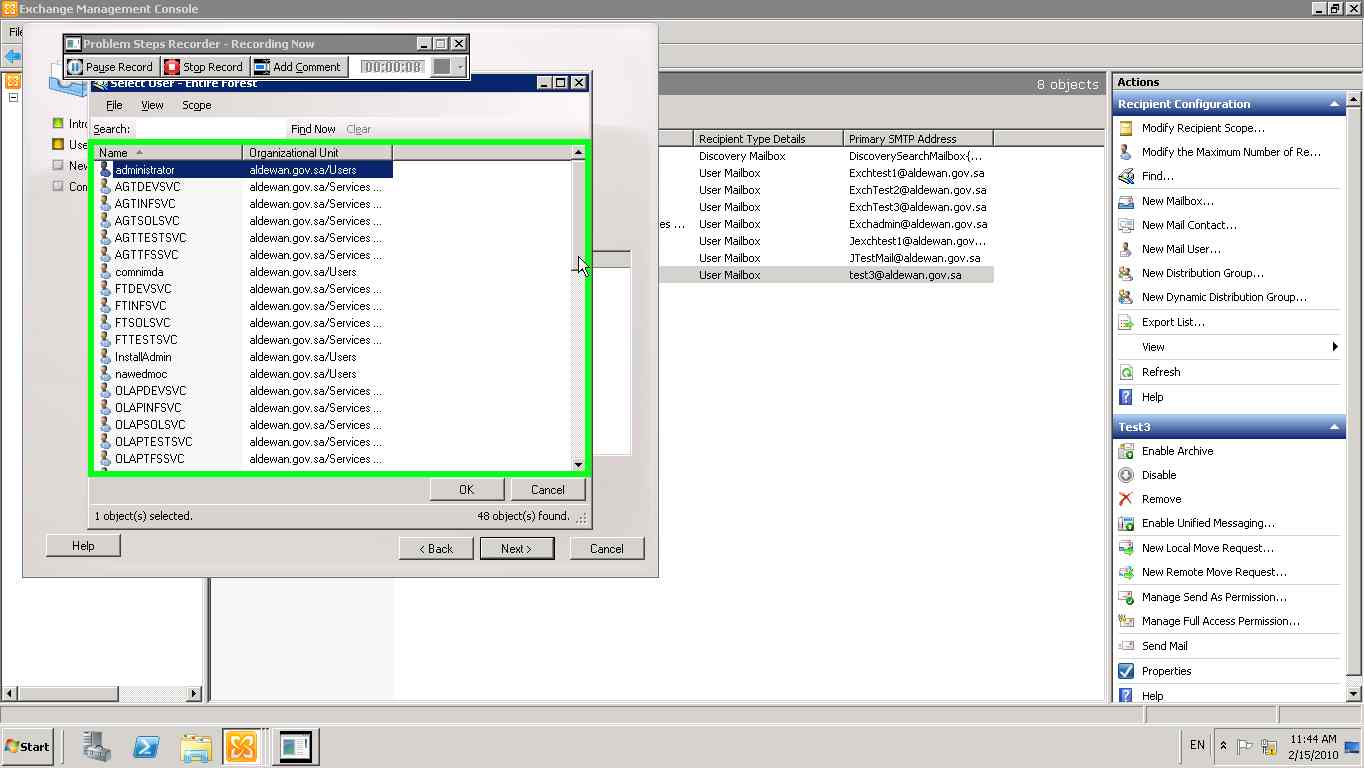
**Screen shots for New and Existing User**

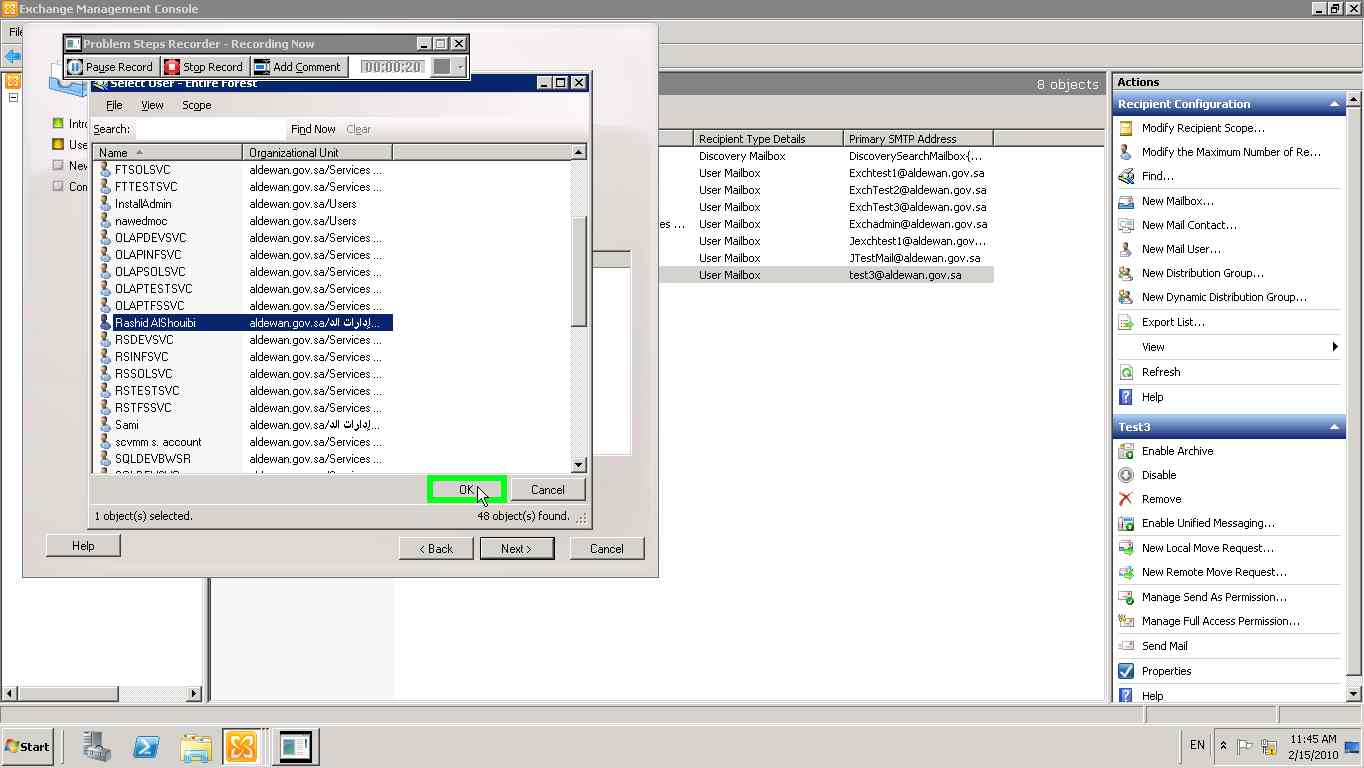
Existing User:

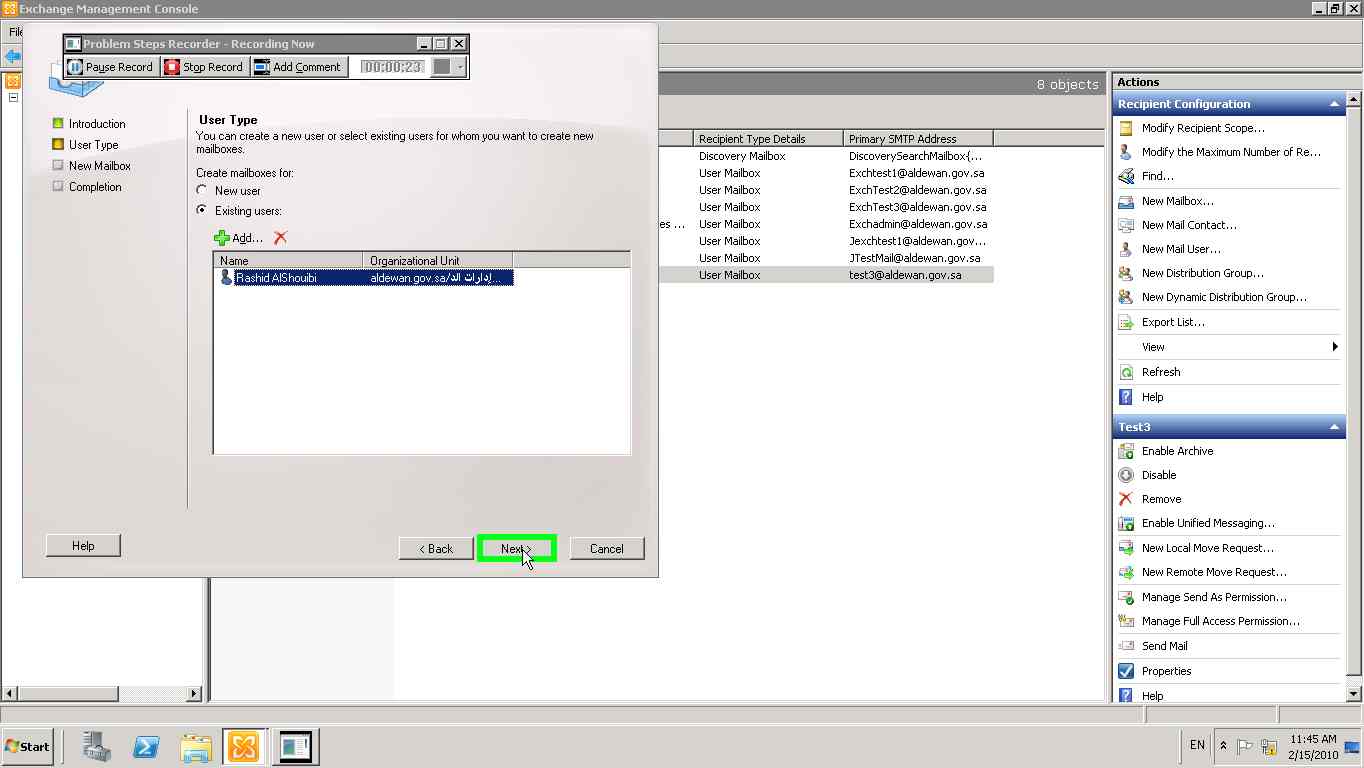
[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_newuser1.zip\Problem_20100215_1145.mht!screenshot_0002.jpeg)

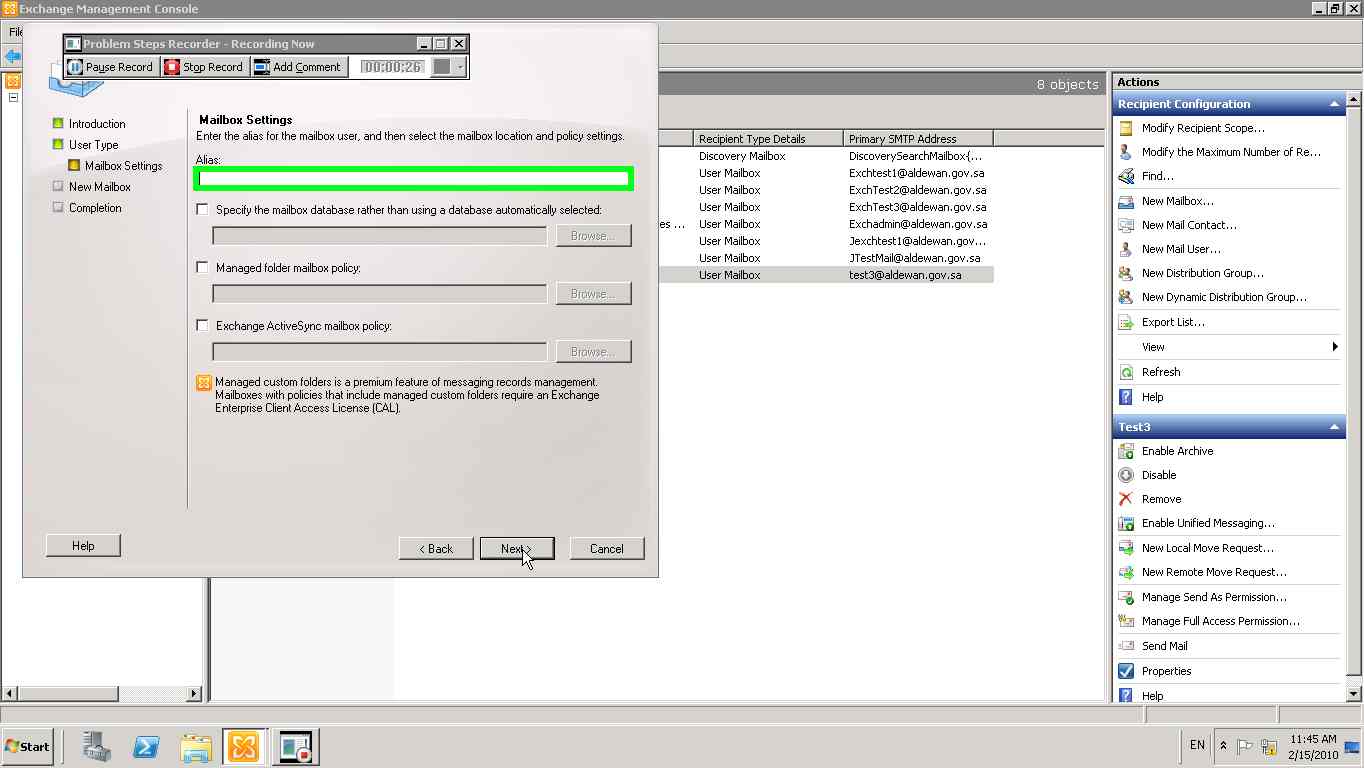
[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_newuser1.zip\Problem_20100215_1145.mht!screenshot_0003.jpeg)

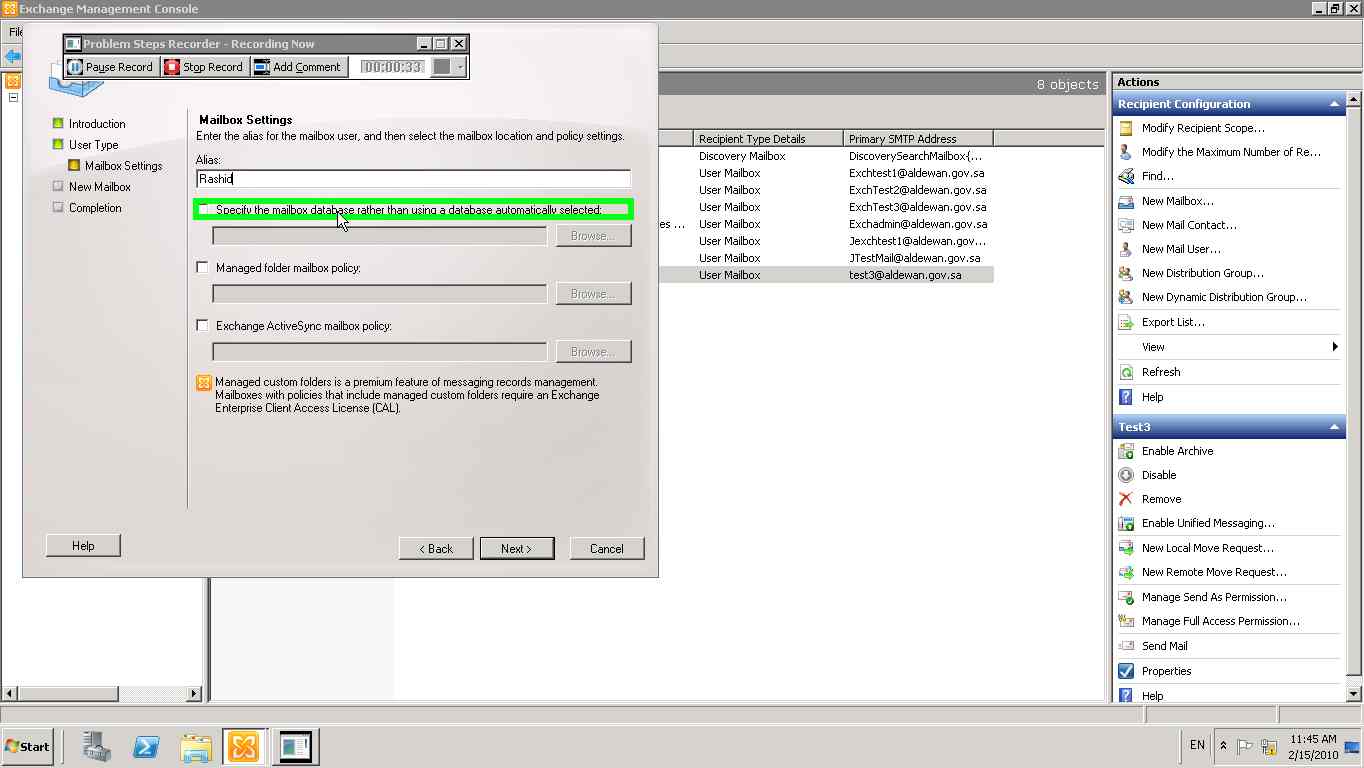
[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_newuser1.zip\Problem_20100215_1145.mht!screenshot_0004.jpeg)

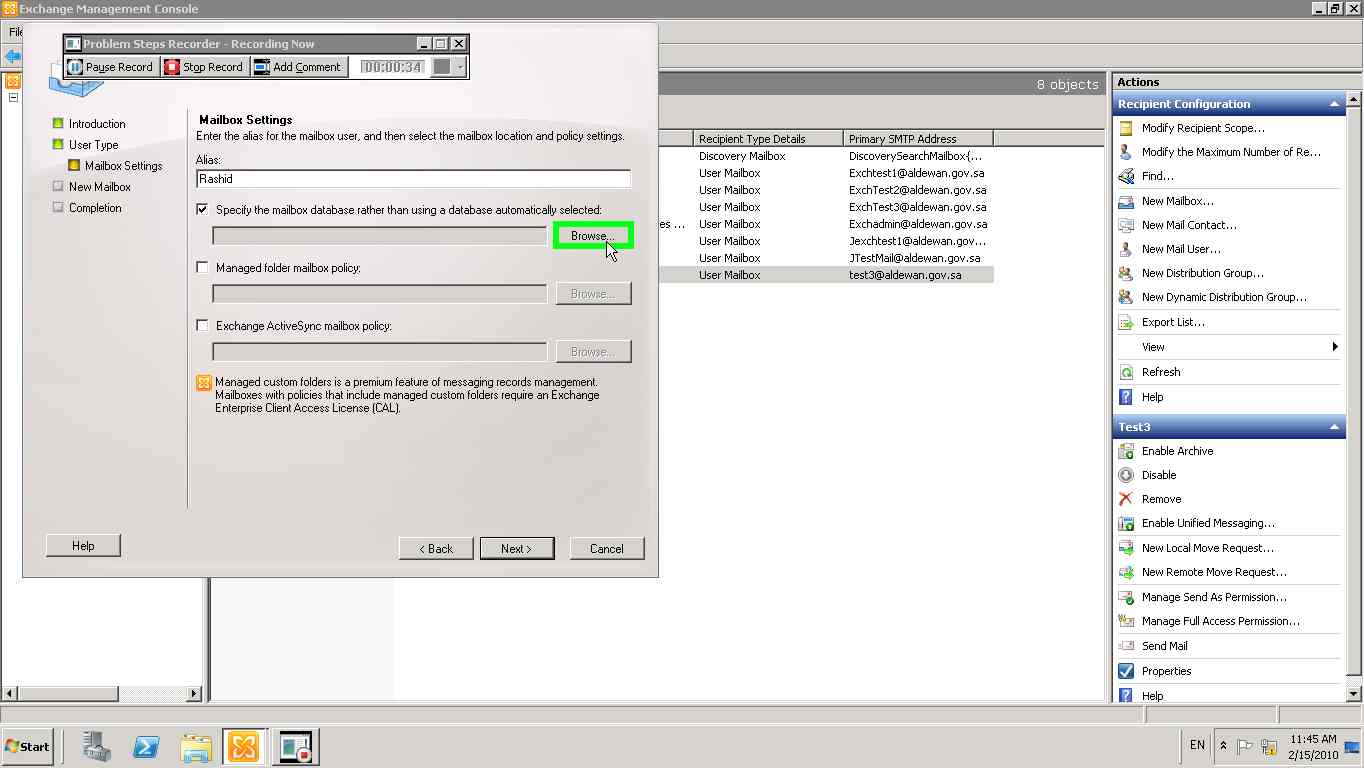
[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_newuser1.zip\Problem_20100215_1145.mht!screenshot_0005.jpeg)

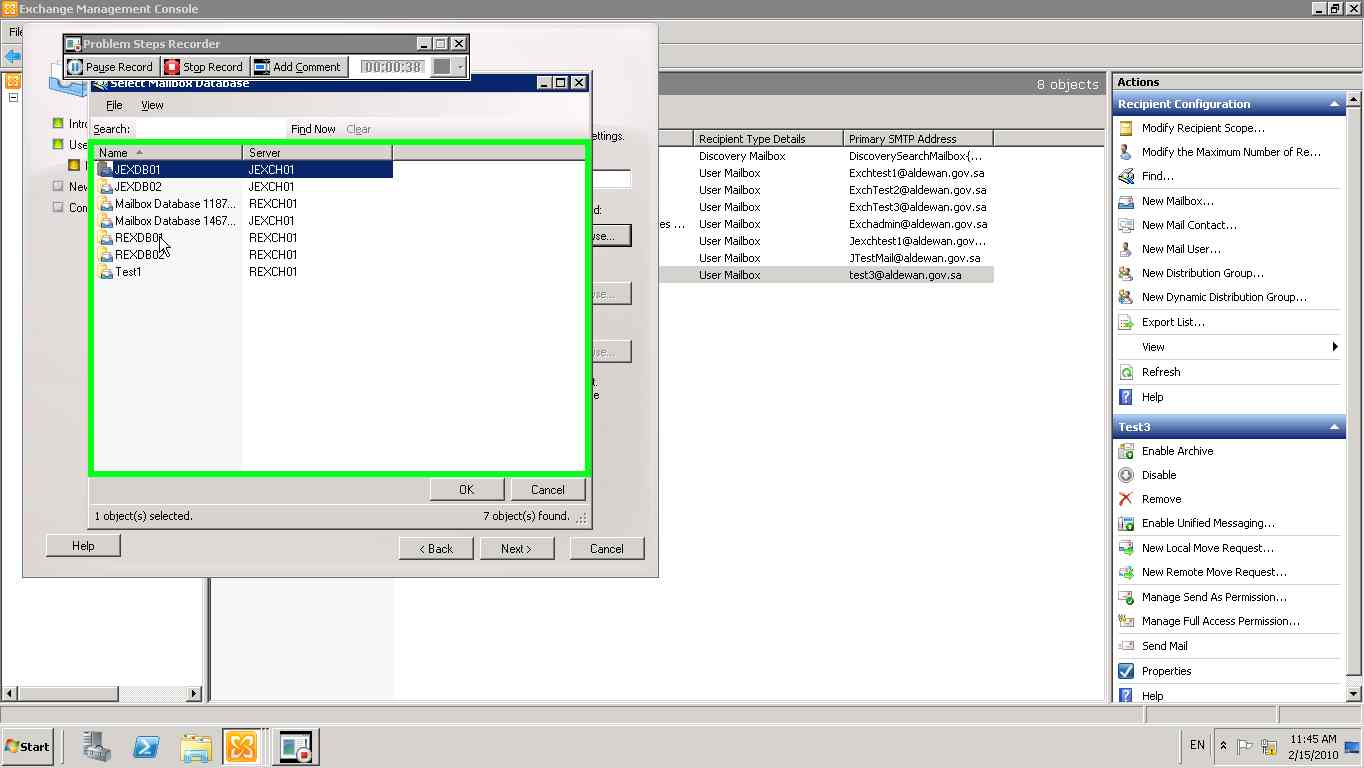
[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_newuser1.zip\Problem_20100215_1145.mht!screenshot_0011.jpeg)

[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_newuser1.zip\Problem_20100215_1145.mht!screenshot_0012.jpeg)

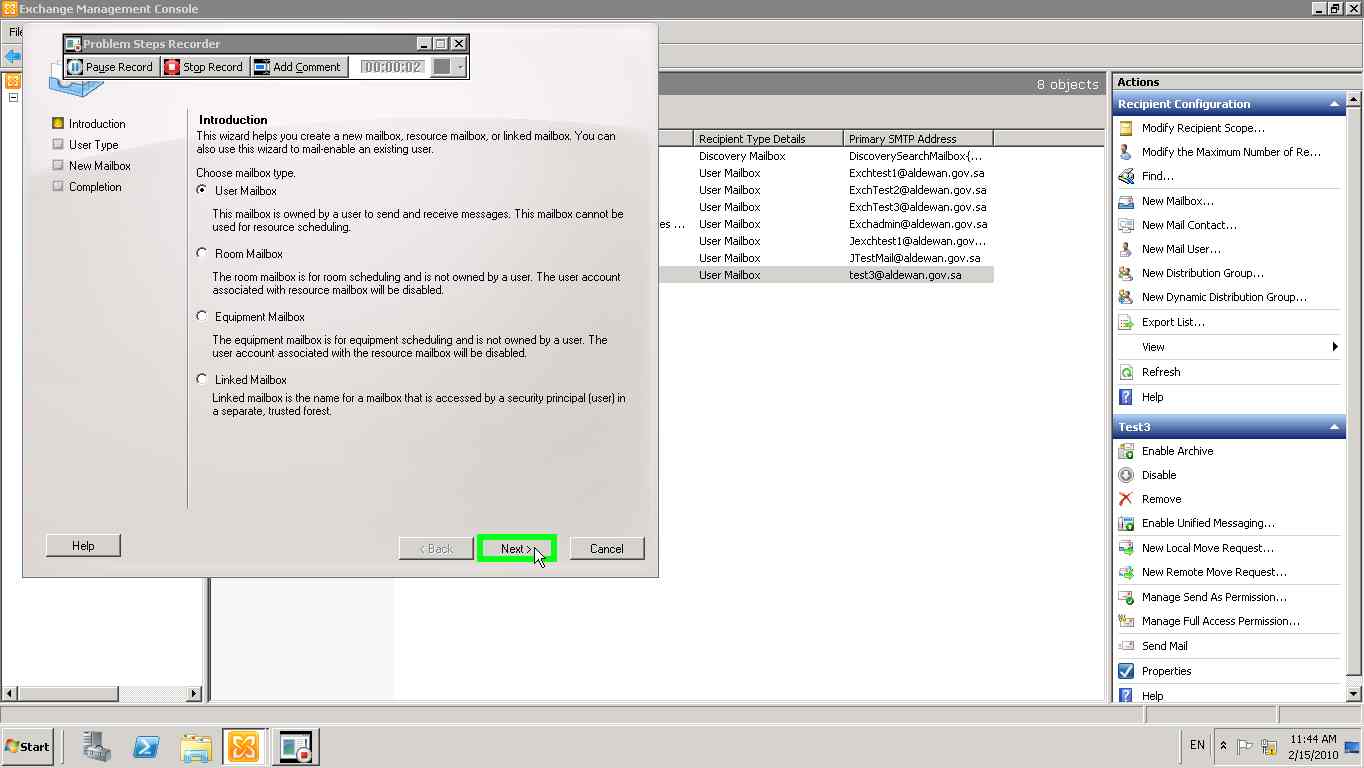
[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_newuser1.zip\Problem_20100215_1145.mht!screenshot_0013.jpeg)

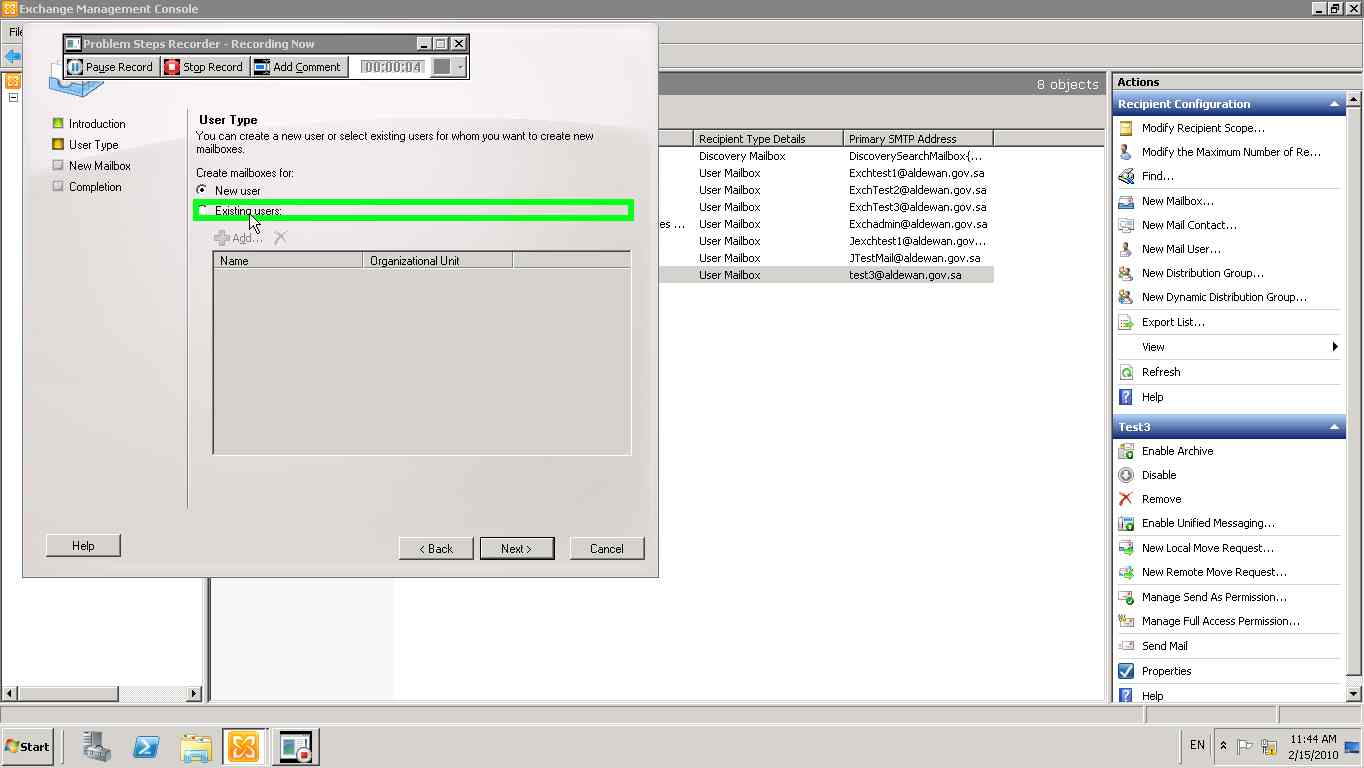
[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_newuser1.zip\Problem_20100215_1145.mht!screenshot_0014.jpeg)

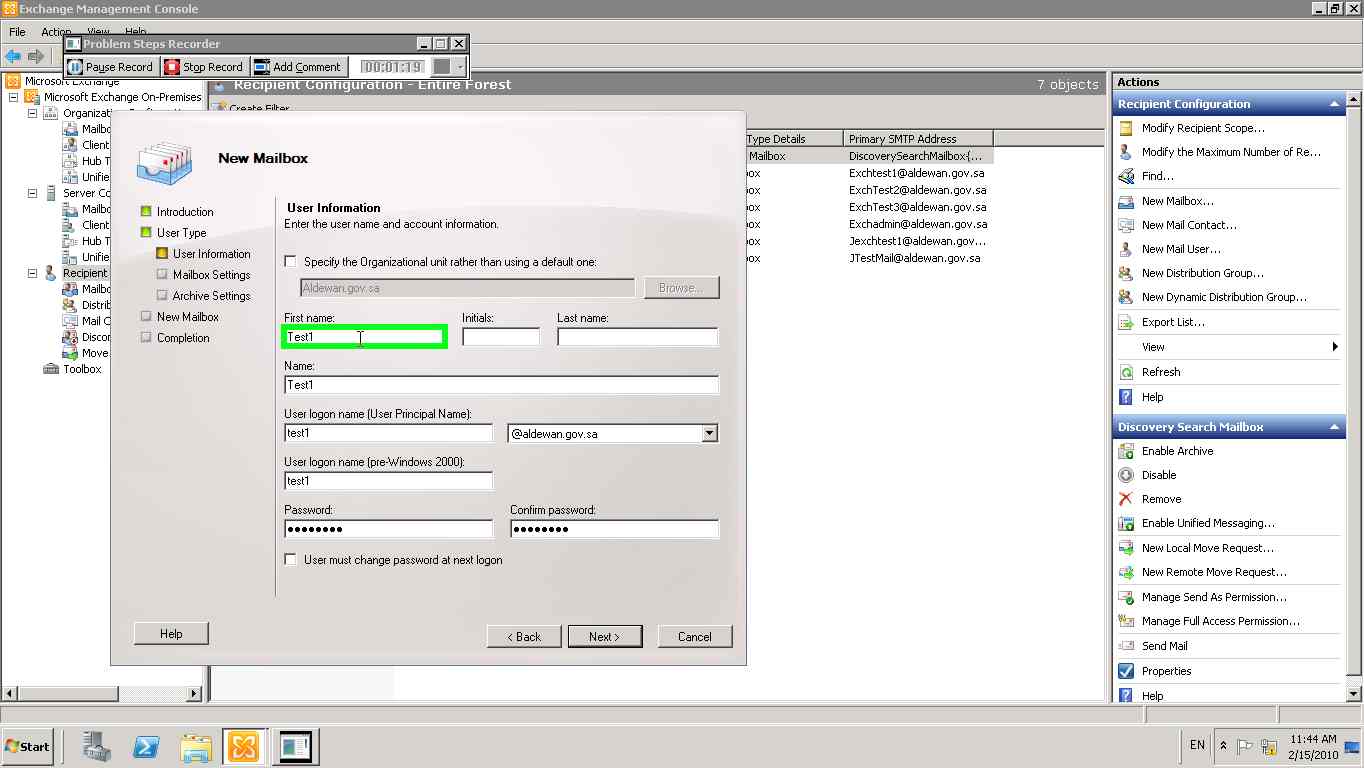
[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_newuser1.zip\Problem_20100215_1145.mht!screenshot_0015.jpeg)

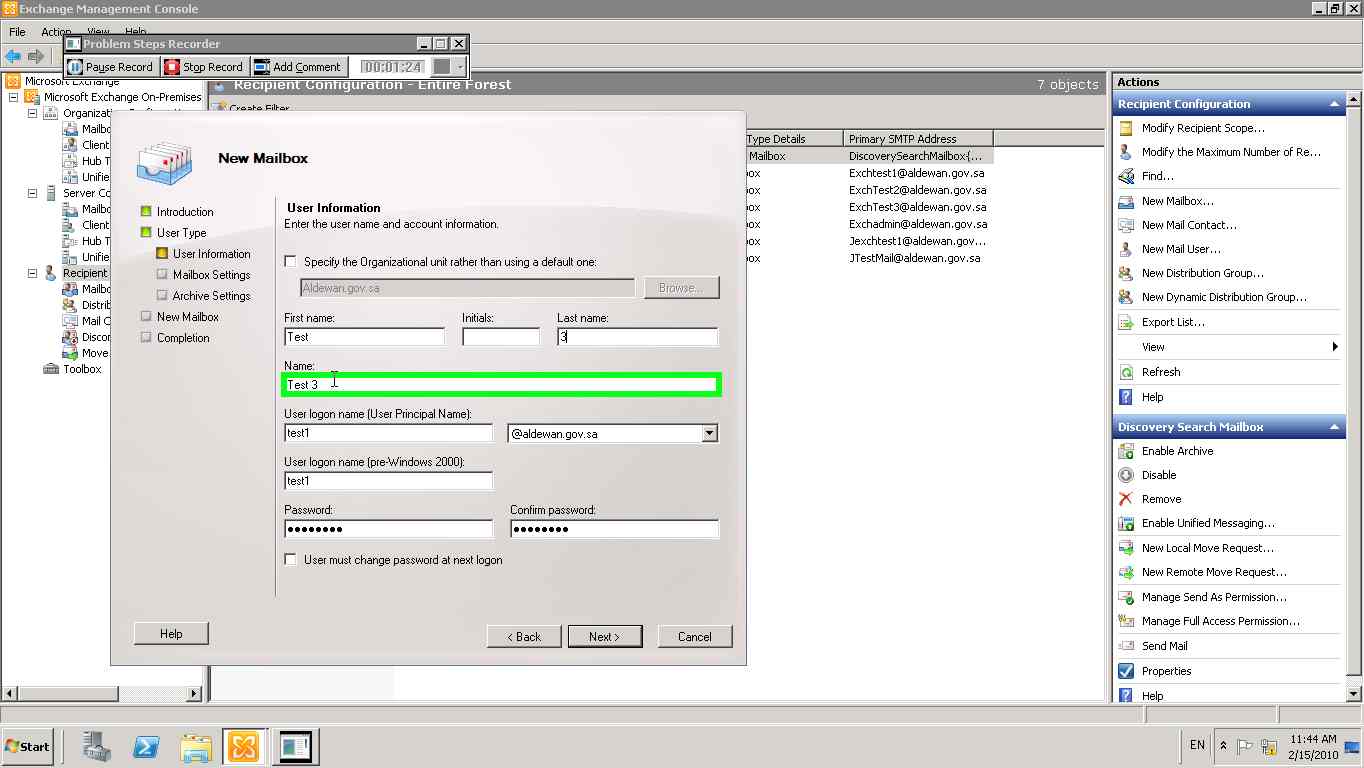
[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_newuser1.zip\Problem_20100215_1145.mht!screenshot_0016.jpeg)

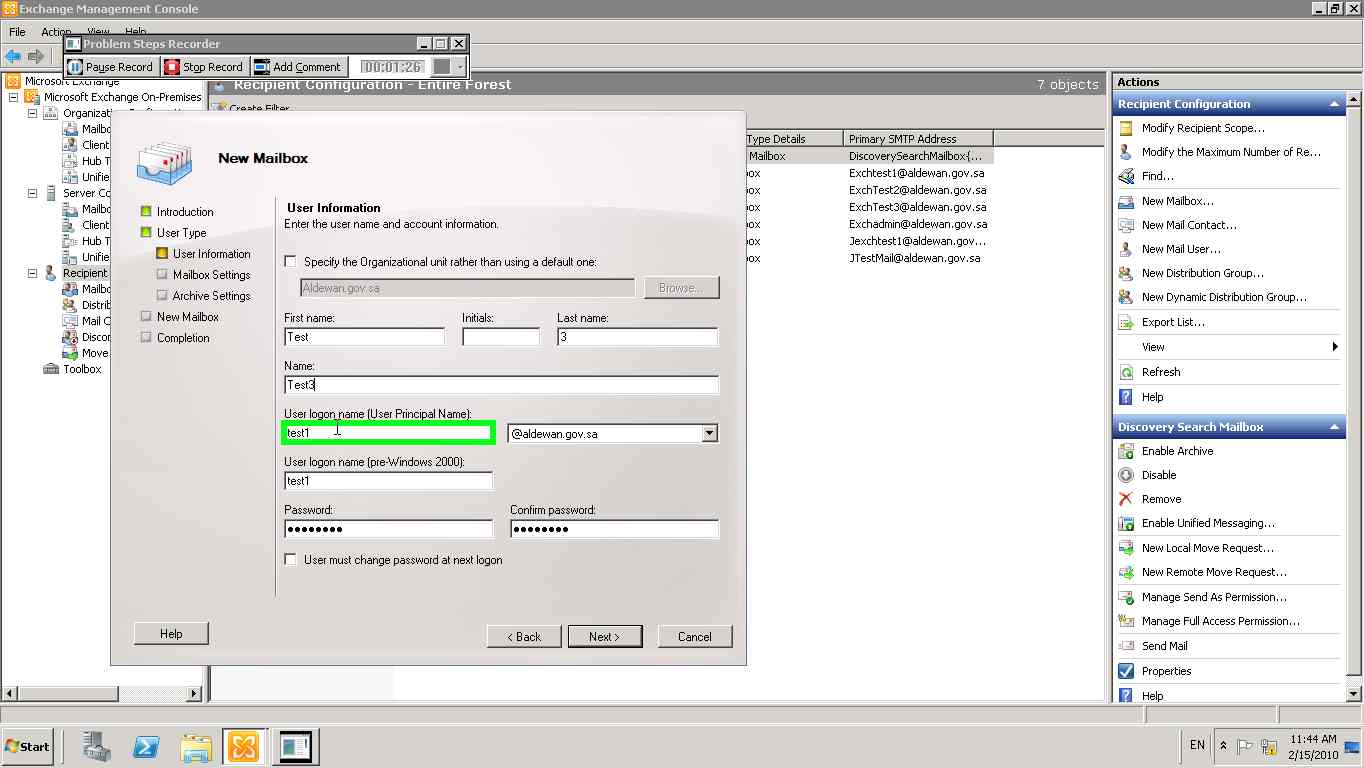
**New user**

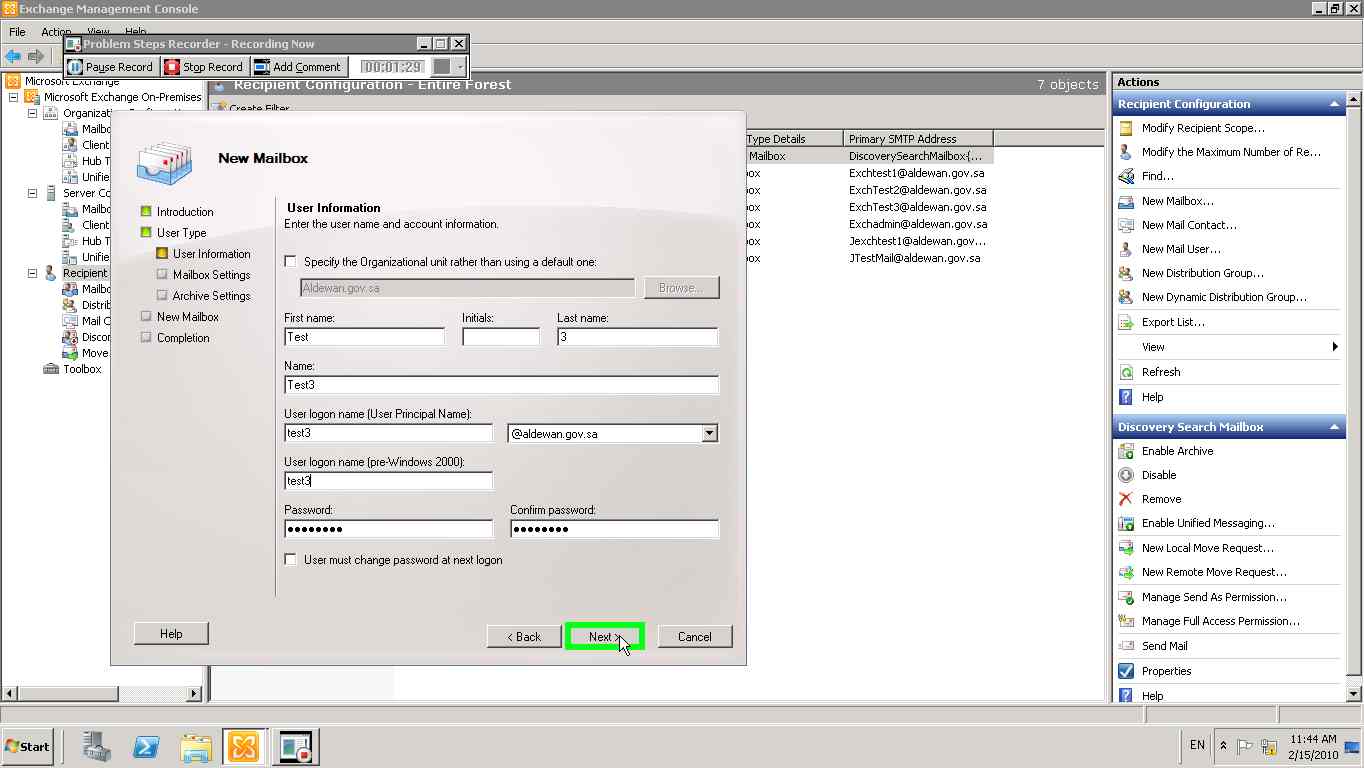
[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_newuser1.zip\Problem_20100215_1145.mht!screenshot_0002.jpeg)

[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_newuser1.zip\Problem_20100215_1145.mht!screenshot_0003.jpeg)

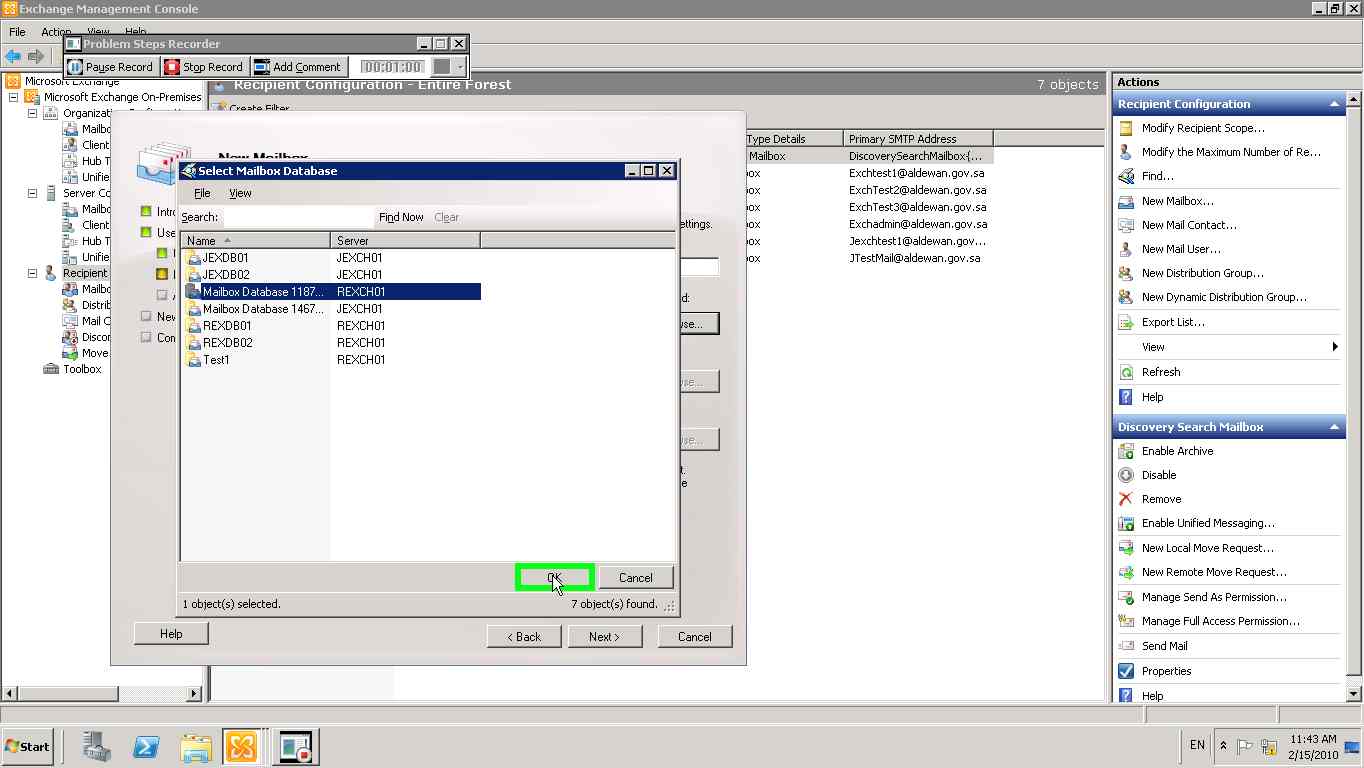
[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_new%20user.zip\Problem_20100215_1144.mht!screenshot_0031.jpeg)

