Notes from CBT Nuggets Exam-Pack 70-236: Exchange Server 2007, Configuring
(http://www.cbtnuggets.com/webapp/product?id=398)

Notes taken in July and August of 2009. I also checked other resources when the CBT wasn't clear or detailed enough.

Be aware that the CBT is for the RTM version. There were several changes and new features added in SP1 and SP2. Some settings that were only available through EMS were added to EMC in SP1. Also, SP1 added Standby Continuous Replication.

VIDEO 01: Introduction to Exchange 2007

- AD forest is made of domain trees that share common schema and AD configuration. All domain trees in a forest have transitive trusts to each other by default.
- Only one Exchange org per AD forest. DCs replicate all object attributes. GCs replicate a subset of object attributes of all domains in forest.

1. **Server Role: Mailbox (installed by default)**
    a. User mailboxes and PFs.
    b. Must be part of AD domain.
    c. 50 storage groups per sever [Enterprise Ed. only, 5 for Standard Ed.].
2. **Server Role: Hub Transport (installed by default)**
    a. Internal mail flow. Similar to bridgehead.
3. **Server Role: Edge Transport (optional)**
    a. NOT part of production AD domain. Must be installed on standalone server or DMZ AD domain.
    b. Uses ADAM and EdgeSync to enable one way synch from production AD for address lookup.
    c. Secures perimeter with anti-spam, AV, and security policies.
    d. Same functionality can be done on Hub Transport also.
    e. [Isn't really necessary if an e-mail appliance is already used, but the ADAM address lookup is a nice feature that some appliances/services don't have.]
4. **Server Role: Client Access (installed by default)**
    a. OWA, ActiveSync, Outlook Anywhere (RPC/HTTP)
    b. Similar to FE in Ex2003.
5. **Server Role: Unified Messaging**
    a. Integrates with VoIP systems.
    b. Outlook Voice Access (text to speech)

- At minimal, Mailbox, Hub Transport, and Client Access roles are required for a functional Exchange server. The default install option will install these three roles on one server.

VIDEO 02: Preparing and Installing Exchange 2007

- Must be Windows Server 2003 SP1 x64 or later for production version of Exchange. **MMC 3.0**, **.NET 2.0**, and **Windows PowerShell** are required. Exchange setup will check for these requirements and then have options for downloading them from MS if they're not present.
- Must be in Schema Admins group to prep AD schema. Most other task can be done as member of Enterprise Admins. For changes to specific domains, must also be member of domain's Domain Admins group.
- Schema Master must be running Windows Server **2003 SP1 or higher**.
- Must have one GC per AD site
- Setup switches:
    - **/PrepareLegacyExchangePermissions** Required for coexisting with Exchange Server 2000/2003
    - **/PrepareSchema** Must be run by member of Schema Admins group against schema master. Server that is being used to run setup must be in same AD site and domain as schema master.
    - **/PrepareAD** Prepares forest and creates *Microsoft Exchange Security Groups* OU in forest root domain, creates Universal Security Groups for Exchange Admin roles. You'll provide the Exchange organization name at this step. [Creates *Exchange Administrative Group (FYDIBOHF23SPDLT)* and *Exchange Routing Group (DWBGZMFD01QNBJR)* for backwars compatibility. Runs all other switches as needed if they haven't been run for forest or root domain. Server that is being used to run setup must be in same AD site and domain as schema master.]
    - **/PrepareDomain *[domain name]*** Run in each domain that will host Exchange server or Exchange objects.
    - **/PrepareAllDomains** Prepares ALL domains.
- Domain functional level must be at Windows 2000 native or higher.
- Exchange 5.5 not supported at all within same org.
- Client Access role needs IIS and ASP.NET [2.0] (it's installed with .NET, but might need to be enabled in IIS). **If installed before IIS,** you'll have to manually allow ASP.NET from within IIS MMC.
- Hub Transport and Edge roles should NOT have IIS SMTP service installed [because Exchange now uses its own SMTP agent in *Microsoft Exchange Transport Service*.]
- Typical Exchange Server Installation:
    - Installs 3 roles: Hub Transport, Client Access, and Mailbox; and Exchange Management Tools [Exchange Management Console—EMC, and Exchange Management Shell--EMS].
- Custom Exchange Server Installation:
    - If you choose Edge Transport, all other roles are grayed out. This role cannot be on a domain member server, so choosing it removes the option to install other roles that require domain membership.
    - You can install individual roles, cluster options, and Management Tools.
- Outlook 2003 and earlier and Entourage clients require a PF database in order to connect to Exchange 2007. You must select yes to have Exchange setup install a PF database if you have these older clients.
- Exchange Management Console opens up after setup is completed.
- Run Exchange Best Practices Analyzer (ExPBA) regularly to make sure Exchange is working properly.

- UPGRADES: This is NOT possible—direct upgrade cannot be performed at all from Exchange 2000/2003. Two options available for deploying Exchange 2007 with older version:
    - TRANSITION: Add Exchange 2007 servers to org and move mailboxes and roles over from older versions. Eventually phase out older versions. Must upgrade all 5.5 servers to 2000/2003 first.
    - MIGRATION: Move to a new Exchange 2007 org.
    - Run readiness check from ExPBA to help plan for transition/migration.

