



SumITUp

A Quick Summary for Practice Test 70-236

TS: Exchange Server 2007, Configuring

SumITUp is a free, quick summary reference of the objectives and material covered on the exam. Use it in addition to your practice test as:

- A quick overview of the exam scope and objectives before you start taking your practice test
- A review of topics covered within each objective to make sure you have studied all the areas
- A tool you can print out for study on the go
- A rapid review for re-focusing right before taking the exam

MEASUREUPTM
www.measureup.com

Installing and Configuring Microsoft Exchange Servers

Prepare the infrastructure for Exchange installation

- Run Setup /PrepareSchema to prepare the Active Directory schema for Exchange
 - You must be a member of the Schema Admins and Enterprise Admins groups
- Run Setup /PrepareAD to configure Active Directory objects and permissions
 - Specify the /OrganizationName switch to specify the name of the Exchange organization
 - This command configures global Exchange objects and creates universal security groups
 - You must be a member of the Enterprise Admins group
- Run Setup /PrepareDomain to prepare a specific domain or Setup /PrepareAllDomains to prepare all domains
- Run Setup /PrepareLegacyExchangePermissions if you are upgrading from Exchange 2000 or Exchange 2003

Prepare the servers for Exchange installation

- You must join each Exchange server that hosts one of the following server roles to the domain:
 - Mailbox
 - Client Access
 - Hub Transport
 - Unified Messaging
- An Edge Transport server must be able to communicate with a Hub Transport server
 - The Hub Transport server is usually placed on the intranet
 - The Edge Transport server is usually placed on the perimeter network
 - You must configure a DNS suffix for the Edge Transport server
- All Exchange servers must be registered in DNS
- The DNS suffix on each Exchange server must be the same as the Active Directory domain name suffix

Install Exchange

- The schema master must be running Windows Server 2003 Service Pack 1 or later
- Ensure that at least one GC server exists at every site where you plan to install Exchange
- Set the domain functional level to Windows 2000 Native or higher
- A minimum of two GB of RAM is required
 - A minimum of five MB per mailbox is required
- At minimum, an 800-MHz 32-bit processor is required
- A minimum of 1.2 GB of free disk space is required on the installation drive
- A minimum of 200 MB of free disk space is required on the system drive
- You must install the following components:
 - Microsoft .NET Framework 2.0
 - Windows PowerShell
 - MMC 3.0
- You must install the following components on mailbox servers:
 - COM+
 - IIS with WWW service
- You must install the following components on Client Access servers:
 - WWW service
 - RPC over HTTP if using Outlook Anywhere

- ASP.NET 2.0
- You must install the following components on Unified Messaging servers:
 - Microsoft Speech
 - Windows Media Encoder
 - Windows Media Audio Voice Codec
 - MSXML 6.0

Configure Exchange server roles

- The Mailbox server hosts Exchange mailboxes and public folders
- The Client Access server allows users to connect to Exchange by using the following technologies:
 - Outlook Anywhere
 - This technology uses RPC over HTTP
 - This allows users to use Outlook to connect to Exchange over the Internet
 - This is useful when a corporate firewall is in place
 - By default, Outlook Anywhere accepts connections over TCP port 80 and SSL port 443
 - OWA
 - This technology uses ASP.NET 2.0
 - Users can use Web browsers to access Exchange
 - The user interface is very similar to the desktop version of Outlook
 - By default, OWA accepts connections over TCP port 80 and SSL port 443
 - POP3
 - Users can download messages to their computers
 - By default, messages are deleted from the server after they are downloaded
 - Deleting a message locally does not delete the message from the server if the client is configured to leave messages on the server
 - You must start the Microsoft Exchange POP3 service to allow users to use POP3 to access their mailboxes
 - By default, POP3 accepts connections over TCP port 110 and SSL port 995
 - IMAP4
 - Users can download messages to their computers
 - Deleting a message locally causes a request to be sent to the server to delete the message on the server if the client is configured to leave messages on the server
 - You must start the Microsoft Exchange IMAP4 service to allow users to use IMAP4 to access their mailboxes
 - By default, IMAP4 accepts connections over TCP port 143 and SSL port 993
 - Exchange ActiveSync
 - Users can synchronize their mailboxes with their mobile devices
 - A sync partnership exists for each user device
 - Exchange ActiveSync uses HTTP and XML to synchronize mailboxes with devices
 - The Exchange ActiveSync virtual directory in IIS is always named Microsoft-Server-ActiveSync
 - Autodiscover Service
 - This service provides users with profile information necessary for connecting to Exchange
 - Profile information includes the user's display name, mailbox server location, and Outlook Anywhere settings
 - You should create a separate Web site in IIS to host the Autodiscover service
 - You must install an SSL certificate to be used by the Autodiscover Web site
- The Hub Transport server routes mail within the Exchange organization
 - You should place this server on the intranet