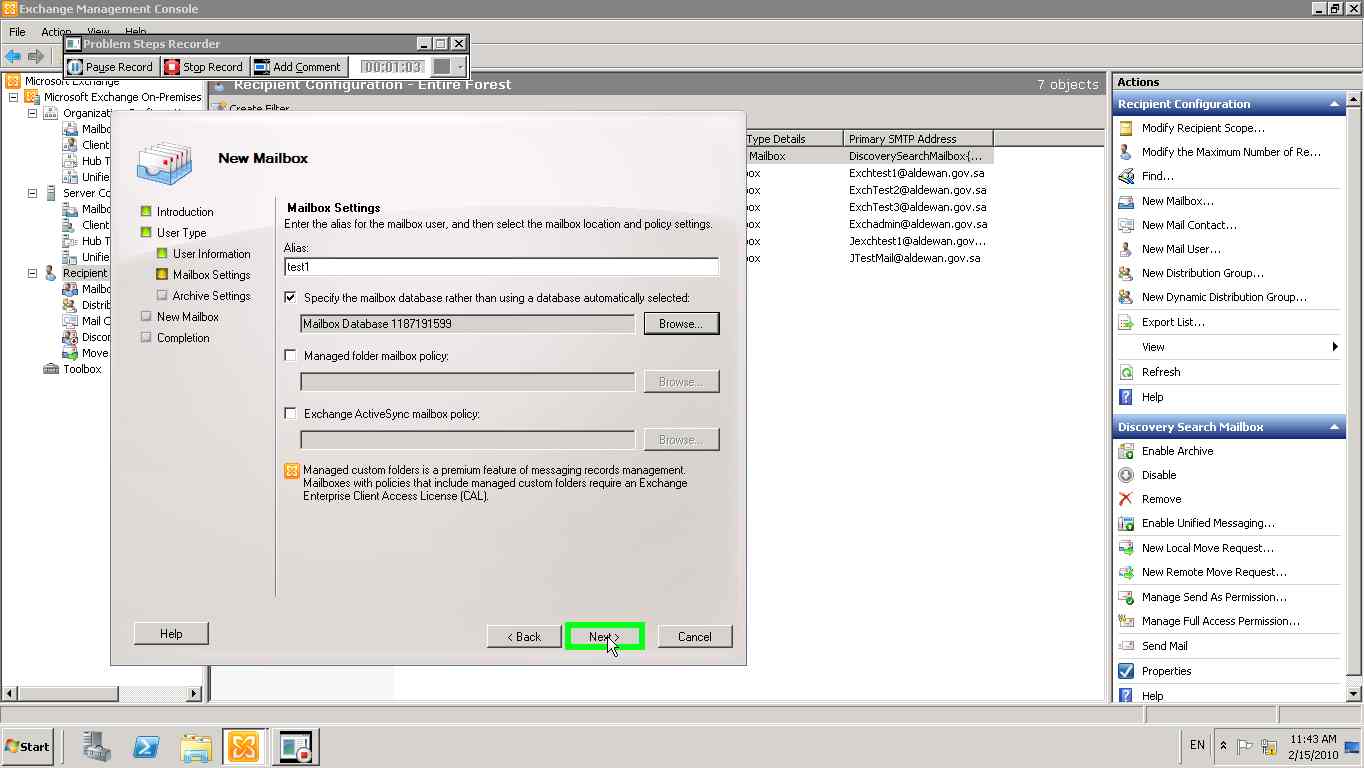
[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_new%20user.zip\Problem_20100215_1144.mht!screenshot_0035.jpeg)

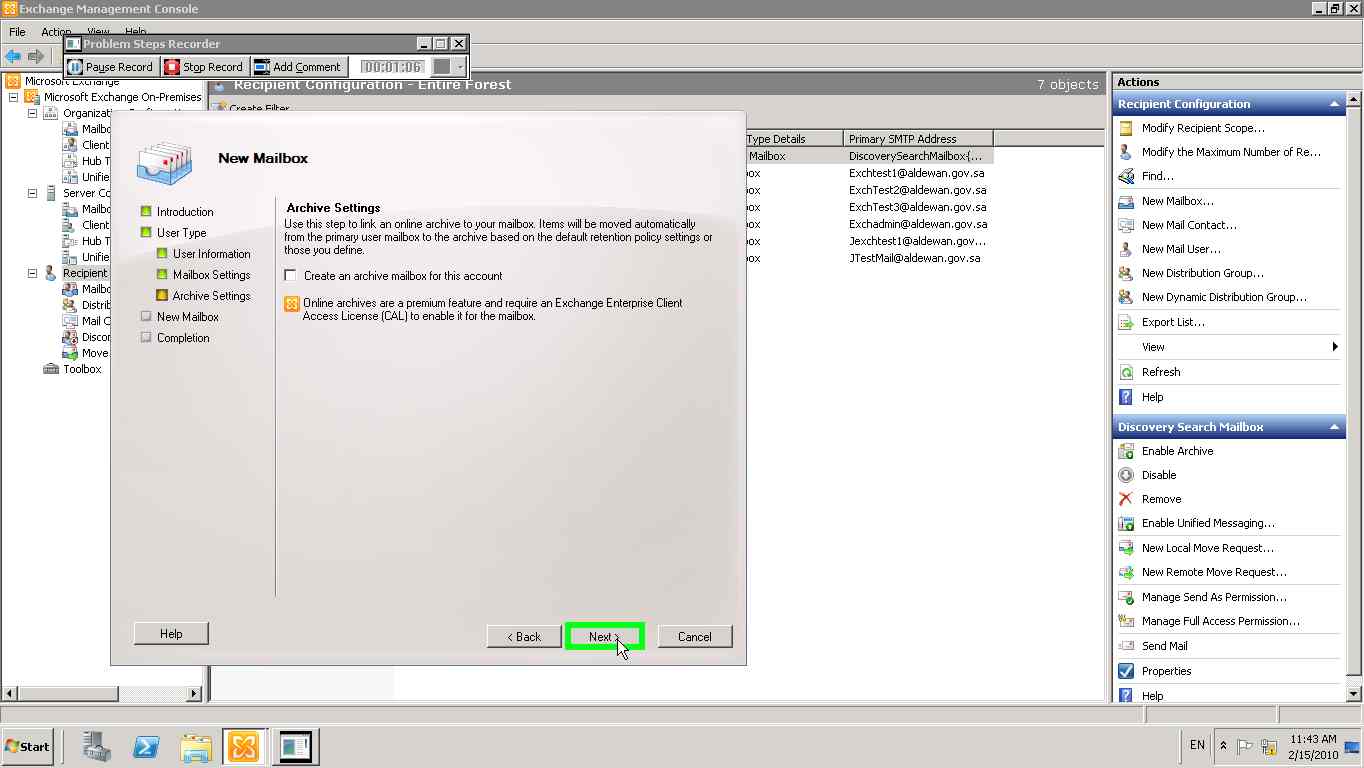
[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_new%20user.zip\Problem_20100215_1144.mht!screenshot_0037.jpeg)

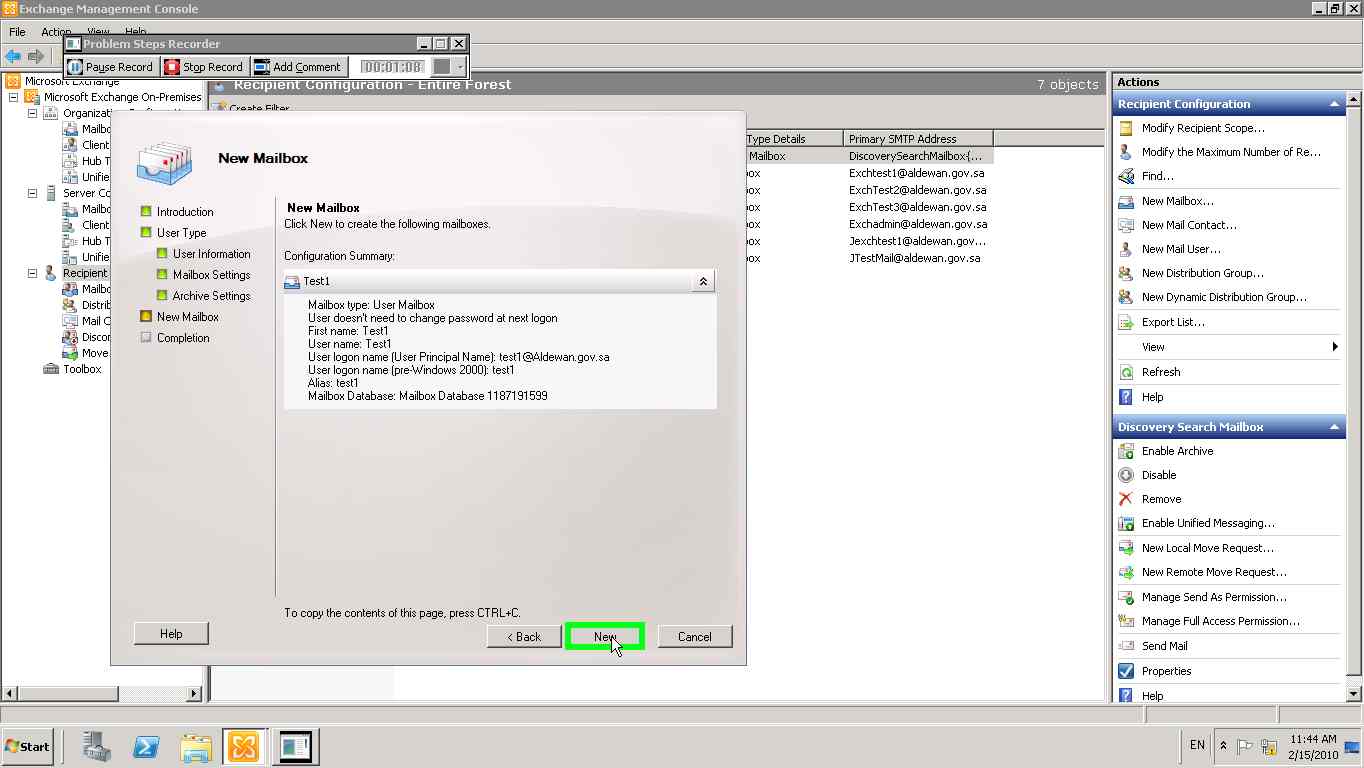
[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_new%20user.zip\Problem_20100215_1144.mht!screenshot_0041.jpeg)

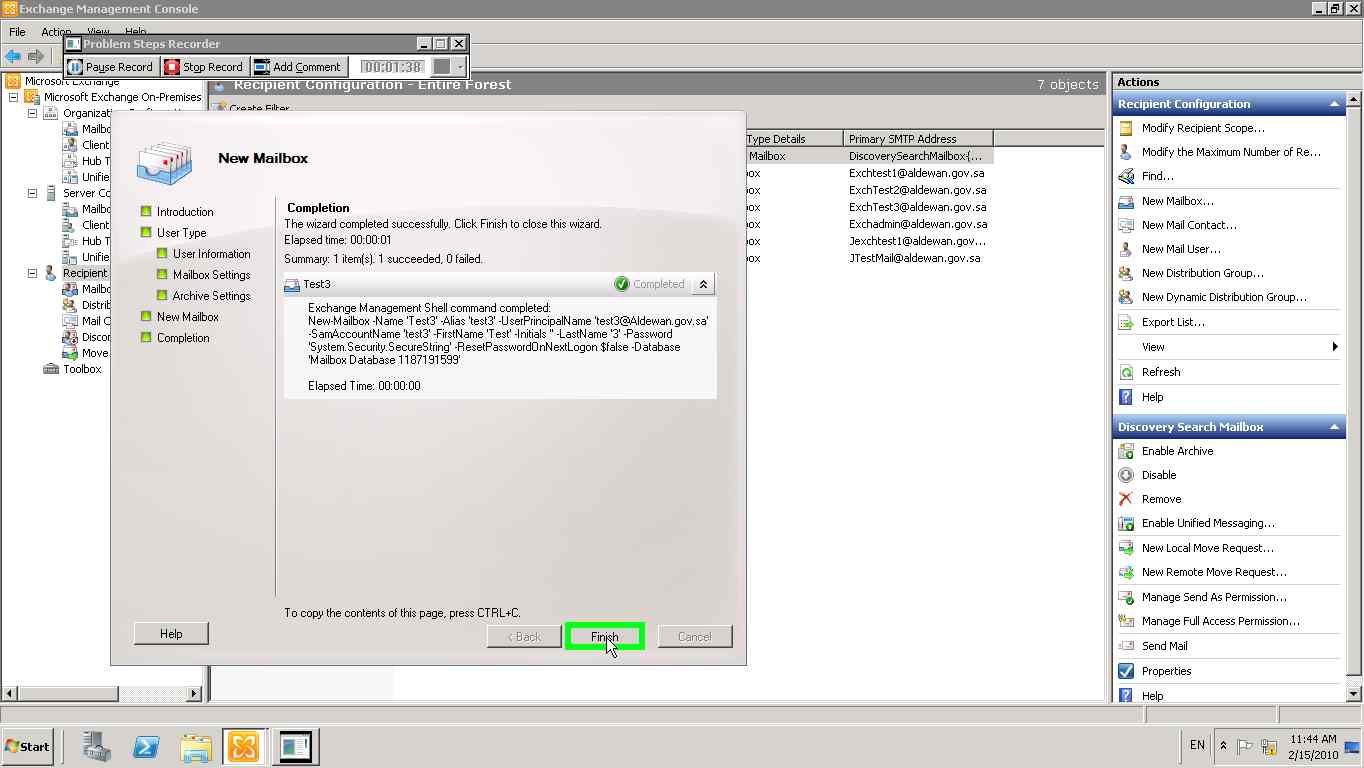
**Note:** the below screen shots are same for New user and existing user

[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_new%20user.zip\Problem_20100215_1144.mht!screenshot_0023.jpeg)

[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_new%20user.zip\Problem_20100215_1144.mht!screenshot_0024.jpeg)

[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_new%20user.zip\Problem_20100215_1144.mht!screenshot_0025.jpeg)

[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_new%20user.zip\Problem_20100215_1144.mht!screenshot_0026.jpeg)

[](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_new%20user.zip\Problem_20100215_1144.mht!screenshot_0047.jpeg)

### Enable a Personal Archive for a New mailbox

You need to be assigned permissions before you can perform this procedure.

**Using EMC:**

1. In the console tree, click **Recipient Configuration**.
2. In the action pane, click **New Mailbox**.
3. On the **Introduction** page, select one of the following options:
   * **User Mailbox**   Click this button to create a mailbox that is owned by a user to send and receive e-mail messages.  
       
     The Active Directory account that is associated with user mailboxes must reside in the same forest as the Exchange server. To use an account in a trusted forest, select **Linked Mailbox**.
   * **Linked Mailbox**   Click this button to create a user mailbox that is accessed by a user in a separate, trusted forest. You must still create a user account in the forest in which Exchange Server resides. This is required to create the necessary Active Directory object for storing the mailbox information.  
       
     Linked mailboxes might be necessary for organizations that choose to deploy Exchange in a resource forest. The resource forest scenario allows an organization to centralize Exchange in a single forest, while allowing access to the Exchange organization with user accounts in one or more trusted forests.
4. On the **User Type** page, click **New User**.
5. On the **User Information** page, complete the following fields:
   * **Specify the organizational unit rather than using a default one**   Select this check box to select an organizational unit (OU) other than the default (which is the recipient scope). If the recipient scope is set to the forest, the default value is set to the **Users** container in the Active Directory domain that contains the computer on which the Exchange Management Console is running. If the recipient scope is set to a specific domain, the **Users** container in that domain is selected by default. If the recipient scope is set to a specific OU, that OU is selected by default. To select a different OU, click **Browse** to open the **Select Organizational Unit** dialog box. This dialog box displays all OUs in the forest that are within the specified scope. Select the desired OU, and then click **OK**.
   * **First name**   Use this box to type the first name of the user. This field is optional.
   * **Initials**   Use this box to type the initials of the user. This field is optional.
   * **Last name**   Use this box to type the last name of the user. This field is optional.
   * **Name**   Use this box to type a name for the user. This is the name that's listed in Active Directory. By default, this box is populated with the names you enter in the **First name**, **Initials**, and **Last name** boxes. If you didn't use those boxes, you must still type a name in this field. The name can't exceed 64 characters.
   * **User logon name (User Principal Name)**   Use this box to type the name that the user will use to log on to the mailbox. The user logon name consists of a user name and a suffix. Typically, the suffix is the domain name in which the user account resides.
   * **User logon name (pre-Windows 2000)**   Use this box to type the name for the user that is compatible with the legacy versions of Microsoft Windows (prior to the release of Windows 2000 Server). This field is automatically populated based on the **User logon name (User Principal Name)** field. This field is required.
   * **Password**   Use this box to type the password that the user must use to log on to his or her mailbox.

|  |
| --- |
| **Note:** |
| Make sure that the password you supply complies with the password length, complexity,  And history requirements of the domain in which you are creating the user account. |

* + **Confirm password**   Use this box to confirm the password that you typed in the **Password** box.
  + **User must change password at next logon**   Select this check box if you want the user to reset the password when they first logon to the mailbox.   
      
    If you select this check box, at first logon, the new user will be prompted with a dialog box in which to change the password. The user won't be allowed to perform any tasks until the password is successfully changed.

1. On the **Mailbox Settings** page, complete the following fields:
   * **Alias**   Use this box to type an alias for the mailbox. The alias can't exceed 64 characters and must be unique in the forest.
   * **Specify the mailbox database rather than using a database automatically selected**   Select this check box to specify an Exchange 2010 mailbox database instead of allowing Exchange to select a database for you. Click **Browse** to open the **Select Mailbox Database** dialog box. This dialog box lists all the Exchange 2010 mailbox databases in your Exchange organization. By default, the mailbox databases are sorted by name. You can also click the title of the corresponding column to sort the databases by database name or server name. Select the mailbox database you want to use, and then click **OK**. This is an optional field.
   * **Managed folder mailbox policy**   Leave this check box cleared. Managed folders are not compatible with personal archives. Personal archives use retention policies.
   * **Exchange ActiveSync mailbox policy**   Select this check box to specify an Exchange ActiveSync mailbox policy for the mailbox. Exchange ActiveSync enables access to an Exchange mailbox from a mobile device.   
       
     Click **Browse** to open the **Select ActiveSync Mailbox Policy** dialog box. Use this dialog box to select the policy that you want associated with this mailbox. This is an optional field.
2. On the **Archive Settings** page, select the **Create an archive mailbox for this account** check box. Mailbox items will be moved automatically from the primary user mailbox to the archive, based on the default retention policy settings or those you define.
3. On the **New Mailbox** page, review your configuration settings. To make any configuration changes, click **Back**. To create the new mailbox, click **New**.
4. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   * A status of **Completed** indicates that the wizard completed the task successfully.
   * A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

**Using PowerShell:**

This example creates the user Chris Ashton in Active Directory and creates the mailbox on mailbox database DB01 with archive enabled. The password must be reset at the next logon. To set the initial value of the password, this example creates a variable (*$password*), prompts you to enter a password, and assigns that password to the variable as a **SecureString** object.

$password = Read-Host "Enter password" -AsSecureString

New-Mailbox -UserPrincipalName chris@contoso.com -Alias chris -Archive -Database "DB01" -Name ChrisAshton -OrganizationalUnit Users -Password $password -FirstName Chris -LastName Ashton -DisplayName "Chris Ashton" -ResetPasswordOnNextLogon $True

After you create the mailbox with archive enabled, you may also want to configure archive quotas to limit the size of the personal archive.

### Enable a Personal Archive for an Existing Mailbox

By enabling the personal archive for a mailbox, you can regain control of the organization's messaging data by eliminating the need for .pst files. The personal archive also allows users to store messages in an archive mailbox, which is then accessible to users from Microsoft Outlook 2010 and Microsoft Office Outlook Web App.

When you enable a personal archive for a mailbox, the archive and the mailbox will reside on the same server.

**Prerequisites**:

* We recommend that mailbox users move all current archive data stored in their .pst files into their Inbox so they don't lose any messages. Alternatively, administrators can move the mailbox data by using the **Import-Mailbox** cmdlet.
* Online archives are a premium feature and require an Exchange Enterprise client access license to enable an archive for a mailbox.

**Using EMC:**

You need to be assigned permissions before you can perform this procedure.

Properties specific to a user mailbox are controlled by the **Set-Mailbox** cmdlet. In the EMC, you can set additional properties, and the permissions may vary depending upon the feature that you're configuring. With the permissions listed for this procedure, you can edit all of the settings available in the **<User Mailbox> Properties** dialog box.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the user you want to enable an archive for.
3. In the action pane, click **Enable Archive**.
4. A warning appears confirming that you want to enable the personal archive. Click **Yes**.

**Use PowerShell:**

You need to be assigned permissions before you can perform this procedure.

This example enables the personal archive for Tony Smith's mailbox

Enable-Mailbox "Tony Smith" -Archive

This example enables the personal archive for all mailboxes on mailbox database DB01.

Get-Mailbox -Database DB01 | Enable-Mailbox -Archive

After you enable the personal archive, you may want to configure the archive storage quotas.

### Configure Personal Archive Quotas for a Mailbox

Because personal archives are created with unlimited storage quotas by default, you'll need to use the mailbox's property page to configure storage quotas for the personal archive. The following is a list of the quotas that you can configure with a description of each.

* Archive warning quota – When archives are created with unlimited storage quotas by default, you'll need to use the mailbox's property page to configure storage quotas for the personal archive. The following is a list of the quotas that you can configure with a description of each.
* Archive Quota – When a personal archive exceeds the specified archive quota, messages are no longer moved to the archive and a warning message is sent to the mailbox user.

In the EMC, you can configure only the archive warning quota. In the Shell, you can configure the archive quota and the archive warning quota.

**Using EMC**

You need to be assigned permissions before you can perform this procedure.

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the result pane, select the user mailbox you want to configure.
3. In the action pane, click **Properties**.
4. In **<Mailbox Name> Properties**, click the **Mailbox Settings** tab.
5. Select **Archive Quota**, and then click **Properties**.
6. Select the **Issue warning at (MB)** check box, and then use the corresponding box to type the personal archive size in megabytes (MB), at which a warning will be sent to the user.
7. Click **OK**.

**Using PowerShell**

You need to be assigned permissions before you can perform this procedure.

This example sets the Chris Ashton mailbox archive quota to 1 gigabyte (GB), at which time the user will receive a warning message that the personal archive is full and will no longer be able to move items to the personal archive. This example also sets the archive warning quota to 950 MB, at which time the user will receive a warning message that the personal archive is almost full:

|  |
| --- |
|  |
| Set-Mailbox -Identity "Chris Ashton" -ArchiveQuota 1GB -ArchiveWarningQuota 950MB |

### Disable a Personal Archive for a Mailbox

You may want to disable a user's personal archive for troubleshooting purposes or if you're moving the mailbox to a version of Exchange that doesn't support personal archives,

If you disable the personal archive, all information in the archive will be kept in the mailbox database until the default time passes and the personal archive is permanently deleted. (By default, Exchange keeps all messages for 30 days.) If you want to reconnect the personal archive to that mailbox, you can use the **Connect-Mailbox** cmdlet with the *Archive* parameter.

**Using EMC**

You need to be assigned permissions before you can perform this procedure.

1. In the console tree, navigate to Recipient Configuration > Mailbox.
2. In the result pane, select the mailbox for which you want to disable the personal archive.

Note: You can create a filter to find all of the personal archive in your organization. In the result pane, click Add Filter, In the filter’s list boxes, specify the following values: Has Archive > Equals > Yes. Click Apply Filter.

1. In the action pane, click Disable Archive.
2. A warning box appears confirming that you want to disable the archive. Click Yes.

**Using PowerShell**

You need to be assigned permissions before you can perform this procedure,

Disabling the personal archive will remove the archive from the mailbox and mark it in the mailbox database for deletion. This example disables the archive for Chris Ashton's mailbox. It doesn't disable the mailbox.

Disable-Mailbox -Identity "Chris Ashton" -Archive

A warning appears confirming that you want to disable the archive. Type **Y** to continue.

### Connect a Disconnected Personal Archive

Personal Archive becomes disconnected when they're disabled. When disabled, the personal archive is retained in the mailbox database for a specified amount of time. During that time, the personal archive is in a disconnected state. By default, Exchange retains disconnected personal archives for 30 days. During this time, you can recover the personal archive by associating it with an existing mailbox.

**Note:**

If you disable a personal archive for a user mailbox and then enable a personal archive for that same mailbox, the mailbox will get a new personal archive.

**Using EMC**

You need to be assigned permissions before you can perform this procedure.

1. In the console tree, navigate to **Recipient Configuration** > **Disconnected Mailbox**.

**Note:** the personal archive that you want to connect to a mailbox isn't displayed in the result pane, restart the Microsoft Exchange Information Store service, and then run the **Clean-MailboxDatabase** cmdlet against the mailbox database that contains the personal archive.

1. In the result pane, select the personal archive that you want to connect to a primary mailbox.
2. In the action pane, click Connect to Primary Mailbox.
3. A warning appears confirming that you want to connect the personal archive to a specific user. This is the user to whom the archive belongs. Click Yes.

**Using PowerShell**

You need to be assigned permissions before you can perform this procedure.

1. If you don't know the name of the personal archive, you can view it in the Shell by running the following command. This example finds all disconnected personal archives on mailbox database DB01 and displays additional information about the personal archives such as the GUID and item count.

|  |  |
| --- | --- |
| Get-MailboxDatabase "DB01" | Get-MailboxStatistics | Where {($\_.DisconnectDate -ne $null) -and ($\_.IsArchiveMailbox -eq $true)} Format-List |  |
|  | |

1. Connect the personal archive to the primary mailbox. This example connects Chris Ashton's archive to Chris Ashton's primary mailbox and uses the GUID as the personal archive's identity.

|  |  |
| --- | --- |
| Connect-Mailbox -Identity "8734c04e-981e-4ccf-a547-1c1ac7ebf3e2" -Archive -User "Chris Ashton" -Database "DB01" |  |
|  | |

A warning appears stating that you'll have to wait for Active Directory replication to complete before the user can access the personal archive.

### Monitoring Exchange Database Information and Statistics

Database monitoring involves regularly checking the health of your databases. Typically your monitoring procedures are complemented by a notification system that sends alert to administrator when problems occur. The main advantages to daily monitoring are as follows:

* You can quickly detect and address issues that may affect the messaging service or data availability.
* You can ensure the successful completion of specific administrative tasks, such as daily backup operations.
* It helps meet the requirements of your Service Level Agreements.

### Viewing Mailbox Statistics

You can use the *Get-MailboxStatistics* EMS cmdlet to view the statistics for all the mailboxes on a server, for all the mailboxes in a mailbox database, or for a single mailbox. The following command lists the statistics for all the mailboxes on the Mailbox server EX01 server:

*Get-MailboxStatistics –Server EX01 | FL*

The following command lists all the mailboxes in the mailbox database “Mailbox Database 1234567890”:

*Get-MailboxStatistics –Database “Mailbox Database 1234567890” | FL*

If a user mailbox has been created but has never been accessed, that mailbox is not included when you list the statistics of mailboxes on a server or in a mailbox database. If you attempt to obtain statistics for a mailbox that has not been accessed, you will get no statistical information but will instead receive a warning message.

*Get-MailboxStatistics –identity “Don Hall” | FL*

Warning: The user hasn’t logged on to Mailbox “Don Hall” so there is no data to return. After the user logs on, you won’t see this warning anymore.

If a mailbox returns statistics, you can use the PowerShell format-list (FL) cmdlet to display the value of one or more specified statistics. The following command displays the last logon time for Kim Akers mailbox.

*Get-MailboxStatistics –Identity “Kim Akers” | FL LastLogonTime*

You can use the *Sort-Object* PowerShell cmdlet to sort the mailboxes in a mailbox database or on a Mailbox server by the value of one or more mailbox statistics. You can do this either *descending* or *ascending* order and use the *format-table (FT)* PowerShell cmdlet to display the result as a table. The following command lists the mailboxes in the Research mailbox database in descending order of item count:

*Get-MailboxStatistics – Database Research | Sort-Object ItemCount –Descending | FT DisplayName, ItemCount*

The following command lists the mailboxes in the Research mailbox database in descending order of total item size:

*Get-MailboxStatistics –Database Research | Sort-Object TotalItemSize –Descending |FT DisplayName, TotalItemSize*

If you do not want to list all the mailboxes in a mailbox database or on a Mailbox server but instead want to list the top five mailboxes in terms of total item size, you can pipe the results of your search into the *Select-Object* PowerShell cmdlet. The following command lists the top five mailboxes in Mailbox Database 1234567890 in descending order of total item size:

*Get-MailboxStatistics –Database “Mailbox Database 1234567890” | Sort-Object TotalItemSize –Descending | Select-Object – First 5 | FT DisplayName, TotalItemSize*

### Monitoring Resource Usage

Pressure on a mailbox database can be the result of certain users consuming a disproportionate amount of resources, such as by sending an excessive number of large attachments to a large number of recipients. To detect this situation, you can use the Get-StoreUsageStatistics EMS cmdlet to generate a report on the 25 accounts that are using the greatest amount of resources within a mailbox database. The following command returns the 25 users with the largest mailboxes in Mailbox Database 1234567890

*Get-StoreUsageStatistics – database “Mailbox Database 1234567890”*

Use the Get-StoreUsageStatistics cmdlet to obtain statistics about a specific mailbox, but only if this mailbox account is one of the 25 top resource users. The following command would generate a report about the Kim Akers account:

*Get-StoreUsageStatistics –Identity “Kim Akers”*

### Using Performance Monitor Counters

Use the Exchange Server Performance Monitor tool to monitor counters that can indicate whether resources in your Exchange Organization are coming under stress. This is the same tool as Performance Monitor (PerfMon) except that the Performance and Logs Alerts snap-in has been prepopulated with a large number of Exchange-related performance counters. Access Exchange Server Performance Monitor from the EMC by clicking the Toolbox node, clicking Performance Monitor, and clicking Open Tool.

To ensure that your mailbox databases continue to operate efficiently, you need to check that they are being defragmented online on an ongoing basis. Online defragmentation is a background task that operates continuously by default. Exchange Server 2010 provides the following performance counters for monitoring the behaviour of online database defragmentation:

* **MSExchange Database Online Defrag Average Log Bytes:** Shows average size of the log records being generated by online defragmentation.
* **MSExchange Database Online Defrag Data Moves/Sec:** Shows the number of times that data is moved from one page to another by the online defragmentation process.
* **MSExchange Database Online Defrag Log Records/Sec:** Shows the number of times per second that data is moved from one page to another by the online defragmentation process.
* **MSExchange Database Online Defrag Page Moves/Sec:** Shows the number of times that data is moved from one page to a new page by the online defragmentation process.
* **MSExchange Database Online Defrag Pages Dirtied/Sec:** Shows the rate at which online defragmentation is modifying clean database pages.
* **MSExchange Database Online Defrag Pages Freed/Sec:** Shows the number of pages per second that are freed from the database by the online defragmentation process.
* **MSExchange Database Online Defrag Pages Preread/Sec:** Shows the rate at which database pages are read in anticipation of future use by online defragmentation.
* **MSExchange Database Online Defrag Pages Read/Sec:** Shows the rate of database read operations being performed by online defragmentation.
* **MSExchange Database Online Defrag Pages Re-Dirtied/Sec:** Shows the rate at which online defragmentation is modifying database pages that already contained modifications.
* **MSExchange Database Online Defrag Pages Re-Dirtied/Sec:** Shows the rate at which online defragmentation is touching database pages.

### Obtaining Information about Public Folder Databases

When monitoring a public folder database, obtain general information about the database, such as the server where it is located, what public folders it contains, its maximum item size, quota limits, replication schedule, and so on. Use EMS commands based on the *Get-PublicFolderDatabase* cmdlet for this purpose. The following command gets detailed information about evry public folder database in an organization:

*Get-PublicFolderDatabase | FL*

To obtain detailed information about a specific public folder database, you can specify the Exchange Server 2010 Mailbox server on which it is located. The following command gets detailed information about the public folder database on the EX1 server:

*Get-PublicFolderDatabase –Server Ex1 | FL*

It is typically easier to analyse and store this information if the output of the command is redirected to a text file. The following command redirects detailed information about the public folder database on the Van-EX1 server to the text file PublicFolderDetails.txt in the DatabaseInformation folder on the Van-EX1 server:

*Get-PublicFolderDatabase –Server EX1 | FL > C:\databaseinformation\PublicFolderDetails.txt*

Use the Status parameter of the *Get-PublicFolderDatabase* cmdlet to obtain backup and mount status information (if available). Checking the status of public folder databases is an important step in monitoring replication health. The following command gets detailed information about the public folder database on the Van-EX1 server, including status information:

*Get-PublicFolderdatabase –Server EX1 –Status | FL*

### Viewing Public Folder Statistics

No EMS cmdlet exists that returns the statistics for an entire public folder database. However, you can use the Get-PublicFolderStatistics EMS cmdlet to obtain statistics for each individual public folder within a public folder database. Check replication by ensuring that the number and size of items in the public folder replica are the same as in the original public folder. Use the same procedure if you replicate an entire public folder database and want to check that replication is working correctly.

The following command obtains statistics for every public folder in an Exchange 2010 organization:

*Get-PublicFolderStatistics | FL*

The previous command can return an excessive volume of information, particularly if there are a large number of public folders. As with mailbox databases, refine the information to obtain statistics for every public folder on the Mailbox server Van-EX1, enter the following command:

*Get-PublicFolderStatistics –Server EX1 | FL*

To obtain statistics for the public folder MyPublicFolder on the Mailbox server Van-EX1, enter the following command:

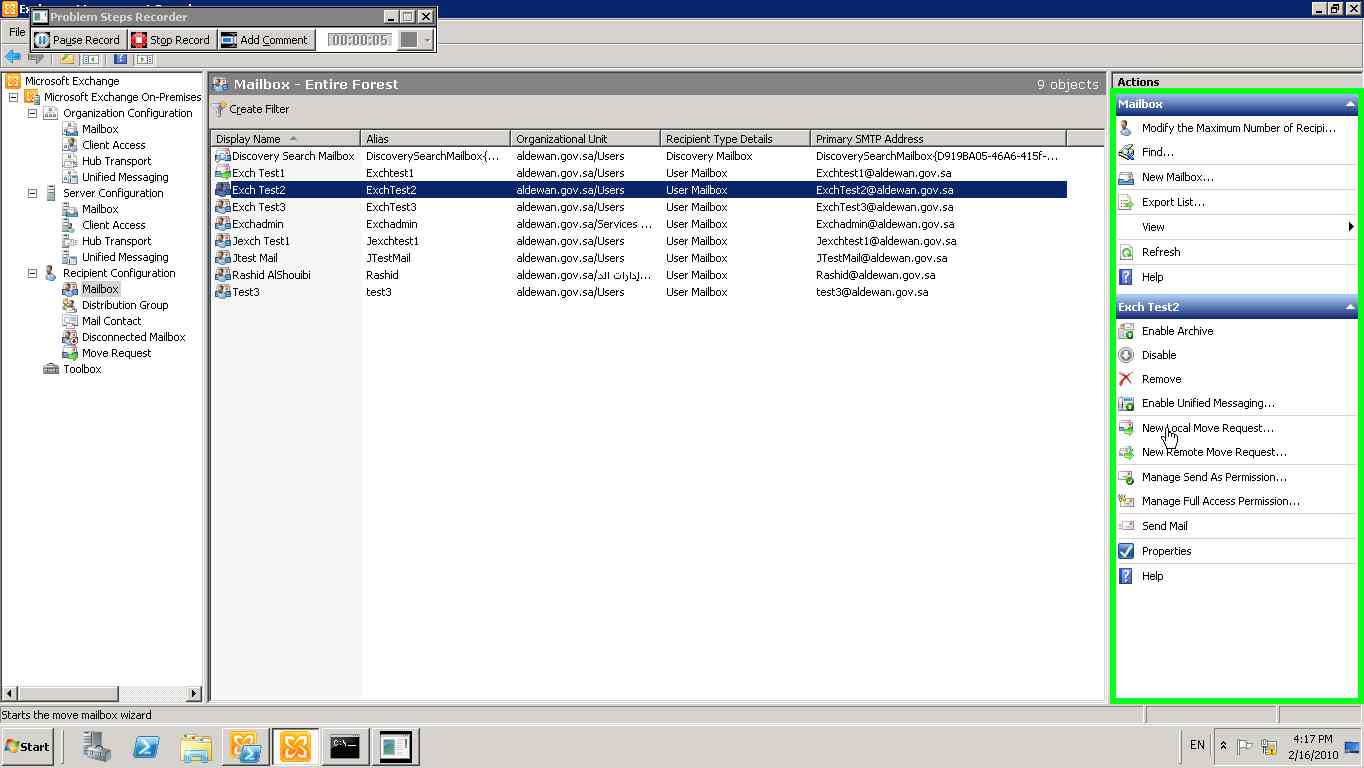
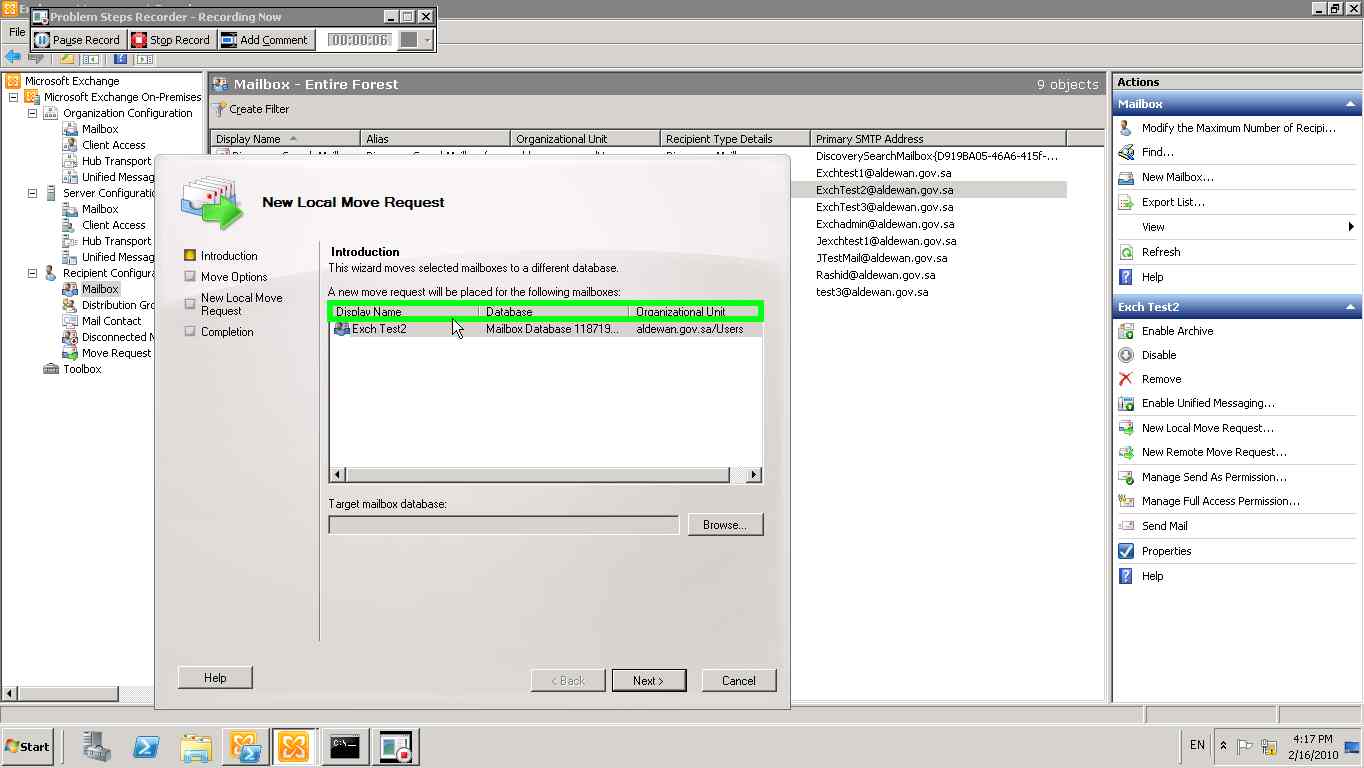
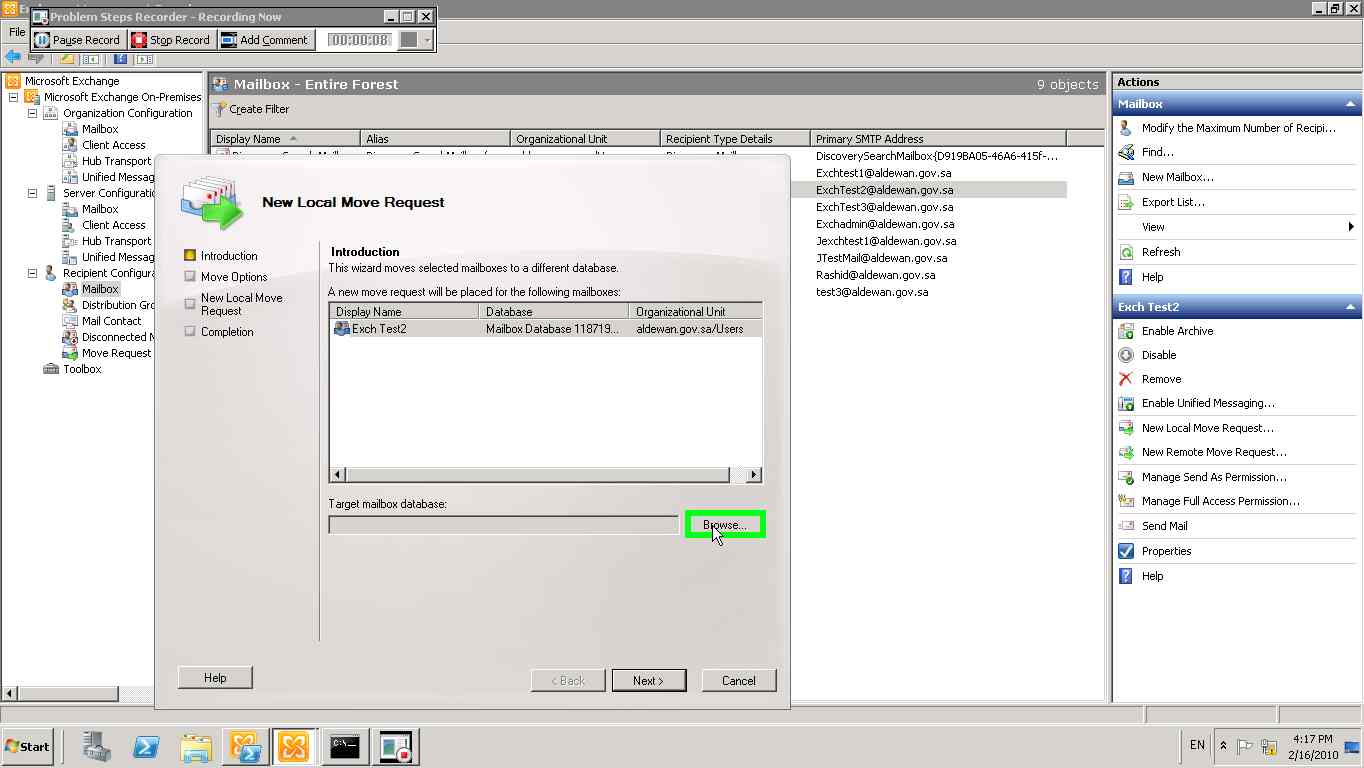
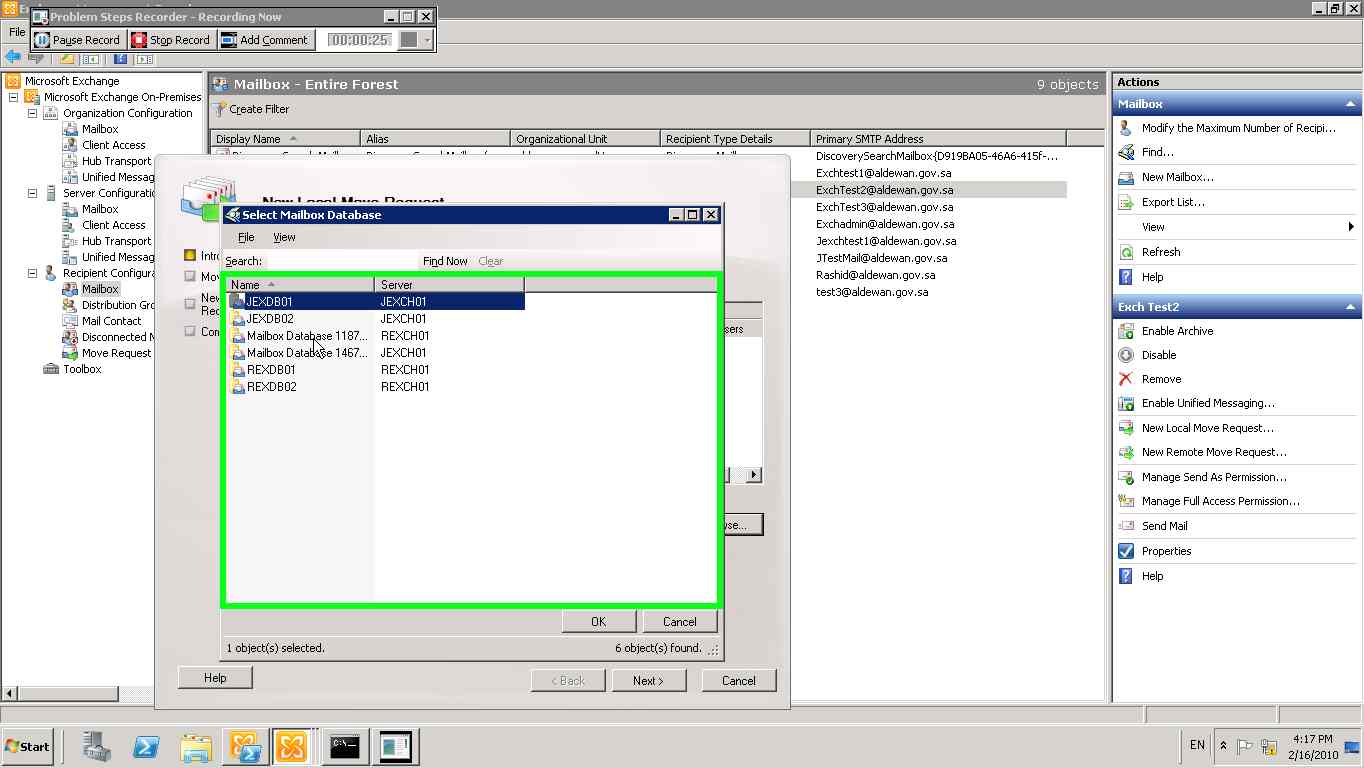
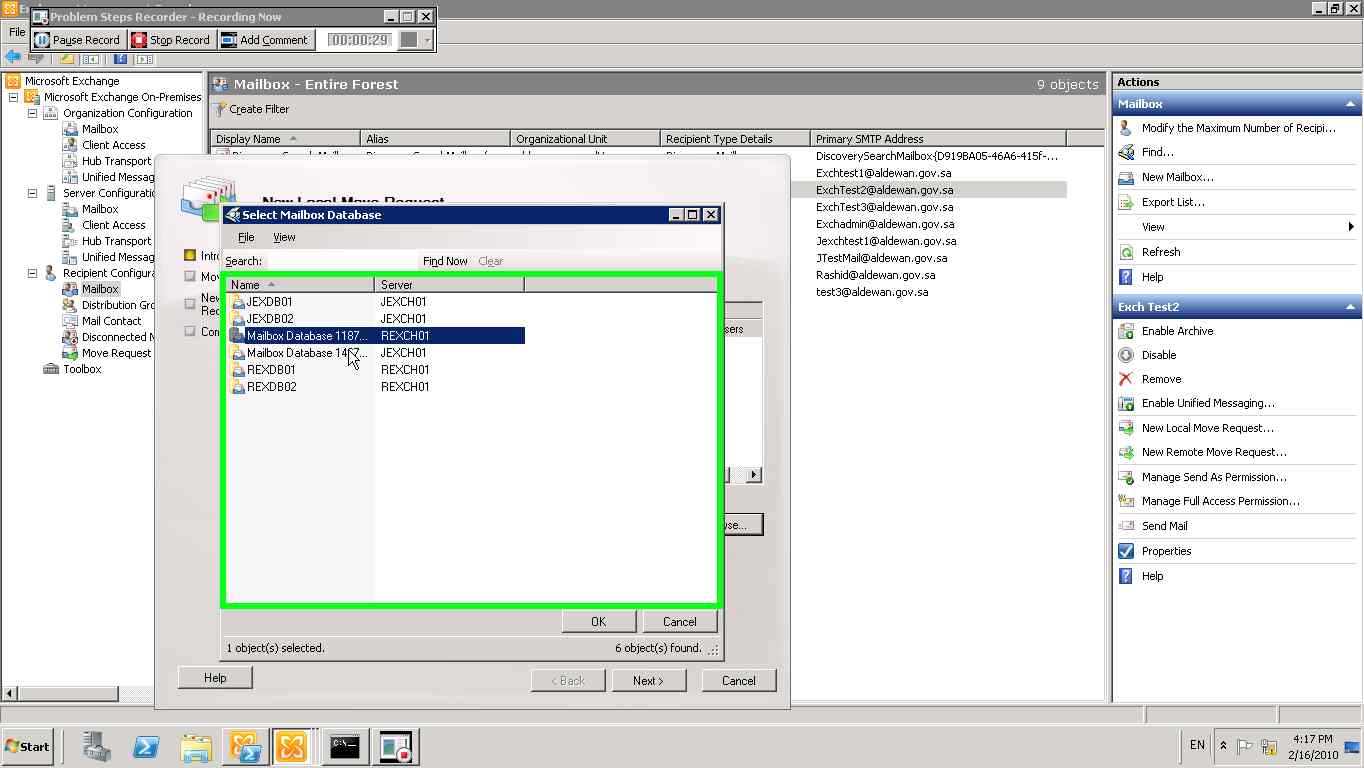
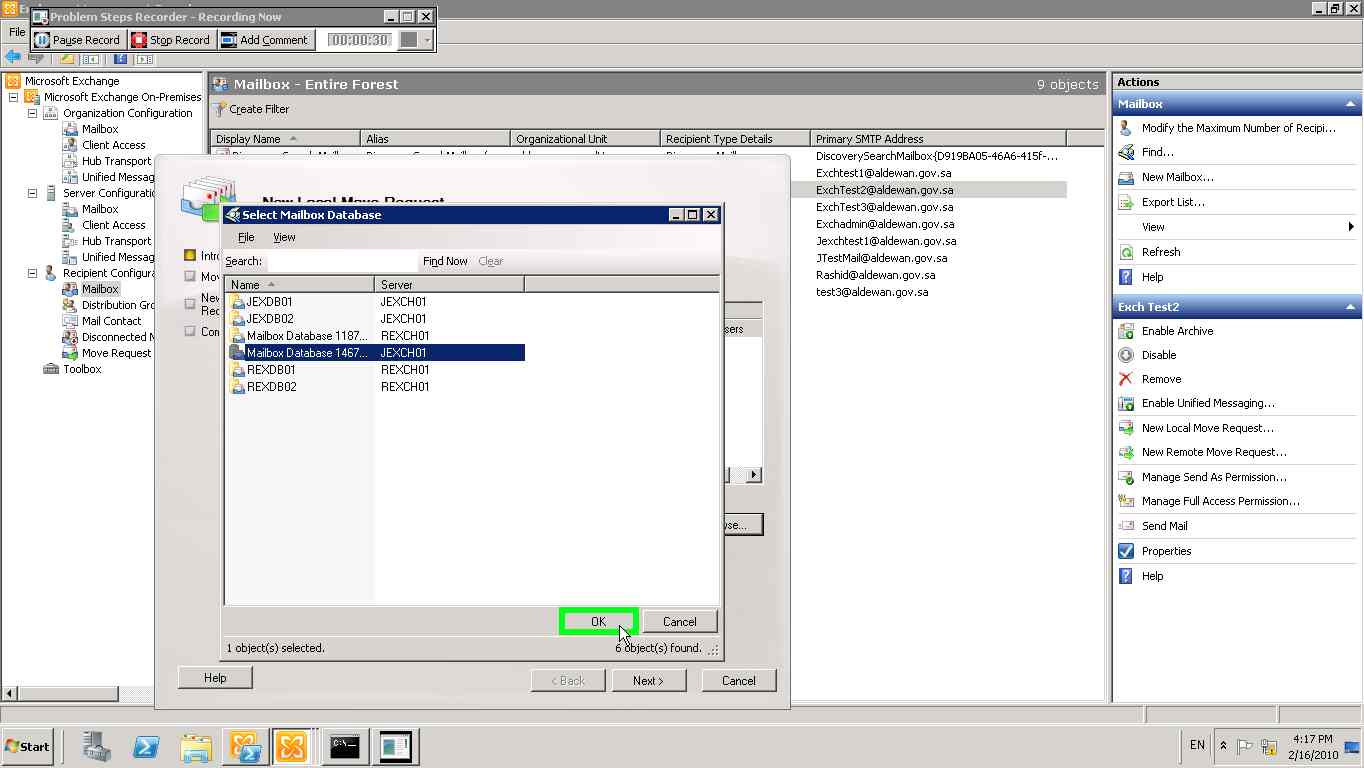
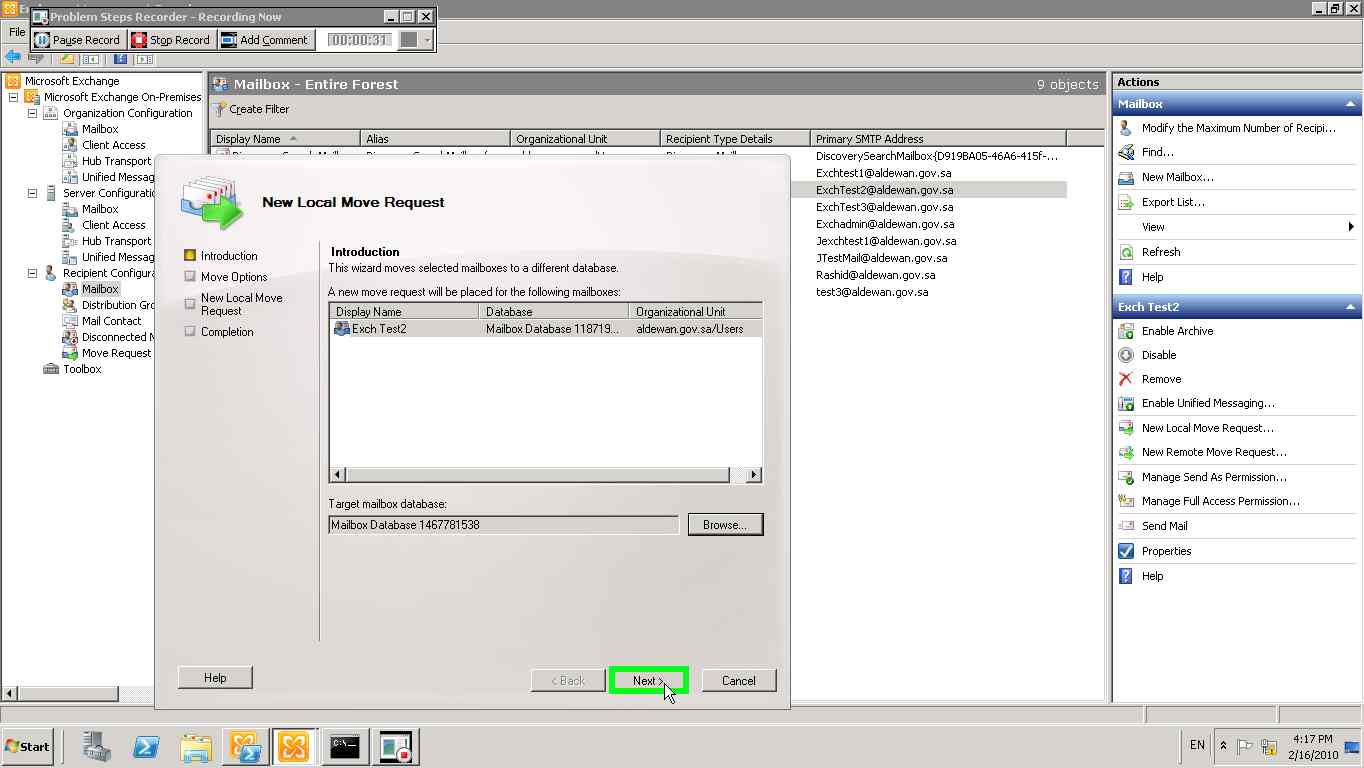
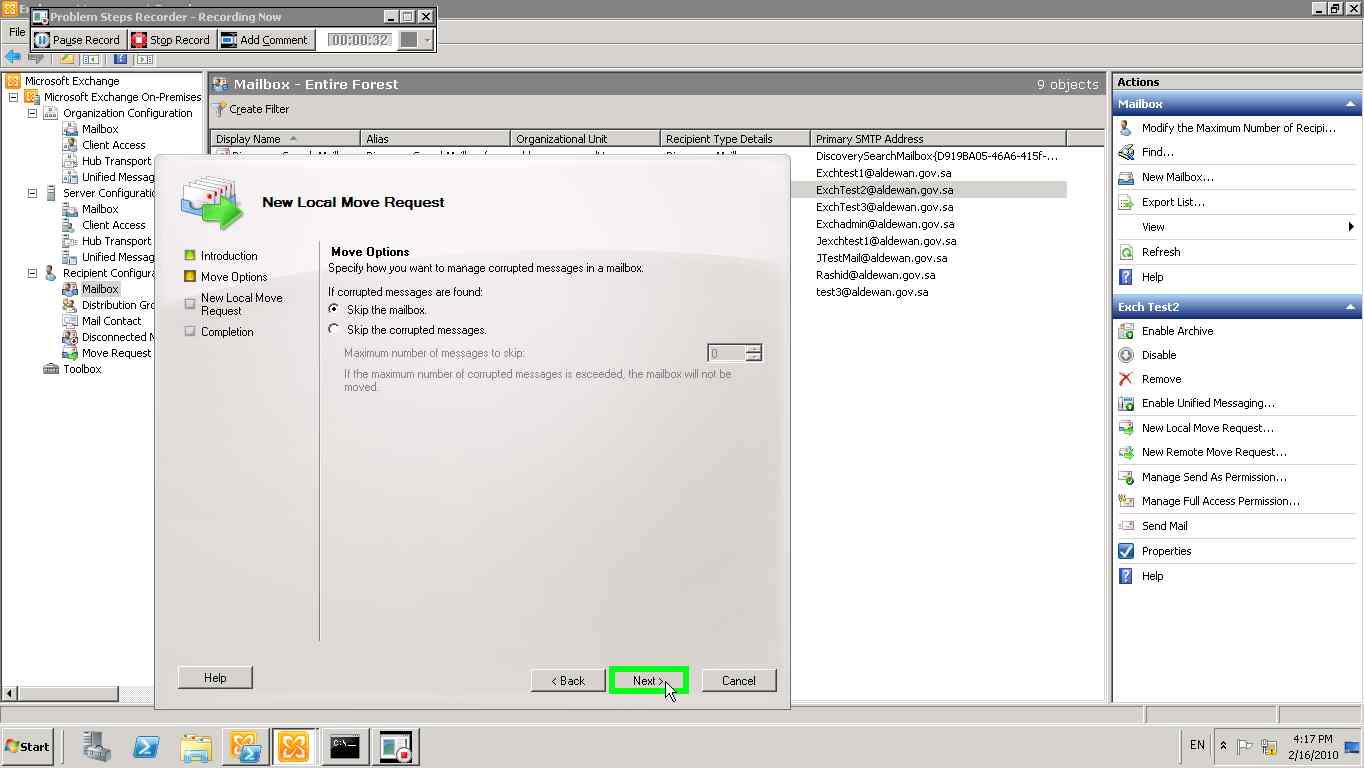
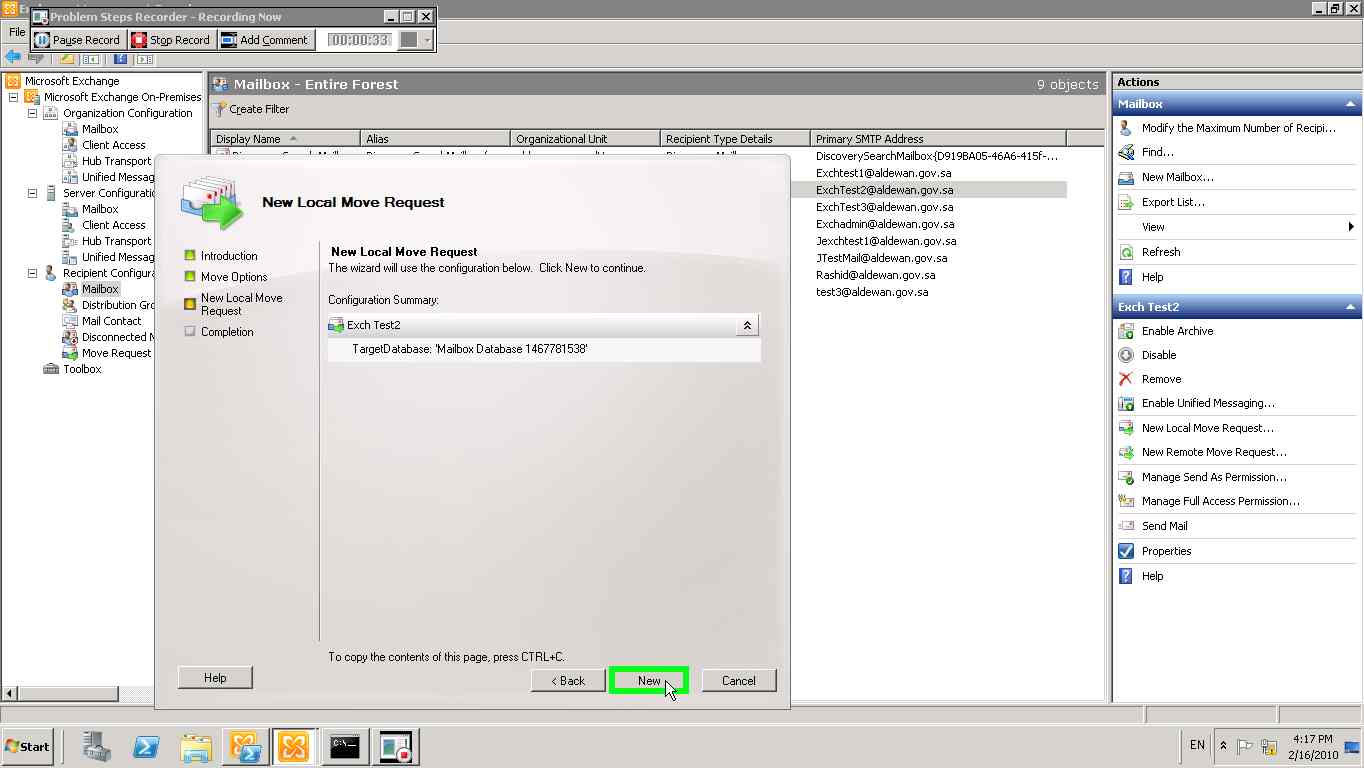
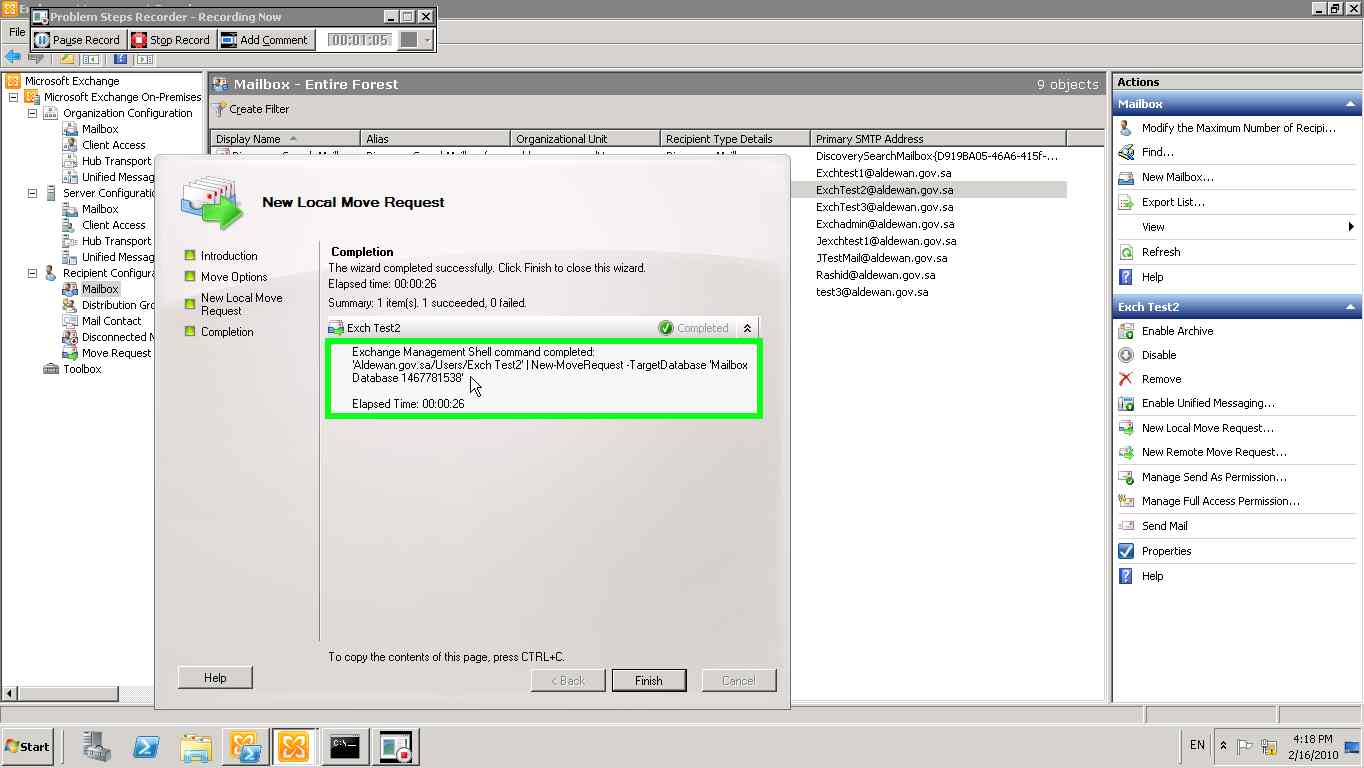
Get-PublicFolderStatistics –Identity \MyPublicFolder –Server EX1 | FL

### Moving a Mailbox

|  |  |
| --- | --- |
| Prerequisites: |  |
| **Built-in Exchange 2010 Role required** | Mailbox Move Role |
| **Scope** | Organization or Organizational Unit  Database list |
| **Execute on** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup) or an Exchange Server 2010 SP1 |
| **Domain** | Domain in which the mailbox is hosted |

Moving mailbox between databases inside the same server or to another server is done in Exchange 2010 by creating move request. Because you have many ways to accomplish the mailbox move, it is recommended to refer to <http://technet.microsoft.com/en-us/library/bb124495.aspx>

#### Use Exchange Management Console

1. Connect to an Exchange 2010 server or from workstation with Exchange Management Tools.
2. Launch an Exchange Management Console with Run as administrator privileges.
3. In the console tree, navigate to **Recipient Configuration** 🡪 **Mailbox**.
4. In the result pane, select one or more mailboxes that you want to move.
5. In the action pane, click **New Local Move Request**.
6. On the **Introduction** page, configure the following settings:
   * **A new move request will be placed for the following mailboxes** This box displays the mailboxes that you selected in the result pane. If you want to add or remove mailboxes, click **Cancel**, and then make the changes in the result pane.
   * **Target mailbox database** Click **Browse** to open the **Select Mailbox Database** dialog box. Use this dialog box to select the mailbox database to which you want to move the mailboxes. Click **OK** to return to the wizard.  
     If the mailbox has an archive associated with it, the following options are displayed:  
     **Move only the user mailbox** Click this button if you want to move only the user's primary mailbox to the new database. This is selected by default.  
     **Move only the archive mailbox** Click this button if you want to move only the user's archive mailbox to the new database.   
     **Move both the mailbox and the archive** Click this button if you want to move both the user's primary mailbox and the associated archive mailbox to the new database.
7. On the **Move Settings** page, specify how you want to manage corrupted messages:
   * **Skip the mailbox** Click this button to specify that mailboxes containing corrupted messages won't be moved. We recommend selecting this option.
   * **Skip the corrupted messages** Click this button to move the mailbox, but not to move any corrupted messages. If you select this option, you need to set the **Maximum number of messages to skip**. We recommend selecting this option only if the move request failed in a previous attempt.
   * **Maximum number of messages to skip** If you select **Skip the corrupted messages**, use this list to specify a number from **1** through **50**. For value higher than 50, use PowerShell cmdlet.
   * **Suspend this move when it is ready to complete** Select this check box to suspend the move request before the completion stage begins. You can resume the move request at a later time.
8. On the **New Local Move Request** page, review your configuration settings. Click **New** to create the move request. Click **Back** to make changes.
9. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   * A status of **Completed** indicates that the wizard completed the task successfully.
   * A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
10. [](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_movembx.zip\Problem_20100216_1618.mht!screenshot_0002.jpeg)
11. [](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_movembx.zip\Problem_20100216_1618.mht!screenshot_0003.jpeg)
12. [](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_movembx.zip\Problem_20100216_1618.mht!screenshot_0004.jpeg)
13. [](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_movembx.zip\Problem_20100216_1618.mht!screenshot_0005.jpeg)
14. [](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_movembx.zip\Problem_20100216_1618.mht!screenshot_0006.jpeg)
15. [](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_movembx.zip\Problem_20100216_1618.mht!screenshot_0007.jpeg)
16. [](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_movembx.zip\Problem_20100216_1618.mht!screenshot_0008.jpeg)
17. [](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_movembx.zip\Problem_20100216_1618.mht!screenshot_0009.jpeg)
18. [](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_movembx.zip\Problem_20100216_1618.mht!screenshot_0010.jpeg)
19. [](mhtml:file://C:\Users\hasanan\AppData\Local\Temp\Temp1_movembx.zip\Problem_20100216_1618.mht!screenshot_0011.jpeg)

#### Use Exchange Management Shell Console

Launch ***Exchange Management Shell*** Console with Run as administrator privilege.

New-MoveRequest -Identity '*<LOGIN or SMTPADDRESS>*’ -TargetDatabase *<DATABASE>*

## Managing Contacts

* + 1. Create a Contact

|  |  |
| --- | --- |
| Prerequisites: |  |
| **Built-in Exchange 2010 Role required** | Mailbox Recipient Creation Role |
| **Scope** | Organization or Organizational Unit |
| **Execute on** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup) or an Exchange Server 2010 SP1 |
| **Domain** | Domain in which the contact will be hosted |

For more details, refer to <http://technet.microsoft.com/en-us/library/aa998858.aspx>

#### Use Exchange Management Console

1. Connect to an Exchange 2010 server or from workstation with Exchange Management Tools.
2. Launch an Exchange Management Console with Run as administrator privileges.
3. In the console tree, click **Recipient Configuration**.
4. In the action pane, click **New Mail Contact**.
5. On the **Introduction** page, under **Create a mail contact for**,select one the following option:
   * **New contact:** click this button to create and mail-enable a new contact and provide the required account information for the contact on the **Contact Information** page of this wizard.
6. Complete the following fields on the **Contact Information** page:
   * **Specify the organizational unit rather than using a default one:** select this check box and select the target organizational unit (OU); click **Browse** to open the **Select Organizational Unit** dialog box and select the appropriate OU, and then click **OK**.
   * **First name:** type the contact's first name. This field is optional.
   * **Initials:** type the contact's initials. This field is optional.
   * **Last name:** type the contact's last name. This field is optional.
   * **Name:** type a name for the contact based on the naming convention
   * **Alias:** type a unique alias based on the naming convention
   * **External e-mail address:**  to specify a SMTP e-mail address, click **Edit**. In the **SMTP address** dialog box, type the SMTP e-mail address.
7. On the **New Mail Contact** page, review your configuration settings. To make changes, click **Back**. To create the new mail contact, click **New**. Click **Cancel** to close the wizard without creating the new mail contact.
8. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   * A status of **Completed** indicates that the wizard completed the task successfully.
   * A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.
9. Click **Finish** to close the wizard.

#### Use Exchange Management Shell Console

Launch ***Exchange Management Shell*** Console with Run as administrator privilege.

**New-MailContact -Name "*<LASTNAME>, <FIRSTNAME>*" –DisplayName “*<CONTACTDISPLAY>*” -ExternalEmailAddress "*<firstname>.<lastname>@<TARGETSMTPDOMAIN>*" -OrganizationalUnit "*<OU\_PATH>*"**

### Change contact properties

|  |  |
| --- | --- |
| Prerequisites: |  |
| **Built-in Exchange 2010 Role required** | [Mail](http://technet.microsoft.com/en-us/library/dd298028.aspx) Recipients Role |
| **Scope** | Target Organizational Unit, target Mailbox database |
| **Execute on** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup) or an Exchange Server 2010 SP1 |
| **Domain** | Domain in which the mailbox account is hosted |

Refer to <http://technet.microsoft.com/en-us/library/aa997434.aspx>

### Remove a contact

For more details, refer to <http://technet.microsoft.com/en-us/library/bb124269.aspx>

***Using Exchange Management Console***

1. Connect to an Exchange 2010 server or from workstation with Exchange Management Tools.
2. Launch an Exchange Management Console with Run as administrator privileges.
3. In the console tree, expand **Recipient Configuration**, and then click **Mail Contact**.
4. In the result pane, click the mail contact that you want to remove.
5. In the action pane, under the name of the mail contact, click **Remove**. You can also right –click on the contact and select **Remove**.
6. In the warning that asks if you're sure you want to remove the mail contact, click **Yes**.

***Using Exchange Management Shell console***

Launch ***Exchange Management Shell*** Console with Run as administrator privilege:

Remove-MailContact -Identity "*<ALIAS or SMTPADDRESS>*" -DomainController *<LOCAL-DC>*

# Daily Tasks

To help ensure the availability and reliability of your Exchange 2010 organization, you must actively monitor the physical platform, the operating system, and all important Exchange 2010 services. Preventive maintenance helps you identify potential errors before any one of these errors cause problems with the operation of your Exchange organization. Preventive maintenance combined with disaster recovery planning and regular backups help minimize problems if they occur.

Monitoring your Exchange organization involves checking for problems with connections, services, server resources, and system resources. You can also set alerts to notify administrators when problems occur. Microsoft Windows Server 2008 R2 and Exchange 2010 provide you with many monitoring tools and services to help make sure that your Exchange organization is running smoothly. The key advantages to daily monitoring are as follows:

* + Meeting the performance requirements of your service level agreements (SLAs).
  + Completing successfully specific administrative tasks, such as daily backup operations, and checking server health.
  + Detecting and addressing issues, such as bottlenecks in the server performance or need for additional resources before they affect productivity.

Daily maintenance tasks help you establish criteria for what is normal for your organization and to detect any abnormal activity. It is important to implement these daily maintenance tasks so that you can capture and maintain data about your Exchange organization, such as usage levels, possible performance bottlenecks, and administrative changes. See the following topics for information about tasks that you should perform daily as a best practice:

* + Performing Physical Environmental Checks
  + Performing and Monitoring Backups
  + Checking Disk Usage
  + Checking the Event Viewer
  + Monitoring Server Performance
  + Monitoring Network Performance

## Performing Physical Environmental Checks

Before you check performance, availability, and functionality of your Microsoft Exchange organization, you should check the physical environment. For example, the server room temperature might need to be lowered or a network cable might need to be replaced. Perform the following physical environmental inspections:

* **Physical security measures -** Physical security protection such as locks, doors, and restricted-access rooms must be secured. Check for any unauthorized and forced entries and signs of equipment damage.
* **Temperature and humidity -** High temperature and humidity can cause hardware components to overheat. Check temperature and humidity to help make sure that the environmental systems such as heating and air conditioning can maintain acceptable conditions and function within the hardware manufacturer's specifications.
* **Devices and components -** Your Exchange organization relies on a functioning physical network and related hardware. Check to make sure that routers, switches, hubs, physical cables, and connectors are operational.

## Performing and Monitoring Backups

Performing backups of your servers is your first line of defense in planning for a disaster. You must have a well-planned and well-rehearsed disaster recovery plan for your Microsoft Exchange organization. Your disaster recovery plan should include backing up Exchange data and Active Directory service data daily. You must back up all critical data from many sources, including server configuration, the Active Directory database, and the Microsoft Exchange Information Store service. You should also back up all logged event and performance data. Make sure that you back up records such as Active Directory data, application software, Exchange Server 2010 message tracking log files, databases and log files.

Proactively monitoring the successful completion of your Exchange backups is critical to success of your disaster recovery plan. Regular testing of the disaster recovery plan for your organization's Exchange infrastructure should be performed in a lab environment that mimics your production environment as closely as practicable.

**Note:** Ensure that Exchange aware backup product is used to backup Exchange infrastructure.

## Checking Disk Usage

Hard disks drives are a critical component of your Exchange organization. Without sufficient free disk volume, neither the operating system nor the Exchange databases can function correctly. You must monitor the Exchange store statistics daily to make sure that you do not run out of disk space and to prepare to add storage resources as required. When the Microsoft Exchange Information Store service runs out of hard drive space, it logs Event ID 1113 in the application event log to indicate the problem.

## Checking Disk Space

Exchange Server needs hard disk space to store its databases and transaction logs. You can check free disk space by using the following methods:

* **Windows Explorer**   Use Windows Explorer to check for disk space on volumes that store Exchange logs and databases. You should monitor the disk space regularly to make sure that the Microsoft Exchange Information Store service will not be negatively affected because of insufficient storage resources. Comparing and maintaining statistical information about available disk space on each Exchange volume and expected growth of the databases and transaction log files, helps you with capacity planning and adding storage when the storage resources are required. To accommodate troubleshooting and disaster recovery situations, it is recommended that available free volume space be equal or greater than 110% of the size of database.

## Checking the Event Viewer

You can use Event Viewer to obtain information about service failures, replication errors in the Active Directory service, and warnings about system resources such as virtual memory and disk space. Use Event Viewer to view and manage event logs; obtain information about hardware, software, and system problems that must be resolved; and identify trends that require future action.

Event Viewer maintains logs about application, security, and system events on your computer. Both Microsoft Exchange Server and Microsoft Windows report warnings and error conditions to the event logs. Therefore, make sure that you review event logs daily.

## Monitoring Server Performance

Microsoft Exchange performance is affected by many factors such as user profiles, system architecture, software, and hardware components. Make sure that Windows is functioning correctly because, if it is not, your Exchange performance will be affected.

Monitoring server performance helps to make sure that your servers are functioning correctly and helps you identify bottlenecks in the system. You can use the performance monitoring data to identify problems and apply corrective action. You can also use the monitoring data to enhance the performance of your servers by identifying areas that need additional resources. For example, you may need to increase your storage capacity to handle the growing number of users in your organization.

## Monitoring the Operating System

Monitoring the performance of all servers and components on an Exchange Server, such as the Microsoft Exchange Information Store service, is vital. You can use System Monitor, which is a Windows Server 2008 component.

You can also use the Windows Performance console, a Windows Server 2008 R2 snap-in, to verify that your Windows Server 2008 R2 operating system is functioning correctly. The Performance console, which is made up of the System Monitor and Performance Logs and Alerts snap-ins, is the primary toolset used to analyze and maintain Exchange and operating system performance levels. The Performance console is quite flexible and can be used to gather data interactively from a single server or automated to gather data from many servers.

You can also use Task Manager (Taskmgr.exe) to obtain information about the processes and programs that are running on your local computer.

There are important differences between Task Manager and the Performance console, such as the Performance console captures data to a file whereas the Task Manager can end a process. Task Manager is primarily a troubleshooting aid, and the Performance console is used for more detailed troubleshooting and analysis.

### System Monitor

Using the System Monitor tool, you can define, collect, and view extensive data about the usage of hardware resources and the activity of system services on computers that you administer. System Monitor lets you monitor a single computer or several computers simultaneously. This flexibility can be helpful when you want to locate a problem in your system. You can specify the type of data you want to monitor, the source of the data, and establish sampling parameters, such as manual or automatic, within a time interval on real-time data. You can even change the appearance of your System Monitor to use graph, histogram, or report views.

### Performance Logs and Alerts

With Performance Logs and Alerts, you can collect performance data automatically from local or remote computers. You can view logged counter data using System Monitor or import the data into spread sheet programs or databases for analysis and report generation. Performance Logs and Alerts collect data in a comma-separated or tab-separated format for easy import to spread sheet programs. It also supports setting sampling intervals for monitoring data about hardware resources and system services. You can set an alert on a counter, thereby defining that a message be sent, a program be run, an entry made to the application event log, or a log be started when the selected counter's value exceeds or falls under a specified setting.

An alert is a system-generated event that is triggered when counters that you are tracking perform outside predefined thresholds. You use Performance Logs and Alerts to configure alerts.

### Task Manager

Task Manager is a Windows Server 2008 R2 tool that provides information about the processes and programs that are running on your local computer. You can use Task Manager to monitor key indicators of your computer's performance. You can see the status of the programs that are running and end programs that have stopped responding. You can also assess the activity of running processes using up to 15 parameters, and see graphs and data on CPU and memory usage. In addition, you can view the network status and see how your network adapter is functioning. If you have more than one user logged on to your computer, you can see who is connected, what they are working on, and you can send them a message.

## Monitoring Network Performance

It is important to monitor your network performance because its performance can affect the performance of your Exchange 2010 environment. You can monitor your network by using the following tools:

* + Network Monitor
  + Windows Management Instrumentation (WMI)
  + Simple Network Management Protocol (SNMP)
  + Microsoft System Center Operations Manager (SCOM) to monitor your Exchange system.

### Network Monitor

Network Monitor, a Microsoft Windows Server 2008 R2 tool, collects, displays, and analyses resource usage on a server and measure network traffic. Network Monitor exclusively monitors network activity. By capturing and analyzing network data and using this data with performance logs, you can determine your network usage, identify network problems, and forecast your network needs for the future.

## Verify MAPI Connectivity through system mailboxes

|  |  |
| --- | --- |
| Prerequisites: |  |
| **Required Permissions:** | [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Execute on:** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup), Exchange Server 2010 sp1 |
| **Domain:** | Domain that hosts the Exchange server |

1. Connect to an Exchange 2010 server or from workstation with Exchange Management Tools.
2. Launch an Exchange Management Shell Console with Run as administrator privileges.
3. The following PowerShell cmdlet will verify the ability to connect to the System Mailbox of each mailbox database of the specified server:

Test-MapiConnectivity –server “*<SRV\_NAME>*”

(Where Server is the name of one of Exchange Mailbox server)

Verify the “result” column which must be always “Success”. Any failure must be reported and escalated.

## Monitoring Mail Queues

Microsoft Exchange uses queues to hold messages as they are being processed for routing and delivery. The Queue Viewer is a tool that helps to maintain and administer Organization's messaging queues and identify mail flow issues. The Queue Viewer is available on all Exchange 2010 servers with the Hub Transport or Edge server role installed.

|  |  |
| --- | --- |
| Prerequisites: |  |
| **Built-in Exchange 2010 Role required** | Server Management Role |
| **Scope** | Server |
| **Execute on** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup) or an Exchange Server 2010 SP1 |
| **Domain** | Domain in which the Exchange server is hosted |

***Use Exchange Management Console***

The Queue Viewer to check for the following:

* **Messages that are queued for extended periods of time** - Unless an Exchange Server 2010 handles an extremely high volume of e-mail messages, the server will not typically have queued messages for any extended duration. Extended periods of queuing typically indicate a system issue that warrants your attention. Review your performance metrics to see if some other performance issues are causing e-mail messages to queue. If not, look for connectors or servers that are not functioning. SMTP protocol logging might also help you discover the problem.

1. Connect to an Exchange 2010 server or from workstation with Exchange Management Tools.
2. Launch an **Exchange Management Console** with Run as administrator privileges.
3. In the console tree of the EMC, navigate to **Toolbox**
4. In the toolbox click the **Queue Viewer**
5. In the action pane, select the **Queue Viewer Manage Exchange mail queues**.
6. Double click on the “**Queue Viewer**” and select the server where queue must be checked.
7. Select a specific server from which you want to view messages
8. After selecting the server in the Queue viewer check the queues and also messages give the amount of messages are blocked are submitted and errors
9. In the tab messages all messages in all queues on the server is displayed.
10. Peaks in queued messages will occurs when users send a message to large distribution list or an extremely large message too many people or a message whose destination is across a slow network link.

***Use Exchange Management Shell***

From Exchange Management Shell (PowerShell) run:

Get-TransportServer | get-queue

Verify queues are empty or nearly empty.

You may want to filter the queues per messages number. For example, if you want to show only queues where messages are greater than 100:

Get-TransportServer | Get-Queue -Filter {MessageCount -gt 100}

# Weekly Tasks

As a recommended practice, perform the following tasks and procedures weekly:

* **Check for Security Updates** - Identify any new service packs, hotfixes, or updates. If appropriate, test these in a test lab and use the change control procedures to arrange for deployment to the production servers.
* **Review Performance Figures** - Check the key performance data for the previous week. Review performance against this week. Identify trends and items that have not met their targets.
* **Environmental Tests** - Check periodically and maintain air conditioning, temperature and humidity monitors, and physical security measures.
* **Site Link Utilization** – Weekly utilization reports of the network link should be provided by the Network Team

# Monthly Tasks

As a recommended practice, perform the following tasks and procedures monthly:

* **Security Checks** - Depending on the level of security that your organization requires, it may be appropriate to perform regular audits of security, including firewall rules, user rights, group membership, delegate rights, and so on.
* **Capacity Planning** - Review capacity figures for the previous month, and produce a plan for any upgrades that may be required in the coming months to keep the system operating within limits specified by the organization's service level agreements (SLAs).
* **Disaster Recovery Test** - Perform a system recovery for a single server to test your organization's documented recovery process. This test will simulate a complete hardware failure for one server, and make sure that the resources, plans, and data are available for recovery. Try to rotate the focus of the test each month, so that you test the failure of a different server or other piece of equipment every time.

# As Needed Tasks

Perform the following tasks as necessary; however, they are frequently also covered by standard procedures:

 New and Departing Users   New users typically require a user account, a mailbox, certain rights and group memberships, possibly an e-mail copy of the organization’s IT and security procedures, and so on. Document the exact requirements and a procedure to fulfill the requirements so that new users can be established quickly. People who leave the organization must have access to their mailbox and other systems revoked (often urgently). You may require a policy to define what should be done with e-mail destined for the user (for example, should it be re-routed or rejected). You will also need a procedure to explain what happens to a user’s Exchange data after they leave the organization.

 Public Folder Creation   You can grant users permission to create some public folders, but other folders (especially top-level folders) should be created by administrators only. A procedure should define who can make requests and what permissions should be applied.

 Mailbox Recovery   You can recover an entire mailbox from the deleted mailbox retention dumpster or from a database backup by using a recovery database. Create a procedure for mailbox recovery. For more information about mailbox recovery options, see [Single Mailbox Recovery](http://technet.microsoft.com/en-us/library/dd876954.aspx).

 Full Security Audit   You can perform this audit regularly, in response to an upgrade or redesign of the messaging system, or in response to an attempted (or successful) security breach. The procedure may involve port scans on servers and firewalls, audits of security fixes, and third-party penetration tests.

 Update Performance Baselines   Update performance baselines after an upgrade or configuration change. You can use baselines to measure performance changes and to detect problems that affect system performance.

 Database Maintenance   Exchange databases can become fragmented over time. Typically, online maintenance is sufficient to address this issue. However, in some cases manual defragmentation may be warranted, for example, after moving or deleting a large number of mailboxes. By defragmenting the databases, you can reduce the file size and create contiguous storage space. You can defragment Exchange databases by using Exchange Server Database Utilities (Eseutil.exe). For more information about Eseutil, see [Eseutil.](http://technet.microsoft.com/en-us/library/bb331958.aspx)

* Other Database Maintenance   Other database maintenance is usually reserved for times when you are performing system troubleshooting. You can resolve inconsistencies in Exchange databases by verifying and repairing the integrity of the database by using two new commandlets: *New-MailboxRepairRequest and New-*PublicFolderDatabaseRepairRequest. These new commandlets work with the database mounted. New functionality with the use of the cmdlets in the following list:

(There is no longer a requirement to dismount the database to perform integrity check or fix database errors.

You can repair logical corruption at the mailbox level.

You can fix corrupt search folders.

You can fix Provisional Fid

You can fix Aggregate Counts.

For more information, see [Exchange 2010 SP1: Database Integrity checking](http://blogs.technet.com/b/exchange/archive/2010/08/23/3410708.aspx).

* Message Tracking The Message Tracking tool helps you access and configure delivery reports. When you open this tool, you need to sign in to Outlook Web App as a user who has permission to perform this task. After you sign in, you are directed to the **Delivery Reports** tab. For more information, see [Understanding Message Tracking](http://technet.microsoft.com/en-us/library/bb124375.aspx).
* Mail Flow Troubleshooter The Mail Flow Troubleshooter assists you in troubleshooting common mail flow problems. You can diagnose a problem by selecting the symptoms observed. Based on the symptoms, the tool walks you through the correct troubleshooting path. It shows an analysis of possible root causes and provides suggestions for corrective actions.
* Tracking Log Explorer Tracking Log Explorer provides a detailed log of all message activity as messages are transferred to and from an Exchange server that has the Hub Transport server role, the Mailbox server role, or the Edge Transport server role installed. Exchange servers that have the Client Access server role or Unified Messaging (UM) server role installed don't have message tracking logs. Message tracking logs can be used for message forensics, mail flow analysis, reporting, and troubleshooting.