VIDEO 03: Managing Storage Groups and Databases

- Exchange 5.5 had only 3 DBs: PRIV.EDB, PUB.EDB, and DIR.EDB. All mailboxes were in PRIV.EDB and all PFs were in PUB.EDB. This resulted in single points of failure and long restoration and recovery.
- Exchange 2000 introduced Storage Groups with separate DBs. No more single points of failure.
    - Exchange 2007 Enterprise: 50 SGs with 5 DBs per SG, but maximum 50 DBs total.
    - Exchange 2007 Standard: 5 SGs with 5 DBs per SG, but maximum 5 DBs total.
    - [Both versions: max 16 TB per database]
    - [See http://www.microsoft.com/exchange/2007/evaluation/editions.mspx.]
- Transaction log files are now 1 MB each [instead of 5 MB as in Exchange 2003]. All transactions go to logs and memory first before being committed to DB.
- Checkpoint file (*.chk) keeps track of which transactions have been committed to DB.
- Log files (*.log). There's always a current log file and it gets saved and renamed after it reaches 1 MB. There are two reserved log files (*E<nn>res00001.jrs* with <nn> being the storage group's log file prefix number) that are used in case there's no free space left (only totals 2 MBs though).
- Temporary DB (tmp.edb) is used as temporary workspace for actual DB file (*.edb).
- Log files and DBs both should be on separate, dedicated hard drives. This allows better recoverability and increases performance—DB drive can crash and would not affect recoverable up to point of failure since logs are on separate drive. Logs should be on RAID 1 [or better]. DBs should be on RAID 5 [or better].
- SG log files path and system files path options are the same as Ex2003. Ex2007 uses the term "database" instead of "store." Mailbox storage limit/quota settings for DB are the same as in Ex2003.
- Circular logging is set per SG and allows fully committed transaction logs to be overwritten. Enabling this will not allow recoverability up to the point of failure. Without circular logging, logs are only deleted after a backup. [Same as older versions of Exchange.]

VIDEO 04: Configure Public Folders

- PFs are NOT required in Ex2007 because Outlook 2007+ doesn't require PFs. PFs are de-emphasized in Ex2007 in favor of SharePoint.
- After PF DB is created, PFs can be created using Outlook or EMS (Exchange Management Shell). By default, regular users cannot create any additional PFs. PF permission roles consists of specific permissions for simplified management.
- PF structure is replicated via AD replication. PF content/data is replicated by creating replicas on different servers. Replicas are created via EMS. Replication is 15 minutes by default.
- If a PF is not on the user's local Exchange server, the user will be directed to a replica on an Exchange server in an AD site that has the lowest cost link. [Ex2003 did not rely on AD sites for PF referrals—routing groups were used.]

VIDEO 05: Managing Recipient Objects: Mailboxes

- **Mailbox User** Consists of AD account, mailbox, and e-mail address. Can be created for new or existing user.
- Recipients are now created and managed from EMC → Recipient Configuration (can no longer manage Exchange attributes from ADUC).
- Move Mailbox wizard in EMC is the same as in Ex2003. Cross-forest mailbox moves must be done via EMS.
- Mailbox storage quotas are set in mailbox properties → Mailbox Settings → Storage Quotas option. The settings are the same as in Ex2003—issue warning, prohibit send, prohibit send and receive, keep deleted items for n days, and do not permanently delete items until backup of database.
- MAPI access can be disabled from mailbox properties → Mailbox Features. This option was not available in Ex2003. This means you can prohibit users from connecting to their mailboxes via the Outlook client.
- Mailbox properties → Mail Flow tab contains the send on behalf, forwarding, recipient limits settings, send and receive message size limits, and accept/reject message from specific senders.

VIDEO 06: Managing More Recipient Objects

- **Mail User** AD account and e-mail address only (address is external to Exchange org and has globe on user icon in GAL). These types of accounts show up under EMC → Recipient Configuration → Mail Contact.
- **Room Mailbox** and **Equipment Mailbox** For resource sharing. AD account is disabled when created. If creating mailbox for existing account, existing account must be disabled. Some other differences:
    - Icon in EMC has a different icon and the recipient type is either *Room Mailbox* or *Equipment Mailbox*.
    - Has *Resource Information* tab in properties. Contains resource capacity field (how many users can a room hold) and custom properties (custom properties can only be added after resource property schema is extended).
- **Mail Contact** No AD account, just e-mail address. Shows up in GAL and can be added to DGs.
- **Linked Mailbox** For a user account in a separate, externally trusted forest/domain. [The mailbox is actually created with a disabled user account in the resource forest/domain. You then link that account to a linked master account in the external forest/domain.]
- Distribution Groups
    - Only Universal DGs can be created in Ex2007, but non-UDGs from older Exchange org can be managed.
    - Dynamic DG: Filter- and condition-based. [Like Query-based Distribution Groups in Ex2003.]

VIDEO 07: E-mail Policies, Accepted Domains and Address Lists

- **E-mail Address Policies** EMC → Organization Configuration → Hub Transport → E-mail Address Policy. Contains *Default Policy* with lowest priority. [These policies are similar to Ex2003, but have several improvements and only apply to the mailbox name (the part before @domain.com).]

- **Accepted Domains** [This is new in Ex2007. They took this part from the Ex2003 Recipient Policy.]: An Exchange org can host multiple SMTP domains. If the external message is sent all the way through from the Edge Transport to the Hub Transport and accepted by a Mailbox server, this means that the Exchange org is authoritative for that domain. Besides authoritative domains, there are two types of relay domains:

    - **External Relay Domain** The Edge Transport will accept mail for the domain and then relay it to another server outside of the Exchange org.

    - **Internal Relay Domain** The Mailbox server accepts the mail for the domain and then relays it to a server in another AD forest.

  [The author skipped an important part: how do you tell Exchange which host to relay to? I looked this up and what you'll need to do is create send connectors for the relayed domains. See this link for details on that.]

- **Address List**s EMC → Organization Configuration → Mailbox → Address Lists. ALs are filter- and condition-based, just like Dynamic DGs.

- New GALs can only be created through EMS. [The author failed to provide details on when additional GALs should be used and how to limit users to a particular GAL. See this link for details on that.]