- The Hub Transport server must be able to perform DNS name resolution for servers on the intranet and for the Edge Transport servers
- The Edge Transport server routes mail in and out of the Exchange organization
 - You should place this server on the perimeter network
 - You can configure the Edge Transport server to use DNS settings assigned to a network adapter or to use specific DNS servers for name resolution
 - The Edge Transport server must be able to perform DNS name resolution for Hub Transport servers and external mail servers
- The Unified Messaging server communicates with PBX systems

Configuring Recipients and Public Folders

Configure recipients

- Active Directory users typically can log on to a domain and access domain resources
 - Get-User - Retrieves user information from Active Directory
 - Set-User - Modifies user attributes in Active Directory
- Mail-enabled users have external e-mail accounts
 - New-MailUser - Creates a new mail-enabled user
 - Set-MailUser - Modifies mail attributes for a mail-enabled user
 - Get-MailUser - Retrieves mail-enabled user information
 - Remove-MailUser - Deletes a mail-enabled user
 - Enable-MailUser - Configures Exchange attributes to mail-enable a user
 - Disable-MailUser - Removes Exchange attributes to mail-disable a user
- Mailbox-enabled users have mailboxes in the Exchange organization
 - New-Mailbox - Creates a new user with a mailbox
 - Set-Mailbox - Sets mailbox attributes for a user
 - Get-Mailbox - Gets mailbox information for users
 - Remove-Mailbox - Deletes a mailbox-enabled user from Active Directory and disconnects the mailbox
 - Connect-Mailbox - Connects a disconnected mailbox to an Active Directory user
 - Enable-Mailbox - Configures Exchange attributes to mailbox-enable a user
 - Disable-Mailbox - Removes Exchange attributes to mailbox-disable a user
- Contacts cannot log on to a domain and they have external e-mail accounts
 - Get-Contact - Retrieves contacts from Active Directory
 - Set-Contact - Modifies contact attributes in Active Directory
 - Get-MailContact - Retrieves contacts that are configured with Exchange attributes
 - Set-MailContact - Modifies Exchange attributes for a contact
 - New-MailContact - Creates a new contact in Active Directory and configures Exchange attributes
 - Remove-MailContact - Deletes a contact that is configured with Exchange attributes
 - Enable-MailContact - Configures Exchange attributes to mail-enable a contact
 - Disable-MailContact - Removes Exchange attributes to mail-disable a contact

Configure mail-enabled groups

- Use a security group to grant or deny members of the group access to resources
 - Use a mail-enabled security group to send e-mail to each of its members that has an e-mail address
 - Get-Group - Retrieves group information from Active Directory
 - Set-Group - Modifies attributes for a group in Active Directory
- Use a distribution group to send e-mail to each of its members that has an e-mail address