For more information, see [Managing Tools in the Toolbox](http://technet.microsoft.com/en-us/library/aa997892.aspx)

# ****Evolutions and updates-Servicing****

[**http://technet.microsoft.com/en-us/library/ff637979.aspx**](http://technet.microsoft.com/en-us/library/ff637979.aspx)

## Installing Updates (Rollups and all patches) on DAG Members

|  |  |
| --- | --- |
| Prerequisites: |  |
| **Built-in Exchange 2010 Role required** | Server Management Role |
| **Scope** | Server |
| **Execute on** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup) or an Exchange Server 2010 SP1 |
| **Domain** | Domain in which the Exchange server is hosted |

Before installing update, rollups for Exchange or Windows server and any others patches for hardware on a DAG member follow this procedure. For more details, refer to <http://technet.microsoft.com/en-us/library/ee861125.aspx>

**Note**: In order to update any DAG members, perform the following procedures on each DAG member, only one server at a time. (I.e. one by one)

This is the summary of the process:

1. Suspend activation for the databases on the server being updated.
2. Perform a server switchover so that all databases on the server are passive copies. During the switchover process, there will be a brief interruption in service for the mailboxes hosted on the active databases.
3. Install the updates rollup Exchange and all updates for windows and other patches for the hardware as by planning in the production environments (patches, etc.)
4. Resume activation for the databases on the updated server.
5. Perform database switchovers and rebalance the DAG.

### ****Suspend activation for the database copies on the server being updated****

Log on to a DAG member and launch the Exchange Management Console with Run as administrator privileges.

Get-MailboxDatabaseCopyStatus -Server <SRV\_NAME> | Suspend-MailboxDatabaseCopy -ActivationOnly -Confirm:$False -SuspendComment "*Install E2010 rollup <BUILDNUMBER>*"

### Perform a server switchover on the server being updated

A server switchover is a task that you perform to move all active mailbox database copies from their current Mailbox server to one or more other Mailbox servers in a database availability group (DAG). This task is performed as part of preparation for a scheduled outage for the current Mailbox server.

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "*Mailbox database copies*" entry in the [High Availability Permissions](mk:@MSITStore:D:\My%20Documents\1MyDoc\Help_\Exchange%202010\Exch2010Help.chm::/html/66085107-4d4d-41c3-a425-82314acd9eee.htm) topic.

***Use the EMC to perform a server switchover***

1. In the console tree of the Exchanger Management Console (EMC), navigate to **Server Configuration** > **Mailbox**.
2. In the result pane, select the Mailbox server you want.
3. In the action pane, select **Switchover Server**.
4. In **Switchover server database copies**, either leave it automatically or select target server.
   * Accept the default setting of **automatically choose a target server** (in which case, the system automatically selects the best Mailbox server for each database being switched over), and then click **OK.**
   * Click **Use the specified server as the target for switchover**, click **Browse** to select a Mailbox server, and then click **OK**

**This server will be taken as target server for switchover and once switchover is done a message will be returned.**

**Note: A message warning is sent as “*An active manager operation failed error*” because the public folder databases are unable to switchover on the selected server. As the public folders are not member of the group DAG, it is not possible to switchover on the others servers. You can safely ignore this message.**

***Use the Shell to perform a server switchover***

Execute this command:

Move-ActiveMailboxDatabase -Server <SRV\_NAME>

**Note**: To force all database to be activated on a particular Mailbox server, use this command:

*Move-ActiveMailboxDatabase -Server <SRV\_NAME> -ActivateOnServer <TARGET\_SRV>*

*For detailed syntax and parameter information, see* [*Move-ActiveMailboxDatabase*](mk:@MSITStore:D:\My%20Documents\1MyDoc\Help_\Exchange%202010\Exch2010Help.chm::/html/755d1ecb-95d1-45e3-9a21-56df9f196f37.htm)

### Install the updates rollup Exchange

**Important**: Install the updates on the server by following the update KB note published on the Microsoft Support web site.

Reboot the server if required by the Support KB.

### Resume activation for the databases on the updated server

Get-MailboxDatabaseCopyStatus -Server “<SRV\_NAME>” | Resume-MailboxDatabaseCopy

### Perform database switchovers and re-balance the DAG

***Use Exchange Management Console***

1. In the EMC console, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Database Management** tab, and then click the mailbox database select “<DATABASE>”
3. Click **Activate a Database Copy**.
4. On the **Activate a Database Copy** page, click **Browse** to select the **“<SRV\_NAME>”**
5. Click **Move** to activate the selected passive copy of the database to the updated server.
6. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   * A status of **Completed** indicates that the wizard completed the task successfully.

***Use PowerShell script***

This following script will force all databases to move to their preferred Mailbox server based on the ActivationPreference set with “1”:

RedistributeActiveDatabases.ps1 -DagName <DAGNAME> -BalanceDbsByActivationPreference –Confirm $False

For more information, refer to <http://technet.microsoft.com/en-us/library/dd335158.aspx>

## Replace a hard disk failed in a database of a DAG member

|  |  |
| --- | --- |
| Prerequisites: |  |
| **Built-in Exchange 2010 Role required** | Database Availability Groups Role |
| **Scope** | Server |
| **Execute on** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup) or an Exchange Server 2010 SP1 |
| **Domain** | Domain in which the Exchange server is hosted |

When hard disk failure affects a database, there are two scenarios:

* Active database: PAM will failover the database to another copy
* Passive database: This copy will be tagged as failed

**Procedure**

|  |  |
| --- | --- |
|  |  |
| Replace the failed hard disk in the Mailbox Server | The failed hard disk can be replaced without stopping any services Exchange and database copy must be replicated using update mailbox database copy process. |
| Suspend the database copy | Apply the procedure ***§ Suspend a Mailbox database copy*** |
| Update a Mailbox database Copy | Apply section ***§ Suspend a Mailbox database copy***   |  |  | | --- | --- | | Prerequisites: |  | | **Built-in Exchange 2010 Role required** | Database Availability Groups Role | | **Scope** | Server | | **Execute on** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup) or an Exchange Server 2010 SP1 | | **Domain** | Domain in which the Exchange server is hosted |   ***Use Exchange Management Console***   1. Connect to an Exchange 2010 server or from workstation with Exchange Management Tools. 2. Launch an **Exchange Management Console** with Run as administrator privileges. 3. In the console tree, navigate to **Organization Configuration** > **Mailbox**. 4. In the result pane, on the **Database Management** tab, select the database whose copy you want to suspend. 5. In the work pane, on the **Database Copies** tab, right-click the database for which you want to suspend continuous replication, and then click **Suspend Database Copy**. 6. Add an optional comment of up to 430 characters in the **Comment** field. 7. Click **Yes** to suspend continuous replication.   ***Use Exchange Management Sell console***  Suspend-MailboxDatabaseCopy –Identity *<DATABASE>\<SRV\_NAME>* -SuspendComment "<COMMENT>”  # Validate with “Y” and ENTER  Update a Mailbox database Copy |

## Suspend a Mailbox database copy

|  |  |
| --- | --- |
| Prerequisites: |  |
| **Built-in Exchange 2010 Role required** | Database Availability Groups Role |
| **Scope** | Server |
| **Execute on** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup) or an Exchange Server 2010 SP1 |
| **Domain** | Domain in which the Exchange server is hosted |

***Use Exchange Management Console***

1. Connect to an Exchange 2010 server or from workstation with Exchange Management Tools.
2. Launch an **Exchange Management Console** with Run as administrator privileges.
3. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
4. In the result pane, on the **Database Management** tab, select the database whose copy you want to suspend.
5. In the work pane, on the **Database Copies** tab, right-click the database for which you want to suspend continuous replication, and then click **Suspend Database Copy**.
6. Add an optional comment of up to 430 characters in the **Comment** field.
7. Click **Yes** to suspend continuous replication.

***Use Exchange Management Sell console***

Suspend-MailboxDatabaseCopy –Identity *<DATABASE>\<SRV\_NAME>* -SuspendComment "<COMMENT>”

# Validate with “Y” and ENTER

## Update a Mailbox database Copy

|  |  |
| --- | --- |
| Prerequisites: |  |
| **Built-in Exchange 2010 Role required** | Database Availability Groups Role |
| **Scope** | Server |
| **Execute on** | Workstations (Exchange 2010 SP1 Admin tools installed with the last validated rollup) or an Exchange Server 2010 SP1 |
| **Domain** | Domain in which the Exchange server is hosted |

***Use Exchange Management Console***

1. In the EMC console, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Database Management** click and select “***<DATABASE>***” in the server ***<SRV\_NAME>***
3. In the work pane, on the **Database Copies** tab, right-click the database “***<DATABASE>***” to be update, and then select **Update Database Copy**.
4. On the **Update Database Copy** page, configure the available options for updating a database copy and select the option, “**Delete them and continue to update process”** to remove all existing files and proceed with the seeding operation. By default, once seeding has completed, continuous replication will automatically resume for the database. And select the option “automatically resume data replication from the active database copy to this database copy”
5. Once you have configured the available options, click **Update** to update the database copy.
6. On the **Completion** page, the **Summary** states whether the operation was successful.
7. Click **Finish** to exit the wizard.

***Use Exchange Management Shell***

Update-MailboxDatabaseCopy -Identity *<DATABASE>\<SRV\_NAME>* -SourceServer *<MBX\_SERVER>*

# Disaster Recovery Strategies

A disaster recovery strategy should be developed that is best suited for your business requirements. These strategies and practices help you prepare and be ready in case of a disaster. Some of the strategies include the following:

## Implement Best Practices

One of the critical steps in implementing a Disaster Recovery strategy is implement best practices in the environment. Consider implementing the following best practices to minimize the impact of a Disaster and help avoid the need to perform a restore

* **Use Database Availability Groups to protect Mailbox Data** Microsoft Exchange Server 2010 helps by protecting mailbox databases and the data they contain by configuring your mailbox databases for [high availability and site resilience](http://technet.microsoft.com/en-us/library/dd335211.aspx).
* **Use Deleted Item Retention** Deleted items retention allows a single item or entire folders to be restored from the Microsoft Outlook client without administrator intervention.
* **Use Deleted Mailbox Retention** Deleted mailbox retention allows for the restore of deleted mailboxes by using the Exchange Management Console without restoring from backups.
* **Monitor Servers Proactively** One of the best ways to deal with a disaster is to prevent it before it occurs. Monitor your servers to solve problems before they worsen.
* **Locate Users on Multiple Mailbox Databases** Distributing users across a larger number of mailbox databases can lessen the impact of the loss of a single database, and allow for quicker restores when a restore is needed
* **Document and test your recovery procedures** Documenting and testing the recovery procedures will provide the required validation and help identify any gaps in the process. This also helps ensure that all the staff is trained on disaster recovery procedures.
* **Asset Management** Maintain hardware and software records and have all software, firmware and updates readily available. This also should include all the Design, Build and configuration documents stored in a safe place.
* **Design Considerations** Implement fault tolerance at the hardware or software level. Put your transaction log files and database files on separate physical drives and having sufficient space on hard disk to restore both the database and the log files of your largest database. Implement practices to minimize Exchange database backup and restore times
* **SLA** DevelopService level agreement that meets business requirements for variables such as allowed downtime, allowed recovery time, and data loss tolerance that will define the type of data to protect.
* **Plan for different service failures** Plan for recovering from different service failures, such as a single or multiple database failures, entire mailbox server failure, client access server failure, Hub transport Server failure, edge server failure, dependency service failure.

## Identify Data to Protect

As a part of the disaster recovery strategy, it is critical to identify the data that needs to be protected The Microsoft Exchange Server 2010 data that you must back up depends on which server roles are installed on the server that is running Exchange. In addition, the data that you decide to back up as part of your disaster recovery strategy determines the recovery processes that you can perform.

### Mailbox Servers

This topic identifies the data that is specific to the Microsoft Exchange Server 2010 Mailbox server role. Mailbox server role is designed to store large amounts of end-user data. Although you can recover most of the settings for a Mailbox server from the Active Directory service, your major concern in a disaster recovery scenario for a Mailbox server is the end-user data.

|  |  |  |  |
| --- | --- | --- | --- |
| Critical data | Location | Backup method | Restore method |
| Exchange database files, including both mailbox and public folder databases | File system \Database Copy Path | Exchange-aware vss backup application | Exchange-aware vs backup application |
| Exchange transaction log files that are specific to each database | File system\Database Log Path | Exchange-aware backup application | Exchange-aware backup application |
| Exchange Search information that is specific to each mailbox database copy | File system \Database Copy Path \ CatalogData-<guid>-<guid> | None | Rebuild |
| Offline address book (OAB) | File system  \ExchangeOAB on the Mailbox server that generates the OAB | File system backup | File system restore, or rebuild the OAB |
| Offline address book (OAB) | Public folder | Public folder replication or backup | Public folder replication, backup, or rebuild |
| Windows registry | HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Exchange  HKLM\SYSTEM\currentcontrolset\Services | System state backup or registry export | System state restore or registry import |

### Hub Transport Server

The Hub Transport server role is designed to store all configuration data in the Active Directory directory configuration container. In addition to configuration data, the Hub Transport server stores queues in Microsoft Extensible Storage Engine (ESE) databases, message tracking and protocol logs in files, and limited configuration information in the registry. The queue database is used to store messages while they are being processed by agents and relayed to their final destination on the server. After the message is delivered to an internal or external host, the message is removed from the queue database. Because the data in the database is transient, this database uses circular logging and is not backed up.

|  |  |  |  |
| --- | --- | --- | --- |
| Critical data | Location | Backup method | Restore method |
| Message queues are not backed up. Message queues can be mounted on a new server if they are recovered from a failed server. | File System\TransportRoles\data\Queue | None | Message queues can be mounted on a new server if they are recovered from a failed server. |
| Message tracking and protocol logs are not backed up. The logs are filled with historical data that might be needed for forensic analysis. | File System\TransportRoles\Logs | File level backup | File-level restore |
| There is limited information stored in the registry by Setup that is not essential to server restore. | Windows registry: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Exchange HKLM\SYSTEM\currentcontrolset\Services | System State backup or registry export | System State restore or registry import |

For Transport Server, If Shadow redundancy is configured in the environment; it provides the required resilience and simplifies recovery from a transport server failure. If a transport server fails, you can remove it from production without emptying its queues or losing messages. It eliminates the reliance on the state of any specific Hub Transport or Edge Transport server. As long as redundant message paths exist in your routing topology, any transport server becomes disposable. Follow the steps below to [enable Shadow Redundancy](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Shadow_Redundancy)

### Edge Transport Server

The Edge Transport server role is designed to function as a stand-alone server and does not store any end-user data in the Active Directory service. The Edge Transport server role stores configuration, queues, and data replicated from Active Directory in ADAM Database;

|  |  |  |  |
| --- | --- | --- | --- |
| Critical data | Location | Backup method | Restore method |
| Active Directory Application Mode (ADAM). Data is replicated from Active Directory. If custom settings are applied, those will be backed up with the ExportEdgeConfig.ps1 file. | File System\TransportRoles\data\Adam | Clone Config (ExportEdgeConfig.ps1) | Clone Config (ImportEdgeConfig.ps1) and EdgeSync |
| Content Filtering ESE database will not be backed up. Instead, user settings will be cloned. Only custom settings are needed. If nothing was changed, nothing needs to be backed up. | File System\TransportRoles\data\IpFilter | Clone Config (ExportEdgeConfig.ps1) | Clone Config (ImportEdgeConfig.ps1) |
| Message queues are not backed up. Message queues can be mounted on a new server if they are recovered from a failed server. | File System\TransportRoles\data\Queue | None | None |
| Message tracking and protocol logs are not backed up. The logs contain historical data that might be needed for forensic analysis. | File System\TransportRoles\Logs | File level backup | File level restore |
| There is limited information stored in the registry by Setup that is not essential to server restore. | Windows registry:   * HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Exchange * HKLM\SYSTEM\currentcontrolset\Services | System State backup or registry export | System State restore or registry import |

### Client Access Server

The Client Access server role stores configuration data in the Active Directory service Database, the Internet Information Services (IIS) metabase, and local configuration files. Parts of the two data stores (IIS and Active Directory) are not synchronized or duplicated.

|  |  |  |  |
| --- | --- | --- | --- |
| Critical data | Location | Backup method | Restore method |
| Microsoft Office Outlook Web Access Web site, and Web.config file | File system  \ClientAccess\Owa | File-level backup | File-level restore |
| IMAP4 and POP3 protocol settings | File system  \ClientAccess\ | File-level backup | File-level restore |
| Availability service | Active Directory configuration container and file system, including the Web.config file  \ClientAccess\exchweb\ews | Domain controller replication or Active Directory backup  File-level backup | Use Exchange Management Shell scripts to configure Availability service  File-level restore |
| Autodiscover | IIS metabase | System state backup, metabase export of Web sites | System state restore, or metabase import of the Web sites |
| Exchange ActiveSync | * Active Directory configuration container * File system, including the Web.config file in the \ClientAccess\Sync folder * IIS Metabase | Domain controller replication or Active Directory backup  File-level backup  Metabase export of Web sites | Use Exchange Management Shell scripts to reconfigure the service.  File-level restore  Metabase import |
| Outlook Web Access virtual directories | Active Directory configuration container and file system  \ClientAccess\ | Domain controller replication or Active Directory backup  File-level backup | Use Exchange Management Shell scripts to configure clean Outlook Web Access virtual directories to match the old virtual directories  File-level restore |
| Registry (There is very limited information stored in the registry by Setup that is not essential to server restore. Unless changes were made to the settings, those changes should be backed up.) | Microsoft Windows registry | System state backup or registry export | System state restore or registry import |
| Web services configuration | IIS metabase | System state backup; metabase export of Web sites | System state restore or metabase import |

### Active Directory Data

As part of your Exchange disaster recovery planning, you should understand the dependence that Exchange has on Active Directory. Servers running Exchange use Active Directory extensively for the following:

* Active Directory is the configuration repository for Exchange organization data. Without this configuration information, Exchange servers cannot start or function.
* All Exchange directory information, including configuration information regarding mailboxes, contacts, distribution lists, servers, and sites within the Exchange organization, is stored in Active Directory.
* Items such as distribution lists and access permissions for users and groups are also stored within Active Directory.

|  |  |  |  |
| --- | --- | --- | --- |
| Critical data | Location | Backup method | Restore method |
| Active Directory domain container | Active Directory  DC=<Domain>,DC=<Domain\_Root> | System State backup of a domain controller | System State restore of a domain controller |
| Active Directory configuration container | Active Directory  CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain>,DC=<Domain\_Root> | System State backup of a domain controller | System State restore of a domain controller |
| Active Directory schema container | Active Directory  CN=Schema,CN=Configuration,DC=<Domain>,DC=<Domain\_Root> | System State backup of a domain controller | System State restore of a domain controller |

### Unified Messaging Server

The Unified Messaging server stores the majority of its configuration information in Active Directory, transient message queues in the file system, limited server setup information in the registry, server-specific configuration data in XML files in the \bin folder, and custom audio files in the file system.

|  |  |  |  |
| --- | --- | --- | --- |
| Critical data | Location | Backup method | Restore method |
| Custom audio prompts:   * Custom audio files (.wav) for UM Dial Plans and UM Auto Attendants * Custom audio files (.wav) for telephone user interface (TUI) or Microsoft Outlook Voice Access | File system  \UnifiedMessaging\Prompts | File-level backup is only needed on the prompt publishing server. | File-level restore is only needed on the prompt publishing server. |
| Incoming calls: .eml and .wma files for each voice mail | File system  \UnifiedMessaging\temp | None | None |
| Server configuration data | Active Directory configuration container | Backup method is domain controller replication or Active Directory backup. | This data is reapplied to a server during a **Setup /m:recoverserver** restore. |
| Limited information is stored in the registry by Setup that is not essential to server restore. | Microsoft Windows registry:   * HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Exchange * HKLM\SYSTEM\currentcontrolset\Services | Backup method is system state backup or registry export. | Restore method is system state restore or registry import. |

### Other

When you are planning for a disaster recovery plan, you should understand the backup and restore methods available for end user data like PSTs, Profile information, Microsoft Office Outlook custom configuration files where Outlook stores local end user client customizations.

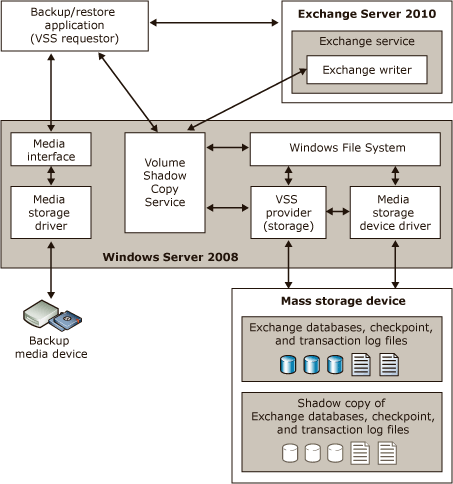
# Backup Process and Procedures

Data Protection in Exchange 2010 for the Mailbox Database can be achieved in different ways based on the organizational business requirements. The options available are

1. VSS-based backups of Exchange data
2. Exchange Native Data Protection

## VSS-based backups of Exchange data

Exchange 2010 only supports the use an Exchange-aware application that supports the VSS writer for Exchange 2010, such as Windows Server Backup (with the VSS plug-in), Microsoft System Center Data Protection Manager, or a third-party Exchange-aware VSS-based application. The Volume Shadow Copy Service (VSS) provides an infrastructure that enables third-party storage management programs, business programs, and hardware providers to cooperate to create and manage shadow copies. Solutions that are based on this infrastructure, and use the Exchange 2010 VSS Writer, can use the shadow copies to back up and restore one or more Exchange 2010 databases.



The Planning of a backup solution should include the limitations below when using VSS for backup and restore of Exchange data:

* The VSS plug-in that ships with Exchange 2010 can be used to back up volumes containing active mailbox database copies or standalone (non-replicated) mailbox databases only. It can't be used to back up volumes containing passive mailbox database copies. To back up passive mailbox database copies, you need either Microsoft System Center Data Protection Manager or a third-party Exchange-aware VSS-based application.
* Passive mailbox database copies are backed up using a separate VSS writer in the Microsoft Exchange Replication service. The Microsoft Exchange Replication service VSS Writer doesn't support restores. Although you can back up a passive mailbox database copy using Microsoft System Center Data Protection Manager or a third-party Exchange-aware VSS-based application, you can't perform a VSS restore directly to a passive mailbox database copy. However, you can perform a VSS restore to an alternate location, suspend replication to the passive copy, and then copy the database and log files from the alternate location to the location of the passive database copy in the file system.
* To be compliant with Exchange 2010 and to guarantee the integrity and recoverability of shadow copy backups, VSS-based backup applications must comply with the following basic requirements:
  + Exchange 2010 database, transaction log, and checkpoint files must be backed up exclusively through the Microsoft Exchange Server 2010 Writers for the Windows Server 2008 Volume Shadow Copy Service.
  + The backup application must validate the integrity of the shadow copy backup set.
  + Restores onto a computer that is running Exchange 2010 in most cases use the Exchange 2010 Store Writer. In some cases the application will instead place the data into the database directory, and then remount the store.
* The Store Writer and the Replication Writer in Exchange 2010 support full, copy, differential, and incremental backups

### Use Windows Server Backup to Perform a Backup of Exchange

Microsoft Exchange Server 2010 includes a plug-in for Windows Server Backup that allows you to make Volume Shadow Copy Service (VSS)-based backups of Exchange data. You can use Windows Server Backup to back up and restore your Exchange databases. During the backup operation, a consistency check of the Exchange data files is run to make sure that the files are in a good state and can be used for recovery. Some of the pre requisites for Windows Server backup are

* This procedure can only be performed locally on a computer running Exchange 2010 on the Windows Server 2008 or Windows Server 2008 R2 operating system.
* The Windows Server Backup feature must be installed on the local computer.
* If a server hosting the data being backed up is a member of a database availability group (DAG) and hosts both active and passive database copies, you must disable the Microsoft Exchange Replication service VSS writer. To disable the Microsoft Exchange Replication service VSS writer, Navigate to HKEY\_LOCAL\_MACHINE\Software\Microsoft\ExchangeServer\v14\Replay\Parameters and Add a new DWORD value named **EnableVSSWriter**, and set its value to **0**.

1. Start Windows Server Backup.
2. In the **Actions** pane, click **Backup Once**. The Backup Once wizard appears.
3. On the **Backup options** page, select **Different options**, and then click **Next**.
4. On the **Select backup configuration** page, select the type of backup that you want, and then click **Next**:
   1. Select **Full server (recommended)** to back up all volumes on the server.
   2. Select **Custom** to specify which volumes should be included in the backup. If you select this option, the **Select backup items** page appears. Select the volumes to be backed up, and then click **Next**.  
      Note:

By default, volumes that contain operating system components or applications are included in the backup and can't be excluded.

1. On the **Specify destination type** page, select the location where you want to store the backup, and then click **Next**. If **Remote shared folder** is selected, the **Specify remote folder** page appears. Specify a UNC path for the backup files, and then do one of the following to configure access control settings:
   1. Select **Do not inherit** if you want the backup to be accessible only by a set of specified user credentials, and then click **Next**. Type a user name and password for a user account that has write permissions on the computer that is hosting the remote folder, and then click **OK**.
   2. Select **Inherit** if you want the backup to be accessible by everyone who has access to the remote folder, and then click **Next**.
2. On the **Specify advanced options** page, select **VSS full backup**, and then click **Next**.
3. On the **Confirmation** page, review the backup settings, and then click **Backup**.
4. On the **Backup progress** page, you can view the status and progress of the backup operation.
5. Click **Close** when the backup operation has completed.

## Exchange Native Data Protection

Exchange 2010 includes several new features and core changes that, when deployed and configured correctly, can provide native data protection that eliminates the need to make traditional backups of your data. The technical feasibility should be evaluated against the business requirements to validate the solution. The requirements for Backup have to be mapped to the Exchange 2010 features available and careful planning and evaluation of the impact of data loss should be considered when looking into eliminating the Traditional Backups and use Exchange Native Data Protection. Some of the reasons for Backup that should be evaluated are below. But other requirements based on the business needs should also be considered

Use the following table to decide whether you need to continue utilizing a traditional backup model or whether you can implement the native data protection features in Exchange 2010.

|  |  |
| --- | --- |
| Issue | Mitigation |
| Software failures | Mailbox resiliency (multiple database copies) |
| Hardware failures | Mailbox resiliency (multiple database copies) |
| Site or data center failures | Mailbox resiliency (multiple database copies) |
| Accidental or malicious deletion of items | Single item recovery and deleted item retention with a window that meets or exceeds the item recovery SLA |
| Physical corruption scenarios | Single page restore (highly available database copies) |
| Logical corruption scenarios | Single item recovery  Calendar Repair Assistant  Mailbox moves  **New-MailboxRepairRequest** cmdlet  Point-in-time backup |
| Administrative errors | Point-in-time backup |
| Automation errors | Point-in-time backup |
| Rogue administrators | Point-in-time backup (isolated) |
| Corporate or regulatory compliance requirements | Point-in-time backup (isolated) |

### Mailbox Resiliency

In Microsoft Exchange Server 2010, you can protect mailbox databases and the data they contain by configuring your mailbox databases for high availability and site resilience. Exchange 2010 provides the data redundancy by using Database availability groups and up to 16 Database copies in geographically distributed sites. Any server in a DAG can host a copy of a mailbox database from any other server in the DAG. When a server is added to a DAG, it works with the other servers in the DAG to provide automatic recovery from failures that affect mailbox databases, such as a disk failure or server failure. The architecture has changed so that automatic failover protection is now provided at the individual mailbox database level instead of at the server level also known as *database mobility*. As a result of this and other database cache architectural changes, failover actions now complete much faster than in previous versions of Exchange.

SP1 also introduces a new form of continuous replication known as continuous replication - block mode. In block mode, as each update is written to the active database copy's active log buffer, it's also shipped to a log buffer on each of the passive mailbox copies. When the log buffer is full, each database copy builds, inspects and creates the next log file in the generation sequence. In the event of a failure affecting the active copy, the passive copies will have been updated with most or all of the latest updates. The active copy doesn't wait for replication to complete in order to preclude replication issues from affecting the client experience.

The transport dumpster has also been enhanced to account for the changes to the Mailbox server role that enable a single mailbox database to move between Active Directory sites. DAGs can be extended to multiple Active Directory sites, and as a result, a single mailbox database in one Active Directory site can fail over to another Active Directory site. When this occurs, any transport dumpster redelivery requests will be sent to both Active Directory sites: the original site and the new site.

The following list includes some of these considerations for Implementing Exchange Native Data Protection, although the list isn't exhaustive. There may also be special considerations or considerations unique to your organization. Consider the following issues:

* How many copies of the database will be deployed? **We strongly recommend deploying a minimum of three (non-lagged) copies of a mailbox database before eliminating traditional forms of protection for the database, such as RAID or traditional VSS-based backups.**
* Your recovery time objective and recovery point objective goals should be clearly defined, and you should establish that using a combined set of built-in features in lieu of traditional backups enables you to meet these goals.
* You should determine how many copies of each database are needed to cover the various failure scenarios against which your system is designed to protect.
* If you eliminate the use of a DAG or some of its members, does that capture sufficient costs to support a traditional backup solution? If so, does that solution improve your recovery time objective or recovery point objective service level agreements (SLAs)?
* Can you afford to lose a point-in-time copy if the DAG member hosting the copy experiences a failure that affects the copy or the integrity of the copy?
* Exchange 2010 allows you to deploy larger mailboxes, and the recommended maximum mailbox database size has been increased from 200 gigabytes (GB) in Exchange 2007 to 2 terabytes (when two or more highly available mailbox database copies are being used). Based on the larger mailboxes that most organizations are likely to deploy, what will your recovery point objective be if you have to replay a large number of log files when activating a database copy or a lagged database copy?
* How will you detect and prevent logical corruption in an active database copy from replicating to the passive copies of the database? What is your recovery plan for this situation? How frequently has this scenario occurred in the past? If logical corruption occurs frequently in your organization, we recommend that you factor that scenario into your design by using one or more lagged copies, with a sufficient replay lag window to allow you to detect and act on logical corruption when it occurs, but before that corruption is replicated to other database copies.

For more information, <http://technet.microsoft.com/en-us/library/dd335211.aspx>

### Single Item Recovery

Single item recovery provides an additional layer of protection so that you can recover items accidentally deleted by a user or by automated processes such as the Managed Folder Assistant. Single item recovery simplifies recovery and reduces recovery time because you can recover items without recovering an entire mailbox or mailbox database from backup media.

**Enable Single Item Recovery for a Mailbox**use the Exchange Management Shell to enable single item recovery on a mailbox.

*Set-Mailbox -Identity MBX01 -SingleItemRecoveryEnabled $True*

### Single Page Restore

When a lost flush condition occurs (when the database pages checksum matches), but the data on the pages is wrong logically. This can occur when ESE attempts to write a database page and even though the operating system returns a success message, the data is either never written to the disk or it's written to the wrong place. To prevent lost flushes from losing data, ESE includes a lost flush detection mechanism in the database along with a page patching feature (single page restore).

The following are the steps involved in the Single Page Restore Process on an Active Copy

1. Page corruption detected on Active Copy (e.g. -1018)
2. Active DB places *marker* in log stream to notify passive copies to ship up to date page
3. Passive receives log and replays up to marker, retrieves good page, invokes Replay Service callback and ships page
4. Active receives good page, writes page to log, DB page is *patched*
5. Subsequent page repair from additional copies ignored

The following are the steps involved in the Single Page Restore Process on an Passive Copy

1. Page corruption detected on DB Copy (e.g. -1018)
2. Passive copy pauses log replay (log copying continues)
3. Passive retrieves the corrupted page # from the active using DB seeding infrastructure
4. Passive copy waits till log file which meets max required generation requirement is copied/inspected, then patches page
5. Passive resumes log replay

### Calendar Repair

The Calendar Repair Assistant detects and corrects inconsistencies that occur for single and recurring meeting items for mailboxes homed on that Mailbox server so that recipients won't miss meeting announcements or have unreliable meeting information

**Detects inconsistencies** The Calendar Repair Assistant uses the organizer's copy of the calendar item as a master copy for all meeting items. The assistant compares the attendee's calendar item with the organizer's calendar item for inconsistencies. The only exception to this rule is when the assistant compares the attendee's and organizer's response status. The assistant assumes that the attendee's response status is the correct one, and, if necessary, updates the organizer's tracking information.

**Determines if inconsistencies were intentional** If an inconsistency is detected, the Calendar Repair Assistant determines whether the attendee intentionally introduced the inconsistency. For example, an attendee can introduce an inconsistency by deleting the meeting request and not notifying the organizer. If the assistant determines that the attendee didn't introduce the inconsistency, it corrects the problem. If the assistant can't determine if the inconsistency was intentional, it performs no further action.

**Corrects inconsistencies** The Calendar Repair Assistant corrects inconsistencies on the Mailbox server on which it runs. However, if the organizer's mailbox is on a different server than the attendee's mailbox, the assistant reads from other Exchange 2010 Mailbox servers to compare the calendar items. The assistant doesn't overwrite the recipient's calendar information. Instead, it merges the information so data isn't lost. In addition, the repair update messages are moved to the recipient's Deleted Items folder. For more information about the inconsistencies detected and repaired, see Conflict Detection and Resolution later in this topic.

**Sends a calendar repair update message if a correction was made**  Calendar repair update messages are sent to users whose calendar items were updated by the Calendar Repair Assistant. Instead of sending the message to the user's Inbox, the assistant sends the message to the user's Deleted Items folder. By doing so, a record of the repair is kept in the mailbox without causing user confusion. If the user is experiencing calendar inconsistencies, you can advise the user to look in the Deleted Items folder for troubleshooting purposes. The assistant only sends repair update messages if the issue is fixed.

To enable Calendar Repair Assistant for a Mailbox,

*Set-Mailbox -Identity <mailboxName> -CalendarRepairDisabled $false*

### Mailbox Moves

During mailbox moves, the Microsoft Exchange Mailbox Replication service detects corrupted items and won't move those items to the target mailbox database.

To move a mailbox from one database to another Database

*New-MoveRequest -Identity <Alias> -TargetDatabase <DatabaseName> -ArchiveTargetDatabase -<DatabaseName>*

### New-MailboxRepairRequest

Service Pack 1 introduces the New-MailboxRepairRequest which can address corruptions with search folders, item counts, folder views, and parent/child folder issues

Use the **New-MailboxRepairRequest** cmdlet to detect and fix mailbox corruptions. You can run this command against a specific mailbox or against a database. While this task is running, mailbox access is disrupted only for the mailbox being repaired. If you're running this command against a database, only the mailbox being repaired is disrupted. All other mailboxes on the database remain operational.

To detect and repair all folder views for the mailbox

*New-MailboxRepairRequest -Mailbox <userAlias> -CorruptionType FolderView*

### Personal Archive

In Microsoft Exchange Server 2010, personal archives provide users with an alternate storage location in which to store historical messaging data. A personal archive is an additional mailbox (called an archive mailbox) enabled for a mailbox user. Outlook 2010, Outlook 2007, and Outlook Web App users have seamless access to their archive mailbox. Using either of these client applications, users can view an archive mailbox and move or copy messages between their primary mailbox and the archive. Personal archives present a consistent view of messaging data to users and eliminate the user overhead required to manage .pst files. Eliminating the use of .pst files significantly reduces your organization's exposure to the risks outlined in the previous section.

**Enable a Personal Archive for Mailboxes in a Database**

*Get-Mailbox -Database DB01 | Enable-Mailbox -Archive*

# Recovery Process and Procedures

There are a number of restore and recovery procedures for Microsoft Exchange Server 2010. The type of Recovery process varies based on the Server Roles installed on the Server and the disaster recovery plan for that server. The Recovery process could be used in different types of failures like server loss caused by software or hardware loss, or by physical loss of the site. The Recovery Operations Guide should include the steps required for various types of failures

## Client Access Server

If the Messaging Environment architecture has High Availability designed for the Client Access Servers using a Load Balancer or NLB, and if a failure occurs for Client Access Services, the load balancer will automatically redirect the client requests to the active server. The possible failures that can occur on a Client Access Server are

### Server Failure: Hardware

When a hardware failure occurs, the monitoring solution in place should alert about the failure and the hardware vendor should replace the required failed parts with in the defined SLA.

When a Complete Hardware failure occurs and the server needs to be restored to an alternative hardware, follow the steps defined in the How to Guides: [Recover an Exchange Server](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Recover_an_Exchange)

Use the Client Access Server Build Guide to reconfigure the custom settings that are configured on the server

### Server Failure: Software

When a software failure occurs due to Windows patches, firmware updates and driver updates, the Team will work on uninstalling the related Patches following the guidelines defined by the patch documentation.

When a software failure occurs due to Exchange Patches, the Messaging Group should work on rolling back the updates applied to the servers

* To remove an Exchange 2010 update rollup package that is installed on Windows Server, open Installed Updates in Add or Remove Programs in Control Panel, and then select the appropriate update based on the Knowledge Base article.
* When a Complete Hardware failure occurs and the server needs to be restored to an alternative hardware, follow the steps defined in the How to Guides: [Recover an Exchange Server](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Recover_an_Exchange)

### Non Recoverable Failure

When a failure occurs that is non-recoverable and the server needs to be restored to an alternative hardware, follow the steps defined in the How to Guides: [Recover an Exchange Server](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Recover_an_Exchange)

### Site Failure

Clients connect to service endpoints (for example Outlook Web App, Autodiscover, Exchange ActiveSync, Outlook Anywhere, POP3, IMAP4, and the RPC Client Access array) to access Exchange services and data. Therefore, activating Client Access servers involves changing the mapping of the DNS records for these service endpoints from IP addresses in the primary datacenter to the IP addresses in the second datacenter that are configured as the new service endpoints. Depending on your DNS configuration, the DNS records that need to be modified may or may not be in the same DNS zone.

Clients will then automatically connect to the new service endpoints in one of two ways:

* Clients will continue to try to connect, and should automatically connect after the TTL has expired for the original DNS entry, and after the entry is expired from the client's DNS cache. Users can also run the ipconfig /flushdns command from a command prompt to manually clear their DNS cache.
* Clients starting or restarting will perform a DNS lookup on startup and will get the new IP address for the service endpoint, which will be a Client Access server or array in the second datacenter.

Assuming that all appropriate configuration changes have been completed to define and configure the services in the second datacenter to function as they were in the primary datacenter, this includes configuration information Related to

* Client Access Array
* Internal and External URLs for OWA, ECP, EWS, ActiveSync, OAB
* Authentication settings for various virtual directories
* Outlook Anywhere Configuration
* Proxying and Redirection Configuration

Assuming that the established DNS configuration is correct, no further changes should be needed to activate Client Access servers.

## Hub Transport Server

If Shadow redundancy is configured in the environment, it provides the required resilience and simplifies recovery from a transport server failure. Follow the steps below to [enable Shadow Redundancy](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Shadow_Redundancy)

### Server Failure: Hardware

When a hardware failure occurs, the monitoring solution in place should alert about the failure and the hardware vendor should replace the required failed parts with in the defined SLA.

When a Complete Hardware failure occurs and the server needs to be restored to an alternative hardware, follow the steps defined in the How to Guides: [Recover an Exchange Server](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Recover_an_Exchange)

Use the Hub Transport Server Build Guide to reconfigure the custom settings that are configured on the server

If Shadow redundancy is configured in the environment, it provides the required resilience and simplifies recovery from a transport server failure. Follow the steps below to [enable Shadow Redundancy](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Shadow_Redundancy)

### Server Failure: Software

When a software failure occurs due to Windows patches, firmware updates and driver updates, the Team will work on uninstalling the related Patches following the guidelines defined by the patch documentation.

When a software failure occurs due to Exchange Patches, the Messaging Group should work on rolling back the updates applied to the servers

* To remove an Exchange 2010 update rollup package that is installed on Windows Server, open Installed Updates in Add or Remove Programs in Control Panel, and then select the appropriate update based on the Knowledge Base article.
* When a Complete Hardware failure occurs and the server needs to be restored to an alternative hardware, follow the steps defined in the How to Guides: [Recover an Exchange Server](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Recover_an_Exchange)

### Non Recoverable Failure

When a failure occurs that is non-recoverable and the server needs to be restored to an alternative hardware, follow the steps defined in the How to Guides: [Recover an Exchange Server](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Recover_an_Exchange)

### Site Failure

Clients and other servers that submit messages to Hub Transport servers typically identify those servers using DNS. Activating Hub Transport servers involves changing DNS records to point to the IP addresses of the Hub Transport servers in the second datacenter. Clients and sending servers will then automatically connect to the Hub Transport servers in the second datacenter in one of two ways:

* Clients will continue to try to connect, and should automatically connect after the TTL has expired for the original DNS entry, and after the entry is expired from the client's DNS cache. Users can also run the ipconfig /flushdns command from a command prompt to manually clear their DNS cache.
* Clients starting or restarting will perform a DNS lookup on startup and will get the new IP address for the SMTP endpoint, which will be a Hub Transport server in the second datacenter.

Assuming that all appropriate configuration changes have been completed to define and configure the services in the second datacenter to function as they were in the primary datacenter, this also includes any changes required for internet email if a third party solution is used. Assuming that the established DNS configuration is correct, no further changes should be needed to activate Hub Transport servers.

## Edge Transport Server

### Server Failure: Hardware

When a hardware failure occurs, the monitoring solution in place should alert about the failure and the hardware vendor should replace the required failed parts with in the defined SLA.

When a Complete Hardware failure occurs and the server needs to be restored to an alternative hardware, follow the steps defined in the How to Guides: [Recover an Exchange Server](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Recover_an_Exchange)

Use the Hub Transport Server Build Guide to reconfigure the custom settings that are configured on the server

### Server Failure: Software

When a software failure occurs due to Windows patches, firmware updates and driver updates, the Team will work on uninstalling the related Patches following the guidelines defined by the patch documentation.

When a software failure occurs due to Exchange Patches, the Messaging Group should work on rolling back the updates applied to the servers

* To remove an Exchange 2010 update rollup package that is installed on Windows Server, open Installed Updates in Add or Remove Programs in Control Panel, and then select the appropriate update based on the Knowledge Base article.
* When a Complete Hardware failure occurs and the server needs to be restored to an alternative hardware, follow the steps defined in the How to Guides: [Recover an Exchange Server](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Recover_an_Exchange)
* Use the Edge Server Cloned Configuration Recovery to recover the configuration information, follow the steps defined in the How to Guides: [Edge Transport Server Cloned Configuration](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Edge_Transport_Server)

### Non Recoverable Failure

When a failure occurs that is non-recoverable and the server needs to be restored to an alternative hardware, follow the steps defined in the How to Guides: [Recover an Exchange Server](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Recover_an_Exchange)

Use the Edge Server Cloned Configuration Recovery to recover the configuration information, follow the steps defined in the How to Guides: [Edge Transport Server Cloned Configuration](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Edge_Transport_Server)

### Site Failure

The steps to activate the Edge Transport server role will vary, depending on the specific configuration. Edge Transport servers in two datacenters can be configured in either an active/passive or an active/active configuration. In an active/passive configuration, the Edge Transport server in the second datacenter is idle until the second datacenter is activated. In an active/active configuration, Edge Transport servers in both datacenters are delivering mail at all times.

In an active/active configuration, no steps are necessary to activate the second datacenter's Edge Transport servers because they are already running. In an active/passive configuration, the DNS MX resource record for each SMTP domain needs to be updated as part of the switchover from the primary datacenter to the standby datacenter. Although the active/active configuration provides a simple datacenter switchover solution, it has the drawback of requiring careful load monitoring to make sure that after the datacenter switchover, the Edge Transport servers in the second datacenter can provide sufficient capacity to support the increased load now flowing through it, as a result of the Edge Transport servers in the primary datacenter being unavailable.

Even with an active/active configuration, it may be appropriate to update the MX resource records for your Edge Transport servers during a datacenter switchover. Allowing the MX resource record for the failed datacenter to continue to point at the failed datacenter means that when the datacenter starts recovering, it could start experiencing connection attempts to its Edge Transport servers. This could happen while the Edge Transport services are in an unstable state (for example, because dependent services in the datacenter are being restored).

Assuming the DNS records are under the control of the organization, activating Edge Transport servers involves updating the MX resource record for each SMTP domain hosted by the server.

DNS updates enable incoming traffic, and outgoing traffic is handled by the activation of the mailbox databases in a site that has functioning Edge Transport servers:

* When incoming SMTP connections are initiated using the updated name resolution information, SMTP clients will connect to the Edge Transport servers in the second datacenter. Traffic will be appropriately routed by the Edge Transport server, and no further changes are required.
* When outgoing SMTP connections are initiated, they will try the locally available Edge Transport server, and those messages will be queued or immediately sent based on the status of the receiving server.

## Mailbox Server

### Lost Mail Item

To protect from accidental or malicious deletion, Microsoft Exchange Server 2010 provides the Recoverable Items folder. The Recoverable Items folder replaces the feature known as the dumpster in Exchange Server 2007. The Recoverable Items folder is used by the following Exchange features:

**Deleted item retention**  
An item is considered to be soft deleted in the following cases:

* A user deletes an item or empties all items from the Deleted Items folder.
* A user presses Shift+Delete to delete an item from any other mailbox folder.

Soft-deleted items are moved to the Deletions subfolder of the Recoverable Items folder. This provides an additional layer of protection so users can recover deleted items without requiring Help desk intervention. Users can use the Recover Deleted Items feature in Outlook or Outlook Web App to recover a deleted item.

Items remain in the Deletions subfolder until the deleted item retention period is reached. The default deleted item retention period for a mailbox database is 14 days. You can modify this period for a mailbox database or for a specific mailbox. In addition to a deleted item retention period, the Recoverable Items folder is also subject to quotas.   
After the deleted item retention period elapses, the item is moved to the Purges folder and is no longer visible to the user. When the Managed Folder Assistant processes the mailbox, items in the Purges subfolder are purged from the mailbox database.

To recover deleted items from the Deleted Items folder with Outlook

1. Open an Outlook client that has access to the mailbox that has deleted items.
2. Select the **Deleted Items** folder.
3. From the **Tools** menu, select **Recover Deleted Items**.
4. Select the item that you want to recover, and then click **Recover Selected Items**.

Description: http://i.msdn.microsoft.com/Global/Images/clear.gifTo use the DumpsterAlwaysOn registry key to recover hard-deleted items for all the folders in outlook.

1. On the client computer used to perform the deleted items recovery operation, click **Start**, click **Run**, type **regedit**, and then click **OK.**
2. Locate, and then click the following registry subkey:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Exchange\Client\Options

1. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
2. Type **DumpsterAlwaysOn**, and then press **ENTER**.
3. Double-click **DumpsterAlwaysOn**.
4. Type **1** in the **Value** **data** area, click **Decimal** in the **Base** area, and then click **OK**.
5. Close Registry Editor.
6. Restart Outlook.