- CAS is used for non-MAPI clients: OWA, ActiveSync, Outlook Anywhere (RPC/HTTP), POP3/IMAP4
- CAS role configures IIS virtual directories for OWA.
    - Under IIS Mgr → <*ExchangeServer*> → Web Sites → Default Web Site:
        - **owa**: For users who have mailboxes on Ex2007 servers.
        - **Public**: Access to PFs on Ex2000/2003 servers.
        - **Exchweb**: Access to previous OWA virtual directories.
        - **Exchange**: Access to mailboxes on Ex2000/2003 servers.
- From EMC → Server Configuration → Client Access.
    - Outlook Web Access tab contains the IIS virtual directories. The *owa* folder has more options and configuration tabs than the other folders because it's native for Ex2007. Some *owa* options are:
        - The site uses forms-based authentication with *domain\username* format, by default.
        - The *Segmentation* tab allows very granular control by allowing the admin to disable/enable OWA features such as Calendar or Contacts folders, e-mail signatures, spelling checker, etc. I don't recall this level of granularity in Ex2003.
        - *Public Computer File Access* tab applies when the public/shared computer option is selected at logon
            - Under *Direct file access* →*Customize*, you can specify the types of files allowed, blocked, or forced to save first before opening.
            - *WebReady Document View* determines the behavior for showing convertible documents in HTML format instead of the document's native format. This applies to computers that don't have Word installed, for example WebReady would show the Word attachment in HTML format in that case. You can also force WebReady to be used when a converter is available.
            - Windows file shares and SharePoint files can be accessed via OWA, by default [but only if they're explicitly on the allow list]. [You would open the location of the resource URL/UNC from the *Documents* button on the left pane of OWA.]
        - *Private Computer File Access* tab applies when the private computer option is selected at logon and has the same options as the *Public Computer File Access* tab.
        - *Remote File Servers* tab has block and allow lists for access to internal Windows file share and SharePoint servers based on host names. You can also allow access to all servers with particular domain suffixes in their FQDN.
    - OWA configuration is a lot easier and intuitive compared to Ex2003—most of the settings are in EMC instead of IIS Mgr.
- Exchange ActiveSync is enabled by default. Allows online and OFFLINE access.
        - Direct Push: Used with Windows Mobile 5.0 (with Messaging and Security Feature Pack [MSFP]) or later. Allows constant HTTPS connection with CAS for real-time access.
        - EMC → Organization Configuration →Client Access → Exchange ActiveSync Mailbox Policies.
            - No policy is set by default, so you should set one up since ActiveSync is enabled by default.

        - A non-provisionable device is a Windows mobile device that can only apply a subset of a policy or none of the policy. If you enable “allow non-provisionable devices,” then even if the device can’t apply all the policies, it’ll still be able to use ActiveSync. This is not enabled by default on new policies, which makes sense from a security perspective.

    - Password (complexity, attempt thresholds, length, expiration, history, etc) and encryption settings are managed here.

    - ActiveSync policies are applied to individual mailboxes in the mailbox’s *Mailbox Features* tab. You can create multiple policies and apply them to different mailboxes (only one policy can apply to a mailbox though).

- Remote Wipe: Allows Exchange to send a wipe command to device so that the next time it connects, it’ll clear out its memory. Ex2007 has an option in OWA that allows users to perform a remote wipe on their own.

- The *Export-ActiveSyncLog* cmdlet allows you to get a report on ActiveSync.

VIDEO 09: Outlook Anywhere and POP/IMAP Configuration

- Outlook Anywhere: Uses RPC over HTTP/HTTPS to allow MAPI clients (Outlook 2003/2007) to connect to Exchange 2003 SP1/2007 mailboxes via CAS *RPC over HTTP Proxy* service.
- On CAS server (doesn't have to be CAS, but it's a best practice), add *RPC over HTTP Proxy* networking service to Windows Server OS.
- From EMC → Server Configuration → Client Access → Enable Outlook Anywhere (in actions pane).
    - Enter external host name.
    - Basic authentication or NTLM authentication (basic is default, NTLM can have issues with firewalls). If you're using basic authentication and SSL also, then the password is actually encrypted in the HTTPS tunnel.
    - Enable SSL offloading if you have an SSL accelerator.
- IMAP4 and POP3 are installed, but set for manual startup. These two services cannot be managed in EMC—they can only be managed via EMS (at least in RTM version). Exchange installs a self signed cert by default. If you get a real cert, you need to get the thumbprint of the new cert and use that as a parameter in an EMS cmdlet and apply it to IMAP4 or POP3.
    - IMAP4 and POP3 are enabled by default for each mailbox in its *Mailbox Features* tab.
- **Autodiscover** Outlook 2007 will query Autodiscover on CAS to get information to build Outlook profile. This works with Outlook 2007 and Windows Mobile 6.
- Other CAS services:
    - *Calendar Attendant*: handles meeting requests for mailboxes.
    - *Scheduling Assistant*: makes it easier to plan meeting.
    - *Resource Booking Assistant*: Handles accepting/declining meetings for resource mailboxes.
    - *Availability Service*: Free/Busy information now available as a Web service instead of through PF. For Outlook 2007 and OWA only.
    - *Offline Address Book*: Can be distributed through PF [like Ex2003] or through IIS virtual directory on CAS.

VIDEO 10: Configuring Disaster Recovery

- Backup strategies
    - Full (and copy):
        - A full backup deletes transaction logs after backing them up. This is the best choice since a restore only requires the full backup. The only issue is that the backup window might be too long to do a full backup during the weekdays.
        - A copy doesn't delete transaction logs at all. There's nothing that indicates that a copy was done since no logs are deleted. This is strictly a copy, hence the name. Can be used for weekly or monthly archiving.
    - Incremental
        - Backs up all files that have changed since last full or incremental backup. Deletes transaction logs after backing them up. A restore requires full + all subsequent incrementals.
        - Does NOT work with circular logging.
    - Differential
        - Backs up all files that have changed since last full backup. Does NOT delete transaction logs after backing them up. A restore requires full + most recently differential only.
        - Does NOT work with circular logging.
    - Brick-level
        - Backs up mailboxes individually, message by message. Takes longer, but restores are quicker.
        - Not natively included—must use third-party backup programs.
    - VSS
        - Supported, but not natively included—must use third-party backup programs.
        - Provides point-in-time snapshots, allowing quicker backups and restores.
- Backups based on server role
    - Mailbox
        - Transaction logs and databases, and system state.
        - Search index catalog cannot be backed up. After restore/rebuild, stop the *Microsoft Search* service and delete the *CatalogData* folder in the storage group folder and restart *Microsoft Search* to force a rebuild of the catalog.
    - Hub Transport
        - Uses circular logging since message queues are only temporary so they don't really need to be backed up. [The queue now uses an ESE database instead of flat files. The database is named *mail.que* and is in *C:\Program Files\Microsoft\Exchange Server\TransportRoles\data\Queue* along with the logs, checkpoint, tmp.edb, and reserved logs. You can move these files for performance reasons.]
        - Message tracking logs and protocol logs should be backed up using file system backup. The folders to backup are in *MessageTracking* and *ProtocolLog* under *C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs*.