- Get-DistributionGroup - Retrieves distribution group information from Active Directory
- Set-DistributionGroup - Modifies attributes for a distribution group in Active Directory
- New-DistributionGroup - Creates a new distribution group in Active Directory
- Remove-DistributionGroup - Deletes an existing distribution group from Active Directory
- Enable-DistributionGroup - Mail-enables an existing universal distribution group
- Disable-DistributionGroup - Mail-disables an existing universal distribution group
- Add-DistributionGroupMember - Adds a member to a distribution group
- Remove-DistributionGroupMember - Deletes a member from a distribution group
- Get-DistributionGroupMember - Retrieves distribution group membership
- Dynamic distribution groups use search filters to create membership at the time e-mail messages are sent
 - Get-DynamicDistributionGroup - Retrieves dynamic distribution group information
 - Set-DynamicDistributionGroup - Modifies an existing dynamic distribution group
 - New-DynamicDistributionGroup - Creates a new dynamic distribution group
 - Remove-DynamicDistributionGroup - Deletes an existing dynamic distribution group
- Domain local group
 - Visible to only the domain where the group exists
 - Can contain members from any domain in the Active Directory forest
- Global group
 - Visible to all domains in an Active Directory forest
 - Can contain members only from the domain where the group exists
- Universal group
 - Visible to all domains in an Active Directory forest
 - Can contain members from any domain in the Active Directory forest
- In Exchange Server 2007, you can only mail-enable universal groups
 - You can still manage domain local and global mail-enabled groups that were migrated from previous versions of Exchange

Configure resource mailboxes

- Resource mailboxes are not associated with an actual user
- You can use Outlook to schedule resources associated with resource mailboxes for meetings
- Resource mailbox types
 - Room
 - When using the New-Mailbox cmdlet to create a room resource mailbox, specify the Room parameter
 - Only the custom properties that are associated with the Room type will be available to be set for the mailbox
 - Equipment
 - When using the New-Mailbox cmdlet to create a room resource mailbox, specify the Equipment parameter
 - Only the custom properties that are associated with the Equipment type will be available to be set for the mailbox
- You can create custom properties for resource types
 - Set-ResourceConfig -ResourcePropertySchema ("Room/TV")
 - This cmdlet creates a new custom property named TV for the Room resource type
 - When you create or modify a room resource mailbox, you can indicate whether the room has a TV by choosing the TV property from the list of available properties
 - Example: Set-Mailbox -Identity "Conference Room A" -ResourceCustom("TV")
 - Set-ResourceConfig -ResourcePropertySchema ("Equipment/Wireless")
 - This cmdlet creates a new custom property named Wireless for the Equipment resource type

- When you create or modify an equipment mailbox, you can indicate whether the equipment has wireless capabilities by choosing the Wireless property from the list of available properties
- Example: Set-Mailbox -Identity "Projector" -ResourceCustom("Wireless")
- You can configure resource mailboxes to automatically accept meeting requests
 - When a resource is booked, it automatically accepts meeting requests if booking is enabled and if the user has permission to book the resource
- Use Set-MailboxCalendarSettings to configuring booking
 - AutomateProcessing parameter
 - None - The resource will not automatically accept meeting requests
 - AutoAccept - The resource will automatically accept meeting requests from those who have booking permissions
 - AutoUpdate - The resource will tentatively accept the meeting request, and a delegate must manually accept it
 - AllBookInPolicy
 - True - All users can book the resource by default
 - False - No user can book the resource by default
 - BookInPolicy
 - Specifies the user accounts that are allowed to book the resource
 - To allow booking, you must set this parameter if AllBookInPolicy is set to False

Configure public folders

- Get-PublicFolder - Retrieves public folder information
- Set-PublicFolder - Modifies an existing public folder
- New-PublicFolder - Creates a new public folder
- Remove-PublicFolder - Deletes an existing public folder
- Update-PublicFolder - Forces replication of a public folder to another server
- Update-PublicFolderHierarchy - Forces replication of a public folder hierarchy to another server
- Enable-MailPublicFolder - Mail-enables a public folder
- Disable-MailPublicFolder - Mail-disables a public folder
- Add-PublicFolderClientPermission - Grants a user permission to access a public folder
- Remove-PublicFolderClientPermission - Removes a user from the client access permissions list
- Get-PublicFolderClientPermission - Retrieves the access permissions list for a public folder
- Add-PublicFolderAdministrativePermission - Grants a user permission to administer a public folder
- Remove-PublicFolderAdministrativePermission - Removes a user from the administrative permissions list
- Get-PublicFolderAdministrativePermission - Retrieves the administrative permissions list for a public folder

