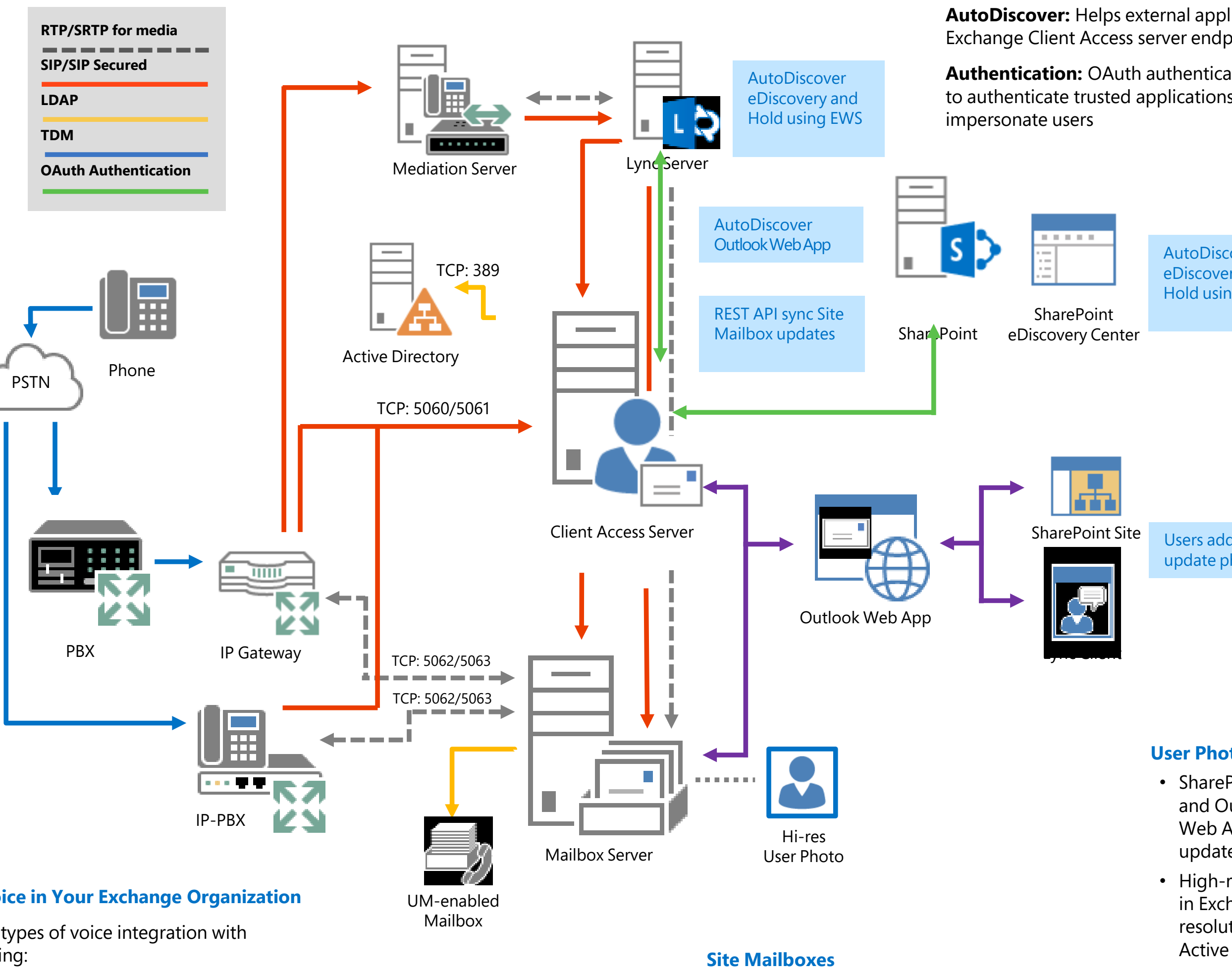
Microsoft Exchange Server 2013 Service Pack 1 Architecture Overview

Exchange Integration with Unified Messaging, Lync and SharePoint



AutoDiscover: Helps external applications discover Exchange Client Access server endpoints

Authentication: OAuth authentication used to authenticate trusted applications and impersonate users

Integrating Voice in Your Exchange Organization

There are three types of voice integration with Unified Messaging:

- With a legacy PBX and VoIP gateway. VoIP gateway translates TDM protocols to VoIP protocols
- With an IP enabled PBX (IP PBX). The IP PBX translates the TDM protocols to VoIP protocols
- With Lync Server. An advanced IP gateway and Mediation server translate the TDM protocols into VoIP protocols

SharePoint eDiscovery Center

- Perform eDiscovery searches across SharePoint 2013 sites, documents, and file shares; Exchange Server 2013 mailboxes; and Lync 2013 archived conversations and meetings stored in Exchange 2013
- Place an In-Place Hold on Exchange 2013 mailboxes and SharePoint 2013 sites
- OAuth authentication (service and user impersonation)
- Uses Exchange 2013 Role-Based Access Control (RBAC) permissions for eDiscovery searches from SharePoint 2013
- Multi-Mailbox Search API to search mailbox content
- Preview search results
- Export eDiscovery search results (from Exchange) to PST file(s) with appropriate metadata stored in EDRM XML