Description: http://i.msdn.microsoft.com/Global/Images/clear.gifTo recover deleted items from any folder with Outlook

1. If the **DumpsterAlwaysOn** registry key has not been set, set it before proceeding by following the steps outlined in "To use the DumpsterAlwaysOn registry key to recover hard-deleted items" earlier in this topic. If the DumpsterAlwaysOn registry key has been set, proceed to Step 2.
2. Open an Outlook client that has access to the mailbox that has deleted items.
3. Select the folder that has deleted items in it.
4. From the **Tools** menu, select **Recover Deleted Items**.
5. Select the items that you want to recover, and then click **Recover Selected Items**.

**Single item recovery**

The method you use to search for and recover missing items depends on the client access license (CAL) for the mailbox you're searching. If the mailbox has an enterprise CAL, you can use the Multi-Mailbox Search feature in the Exchange Control Panel (ECP) or the **New-MailboxSearch** cmdlet in the Shell. These features also allow you to search multiple mailboxes simultaneously.

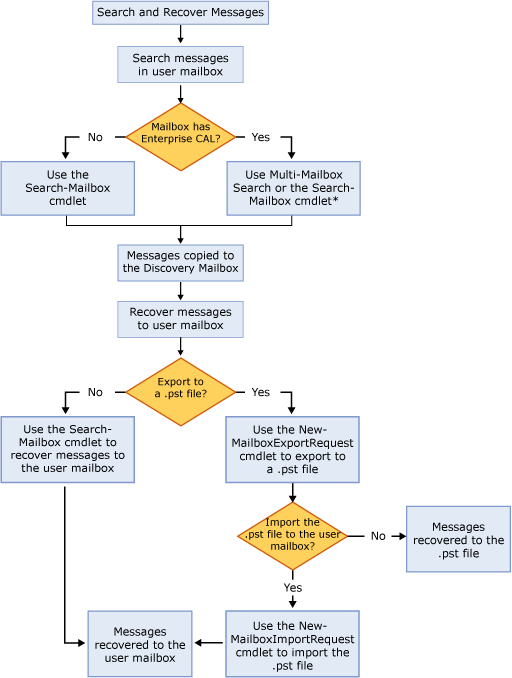
You can also use the **Search-Mailbox** cmdlet in the Shell to search for and recover missing items. If the mailbox has a standard CAL, this is the only method you can use. If you use this cmdlet, you can search only one mailbox at a time.

To search for and recover items, you must have the following information:

**Source mailbox:** This is the mailbox being searched.

**Target mailbox:** This is the discovery mailbox in which messages will be recovered. Exchange Setup creates a default discovery mailbox.

**Search criteria**: Criteria include sender or recipient, or keywords (words or phrases) in the message.



**Search for and recover missing items**

*Search-Mailbox "<mailboxName>" -SearchQuery "from:'<sender>' AND keywords" -TargetMailbox "Discovery Search Mailbox" -TargetFolder "<Target Recovery Folder>” -LogLevel Full*

***Restore recovered items***

***New-MailboxExportRequest -Mailbox "Discovery Search Mailbox" -SourceRootFolder*** *"<Target Recovery Folder>”*  ***-ContentFilter {Subject -eq "<subject>"} -FilePath <pathtopstfile>***

### Lost Mailbox

When a mailbox is deleted the mailboxes remain in the Exchange database for the duration specified in the deleted mailbox retention settings for the mailbox database. By default, disconnected mailboxes are retained for 30 days. During this retention period, a mailbox can be recovered by connecting it to a new or existing Active Directory user account. A disconnected mailbox is a mailbox object in the Exchange store that isn't associated with an Active Directory user account.

There are two types of disconnected mailboxes:

**Soft-deleted mailboxes:** When mailboxes are moved from a Microsoft Exchange Server 2010 Service Pack 1 (SP1) database to any other database, Exchange doesn't fully delete the mailbox from the source database upon completion of the move. Instead, the mailbox in the source mailbox database is switched to a *soft-deleted* state. With soft-deleted mailboxes, you can use the **MailboxRestoreRequest** cmdlet set to access mailbox data during a mailbox restore operation. Soft-deleted mailboxes are retained in the source database until either the deleted mailbox retention period expires or until the **Remove-StoreMailbox** cmdlet is used to purge the mailbox.

**Restore a soft-deleted mailbox**  
Use the Get-MailboxStatistics cmdlet to find the display name, legacy distinguished name (DN), or mailbox GUID of the soft-deleted mailbox.

1. This example returns the DisplayName, LegacyDN, MailboxGUID, and DisconnectReason values for all mailboxes on mailbox database MBD01 that have a disconnect reason of SoftDeleted.  
     
   Get-MailboxStatistics -Database MBD01 | Where { $\_.DisconnectReason -eq "SoftDeleted" } | Format-List LegacyDN, DisplayName, MailboxGUID, DisconnectReason

Use the New-MailboxRestoreRequest cmdlet to create the restore request.

1. This example restores the source mailbox that has the display name User1 on mailbox database MBD01 to User1's mailbox.  
   New-MailboxRestoreRequest -SourceDatabase "MBD01" -SourceStoreMailbox "User1" -TargetMailbox User1
2. This example restores the source mailbox that has the mailbox GUID 1d20855f-fd54-4681-98e6-e249f7326ddd on mailbox database MBD01 to User2’s archive mailbox.  
   New-MailboxRestoreRequest -SourceDatabase "MBD01" -SourceStoreMailbox 1d20855f-fd54-4681-98e6-e249f7326ddd -TargetMailbox User2 –TargetIsArchive

**Disabled mailboxes:** When a mailbox is disconnected or removed using the **Disable-Mailbox** or **Remove-Mailbox** cmdlet, Exchange retains the deleted mailbox, and the mailbox is switched to a disabled state. With disabled mailboxes, you can recover mailbox data without having to restore the entire mailbox database. Disabled mailboxes are retained in the mailbox database until the deleted mailbox retention period expires or until the mailbox is permanently deleted.

**Connect a disabled mailbox**

1. In the console tree, navigate to **Recipient Configuration** > **Disconnected Mailbox**.
2. In the result pane, select the disabled mailbox that you want to reconnect.
3. In the action pane, click **Connect**.
4. On the **Introduction** page, select one of the following to specify the mailbox type for the mailbox you're connecting:
   * **User Mailbox** Click this button to connect the mailbox as a mailbox owned by a user to send and receive e-mail messages. User mailboxes can't be used for resource scheduling.  
     The Active Directory account associated with a user mailbox must reside in the same forest as the Exchange server. To use an account in a trusted forest, select **Linked Mailbox**.
   * **Room Mailbox** or **Equipment Mailbox** Click one of these buttons to connect the mailbox as a mailbox that will be used as a location resource for scheduling meetings (room mailbox) or a shared resource (equipment mailbox) that isn't location specific. Room and equipment mailboxes can be included in meeting requests as resources and can be configured to automatically process incoming requests.

|  |
| --- |
| Description: Bb123490.note(en-us,EXCHG.141).gifNote: |
| You can connect a room or equipment mailbox only to a disabled user account. Therefore, the **Select Recipient** dialog box that you use to select a user account on the **Mailbox Settings** page of this wizard will display only a list of disabled user accounts in the Active Directory forest. |

* + **Linked Mailbox** Click this button to connect the mailbox as a user mailbox that's accessed by a user in a separate, trusted forest. To store the mailbox information, you must select a user account in the forest in which the Exchange server resides.  
    Linked mailboxes might be required for organizations that choose to deploy Exchange in a resource forest. Using the resource forest scenario, you can centralize Exchange in a single forest, while allowing access to the Exchange organization with user accounts in one or more trusted forests.

1. On the **Mailbox Settings** page, configure the following settings:
   * **Matching User** Click this button to have Exchange locate a matching user object in Active Directory. Click **Browse** to open the **Select User** dialog box. If Exchange locates a matching user, it will appear in this dialog box. Select the user, and then click **OK**.   
     If Exchange can't find a matching user, you must click **Existing User**. To locate a user account that matches the mailbox object, Exchange uses the **LegacyExchangeDN** and **DisplayName** attributes of the Exchange store mailbox object.
   * **Existing User** Click this button if you want to connect the mailbox to a user other than the matching user. Click **Browse** to see a list of users available in Active Directory. The list contains only users that don't have an associated mailbox.

|  |
| --- |
| Description: Bb123490.note(en-us,EXCHG.141).gifNote: |
| If you're connecting a room, equipment, or linked mailbox, the **Select User** dialog box displays only users that are disabled in Active Directory. If you're connecting a user mailbox, the **Select User** dialog box displays only users that are enabled in Active Directory. |

* + **Alias** Use this box to type an alias for the mailbox.
  + **Retention Policy** Select this check box to assign a retention policy to the mailbox. Click **Browse** to select a policy from a list of available retention policies.
  + **Exchange ActiveSync mailbox policy** Select this check box to assign a Microsoft Exchange ActiveSync policy to the mailbox. Click **Browse** to select a policy from a list of available Exchange ActiveSync policies.

1. If you're connecting a linked mailbox, use the **Master Account** page to configure the following settings for the mailbox:
   * **Trusted forest or domain** Click **Browse** to open the **Select Forest** dialog box. Select the forest that contains the master account, and then click **OK**. This enables the **Browse** button next to the **Linked domain controller** check box.
   * **Use the following Window user account to access linked domain controller** Select this check box if you want to specify a different user account. To access the domain controller in the linked forest, you can use a user account other than the one you're currently logged on as. Select the **User name** and **Password** check boxes to type the credentials of the user account.
   * **Linked domain controller** Click **Browse** to open the **Select Domain Controller** dialog box. Select the domain controller you want, and then click **OK**. Selecting a valid linked domain controller enables the **Browse** button next to the **Linked master account** check box.
   * **Linked master account** Click **Browse** to open the **Select Master Account** dialog box. Select the user account that you want to use as the master account, and then click **OK**.
2. On the **Connect Mailbox** page, review your configuration settings. Click **Connect** to associate the disconnected mailbox with the Active Directory user that you selected on the **Mailbox Settings** page. Click **Back** to make configuration changes.
3. On the **Completion** page, review the following, and then click **Finish** to close the wizard:
   * A status of **Completed** indicates that the wizard completed the task successfully.
   * A status of **Failed** indicates that the task wasn't completed. If the task fails, review the summary for an explanation, and then click **Back** to make any configuration changes.

### Lost Database or Logs

When a database drive or log drive is lost in the Exchange environment, the recovery procedure will depend on the deployed high availability.

1. In a DAG Environment with multiple copies, you can use the database reseeding process to restore the database copy. To reseed a database please use steps defined in [Reseeding a Database](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Seeding_a_Mailbox)
2. In a Single Database copy environment, If the SLA requires that the Email services be immediately restored use the steps defined [Dial Tone Portability](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Dial_Tone_Portability)
3. In a Single Database copy environment, If the Database has to restored from backup, follow the process described in the [Restore Exchange Server from Backup](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Use_Windows_Server)

### Lost Server

When a database drive or log drive is lost in the Exchange environment, the recovery procedure will depend on the deployed high availability solution.

1. In a DAG Environment with multiple servers hosting multiple copies, use the steps defined in [Recover a Database availability Group member](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Recover_a_Database)
2. In a Standalone environment use the steps defined in the [Recover an Exchange Server](file:///C:\Users\jamaye\Documents\Exchange%202010%20Operations%20Guide\Contoso%20Exchange%202010%20Operations%20Guide-v1.3-Added%20Public%20folders,Tasks,%20Checklists%20and%20As%20Needed%20Tasks-JGM.docx#_Recover_an_Exchange)

### Lost Site

When a site is Lost in an Exchange environment, It is considered a complete datacenter failure and disaster recovery event, and recovery must be manually performed and completed for the client service to be restored, and for the outage to end. This is in contrast to the high availability configuration, where automatic recovery is initiated by the system, and the failure typically leaves the messaging system in a fully functional state.

There are four basic steps that you complete to perform a datacenter switchover, after making the initial decision to activate the second datacenter:

**Terminate a partially running datacenter**

This step involves terminating Mailbox and Unified Messaging services in the primary datacenter, if any services are still running. This is particularly important for the Mailbox server role because it uses an active/passive high availability model. If services in a partially failed datacenter aren't stopped, it's possible for problems from the partially failed datacenter to negatively affect the services during a switchover back to the primary datacenter. If network or Active Directory infrastructure reliability has been compromised as a result of the primary datacenter failure, we recommend that all messaging services be off until these dependencies are restored to healthy service. If any DAG members in the failed datacenter are still running, they should be terminated

When the DAG is in DAC mode, the specific actions to terminate any surviving DAG members in the primary datacenter are as follows:

1. The DAG members in the primary datacenter must be marked as stopped in the primary datacenter. Stopped is a state of Active Manager that prevents databases from mounting, and Active Manager on each server in the failed datacenter is put into this state by using the Stop-DatabaseAvailabilityGroup cmdlet. The ActiveDirectorySite parameter of this cmdlet can be used to mark all of the servers in the primary datacenter as stopped with a single command. This step may not be possible depending on the failure. This step should be taken if the state of the datacenter permits it. The Stop-DatabaseAvailabilityGroup cmdlet should be run against all servers in the primary datacenter. If the Mailbox server is unavailable but Active Directory is operating in the primary datacenter, the Stop-DatabaseAvailabilityGroup command with the ConfigurationOnly parameter must be run against all servers in this state in the primary datacenter, or the Mailbox server must be turned off. Failure to either turn off the Mailbox servers in the failed datacenter or to successfully perform the Stop-DatabaseAvailabilityGroup command against the servers will create the potential for split-brain syndrome to occur across the two datacenters. You may need to individually turn off computers through power management devices to satisfy this requirement.

2. The second datacenter must now be updated to represent which primary datacenter servers are stopped. This is done by running the same Stop-DatabaseAvailabilityGroup command with the ConfigurationOnly parameter using the same ActiveDirectorySite parameter and specifying the name of the Active Directory site in the failed primary datacenter. The purpose of this step is to inform the servers in the second datacenter about which mailbox servers are available to use when restoring service.

When the DAG isn't in DAC mode, the specific actions to terminate any surviving DAG members in the primary datacenter are as follows:

1. The DAG members in the primary datacenter must be forcibly evicted from the DAG's underlying cluster by running the following commands on each member:

net stop clussvc

cluster <DAGName> node <DAGMemberName> /forcecleanup

2. The DAG members in the second datacenter must now be restarted and then used to complete the eviction process from the second datacenter. Stop the Cluster service on each DAG member in the second datacenter by running the following command on each member:

net stop clussvc

3. On a DAG member in the second datacenter, force a quorum start of the Cluster service by running the following command:

net start clussvc /forcequorum

4. Open the Failover Cluster Management tool and connect to the DAG's underlying cluster. Expand the cluster, and then expand Nodes. Right-click each node in the primary datacenter, select More Actions, and then select Evict. When you're done evicting the DAG members in the primary datacenter, close the Failover Cluster Management tool.

If any Unified Messaging servers are in use in the failed datacenter, they must be disabled to prevent call routing to the failed datacenter. You can disable a Unified Messaging server by using the Disable-UMServer cmdlet (for example, Disable-UMServer UM01). Alternatively, if you are using a Voice over IP (VoIP) gateway, you can also remove the Unified Messaging server entries from the VoIP gateway, or change the DNS records for the failed servers to point to the IP address of the Unified Messaging servers in the second datacenter if your VoIP gateway is configured to route calls using DNS.

**Validate and confirm the prerequisites for the second datacenter**  
This step can be performed in parallel with step 1 because validation of the health of the infrastructure dependences in the second datacenter is largely independent of the first datacenter services. Each organization typically requires its own method for performing this step. For example, you may decide to complete this step by reviewing health information collected and filtered by an infrastructure monitoring application, or by using a tool that's unique to your organization's infrastructure. This is a critical step, because activating the second datacenter when its infrastructure is unhealthy and unstable is likely to yield poor results.

**Activate the Mailbox servers**This step begins the process of activating the second datacenter. This step can be performed in parallel with step 4 because the Microsoft Exchange services can handle database outages and recover. Activating the Mailbox servers involves a process of marking the failed servers from the primary datacenter as unavailable followed by activation of the servers in the second datacenter. The activation process for Mailbox servers depends on whether the DAG is in database activation coordination (DAC) mode. For more information about database activation coordination mode, see Understanding Datacenter Activation Coordination Mode.

If the DAG is in DAC mode, you can use the Exchange site resilience cmdlets to terminate a partially failed datacenter (if necessary) and activate the Mailbox servers. For example, in DAC mode, this step is performed by using the Stop-DatabaseAvailabilityGroup cmdlet. In some cases, the servers must be marked as unavailable twice (once in each datacenter). Next, the Restore-DatabaseAvailabilityGroup cmdlet is run to restore the remaining members of the database availability group (DAG) in the second datacenter by reducing the DAG members to those that are still operational, thereby reestablishing quorum. If the DAG isn't in DAC mode, you must use the Windows Failover Cluster tools to activate the Mailbox servers. After either process is complete, the database copies that were previously passive in the second datacenter can become active and be mounted. At this point, Mailbox server recovery is complete.

The steps needed to activate Mailbox servers during a datacenter switchover also depend on whether the DAG is in DAC mode. Before activating the DAG members in the second datacenter, we recommend that you validate that the infrastructure services in the second datacenter are ready for messaging service activation.

When the DAG is in DAC mode, the steps to complete activation of the mailbox servers in the second datacenter are as follows:

1. The Cluster service must be stopped on each DAG member in the second datacenter. You can use the Stop-Service cmdlet to stop the service (for example, Stop-Service ClusSvc), or use net stop clussvc from an elevated command prompt.

2. The Mailbox servers in the standby datacenter are then activated by using the Restore-DatabaseAvailabilityGroup cmdlet. The Active Directory site of the standby datacenter is passed to the Restore-DatabaseAvailabilityGroup cmdlet to identify which servers to use to restore service and to configure the DAG to use an alternate witness server. If the alternate witness server wasn't previously configured, you can configure it by using the AlternateWitnessServer and AlternateWitnessDirectory parameters of the Restore-DatabaseAvailabilityGroup cmdlet. If this command succeeds, the quorum criteria are shrunk to the servers in the standby datacenter. If the number of servers in that datacenter is an even number, the DAG will switch to using the alternate witness server as identified by the setting on the DAG object.

3. The databases can now be activated. Depending on the specific configuration used by the organization, this may not be automatic. If the servers in the standby datacenter have an activation blocked setting, the system won't do an automatic failover from the primary datacenter to the standby datacenter of any database. If no failover restrictions are present for any of the database copies in the standby datacenter, the system will activate copies in the second datacenter assuming they are healthy. If databases are configured with an activation blocked setting that requires explicit manual action, there are two choices for action:

a. Clear the setting that blocks activation. This will make the system return to its default behavior, which is to activate any available copy.

b. Leave the setting unchanged and use the Move-ActiveMailboxDatabase cmdlet to complete the database activation in the second datacenter. To complete this step using the Move-ActiveMailboxDatabase cmdlet when activation blocked is set, you must explicitly identify the target of the move.

4. The last step is to review all error and warning messages from the tasks. Any indicated warnings should be followed up and corrected. The task design model for these commands is to only fail if they can't achieve the fundamental goal of their design. For example, the Restore-DatabaseAvailabilityGroup cmdlet will fail if it can't shrink the quorum of the DAG to allow a server in the second datacenter to be restarted for servicing without causing a quorum outage. However, each task's output is also used to identify the issues that require administrator follow-up. You're strongly encouraged to save all task output and review it for follow-up actions.

When the DAG isn't in DAC mode, the steps to complete activation of the mailbox servers in the second datacenter are as follows:

1. The quorum must be modified based on the number of DAG members in the second datacenter.

a. If there's an odd number of DAG members, change the DAG quorum model from a Node a File Share Majority to a Node Majority quorum by running the following command:

Cluster <DAGName> /quorum /nodemajority

b. If there's an even number of DAG members, reconfigure the witness server and directory by running the following command in the Exchange Management Shell:

Set-DatabaseAvailabilityGroup <DAGName> -WitnessServer <ServerName>

2. Start the Cluster service on any remaining DAG members in the second datacenter by running the following command:

net start clussvc

3. Perform server switchovers to activate the mailbox databases in the DAG by running the following command for each DAG member:

Move-ActiveMailboxDatabase -Server <DAGMemberinPrimarySite> -ActivateOnServer <DAGMemberinSecondSite>

4. Mount the mailbox databases on each DAG member in the second site by running the following command:

Get-MailboxDatabase <DAGMemberinSecondSite> | Mount-Database

**Activate the other server roles**   
This involves using the URL mapping information and the Domain Name System (DNS) change methodology to perform all required DNS updates. The mapping information describes what DNS changes to perform. The amount of time required to complete the update depends on the methodology used and the Time to Live (TTL) settings on the DNS record (and whether the deployment’s infrastructure honors the TTL).

# How to Guides

This section will provide required steps necessary to recover from various scenarios.

## Recover an Exchange Server

Most of the settings for a computer running Exchange 2010 are stored in Active Directory. The */m:RecoverServer* switch rebuilds an Exchange server with the same name by using the settings and other information stored in Active Directory. Recovering a lost Exchange server is often accomplished by using new hardware

**Pre Requisites**

* The server on which recovery is being performed must be running the same operating system as the lost server. For example, you can't recover a server that was running Exchange 2010 and Windows Server 2008 on a server running Windows Server 2008 R2, or vice versa.
* The same disk drive letters on the failed server for mounted databases must exist on the server on which you're running recovery.
* The server on which recovery is being performed should have the same performance characteristics and hardware configuration as the lost server.

**Recover a Lost Exchange Server**

You need to be assigned permissions before you can perform this procedure.

1. Reset the computer account for the lost server.  
   dsmod computer <ComputerDN> -reset
2. Install the proper operating system and name the new server with the same name as the lost server. Recovery won't succeed if the server on which recovery is being performed doesn't have the same name as the lost server.
3. Join the server to the same domain as the lost server.
4. Install the necessary prerequisites and operating system components.
5. Log on to the server being recovered and open a command prompt.
6. Navigate to the Exchange 2010 installation files, and run the following command:  
   ***Setup /m:RecoverServer***
7. After Setup has completed, but before the recovered server is put into production, reconfigure any custom settings that were previously present on the server based on the Build Guide.

## Recover a Database Availability Group Member Server

If a Mailbox server that's a member of a database availability group (DAG) is lost or otherwise fails and is unrecoverable and needs replacement, you can perform a server recovery operation. Microsoft Exchange Server 2010 Setup includes the switch /m:RecoverServer that can be used to perform the server recovery operation. Running Setup with the /m:RecoverServer switch causes Setup to read the server's configuration information from Active Directory for a server with the same name as the server from which you're running Setup. After the server's configuration information is gathered from Active Directory, the original Exchange files and services are then installed on the server, and the roles and settings that were stored in Active Directory are then applied to the server.

Use Setup /m:RecoverServer to recover a server

1. Retrieve any replay lag or truncation lag settings for any mailbox database copies that exist on the server being recovered by using the Get-MailboxDatabase cmdlet.

Get-MailboxDatabase DB1 | Format-List \*lag\*

2. Remove any mailbox database copies that exist on the server being recovered by using the Remove-MailboxDatabaseCopy cmdlet.

Remove-MailboxDatabaseCopy DB1\MBX1

3. Remove the failed server's configuration from the DAG by using the Remove-DatabaseAvailabilityGroupServer cmdlet.

Remove-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX1

If the DAG member being removed is offline and cannot be brought online, you must add the ConfigurationOnly parameter to the above command.

1. Reset the server's computer account in Active Directory. For detailed steps, see Reset a Computer Account.

2. Open a Command Prompt window. Using the original Setup media, run the following command.

Setup /m:RecoverServer

3. When the Setup recovery process is complete, add the recovered server to the DAG by using the Add-DatabaseAvailabilityGroupServer cmdlet.

Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX1

4. After the server has been added back to the DAG, you can reconfigure mailbox database copies by using the Add-MailboxDatabaseCopy cmdlet. If any of the database copies being added previously had replay lag or truncation lag times greater than 0, you can use the ReplayLagTime and TruncationLagTime parameters of the Add-MailboxDatabaseCopy cmdlet to reconfigure those settings.

Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX1

Add-MailboxDatabaseCopy -Identity DB2 -MailboxServer MBX1 -ReplayLagTime 3.00:00:00

Add-MailboxDatabaseCopy -Identity DB3 -MailboxServer MBX1 -ReplayLagTime 3.00:00:00 -TruncationLagTime 3.00:00:00

## Shadow Redundancy

Exchange Server 2010 introduces the shadow redundancy feature to provide redundancy for messages for the entire time they're in transit. With shadow redundancy, the deletion of a message from the transport databases is delayed until the transport server verifies that all of the next hops for that message have completed delivery. If any of the next hops fail before reporting back successful delivery, the message is resubmitted for delivery to that next hop.

Shadow redundancy provides the following benefits:

* It eliminates the reliance on the state of any specific Hub Transport or Edge Transport server. As long as redundant message paths exist in your routing topology, any transport server becomes disposable.
* If a transport server fails, you can remove it from production without emptying its queues or losing messages.
* If you want to upgrade a Hub Transport or Edge Transport server, you can bring that server offline at any time without the risk of losing messages.
* It eliminates the need for storage hardware redundancy for transport servers.
* It consumes less bandwidth than creating duplicate copies of messages on multiple servers. The only additional network traffic generated with shadow redundancy is the exchange of *discard status* between transport servers. Discard status is the information each transport server maintains. It indicates when a message is ready to be discarded from the transport database.
* It provides resilience and simplifies recovery from a transport server failure.

**To enable shadow redundancy for your organization, Use the following**

*Set-TransportConfig -ShadowRedundancyEnabled $true*

If due to the hardware constraints on your servers, you don't want to retain shadow copies for messages that are delayed. You can reduce the retention period of shadow messages for your organization

*Set-TransportConfig -ShadowMessageAutoDiscardInterval 04:00:00*

## Working with the Queue Database on Transport Servers

A *queue* is a temporary holding location for messages that are waiting to enter the next stage of processing. Each queue represents a logical set of messages that an Exchange transport server processes in a specific order. Queues exist only on computers that have the Hub Transport server role or Edge Transport server role installed.

Microsoft Exchange Server 2007 uses a single Extensible Storage Engine (ESE) database for queue message storage. Formerly known as JET, ESE is a method that defines a low-level API to the underlying database structures in Exchange Server.

The following scenarios may result in an unresponsive Hub Transport server or Edge Transport server that has a queue database that contains undelivered messages:

* An Exchange transport server fails when there are undelivered messages in the queues. Additionally, you can't bring the server back online in a timely manner.
* An Exchange transport server has a fragmented queue database that grows so large that it consumes all available hard disk drive space.

**Recovering a Queue Database on the Target Exchange Transport Server**

The basic steps of the queue database recovery are as follows:

1. Move the queue database to a temporary location on the target Exchange transport server.
2. Perform a recovery of the queue database by using Exchange Server Database Utilities (Eseutil.exe)  
   *Eseutil /r Trn /d. /8.*
3. Perform an offline defragmentation of the queue database by using Eseutil.  
   *Eseutil /d mail.que*
4. Prepare the existing queue database on the target Exchange transport server for replacement by the recovered queue database.
   1. Stop the flow of new messages into the queues and allow the existing messages to be delivered.
   2. Monitor the mailbox delivery queues and remote delivery queues until all messages have been delivered.
   3. Resubmit, or suspend and export any messages in the Unreachable queue that you want to save.
   4. Resume or export any messages in the poison message queues that you want to save.
   5. Modify the message expiration time-out on the Exchange transport server so the messages in the recovered queue database are preserved.
5. Start the repaired queue database on the target Exchange transport server.

## Edge Transport Server Cloned Configuration

The Microsoft Exchange Server 2010 Edge Transport server role stores its configuration information in Active Directory Lightweight Directory Services (AD LDS). To make sure that all Edge Transport servers that you deploy are using the same configuration information, you can use the provided cloned configuration scripts in the Exchange Management Shell to duplicate the configuration of a source server to a target server.

You use cloned configuration to deploy new Edge Transport servers based on a configured source server. The configuration information for the source server is duplicated and then exported to an XML file. The XML file is then imported to the target server.

The cloned configuration process consists of three steps:

1. Export the configuration on the source server.   
   In this step, you run the ExportEdgeConfig.ps1 script to export the source server's configuration information to an intermediate XML file.
2. Validate the configuration on the target server.   
   In this step, you run the ImportEdgeConfig.ps1 script. This script checks the existing information in the intermediate XML file to see whether the settings that were exported are valid for the target server and then creates an answer file. The answer file specifies the server-specific information that's used during the next step when you import the configuration on the target server. The answer file contains entries for each source server setting that isn't valid for the target server. You can modify these settings so that they're valid for the target server. If all settings are valid, the answer file contains no entries.
3. Import the configuration on the target server.   
   In this step, the ImportEdgeConfig.ps1 script uses the intermediate XML file and the answer file to clone an existing configuration or to restore the server to a specific configuration.

## Disk Full on Exchange Log Drive

There are two basic rules to follow when freeing up space on a log drive based on the configuration of the Databases:

If the Database is a standalone copy

* Do not delete log files outright. Move them to a different drive so that you can get them back if they are needed.
* Do not remove all the log files, even if the databases have been shut down cleanly. Remove only log files that are older than the current checkpoint.

1. **Backup the Storage Groups**   
   Taking an online backup. After a Normal (Full) backup completes successfully, Exchange will automatically remove logs that are not needed to roll forward from the backup. Logs are also pruned after an Incremental backup.

If the Database has multiple copies, make sure that the copy queue lengths and the replay queue lengths are zero,

## Rebuild the Full-Text Index Catalog

If the mailbox database copy is the only copy, Exchange Search must create a new content index catalog. You can use the ResetSearchIndex.ps1 script to do this

**Reseed the content index catalog from any source**

TO reseed the content index catalog for the database copy DB1 on Mailbox server MBX1 from any source server that has a copy of the database.

*Update-MailboxDatabaseCopy -Identity DB1\MBX1 –CatalogOnly*

## Restore Data Using a Recovery Database

An RDB (Recovery Database) can be used to recover data in several situations, such as:

**Same server dial tone recovery:** You can perform a recovery from an RDB after the original database has been restored from backup, as part of a dial tone recovery operation.

**Alternate server dial tone recovery:** You can use an alternate server to host the dial tone database, and then later recover data from an RDB after the original database has been restored from backup.

**Mailbox recovery:** You can recover an individual mailbox from backup when the deleted mailbox retention period has elapsed. You then extract data from the restored mailbox and copy it to a target folder or merge it with another mailbox.

**Specific item recovery:** You can restore from backup data that has been deleted or purged from a mailbox.

An RDB is designed for mailbox database recovery under the following conditions and scenarios:

* The logical information about the original database and the mailboxes in that database remains intact and unchanged in Active Directory.
* You need to recover a single mailbox or a single database. Recovery scenarios include:
  + Recovering or repairing a database while a dial tone database is in use, with the goal of merging the two databases.
  + Recovering a database on a server other than the original server for that database. If needed, you can then merge the recovered data back to the original server.
  + Recovering deleted items that users previously deleted from their mailbox, after the deleted item retention period has expired.

An RDB cannot be used when you have to recover public folder content. In addition, RDBs are generally not designed for scenarios in which you have to restore entire servers, when you have to restore multiple databases, or when you're in an emergency situation that requires changing or rebuilding your Active Directory topology.  
Note:

Please note that you can't use the EMC to create a recovery database. You can't use the EMC to restore data using an RDB.

**Create a recovery database**

Create the recovery database RDB1 on the Mailbox server MBX2.

*New-MailboxDatabase -Recovery -Name RDB1 -Server MBX2*

Create the recovery database RDB2 on the Mailbox server MBX1 using a custom path for the database file and log folder.

*New-MailboxDatabase -Recovery -Name RDB2 -Server MBX1 -EdbFilePath "C:\Recovery\RDB2\RDB2.EDB" -LogFolderPath "C:\Recovery\RDB2"*

**Recover data using a recovery database**

Restore a mailbox database into the RDB by using your backup application or if you have the database and its log files in the file system, by copying them to the RDB file structure.

Restore the source mailbox that has the MailboxGUID 1d20855f-fd54-4681-98e6-e249f7326ddd on mailbox database DB1 to the target mailbox with the alias User1.

*New-MailboxRestoreRequest -SouceDatabase DB1 -SourceStoreMailbox 1d20855f-fd54-4681-98e6-e249f7326ddd -TargetMailbox User1*

Restore the content of the source mailbox that has the display name User2 on mailbox database DB1 to the archive mailbox for user2@contoso.com.

*New-MaiboxRestoreRequest -SourceDatabase DB1 -SourceStoreMailbox "User2" -TargetMailbox user2@contoso.com -TargetIsArchive*

## Database Portability

Database portability is a feature that enables a Microsoft Exchange Server 2010 mailbox database to be moved to or mounted on any other Mailbox server in the same organization. By using database portability, reliability is improved by removing several error-prone, manual steps from the recovery processes. In addition, database portability reduces the overall recovery times for various failure scenarios.

**Move a Mailbox Database Using Database Portability**You can use database portability to move a Microsoft Exchange Server 2010 mailbox database between Exchange 2010 Mailbox servers in the same organization. This can help reduce overall recovery times for various failure scenarios.

To move user mailboxes to a recovered or dial tone database using database portability

1. Verify that the database is in a Clean Shutdown state. If the database isn't in a Clean Shutdown state, perform a soft recovery.
2. If you don't have all of the required log files To commit all uncommitted log files to the database, from a command prompt, run the following command.  
   *ESEUTIL /R <Enn>*
3. Create a database on the new server,  
   *New-MailboxDatabase -Name DB1 -Server MBX1 -EdbFilePath C:\Databases\DB1\DB1.edb -LogFolderPath C:\Databases\DB1*
4. Set the This database can be over written by restore attribute using the following syntax.  
   *Set-MailboxDatabase <Database Name> -AllowFileRestore:$true*
5. Move the database files (.edb file, log files, and Exchange Search catalog) to the appropriate location. The database files need to be present and in the correct location for recovery operations to succeed.
6. Mount the database using the following syntax.  
   *Mount-Database <Database Name>*
7. After the database is mounted, modify the user account settings with the Set-Mailbox cmdlet so that the account points to the mailbox on the new mailbox server. To move all of the users from the old database to the new database, use the following syntax.  
   *Get-Mailbox -Database <SourceDatabase> |where {$\_.ObjectClass -NotMatch '(SystemAttendantMailbox|ExOleDbSystemMailbox)'}| Set-Mailbox -Database <TargetDatabase>*

After Active Directory replication is complete, all users can access their mailboxes on the new Exchange server. Clients can connect to the new server as follows:

* Microsoft Outlook 2010, Office Outlook 2007, and Windows Mobile 6.1 and later clients are redirected via the Autodiscover service.
* Outlook Web App users are automatically redirected to the new server.
* Older Outlook clients need to be manually configured to point to the new server, if the server name has changed.

## Dial Tone Portability

Using dial tone portability, users can have a temporary mailbox for sending and receiving e-mail while their original mailbox is being restored or repaired. The temporary mailbox can be on the same Exchange 2010 Mailbox server or on any other Exchange 2010 Mailbox server in your organization. The process for using dial tone portability is called a dial tone recovery, which involves creating an empty database on a Mailbox server to replace a failed database.

1. Make sure that any existing files for the database being recovered are preserved in case they're needed later for further recovery operations.
2. Use the New-MailboxDatabase cmdlet to create a dial tone database, as shown in this example.

*New-MailboxDatabase -Name DTDB1 -EdbFilePath D:\DialTone\DTDB1.EDB*

1. Use the Set-Mailbox cmdlet to rehome the user mailboxes hosted on the database being recovered, as shown in this example.

*Get-Mailbox -Database DB1 | Set-Mailbox -Database DTDB1*

1. Use the Mount-Database cmdlet to mount the database so client computers can access the database and send and receive messages, as shown in this example.

*Mount-Database -Identity DTDB1*

1. Create a recovery database (RDB) and restore or copy the database and log files containing the data you want to recover into the RDB..
2. After the data is copied to the RDB, but before mounting the restored database, copy any log files from the failed database to the recovery database log folder so they can be played against the restored database.
3. Mount the RDB, and then use the Dismount-Database cmdlet to dismount it, as shown in this example.

*Mount-Database -Identity RDB1*

*Dismount-Database -Identity RDB1*

1. After the RDB is dismounted, move the current database and log files within the RDB folder to a safe location. This is done in preparation for swapping the recovered database with the dial tone database.
2. Dismount the dial tone database, as shown in this example. Note that your end users will experience an interruption in service when you dismount this database.

*Dismount-Database -Identity DTDB1*

1. Move the database and log files from the dial tone database folder into the RDB folder.
2. Move the database and log files from the safe location containing the recovered database into the dial tone database folder, and then mount the database, as shown in this example.

*Mount-Database -Identity DTDB1*

This ends the service interruption for your end users. They will be able to access their original production database and send and receive messages.

1. Mount the RDB, as shown in this example.

*Mount-Database -Identity RDB1*

1. Use the Get-Mailbox and Restore-Mailbox cmdlets to export the data from the RDB and import it into the recovered database, as shown in this example. This will import all the messages sent and received using the dial tone database into the production database.

*Get-Mailbox -Database DTDB1 | Restore-Mailbox -RecoveryDatabase RDB1*

1. After the restore operation is complete, you can dismount and remove the RDB, as shown in this example.

*Dismount-Database -Identity RDB1*

*Remove-MailboxDatabase -Identity RDB1*

## Use Windows Server Backup to Restore a Backup of Exchange

Microsoft Exchange Server 2010 includes a plug-in for Windows Server Backup that enables you to make Volume Shadow Copy Service (VSS)-based backups of Exchange data. You can use Windows Server Backup to back up and restore your Exchange databases.

**Use Windows Server Backup to restore a backup of Exchange**

1. Start Windows Server Backup.
2. In the **Actions** pane, click **Recover**. The Recovery wizard appears.
3. On the **Getting Started** page, do either of the following:
   1. If the data being recovered was backed up from the server on which Windows Server Backup is running, select **This server (ServerName)**, and then click **Next**.
   2. If the data being recovered wasn't from the server on which Windows Server Backup is running, or if the backup being recovered is located on another computer, select **Another server**, and then click **Next**. On the **Specify location type** page, select **Local drives** or **Remote shared folder**, and then click **Next**. If you select **Local drives**, select the drive containing the backup on the **Select backup location** page, and then click **Next**. If you select **Remote shared folder**, enter the UNC path for the backup data on the **Specify remote folder** page, and then click **Next**.
4. On the **Select backup date** page, select the date and time of the backup that you want to recover, and then click **Next**.
5. On the **Select recovery type** page, select **Applications**, and then click **Next**.
6. On the **Select application** page, verify that Exchange is selected in the **Applications** field. Click **View Details** to view the application components of the backups. If the backup that you're recovering is the most recent, the **Do not perform a roll-forward recovery of the application database** check box is displayed. Select this check box if you want to prevent Windows Server Backup from rolling forward the database being recovered. Click **Next**.
7. On the **Specify recovery options** page, select where you want to recover the data, and then click **Next**:
   1. Select **Recover to original location** to recover backed up data to its original location. If you use this option, you can't set a single database or multiple databases; all backed up databases are restored to their original location.
   2. Select **Recover to another location** to restore individual databases and files to a specified location. Click **Browse** to specify the alternate location. If you use this option, you can restore a single database or multiple databases into a custom location. After being restored, the data files can then be moved into a recovery database, and manually moved back to their original location. When you restore databases to an alternate location, the restored database is in a Dirty Shutdown state.
8. On the **Confirmation** page, review the recovery settings, and then click **Recover**.
9. On the **Recovery progress** page, you can view the status and progress of the recovery operation.
10. Click **Close** when the recovery operation has completed.

## Rebuild an Entire Database Availability Group

A database availability group (DAG), together with mailbox database copies, can provide automatic recovery from a variety of server, storage, network, and other hardware failures. A DAG can also provide a site resilience solution so that you can perform a datacenter switchover in the event of a site-level disaster. But even a comprehensive, intelligent, and robust solution such as a DAG can't protect you from all possible disasters, including disasters that affect an entire DAG.

For example, consider a two-member DAG deployed in a single datacenter. If the datacenter experiences a flood, fire, or other cataclysmic event that destroys the DAG, the entire DAG will need to be rebuilt from scratch. Rebuilding a DAG is a straightforward process that consists of nine primary steps:

1. Prepare Active Directory for the introduction of servers with the same name
2. Prepare the DAG's cluster name object
3. Remove the database copies from the DAG
4. Remove the Mailbox servers from the DAG
5. Build replacement Mailbox servers
6. Run Setup /m:RecoverServer on each DAG member
7. Restore and/or mount mailbox databases
8. Add Mailbox servers to the DAG
9. Add mailbox database copies to the DAG

Example DAG Environment with a two-member DAG named DAG1 that contains Mailbox servers named MBX1 and MBX2. MBX1 hosts the active copy of a database named DAG1-DB1, which is replicated to MBX2. In addition to hosting the passive copy of DAG1-DB1, MBX2 also hosts the active copy of DAG1-DB2, which is replicated to MBX1.

**Prepare Active Directory for the Introduction of Servers with the Same Name**

Microsoft Exchange Server 2010 derives security permissions based on the computer account for each server. To preserve these security permissions, the computer account for each DAG member needs to be reset and disabled using Active Directory Users and Computers.

1. Using Active Directory Users and Computers, locate the computer account for each DAG member.

2. Right-click the computer account for MBX1, point to All Tasks, and then select Reset Account.

3. Right-click the computer account for MBX1, point to All Tasks, and then select Disable Account. When the prompt appears, click Yes, and then click OK.

4. Repeat steps 2 and 3 for MBX2.

After Active Directory replication is complete, you can build new Windows servers using the names MBX1 and MBX2. If you've already built two replacement servers, you can rename them to MBX1 and MBX2 respectively.

**Prepare the DAG's Cluster Name Object**

Each DAG has an underlying Windows failover cluster. The name you give to a DAG becomes the name of the cluster, and a corresponding cluster name object (CNO) is created in Active Directory with this name. A CNO is the equivalent of a computer account for a cluster.

The names of the DAG and the CNO aren't used by end users or administrators. They're used by the system for internal communication and to secure the DAG. To preserve and reuse this name for the rebuilt DAG, the CNO for the DAG also needs to be reset and disabled using Active Directory Users and Computers.

1. Using Active Directory Users and Computers, locate the CNO for the DAG. In our example, the name of the CNO is DAG1.

2. Right-click the computer account for DAG1, point to All Tasks, and then select Reset Account.

3. Right-click the computer account for DAG1, point to All Tasks, and then select Disable Account. When the prompt appears, click Yes, and then click OK.

Allow time for Active Directory replication to complete before proceeding with the next step.

**Remove the Database Copies from the DAG**

Before you can recover Mailbox servers that are members of a DAG, you must first remove all mailbox database copies from the server. When that is complete, you must then remove the server from the DAG. In our example environment, this process involves removing all passive database copies from the DAG. Specifically, you would use the Remove-MailboxDatabaseCopy cmdlet to remove the passive copy of DAG1-DB1 from MBX2 and the passive copy of DAG1-DB2 from MBX1.

1. Run the following Exchange Management Shell commands.

*Remove-MailboxDatabaseCopy -Identity DAG1-DB1\MBX2 -Confirm:$False*

*Remove-MailboxDatabaseCopy -Identity DAG1-DB2\MBX1 -Confirm:$False*

2. Because the DAG members aren't operational, the commands will complete successfully but with several warning messages. You can verify that each mailbox database has a single copy by using the *Get-MailboxDatabase cmdlet, as shown in the following examples.*

*Get-MailboxDatabase -Server MBX1 | Format-List Name,DatabaseCopies*

*Get-MailboxDatabase -Server MBX2 | Format-List Name,DatabaseCopies*

**Remove the Mailbox Servers from the DAG**

Before you can recover a Mailbox server that is a member of a DAG, you must first use the Remove-DatabaseAvailabilityGroupServer cmdlet to remove the Mailbox server from the DAG. Because our example is a disaster recovery operation, we assume that MBX1 and MBX2 are either not operational or don't exist. As a result, the ConfigurationOnly parameter is used with the Remove-DatabaseAvailabilityGroupServer cmdlet. When this parameter is used, Remove-DatabaseAvailabilityGroupServer removes the Mailbox server from the DAG object in Active Directory.

1. Run the following Exchange Management Shell commands.

*Remove-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX1 -ConfigurationOnly:$True -Confirm:$False*

*Remove-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX2 -ConfigurationOnly:$True -Confirm:$False*

2. You can verify that each DAG member was removed by using the Get-DatabaseAvailabilityGroup cmdlet, as shown in this example.

*Get-DatabaseAvailabilityGroup -Identity DAG1 | Format-List* Servers After all DAG members are removed, the *Get-DatabaseAvailabilityGroup* cmdlet should return a Servers attribute that's empty.

**Build Replacement Mailbox Servers**

The next step is to rebuild the servers you're recovering, using the same computer names as the original production servers (in this example, MBX1 and MBX2), and the same operating system version as the servers being recovered.

The server recovery process is based on the name of the computer on which Setup is run. You can use different IP addresses, but the name of the server must match the original Mailbox server name for server recovery to complete.

The rebuild process is effectively the same process used to build the original production Mailbox servers.

1. Install and configure Windows Server.

2. Rename the computer with the appropriate name.

3. Join the computer to the appropriate Active Directory domain.

4. Install the prerequisites for running installed Exchange server roles. For details, see Exchange 2010 System Requirements.

Run Setup /m:RecoverServer on Each DAG Member

After the replacement servers are built and ready for Exchange server recovery, the next step is to run the Exchange 2010 unattended setup process in recovery mode. You don't need to complete this step on each DAG member before moving to the next step (restoring and/or mounting databases). However, you do need to perform this step for each DAG member on which you want to mount databases.

1. Open a Command Prompt window and navigate to the Exchange 2010 installation files.

2. Run the following command.

Setup /m:RecoverServer

3. After Setup completes successfully, restart the recovered server to complete the recovery process.

**Restore and/or Mount Mailbox Databases**Depending on the nature of the failure, the previously active copy of the databases hosted on these servers may not be available. If the files on disk are preserved and in their original location or copied to the original location, you should be able to use the Mount-Database cmdlet to mount the databases. Alternatively, you can restore your databases from backup to their original location, and then mount the databases.