        - Server configuration is stored in AD, so to rebuild a HT server, run EMS command *setup /m:RecoverServer*.

    - Client Access

        - Perform file system backup of *C:\Program Files\Microsoft\Exchange Server\Client Access* folder for settings for OWA site, POP3, IMAP4, etc. [These are the subfolders:

            1. Autodiscover
            2. exchweb
            3. OAB
            4. Owa
            5. PopImap
            6. Sync.]

        - Server configuration is stored in AD, so to rebuild a HT server, run EMS command *setup /m:RecoverServer*.
        - System state and IIS metabase.

    - Edge Transport

        - Server is not part of AD domain. Customized settings can be backed up with *ExportEdgeConfig.ps1*. To restore custom settings, run *ImporttEdgeConfig.ps1*.
        - Recipient and Exchange org configuration data (not Edge server configuration since Edge isn't part of AD) in AD will be replicated to ADAM after restore.

    - Unified Messaging

        - Run EMS command *setup /m:RecoverServer*.
        - Custom audio files in *C:\Program Files\Microsoft\Exchange Server\UnifiedMessaging\Prompts* folder should be backed up with file system backup.

- Windows Backup utility [Windows 2003 only]

        - Can only backup Microsoft Information Store entirely or individual storage groups—databases cannot be backed up individually.
        - When restoring, you'll have to enter a temporary location for log and patch files. If this is the last restore set, enable "last restore set . . ." so the log files will be replayed. After that's enabled, you can enable "mount database after restore."

- Recovery Storage Group

    - From EMC → Toolbox → Disaster recovery tools/Database Recovery Management . . .
    - When creating a RSG, you must link it to an existing production SG. Only databases from the linked SG can be mounted in the RSG.
    - Once a RSG is linked, a Windows Backup restore actually gets intercepted and restored to the RSG instead of the linked production SG.

VIDEO 11: Configure High Availability

- HA means application accessibility to users, not just uptime. Not the same as DR. DR is a backup to HA.
- **Local Continuous Replication (LCR) [database redundancy only]**
    - Only requires one server.
    - Asynchronous log shipping and replay.
    - Dual storage groups—one is active, the other is passive. Should use separate storage controllers.
    - Initial LCR setup copies database from active SG to passive SG. After that, logs are replicated to passive SG after they're committed to the active SG. This means it's not 100% real-time.
    - Requires manual failover.
    - LCR is implemented at the SG-level, and the source SG can only contain one database.
    - From EMC → Server Configuration → Mailbox → select SG → Actions pane: Enable LCR
        - Point *system files path*, *log files path*, and *database file path* to the dedicated LCR drive.
        - LCR-enabled SGs have an arrow on their icons.
- **Cluster Continuous Replication (CCR) [database AND server redundancy—this is the ideal option]**
    - Requires two severs configured in a cluster. Uses asynchronous log shipping and replay, just like LCR, but with two servers, one being active and hosting the production storage group and the other being passive and having a copy of the storage group. Logs are copied from active node to passive node.
    - Quorum should be implemented as a majority node set (MNS) with file share witness. You can use a Hub Transport server to host the Witness File Share and point both nodes to that share.
    - Supports automatic failover.
    - Transport Dumpster is located on Hub Transport. It retains mail that it sends to the active node so that the passive node can ask for them in the event of failover. This will allow the passive node's database to be as close to 100% of the active node as possible.
    - Requirements:
        - Two servers (does not need to be identical or cluster certified).
        - Two NICs on each server (one for public and one for private/heartbeat)
        - Two hard drives on each node.
        - If using Windows Server 2003 Ent Ed SP1, must install KB92118 or SP2 for file share witness functionality.
        - Shared folder for witness file share. Recommended to be on Hub Transport server.
    - CCR Install Overview (on Windows Server 2003 Ent Ed SP1)
        - Create cluster on active node, using cluster service account. Add that service account to each node's local Administrators group and domain Exchange Server Administrators.
        - Add second node.
        - Point nodes to MNS file share.
        - On active node, do a custom install of Exchange and choose *Active Clustered Mailbox Role.*

        - On passive node custom install of Exchange and choose *Passive Clustered Mailbox Role*.
    - MS Cluster Service setup (on Windows Server 2003 Ent Ed SP1)
        - On active node, start Cluster Administrator and create new cluster.
        - Give the cluster a name and select the first node. Give the cluster an IP address.
        - Enter cluster service account credentials.
        - Quorum button → select *Majority Node Set* (instead of *Local Quorum*).
        - On passive node, start Cluster Administrator and join it to the new cluster.
        - Create witness folder and share on Hub Transport.
        - On active cluster, run cmd to point the MNS file share to the Hub Transport:

          ```
          cluster res "Majority Node Set" /priv MNSFileShare=\\Hub_Transport\MNS_FSW
          ```

- **Single Copy Clusters (SCC) [server redundancy only]**
    - Same as Ex2003 two-node active/passive cluster with shared storage, hence "single copy."
    - Quorum is on shared storage—does not use MNS.

VIDEO 12: Understanding Message Transport

- Two default SMTP Receive Connectors in EMC → Server Configuration → Hub Transport.
    - *Client <ServerName>*
        - Uses port 587 for receiving mail from all non-MAPI clients for SMTP relay.
    - *Default <ServerName>*
        - Uses port 25 for receiving mail from other hub transport servers, edge transport servers, or directly from Internet [via PAT/NAT of course].
- No Send Connectors by default, so you need to manually set these up. Send Connectors are under EMC → Organization Configuration → Hub Transport → Send Connectors
    - You must explicitly configure a send connector for outbound to the Internet (either directly from Hub or via Edge).
    - If configuring a send connector to an Edge Transport server, first export an Edge Subscription file from the Edge Transport and then import it into the Hub Transport. The file will contain all the necessary configuration information.
- Receive and Send Connectors between Hub Transport servers within the same Exchange org are configured automatically and dynamically. This allows all internal servers to exchange mail.
- The Transport Pipeline
    - All received mail → Submission Queue → Categorizer →
    - Ways to submit mail
        - Store Driver [*Microsoft Exchange Mail Submission* service]
            - Submits mail from Mailbox server to Hub Transport servers
        - Receive Connector
            - SMTP from other servers/clients using the default Receive Connectors.
        - Pickup Directory [Folder for properly formatted *.eml files]
- Even messages sent between mailboxes on the same Mailbox server still go through a Hub Transport.
- AD Site Connections
    - Exchange uses AD site link costs for mail routing. You can override this through a cmdlet. [The author was not very detailed or clear on this topic.]