Site Mailboxes

- Functionally comprised of SharePoint 2013 site membership (owners and members), shared storage through an Exchange 2013 mailbox for email messages and a SharePoint 2013 site for documents, and a management interface that addresses provisioning and lifecycle needs
- AutoDiscover to determine CAS endpoints
- OAuth authentication (service and user impersonation)
- Site Mailboxes provisioned and managed from SharePoint 2013
- SharePoint Team Site documents displayed in Site Mailboxes in Outlook 2013
- Inbox messages can be read from SharePoint 2013
- REST (Representation State Transfer) API used to synchronize updates from SharePoint to Site Mailbox over HTTPS

User Photos

- SharePoint 2013, Lync 2013 client, and Outlook 2013 use the Outlook Web App Options page to add or update user photos
- High-resolution user photos stored in Exchange 2013 mailbox; Low-resolution user photos stored in Active Directory
- User photos accessed by Outlook Web App, Outlook, SharePoint 2013, and Lync 2013

Lync Archiving

- Archives Lync 2013 conversations and meetings in Exchange 2013 mailboxes
- OAuth authentication
- Archive conversations using EWS
- Compliance management (Hold and eDiscovery)
of Lync content using Exchange 2013
- Unified Contacts Store, with Lync 2013 contacts stored in Exchange 2013 mailbox

Client Access Server

A thin, stateless front end server that provides a unified namespace, authentication, and network security as well as proxy and redirection logic. Transport is provided by the Front End Transport service which provides mailbox locator services.

In addition, the Client Access Server:

- Houses the logic to proxy or redirect a specific protocol request from a client to the correct Mailbox server
- Is designed to work with TCP affinity (Layer 4)—does not require session affinity (Layer 7)
- Provides an SMTP Front End proxy and a UM call router
- Handles all inbound and outbound external SMTP traffic via Front End Transport Service and provides a client endpoint for SMTP Traffic

The Client Access server provides network security functionality such as Secure Sockets Layer (SSL) and client authentication, and manages client connections through redirection and proxy functionality. The Client Access server authenticates client connections and, in most cases, will proxy a request to the Mailbox server that houses the currently active copy of the database that contains the user's mailbox. In some cases, the Client Access server might redirect the request to a more suitable Client Access server, either in a different location or running a more recent version of Exchange Server.

Client Access Protocols

Outlook Connectivity

In Exchange 2013, RPC/TCP has been removed and Outlook connections take place via Outlook Anywhere (RPC over HTTP). This provides several benefits:

- Simplifies the protocol stack
- Provides a reliable and stable connectivity model
- Maintains the RPC session on the Mailbox server that hosts the active copy of the user's mailbox, there by eliminating the need for the RPC Client Access Array and its namespace

MAPI over HTTP is a new communication protocol available in Exchange 2013 SP1 and Outlook 2013 SP1 and later. It improves the reliability and stability of Outlook and Exchange connections by removing the dependency on RPC. This allows a higher level of visibility of errors and enhanced recoverability due to the overall reduction in complexity. Additional functionality includes support for explicit pause-and-resume, which enables supported clients to change networks or resume from hibernation while maintaining the same server context.

Exchange ActiveSync

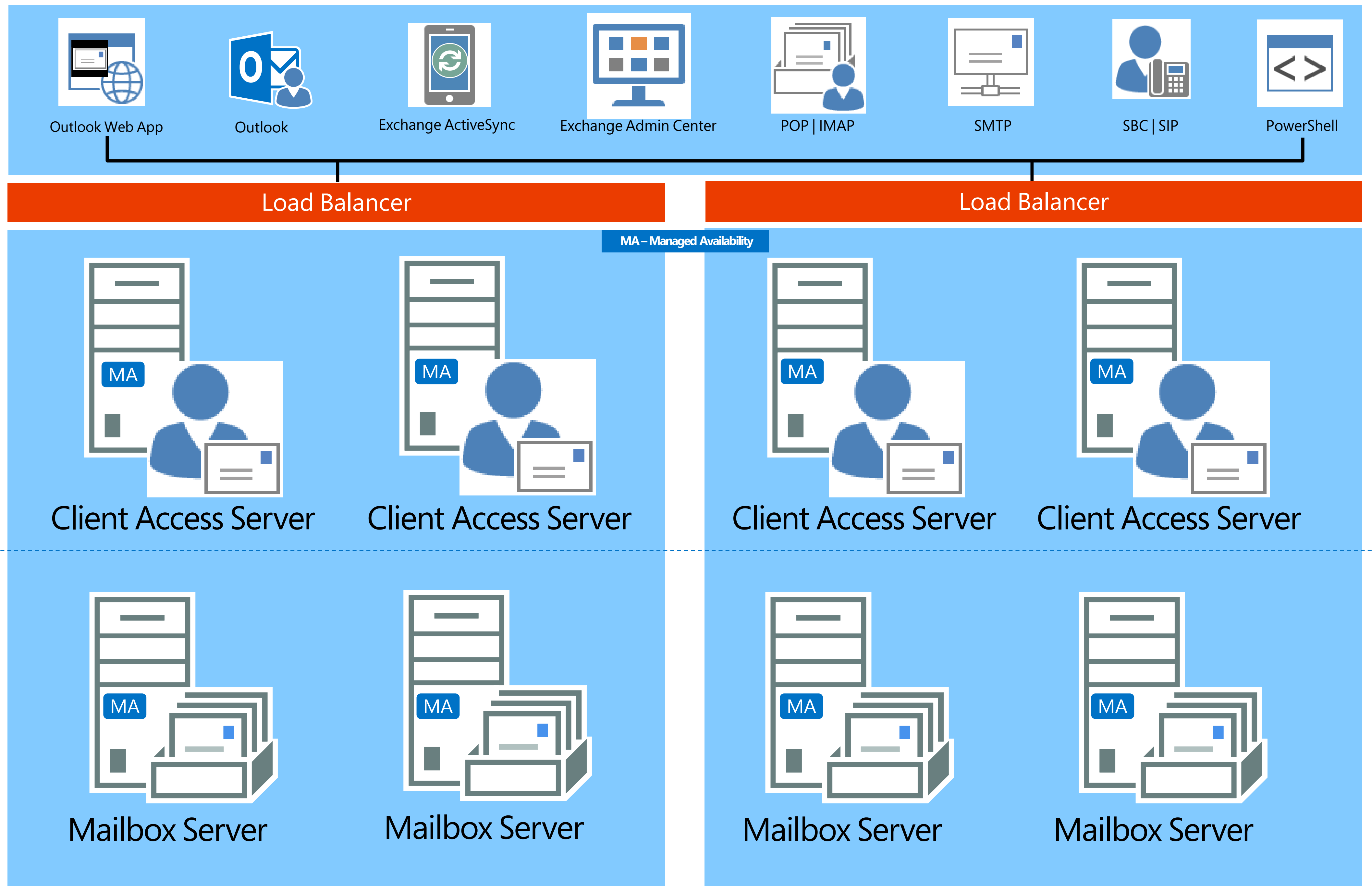
- Allow/Block Quarantine List
- Approved device list (by device type or by user)
- Block an unsupported device
- Quarantine and notify
- Configure multiple mobile device mailbox policies
- PIN policies and local device wipe
- Remote device wipe

