**What's new in Exchange 2013**

**Integrate with SharePoint and Lync**:

**Help meet evolving compliance needs**

## Exchange admin center

**Secure the ECP virtual directory: y**ou can partition access from the Internet and intranets from within the ECP IIS virtual directory to allow or disallow management features

**Public Folder management**: Public folders are now in the EAC, and you don't need a separate tool to manage them.

**Role Based Access Control (RBAC) User Editor**

## Exchange 2013 architecture

server roles in Exchange 2007 and Exchange 2010 were tightly coupled. The tight coupling of the roles had several downsides including version dependency, geo-affinity (requiring all roles in a specific site), session affinity (requiring expensive layer 7 hardware load balancing), and namespace complexity.

the primary design goal for Exchange 2013 is for simplicity of scale, hardware utilization, and failure isolation. With Exchange 2013, we reduced the number of server roles to three: the Client Access, Mailbox, and Edge Transport server roles.

The Mailbox server includes all the traditional server components found in Exchange 2010: the Client Access protocols, Transport service, Mailbox databases, and Unified Messaging. The Mailbox server handles all activity for the active mailboxes on that server. The Client Access server provides authentication, limited redirection, and proxy services. The Client Access server itself doesn't do any data rendering. The Client Access server is a thin and stateless server. There is never anything queued or stored on the Client Access server. The Client Access server offers all the usual client access protocols: HTTP, POP and IMAP, and SMTP.

The Exchange 2013 architecture provides the following benefits:

* **Version upgrade flexibility**: No more rigid upgrade requirements. A Client Access server can be upgraded independently and in any order in relation to the Mailbox server.
* **Session indifference:** inbound connections to Client Access servers to be balanced using techniques provided by load-balancing technology like least connection or round-robin. Client Access server simply proxies all connections for a user to a specific Mailbox server, no session affinity is required
* **Deployment simplicity**: With an Exchange 2010 site-resilient design, you needed up to eight different namespaces: two Internet Protocol namespaces, two for Outlook Web App fallback, one for Autodiscover, two for RPC Client Access, and one for SMTP. A legacy namespace was also required if you were upgrading from Exchange 2003 or Exchange 2007. With Exchange 2013, the minimum number of namespaces drops to two. If you're coexisting with Exchange 2007, you still need to create a legacy hostname, but if you're coexisting with Exchange 2010 or you're installing a new Exchange 2013 organization, the minimum number of namespaces you need is two: one for client protocols and one for Autodiscover. You may also need an SMTP namespace.

As a result of these architectural changes, there have been some changes to client connectivity.

* RPC is no longer a supported direct access protocol. This means that all Outlook connectivity must take place using RPC over HTTP (also known as Outlook Anywhere)
* Outlook clients no longer connect to a server FQDN as they have done in all previous versions of Exchange. Outlook uses Autodiscover to create a new connection point comprised of mailbox GUID, @ symbol, and the domain portion of the user's primary SMTP address.
* The DAG still uses Windows Server failover clustering. Continuous replication still supports both file mode and block mode replication
* Now, each database runs under its own process, allowing for isolation of store issues to a single database

## Managed Store

* The Managed Store works with the Microsoft Exchange Replication service to manage mailbox databases, which continues to use Extensible Storage Engine (ESE) as the database engine
* Microsoft Exchange Replication service is responsible for all service availability related to Mailbox servers. The architectural changes enable faster database failover and better physical disk failure handling.

## Certificate management

* Certificate management can be performed on the Client Access server or the Mailbox server. The Mailbox server has a self-signed certificate installed by default. The Client Access server automatically trusts the self-signed certificate on the Exchange 2013 Mailbox server

## Messaging policy and compliance

* Data loss prevention (DLP) capabilities help you protect your sensitive data and inform users of internal compliance policies. DLP can also help keep your organization safe from users who might mistakenly send sensitive information to unauthorized people
* Microsoft Rights Management connector (RMS connector) is an optional application that helps you enhance data protection for your Exchange 2013 server by connecting to cloud-based Microsoft Rights Management services

## In-place Archiving, retention, and eDiscovery

* **In-Place Hold**: is a new unified hold model that allows you to meet legal hold requirements
* **In-Place eDiscovery:** allows authorized users to search mailbox data across all mailboxes and In-Place Archives in an Exchange 2013 organization and copy messages to a discovery mailbox for review

## Auditing

* **Auditing reports**: The EAC includes auditing functionality so that you can run reports or export entries from the mailbox audit log and the administrator audit log.

## Anti-malware protection

* All messages sent or received by your Exchange server are scanned for malware (viruses and spyware). If malware is detected, the message is deleted. Notifications may also be sent to senders or administrators when an infected message is deleted and not delivered. You can also choose to replace infected attachments with either default or custom messages that notify the recipients of the malware detection.

## Mail flow

* **Transport pipeline**: The transport pipeline in Exchange 2013 is now made up of several different services: the Front End Transport service on Client Access servers, the Transport service on Mailbox servers, and the Mailbox Transport service on Mailbox servers.
* **Routing**: Mail routing in Exchange 2013 recognizes DAG boundaries as well as Active Directory site boundaries. Also, mail routing has been improved to queue messages more directly for internal recipients.
* **Connectors**: The default maximum message size for a Send connector or a Receive connector, as specified by the MaxMessageSize parameter, has been increased from 10MB to 25MB.

## Recipients

* **Group naming policy**: Administrators can now use the EAC to create a group naming policy, which lets you standardize and manage the names of distribution groups created by users in your organization. You can require a specific prefix and suffix be added to the name for a distribution group when it's created, and you can block specific words from being used.
* **Message tracking**: Administrators can also use the EAC to track delivery information for email messages sent to or received by any user in your organization

## Batch mailbox moves

 Ability to move multiple mailboxes in large batches.

 Email notification during move with reporting.

 Automatic retry and automatic prioritization of moves.

 Primary and personal archive mailboxes can be moved together or separately.

 Option for manual move request finalization, which allows you to review a move before you complete it.

## High availability and site resilience

Exchange 2013 uses DAGs and mailbox database copies, along with other features such as single item recovery, retention policies, and lagged database copies, to provide high availability, site resilience, and Exchange native data protection.

* **Managed availability**: With managed availability, internal monitoring and recovery-oriented features are tightly integrated to help prevent failures, proactively restore services, and initiate server failovers automatically or alert administrators to take action
* **Automatic reseed**: Enables you to quickly restore database redundancy after disk failure. If a disk fails, the database copy stored on that disk is copied from the active database copy to a spare disk on the same server.
* **Automatic recovery from storage failures**:
* **Lagged copy enhancements**: Lagged copies will automatically play down log files in a variety of situations, such as single page restore and low disk space scenarios. If the system detects that page patching is required for a lagged copy, the logs will be automatically replayed into the lagged copy to perform page patching.