VIDEO 13: Troubleshoot Message Transport

- EMC → Toolbox → Mail Flow Tools/*Mail Flow Troubleshooter* → select a symptom to get suggested solutions
    - Handles NDRs, queue backups, slow deliveries
    - This tool basically does an end-to-end Exchange health check of the message transport pipeline and might find that an Exchange service on a particular server isn't running, for example. It also shows an *Information Items* tab with details about a particular Exchange server.
- EMC → Toolbox → Mail Flow Tools/*Message Tracking*
    - Enabled by default on Hub Transport servers to log the routing of messages. [Per MS: A unique message tracking log exists on each computer that has the Hub Transport server role, the Mailbox server role, or the Edge Transport server role installed. Logs are stored in *C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking* as text files with .LOG extension.]
    - With the search results, you can select a specific one to get a more detailed search query.
- EMC → Toolbox → Mail Flow Tools/*Queue Viewer*
    - You can see the status of a message. [The queue now uses an ESE database instead of flat files. The database is named *mail.que* and is in *C:\Program Files\Microsoft\Exchange Server\TransportRoles\data\Queue* along with the logs, checkpoint, tmp.edb, and reserved logs. You can move these files for performance reasons.]
- Protocol Logging
    - Disabled by default. Used on Send and Receive Connectors to record SMTP conversations.
    - Saved as CSV text files with .LOG extension in *C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\ProtocolLog* in either *SmtpReceive* or *SmtpSend* folders.
    - To enable, go to the send or receive connector properties → General tab → change *protocol logging level* from *None* to *Verbose* (those are the only two options).
        - For receive connectors go to EMC → Server Configuration → Hub Transport → *Client <ServerName>* and *Default <ServerName>*
        - For send connectors go to EMC → Organization Configuration → Hub Transport. → Send Connectors → <specific send connector>

VIDEO 14: Configuring Your Edge Transport Role

- Server cannot be part of production AD domain that Hub Transport is a member of. Can only be in separate DMZ domain or stand-alone workgroup.

- Must install *ADAM (Active Directory Application Mode)* and same prerequisites as regular Exchange server. [In Windows Server 2008, ADAM was renamed to Active Directory Lightweight Directory Services (AD LDS)].

- Edge Transport role is the only Exchange role that can be installed.

- [For the Edge Transport role, you must assign the server a primary DNS suffix if it's not in an AD domain. The Edge role requires the server to have a FQDN, which requires a DNS suffix. You must verify that the Hubs and Edges can resolve each others hostnames via their respective DNS servers, otherwise they won't be able to communicate. You might have to manually add a new zone or record in each DNS (preferred), or use host files (not preferred).]

- Inbound TCP/IP ports required from *Internet* to external NIC of Edge Transport server:
    - 25 TCP

- Inbound TCP/IP ports required from *internal* network to *internal* NIC on Edge Transport server:
    - 25 TCP
    - 50389 TCP for LDAP local connection to ADAM
    - 50636 TCP for Secure LDAP for EdgeSync from Hub to Edge
    - 3389 TCP for RDP (optional for server administration)

- EdgeSync
    - Configures one-way replication of AD data from Hub Transport to Edge Transport to allow ADAM on Edge Transport to have a subset of AD data (recipient and Exchange org configuration data).

    1. Create an XML subscription file from the Edge Transport server.
        - EMS: `New-EdgeSubscription -File "C:\Edge-Sub.xml"`
        - The file has configuration sections for the following: *EdgeServerName*, *EdgeServerFQDN*, *EdgeCertificateBlob*, *ESRAUsername*, *ESRAPassword,* et al. [Since the file has a lot of security information, you should protect it with care. There's actually a time limit of a few hours until the XLM file expires.]
    2. Copy the XML subscription file to a Hub Transport server and set up the subscription.
        - EMC → Organization Configuration → Hub Transport → Edge Subscriptions tab → New Edge Subscription from actions pane.
            - Identify the AD site that the Edge Transport server will be assigned to. [This is the site that the Hub Transport server is in. The Edge Transport serve is subscribing to membership in that AD site so that all Hub Transport servers in that AD site will use it for routing external mail. The subscription is not Hub Transport server-specific.]
            - Browse to open the Edge Subscription XML file.
            - Notice that the checkbox *"Automatically create a Send connector for this Edge Subscription"* is already enabled. [Note that any Hub Transport server within the AD site can use this new Edge Transport server. So this new subscription is not specific to just one Hub Transport server—it's for use by all HTs in the same AD site.]

    - There's a service running on the Hub Transport servers named *Microsoft Exchange EdgeSync* that's responsible for synchronizing AD data to the Edge Transport server.

- You can run this EMS cmdlet to force a synch: `Start-EdgeSynchronization`. This is a good way to see if the configuration is correct since you'll get status output.
- On the Edge server, run the Security Configuration Wizard (SCW) to lock it down.
  - Install SCW via add/remove Windows components.
  - Register Exchange Edge Transport role SCW extensions: `scwcmd register ...`
    - *Exchange2007Edge.xml* or *Exchange2007Edge_WinSrv2008.xml*
  - Create SCW security policy → Select *Exchange 2007 Edge Transport* role . . . open up specific ports below . . . then apply policy
    - 25 TCP (internal and external NICs)
    - 50389 TCP for LDAP local connection to ADAM (internal NIC only)
    - 50636 TCP for Secure LDAP for EdgeSync (internal NIC only)

[Per this article: In Exchange 2007, Setup creates a self-signed certificate. By default, TLS is enabled. . . When you subscribe an Edge Transport server to the Exchange organization, the Edge Subscription publishes the Edge Transport server certificate in Active Directory for the Hub Transport servers to validate. The Microsoft Exchange EdgeSync service updates ADAM with the set of Hub Transport server certificates for the Edge Transport server to validate.]