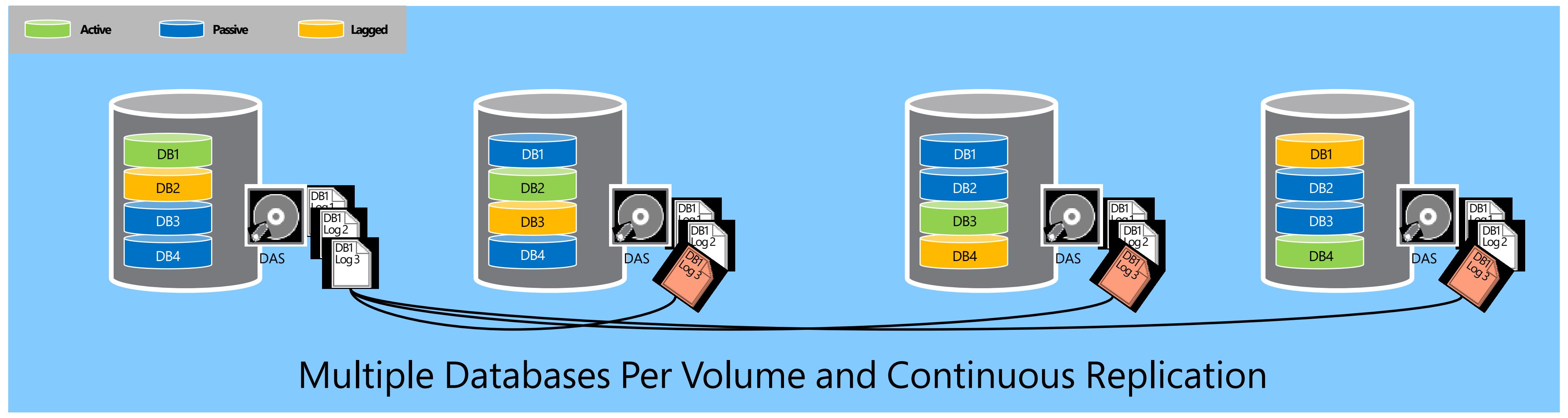
Exchange Web Services

- Exchange Web Services (EWS) provides the functionality to implement client applications that access and manipulate Exchange store items
- EWS provides programmatic access to the data stored within Exchange
- EWS clients can integrate Exchange information into line-of-business (LOB) applications
- SOAP provides the messaging framework for messages sent between the client application and the Exchange server
- The Managed API provides an easy way to use the Microsoft .NET interface with EWS