After your mailbox databases are restored and/or mounted, service and data access should be restored for clients. The final steps are to reconfigure the Mailbox servers and databases for high availability by adding the recovered servers back to the DAG, and then creating mailbox database copies.

**Add Mailbox Servers to the DAG**

Adding Mailbox servers to a DAG can be accomplished by using the Add-DatabaseAvailabilityGroupServer cmdlet.

1. Run the following Exchange Management Shell commands.

*Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX1*

*Add-DatabaseAvailabilityGroupServer -Identity DAG1 -MailboxServer MBX2*

2. You can verify that each DAG member was added by using the *Get-DatabaseAvailabilityGroup* cmdlet, as shown in this example.

*Get-DatabaseAvailabilityGroup -Identity DAG1 | Format-List Servers*

**Add Mailbox Database Copies to the DAG**

The final step is to add mailbox database copies back to the appropriate DAG member. Depending on the nature of the failure, the previously passive copies of the databases hosted on these servers may not be available. If the files on disk are preserved and in their original location or copied to the original location, the Microsoft Exchange Replication service may be able to perform an incremental resynchronization of the passive copies, thereby eliminating the need for a full reseed. However, if the original passive copies aren't available, you'll need to perform a full reseed.

1. To add the mailbox database copies back to the DAG, run the following commands.

*Add-MailboxDatabaseCopy -Identity DAG1-DB1 -MailboxServer MBX2*

*Add-MailboxDatabaseCopy -Identity DAG1-DB2 -MailboxServer MBX1*

2. You can verify that each mailbox database copy was added successfully by using the Get-MailboxDatabase cmdlet, as shown in the following example.

*Get-MailboxDatabase | Format-List Name,DatabaseCopies*

3. You can also verify the health and status of all mailbox database copies in the DAG by using the *Get-MailboxDatabaseCopyStatus cmdlet, as shown in these examples.*

*Get-MailboxDatabaseCopyStatus -Server MBX1*

*Get-MailboxDatabaseCopyStatus -Server MBX2*

## Seeding a Mailbox Database Copy

Updating a database copy can take a very long time, especially if the database being copied is very large, or if there is high network latency or low network bandwidth. Once the seeding process has started, don't close the EMC or the Shell until the process has completed. If you do, the seeding operation will be terminated.

A database copy can be seeded using either the active copy or an up-to-date passive copy as the source for the seed.

**Use the EMC to update a mailbox database copy**

1. In the console tree, navigate to **Organization Configuration** > **Mailbox**.
2. In the result pane, click the **Database Management** tab.
3. In the work pane, on the **Database Copies** tab, right-click the database copy you want to update, and then select **Update Database Copy**.
4. On the **Update Database Copy** page, configure the available options for updating a database copy:
   * By default, the active copy of the database is used as the source database for seeding. If you prefer to use a passive copy of the database for seeding, check the Select a source server for seeding checkbox, and then click **Browse** to select the server containing the passive copy you want to use for the source.
   * Configure the task's behavior if files exist in the path of the database copy being seeded. If any existing files are in the database path, you can either select **Delete them and continue to update process** to remove all existing files and proceed with the seeding operation, or you can select **Cancel the update process** to terminate the task.
   * By default, once seeding has completed, continuous replication will automatically resume for the database. If you don't want replication to automatically resume, select **Leave the database copy suspended. I will manually resume replication later**.
   * Optionally specify a DAG network to be used for seeding. Click **Browse** to select the DAG network you want to use.
5. Once you have configured the available options, click **Update** to update the database copy.
6. On the **Completion** page, the **Summary** states whether the operation was successful. The summary also displays the Shell command that was used to perform this procedure.
7. Click **Finish** to exit the wizard.

**Manually copy an offline database**

1. If circular logging is enabled for the database, it must be disabled before proceeding. You can disable circular logging for a mailbox database by using the Set-MailboxDatabase cmdlet, as shown in this example.

*Set-MailboxDatabase DB1 -CircularLoggingEnabled $false*

2. Dismount the database. You can use the Dismount-Database cmdlet, as shown in this example.

*Dismount-Database DB1 -Confirm $false*

3. Manually copy the database files (the database file and all log files) to a second location, such as an external disk drive or a network share.

4. Mount the database. You can use the Mount-Database cmdlet, as shown in this example.

*Mount-Database DB1*

5. On the server that will host the copy, copy the database files from the external drive or network share to the same path as the active database copy. For example, if the active copy database path is D:\DB1\DB1.edb and log file path is D:\DB1, then you would copy the database files to D:\DB1 on the server that will host the copy.

6. Add the mailbox database copy by using the Add-MailboxDatabaseCopy cmdlet with the SeedingPostponed parameter, as shown in this example.

*Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX3 -SeedingPostponed*

7. If circular logging is enabled for the database, enable it again by using the Set-MailboxDatabase cmdlet, as shown in this example.

*Set-MailboxDatabase DB1 -CircularLoggingEnabled $true*

**Use the Shell to update a mailbox database copy**

*Update-MailboxDatabaseCopy -Identity DB1\MBX1*

## Restoring Service to the Primary Datacenter

Generally, datacenter failures are either temporary or permanent. With a permanent failure, such as an event that has caused the permanent destruction of a primary datacenter, there's no expectation that the primary datacenter will be activated. However, with a temporary failure (for example, an extended power loss or extensive but repairable damage), there's an expectation that the primary datacenter will eventually be restored to full service.

The process of restoring service to a previously failed datacenter is referred to as a failback. The steps used to perform a datacenter failback are similar to the steps used to perform a datacenter switchover. A significant distinction is that datacenter failbacks are scheduled, and the duration of the outage is often much shorter.

It's important that failback not be performed until the infrastructure dependencies for Exchange have been reactivated, are functioning and stable, and have been validated. If these dependencies aren't available or healthy, it's likely that the failback process will cause a longer than necessary outage, and it's possible the process could fail altogether.

**Mailbox Server Role Failback**

The Mailbox server role should be the first role that's failed back to the primary datacenter. The following steps detail the Mailbox server role failback process:

1. As part of the datacenter switchover process, the Mailbox servers in the primary datacenter were put into a stopped state. When the environment (such as primary datacenter, Exchange dependencies, and wide area network (WAN) connectivity) is ready, the first step is to put the Mailbox servers in the restored primary datacenter into a started state and incorporate them into the DAG. The way in which this is done depends on whether the DAG is in DAC mode.

a. If the DAG is in DAC mode, you can reincorporate the DAG members in the primary site by using the Start-DatabaseAvailabilityGroup cmdlet. Then, to make sure that the proper quorum model is being used by the DAG, run the Set-DatabaseAvailabilityGroup cmdlet against the DAG without specifying any parameters.

b. If the DAG isn't in DAC mode, you can reincorporate the DAG members by using the Add-DatabaseAvailabilityGroupServer cmdlet.

2. After the Mailbox servers in the primary datacenter have been incorporated into the DAG, they will need some time to synchronize their database copies. Depending on the nature of the failure, the length of the outage, and actions taken by an administrator during the outage, this may require reseeding the database copies. For example, if during the outage, you remove the database copies from the failed primary datacenter to allow log file truncation to occur for the surviving active copies in the second datacenter, reseeding will be required. Each database can individually proceed from this point forward. After a replicated database copy in the primary datacenter is healthy, it can proceed to the next step.

This process doesn't require that all databases be moved at the same time. You are encouraged to move the majority of your organization's databases at one time, but some databases many linger in the second datacenter if there are issues associated with the database copies in the primary datacenter.

3. After a majority of the databases are in a healthy state in the primary datacenter, the failback outage can be scheduled. When the scheduled time arrives, the following steps must be taken:

a. During the datacenter switchover process, the DAG was configured to use an alternate witness server. The DAG must be reconfigured to use a witness server in the primary datacenter. If you are using the same witness server and witness directory that was used prior to the primary datacenter outage, you can run the Set-DatabaseAvailabilityGroup -Identity DAGName command. If you plan on using a witness server or witness directory that is different from the original witness server and directory, use the Set-DatabaseAvailabilityGroup command to configure the witness server and witness directory parameters with the appropriate values.

b. The databases being reactivated in the primary datacenter should be dismounted in the second datacenter. You can use the Dismount-Database cmdlet to dismount the databases.

c. After the databases have been dismounted, the Client Access server URLs should be moved from the second datacenter to the primary datacenter. This is accomplished by changing the DNS record for the URLs to point to the Client Access server or array in the primary datacenter. This will result in the system acting as though a database failover has occurred for each database being moved.

Don't proceed to the next step until the Client Access server URLs have been moved and the DNS TTL and cache entries have expired. Activating the databases in the primary datacenter prior to moving the Client Access server URLs to the primary datacenter will result in an invalid configuration (for example, a mounted database that has no Client Access servers in its Active Directory site).

d. Because each database in the primary datacenter is in a healthy state, it can be activated in the primary datacenter by performing database switchovers. This is accomplished by using the Move-ActiveMailboxDatabase cmdlet for each database that will be activated.

e. After each database is moved to the primary datacenter, it can be mounted by using the Mount-Database cmdlet.

After one or more databases are active and mounted in the primary datacenter, failback procedures for the other server roles can be performed.

**Other Server Role Failback**

As part of the switchover process, the internal and external DNS records used by clients, other servers, and IP gateways to resolve the service endpoints for Client Access, Hub Transport, Edge Transport, and Unified Messaging servers were modified to point to the corresponding endpoints in the second datacenter. The failback process for the other server roles involves modifying those records to point to the restored service endpoints in the primary datacenter.

As with the DNS changes that were made during the switchover to the second datacenter, clients, servers, and IP gateways will continue to try to connect, and should automatically connect after the TTL has expired for the original DNS entry, and after the entry is expired from their DNS cache.

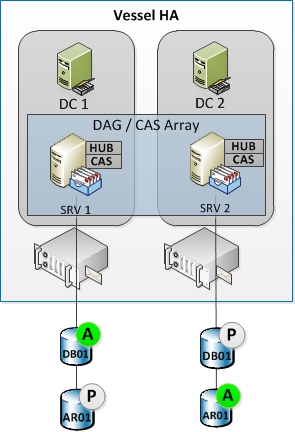
## Database Availability Group, (DAG) Disaster Recovery

A database availability group (DAG), together with mailbox database copies, can provide automatic recovery from a variety of server, storage, network, and other hardware failures. But even a comprehensive, intelligent, and robust solution such as a DAG can't protect you from all possible disasters, including disasters that affect an entire DAG.

Rebuilding a DAG is a straightforward process that consists of nine primary steps:

1. Prepare Active Directory for the introduction of servers with the same name
2. Prepare the DAG's cluster name object
3. Remove the database copies from the DAG
4. Remove the Mailbox servers from the DAG
5. Build replacement Mailbox servers
6. Run Setup /m:RecoverServer on each DAG member
7. Restore and/or mount mailbox databases
8. Add Mailbox servers to the DAG
9. Add mailbox database copies to the DAG

The DAG for CONTOSO on which this procedure will be applied is as follows:



### Prepare Active Directory for the Introduction of Servers with the Same Name

**Requirements**: A Global Catalog must be running in each site before trying to recover the DAG. If it is not the case, apply the disaster recovery procedure for Active Directory to restore a DC/GC before continue with Exchange.

Microsoft Exchange Server 2010 derives security permissions based on the computer account for each server. To preserve these security permissions, the computer account for each DAG member needs to be reset and disabled using Active Directory Users and Computers.

1. Using ***Active Directory Users and Computers*** (dsa.msc), locate the computer account for each DAG member.
2. Right-click the computer account for <SERVER1>, point to *All Tasks*, and then select ***Reset Account***.
3. Right-click the computer account for <SERVER1>, point to *All Tasks*, and then select ***Disable Account***. When the prompt appears, click Yes, and then click OK.
4. Repeat steps 2 and 3 for <SERVER2>.

After Active Directory replication is complete, you can build new Windows servers using the names <SERVER1> and <SERVER2>. If you've already built two replacement servers, you can rename them to <SERVER1> and <SERVER2> respectively.

### Prepare the DAG's Cluster Name Object

Each DAG has an underlying Windows failover cluster. The name you give to a DAG becomes the name of the cluster, and corresponding cluster names object (CNO) is created in Active Directory with this name. A CNO is the equivalent of a computer account for a cluster.

The CNO for the DAG also needs to be reset and disabled using Active Directory Users and Computers.

1. Using ***Active Directory Users and Computers*** (dsa.msc), locate the CNO for the DAG represented by **<DAG\_NAME>**.
2. Right-click the computer account for <DAG\_NAME>, point to *All Tasks*, and then select **Reset Account**.
3. Right-click the computer account for <DAG\_NAME>, point to *All Tasks*, and then select **Disable Account**. When the prompt appears, click Yes, and then click OK.

Allow time for Active Directory replication to complete before proceeding with the next step.

### Remove the Database Copies from the DAG

Before you can recover Mailbox servers that are members of a DAG, you must first remove all mailbox database copies from the server. When that is complete, you must then remove the server from the DAG. This process involves removing all passive database copies from the DAG. Specifically, you would use the *Remove-MailboxDatabaseCopy* cmdlet to remove the passive copy of <DAG\_NAME>-DB01 from <SERVER2> and the passive copy of <DAG\_NAME>-DBP01 from <SERVER1>.

1. Open an ***Exchange Management Shell*** console with “Run as administrator” privileges and execute the following commands:

Remove-MailboxDatabaseCopy -Identity *<DAG\_NAME>-DB01\<SERVER2>* -Confirm:$False

Remove-MailboxDatabaseCopy -Identity *<DAG\_NAME>-DBP01\<SERVER1>* -Confirm:$False

1. Because the DAG members aren't operational, the commands will complete successfully but with several warning messages. You can verify that each mailbox database has a single copy by using the ***Get-MailboxDatabase*** cmdlet:

Get-MailboxDatabase -Server *<SERVER1>* | Format-List Name,DatabaseCopies

Get-MailboxDatabase -Server *<SERVER2>* | Format-List Name,DatabaseCopies

### Remove the Mailbox Servers from the DAG

Before you can recover a Mailbox server that is a member of a DAG, you must remove the Mailbox server from the DAG. Because is a disaster recovery operation, we assume that <SERVER1> and <SERVER2> are either not operational or don't exist. As a result, the ConfigurationOnly parameter is used to remove the Mailbox server from the DAG object in Active Directory.

1. Run the following Exchange Management Shell commands.

Remove-DatabaseAvailabilityGroupServer -Identity *<DAG\_NAME>* -MailboxServer *<SERVER1>* -ConfigurationOnly:*$True* -Confirm:$False

Remove-DatabaseAvailabilityGroupServer -Identity *<DAG\_NAME>* -MailboxServer *<SERVER2>* -ConfigurationOnly:*$True* -Confirm:$False

1. You can verify that each DAG member was removed by using the Get-DatabaseAvailabilityGroup4 cmdlet, as shown in this example.

Get-DatabaseAvailabilityGroup -Identity *<DAG\_NAME>* | Format-List Servers

After all DAG members are removed, the *Get-DatabaseAvailabilityGroup* cmdlet should return a Servers attribute that's empty.

### Build Replacement Mailbox Servers

The next step is to rebuild the servers you're recovering, using the same computer names as the original production servers (<SERVER1> and <SERVER2>), and the same operating system version as the servers being recovered.

**Note**: The server recovery process is based on the name of the computer on which Setup is run. You can use different IP addresses, but the name of the server must match the original Mailbox server name for server recovery to complete.

The rebuild process is effectively the same process used to build the a production Mailbox server.

1. Install and configure Windows Server.
2. Rename the computer with the appropriate name.
3. Join the computer to the appropriate Active Directory domain.
4. Install the prerequisites for running installed Exchange server roles. <http://technet.microsoft.com/en-us/library/bb691354.aspx>
5. **Important: Do not install Exchange 2010 at this step.**

### Recover each DAG Member

After the replacement servers are built and ready for Exchange server recovery, the next step is to run Exchange 2010 setup process in recovery mode.

1. Open a Command Prompt window with Run as administrator privileges and navigate to the Exchange 2010 installation files.
2. Run the following command:

Setup /m:*RecoverServer*

1. After Setup completes successfully, restart the recovered server to complete the recovery process.

### Restore and/or Mount Mailbox Databases

Depending of the Exchange data availability, two cases are possible:

* ***Case 1***: If the database files and logs on disk are preserved and in their original location or copied to the original location, you should be able to use the ***Mount-Database*** cmdlet to mount the databases:

Get-MailboxDatabase –Server *<SERVER1>* | Mount-Database

Get-MailboxDatabase –Server *<SERVER2>* | Mount-Database

* ***Case 2***: The previous database file and/or logs are not available. You can restore the databases from backup to their original location and then mount the databases. Or start with empty database and merge the restore data later:
  + Apply the database restore procedure by following the backup solution documentation

After your mailbox databases are restored and/or mounted, service and data access should be restored for clients. The final steps are to reconfigure the Mailbox servers and databases for high availability by adding the recovered servers back to the DAG, and then creating mailbox database copies.

### Add Mailbox Servers to the DAG

Adding Mailbox servers to a DAG can be accomplished by using the *Add-DatabaseAvailabilityGroupServer* cmdlet.

1. Run the following Exchange Management Shell commands.

Add-DatabaseAvailabilityGroupServer -Identity *<DAG\_NAME>* -MailboxServer *<SERVER1>*

Add-DatabaseAvailabilityGroupServer -Identity *<DAG\_NAME>* -MailboxServer *<SERVER2>*

1. You can verify that each DAG member was added by using running:

Get-DatabaseAvailabilityGroup -Identity *<DAG\_NAME>* | Format-List Servers

### Add Mailbox Database Copies to the DAG

The final step is to add mailbox database copies back to the appropriate DAG member.

* ***Case 1***: If the database files and logs on disk are preserved and in their original location or copied to the original location, the Microsoft Exchange Replication service may be able to perform an incremental resynchronization of the passive copies:

Update-MailboxDatabaseCopy -Identity *<DAG\_NAME>-DB01\<SERVER1>*

Update-MailboxDatabaseCopy -Identity *<DAG\_NAME>-AR01\<SERVER2>*

* ***Case 2***: The database files and logs on disk are not preserved. To add the mailbox database copies back to the DAG:
  1. Ensure or cleanup the database and log locations
  2. Add the mailbox and archive database copies back to the DAG:

Add-MailboxDatabaseCopy -Identity *<DAG\_NAME>-DB01* -MailboxServer *<SERVER2>*

Add-MailboxDatabaseCopy -Identity *<DAG\_NAME>-AR01* -MailboxServer *<SERVER1>*

* 1. You can verify that each mailbox database copy was added successfully by using:

Get-MailboxDatabase <SITE>\*| Format-List Name,DatabaseCopies

* 1. You can also verify the health and status of all mailbox database copies in the DAG :

Get-MailboxDatabaseCopyStatus -Server <SERVER1>

Get-MailboxDatabaseCopyStatus -Server <SERVER2>

## Disaster Recovery procedure for Standalone server

Actions to do in case of disaster on server at Exchange site:

|  |  |
| --- | --- |
| Disaster | Action |
| Database lost due to disk issue | Repair disk and LUN  Restore database (See Restore/Backup documentation) |
| Database lost due to corruption | Restore database (See Restore/Backup documentation) |
| Server lost | Here are the steps to recover an Exchange 2010 SP1 Mailbox server as a DAG member:   |  | | --- | | 1. Reinitialize the computer account of the server to recover (in Active Directory):    1. Open Active Directory Users and Computers console.    2. Search of localize the computer account in the organizational unit.    3. Right click on the computer account and click on “*Reinitialize the account*”. | | 1. Rebuild the server in the same way that it was before the disaster:    1. The same OS version and the same name as the lost server    2. The storage as it was on the lost server and recreate al of the adequate folder trees    3. Network interfaces parameters    4. Exchange 2010 SP1 requirements and prerequisites   For these purpose, apply the last validated version of “***Exchange 2010 SP1 Server build guides***”. (documentation for your environment) | | 1. Open Command Prompt console, navigate to Exchange 2010 SP1 setup and execute this command:   **Setup /m:RecoverServer**  ***Note***: This step can be time consuming. | | 1. Set all of the mandatory custom parameters as they were present on the lost server: certificates, storage path for HUB server, etc.). |   *For more information, refer to* [*http://technet.microsoft.com/en-us/library/dd876880.aspx*](http://technet.microsoft.com/en-us/library/dd876880.aspx) |

Database Reseed Scenarios

Before discussing which situations require database reseeds, note that the following scenarios do not require database reseeds.

* In a scheduled outage scenario, the active log file is closed and all required log files are shipped to the target database copy ensuring that the copy activation is lossless.
* Unscheduled outages where log shipping is healthy and keeping up with the log generation on the active will not diverge the database copies. This can be corrected by incremental reseed as a result of LLR enforcing a database lag so that the updated log stream can just be applied and rolled forward. Ensuring that log shipping is healthy is critical for environments that utilize continuous replication. For more information, see [Monitoring Continuous Replication](http://technet.microsoft.com/en-us/library/bb629521(EXCHG.80).aspx).
* Network outages do not require database reseeds as long as the log streams on the source are not truncated. Log truncation will not happen automatically as continuous replication is in an unhealthy state or otherwise inoperable. For more information, see the "Log Truncation" section.
* Network outages where there are multiple cluster replication host names defined do not require database reseeds, as automatic failover between the defined networks will occur, thus ensuring that the log streams are successfully copied to the passive node.

The following scenarios require reseeds:

* The administrator performed offline maintenance (ESEUTIL defragmentation, ISINTEG, ESEUTIL hard repair) against the production database. Offline maintenance operations like offline defragmentation change the structure of the database and these changes are not logged; therefore, a database reseed is required.
* A log in the log stream is corrupted or accidentally deleted before it was copied to the passive. In this case the only way past that log for the copy is to perform a database reseed.

# Server and Database Operations

## Databases

### Check the database copies status

Execute the following command to check the state of all databases and their copies replication health:

|  |
| --- |
| From the **Exchange Management Shell** console, execute the following command:  Get-MailboxDatabase | Get-MailboxDatabaseCopyStatus  The result must show :   * **Status** : ***Healthy*** for database passive copies / ***Mounted*** for database active copies * **ContentIndexState**: ***Healthy*** |

Execute the following command to check the state of the database copies status:

|  |
| --- |
| From the **Exchange Management Shell** console, execute the following command :  Get-MailboxDatabaseCopyStatus -Identity *<DB\_NAME>\<SRV\_NAME>*  *(Ex: Get-MailboxDatabaseCopyStatus -Identity EDV-DB01\EDV-CHM01)*  The result must show :   * **Status** : ***Healthy*** for database passive copy / ***Mounted*** for database active copy * **ContentIndexState**: ***Healthy*** |

*For more information, refer to* [*http://technet.microsoft.com/en-us/library/dd298044.aspx*](http://technet.microsoft.com/en-us/library/dd298044.aspx)

|  |  |
| --- | --- |
| ***Note*** | |
|  | *If the database copy is not in a running state (mounted/healthy) but the hosting Mailbox server is running and healthy, the command* ***Update-MailboxDatabaseCopy*** *can**used to**resume the database copy. For more information, refer to* [*http://technet.microsoft.com/en-us/library/dd335201.aspx*](http://technet.microsoft.com/en-us/library/dd335201.aspx) |

### Activate the initial database copies

The initial database copy is the first instance of the database that was created and has the *ActivationPreference* set to “1”.

When a database is failover or switchover to another copy, it will still stay as is even if the initial are up to running again.

The script **RedistributeActiveDatabases.ps1** allows to redistributes the active copies across the DAG based on different criterias. Especially, with the option **BalanceDbsByActivationPreference**, for each database in the DAG, the script will move the active database to the preferred copy (*Activation Preference* at “1”).

To redistribute databases across a DAG, run this following command:

|  |
| --- |
| From an ***Exchange Management Shell*** console, navigate to the folder tree and set the default path to the Exchange 2010 SP1 scripts folder ***e:\Program Files\Microsoft\Exchange Server\V14\Scripts*** in the CGGVeritas context (In a default installation: “*C:\Program Files\Microsoft\Exchange Server\V14\Scripts”*) and run this command:  RedistributeActiveDatabases.ps1 -DagName *<DAG\_NAME>* –*BalanceDbsByActivationPreference*  *(Confirm the operation by entering “A” for ALL)* |

*For more information, refer to* [*http://technet.microsoft.com/en-us/library/dd335158.aspx*](http://technet.microsoft.com/en-us/library/dd335158.aspx)

### Failback – Resume database copy

Following a failure, a database can restart it activity by itself or may need an administrator action. For example:

* In the case of stopping a server hosting a database copy, the stopping of the replication service will be detected and the copy status will be ***ServiceDown***. Once the server (and thus the replication service) returns online, replication will automatically resume
* In the case of hard disk failure, the status of the database copy hosted on this disk will change to **FailedAndSuspended**. Once the disk returns online, it will be necessary to resume the database copy with the cmdlet **Resume-MailboxDatabaseCopy**.

It is thus necessary to [check the database copy status](#_Vérification_de_l’état_1) to determine if a manual action is mandatory or not. The complete list of a database state can be found on this TechNet link: <http://technet.microsoft.com/en-us/library/dd351258.aspx>

To resume the database copy, execute this command:

|  |
| --- |
| From an **Exchange Management Shell** console, run this command:  Resume-MailboxDatabaseCopy -Identity <DB\_NAME>\<MBX\_NAME>  *(Ex: Resume-MailboxDatabaseCopy -Identity EDV-DB01\EDV-CHM01)* |

### Log Truncation

#### Introduction

When passive database copies are unavailable, the Active copies will try in vain to synchronize their data with faulty copies. These attempts and successive failures prevent the truncation of database transaction logs. Transaction logs can become too large and compromising capacity storage and at long-term the server operation.

Also during an unavailability period, it is recommended to check available disk space on all volumes hosting databases and transaction log files to avoid saturation that would result an interruption of messaging services.

And to maintain a reasonable size of transaction logs, unavailable database copies can be deleted. In this case the active copies stop trying to synchronize their data and the transaction logs are truncated. This operation is especially important in a context where the downtime of copies is prolonged.

Once back to normal, deleted copies must be added to the DAG.

***Note***: For simplicity sake, let’s say **the log space was sized for 3 days retention**. If the downtime is **more than 2 days**, the database copy(ies) **must be deleted** to avoid a full log space.

In this case, you must take into account the duration for reseeding the databases when applying the failback operations.

#### Delete database passive copy

Run this command to remove database passive copy:

|  |
| --- |
| From an **Exchange Management Shell** console, run this command:  Remove-MailboxDatabaseCopy -Identity <DB\_NAME>\<MBX\_NAME>  *Confirm by “Y” and ignore all of the warning*  *(For example: Remove-MailboxDatabaseCopy -Identity EDV-DB01\EDV-CHM01)* |

#### Add database copy

Run this command with the mandatory parameters to add a database copy:

|  |
| --- |
| From an **Exchange Management Shell** console, execute this command:  Add-MailboxDatabaseCopy -Identity *<DB\_NAME>* -MailboxServer *<SRV\_NAME>* -ActivationPreference *<PREFERENCE>*  *(Ex: Add-MailboxDatabaseCopy –Identity EDV-DB01 -MailboxServer EDV-CHM01 -ActivationPreference 2)* |

|  |  |
| --- | --- |
| ***Note*** | |
|  | *After adding the passive database copies, log replication update or boot (seeding) is automatically performed. Continuous replication is automatically enabled. After synchronization, the passive copy status is Healthy.* |

### Dismount a database

Run this command to dismount a database:

|  |
| --- |
| From an **Exchange Management Shell** console, run this command:  Dismount-Database <DB\_NAME>  *(If the database files are no longer available, the command must be confirmed by “Y” for the creation of missing elements during mounting)* |

### Mount a database

Run this command to mount a database:

|  |
| --- |
| From an **Exchange Management Shell** console, run this command:  Mount-Database <DB\_NAME>  *(If the database files are no longer available, the command must be confirmed by “Y” for the creation of missing elements during mounting)* |

## Maintenance

Note: This chapter can be applied only on a DAG. If you are using a standalone Exchange 2010 server (multirole) you can skip the whole chapter.

### Activate Maintenance mode

Run this command to prepare a schedule downtime of a DAG member:

|  |
| --- |
| From an ***Exchange Management Shell*** console, navigate to the folder tree and set the default path to the Exchange 2010 SP1 scripts folder ***e:\Program Files\Microsoft\Exchange Server\V14\Scripts*** in the CGGVeritas context (In a default installation: “*C:\Program Files\Microsoft\Exchange Server\V14\Scripts”*) and run this command:  StartDagServerMaintenance.ps1 -ServerName *<MBXSRV\_NAME>* |

|  |  |
| --- | --- |
| ***Note*** | |
|  | *During maintenance activation on a server, all active databases running in the server are moved to another copy location based on the action preference parameter.*  *If a single passive copy of a database is unavailable, the database will not be moved and the script will generate related errors. In this case, it is necessary to move the database to another server with the following command:*  **Move-ActiveMailboxDatabase *<DB\_NAME>* –ActivateOnServer *<TARGETMAILBOXSERVER>***  *(Ex: Move-ActiveMailboxDatabase EDV-DB01 –ActivateOnServer EDV-CHM02)*  *Then, the maintenance script* ***StartDagServerMaintenance.ps1*** *must re-run as initially.* |

### Back from maintenance

Execute this command to bring online a mailbox server that is member of a DAG:

|  |
| --- |
| From an ***Exchange Management Shell*** console, navigate to the folder tree and set the default path (In a default installation: “*C:\Program Files\Microsoft\Exchange Server\V14\Scripts”*) and run this command:  StopDagServerMaintenance.ps1 -ServerName *<SRV\_NAME>* |

### Suspend a DAG node

Execute this command to suspend a mailbox server that is member of a DAG:

|  |
| --- |
| From an **Exchange Management Shell** console, execute the following command to load the cluster management cmdlets:  Import-Module FailoverClusters |
| Run the following command to suspend the DAG node:  Suspend-ClusterNode *<SRV\_NAME>* |

### Witness Server

#### Force to use the Assign the server to use

Execute this command to force the DAG to use the default witness server:

|  |
| --- |
| From **Exchange Management Shell** console, execute this following command:  Set-DatabaseAvailabilityGroup *<DAG\_NAME>*  *(Ex: Set-DatabaseAvailabilityGroup DAG01)* |

|  |  |
| --- | --- |
| ***Note*** | |
|  | *During the normal run of a DAG (no server is declared as stopped or suspend), running this command will force the DAG to use the witness server that is set on the parameter* ***WitnessServer*** *of DAG. If the witness folder is not present on the witness server (for example after a server recovery) this folder will be automatically recreate.* |

#### Change the witness server

For using a server as a witness server of an Exchange 2010 DAG, the server must be compliant with these following prerequisites:

* The witness server is not a member of the DAG and it is not a Domain Controller. Ideally, the witness server must be a HUB server.
* The witness folder must be empty.
* The Exchange Security group “***Exchange Trusted Subsystem***” must be local Administrators of the witness server.

Execute this following command to change the default witness server of the DAG:

|  |
| --- |
| From **Exchange Management Shell** console, run this following command:  Set-DatabaseAvailabilityGroup *<DAG\_NAME>* -WitnessServer *<WITNESS\_SERVER>* –Witnessdirectory “*<WITNESS\_FOLDER>*”  *(Ex: Set-DatabaseAvailabilityGroup DAG01 -WitnessServer SVRNAME -Witnessdirectory “C:\FSW-DAG01”)* |

## Transport

### Disable Receive connectors

Execute the following command to disable all the receive connectors of a HUB server:

|  |
| --- |
| From **Exchange Management Shell** console, execute the following command:  Get-ReceiveConnector –Server *<HUB\_NAME>*| Set-ReceiveConnector -Enabled *$False* |

### Enable Receive connectors

Execute the following Execute the following command to enable all the receive connectors of a HUB server:

|  |
| --- |
| From **Exchange Management Shell** console, execute tis following command:  Get-ReceiveConnector –Server *<HUB\_NAME>*| Set-ReceiveConnector -Enabled *$True* |

### Check HUB queues

Execute the following command to display all the queue of a HUB server:

|  |
| --- |
| From **Exchange Management Shell** console, execute this following command:  Get-Queue –Server *<HUB\_NAME>* |

# Monitoring Exchange Database Information and Statistics

## Viewing Mailbox Statistics

You can use the *Get-MailboxStatistics* EMS cmdlet to view the statistics for all the mailboxes on a server, for all the mailboxes in a mailbox database, or for a single mailbox. The following command lists the statistics for all the mailboxes on the Mbx-Ex01 server:

*Get-MailboxStatistics –Server Ex01 | FL*

The following command lists all the mailboxes in the mailbox database “Mailbox Database 1234567890”:

*Get-MailboxStatistics –Database “Mailbox Database 1363123687” | FL*

If a user mailbox has been created but has never been accessed, that mailbox is not included when you list the statistics of mailboxes on a server or in a mailbox database. If you attempt to obtain statistics for a mailbox that has not been accessed, you will get no statistical information but will instead receive a warning message.

*Get-MailboxStatistics –identity “John Hall” | FL*

Warning: The user hasn’t logged on to Mailbox “John Hall” so there is no data to return. After the user logs on, you won’t see this warning anymore.

If a mailbox returns statistics, you can use the PowerShell format-list (FL) cmdlet to display the value of one or more specified statistics. The following command displays the last logon time for Kim Akers mailbox.

*Get-MailboxStatistics –Identity “Jennifer Akers” | FL LastLogonTime*

You can use the *Sort-Object* PowerShell cmdlet to sort the mailboxes in a mailbox database or on a Mailbox server by the value of one or more mailbox statistics. You can do this either *descending* or *ascending* order and use the *format-table (FT)* PowerShell cmdlet to display the result as a table. The following command lists the mailboxes in the Research mailbox database in descending order of item count:

*Get-MailboxStatistics – Database DB01 | Sort-Object ItemCount –Descending | FT DisplayName, ItemCount*

The following command lists the mailboxes in the Research mailbox database in descending order of total item size:

*Get-MailboxStatistics –Database DB01 | Sort-Object TotalItemSize –Descending |FT DisplayName, TotalItemSize*

If you do not want to list all the mailboxes in a mailbox database or on a Mailbox server but instead want to list the top five mailboxes in terms of total item size, you can pipe the results of your search into the *Select-Object* PowerShell cmdlet. The following command lists the top five mailboxes in Mailbox Database 1234567890 in descending order of total item size:

*Get-MailboxStatistics –Database “Mailbox Database 1234567890” | Sort-Object TotalItemSize –Descending | Select-Object – First 5 | FT DisplayName, TotalItemSize*

## Monitoring Resource Usage

The Microsoft Exchange Information Store collects per user information on latency, I/O, page counts, processor usage, and *TimeInServer*. The *TimeInServer* metric represents the total time that sync and async requests spend in the Microsoft Exchange Information Store for a user's mailbox. You can retrieve this resource information in the Microsoft Exchange Information Store for the 25 highest usage accounts on a specified database by using the **Get-StoreUsageStatistics** cmdlet in the EMS.

|  |
| --- |
| **Description: Description: Dd351172.note(en-us,EXCHG.141).gifNote:** |
| Usage of a mailbox is defined as the amount of server time spent in performing operations for that mailbox. The cmdlet reports the top 25 users for every one-minute period for the last 10 minutes (250 objects per ten-minute interval). The resource usage is an indicator of the load that different users are placing on the server. |

The following command returns the 25 highest usage accounts in Mailbox Database 1234567890:

*Get-StoreUsageStatistics – database “Mailbox Database 1234567890”*

Use the Get-StoreUsageStatistics cmdlet to obtain statistics about a specific mailbox, but only if this mailbox account is one of the 25 top resource users during the previously stated interval. The following command would generate a report about the Kim Akers account:

*Get-StoreUsageStatistics –Identity “Jennifer Akers”*

## Using Performance Monitor Counters

Use the Exchange Server Performance Monitor tool to monitor counters that can indicate whether resources in your Exchange Organization are coming under stress. This is the same tool as Performance Monitor (PerfMon) except that the Performance and Logs Alerts snap-in has been prepopulated with a large number of Exchange-related performance counters. Access Exchange Server Performance Monitor from the EMC by clicking the Toolbox node, clicking Performance Monitor, and clicking Open Tool.

To ensure that your mailbox databases continue to operate efficiently, you need to check that they are being defragmented online on an ongoing basis. Online defragmentation is a background task that operates continuously by default. Exchange Server 2010 provides the following performance counters for monitoring the behaviour of online database defragmentation:

* **MSExchange Database Online Defrag Average Log Bytes:** Shows average size of the log records being generated by online defragmentation.
* **MSExchange Database Online Defrag Data Moves/Sec:** Shows the number of times that data is moved from one page to another by the online defragmentation process.
* **MSExchange Database Online Defrag Log Records/Sec:** Shows the number of times per second that data is moved from one page to another by the online defragmentation process.
* **MSExchange Database Online Defrag Page Moves/Sec:** Shows the number of times that data is moved from one page to a new page by the online defragmentation process.
* **MSExchange Database Online Defrag Pages Dirtied/Sec:** Shows the rate at which online defragmentation is modifying clean database pages.
* **MSExchange Database Online Defrag Pages Freed/Sec:** Shows the number of pages per second that are freed from the database by the online defragmentation process.
* **MSExchange Database Online Defrag Pages Preread/Sec:** Shows the rate at which database pages are read in anticipation of future use by online defragmentation.
* **MSExchange Database Online Defrag Pages Read/Sec:** Shows the rate of database read operations being performed by online defragmentation.
* **MSExchange Database Online Defrag Pages Re-Dirtied/Sec:** Shows the rate at which online defragmentation is modifying database pages that already contained modifications.
* **MSExchange Database Online Defrag Pages Re-Dirtied/Sec:** Shows the rate at which online defragmentation is touching database pages.

## Obtaining Information about Public Folder Databases

When monitoring a public folder database, obtain general information about the database, such as the server where it is located, what public folders it contains, its maximum item size, quota limits, replication schedule, and so on. Use EMS commands based on the *Get-PublicFolderDatabase* cmdlet for this purpose. The following command gets detailed information about evry public folder database in an organization:

*Get-PublicFolderDatabase | FL*

To obtain detailed information about a specific public folder database, you can specify the Exchange Server 2010 Mailbox server on which it is located. The following command gets detailed information about the public folder database on the VAN-EX1 server:

*Get-PublicFolderDatabase –Server Exch1 | FL*

It is typically easier to analyse and store this information if the output of the command is redirected to a text file. The following command redirects detailed information about the public folder database on the Exch1 server to the text file PublicFolderDetails.txt in the DatabaseInformation folder on the Exch1 server:

*Get-PublicFolderDatabase –Server Exch1 | FL > C:\databaseinformation\PublicFolderDetails.txt*

Use the Status parameter of the *Get-PublicFolderDatabase* cmdlet to obtain backup and mount status information (if available). Checking the status of public folder databases is an important step in monitoring replication health. The following command gets detailed information about the public folder database on the Exch1 server, including status information:

*Get-PublicFolderdatabase –Server Exch1 –Status | FL*

## Viewing Public Folder Statistics

No EMS cmdlet exists that returns the statistics for an entire public folder database. However, you can use the Get-PublicFolderStatistics EMS cmdlet to obtain statistics for each individual public folder within a public folder database. Check replication by ensuring that the number and size of items in the public folder replica are the same as in the original public folder. Use the same procedure if you replicate an entire public folder database and want to check that replication is working correctly.

The following command obtains statistics for every public folder in an Exchange 2010 organization:

*Get-PublicFolderStatistics | FL*

The previous command can return an excessive volume of information, particularly if there are a large number of public folders. As with mailbox databases, refine the information to obtain statistics for every public folder on the Mailbox server Exch1, enter the following command:

*Get-PublicFolderStatistics –Server Exch1 | FL*

To obtain statistics for the public folder MyPublicFolder on the Mailbox server Exch1, enter the following command:

Get-PublicFolderStatistics –Identity \MyPublicFolder –Server Exch1 | FL

## Viewing Mailbox Database Replication Health

When operating Database Availability Groups, making sure that database copies are healthy are key objectives for daily messaging operations. In addition to hardware and operating system monitoring covered earlier in this section, messaging administrators should proactively monitor the replication status and health of databases within each DAG. The following two PowerShell cmdlets can be used in the EMC to perform this monitoring:

* Get-MailboxDatabaseCopyStatus
* Test-ReplicationHealth

**Get-MailboxDatabaseCopyStatus**

This cmdlet is used to view the status information about mailbox database copies. This cmdlet allows you to view information about all copies of a particular database, information about a specific copy of a database on a specific server or information about all database copies of a server.

This example returns status information for all copies of the database ContosoDB1.

Get-MailboxDatabaseCopyStatus –Identity ContosoDB1 | Format-List

This example returns status information for all database copies on the Mailbox server JEXCH01.

Get-MailboxDatabaseCopyStatus –Server EXCH01 | Format-List

This example returns status, log shipping and seeding network information for database ContosoDB1 on Mailbox server JEXCH01.

Get-MailboxDatabaseCopyStatus –Identity EXCH01\ContosoDB1 –ConnectionStatus | Format-List

The health of an individual Mailbox Database can be viewed in the Exchange Management Console (EMC):

1. In the console tree, expand Organization Configuration, and then click **Mailbox**.
2. In the result pane, on the **Database Management** tab, select the database you want to monitor.
3. The action pane will display the health of each database in the DAG and the status or replication to each passive copy of the database.

**Test-ReplicationHealth**

This cmdlet is designed for the proactive monitoring of continuous replication and continuous replication and status of the underlying cluster service, quorum and network components. It can be run locally on or remotely against any Mailbox server in a DAG.

This example tests the health of replication for the Mailbox server JEXCH01.

Test-ReplicationHealth–Identity EXCH01

For additional information on these cmdlets and instructions on scripts provided by Microsoft to automate these tasks, reference **Monitoring High Availability and Site Resilience**:

[*http://technet.microsoft.com/en-us/library/dd351258.aspx*](http://technet.microsoft.com/en-us/library/dd351258.aspx)

## Verifying Success of Database Backups

You have several options when approaching your Organization’s data protection methodology. With the new native data protection features that Exchange 2010 introduces, many Organizations are choosing not to implement a traditional backup solution for their Exchange messaging infrastructure. Those Organizations wishing to maintain a traditional backup process should perform daily tasks to validate that backups completed successfully.

* Verify the backup timestamps of the mailbox database. This can be performed by right clicking the mailbox database under Organizational Configuration in the Exchange Management Console (EMC) and selecting **Properties** or via cmdlets executed in the Exchange Management Shell (EMS):

This example will produce the **LastFullBackup**, **LastIncrimentalBackup**, **LastDifferentialBackup** and **LastCopyBackup** values for the mailbox database ContosoDB1

Get-MailboxDatabase –Identity ContosoDB1 | Format-List Identity, Last\*

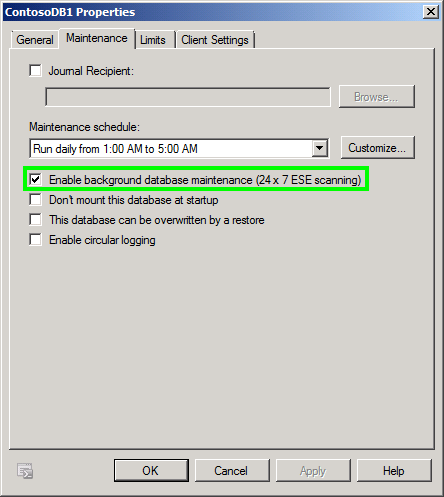
* Check the Event Logs on the Exchange 2010 Mailbox server hosting the backup target. Be aware that most third party backup applications leverage the Microsoft Exchange Replication service VSS Writer to perform the backup against a passive copy of the Mailbox database. This will log backup events on the Mailbox server hosting the target passive copy.
* If a Full or Incremental backup was performed, validate that Exchange Mailbox Database transaction logs have been truncated.

|  |
| --- |
| **Description: Description: Dd351172.note(en-us,EXCHG.141).gifNote:** |
| If the database being backed up has lagged copies, are there log files older than ReplayLagTime + TruncationLagTime?  If Circular Logging is enabled, logs will truncate once they’ve replayed to all copies of the Mailbox database regardless of backups. |

* If a third party application was used to perform the Mailbox database backup, check the appropriate logs in the third party application to confirm a successful backup.

## Monitoring Background Database Maintenance

Different in Exchange 2010, the Online Defragmentation tasks no longer run at the end of Online Maintenance by default, but rather run as a 24x7 background task and is throttled so it does not negatively affect database performance. This value is managed by the **Enable background database maintenance (24 x 7 ESE scanning)** checkbox on the **Maintenance** tab of the Mailbox database properties:



In previous versions of Exchange, the health of Online Defragmentation could be monitored by checking for 70x Events in the Exchange server’s Application Event Log. In Exchange 2010, these events are only logged if there is a problem with Online Maintenance. Inversely, administrators wishing to check the status of Online Maintenance as part of a regular maintenance task can use the **–Status** switch of the **Get-MailboxDatabase** cmdlet.

The following command displays the Online Defragmentation statistics for database ContosoDB1:

Get-MailboxDatabase ContosoDB1 –Status | Format-List Identity, \*Background\*

The following command checks the available whitespace for database ContosoDB1:

Get-MailboxDatabase ContosoDB1 –Status | Format-List AvailableNewMailboxSpace

|  |
| --- |
| **Description: Description: Dd351172.note(en-us,EXCHG.141).gifNote:** |
| Queue databases still report 70x Event ID’s for Online Defragmentation. |

* **Installing Update Rollups on DAG Members -** Installing Microsoft Exchange Server 2010 update rollups on a server that is a member of a database availability group (DAG) is a relatively straight forward process. When you install an update rollup on a server that is a member of a DAG, several services will be stopped during the installation, including all Exchange and the Windows Cluster service. The general process for applying update rollups to a DAG member is as follows:
  1. Perform a server switchover so that all databases on the server are passive copies.
  2. Suspend activation for the databases on the server being updated.
  3. Install the update rollup.
  4. Resume activation for the databases on the updated server.
  5. Perform database switchovers as needed.