VIDEO 15: Finalizing Edge Transport

- Create a postmaster mailbox to receive NDRs and delivery status notifications, per RFC 2822
    - Run EMS cmdlet `Get-TransportServer` to see if a postmaster address exists by looking at the *ExternalPostmasterAddress* column. If the column is blank, a postmaster mailbox will need to be created.
    - Run EMS cmdlet `Set-TransportServer <TransportServerName> -ExternalPostmasterAddress <ExternalPostmasterSMTPAddress>`

      If you had only Hub servers, then you'd need to do this on the HT servers.

      [The postmaster address actually has a default already, so you only need to do this if you want to change it to something other than *postmaster@<your-external-SMTP-domain.com>*. See this link for details. Make sure that whatever you use as the address is associated with a real mailbox by adding it as an alias to an existing mailbox or creating a new mailbox for it.]
- DNS settings
    - You need to create a host record in your internal AD DNS for the Edge server. This is because the Edge is not a member of your internal AD domain, so it won't automatically register itself. Your Hubs need to be able to find the Edge by its FQDN.
    - For all accepted domains, their external DNS MX records must point to [the NAT'd/PAT'd IP address of] the Edge server.
- Anti-spam, Receive and Send Connectors, Transport Rules, Accepted Domains, Address Re-writing
- EMC → Edge Transport → <EdgeServer> → Accepted Domains tab
    - You can configure inbound accepted domains and have them delivered internally within the Exchange org, relayed internally to another AD forest/Exchange org, or relayed externally.
- Address Re-writing
    - Used in large organizations with multiple sub-domains or after mergers.
    - On Edge, run EMS cmdlet `Get-TransportAgent` to verify that all transport agents are running.
        - Verify that *Address Rewriting Inbound Agent* or *Address Rewriting Outbound Agent* is enabled
        - Run cmdlet `Get-AddressRewriteEntry` to see existing entries.
        - Run cmdlet `New-AddressRewriteEntry` to add new entries.

VIDEO 16: Configuring Anti-Spam

- Connection Filter is a transport agent that runs on Edge or Hub server. It's the first level of defense.
    - *IP Allow List* and *IP Block List*
        - Checks specific IP address or range of incoming SMTP connection and allows or blocks based on list entry.
    - IP Allow List Provider (Safe Provider List whitelist)
    - IP Block List Provider (Realtime Block List blacklist)
- Sender Filtering
    - Blocks individual senders, blank senders, or entire domains.
    - Actions: reject or stamp message (stamping flags the message so that filters further on down the chain are aware of it).
- Recipient Filtering
    - Blocks e-mails sent to specific recipients in your org.
    - Action: reject
- Sender ID Filtering
    - Purported Responsible Address (PRA) check queries sender's DNS to verify that sending SMTP IP address is authorized for sending domain. Sender Policy Framework (SPF) records on DNS servers identify authorized outbound SMTP servers.
    - Actions: reject, delete, or stamp message
- Content Filtering
    - Assigns Spam Confidence Level (SCL) to messages based on their content
        - 0 (not spam) through 9 (spam)
        - *Content Filter Agent* is updated regularly from MS.
        - Actions based on SCL: delete, reject, or quarantine (goes to spam mailbox).
- To configure these settings, go to EMC → Edge Transport → Anti-spam tab.
    - Connection Filtering (four components)
        - *IP Allow List*
        - *IP Block List*
            - For the IP Block List, you can add a host/subnet and optionally assign the block an expiration date and time.
        - *IP Allow List Provider*
            - Add providers by domain name. Settings for return status codes and mask and responses will be provided by the provider.
            - You can add multiple providers and disable specific providers.
        - *IP Block List Provider*

        - Same settings as Allow List but includes options to add custom error message and recipient exceptions.

- *Sender Filtering*
    - Can block individual address and domain (with default option to include all sub-domains)
    - Block messages from blank senders.
    - Actions: reject (default) or stamp message with result and continue processing.
- *Recipient Filtering*
    - Block messages sent to recipients not listed in GAL
        - If this is on Edge, EdgeSync must be working so that Edge has copy of GAL.
    - Block the following recipients:
        - Used to add commonly abused addresses such as *postmaster* and *helpdesk*.
- *Sender ID*
    - If Sender ID check fails, there are three selectable actions:
        - Reject
        - Delete
        - Stamp message with result and continue processing (default). Be careful changing this because not all sending organizations have Sender ID configured.
- *Sender Reputation* collects information about recent e-mail message received and adds sender's IP address to *IP Block List* if sender displays spammer characteristics
    - Sender Confidence tab
        - Perform an open proxy test . . . (enabled by default)
    - Action tab
        - Sender Reputation Level Block Threshold
            - Set from 0 to 9 (default is 7)
        - Threshold Action
            - If threshold is exceeded, adds sender IP address to IP Block List for *n* hours (default is 24)
- *Content Filtering*
    - Custom Words tab
        - Add words and phrases that are allowed or blocked. Messages with both allowed words/phrases and blocked words/phrases will be allowed through.
    - Exceptions tab
        - Add recipients to exclude from content filtering.
    - Actions tab

        - Delete messages that have an SCL rating greater than or equal to *n*.
            - Not enabled by default.
        - Reject messages that have an SCL rating greater than or equal to *n*.
            - Enabled by default with n = 7.
        - Quarantine messages that have an SCL rating greater than or equal to *n*.
            - Not enabled by default. You have to specify a mailbox e-mail address if you enable this.

- Attachment filtering must be configured and viewed from EMS
    - `Get-AttachmentFilterEntry` shows list of all content types and filename extensions.
    - To add a new filename extension, such as .xyz123:
        - `Add-AttachmentFilterEntry –Name *.xyz123 –Type Filename`
    - `Set-AttachmentFilterListConfig` configures parameters such as actions
        - Default action is to strip attachment
- Enabling Ant-Spam Option on Hub Transport server
    - You should only enable this if you aren't using an Edge Transport server
    - From Hub server, run `Install-AntispamAgents.ps1` to install the following agents on the *Microsoft Exchange Transport* service (this service must be restarted for agents to take effect):
        - Connection Filtering Agent
        - Content Filter Agent
        - Sender Id Agent
        - Sender Filter Agent
        - Recipient Filter Agent
        - Protocol Analysis Agent
        - [Note that Attachment Filtering Agent doesn't get installed on the hub.]
    - Configure settings from EMC → Organization Configuration → Hub Transport → Anti-spam tab.