Move mailboxes

- Use the Move-Mailbox cmdlet to move a mailbox to another mailbox database
 - Specify the ConfigurationOnly parameter if you only need to update the mailbox attributes in Active Directory with the new location of the mailbox
 - Specify the StartDate parameter to indicate that only items newer than the specified start date should be moved
 - Specify the EndDate parameter to indicate that only items older than the specified end date should be moved
 - Specify the AttachmentFileNames parameter to indicate that only items that contain the specified attachments should be moved
 - You can specify a wildcard such as *.zip to move all messages that have ZIP attachments
- Use Task Scheduler to schedule a mailbox move
- To move mailboxes across forests, you must specify the domain controller of the target domain and GC server of the source or target forest
 - If you run the Move-Mailbox cmdlet from the target domain, you must set the SourceForestGlobalCatalog parameter to the GC server of the source forest

- If you run the Move-Mailbox cmdlet from the source domain, you must set the GlobalCatalog parameter to the GC server of the target forest

Implement bulk management of mail-enabled objects

- Use piped commands to implement bulk-management of objects
- Get-User | Enable-Mailbox
 - This command mailbox-enables all users in Active Directory
- Get-Mailbox | Set-Mailbox -MaxSendSize 15mb
 - This cmdlet sets a send messages size limit of 15 MB for all mailboxes
- Get-Mailbox -OrganizationalUnit Probationary | Set-Mailbox -DeliverToMailboxAndForward \$true -ForwardingAddress vick@bcdtrain.com
 - This cmdlet forwards to vick@bcdtrain.com all e-mail messages that are sent to users in the Probationary OU
- Use the Import-Csv cmdlet to process data in CSV files
 - Variables are created for headers in the CSV files
 - A header named FirstName has an associated variable named \$_.FirstName

Configuring the Exchange Infrastructure

Configure connectors

- Routing group connectors allow Exchange servers at different sites to communicate with each other
- Foreign connectors allow Exchange to communicate with third-party messaging systems that do not support SMTP
 - You can only create foreign connectors on Hub Transport servers
- Send connectors allow Exchange to send SMTP and other types of messages to other servers
- Receive connectors allow Exchange to receive SMTP messages from other servers
- To send e-mail to the Internet
 - Create a send connector on an Edge Transport server
 - Set the address space to * to indicate that the connector should be used for all domains
 - Enable DNS routing if the connector should query the target domain's MX record, or target SMTP server
 - Use smart hosts if your ISP requires all outbound SMTP traffic to be forwarded through its SMTP server
 - Create a send connector on a Hub Transport server that sends Internet SMTP messages to the Edge Transport server
- To receive e-mail from the Internet
 - Create a receive connector on an Edge Transport server
 - Create a receive connector on a Hub Transport server that accepts incoming SMTP messages from the Edge Transport server

Configure the antivirus and anti-spam system

- Configure connection filtering to restrict the mail servers that can send messages to your Exchange organization
- Configure recipient filtering to block incoming messages to specific recipients
- Configure sender filtering to block incoming messages that appear to be from specific e-mail addresses or domain names
- Configure content filtering to accept or reject a message based on its contents

Configure transport rules and message compliance

- Message classifications allow you to supply an intended use for a message so that transport rules can perform actions
 - For example, a message classified as Attorney Client Privileged might automatically have a disclaimer added to it by a transport rule's action
- Transport rules allow you to perform actions on messages that meet certain conditions and exceptions
 - Example
 - Delete all messages that have a file named Virus.zip attached unless the message is sent between members in the IT department

