TIER 3 Best Practices Series

Microsoft Exchange Server 2010© in the Cloud

White Paper

A Step-by-Step Guide to Planning and Architecting Your Migration

Introduction

Microsoft Exchange Server 2010© offers a number of exciting new features, including breakthroughs to be an effective cloud-based email solution. Making the upgrade to Exchange Server 2010 in the cloud, however, is not a push-button process. Through real world examples and learning experiences, this paper will serve as your guide to decide which Exchange upgrade path is right for you, how to best approach each step of the upgrade process and what questions to ask to get the most out of your Exchange investment. This paper will guide you through real world experiences and the industry's most effective proven practices for success with Exchange in the cloud.

This paper will also help you make the decision if Exchange in the cloud is right for your business and, if yes, helping you get there. The Exchange cloud upgrade discussion is broken out into three core steps: First you'll need to decide on a deployment option. Will you go with a single server or multi-server deployment? This decision will affect your ability to scale. Then, there is configuration. Exchange Server 2010 gives you many new options for configuring your client, relays, public folders, and so on. Included are real world Exchange usage scenarios to help you decide which configuration approach best serves your particular business needs. Finally, you have the migration itself. Migrating to Exchange 2010 in the cloud can be a fairly involved process, though this paper will help you steer clear of a range of unnecessary challenges.

Through real world examples and learning experiences, this paper will serve as your guide to decide which Exchange upgrade path is right for you.

Contents

1. Benefits of Exchange Server 2010

Microsoft has done much to improve its already respected, world-leading email server. Compared to Exchange Server 2007, Exchange Server 2010 enables reduced deployment costs, simplified high availability and disaster recovery. Self-service support features decrease dependence on the help desk. From a user perspective, Exchange Server2010 offers an enhanced universal inbox experience that gives access to all business communications from a single location. Other key upgrades in functionality include:

- Backup, email archiving, mobile email, and voice mail with no need for third-party tools.
- New Inbox organization and prioritization features.
- Voice mail in the inbox with text preview.
- Simplified compliance with regulatory archiving policies and discovery procedures.
- Centrally managed and enforced information protection and control capabilities.
- Reduced risk of malware and spam through built-in defenses and support for third party security products.

2. Key Principles of the Exchange Server 2010 Cloud Upgrade

A set of key principles underlie the three core steps of choosing deployment options, configuring your Exchange Server 2010 cloud environment, and making the actual migration itself. Youroverall approach to making the Exchange Server 2010 upgrade is based on these principles, which are woven directly and indirectly into the three core steps.

- Scalability – Email is perhaps your most important business application. It needs to scale easily as your organization grows. Your Exchange 2010 up grade needs to take into account your anticipated scalability requirements.
- Availability – Email must be available to the greatest extent possible, with interruptions in service constituting a negligible amount of the user experience. Increasingly, this means enabling users to have persistent access to email from multiple device types and browsers. Your Exchange Server 2010 instantiation needs to be highly available.
- Cost effective system management – Your email budget is not unlimited. The Exchange Server 2010 instantiation you deploy to the cloud should be as cost effective as possible, given your specific requirements.
- License management – Licenses is a major cost factor in using Exchange. Your migration to Exchange Server 2010 in the cloud should enable efficient use of licenses and the ability scale licensing up or down as needed without financial penalties.
- Transparent transition – Ideally, your users should have only the slightest awareness that you are making a big change in the back end of the email system. The migration to Exchange Server 2010 in the cloud should be transparent to the end user and present no service interruptions.
- Backup – Email is precious in almost every organization. Data loss with email is catastrophic. Migrating to Exchange Server 2010 in the cloud should provide the opportunity for better, more efficient backup and restoration than you have with your current Exchange environment.
- Security – Email is a prime target for security threats. Your Exchange Server 2010 cloud instantiation needs to provide the highest possible level of security in terms of protection against malware, unauthorized use, eavesdropping, and so forth.
- Compliance – Government authorities have promulgated an increasingly complex array of regulations that affect the way you manage your email solution. Archiving and e-discovery requirements are two of many new rules that affect email systems. Exchange Server 2010 in the cloud must enable compliance with the regulations that affect your organization.