For additional tips and considerations when installing Update Rollups for Exchange 2010, reference **Installing the Latest Update Rollup for Exchange 2010**:

<http://technet.microsoft.com/fr-be/library/ff679928(en-us).aspx>

For instructions for the steps required to install Update Rollups on Database Availability Group (DAG) member, reference **Installing Update Rollups on Database Availability Group Members**:  
<http://technet.microsoft.com/en-us/library/ee861125.aspx>

# Unified Messaging

Operations management involves the administration of an organization's Unified Messaging infrastructure components and includes the day-to-day administrative tasks, both planned and on-demand, that are required to keep Unified Messaging operating smoothly.

In a Microsoft Exchange Server 2010 environment, typical system administration tasks associated to Unified Messaging include managing servers, managing users, managing Unified Messaging components including IP Gateways and monitoring logs, etc.

## Standard Procedures

Several resources can help you define what standard procedures are required in your organization and how to perform them. Because each organization is unique, you will have to customize and adapt these resources to suit your requirements.

Standard procedures will change, and documentation will occasionally need to be revised. As changes are made, your change management process should identify how each change is likely to affect how and when administrative tasks are performed. Use the change management function to update and control the documentation.

* **Managing Unified Messaging Servers**   
  <http://technet.microsoft.com/en-us/library/aa998602.aspx>
* **Managing Unified Messaging Users**<http://technet.microsoft.com/en-us/library/aa996734.aspx>
* **Managing Unified Messaging Components**   
  <http://technet.microsoft.com/en-us/library/bb124372.aspx>
* **Managing IP Gateways**   
  <http://technet.microsoft.com/en-us/library/bb125228.aspx>

## Unified Messaging Availability

Minimum uptime requirements may vary among organizations. However, every organization wants to achieve a high level of uptime, especially for their telephony system. An organization's telephony system is frequently business-critical and must be highly available to users. One of the factors that you must consider when you deploy a Unified Messaging system is the ability for the system to provide services for users when a key component such as a Unified Messaging server or an IP/VoIP gateway becomes unavailable.

* **Unified Messaging Servers** In Exchange 2010, Unified Messaging is designed to run as a service and a worker process. Unified Messaging deployments can be made more resilient and more available by adding Unified Messaging servers to a single dial plan in an N+1 configuration. This means that, if you must have two Unified Messaging servers, you would install and configure an additional Unified Messaging server so that you would have a Unified Messaging server to take the place of a Unified Messaging server that is failing or must be taken offline. When you add multiple servers to a single dial plan, the IP/VoIP gateway must try to connect to a Unified Messaging server that is listed in the configuration on the IP/VoIP gateway (or via multiple SIP Trunks).
* **IP/VoIP Gateways** If you need to create redundancy to provide for IP/VoIP gateway availability, you should add multiple IP/VoIP gateways in an N+1 configuration. This means that, if you must have two IP/VoIP gateways, you would install and configure an additional IP/VoIP gateway so that you would have an IP/VoIP gateway to take the place of an IP/VoIP gateway that is failing or must be taken offline.

### Load Balancing and Redundancy; How does UM failover work?

Unified Messaging servers don’t have any load balancing logic built-in. The Unified Messaging server will not accept new calls only when the max calls have been reached. If the Unified Messaging Server is unreachable (or in maintenance mode), you must configure your PBX so that it will send the incoming calls that it has received to different IP/VoIP gateways. After you configure the PBX, the PBX will detect a failure or no signal or that a port is not answering call. This will enable the PBX to redirect calls to an IP/VoIP gateway that can answer incoming calls.

**Load Balancing in Unified Messaging**

Depending upon the SLA requirements, Exchange 2010 Unified Messaging deployments can be made more resilient by deploying multiple Unified Messaging servers to a single dial plan to balance the load of incoming calls. The IP/VoIP gateways that are supported by Unified Messaging can be configured to route calls in a round-robin manner to balance the load between multiple Unified Messaging servers that are within a dial plan.

Round robin is a method for distributing the workload among multiple servers. However, round robin does not by itself enable an IP/VoIP gateway to detect a server failure. If one of the Unified Messaging servers fails and if the IP/VoIP gateway cannot detect that a Unified Messaging server is unavailable, the IP/VoIP gateway will continue to send incoming calls to the Unified Messaging server until you detect the failure and remove the server from the dial plan. After you remove the Unified Messaging server from the dial plan, you should also remove the IP address or FQDN for the Unified Messaging server from the configuration on the IP/VoIP gateway.

When Exchange 2010 is deployed in coexistence mode with Office Communications Server or Lync Server 2010, this load balancing happens automatically in the EXUMROUTING component that runs on the Front Ends. However, if Unified Messaging is deployed against any other gateway, the Unified Messaging server has no mechanism to load balance the traffic automatically (i.e. redirect a call from UMSrv1 to UMSrv2), the Gateway () must have the following capability to evenly distribute the calls across all the servers in the Dial Plan (i.e. the ability to configure multiple SIP trunks, one to each Unified Messaging Server in the dial plan). These SIP trunks are then configured to load balance the endpoints (all servers in the dial plan)

Exchange Server 2010 Unified Messaging provides the following performance counters for monitoring concurrent calls:

**Get-UMActiveCalls**

This cmdlet can be used to monitor the current number of concurrent calls that are connected to a Unified Messaging server.

If the number of concurrent calls required by your organization is larger than the number that is supported by a single Unified Messaging server, you can scale horizontally and increase the capacity of concurrent calls by installing the Unified Messaging server role and then adding the Unified Messaging server to a dial plan

**Number of concurrent calls** By default, a Unified Messaging server can accept 100 concurrent voice messages and 100 concurrent fax messages. When you increase the number of concurrent connections on a single Unified Messaging server, more system resources are required than if you decrease the number of concurrent connections. It is especially important to decrease this setting on low-end, slower computers on which the Unified Messaging server is installed..

**Monitoring/Capacity**

|  |  |  |  |
| --- | --- | --- | --- |
| **Performance Counter** | **Performance Object** | **Description** | **Expected Values** |
| Current Calls | MSExchangeUMGeneral | Number of calls that are currently connected to the UM server. | Less than 60 under normal conditions |
| Delayed Calls | MSExchangeUMGeneral | Delayed Calls is the number of calls that experienced one or more delays longer than 2 seconds. | Should be 0 at all times |

**Performance**

|  |  |  |  |
| --- | --- | --- | --- |
| **Performance Counter** | **Performance Object** | **Description** | **Expected Values** |
| Call Answer Queued Messages | MSExchangeAvailability | Shows the number of messages created and not yet submitted for delivery. | Should be less than 50 at all times. |
| Calls Disconnected by Callers During UM Audio Hourglass | MSExchangeUMCallAnswer | Shows the number of calls during which the caller disconnected while Unified Messaging was playing the audio hourglass tones. A non-zero value suggests excessive latency between a Unified Messaging server and targeted domain controller. | Should be 0 at all times. |
| Direct Access Failures | MSExchangeAvailability | Shows the number of times that attempts to access Active Directory failed | Should be 0 at all times |
| Hub Transport Access Failures | MSExchangeAvailability | Shows the number of times that attempts to access a Hub Transport server failed. This number is only incremented if all Hub Transport servers were unavailable | Should be 0 at all times |
| Mailbox Server Access Failures | MSExchangeAvailability | Shows the number of times the system did not access a Mailbox server. A non-zero value indicates that Unified Messaging is having problems with MAPI connectivity to mbx servers. | Should be 0 at all times |
| Operations over Six Seconds | MSExchangeUMPerformance | Shows the number of all Unified Messaging operations that took more than six seconds to complete. This is the time during which a caller was waiting for Unified Messaging to respond. | Should be 0 at all times |
| Queued OCS User Event Notifications | MSExchangeAvailability | Shows the number of notifications that have been created and not yet submitted for delivery. Represents the number of missed call notifications that have been generated in the Office Communications Server environment and have not been submitted for delivery. | Should be 0 at all times |
| Unhandled Exceptions/sec | MSExchangeAvailability | Shows the number of calls that were disconnected after an internal system error occurred in the last second.   Note: The name of this performance counter (Calls Disconnected on Irrecoverable Internal Error Per Second) does not match the name listed in its description. | Should be 0 at all times |
|  |  |  | Should be 0 at all times |

**Health Indicators**

|  |  |  |  |
| --- | --- | --- | --- |
| **Performance Counter** | **Performance Object** | **Description** | **Expected Values** |
| Calls Disconnected by UM on Irrecoverable External Error | MSExchangeAvailability | Calls Disconnected by UM on Irrecoverable External Error is the number of calls disconnected after an irrecoverable external error occurred. | Should be 0 at all times |
| Calls Disconnected by UM on Irrecoverable External Error/sec | MSExchangeAvailability | Calls Disconnected by UM on Irrecoverable External Error/sec is the number of calls disconnected after an irrecoverable external error occurred in the last second | Should be 0 at all times |
| Calls Disconnected on Irrecoverable Internal Error | MSExchangeAvailability | Calls Disconnected on Irrecoverable Internal Error is the number of calls that were disconnected after an internal system error occurred. | Should be 0 at all times |
| Failed to Redirect Call | MSExchangeAvailability | Failed to Redirect Call is the number of times the Microsoft Exchange Unified Messaging service didn't redirect calls to a UM worker process | Should be 0 at all times |
| Incomplete Signaling Information | MSExchangeAvailability | Incomplete Signaling Information is the number of calls for which the signaling information was missing or incomplete | Should be 0 at all times |
| Calls Rejected | MSExchangeUMGeneral | Calls Rejected is the number of new call invitations that have been rejected | Should be 0 at all times |
| Calls Rejected per Second | MSExchangeUMGeneral | Calls Rejected per Second is the number of new call invitations that have been rejected in the last second | Should be 0 at all times |
| Diverted Extension Not Provisioned | MSExchangeUMCallAnswering | Diverted Extension Not Provisioned is the number of calls received for which the diverted extension supplied with the call is not a UM subscriber extension. If the number of extensions not provisioned eventually goes over 0, the administrator can access the events logger on the server, identify the improperly configured extension and make adjustments proactively | Should be 0 all times |
|  |  |  |  |

## Unified Messaging Redundancy and Timeouts (EXUMROUTING)

**EXUM Routing Configuration Overview**  
**Adding more redundancy & Understanding Timeouts**

On each OCS/Lync Front End, there are component specific <appSettings> for EXUM Routing stored in the ‘**ExUMRouting.exe.config’** file. These configuration options determine how long the Front End will wait for UM to connect the call -and- determine how many UM Servers to try if the first or subsequent server is unavailable.

The value **ExumAttemptTimeLimit** allows a timer to be started to keep track of the response. If the UM server does not respond before the timer expires the server will be marked as ‘deprecated’ and will be given a lower priority so that it is selected less frequently for call processing. The default value for the timer is 5 seconds.

**<configuration> <appSettings>   
 <add key="ExumAttemptTimeLimit" value="x"/>  
 <!-- Time to wait for ExUM server to respond before giving up.   
Default is 5 seconds for R2, 10 for Lync -->**

There is also a **ExumFinalAttemptTimeLimit** that defines the Final Timeout Value to wait for the last EXUM Serer to respond before dropping the call.

**<add key="ExumFinalAttemptTimeLimit" value="20000"/>  
 <!-- Time to wait for the final ExUM server to respond before giving up.**

**Default is 20000 milliseconds-->**

The **ExumNumberOfServersToTry** value determines how many UM Servers will be tried for a given call. To distribute inbound calls this number should equate to the maximum number of UM Servers that will host Dial Plans in that region.

**<configuration> <appSettings>**<add key="ExumNumberOfServersToTry" value="x">   
 <!-- Number of ExUM servers to try before giving up. -->

**This value should be based on the maximum # of UM Servers you want to try.  
(i.e. account for each UM Server that will host a given Dial Plan)**

By default Office Communications Server will only try two Exchange Unified Messaging servers, and if they are not available, will drop the call. Once a Server does not respond, it will be marked “down” and another server will be chosen based on the Dial Plan membership.

**Action:** Verify the following line matches the maximum # of UM Servers you have. For example, in a Pool with 5 unified messaging servers, you can enable EXUM Routing component to try all "5" servers before dropping the call.)

<add key="ExumNumberOfServersToTry" value="5">

Exumrouting.exe.config File

One consideration to keep in mind is what happens if the server running Exchange UM is unavailable to answer the call? By default, Lync Server 2010 and Office Communications Server attempt to route to a configured number of UM Servers.

This logic is defined in a configuration file used by the EXUMROUTING.EXE service. This configuration file is located in the %ProgramFiles%\Microsoft Lync Server 2010\Server\Core folder and is called EXUMROUTING.EXE.CONFIG.

The default file contents are as follows:

<configuration>

<runtime>

<gcServer enabled="true" />

</runtime>

<appSettings>

<!-- Time to wait for ExUM server to respond before giving up. Default is 5000 milliseconds-->

<add key="ExumAttemptTimeLimit" value="5000"/>

<!-- Time to wait for the finalExUM server to respond before giving up. Default is 20000 milliseconds-->

<add key="ExumFinalAttemptTimeLimit" value="20000"/>

<!-- Number of ExUM servers to try before giving up. -->

<add key="ExumNumberOfServersToTry" value="2"/>

<!-- Port that all Exchange UM servers listen on. -->

<!-- A value of 0 indicates the port is selected based on the transport (tcp=5060, tls=5061)-->

<add key="ExumListenPort" value="5061"/>

<!-- Transport Exchange UM is configured to use (tcp or tls).-->

<add key="ExumTransport" value="tls"/>

</appSettings>

</configuration>

The following options are defined in this configuration file:

* **Gcserver enabled = true**   Specifies whether the service runtime runs server garbage collection. This should not be changed.
* **ExumAttemptTimeLimit = x milliseconds**   Sets the timeout period that server running Lync Server 2010 waits before it marks the Exchange UM server as failed and moves on to the next Exchange UM server in the list.
* **ExumFinalAttemptTimeLimit = x milliseconds**   Defines the maximum time permitted for the final Exchange UM server to respond. This should be larger than Exumattempttimelimit, allowing the server running Lync Server 2010 extra time in case there is an extremely poor network connection (rather than a server failure).
* **ExumNumberOfServerToTry = x**   Defines the maximum number of Exchange UM servers that the server running Lync Server 2010 attempts to connect before failing to transfer the call to voice mail.
* **ExumTransport = port number**   Defines the port number used to connect to the Exchange UM server. The default ports for Exchange UM are 5060 and 5061 for Transmission Control Protocol (TCP) and for Transport Layer Security (TLS) respectively. If for any reason the port number is changed, the change must be reflected in this setting.

Although we recommend that the servers running Lync Server and the Exchange UM servers are well connected (that is, with less than 120 ms latency), in some customer scenarios this may not be possible. For example, the connectivity may be across poor network links or in a scenario where a firewall negotiation is required, which delays the initial setup. Therefore, you may need to adjust the timeout values for the settings, ExumAttemptTimeLimit and ExumFinalAttemptTimeLimit, based on network conditions.

We recommend that you increase the default value of ExumNumberOfServerToTry from two to the number of Exchange UM servers that the server running Lync Server 2010 can connect to. This ensures that all Exchange UM servers are attempted, which helps ensure the successful routing of the call to voice mail.

In a scenario where connectivity to the Exchange UM servers is completely lost (for example, data center failure), the Exchange UM servers are marked as unavailable. Lync Server retrieves the list of Exchange UM servers from the trusted servers list.

Consider the scenario, a customer has two data centers and two Exchange UM servers in each data center. Under normal conditions, Lync Server 2010 will randomly select an Exchange UM server to connect to for capture of the voicemail message. However, in a failure scenario, where Lync Server 2010 has connectivity to the Exchange UM servers but is unable to exchange media (for example ports blocked), Lync Server 2010 will only attempt connections to two servers. In this scenario, there is a chance that Lync Server will be unable to route the call into Exchange UM. By increasing the ‘ExumNumberOfServersToTry’ value to 3, this will ensure that a third server is attempted and therefore ensuring the successful routing of the call. Lync (EXUMRouting) will randomly select a UM server within the Dial Plan collection (all servers hosting a given dial plan are put in an array and will be used in the case of failover), however EXUMRouting will only initially attempt up to the number defined in ExumNumberOfServersToTry.

From a load balancing perspective, in this example, EXUMRouting will take “2” servers from the dial plan server array (UM-1, UM-2, UM-3 and UM-4) but will only load balance the maximum number defined of two of these four servers.

IF there are no failures, the calls will be evenly distributed between UM-1 and UM-2.

UM-3 will become a viable server ONLY when one of the first two servers (fails to respond 15007 or returns an error 4xx-5xx).

In a scenario where connectivity is completely lost to the Exchange UM servers (for example, datacentre failure), these server would be marked as ‘unavailable’ in the list read of the trusted servers.



## Network Traffic

Description: http://i.msdn.microsoft.com/Global/Images/clear.gif

Every incoming call that is received from an IP/VoIP gateway will generate IP-based network traffic and will consume some amount of your available network bandwidth. Because all the IP-based calls are routed directly to your Unified Messaging servers from the IP/VoIP gateways on your network and this IP-based network traffic consumes some available bandwidth, you should follow these recommendations and guidelines:

* Perform an analysis of the network traffic to determine current usage patterns and identify any potential issues. On most networks, bandwidth demand is not evenly distributed throughout business hours.
* Place your PBXs physically close to your IP/VoIP gateways.
* Place your IP/VoIP gateways and your Unified Messaging servers close together.
* Place your Unified Messaging servers and IP/VoIP gateways on the same subnet.
* Place your Unified Messaging servers and IP/VoIP gateways on the same virtual local area network (VLAN).
* Place your Unified Messaging servers close to other computers that have Exchange 2010 server roles installed, including Mailbox, Hub Transport, and Client Access servers.
* Terminate your Wide Area Network (WAN) connections close to where your telephony equipment is located.
* In branch office scenarios or over WAN connections, use the G.723.1 codec instead of the G.711u or G.711A codec to minimize the network traffic that is passed between your IP/VoIP gateways and your Unified Messaging servers.

When Lync Server and Exchange Unified Messaging are used in conjunction with each other RTAudio wideband is negotiated as the wire codec. OCS & Lync mediation servers and compatible endpoints are the only kind of SIP peers that negotiate RTAudio of any kind with UM.

The audio format and codec that Unified Messaging servers use to store the audio in voice messages depends not only on the audio codec that is configured on the dial plan but on the bit rate of the audio that UM negotiates with the SIP peer.

For example, when wideband RTAudio is negotiated as the wire codec, a Unified Messaging server will then use either 32 kbit/s MP3 or WMA when creating voice mail messages depending on the dial plan setting.   
  
Note: Starting with Exchange 2010 SP1, wire codec and audio port configuration settings are no longer stored in the registry. Now, these configuration settings are controlled by the MSExchangeUM.CONFIG file located in the \Program Files\Microsoft\Exchange Server\v14\Bin folder. The Exchange wire codec options that determine whether UM should advertise g.723 and RTAudio are listed below.

<!-- Whether to offer g.723 or not -->   
<add key="EnableG723" value="true" />   
  
<!-- Whether to offer RTAudio or not -->   
<add key="EnableRTAudio" value="true" />

Also, in Exchange 2010 SP1, the RTP minimum/maximum port ranges are also configured in the MSExchangeUM.CONFIG file, not in the registry.

<!-- The min/max ports to use for RTP media.   
If the values are invalid, or max < min, the default will be used -->   
<add key="MinimumRtpPort" value="xxxxx" />   
<add key="MaximumRtpPort" value="xxxxx" />

Note: Be sure to make a backup copy of your MSExchangeUM.CONFIG file before editing it.Some organizations may find it advantageous to use multiple formats. The voice mail audio codec can be set at the Dial Plan level or at the mailbox level. Both of these settings are configured on the Exchange Server.

// To change the audio codec at the dial plan-level, which applies to all calls that use this dial plan

Set-UMDialPlan –Identity {dialplanname} –AudioCodec {MP3/GSM/WMA/G711}

// To change the audio codec at the mailbox-level, which only applies to a specific user

Set-UMMailbox –Identity {username} –CallAnsweringAudioCodec {MP3/GSM/WMA/G711}

## Monitoring Server Performance

### Using Performance Monitor Counters

Use the Exchange Server Performance Monitor tool to monitor counters that can indicate whether resources in your Exchange Organization are coming under stress. The following performance counters for monitoring the behaviour Unified Messaging components.

|  |
| --- |
| **Unified Messaging Auto Attendant**   * MSExchangeUMAutoAttendant: Average Call Time |
| * MSExchangeUMAutoAttendant: Business Hours Calls |
| * MSExchangeUMAutoAttendant: Directory Accessed |
| * MSExchangeUMAutoAttendant: Disconnected Without Input |
| * MSExchangeUMAutoAttendant: Operator Transfers |
| * MSExchangeUMAutoAttendant: Out of Hours Calls |
| * MSExchangeUMAutoAttendant: Total Calls (Report Collection) |
| * MSExchangeUMAutoAttendant: Transferred Count |
| **Unified Messaging Availability**   * MSExchangeUMAvailability: Calls Disconnected by UM on Irrecoverable External Error (Report Collection) |
| * MSExchangeUMAvailability: Calls Disconnected on Irrecoverable Internal Error |
| * MSExchangeUMAvailability: Directory Access Failures |
| * MSExchangeUMAvailability: Total Queued Messages |
| **Unified Messaging Call Answering**   * MSExchangeUMCallAnswer: Average Voice Message Size |
| * MSExchangeUMCallAnswer: Call Answering Calls (Report Collection) |
| * MSExchangeUMCallAnswer: Call Answering Missed Calls (Report Collection) |
| * MSExchangeUMCallAnswer: Call Answering Voice Messages (Report Collection) |
| * MSExchangeUMCallAnswer: Calls Disconnected by Callers During UM Audio Hourglass |
| * MSExchangeUMCallAnswer: Fetch Greeting Timed Out |
| **Unified Messaging General**   * MSExchangeUMGeneral: Average Call Duration |
| * MSExchangeUMGeneral: Calls Rejected (Report Collection) |
| * MSExchangeUMGeneral: Current Calls |
| * MSExchangeUMGeneral: Delayed Calls (Report Collection) |
| * MSExchangeUMGeneral: Total Calls (Report Collection) |
| * MSExchangeUMGeneral: Total Calls per Second |
| * MSExchangeUMGeneral: User Response Latency |
| **Unified Messaging Subscriber Access**   * MSExchangeUMSubscriberAccess: Average Subscriber Call Duration |
| * MSExchangeUMSubscriberAccess: Calendar Accessed |
| * MSExchangeUMSubscriberAccess: Calendar Items Heard |
| * MSExchangeUMSubscriberAccess: Calls Disconnected by Callers During UM Audio Hourglass |
| * MSExchangeUMSubscriberAccess: Email Message Queue Accessed |
| * MSExchangeUMSubscriberAccess: Email Messages Deleted |
| * MSExchangeUMSubscriberAccess: Email Messages Heard |
| * MSExchangeUMSubscriberAccess: Launched Calls (Report Collection) |
| * MSExchangeUMSubscriberAccess: Reply Messages Sent (Report Collection) |
| * MSExchangeUMSubscriberAccess: Subscriber Logon Failures |
| * MSExchangeUMSubscriberAccess: Subscriber Logons |
| * MSExchangeUMSubscriberAccess: Voice Message Queue Accessed |
| * MSExchangeUMSubscriberAccess: Voice Messages Deleted |
| * MSExchangeUMSubscriberAccess: Voice Messages Heard |
| * MSExchangeUMSubscriberAccess: Voice Messages Sent (Report Collection) |

## Synthetic Transactions

Test Cmdlets TBD

# Edge Transport Server

## Create a new Edge Subscription

By creating a new Edge subscription the Edge Transport Server is included in the Exchange organization, that is, it learns the internal topology of the organization and gets functionality enabled for filtering and securing messaging. This enables integrated and simpler management for the organization's e-mail security.

Prerequisites:

* Exchange Server 2010 SP1 has to be already installed in the server
* Hub Transport server(s) must have been deployed in the Exchange organization
* The Edge subscription will comprise one and only one Active Directory site, so a site with Hub Transport servers has to be selected in order to do this configuration.
* There can be several Edge transport servers subscribed to an Active Directory site.
* The Edge transport server and the Hub transport server must be able to locate each other by using name resolution (DNS)
* Permissions must be applied for the user to execute this procedure (Organization Management - Edge Transport Local Administrator) as described [here](http://technet.microsoft.com/en-us/library/dd638213.aspx).

From the Exchange Management Console

This procedure is not available from the Exchange Management Console

From the Exchange Management Shell

From the Edge transport server, run the following command:

New-EdgeSubscription -FileName "c:\EdgeServerSubscription.xml"

**Note**: "c:\EdgeServerSubscription.xml" is provided as an example, the filename and path can be changed to suit organization's operational standards.

Copy the resulting file (c:\EdgeServerSubscription.xml) to the Hub transport server.

From the Hub transport server, run the following command:

New-EdgeSubscription -FileData ([byte[]]$(Get-Content -Path "C:\EdgeServerSubscription.xml" -Encoding Byte -ReadCount 0)) -Site "Default-First-Site"

**Notes**:

* "c:\EdgeServerSubscription.xml" is provided as an example, the filename and path should correspond to the destination of the file copy in the previous step.
* "Default-First-Site"should be changed for the actual name of the Active Directory site containing the Hub transport used for this procedure.

References:

[New-EdgeSubscription](http://technet.microsoft.com/en-us/library/bb123800.aspx)

## Retrieve the properties of existing Edge Subscriptions

Once configured, Edge Subscriptions will keep the Edge transport servers updated with any new information about changes in the internal Exchange organization. The status of these subscriptions can be queried to get their details.

This procedure can be run in an Edge transport server or in a Hub transport server. In the Edge transport it will only retrieve the properties for the subscription configured in that server.

Prerequisites:

* Permissions must be applied for the user to execute this procedure (Organization Management - Edge Transport Local Administrator) as described [here](http://technet.microsoft.com/en-us/library/dd638213.aspx).

From the Exchange Management Console

This procedure is not available from the Exchange Management Console

From the Exchange Management Shell

From the Edge transport server, run the following command:

Get-EdgeSubscription

References:

[Get-EdgeSubscription](http://technet.microsoft.com/en-us/library/bb124801.aspx)

## Remove an Edge Subscription

By removing an Edge subscription the configuration that allows the Edge transport server to receive the configuration is dropped from the Exchange organization and from the Edge transport server. If the force parameter is not invoked, the procedure will take some time to delete the synchronized information and will allow to stop the deletion.

Prerequisites:

* The Edge subscription has to be created
* Permissions must be applied for the user to execute this procedure (Organization Management - Edge Transport Local Administrator) as described [here](http://technet.microsoft.com/en-us/library/dd638213.aspx).

From the Exchange Management Console

This procedure is not available from the Exchange Management Console

From the Exchange Management Shell

From the Edge transport server, run the following command:

Remove-EdgeSubscription -Identity Edge1

**Note**: Edge1 is provided as an example, this must be the name of the existing edge subscription that should be deleted by the operation.

As an alternative, to force the deletion of the information that has been synchronized from Active Directory the command should be run in this way:

Remove-EdgeSubscription -Identity Edge1 -Force

**Note**: Edge1 is provided as an example, this must be the name of the existing edge subscription that should be deleted by the operation.

References:

[Remove-EdgeSubscription](http://technet.microsoft.com/en-us/library/bb124807.aspx)

## Starting synchronization through an Edge Subscription

Once the Edge subscription has been created, a cmdlet can be issued to force the synchronization process to start. The options in this procedure allow to start a full or incremental synchronization, or also mark the synchronization as successful even if errors occurred.

Prerequisites:

* The Edge subscription has to be created
* Permissions must be applied for the user to execute this procedure (Organization Management - Edge Transport Local Administrator) as described [here](http://technet.microsoft.com/en-us/library/dd638213.aspx).

From the Exchange Management Console

This procedure is not available from the Exchange Management Console

From the Exchange Management Shell

From the Hub transport server, run the following command:

Start-EdgeSynchronization

References:

[Start-EdgeSynchronization](http://technet.microsoft.com/en-us/library/bb123512.aspx)

## Testing the Edge Synchronization

Two ways can be used to test the EdgeSync process, the first one will allow to check the existence of a specific user in the AD LDS information in the Edge transport server, the other way will allow to list the inconsistencies found in AD LDS that make it differ from Active Directory.

Prerequisites:

* The Edge subscription has to be created
* Permissions must be applied for the user to execute this procedure (Organization Management - Edge Transport Local Administrator) as described [here](http://technet.microsoft.com/en-us/library/dd638213.aspx).

From the Exchange Management Console

This procedure is not available from the Exchange Management Console

From the Exchange Management Shell

From the Hub transport server, run the following command to check for the existence of a user listed in AD LDS in the Edge transport server:

Test-EdgeSynchronization -VerifyRecipient adam@contoso.com

**Note**: adam@contoso.com is provided as an example, this must be the e-mail address of an existing user in the Exchange Organization who is enabled to receive mail from the Internet.

To list the inconsistencies found between AD LDS and Active Directory, execute this command

Test-EdgeSynchronization

References:

[Test-EdgeSynchronization](http://technet.microsoft.com/en-us/library/aa996925.aspx)

Test-EdgeSynchronizationTest-EdgeSynchronizationTest-EdgeSynchronization

## Creating the configuration for the EdgeSync service

The EdgeSync process can be configured to follow certain organizational guidelines. The settings defined will govern all the EdgeSync process for the full organization.

Prerequisites:

* The Edge subscription has to be created
* Permissions must be applied for the user to execute this procedure (Organization Management - Edge Transport Local Administrator) as described [here](http://technet.microsoft.com/en-us/library/dd638213.aspx).

From the Exchange Management Console

This procedure is not available from the Exchange Management Console

From the Exchange Management Shell

To create a configuration for the EdgeSync server with the following settings:

Synchronize every 15 minutes

Enable logging for the service in the UNC path [\\server01\EdgeSyncLog](file:///\\server01\EdgeSyncLog) with 5 MB log files that remain stored for 5 days

From the Hub transport server, run the following command to set the configuration for the service:

New-EdgeSyncServiceConfig -ConfigurationSyncInterval 0.0:15:0 -LogEnabled $true -LogPath "[\\Server01\EdgeSyncLog](file:///\\Server01\EdgeSyncLog)" -LogMaxFileSize 5MB -LogMaxAge 5

References:

[New-EdgeSyncServiceConfig](http://technet.microsoft.com/en-us/library/dd298058.aspx)

## Setting the configuration for the EdgeSync service

The EdgeSync process can be configured to follow certain organizational guidelines. The settings defined will govern all the EdgeSync process for the full organization. This procedure applies for a configuration that has already been created, in order to change one or some of its parameters.

Prerequisites:

* The Edge subscription has to be created
* The configuration for the EdgeSync service must have been created (through the New-EdgeSyncServiceConfig cmdlet)
* Permissions must be applied for the user to execute this procedure (Organization Management - Edge Transport Local Administrator) as described [here](http://technet.microsoft.com/en-us/library/dd638213.aspx).

From the Exchange Management Console

This procedure is not available from the Exchange Management Console

From the Exchange Management Shell

To change an existing configuration for the EdgeSync server to synchronize every 5 minutes , run the following command from the Hub transport server:

Set-EdgeSyncServiceConfig -Identity *config-name* -ConfigurationSyncInterval 0.0:5:0

Where *config-name* is a configuration that has been defined in the organization.

References:

[Set-EdgeSyncServiceConfig](http://technet.microsoft.com/en-us/library/dd335128.aspx)

## Retrieve the configurations created for the EdgeSync service

The EdgeSync process can be configured to follow certain organizational guidelines. The settings defined will govern all the EdgeSync process for the full organization. There can be several configurations stored. The present procedure allows to retrieve the configurations available and/or the settings present on them.

Prerequisites:

* Permissions must be applied for the user to execute this procedure (Organization Management - Edge Transport Local Administrator) as described [here](http://technet.microsoft.com/en-us/library/dd638213.aspx).

From the Exchange Management Console

This procedure is not available from the Exchange Management Console

From the Exchange Management Shell

To retrieve the existing configurations for the EdgeSync service, issue the following command from the Hub transport server:

Get-EdgeSyncServiceConfig

To retrieve the settings for a specific configuration created for the EdgeSync service, execute the following from the Hub transport server:

Get-EdgeSyncServiceConfig -Identity *config-name*

Where *config-name* is a configuration that has been defined in the organization.

References:

[Get-EdgeSyncServiceConfig](http://technet.microsoft.com/en-us/library/dd335074.aspx)

## 

# Public Folders

Public Folders have traditionally been popular because they allow users to store and share documents within the e-mail system, distribute organizational forms, and mail-enable folders so that messages can be delivered to them automatically. However, public folders are not a true document sharing system, since they do not provide versioning, document check-in/check-out, or other collaboration features. Today much of this functionality is provided by SharePoint, which has improved collaboration, deployment, and management capabilities. Public folders were once required for distribution of Free/Busy information and Offline Address Books, but this is no longer the case in Exchange 2010, providing all your Outlook clients are running Outlook 2007 or a later version.

Follow these best practices regarding Public Folders:

**Set Size Limits and Age Limits on Public Folder Databases**

To control the growth of your public folder databases, you should set size limits and age limits. You can use the [**Set-PublicFolderDatabase**](http://technet.microsoft.com/en-us/library/aa997225.aspx) cmdlet to set these limits using the following switches:

* **DeletedItemRetention** – This parameter specifies the time that deleted items are kept in the dumpster before being permanently deleted during store maintenance.
* **ItemRetentionPeriod** – This parameter specifies the length of time that items are retained in a folder before they're deleted during store maintenance
* **MaxItemSize** – This parameter specifies the maximum size of an item that can be posted to or received by a public folder.
* **IssueWarningQuota** – This parameter specifies the public folder size at which a warning is issued to public folder owners stating that the folder is almost full.
* **ProhibitPostQuota** – This parameter specifies the size of a public folder at which users are notified that the public folder is full. Users can't post to a folder larger than the ProhibitPostQuota parameter value.

The following example sets the deleted item retention period to 10 days, maximum item size to unlimited, and prohibit post quota to 100 megabytes for database named PFDB:

**Set-PublicFolderDatabase –Identity “PFDB” –DeletedItemRetention ’10.00:00:00’ –MaxItemSize unlimited –ProhibitPostQuota 100MB**

**Set Size and Age Limits on Individual Public Folders When Appropriate**

In some cases, you may find it necessary to set size and age limits on individual public folders that differ from the database settings. Use the [**Set-PublicFolder**](http://technet.microsoft.com/en-us/library/aa998596.aspx) cmdlet for this purpose. Many of the switches are the same as those used for Set-PublicFolderDatabase.

**Centralize Public Folder Creation**

To control growth of the public folder tree, creation of top-level public folders should be centralized and limited to a select group of administrators. Exchange Server 2010 makes this easier than ever through the use of Role-Based Access Control (RBAC), because only members of the Public Folder Management role group can create top-level public folders. Users can be granted permissions to create folders at lower levels of the tree through public folder administrative permissions or by granting the “CreateSubfolders” client permission on an individual folder. Read more about public folder permissions here: <http://technet.microsoft.com/en-us/library/ee633461.aspx>

**Use Native Exchange Scripts to Manage Public Folders**

Exchange Server 2010 provides multiple scripts that you can use to manage public folder replicas, manage user permissions, and verify public folder replication. These scripts are located in the <Exchange Installation Path>\v14\ Server\Scripts folder by default. Some examples:

|  |  |  |
| --- | --- | --- |
| Task | Script | Description |
| Aggregate data across all public folder replicas | AggregatePFData.ps1 | This script aggregates and captures information collected from the following cmdlets:   * Get-PublicFolderItemStatistics * Get-PublicFolderStatistics * Get-PublicFolder     The following information is aggregated at the public folder level, and not at the item level:   * Last user access and last user modification times * Owner of the public folder * Other properties such as MailEnabled, HasRules, ItemCount, FolderType, HasModerator, and TotalItemSize   The ItemCount and TotalItemSize properties help to verify that replication is succeeding across replicas. |
| Move all public folder replicas off one server and onto another | MoveAllReplicas.ps1 | This script replaces a server with a new server in the replication list for all public folders, including system folders. |
| Grant a user permissions to a public folder and all its subfolders | AddUsersToPFRecursive.ps1 | This script adds a user and that user's permissions to the client permissions list for a public folder and all the folders beneath it in the hierarchy. If the user is already listed in the client permissions list for a folder, the user's permissions are updated to the new set specified in the script. |

See this article for a full list of these scripts and their usage: <http://technet.microsoft.com/en-us/library/aa997966.aspx>

**Add Replicas Only for Fault Tolerance**

It is recommended to have two replicas of each public folder (each individual copy of a public folder is called a ‘replica’) to maintain availability and recovery if one public folder database should become damaged or corrupted. However, additional replicas should be added only when absolutely necessary; for example, when users in a remote site with poor network connectivity need access to folders. Keep in mind that the more replicas of a folder you add, the more disparity users on different mailbox databases will see due to replication delay.

**Perform Daily Full or Incremental Backups of Public Folder Databases**

As a best practice, Full backups should be performed on public folder databases each day. If this is not possible due to time constraints, daily Incremental backups should be taken in between the full backups. Only Full and Incremental backups cause the database’s transactions logs to be purged; Copy and Differential backups do not. Failing to perform Full or Incremental backups will cause transaction log disks to fill up because all logs are retained. Here is a summary of the four types of backups:

* **Full Backup:** A full backup is a complete backup that archives every selected database and all necessary log files. Log files older than the checkpoint at the time the backup was started are deleted after the backup completes. If you perform a full backup on a daily basis, you can prevent log files from consuming space on the hard disk.
* **Copy Backup:** A copy backup is a complete backup and is the same as a full backup except that log files are not deleted at the completion of the backup. You can perform a copy backup if you want to save a copy of your Exchange databases at a specific point in time.
* **Incremental Backup:** An incremental backup is a change-only backup that only archives the transaction log files since the last full or incremental backup. Log files older than the checkpoint are deleted after the backup is complete. You cannot perform an incremental backup when circular logging is enabled. To restore data from an incremental backup, you must have the most recent full backup and each subsequent incremental backup set available. After the restore process is complete, the transaction logs are applied to the Exchange database that you restored with the full backup.
* **Differential Backup:** A differential backup is a change-only backup that only archives the transaction log files since the last full or incremental backup. The transaction logs are not deleted. You cannot perform a differential backup when circular logging is enabled. To restore data from a differential backup, you must have the most recent full and differential backups available.

**Audit Public Folder Deletion**

Increasing the event logging level on an individual mailbox server will enable the server to record public folder deletions to the Application Log. Use this cmdlet to increase the logging level:

**Set-EventLogLevel “MSExchangeIS\9001 Public\General” –Level Medium**

This will cause event 9682 to be written to the Application Log when a folder is deleted, similar to this:

Event Type: Information

Event Source: MSExchangeIS Public Store

Event Category: General Event ID: 9682

Description: Folder */Name\_of\_Public\_Folder* with folder ID *ID\_Number* was deleted by */o=Exchange\_Organization\_Name/ou=Exchange\_Site\_Name/cn=Recipients\_Container/cn=User*, user account *Domain\NTAccount\_Name*.

**Configure a Default Public Folder Database for all Mailbox Databases**

Each mailbox database is configured with a default public folder database. MAPI client applications, such as Microsoft Outlook, open a connection to the default public folder database and perform all hierarchy-based operations against the server that contains that database. These operations include viewing public folders, creating and deleting public folders, and querying for the location of public folder content. The default public folder database can be changed via the Exchange Management Shell as follows:

**Set-MailboxDatabase -Identity "Mailbox Database" -PublicFolderDatabase "PFDB"**

**Configure Public Folder Referral Cost**

When a MAPI client attempts to access a public folder, the default public folder database for that user’s mailbox will be queried first. If that database does not contain a replica of the folder, the client is referred to another public folder server based on the connection cost of the other servers. Exchange administrators can adjust the referral cost following the instructions in this article: <http://technet.microsoft.com/en-us/library/bb629643.aspx>. **Be aware that this cost also affects e-mail routing to these public folders. To completely exclude a public folder server from being used for referrals, the preferred method of adjusting cost is to use the Set-AdSiteLink cmdlet with the –ExchangeCost switch, as described here:** <http://technet.microsoft.com/en-us/library/aa998825.aspx>.

# Appendix – Operations Checklists for Unified Messaging

The Microsoft Exchange Server 2010 Operations Checklists for Unified Messaging provide guidelines for IT professionals to perform the daily, weekly, and monthly maintenance tasks required to keep your Exchange Unified Messaging servers performing optimally. Use the following checklists as is, or adapt them to suit your company's specific needs:

* Daily Operations Checklist
* Weekly Operations Checklist
* Monthly Operations Checklist
* Summary Checklist

## Daily Operations Checklist for Unified Messaging

Use these checklists to record daily operations. You can modify these checklists based on your organization's requirements.

Prepared by:

Date:

|  |  |
| --- | --- |
| **Completed (Yes / No)** | **Task** |
|  | Verify that environmental conditions are tracked and maintained. Check of physical environment including IP Gateways/HuntGroups |
|  | Confirm inbound calls are load balanced across all UM Servers as expected |
|  | Filter application and system logs on the Exchange Unified Messaging server to see all errors. |
|  | Filter application and system logs on the Exchange Unified Messaging server to see all warnings. |
|  | Note repetitive warning and error logs. |
|  | Respond to discovered failures and problems. |
|  | Check logical environment including DialPlans and Server membership |

|  |  |  |
| --- | --- | --- |
| **Counter** | **Measured value** | **Time when recorded** |
|  |  |  |
|  |  |  |
|  |  |  |

## Weekly Operations Checklist

Use these checklists to record weekly operations. You can modify these checklists based on your organization's requirements.

Prepared by:

Date:

|  |  |
| --- | --- |
| **Completed** | **Task** |
|  | Create reports on memory and CPU usage |
|  | Generate uptime and availability reports |
|  | Create Capacity reports |
|  | List the top generated, resolved, and pending incidents |
|  | Create solutions for unresolved incidents |
|  | Update reports to include new trouble tickets |
|  | Create a document depository for troubleshooting guides and post- mortems about outages |

## Monthly Operations Checklist for Unified Messaging

Use these checklists to record monthly operations. You can modify these checklists based on your organization's requirements.

Prepared by:

Date:

|  |  |
| --- | --- |
| **Completed (Yes / No)** | **Task** |
|  | Check capacity and performance against service level agreement (SLA) requirements |
|  | Review SLA requirements and capacity figures from previous month |
|  | Maintain a list of applied hotfixes, service packs, update rollups, and security updates |
|  | See if there are new hotfixes for Microsoft Windows Server |
|  | See if there are service packs for Windows Server |
|  | See if there are updates to complementary services such as Internet Information Services (IIS), Active Directory directory service, and DNS server |
|  | Apply updates uniformly across servers and workstations in the organization. |
|  | Perform critical security updates as soon as possible, based on policy. |

# Appendix - Operations Checklists

The Exchange 2010 Operations Checklists provide guidelines for IT professionals to perform the daily, weekly, and monthly maintenance tasks required to keep your Exchange servers performing optimally. Use the following checklists as is, or adapt them to suit your company's specific needs:

* Daily Operations Checklist
* Weekly Operations Checklist
* Monthly Operations Checklist
* Summary Checklist

## Daily Operations Checklist

Use these checklists to record daily operations. You can modify these checklists based on your organization's requirements.

Prepared by:

Date:

|  |  |
| --- | --- |
| **Completed (Yes / No)** | **Task** |
|  | Verify that environmental conditions are tracked and maintained. |
|  | Check temperature and humidity to ensure that environmental systems such as heating and air conditioning settings are within acceptable conditions, and that they function within the hardware manufacturer's specifications. |
|  | Ensure that your physical network and related hardware such as routers, switches, hubs, physical cables, and connectors are operational. |
|  | Verify that the previous backup operation completed. |
|  | Analyse and respond to errors and warnings during the backup operation. |
|  | Follow the established procedure for tape rotation, labelling, and storage. |
|  | Verify that the transaction logs were successfully purged (if your backup type is purging logs). |
|  | Examine **% Processor Time** performance counter. |
|  | Examine **Available MBs** performance counter. |
|  | Examine **% Committed Bytes** in Use performance counter. |
|  | Check against a performance baseline to determine the health of a server. |
|  | Create a list of all drives and label them in three categories: drives with transaction logs, drives with queues, and other drives. |
|  | Check disks with transaction log files. |
|  | Check disks with SMTP queues. |
|  | Check other disks. |
|  | Use server monitors to check free disk space. |
|  | Check performance on disks. |
|  | Filter application and system logs on the Exchange server to see all errors. |
|  | Filter application and system logs on the Exchange server to see all warnings. |
|  | Note repetitive warning and error logs. |
|  | Respond to discovered failures and problems. |
|  | Check the number of transaction logs generated since the last check. Is the number increasing at the “usual” rate? |
|  | Verify that databases are mounted. |
|  | If full-text indexing is enabled, verify that indexes are up-to-date. |
|  | Verify your Perfmon RPC counters against a baseline - RPC average latency/RPC requests/RPC operations. |
|  | Check queues using the Queue Viewer tool in the Exchange Management Console. |
|  | Record queue size. |

|  |  |  |
| --- | --- | --- |
| **Counter** | **Measured value** | **Time when recorded** |
| % Processor Time |  |  |
| Available MBs |  |  |
| % Committed Bytes in Use |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Drive Letter or Mount point** | **Description** | **Available space MB** | **Available % free** |
| *H:* | H: |  |  |

***DAG configuration***:

|  |  |  |  |
| --- | --- | --- | --- |
| Mount point | LUN | Available space MB | Available % free |
| E:\ExchData\DB01 | DB01 |  |  |
| E:\ExchData\DR01 | DR01 |  |  |

***Standalone configuration***:

|  |  |  |  |
| --- | --- | --- | --- |
| Mount point | LUN name | Available space MB | Available % free |
| E:\ExchData\DB01 | DB01 |  |  |
| E:\ExchData\DB02 | DB02 |  |  |
| E:\ExchData\DR01 | DR01 |  |  |
| E:\ExchData\DR02 | DR02 |  |  |
| E:\ExchData\Log01 | Log01 |  |  |
| E:\ExchData\Log02 | Log02 |  |  |
| E:\ExchData\Log01 | DRLog01 |  |  |
| E:\ExchData\Log02 | DRLog02 |  |  |

## Weekly Operations Checklist

Use these checklists to record weekly operations. You can modify these checklists based on your organization's requirements.