VIDEO 17: Analyze and Monitor Exchange 2007

- EMC → Tools → Configuration management tools/**Best Practices Analyzer**
    - o Can analyze entire Exchange org.
    - o Picks a default GC, but you can change that.
    - o If the account you're running ExBPA with doesn't have the appropriate permissions, you need to select *show advanced login options* and provide credentials for each of the following:
        - For AD, an account with "computer administrator"-level permissions to each GC.
        - For Exchange, an account with at least *Exchange administrator View Only* permissions at the org level and local server admin on each Exchange server.
    - o ExBPA will query a GC for Exchange org information.
    - o Select the scope of the scan: org, admin group, specific servers, or some combination of the three scopes.
    - o Five types of scans: Health Check (default), Permission Check, Connectivity Check, Baseline, and Exchange 2007 Readiness Check.
    - o [Note that you can download ExBPA for use on a non-Exchange server.]
- EMC → Tools → Disaster recovery tools/**Database Recovery Management**
    - o Manage Database
        - Analyze log drive space
        - Repair database
        - Show database related event logs (shows entries in application log)
        - Verify database and transaction logs
            - Database must be dismounted to run this. The database status should show as "Clean Shutdown" if there are no issues.
    - o Manage Recovery Storage Group (or create one)
- EMC → Tools → Disaster recovery tools/**Database Troubleshooter**
    - o Checks event log for database events.
- Two command line tools:
    - o ESEUtil
        - Database defrag, check database integrity, repair damaged database
    - o ISInteg
        - Tests IS and fix errors.
- EMC → Tools → Performance tools/**Performance Monitor**
    - o Automatically includes most important Exchange counters.
- EMC → Tools → Performance tools/**Performance Troubleshooter**

- Only used for troubleshooting one server at a time.
- Three RPC-related symptom options to select from. Used to identify causes for the “RPC Cancel Request” dialog box in Outlook.
- Collects performance data for analysis.

- Microsoft Operations Manager
  - Exchange 2007 Management Pack is free
    - Generates alerts for failures or thresholds.
    - Health checks, reporting, usage and reliability patterns, anti-spam reports, various metrics, service availability, etc.

VIDEO 18: A Look At Unified Messaging [not an exam topic]

- What is UM
    - o E-mail, fax (inbound only), and voice mail all get delivered to UM server, and then go to Hub Transport or Mailbox for delivery to end users.
    - o Requires IP/PBX or VOIP gateway that connects to legacy PBX
- UM features
    - o Voicemail: accessible via mobile, OWA, Outlook 2007 (has embedded player), play on phone via Outlook Voice Access.
    - o Faxes received in TIFF format.
    - o Configuration options: PINs, etc.
    - o Auto attendants: voice prompts and navigating menus through keypad or voice input
- Some telephony concepts
    - o Circuit switched network is a dedicated connection between two points for duration of call. (Phone)
    - o Packet switched network divides data units into packets for delivery and then reassembly. (Internet)
    - o Legacy PBX (private branch exchange) is used for switching calls in a circuit switched network. For example, a PBX would take 25 lines from the outside (trunk lines) for use by 100 internal users.
    - o IP PBX takes the same trunk line from the outside, but uses IP on a packet switched network (Ethernet LAN) for internal users. It can also take an IP trunk line.
    - o VOIP (voice over IP) is hardware and software that allows voice calls over IP network.
    - o IP/VOIP gateway is a third-party hardware device that connects legacy PBX to LAN.
- EMC → Organization Configuration → **Unified Messaging → UM Dial Plans** tab
    - o A dial plan is a grouping of unique phone extension numbers. To create one, you just need to provide a name and the number of digits in the extension numbers.
    - o After the dial plan is created, there are several tabs and options such as:
        - *General* tab: allow users to receive faxes
        - *Subscriber Access* tab: welcome greeting and information announcement (you can select a custom WAV file for these)
        - *Dial Codes* tab: outside line access code (such as 9), international access code, etc.
        - *Features* tab: allow callers to transfer to users, allow callers to send voice message, callers can contact . . .
        - *Settings* tab: dial by name primary method and secondary method, audio codec, misc timeouts, etc.
        - *Dialing Rule Groups* tab
        - A UM Mailbox Policy is automatically created for each dial plan.
- EMC → Organization Configuration → **Unified Messaging → UM IP Gateways** tab
    - o Enter the IP address or FQDN of the gateway.

- Select a dial plan. A default hunt group will be created to associate the gateway to the dial plan.
- There aren't many properties for the gateway or hunt group.
- Hunt groups are groupings of lines. Multiple IP gateways can be assigned to one hunt group.

- EMC → Organization Configuration → **Unified Messaging → UM Mailbox Policies** tab

  A mailbox policy is automatically created for each dial plan

  - *General* tab: maximum greeting duration, allow missed call notifications
  - *Message Text* tab: text sent when a UM mailbox is enabled, text sent when a PIN is reset, text included with a voice message, text included with a fax message.
  - *PIN Policies* tab: minimum PIN length, PIN lifetime, allow common patterns in PIN, failed logon options.
  - *Dialing Restrictions* tab: allow calls to users within the same dial plan, allow calls to extensions, etc.

- EMC → Organization Configuration → **Unified Messaging → UM Auto Attendants** tab
  - Each auto attendant is associated with a dial plan.
  - You can assign an extension number(s) for the auto attendant.
  - Must select option to enable newly created AA.
  - Can create AA as speech-enabled with DTMF (dual-tone multi-frequency) failback.
  - *Greetings* tab: You can enabled/disable various greetings and select customized WAV files.
  - *Times* tab: select the business hours (default is always run), time zone, and create a holiday setting for each holiday start and end date with a customizable greeting.
  - *Features* tab: Similar to Features tab in dial plan.
  - *Key Mapping* tab: has options for mapping keys (or phrases, if speech-enabled) to actions. There are settings for business hours and non-business hours key mappings.