Outlook Web App

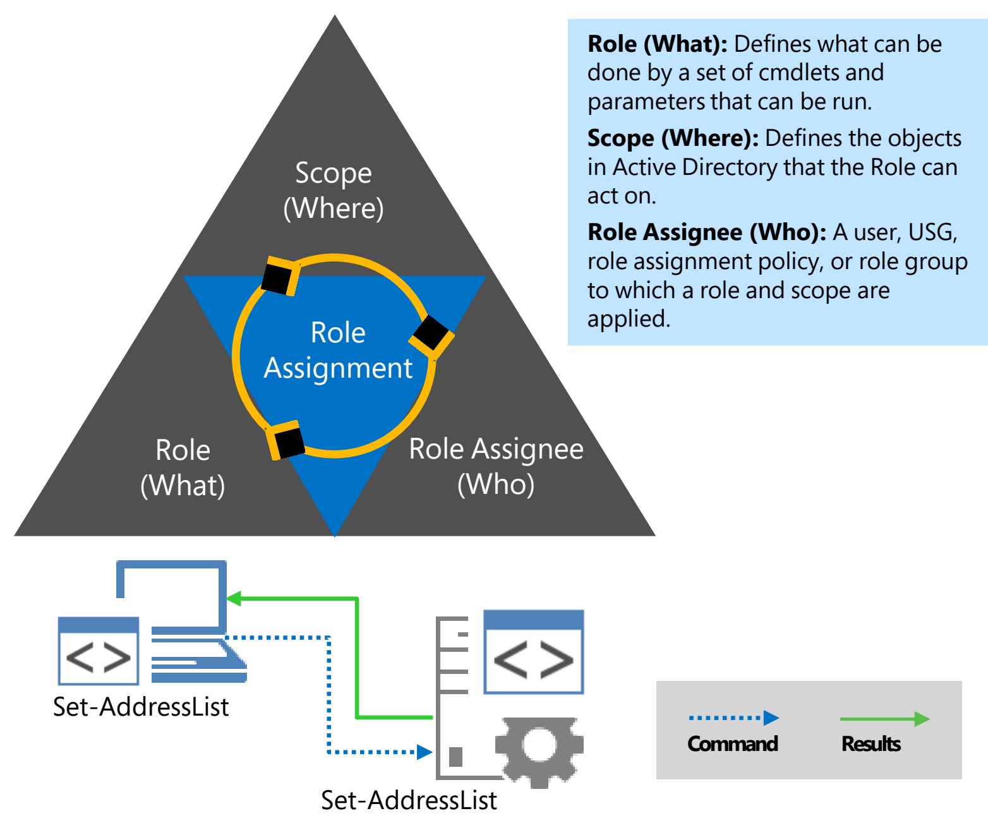
- Redesigned for Exchange 2013
- New user interface that focuses on content
- Supports all major Web browsers
- Enhanced contacts and calendaring functionality including Agenda view
- New Offline Mode
- Three views for Outlook Web App in the browser:
  - Phone view (1-column touch UI)
  - Tablet view (2-column touch UI)
  - Traditional Desktop view (3-column mouse-based UI)
- Inline reply for Desktop view
- Extensibility Improvements Apps, such as the Bing Maps apps for Outlook add features to the overall experience





Multiple Databases Per Volume and Continuous Replication

PowerShell and Management



Role (What): Defines what can be done by a set of cmdlets and parameters that can be run.

Scope (Where): Defines the objects in Active Directory that the Role can act on.

Role Assignee (Who): A user, USG, role assignment policy, or role group to which a role and scope are applied.

Remote PowerShell

- Exchange Server 2013 takes advantage of Windows Management Framework 3.0, which includes PowerShell v3.0 and Windows Remote Management
- All Exchange management tools are built on Remote PowerShell
- Remote PowerShell extends PowerShell from servers to client computers so commands can be executed remotely
- Remote PowerShell enables administrators to run Exchange cmdlets on computers without needing to install Exchange management tools

Role Based Access Control

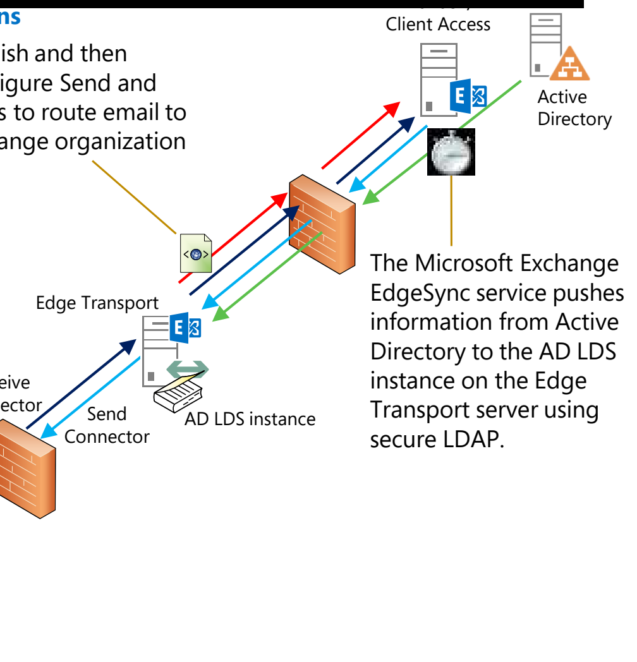
Role Based Access Control (RBAC) enables you to control, at both broad and precise levels, what administrators and users can do. RBAC also enables you to more closely align roles you assign users and administrators with the actual roles they hold within your organization. RBAC is built into all management tools. Configuration is done using Exchange management tools, with dozens of default roles pre-configured and easily customizable.

Three ways of assigning permissions:

- Management Role Groups
- Management Role Assignment Policies
- Direct User Role Assignment

Edge Subscriptions

Run once to establish and then automatically configure Send and Receive connectors to route email to and from the Exchange organization and the Internet.