Prepared by:

Date:

|  |  |
| --- | --- |
| **Completed** | **Task** |
|  | Report on disk usage. |
|  | Create reports on memory and CPU usage. |
|  | Generate uptime and availability reports. |
|  | Generate database and mailbox sizes. |
|  | Create Capacity reports from messages sent and client logons. |
|  | Create reports on queue use, size, and growth. |
|  | List the top generated, resolved, and pending incidents. |
|  | Create solutions for unresolved incidents. |
|  | Update reports to include new trouble tickets. |
|  | Create a document depository for troubleshooting guides and post- mortems about outages. |
|  | Perform a virus scan on the Server; however, exclude drives that are specifically for Exchange (SMTP/Exchange Databases/Logs, and so on). |

## Monthly Operations Checklist

Use these checklists to record monthly operations. You can modify these checklists based on your organization's requirements.

Prepared by:

Date:

|  |  |
| --- | --- |
| **Completed (Yes / No)** | **Task** |
|  | Check capacity and performance against service level agreement (SLA) requirements. |
|  | Review SLA requirements and capacity figures from previous month. |
|  | Produce and implement upgrade path based on projected growth from previous growth data. |
|  | Maintain a list of applied hotfixes, service packs, update rollups, and security updates. |
|  | See if there are new hotfixes for Microsoft Windows Server. |
|  | See if there are service packs for Windows Server. |
|  | See if there are updates to complementary services such as Internet Information Services (IIS), Active Directory directory service, and DNS server. |
|  | Apply updates uniformly across servers and workstations in the organization. |
|  | Perform critical security updates as soon as possible, based on CGGVeritas’s policy. |

## Summary Checklist

This checklist provides you with a summary of Exchange 2010 operations tasks on a daily, weekly, and monthly basis. You can modify these checklists based on your organization's requirements.

Prepared by:

Date:

|  |  |
| --- | --- |
| **Completed (Yes / No)** | **Daily** |
|  | Check of physical environment. |
|  | Check backups. |
|  | Check CPU/memory use. |
|  | Check disk use. |
|  | Examine message queues. |
|  | Examine event logs. |
|  | Check backups. |
|  | Check Exchange Server database health. |
|  | Check MAPI client performance. |
|  | Check Hub Transport Dumpster |
|  | Check Queue Viewer. |
|  | Check message paths and mail flow. |
|  | Check security logs. |
|  | Update virus definitions and scan for viruses. |

## Exchange permissions

Based on the Exchange roles, here are the reference links about the permissions:

* Mail Box: <http://technet.microsoft.com/en-us/library/dd638213.aspx>
* CAS: <http://technet.microsoft.com/en-us/library/dd638131.aspx>
* HUB: <http://technet.microsoft.com/en-us/library/dd638213.aspx>
* DAG: <http://technet.microsoft.com/en-us/library/dd638136.aspx>

The following sections provide the required permissions depending if the feature that needed for the Exchange 2010 administrator.

### Mailbox Permission

|  |  |
| --- | --- |
| **Feature** | **Permissions required** |
| **Calendar repair, server configuration** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx), [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Delegating Mailbox servers** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **E-mail address policies** | [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx), [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Exchange Search** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [View-Only Organization Management](http://technet.microsoft.com/en-us/library/dd351130.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Mailbox moves** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Mailbox recovery** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Mailbox repair request** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Mailbox restore request** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Mailbox server configuration** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **MAPI connectivity** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **OAB virtual directories** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Remove store mailbox** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |

### Calendar and Sharing Permissions

|  |  |
| --- | --- |
| **Feature** | **Permissions required** |
| **Calendar configuration** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Notifications** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Organization relationships** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |

### Resource Mailbox Configuration Permissions

|  |  |
| --- | --- |
| **Feature** | **Permissions required** |
| **Booking policies** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx)  [Help Desk](http://technet.microsoft.com/en-us/library/dd876949.aspx) |
| **Delegation** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Resource mailbox schema configuration** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |

### Address List Permissions

|  |  |
| --- | --- |
| **Feature** | **Permissions required** |
| **Address list paging** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Address lists** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Details templates** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **File distribution service** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Global address lists** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Offline address books** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |

### Mailbox Database Permissions

|  |  |
| --- | --- |
| **Feature** | **Permissions required** |
| **Mailbox databases** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx), [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |

### Recipient Provisioning Permissions

|  |  |
| --- | --- |
| **Feature** | **Permissions required** |
| **Address list, GAL** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Anti-spam** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx),  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Arbitration** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Applying sharing policies** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Assigning offline address books** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Automatic replies** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx)  [Help Desk](http://technet.microsoft.com/en-us/library/dd876949.aspx) |
| **Calendar configuration** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Calendar repair** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Distribution groups** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Dynamic distribution groups** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **E-mail addresses** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Inbox rules** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx)  [Help Desk](http://technet.microsoft.com/en-us/library/dd876949.aspx) |
| **Mail contacts** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Mail tips** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Mail user** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Mailbox folder permissions** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx)  [Help Desk](http://technet.microsoft.com/en-us/library/dd876949.aspx) |
|  |  |
| **Mailbox folders** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Message configuration** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx)  [Help Desk](http://technet.microsoft.com/en-us/library/dd876949.aspx) |
| **Message quotas** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Moderation** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Permissions and delegation** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Personal archives** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Recipient data properties** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Remote mailboxes** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Retention and legal holds** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx)  [Records Management](http://technet.microsoft.com/en-us/library/dd633492.aspx) |
| **Send As** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Spelling configuration** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx)  [Help Desk](http://technet.microsoft.com/en-us/library/dd876949.aspx) |
| **User mailboxes** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |

<http://technet.microsoft.com/en-us/library/dd638132.aspx>

### Transport Permissions

|  |  |
| --- | --- |
| **Feature** | **Permissions required** |
| **Accepted domains** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Active Directory site and site link management** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Anti-spam features** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Hygiene Management](http://technet.microsoft.com/en-us/library/dd776125.aspx) |
| **Certificate management** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Delivery Agent connectors** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Foreign connectors** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Hub Transport server** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Journaling** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Records Management](http://technet.microsoft.com/en-us/library/dd633492.aspx) |
| **Mailbox junk e-mail configuration** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Records Management](http://technet.microsoft.com/en-us/library/dd633492.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx)  [Help Desk](http://technet.microsoft.com/en-us/library/dd876949.aspx) |
| **Message tracking** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Records Management](http://technet.microsoft.com/en-us/library/dd633492.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |
| **Queues** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Receive connectors** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx)  [Hygiene Management](http://technet.microsoft.com/en-us/library/dd776125.aspx) |
| **Send connectors** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Shadow redundancy** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Testing mail flow** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Testing Transport rule processing** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Transport agents** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Records Management](http://technet.microsoft.com/en-us/library/dd633492.aspx) |
| **Transport configuration** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Transport logs** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Records Management](http://technet.microsoft.com/en-us/library/dd633492.aspx) |

### Client Access Server Permissions

|  |  |
| --- | --- |
| **Feature** | **Permissions required** |
| **Client Access server settings** | [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Client Access server security settings** | [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Client Access server management settings** | [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Client Access server user settings** | [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Client Access server array settings** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Client Access user settings** | [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **RPC Client Access settings** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx)  [View-Only Organization Management](http://technet.microsoft.com/en-us/library/dd351130.aspx) |
| **Client Access service e-mail channel settings** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Reset Client Access virtual directories** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |

### Exchange ActiveSync Permissions

|  |  |
| --- | --- |
| **Feature** | **Permissions required** |
| **Exchange ActiveSync settings Exchange ActiveSync virtual directory settings Exchange ActiveSync mailbox policy settings Exchange ActiveSync server settings Exchange ActiveSync security settings** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Exchange ActiveSync user settings Exchange ActiveSync device settings** | [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx) |

### Exchange Web services permissions

|  |  |
| --- | --- |
| **Feature** | **Permissions required** |
| **Test Outlook Web Services Exchange Web Services virtual directory settings** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx) |
| **Test Exchange Web Services** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |

### Outlook Web App Permissions

|  |  |
| --- | --- |
| **Feature** | **Permissions required** |
| **Outlook Web App virtual directories** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **Outlook Web App mailbox policies** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx) |
| **View Outlook Web App virtual directories** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx)  [View-Only Organization Management](http://technet.microsoft.com/en-us/library/dd351130.aspx)  [Delegated Setup](http://technet.microsoft.com/en-us/library/dd876881.aspx)  [Hygiene Management](http://technet.microsoft.com/en-us/library/dd776125.aspx) |
| **View Outlook Web App mailbox policies** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Recipient Management](http://technet.microsoft.com/en-us/library/dd298028.aspx)  [View-Only Organization Management](http://technet.microsoft.com/en-us/library/dd351130.aspx)  [Delegated Setup](http://technet.microsoft.com/en-us/library/dd876881.aspx)  [Hygiene Management](http://technet.microsoft.com/en-us/library/dd776125.aspx) |
| **Test Outlook Web App connectivity** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Server Management](http://technet.microsoft.com/en-us/library/dd876866.aspx)  [View-Only Organization Management](http://technet.microsoft.com/en-us/library/dd351130.aspx) |

### Database Availability Group Permissions

|  |  |
| --- | --- |
| **Feature** | **Permissions required** |
| **Database availability group membership** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Database Availability Groups Role](http://technet.microsoft.com/en-us/library/dd876847.aspx) |
| **Database availability group properties** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Database Availability Groups Role](http://technet.microsoft.com/en-us/library/dd876847.aspx) |
| **Database availability groups** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Database Availability Groups Role](http://technet.microsoft.com/en-us/library/dd876847.aspx) |
| **Database availability networks** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Database Availability Groups Role](http://technet.microsoft.com/en-us/library/dd876847.aspx) |

### Mailbox Database Copy Permissions

|  |  |
| --- | --- |
| **Feature** | **Permissions required** |
| **Database switchover** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Database Copies Role](http://technet.microsoft.com/en-us/library/dd876905.aspx) |
| **Mailbox database copies** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Database Copies Role](http://technet.microsoft.com/en-us/library/dd876905.aspx) |
| **Server switchover** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Database Copies Role](http://technet.microsoft.com/en-us/library/dd876905.aspx) |
| **Update a mailbox database copy** | [Organization Management](http://technet.microsoft.com/en-us/library/dd335087.aspx)  [Database Copies Role](http://technet.microsoft.com/en-us/library/dd876905.aspx) |

### Operation Powershell Scripts

[TechNet Script Center Repository - Exchange 2010](http://gallery.technet.microsoft.com/scriptcenter/site/search?f%5B0%5D.Type=RootCategory&f%5B0%5D.Value=Exchange&f%5B0%5D.Text=Exchange&f%5B1%5D.Type=SubCategory&f%5B1%5D.Value=exchange2010&f%5B1%5D.Text=Exchange%202010)

An Exchange Management Shell is a powerful management interface, built on Microsoft Windows PowerShell technology. You can use the Exchange Management Shell to perform every task available in the Exchange Management Console and tasks that you can't perform in the Exchange Management Console. What's more, when you perform a task in the Exchange Management Console, the same command is made available to the Exchange Management Shell and called to process the request.

At first glance, the shell may look daunting to those unfamiliar with the command line. But let's take a look at the cool stuff you can do and how easy it is to get started:

* **Scripting made safe and easy:** The Exchange Management Console doesn’t simply use the Exchange Management Shell to perform operations. The wizards show you the Exchange Management Shell commands they're performing. You can copy the commands that the wizards create and paste them directly onto the command line or into a script. After you've modified the parameters to your liking, test your scripts or commands by using the WhatIf parameter, which lets you see the results before you make any changes to your environment.   
  Modify parameters? WhatIf? Sounds complicated? Not to worry! Check out the "[Using the Exchange Management Shell](http://technet.microsoft.com/en-us/library/bb123778.aspx)" section in the [Microsoft Exchange Server 2010](http://technet.microsoft.com/en-us/library/bb124558.aspx) documentation. You'll be up and running in no time.
* **Clear and simple:** we’ve used consistent verb-noun pairs to clearly identify the feature or component being managed, and the action that's being taken. You don't have to guess what a cmdlet does anymore. When you see the **Move-Mailbox** cmdlet, you know exactly what it’s used for. (Yep, that's right. You use it to move mailboxes!)
* **Maximize your resources and time, not your frustration:** The Exchange Management Shell gives you a robust and flexible scripting platform to integrate with your current scripting solutions, and it lets you communicate natively with data sources like COM and Windows Management Instrumentation (WMI). Use your resources and time wisely to create useful solutions instead of creating the framework to support them.
* **Repeat after me: No more text parsing!** Based on Microsoft .NET, the Exchange Management Shell cmdlets accept and return structured data instead of plain text. In this way, you can easily pass data back and forth without messy text parsing. You can even turn CSV and XML files into objects that you can manipulate and consume in a single line.

**PowerShell Scripts in Exchange Server 2010**

By default, there are 66 in-built PowerShell scripts on Exchange 2010 Server and the scripts are located at “C:\Program Files\Microsoft\Exchange Server\V14\Scripts” folder.

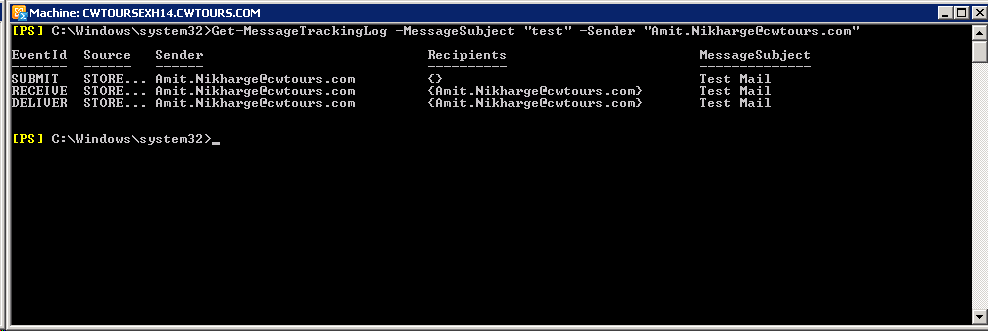
These scripts can be used for operational tasks and automate them.

**Below is the list of available PowerShell scripts in Exchange Server 2010.**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | **Name** | | AddReplicaToPFRecursive.ps1 | | AddUsersToPFRecursive.ps1 | | AggregatePFData.ps1 | | AntispamCommon.ps1 | | CheckDatabaseRedundancy.ps1 | | CheckInvalidRecipients.ps1 | | CITSConstants.ps1 | | CITSLibrary.ps1 | | CITSTypes.ps1 | | CollectOverMetrics.ps1 | | CollectReplicationMetrics.ps1 | | configure-SMBIPsec.ps1 | | ConfigureAdam.ps1 | | ConfigureNetworkProtocolParameters.ps1 | | ConvertTo-MessageLatency.ps1 | | DagCommonLibrary.ps1 | | DiagnosticScriptCommonLibrary.ps1 | | Disable-InMemoryTracing.ps1 | | enable-CrossForestConnector.ps1 | | Enable-InMemoryTracing.ps1 | | enable-OutlookCertificateAuthentication.ps1 | | ExchUCUtil.ps1 | | Export-OutlookClassification.ps1 | | Export-RetentionTags.ps1 | | get-AntispamFilteringReport.ps1 | | get-AntispamSCLHistogram.ps1 | | get-AntispamTopBlockedSenderDomains.ps1 | | get-AntispamTopBlockedSenderIPs.ps1 | | get-AntispamTopBlockedSenders.ps1 | | get-AntispamTopRBLProviders.ps1 | | get-AntispamTopRecipients.ps1 | | get-setuplog.ps1 | | Get-UCPool.ps1 | | GetDatabaseForSearchIndex.ps1 | | GetSearchIndexForDatabase.ps1 | | Import-RetentionTags.ps1 | | install-AntispamAgents.ps1 | | MailboxDatabaseReseedUsingSpares.ps1 | | ManageScheduledTask.ps1 | | MigrateUMCustomPrompts.ps1 | | Move-TransportDatabase.ps1 | | MoveAllReplicas.ps1 | | MoveMailbox.ps1 | | new-TestCasConnectivityUser.ps1 | | Prepare-MoveRequest.ps1 | | RedistributeActiveDatabases.ps1 | | ReinstallDefaultTransportAgents.ps1 | | RemoveReplicaFromPFRecursive.ps1 | | RemoveUserFromPFRecursive.ps1 | | ReplaceReplicaOnPFRecursive.ps1 | | ReplaceUserPermissionOnPFRecursive.ps1 | | ReplaceUserWithUserOnPFRecursive.ps1 | | Reset-AntispamUpdates.ps1 | | ResetAttachmentFilterEntry.ps1 | | ResetCasService.ps1 | | ResetSearchIndex.ps1 | | ResumeMailboxDatabaseCopy.ps1 | | RollAlternateServiceAccountPassword.ps1 | | StartDagServerMaintenance.ps1 | | StopDagServerMaintenance.ps1 | | StoreTSConstants.ps1 | | StoreTSLibrary.ps1 | | Troubleshoot-CI.ps1 | | Troubleshoot-DatabaseLatency.ps1 | | Troubleshoot-DatabaseSpace.ps1 | | uninstall-AntispamAgents.ps1 | |
|  |
|  |
|  |
|  |
| [**A Few Basic Concepts**](javascript:void(0)) |
| Before you get started with the Exchange Management Shell, it's helpful to understand a few basic concepts.   * **The underlying Windows PowerShell technology** The Windows PowerShell is a new, powerful, and extremely flexible command line interface that’s based on the .NET Framework. It combines the best of several shells, plus some great new features. PowerShell is designed to host other applications, just as the Microsoft Management Console (MMC) acts as a host for the various snap-INS that are provided with applications that are installed on a computer. The Exchange Management Shell is the first Microsoft PowerShell snap-in to be released. * **Cmdlets** A cmdlet, pronounced "command-let", is the smallest unit of functionality in the Exchange Management Shell. Cmdlets resemble built-in commands in other shells, for example, the **Dir** command found in cmd.exe. Like these familiar commands, cmdlets can be called directly from the command line in the Exchange Management Shell and run under the context of the shell, not as a separate process. Unlike in other shells, in the Exchange Management Shell, cmdlets have descriptive verb-noun names. The verb describes the action the cmdlet takes, and the noun describes the component or feature that is acted upon. For example, you use the **New-SystemMessage** cmdlet to create new delivery status notification (DSN) or quota messages on computers that have the Hub Transport server role installed.  For more information about specific cmdlets, see the "[Exchange Management Shell](http://technet.microsoft.com/en-us/library/bb123778.aspx)" section in Exchange 2010 Help's Technical Reference node. * **Identity and positional parameters** Parameters are elements that provide information to the cmdlet, either identifying an object and its attributes to act upon, or controlling how the cmdlet performs its task. You can use the Identity parameter with most Exchange cmdlets. The Identity parameter gives you access to the unique identifiers that refer to a particular object in Exchange 2010. This lets you perform actions on a specific Exchange object using the unique value that makes most sense to you.  The Identity parameter is a collection of values from other parameters. These values are guaranteed to be unique across that set of objects. You can specify the values of these other parameters, such as Name and DistinguishedName, or the values can be system-generated, such as a GUID. The additional parameters that are used, if any, and how they are populated, depend on the object you refer to. The Identity parameter is also considered a positional parameter. A positional parameter is a parameter that lets you specify the parameter's value without specifying the parameter's name. A parameter is a positional parameter if the Parameter Position attribute is an integer. This integer indicates the position on the command line where the cmdlet can find the parameter's value. Because Identity is a positional parameter that resides in position 1, which is the first position, any value entered in this position without a parameter name is considered to be an Identity parameter value.  And what does this mean? Well, it reduces the number of keystrokes when you type commands. For example, Get-Mailbox "Kim Akers" performs the same action as Get-Mailbox -Identity "Kim Akers". * **Pipelining** In the Exchange Management Shell, pipelining refers to the act of one cmdlet using the output of another cmdlet when it performs an operation. You can use pipelining to string together two or more cmdlets. That means you can take smaller components and convert them into something more powerful. For example, you can use one cmdlet to gather data, pass that data to a second cmdlet to filter the data to a subset, and then pass that data to a third cmdlet to act on the subset only, as in the following example which moves all the mailboxes in the Sales database to the Research database on the same server:     Get-MailboxDatabase Sales | Get-Mailbox | Move-Mailbox -TargetDatabase Research  See how the pipe "|" symbol is used? First, the Sales mailbox database is retrieved by using the **Get-MailboxDatabase** cmdlet and the resulting object is piped to the **Get-Mailbox** cmdlet. Then, all the mailboxes in the Sales database are retrieved by the **Get-Mailbox** cmdlet. The resulting set of mailboxes is then piped to the **Move-Mailbox** cmdlet, which moves the mailboxes to the Research mailbox database. This command is shown in Figure 1 earlier in this article. All verbs in the same noun-cmdlet set can use piped information from another command. Some noun-cmdlet sets also let you pass data through the pipeline to another noun cmdlet set. "Noun cmdlet set"? What's that? All Exchange Management Shell cmdlets that manage a particular feature share the same noun, such as **Mailbox** or **AddressList**. For a list of all cmdlets arranged by noun, see [Cmdlet List](http://technet.microsoft.com/en-us/library/bb124413.aspx).  [**Starting the Exchange Management Shell**](javascript:void(0)) |
|  |
| Windows PowerShell snap-ins are collections of cmdlets used to administer an application or major component. If you don’t load the snap-in for the specific application, you can’t use its associated cmdlets.  What does that mean to you? If you start PowerShell without loading the Exchange Management Shell snap-in, and try to issue an Exchange Management Shell cmdlet, such as **Get-Mailbox**, you’ll get an error. Why? Because the **Get-Mailbox** cmdlet doesn’t exist in the core set of PowerShell cmdlets.  So first things first: Let's open the Exchange Management Shell. Simply click **Start**, click **Programs**, **Microsoft Exchange Server 2010**, and then **Exchange Management Shell**.  [**Getting Help Where and When You Need It**](javascript:void(0)) |
|  |
| In the shell itself, use the **Get-Help** cmdlet to access cmdlet-specific help in a variety of formats. Typing **Get-Help** by itself displays general help information. And the **Get-Help** cmdlet is even more powerful when you start supplying parameters.  To get help for a specific cmdlet, type **Get-Help** followed by the cmdlet you want information about, such as **Get-Help Get-SystemMessage**. By default, the shell displays a description of the cmdlet and its syntax. It suppresses other sections that may not be used by all administrators.  You can control what information is presented to you by using the *Detailed*, *Full*, and *Example* parameters. Just add them to the end of the command. For example, **Get-Help –Full** returns all the help sections available for a cmdlet. Try the commands out for yourself to see what information is displayed for your favorite cmdlets.  If you want to retrieve information about a specific parameter or parameters on a cmdlet, you can use the *Parameters* parameter with the **Get-Help** cmdlet. For example, if you want to view all the parameters and their descriptions on the **Set-Mailbox** cmdlet that contain the word “quota”, type **Get-Help Set-Mailbox –Parameter \*quota\***.  Or maybe you want to view a list of cmdlets that manage a specific server role or component feature or that affect objects across a certain scope of functionality. You can do this by using the **Get-Help** cmdlet and three parameters: *Role*, *Component*, and *Functionality*. When you use the **Get-Help** cmdlet with these parameters, remember to enclose the values that you specify with these parameters in wildcard characters (\*). The following are examples of how to call **Get-Help** with each parameter:   * **Get-Help -Role \*Mailbox\*** * **Get-Help -Component \*Recipient\*** * **Get-Help -Functionality \*Server\*** |
|  |
|  |
| [**Formatting Command Output**](javascript:void(0))  By default, when command output is displayed to the screen, the Exchange Management Shell displays only a subset of the available properties for each object. Why? Because each object can contain dozens of properties, and you'll want to optimize the command output for your needs. You can easily access and view all these properties by piping the output of a command to the following three formatting cmdlets: **Format-List**, **Format-Table**, and **Format-Wide**.  **Format-List** and **Format-Table** are most frequently used so let's look at them more closely.  The **Format-List** cmdlet takes input from the pipeline and outputs a vertical columned list of all the specified properties of each object. You can specify which properties you want to display by using the *Property* parameter, which is a positional parameter. If you call the **Format-List** cmdlet without any parameters specified, all properties are output. The **Format-List** cmdlet wraps lines instead of truncating them. One of the best uses for the **Format-List** cmdlet is to override the default output of a cmdlet so that you can retrieve additional or more focused information, as in this example, Get-DistributionGroup | Format-List Name, \*OnlyFrom, PrimarySmtpAddress, \*Size\*. Figure 2 shows the output of this command.  **Figure 1 Format-List example output**  The **Format-Table** cmdlet lets you display items in a table format with labeled headers and columns of property data. By default, many cmdlets, such as the **Get-Mailbox** and **Get-JournalRule** cmdlets, use the table format for output. Among the parameters for the **Format-Table** cmdlet are the *Properties* and *GroupBy* parameters. These work exactly as they do with the **Format-List** cmdlet. To display long lines of property information completely instead of truncating at the end of a line, use the *Wrap* parameter with the **Format-Table** cmdlet, as in the following example: Get-Mailbox -Database Research | Format-Table Name, ProhibitSendQuota, Database -Wrap. Figure 3 shows the output of this command.  **Figure 2 Format-Table example output**  You can also specify a wildcard character "\*" with a partial property name with both the **Format-List** and **Format-Table** Cmdlets, as I showed in Figure 2. If you include a wildcard character, you can match multiple properties without having to type each property name individually. For example, Get-Mailbox | Format-List -Property Email\* returns all properties that begin with Email. Less typing and more time to play with Exchange 2010! |
| **Connect Remote Exchange Management Shell to an Exchange Server** |
| Using the remote Shell, you can connect to a remote server running Microsoft Exchange Server 2010 to perform administration without the need to have any Exchange administration tools installed on your local computer. The remote Shell uses Windows PowerShell 2.0 and Windows Remote Management (WinRM) 2.0 to enable you to connect to remote Exchange 2010 servers.  After you connect the remote Shell to an Exchange server, the Exchange 2010 cmdlets that you have access to are made available to you in your local PowerShell session. When you run a cmdlet on your computer, the requests are sent to the remote Exchange 2010 server. The remote Exchange 2010 server then returns the results, if any, to your computer. Use the **Get-Help** cmdlet to access Help for individual cmdlets.  For more information about the remote Shell, see [Create a Manual Remote Shell Connection](http://technet.microsoft.com/en-us/library/dd335083.aspx).  **Enable Remote Exchange Management Shell for a User**  Remote Shell in Microsoft Exchange Server 2010 enables you to manage your server running Exchange 2010 from a remote computer, either on your network or from the Internet. A user must be enabled for remote Shell before the user can use it. For more information about remote Shell, see [Overview of Exchange Management Shell](http://technet.microsoft.com/en-us/library/dd297939.aspx).  Looking for other management tasks related to remote Shell? Check out [Managing Exchange Management Shell Connections](http://technet.microsoft.com/en-us/library/dd638078.aspx). |
|  |
|  |
| **Use the Shell to enable remote Shell for a user**  You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Remote Shell" entry in the [Exchange and Shell Infrastructure Permissions](http://technet.microsoft.com/en-us/library/dd638114.aspx) topic.   |  | | --- | | **Description: http://i.technet.microsoft.com/Dd298084.note(en-us,EXCHG.141).gifNote:** | | **You can't use the EMC to enable remote Shell for a user.** |   To enable remote Shell for a user, set the RemotePowerShellEnabled parameter to $True on the **Set-User** cmdlet. This example enables remote Shell for the user David.  [Copy Code](javascript:CopyCode('ctl00_MTCS_main_ctl16_ctl00_ctl02_code');)  Set-User David -RemotePowerShellEnabled $True  For detailed syntax and parameter information, see [Set-User](http://technet.microsoft.com/en-us/library/aa998221.aspx).  **Exporting Mailbox properties** |
| Many times we face situations where we have to pull multiple reports from Exchange Server. These reports can be related to Exchange Server, Mailbox users, Group Memberships, Mailbox Settings etc.  Below are some examples of PowerShell scripts that can be used to perform operational tasks. |
| **Figure 3 “Get-Mailbox” example output**    This command will show you the list of all mailboxes in your organization.  **Figure 4 “Get-Mailbox” example output**    **Figure 5 “Get-Mailbox –Server” example output**    This command will pull the list of mailbox specific to the specified Exchange Server.  **Figure 6 “Get-Mailbox –Server” example output** |
|  |
|  |
| By default, when command output is displayed to the screen, the Exchange Management Shell displays only a subset of the available properties for each object. Why? Because each object can contain dozens of properties, and you'll want to optimize the command output for your needs. You can easily access and view all these properties by piping the output of a command to the following three formatting cmdlets: **Format-List**, **Format-Table**, and **Format-Wide**.  For Example   1. If you want to pull specific information of mailboxes like Name, Alias, ServerName, OrganizationalUnit and EmailAddresses. You can pipe the above command with “Select option” for e.g.   Get-Mailbox | Select Name, Alias, ServerName, OrganizationalUnit, EmailAddresses  **Figure 7 “Get-Mailbox –Server” example output**    You can also pipe the above command with Format-Table to get output in vertical format.  Get-Mailbox | Select Name, Alias, ServerName, OrganizationalUnit, EmailAddresses | FT  **Figure 8 “Get-Mailbox –Server” example output**    **Archive Mailbox**  This example returns information about the mailboxes with Archive Enabled.  Get-Mailbox –Archive  **Figure 9 “Get-Mailbox –Archive”**    **Distribution List**  You can use Exchange PowerShell to list all distribution groups in the organization using **Get-DistributionGroup** .  **Figure 10 “Get-DistributionGroup”**    **Figure 11“Get-DistributionGroup”**    You can also use Exchange PowerShell to list the group membership.  **Figure 12 “Get-DistributionGroupMember”**    **Exporting list of user mailbox size using Exchange PowerShell.**  It is a day-to-day operation task of Exchange Administrator to keep an eye on the growing mailbox size of the Exchange users. In Exchange 2010 you can export list of mailboxes with the size using below command.  We can use the [Get-MailboxStatistics cmdlet](http://technet.microsoft.com/en-us/library/bb124612(EXCHG.80).aspx) to get the mailbox size.  Get-MailboxStatistics -Identity "nirajan"  **Figure 13 “Get-MailboxStatistics”**    This shows the DisplayName, ItemCount, StorageLimitStatus, and LastLogonTime fields for the specified user.  We can pipe the above command with additional commands to show specific fields.  >Get-MailboxStatistics -Identity "nirajan" | Select DisplayName, TotalitemSize, Itemcount  **Figure 14 “Get-MailboxStatistics”** |
|  |
|  |
| This can be done for all users in the organization or on a mailbox server using a single command  **Figure 14 “Get-MailboxStatistics”** |
| To auto size the columns, we can use “-autosize” switch.  Get-MailboxStatistics -Server "cwtoursexh14" | Select DisplayName, TotalitemSize, Itemcount | F  T –AutoSize  **Figure 15 “Get-MailboxStatistics”** |
| **Message Tracking using Exchange PowerShell.** |
| In Exchange Server 2010, we can use Exchange Message Tracking tool from Exchange Management console.  However you can also use Exchange PowerShell to track the messages using Get-Messagetrackinglog command.  Below is the example of tracking messages using Exchange PowerShell.  This example uses the **Get-MessageTrackingLog** command to retrieve message tracking log entries that were created on Exchange Server 2010.  **Figure 16 “Get-MessageTrackingLog”**    **Filtering Message Tracking Logs**  This example uses the **Get-MessageTrackingLog** command to retrieve message tracking log entries that were created for Message Subject “Test” with a Sender parameter value of Amit.Nikharge@cwtours.com. |

Get-MessageTrackingLog -MessageSubject "test" -Sender [Amit.Nikharge@cwtours.com](mailto:Amit.Nikharge@cwtours.com)

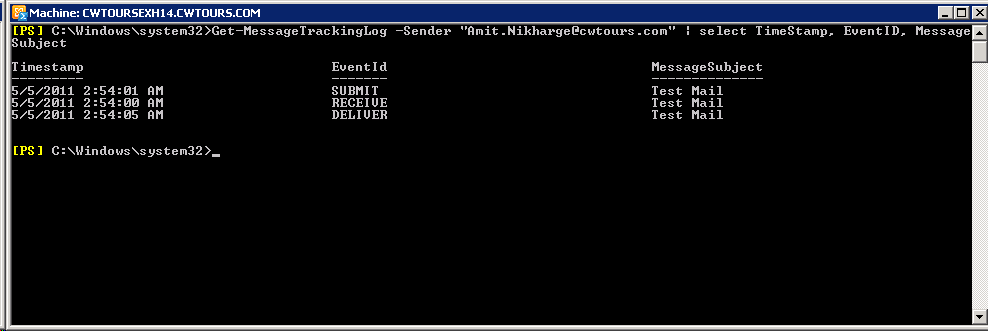
**Figure 17 “Get-MessageTrackingLog”**



**The default 'Get-MessageTrackinglog' PowerShell command can be piped to have the date and time included in the output.**

**Get-MessageTrackingLog -Sender "Amit.Nikharge@cwtours.com" | select TimeStamp, EventID, MessageSubject**

**Figure 18 “Get-MessageTrackingLog”**



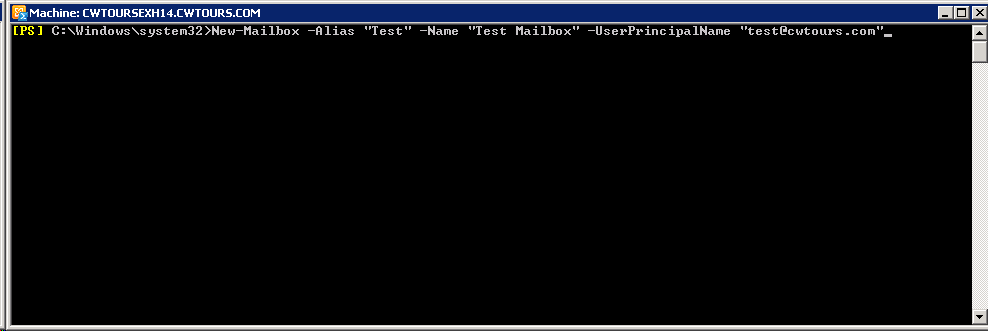
Creating Mailboxes using Exchange PowerShell.

We can use Exchange Management Console to create the mailboxes; however we can also use Exchange Power Shell to create Mailboxe.

Below is the command to create a single mailbox using Exchange PowerShell

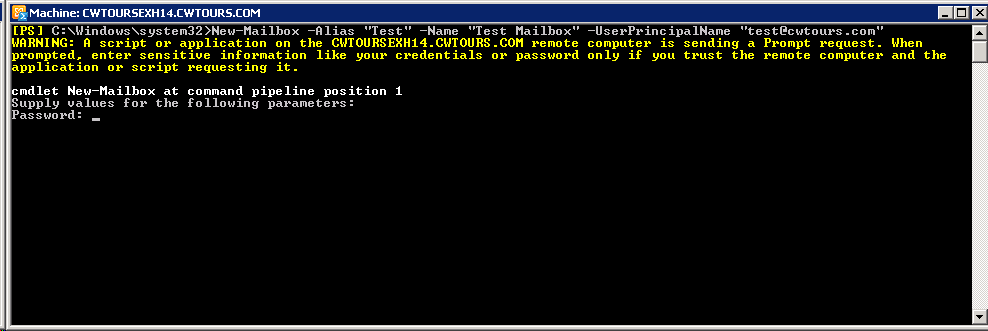
New-Mailbox -Alias "Test" -Name "Test Mailbox" -UserPrincipalName [test@cwtours.com](mailto:test@cwtours.com)

**Figure 19 “New-Mailbox”**



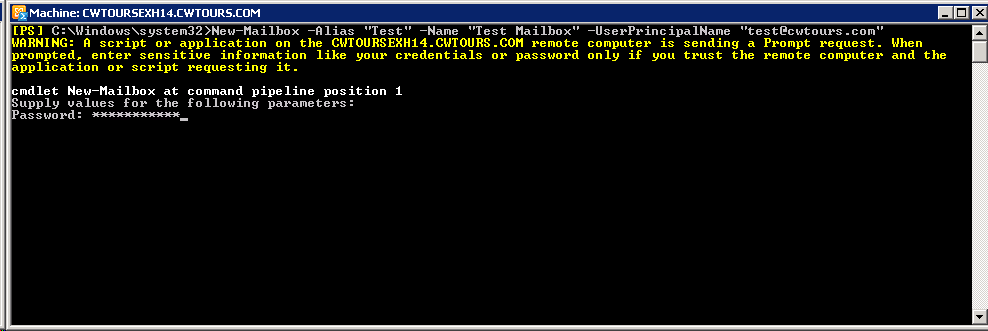
Once you run this command, it will prompt for the password.

**Figure 20 “New-Mailbox”**

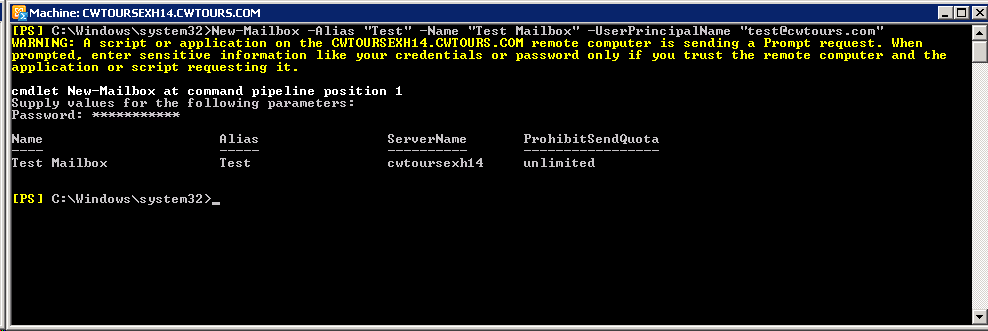


Enter the password as desired and the mailbox gets created.

**Figure 21 “New-Mailbox”**



**Figure 22 “New-Mailbox”**



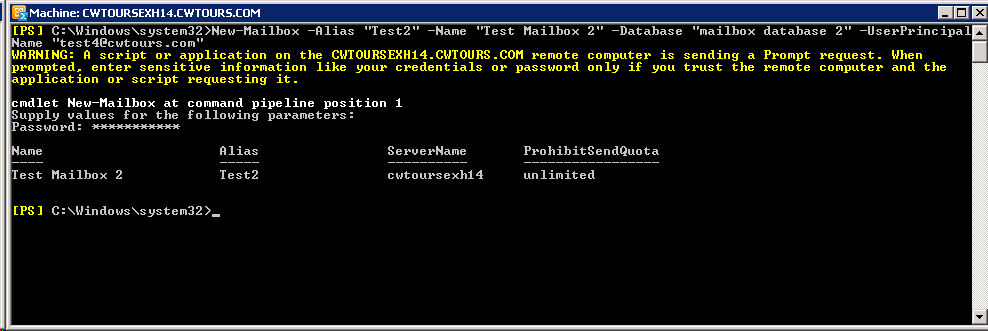
In above command we have not specified a particular Mailbox Database name. You can use –Mailboxdatabase command if you want to create this mailbox on specific mailbox database

New-Mailbox -Alias "Test2" -Name "Test Mailbox 2" -Database "mailbox database 2" -UserPrincipal

Name "test4@cwtours.com"

Enter the desired password and the mailbox gets created on specified mailbox database.

**Figure 23 “New-Mailbox”**



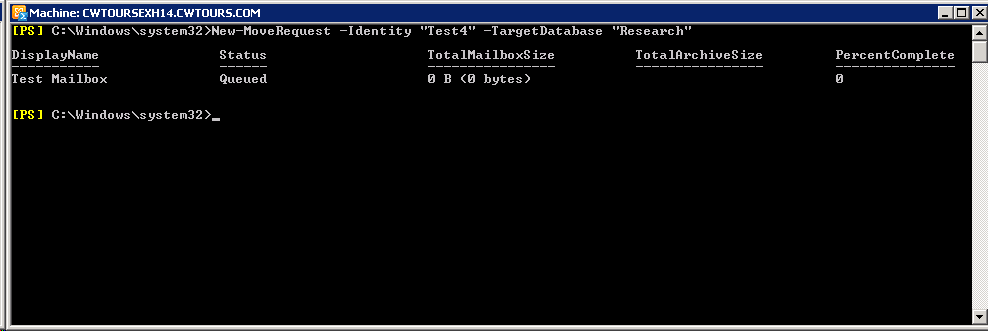
**Move Mailboxes using Exchange PowerShell**

Exchange PowerShell command can be used to move mailboxes between mailbox databases using **New-MoveRequest** command.

Below is the example of moving a mailbox from Mailbox Database “Mailbox Database 2” to “Research”

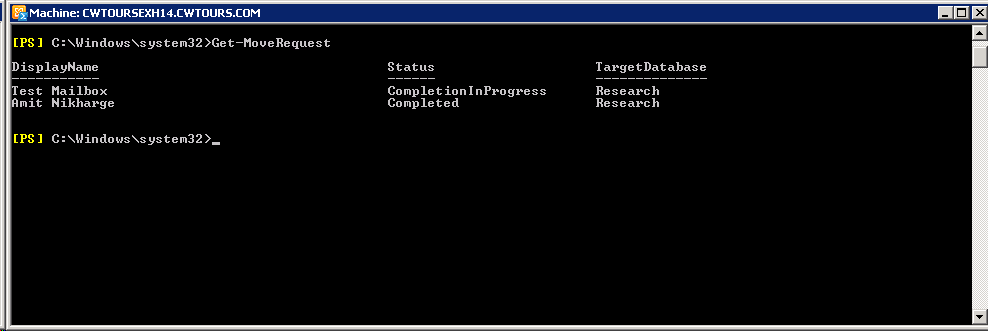
New-MoveRequest -Identity "Test4" -TargetDatabase "Research"

**Figure 24 “New-MoveRequest”**



You can use **Get-MoveRequest** to view the status of mailbox move request.

**Figure 25 “New-MoveRequest”**



Export list of mailbox permissions using Exchange Management Shell.

Exchange Administrator always gets a situation where he wants to view the list of permissions on mailboxes.

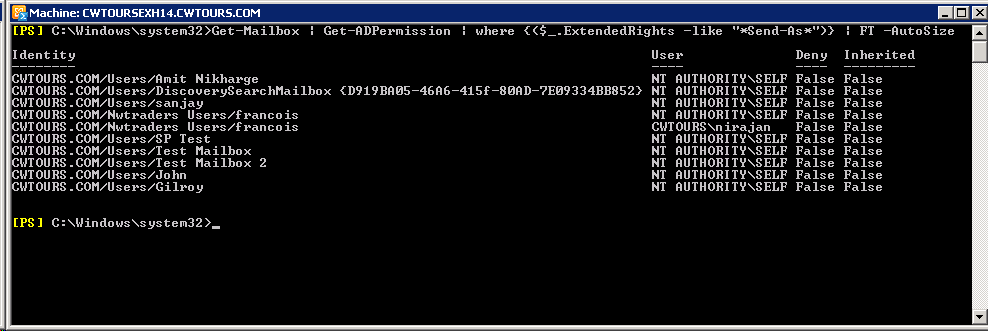
You can use Exchange PowerShell to Export the list of Mailbox Permissions on a mailbox in Exchange 2010 by using **Get-Mailbox | Get-ADPermissions**.

By Default, Get-Mailbox | Get-ADPermissions gives list of all permissions in an Active Directory and Exchange. Live Inherited, Send-As, Extended Rights, Full Access etc.

To filter the output, you can use below command.

Get-Mailbox | Get-ADPermission | where {($\_.ExtendedRights -like “\*Send-As\*”)} | FT –AutoSize

**Figure 26 “Get-Mailbox | Get-ADPermissions”**

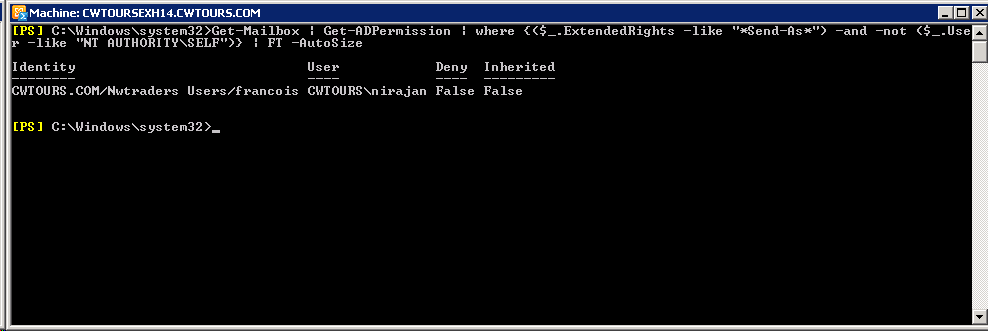


The above command shows that user “cwtours\nirajan” has Send-As rights on mailbox “cwtours\francois”

In the above example output, you will see that the “Self” account is also populated in the list. We can filter the above output and remove “Self” rights and get the actual output by using below command.

Get-Mailbox | Get-ADPermission | where {($\_.ExtendedRights -like “\*Send-As\*”) -and -not ($\_.User -like “NT AUTHORITY\SELF”)} | FT -AutoSize

**Figure 27“Get-Mailbox | Get-ADPermissions”**



This will remove all entries and show the explicit Send-As permissions on the particular mailbox.

References:

Exchange 2010 Performance Counters: <http://gallery.technet.microsoft.com/Performance-and-Threshold-d32ff5a6> and <http://technet.microsoft.com/en-us/library/dd335215.aspx>

<http://technet.microsoft.com/en-us/library/bb331973.aspx>

<http://technet.microsoft.com/en-us/library/ff622322.aspx>

<http://technet.microsoft.com/en-us/library/bb691338.aspx>

Not our link but, a good reference: <http://eightwone.files.wordpress.com/2011/04/visio-exchange-2010-ports-diagram-v31.pdf>

<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=2428>