- Conditions indicate the messages to which a transport rule applies
 - Examples
 - The Attorney Client Privileged classification is applied to a message
 - A message is being sent to or from a specific user
- Exceptions indicate the messages to which a transport rule should not apply
 - Example
 - If a message is sent from the CEO, do not automatically Bcc the IT department
- A transport rule with no conditions and no exceptions applies to all messages

Configure policies

- E-mail address policies automatically generate e-mail addresses for recipients
 - Use the New-EmailAddressPolicy cmdlet to create a new e-mail address policy
- Journal rules allow you to report and archive messages sent and received by the Exchange organization
 - Message reports are forwarded to a journal mailbox
 - The original message is included as an attachment with the report
 - To temporarily suspend journaling, run the Disable-JournalRule cmdlet
 - To permanently remove a journal rule, run the Remove-JournalRule cmdlet

Configure public folders

- Get-PublicFolder - Retrieves public folder information
- Set-PublicFolder - Modifies an existing public folder
- New-PublicFolder - Creates a new public folder
- Remove-PublicFolder - Deletes an existing public folder
- Update-PublicFolder - Forces replication of a public folder to another server
- Update-PublicFolderHierarchy - Forces replication of a public folder hierarchy to another server
- Enable-MailPublicFolder - Mail-enables a public folder
- Disable-MailPublicFolder - Mail-disables a public folder
- Add-PublicFolderClientPermission - Grants a user permission to access a public folder
- Remove-PublicFolderClientPermission - Removes a user from the client access permissions list
- Get-PublicFolderClientPermission - Retrieves the access permissions list for a public folder
- Add-PublicFolderAdministrativePermission - Grants a user permission to administer a public folder
- Remove-PublicFolderAdministrativePermission - Removes a user from the administrative permissions list
- Get-PublicFolderAdministrativePermission - Retrieves the administrative permissions list for a public folder

Configure client connectivity

- Use Exchange ActiveSync to allow users to synchronize their mailboxes with mobile devices
 - Run the Test-ActiveSyncConnectivity cmdlet to verify synchronization with a specific mailbox
- Use OWA to allow users to access their mailboxes in a Web browser
 - Run the Test-OwaConnectivity cmdlet to verify OWA connections to a Client Access server
- Use Outlook Anywhere to allow users to use Outlook to access their mailboxes with RPC over HTTP
 - Run the Enable-OutlookAnywhere cmdlet to enable Outlook Anywhere on a Client Access server
 - Run the Test-WebServicesConnectivity cmdlet to verify the Client Access server is accepting Outlook Anywhere requests
- Use POP3 to allow users to download e-mail to their computers
 - By default, downloaded messages are removed from the mailbox server
 - You can configure a user's account settings to leave messages on the mailbox server

- When a user deletes a downloaded message, no request is sent to the server to delete the message
- Use IMAP4 to allow users to download e-mail to their computers
 - When a user deletes a downloaded message, a request is sent to the server to delete the message if the message is also stored on the server
- Run the Set-CASMailbox cmdlet to modify client access settings for a specific mailbox
 - The ActiveSyncEnabled parameter determines whether ActiveSync is enabled for the mailbox
 - The OWAEnabled parameter determines whether OWA is enabled for the mailbox
 - The PopEnabled parameter determines whether POP3 is enabled for the mailbox
 - The MAPIBlockOutlookRpcHttp parameter determines whether Outlook Anywhere is disabled for the mailbox
- The Autodiscover service provides users with profile information necessary for connecting to Exchange
 - Profile information includes the user's display name, mailbox server location, and Outlook Anywhere settings
 - Run the Test-OutlookWebServices cmdlet to verify Autodiscover service settings on the Client Access server