- EMC → Server Configuration → **Unified Messaging** has a few options, but not much at this level.

- EMC → Recipient Configuration → Mailbox
  - You can right-click on a mailbox and select *Enable Unified Messaging* and assign to a mailbox policy, automatically generate or manually enter a mailbox extension, automatically generate or manually enter a PIN and require user reset at first logon.
  - After this is enabled, an automated e-mail notification with PIN will be sent to the user (based on text in UM mailbox policy).

VIDEO 19: Troubleshooting Your Exchange Environment

- Scenarios
    - Individual user issues could be local user computer issues, not connectivity.
    - Group of users on same mailbox server could be issue with mailbox server.
    - Group of users in same site/subnet could be issue with network, DNS, or AD.
    - Group of users in different sites could be major issue.
- Solutions
    - Find out what type of client it is—MAPI, OWA, Outlook Anywhere, POP3/IMAP4, Outlook 2003 or 2007?
        - Outlook 2003 would most likely be MB role; Outlook 2007 could be CAS and/or MB role also.
        - What's the issue? Can't logon, or can get mail but can't send?
        - Issues with OWA or ActiveSync could be caused by IIS and CAS. Is the device compatible with ActiveSync or ActiveSync policies?
        - Outlook Anywhere (RPC/HTTP) issues could be something with firewall.
        - POP3/IMAP4: Are the server services set up and configured properly? Are the clients' settings correct?
- Network tools: PING, TELNET, RPC PING, IPConfig
- DNS/AD tools: NSLookup, Event Viewer, DCDiag
- Diagnostic Logging
    - Diagnostic logging logs entries to the application log. There are five logging levels: Lowest | Low | Medium | High | Expert.
    - `Get-EventLogLevel` displays all Exchange services/processes and their logging level (most are set to lowest by default).
    - To get information on a specific service, such as *MSExchangeFDS*, type `Get-EventLogLevel MSExchangeFDS`. This would display the logging levels for all the services/processes under that—there are two for this service.
    - To change the logging level for everything within *MSExchangeFDS*, pipe the Get command to a Set command:

      `Get-EventLogLevel MSExchangeFDS | Set-EventLogLevel –Level High`.
    - If you have an issue with a specific service, you can increase its logging level for troubleshooting.
- Services Applet
    - Verify that MS Exchange services are started. POP3 and IMAP4 are not started by default.
- Microsoft Exchange Troubleshooting Assistant
    - This opens up when you use a tool such as EMC → Toolbox → Mail Flow Troubleshooter
    - No matter which tool opened up ExTA, you can select a different tool from within ExTA by clicking on *Select a task* from the left pane. Some of the other tools are *Performance Troubleshooter*, *Database Troubleshooter*, and *Message Tracking*.

    - You can download and install ExTA onto a non-Exchange server and use it for troubleshooting.

- Exchange Management Shell
    - `Get-MailboxServer | FL` outputs details about MB server into a formatted list
    - `Get-ClientAccessServer | FL` does the same for CAS

- Exchange Management Shell `Test` cmdlets
    - `Get-Command *Test*` displays a list of all the test cmdlets relevant to the sever role(s):
    - `Test-MAPIConnectivity` tests MAPI connectivity to each database and displays status along with latency time in ms.
    - `Test-ServiceHealth` displays status of all the required services for each active role on the server
    - For the two commands above, you can append `-Server <ServerName>` to test a specific server
    - `Test-SystemHealth` runs a comprehensive test and displays warnings in yellow and errors in red.

VIDEO 20: Using PowerShell

- You can change the PS window size, font, etc., just like you can with a cmd.exe window.
- EMS runs on top of PS. Standard cmd.exe commands can also be run from within PS.
- Use `Help <command>` to get help on the specific command.
- To search for a command with a specific string, use `Get-Command *<search-string>*`
- If you type a partial command, use the tab key to go through list of full commands. This is a nice shortcut.
- `Get-` is used to get info and `Set-` is used to modify
- For *some* cmdlets, if you don't provide all the parameters, PS will prompt for the parameters [instead of throwing an error like batch files or VBS].
- Pipelining allows output from one command to be used as input for another command.
    - Use `| FL` to pipe the output into a formatted list. Use `| FT` for formatted table. [In most cases, the formatted list actually shows you more details.]
- Add `–WhatIf` to the end of any command to see a list of actions that would be taken *if* the command executed.
- Add `–Confirm` to the end of any command to get prompted to perform each action.
- Add `> C:\some-file.txt` to the end of any command to direct its output to a specific file, just like in DOS.
- Add `| ConvertTo-HTML | Set-Content C:\some-file.html` to the end of any command to convert the output to HTML and save it as a file.
- Default Exchange PS scripts can be found in *C:\Program Files\Microsoft\Exchange Server\Scripts*.
- You make your own PS scripts by adding commands to a text file and saving it with a *.PS1* extension. [For security, you can't execute a .PS1 script directly—you have to execute it from within PS. If you save your scripts in the default directory mentioned, you can execute the script within EMS. For example, if you created a script named *my-first-ps1.PS1*, you can execute it from within ESM by typing just *my-first-ps1* without the extension.]

VIDEO 21: Skills Measured by Exam 70-236

- I skipped this since it will be outdated, and I have the Transcender practice exams anyway. Go here for current exam info.

My Misc Notes:

- Modification of the default Ex2007 routing and administrative groups is not supported (don't add or remove any servers from them).

- Regarding redundancy and load balancing: On CAS use NLB. On Edge, use either NLB or DNS round robin.

- Piping a cmdlet to | FL not only displays the output in a different format, but can display more info than without | FL.

- New DGs must be Universal.

- Clusters require Two Windows 2003 Server R2 Enterprise Editions or Windows 2003 Server SP1 Enterprise Editions (note the editions and SP level).

- If Exchange Server 2007 is installed in an existing org, existing Exchange servers must be at least Exchange Server 2003 SP2 or Exchange Server 2000 SP3 + rollup.

- Sector-align disk if necessary, using DiskPart

- For most tasks (such as setup) you'll need to connect to a DC that is at least Windows 2003 Server SP1. Not all DCs have to be at that level though.

—End of Document—