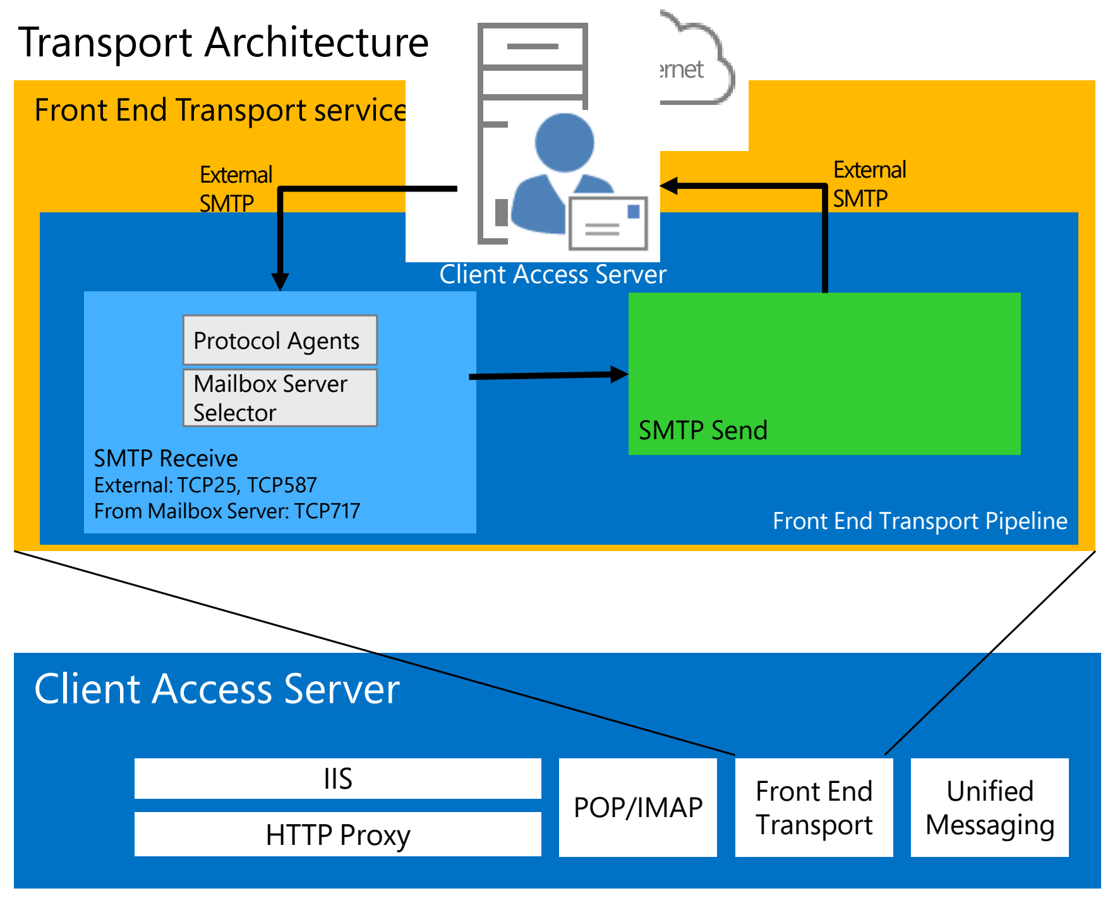


The Microsoft Exchange EdgeSync service pushes information from Active Directory to the AD LDS instance on the Edge Transport server using secure LDAP.

Edge Transport Server

Edge Transport servers minimize the attack surface by handling all Internet-facing mail flow, which provides SMTP (Simple Mail Transfer Protocol) relay and smart host services for your Exchange organization. Edge Transport servers are installed in a perimeter network, and are never a member of your organization's internal Active Directory forest. However, the Edge Transport server requires data that resides in Active Directory. This data is synchronized to the Edge Transport server by the Microsoft Exchange EdgeSync service (EdgeSync). EdgeSync is a collection of processes on an Exchange 2013 Mailbox server to establish one-way replication of recipient and configuration information from Active Directory to the Active Directory Lightweight Directory Services (AD LDS) instance on the Edge Transport server. EdgeSync performs scheduled updates so the information in AD LDS remains current.

Transport Architecture



Front End Transport Service

The Front End Transport service on the Client Access server proxies incoming and outgoing SMTP message traffic. The Front End Transport service quickly selects a single healthy Mailbox server to receive an incoming SMTP message transmission regardless of the number, type, or location of the message recipients.

Message transmissions between the Transport service on different Mailbox servers occur when the Mailbox servers are in different delivery groups. A delivery group is a way to generalize mail routing to help improve efficiency and attempt to deliver a message as close to its destination as possible. A delivery group could be:

- A database availability group
- An Active Directory site
- A connector source server
- A distribution group expansion server

A Send connector on the Mailbox server is specifically configured to route outbound mail through the Client Access server.

If the Client Access and Mailbox server roles are not co-located, Edge Transport servers bypass the Client Access server and communicate directly with the Transport service on the Mailbox server.

Mailbox Server

Mailbox databases, and the components previously associated with other Exchange Server 2007/2010 server roles (Unified Messaging, Client Access, Hub Transport) are hosted on the Mailbox server. All processing for a specific mailbox happens on the Mailbox server that hosts the active copy of the user's mailbox. Client connectivity takes place through the Client Access server.

