One of the many new changes with Exchange Server 2013 is the collapsing of the four roles that made up Exchange Server 2007 and 2010; the fifth role, the Edge Transport role, has been dropped completely from 2013. Similar to the Front End/Back End topology of Exchange 2003, there are now two roles in Exchange Server 2013: the Mailbox Server and the Client Access Server (CAS).

**Client Access Server Key Features**

The CAS in 2013 combines pieces of the older CAS role, as well as pieces of the previous Hub Transport (role). Clients still make their initial connections to the CAS role and are authenticated, but unlike the 2007/2010 CAS, no data rendering occurs on the CAS. Instead, the CAS either proxies the connection from the client to the mailbox server or redirects the client to the appropriate mailbox server.

To facilitate this process, the Exchange Server 2013 CAS no longer uses RPC for Outlook connections, and instead uses HTTP or HTTPS, better known as Outlook Anywhere. POP and IMAP are also still supported.

Another new feature of the Exchange Server 2013 CAS is that it is now stateless and no data is actually stored on the CAS server. This means that a load balancer no longer requires session affinity.

As noted in the Exchange Team Blog Exchange 2013 [Client Access Server Role](#):

From a protocol perspective, the following will happen:

1. A client resolves the namespace to a load balanced virtual IP address.
2. The load balancer assigns the session to a CAS member in the load balanced pool.
3. CAS authenticates the request and performs a service discovery by accessing Active Directory to retrieve the following information:
   1. Mailbox version (for this discussion, we will assume an Exchange 2013 mailbox)
   2. Mailbox location information (e.g., database information, ExternalURL values, etc.)
4. CAS makes a decision on whether to proxy the request or redirect the request to another CAS infrastructure (within the same forest).
5. CAS queries an Active Manager instance that is responsible for the database to determine which Mailbox server is hosting the active copy.
6. CAS proxies the request to the Mailbox server hosting the active copy.
**Things To Keep In Mind**

The protocol used in step 6 depends on the protocol used to connect to CAS. If the client leverages the HTTP protocol, then the protocol used between the Client Access server and Mailbox server is HTTP (secured via SSL using a self-signed certificate). If the protocol leveraged by the client is IMAP or POP, then the protocol used between the Client Access server and Mailbox server is IMAP or POP.

Telephony requests are unique, however. Instead of proxying the request at step 6, CAS will redirect the request to the Mailbox server hosting the active copy of the user’s database, as the telephony devices support redirection and need to establish their SIP and RTP sessions directly with the Unified Messaging components on the Mailbox server.

As mentioned above, the new Client Access Server role also incorporates pieces of the Hub Transport role. This is done through a new service called the Front-End Transport service. This service handles all inbound and outbound external SMTP traffic and can be an endpoint for internal SMTP traffic. This service operates as a layer 7 proxy and has full access to the protocol conversation. Like the client protocols, the Front-End Transport service does not have a message queue and is completely stateless.

**Handling Incoming Email**

For incoming email, the Front-End Transport service must quickly find a single, healthy Mailbox server to receive the message, regardless of the number or type of recipients:

- For emails with a single mailbox recipient, it selects a Mailbox server in the target delivery group and gives preference to the Mailbox server based on the proximity of the Active Directory site
- For emails with multiple mailbox recipients, the service uses the first 20 recipients to select a Mailbox server in the closest delivery group, based on the proximity of the Active Directory site
- If the email has no mailbox recipients, the service selects a random Mailbox server in the local Active Directory site

**Outgoing Email**

For outgoing email, the Client Access Server, via the Front-End Transport service, is used as a proxy if the Mailbox server’s Send Connector has the FrontEndProxyEnabled property set.

Next Steps

Review our case studies and engagements where we helped companies just like yours solve a variety of business needs.

About Oakwood

Since 1981, Oakwood has been helping companies of all sizes, across all industries, solve their business problems. We bring world-class consultants to architect, design and deploy technology solutions to move your company forward. Our proven approach guarantees better business outcomes. With flexible engagement options, your project is delivered on-time and on budget. 11,000 satisfied clients can't be wrong.

Like what you've read? Please spread the word!