Monitoring and Reporting

Monitor mail queues

- Mail queues are located on Hub Transport servers and Edge Transport servers
- Use Queue Viewer to graphically monitor queues
- Run the Get-Queue cmdlet to retrieve queues that have pending messages
- Run the Suspend-Queue cmdlet to temporarily stop mail flow from a transport server
- Run the Resume-Queue cmdlet to resume a suspended queue
- Run the Retry-Queue cmdlet to retry sending messages that are held in queues
- Run the Get-Message cmdlet to retrieve messages that are pending in queues
 - This allows you to determine whether a specific message has been routed
- Run the Suspend-Message cmdlet to temporarily suspend a message
 - This will prevent the message from leaving the queue
- Run the Resume-Message cmdlet to resume a suspended message
- Run the Move-Message cmdlet to delete a message from a queue

Monitor system performance

- Run the Test-ServiceHealth cmdlet to ensure that required services are started
- Run the Test-SystemHealth cmdlet to analyze system performance according to Microsoft best practices
 - The DownloadConfigurationUpdates parameter indicates whether the cmdlet should download updates to the analysis configuration file before analysis is performed
- Use Task Manager to view memory usage, CPU usage, network utilization
- Use Event Viewer to view event logs associated with Exchange
- Use Performance to gather data from Exchange performance counters

Perform message tracking

- Message tracking allows you to record SMTP activity on a Hub Transport server, Edge Transport server, or Mailbox server
- Run the Set-TransportServer cmdlet to configure message tracking on a transport server
- Run the Set-MailboxServer cmdlet to configure message tracking on a Mailbox server
- Set the MessageTrackingLogEnabled parameter to True to enable message tracking
- Set the MessageTrackingLogPath parameter to the path of the message tracking log file
 - The default path is C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking
- Set the MessageTrackingLogMaxAge parameter to specify the circular logging age

- The default age is 30 days
 - Circular logging reuses log files to maximize storage space
- Set the MessageTrackingLogMaxFileSize parameter to the maximum size of a log file
 - When the size of the log file reaches the maximum size, a new log file is created
 - The default maximum size is 10 MB
- Set the MessageTrackingLogMaxDirectorySize to the maximum size of the log directory
 - When the size of the log directory reaches the maximum size, the oldest log file is deleted and reused
 - The default maximum size is 250 MB
- Set the MessageTrackingLogSubjectLoggingEnabled parameter to False to disable subject logging
 - The subject line is stored in the message tracking log file by default

Monitor client connectivity

- Connectivity logging allows you to record connection activity of outbound message queues
 - It includes logging of the source queue, destination Mailbox server, destination domain, destination smart host, DNS resolution, bytes sent, and connection failures
- Use the Set-TransportServer cmdlet to configure connectivity logging
- Set the ConnectivityLogEnabled parameter to True to enable connectivity logging
- Set the ConnectivityLogPath parameter to the path of the connectivity log file
 - The default path is C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\Connectivity
- Set the ConnectivityLogMaxAge parameter to specify the circular logging age
 - The default age is 30 days
 - Circular logging reuses log files to maximize storage space
- Set the ConnectivityLogMaxFileSize parameter to the maximum size of a log file
 - When the size of the log file reaches the maximum size, a new log file is created
 - The default maximum size is 10 MB
- Set the ConnectivityLogMaxDirectorySize to the maximum size of the log directory
 - When the size of the log directory reaches the maximum size, the oldest log file is deleted and reused
 - The default maximum size is 250 MB

Create server reports

- The Exchange 2007 Management Pack works with MOM 2005 to provide health reports
- MOM 2005 must use SQL Server 2000 or SQL Server 2005 to host the report database
 - It uses SQL Server Reporting Services
- The following reports are included by default:
 - Service Availability
 - Metrics
 - Anti-Spam

Create usage reports

- The Exchange 2007 Management Pack works with MOM 2005 to provide health reports
- MOM 2005 must use SQL Server 2000 or SQL Server 2005 to host the report database
 - It uses SQL Server Reporting Services
- The following reports are included by default:
 - Service Availability
 - Metrics
 - Anti-Spam

Configuring Disaster Recovery

Configure backups

- Full backups are complete backups
 - After a full backup completes, the transaction log is deleted
- Differential backups are cumulative backups
 - They back up all changes that occurred since the last full or incremental backup
 - After a differential backup completes, the transaction log is not deleted
 - When restoring differential backups, you need only the most recent differential backup
- Incremental backups are non-cumulative change-only backups
 - They back up all changes since the last full or incremental backup
 - After an incremental backup completes, the transaction log is deleted