In-Place Archive

- Provides users with an alternate storage location to store historical messaging data
- Appears below the user's primary mailbox in Outlook or Outlook Web App
- Search across primary and archive mailboxes in Outlook and Outlook Web App
- Sets archive quota separately from primary mailbox
- Exchange Online Archiving provides a cloud-based archive for on-premises mailboxes

In-Place Hold and Litigation Hold

- Query-based In-Place Hold on specific items in a mailbox-based query (keywords)
- Time-based In-Place Hold retains items for a specified duration
- Litigation Hold can also be used to place an indefinite or time-based hold on the user's mailbox

In-Place eDiscovery

- Enables use of the NEAR operator, allowing you to search for a word or phrase that's in proximity to another word or phrase
- Enhanced management experience and search query improvement
- Preserves the results of the query which allows for scoped immutability across mailboxes
- Federated discovery using the SharePoint eDiscovery Center allows you to search and preserve data across Exchange, SharePoint, and Lync
- Using Exchange 2013 only, you can create a discovery search using the Exchange Admin Center or the Exchange Management Shell
- Primary and Archive mailboxes are searched, including items in the Recoverable Items folder

Recoverable Items Folder

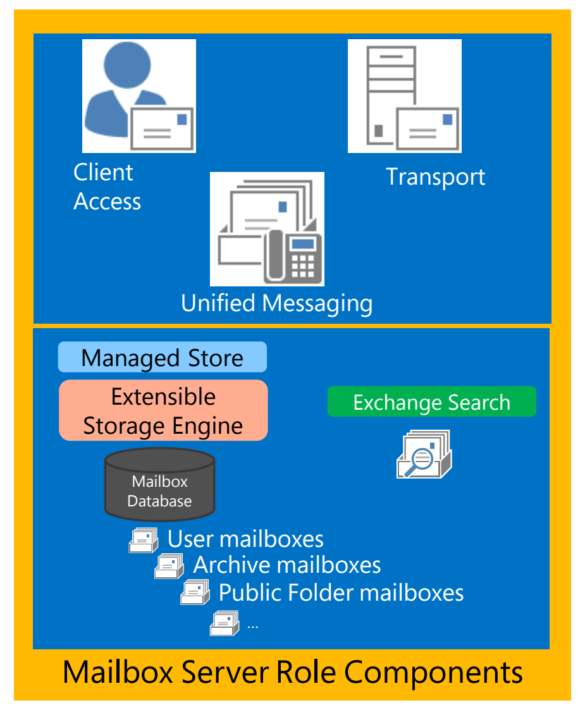
These folders are not visible to the user. They include the Audits sub-folders, which contain mailbox audit and calendar logging entries.

- **Deletions**: Items soft-deleted from Deleted Items folder. Accessed through Outlook "Recover Deleted Items"
- **Versions:** Original and modified copies of items when either In-Place Hold or Single Item Recovery are enabled
- **Purges:** Hard-deleted items when either In-Place Hold or Single Item Recovery are enabled
- **Discovery Holds:** Data that matches the In-Place Hold criteria is saved to this folder

Types of Mailboxes

There are several types of mailboxes in Exchange 2013:

- **Arbitration:** Used for handling moderated recipients and distribution group membership approval
- **Archive:** Used as a secondary mailbox for users
- **Discovery Search:** Used to store results from an In-Place eDiscovery search
- **Equipment:** Used for resources that are not location specific, such as a portable computer, projector, microphone, or a company car
- **Room:** Used with room-based solutions, such as Lync Room Systems
- **Linked:** Used for users in a separate, trusted forest
- **Public Folder:** Used for public folders and public folder content
- **User:** User for typical user to send, receive and store messages, appointments, tasks, notes, and documents



Mailbox Server Role Components

Managed Store

The Managed Store is the name of the newly rewritten Information Store processes in Exchange 2013. The new Managed Store is written in C# and tightly integrated with the Microsoft Exchange Replication service (MSExchangeRepl.exe). It leverages the worker process model and a static database caching algorithm to provide higher availability through improved resiliency.

Exchange Search

Exchange Search is different from full-text indexing available in previous versions of Exchange Server. Exchange Search includes numerous innovations in performance, content indexing, and search. New items are indexed in the transport pipeline or almost immediately after they're created or delivered to the mailbox, providing users with a fast, stable, and more reliable way of searching mailbox data. Content indexing is enabled by default, and there's no initial setup or configuration required.

The underlying content indexing engine has been replaced with Microsoft Search Foundation, which provides performance and functionality improvements and serves as the common underlying content indexing engine in Exchange 2013 and SharePoint 2013.

Managed Availability

Both Exchange 2013 server roles include a new monitoring and high availability feature known as Managed Availability.

Managed Availability includes three main asynchronous components that are constantly doing work. Administrators remain in control with the ability to configure server-specific and global overrides.

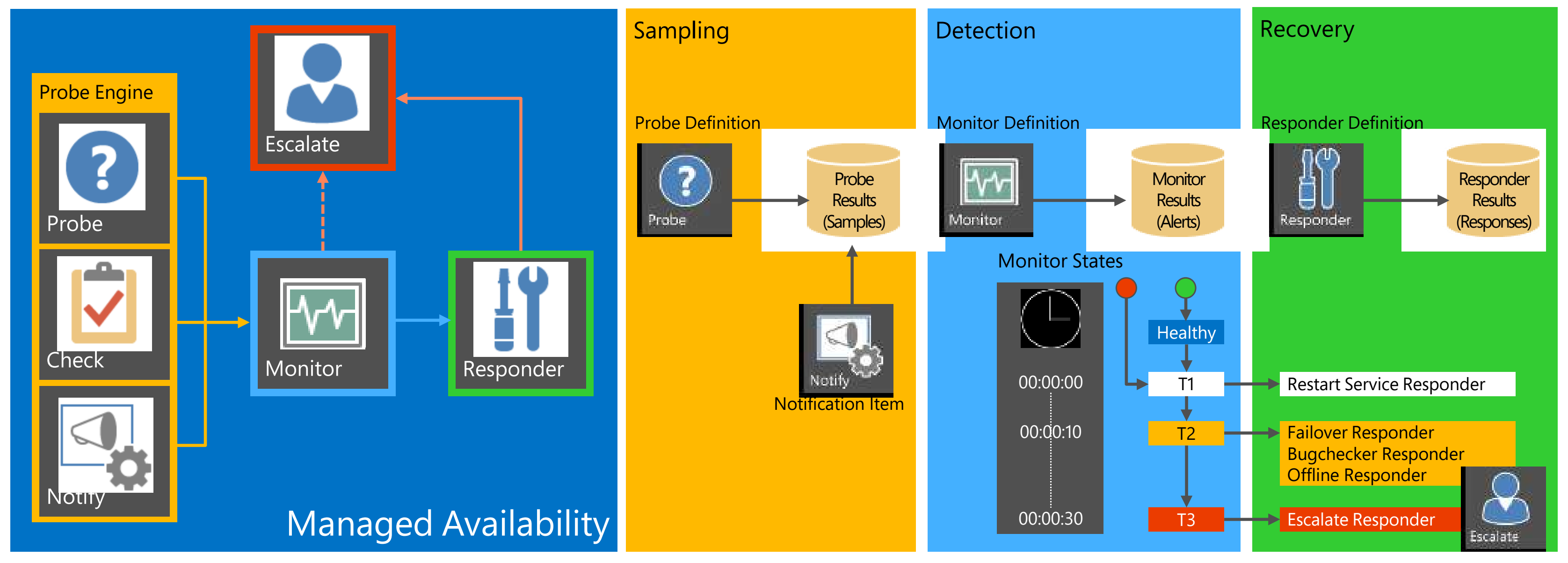
Probe Engine: Responsible for taking measurements on the server and collecting the data; results of those measurements flow into the monitor.

Monitor: Contains business logic used by the system to determine whether something is healthy, based on the data that is collected and the patterns that emerge from all collected measurements.

Responder Engine: Responsible for recovery actions. When something is unhealthy, the first action is to attempt to recover that component via multi-stage recovery actions that can include:

- Restarting an application pool
- Restarting a service
- Restarting a server; and
- Removing a server from service

If recovery actions are unsuccessful, Managed Availability escalates the issue to a human through event log notifications.



Multiple Databases Per Volume

Exchange 2013 is optimized so that it can use large disks multi-terabyte disks in a JBOD configuration more efficiently. With multiple databases per disk, you can have the same size disks storing multiple database copies, including lagged copies. The goal is to drive the distribution of users across the number of volumes that exist, providing you with a symmetric design where during normal operations each DAG member hosts a combination of active, passive, and optional lagged copies on the same volumes. Another benefit of using multiple databases per disk is that it reduces the amount of time to restore data protection in the event of a failure that necessitates a reseed (for example, disk failure).

AutoReseed

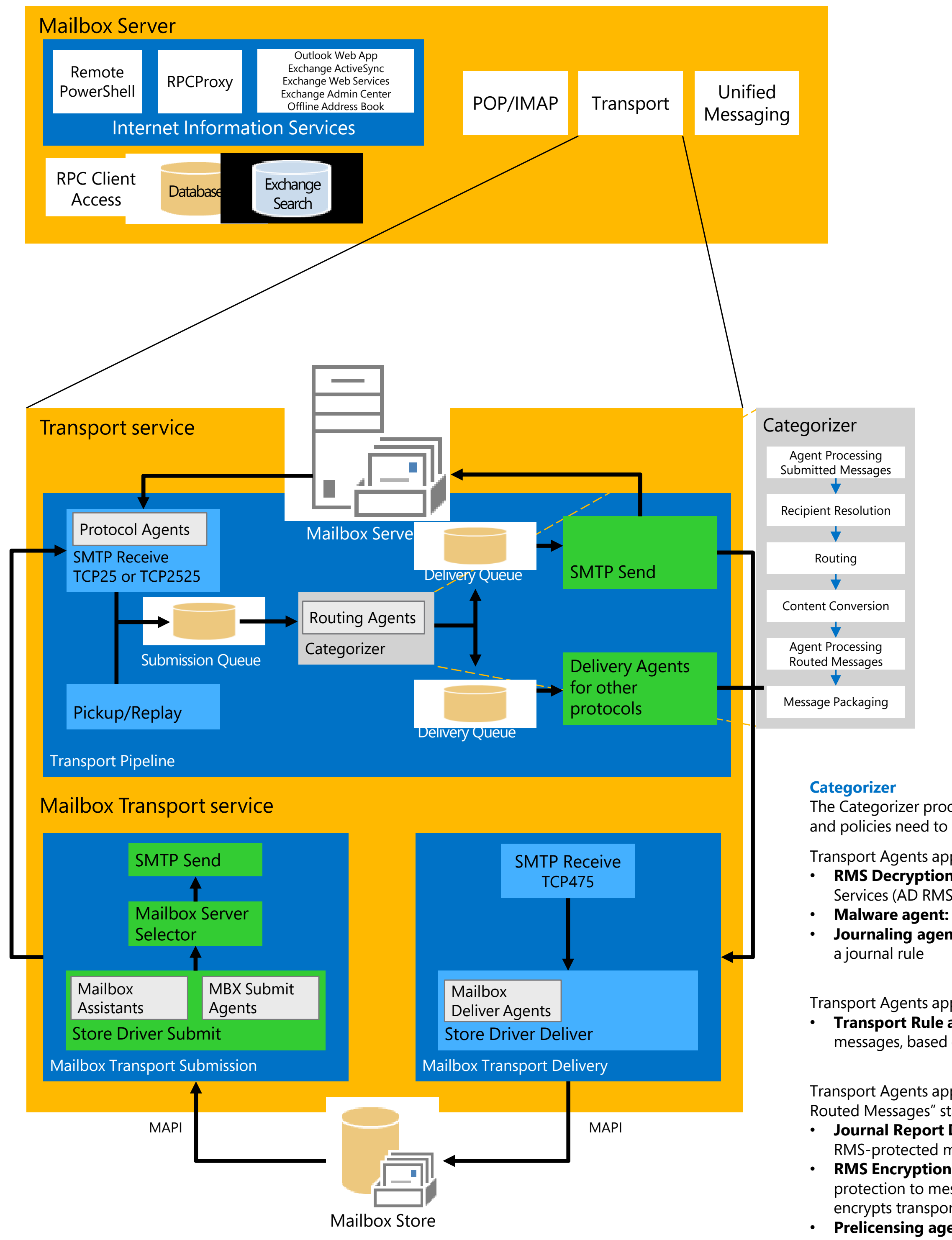
AutoReseed is designed to automatically restore database redundancy after a disk failure by using spare disks that have been provisioned on the system. In the event of a disk failure where the disk is no longer available to the operating system, or is no longer writable, a spare volume is allocated by the system, and the affected database copies are reseeded automatically.