Recover messaging data

- When you move a mailbox database to a new server, you must rename the EDB file name to match the name associated with the new mailbox store
 - Example
 - A file named Priv1.edb is associated with a mailbox store on the source server
 - A file named Mailbox.edb is associated with a mailbox store on the target server
 - If you move Priv1.edb to the target mailbox store, you must rename Priv1.edb to Mailbox.edb
- Full backups only
 - You must restore the most recent full backup
- Full backup and incremental backup combination
 - You must restore the most recent full backup followed by each incremental backup up to the time of the failure
- Full backup and differential backup combination
 - You must restore the most recent full backup followed by the most recent differential backup
- After you restore all necessary backups, you can replay the transaction logs to restore any changes that occurred since the most recent backup

Recover server roles

- Recovering a non-clustered mailbox server
 - Reset the computer account in Active Directory for the failed server
 - Rename a new server to the name of the failed server
 - Run Exchange Setup with the m:RecoverServer switch
 - This restores the roles on the new server that were configured in Active Directory for the old server
 - You cannot use this switch to recover the Edge Transport server role
- Recovering a clustered mailbox server
 - Run Exchange Setup with the RecoverCMS switch
 - Set the CMSName parameter to the name of the clustered mailbox server
 - Set the CMSIPAddress parameter to the IP address of the clustered mailbox server
- Recovering a Client Access server
 - You must first save the client access configuration to an XML file
 - You can then run the Import-ClIXml cmdlet to import the client access configuration

Configure high availability

- LCR uses separate disks to host copies of Exchange databases on a single server
 - If the server fails, access to the databases will be interrupted

- If the active disk fails, the passive copy of the databases will be used
- CCR uses a two-node active-passive cluster to host separate clustered mailbox servers and Exchange databases
 - If the active node fails, functionality automatically fails over to the passive node
 - If the active disk fails, functionality automatically fails over to the passive node
 - Only if the passive node also fails will database access be interrupted
- Single copy clusters consist of multiple nodes that share Exchange databases
 - If the active node fails, the passive node can access the databases
 - If the disk fails, access to the databases will be interrupted
- To seed an LCR or CCR database copy, run the Update-StorageGroupCopy cmdlet
 - Seeding is the process of initializing the database copy
 - This is necessary when a failure occurred but the log files cannot be replayed
- Run the Enable-DatabaseCopy cmdlet to enable a database for LCR replication
 - Set the CopyEdbFilePath parameter to the path of the LCR copy
- Run the Enable-StorageGroupCopy cmdlet to enable a storage group for LCR replication
- Run the Move-ClusteredMailboxServer cmdlet to move a clustered mailbox server from the active node to the passive node
- Run the Start-ClusteredMailboxServer cmdlet to start a clustered mailbox server when one is not already running

Acronyms

Acronym	Definition
ASP	Active Server Pages
CCR	Cluster Continuous Replication
CMS	Clustered Mailbox Server
COM	Component Object Model
CPU	Central Processing Unit
CSV	Comma Separated Value
DNS	Domain Name System
EDB	Embedded Database Engine
GB	Gigabyte
GC	Global Catalog
GHz	Gigahertz
HTTP	Hypertext Transfer Protocol
IIS	Internet Information Services
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ISP	Internet Service Provider
LCR	Local Continuous Replication
MB	Megabyte
MHz	Megahertz
MMC	Microsoft Management Console
MOM	Microsoft Operations Manager
MSXML	Microsoft Core XML Services

Acronym	Definition
MX	Main Exchange
OU	Organizational Unit
OWA	Outlook Web Access
PBX	Private Branch eXchange
POP	Post Office Protocol
RPC	Remote Procedure Call
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
WWW	World Wide Web
XML	Extensible Markup Language