DAGs without Administrative Access Points

Exchange 2013 SP1 supports creating a DAG without a cluster administrative access point as a new optional configuration. Creating a DAG without an AAP reduces the complexity of your DAG and simplifies DAG management.

High Availability Message Flow

1. A Mailbox server receives a message from any SMTP server that's outside the Transport high availability boundary. The Transport high availability boundary is a DAG or an Active Directory site in non-DAG environments.
2. Before acknowledging receipt of the primary message, the primary Mailbox server initiates a new SMTP session to a shadow Mailbox server within the Transport high availability boundary and makes a shadow copy of the message. In DAG environments, a shadow server in a remote Active Directory site is preferred.
3. The primary server processes the primary message and delivers it to users within the Transport high availability boundary or relays it to the next hop. The primary server queues a discard status for the shadow server that indicates the primary message was successfully delivered, and the primary server moves the primary message into the local Primary Safety Net.
4. The shadow server periodically polls the primary server for the discard status of the primary message.
5. When the shadow server determines the primary server successfully delivered the primary message or relayed it to the next hop, the shadow server moves the shadow message into the local Shadow Safety Net.
6. The message is retained in the Primary Safety Net and the Shadow Safety Net until the message expires.



Principles of Transport High Availability

- Messages in transit are redundantly persisted before their receipt is acknowledged to the sending SMTP server
- Redundant copies of messages processed by Transport are kept in Safety Net for resubmission in the event of a mailbox failover, and Safety Net itself is made redundant on another server
- Message resubmissions due to queue database loss or mailbox database failover are fully automatic and do not require any manual intervention

Transport Service

The Transport Service on the Mailbox server is responsible for all mail flow inside the organization. It's also where DLP rules, transport rules, journaling policies, and Information Rights Management policies are applied.

Anti-Malware: The Malware Agent is enabled by default in the Transport service on Mailbox servers to help protect the organization from malware and other unwanted content.

Anti-Spam Agents in Transport: All built-in anti-spam agents are disabled by default, but they can be enabled by running a PowerShell script. The following anti-spam agents are available in the Transport service on a Mailbox server:

- Content Filter agent
- Sender ID agent
- Sender Filter agent
- Protocol Analysis agent for sender reputation filtering

Note: The Connection Filtering agent, the Attachment Filtering agent and the Recipient Filter agent are available on Edge Transport servers.

Mailbox Transport Service

The Mailbox Transport Service on the Mailbox server is the broker between the Transport service and the mailbox databases. The Mailbox Transport service communicates directly with local mailbox databases using RPC, and with the Transport service on local and remote Mailbox servers using SMTP.

Categorizer

The Categorizer processes all email messages and determines what rules and policies need to be applied based on the final recipient of the message.

Transport Agents applied at "Agent Processing Submitted Messages" stage:

- **RMS Decryption agent:** Decrypt Active Directory Rights Management Services (AD RMS) protected messages
- **Malware agent:** Provides built-in anti-malware protection
- **Journaling agent:** Generates a journal report when a message matches a journal rule

Transport Agents applied at "Recipient Resolution" stage:

- **Transport Rule agent:** Apply transport rules and DLP policies to messages, based on the specified conditions

Transport Agents applied at "Content Conversion" and "Agent Processing Routed Messages" stages:

- **Journal Report Decryption agent:** Decrypt journal reports that contain RMS-protected messages
- **RMS Encryption agent:** Applies Information Rights Management protection to messages flagged by the Transport Rules agent and re-encrypts transport-decrypted messages
- **Prelicensing agent:** Requests an AD RMS Usage License on behalf of the recipient
- **Journaling agent:** The Journaling agent is also applied here so modified messages can't bypass the Journaling agent

Poster Feedback: eapf@microsoft.com

Not all listed features are compatible with legacy versions of Exchange, SharePoint or Lync