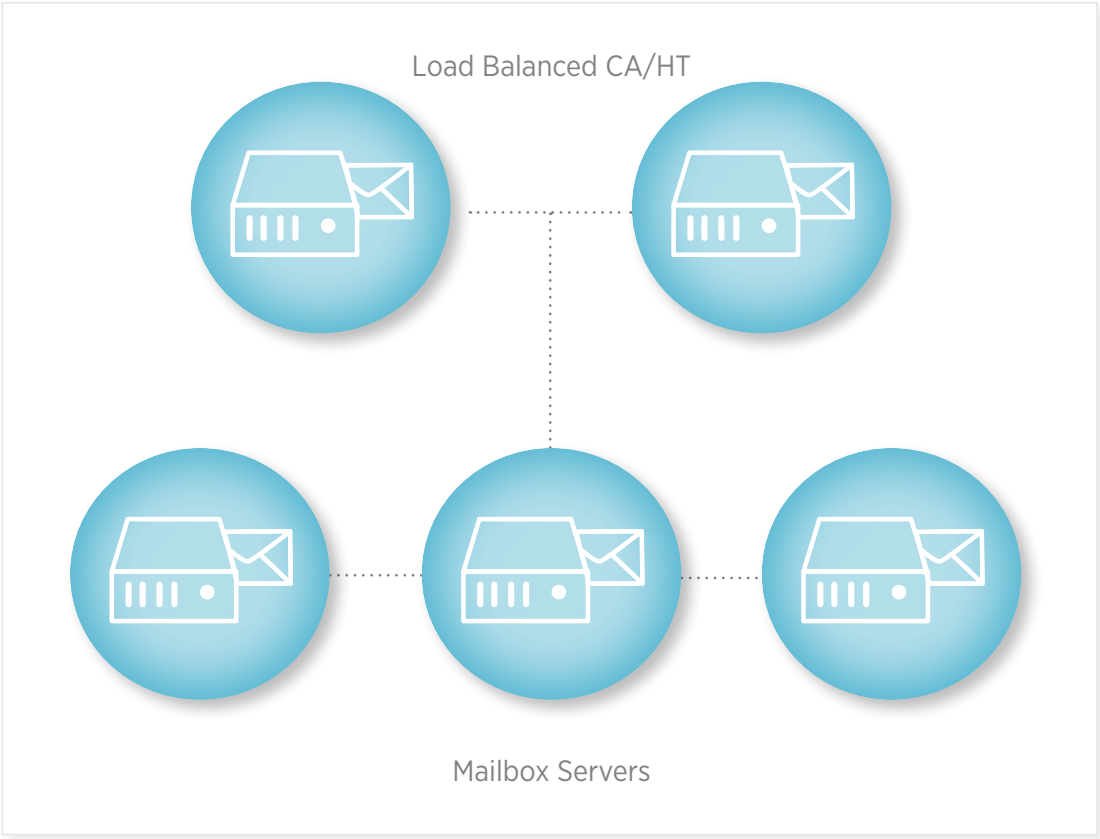
3. Architecture and Planning for Your Move

Moving to Exchange Server 2010 in the cloud involves making a number of architectural choices as you form your migration plan. These choices involve whether you are going to pursue a single or multi-server deployment, how to configure your Exchange cloud instantiation, and the way you migrate the solution itself.

3.1. Deployment Options (Single vs. Multi Server)

One of the most fundamental choices you face in making your upgrade to Exchange Server 2010 in the cloud is between single and multi-server deployment. The choice you make will have an impact on your ability to scale your solution and deploy Exchange Server 2010's new Data Availability Groups (DAGs). Of course, the single vs. multi-server choice also has a big impact on your overall cloud Exchange solution cost.

FULLY REDUNDANT



Reference architecture for a fully-redundant multi-server deployment of Exchange Server 2010 in the cloud.

> LOAD BALANCED CLIENT
> ACCESS AND HUB
>TRANSPORT SERVERS
> MULTIPLE DATABASE SERVERS
> PROTECTED WITH DAG

3.1.1. Scaling on the Cloud: Multiple Server

As organizations grow, IT costs increase and so does the need for "can't-go-down," business critical, redundant architecture. To be able to leverage the high availability technology built into Exchange Server 2010, it is important that the IT infrastructure that your Exchange instantiation is on, also has high availability capabilities built in. With these two elements in place, you can realize very high availability and ensure mail is up and running.

Using DNS load balancing and multiple Client Access/ Hub Transport servers ensure that email clients can always connect and mail keeps flowing.

SINGLE SERVER

Mailbox Server

Single server capabilities

> MAILBOX
> HUB TRANSPORT
> CLIENT ACCESS
> ROLES ALL ON 1 SERVER

Remember LCR, SCR, CCR and SCC from Exchange 2007? Did you have look up those acronyms every time you see them? Exchange 2010 does away with all of those and introduces a single simple high availability technology called Database Availability Groups (DAG). DAG is like clustering on the database level. If you lose a mailbox server or a database, DAG keeps passive copies of databases that can be automatically switched to "active" if needed. Outlook clients, using Autodiscover, will rediscover the new location of their mailbox and continue to function without interruption.

3.1.2. Scaling on the Cloud: DAG with Multi Zone

Exchange Server 2010 Database Availability Groups (DAG) are an effective way to ensure your users' mailbox databases are always online. The innovation of the DAG technology is that it also works across a WAN connection. A benefit of Exchange Server 2010 in the cloud is that with the right service provider, enterprise customers can take of multiple datacenters dispersed geographically, thereby distributing Exchange resources across locations to ensure that users' mailboxes are close to them and also that they remain available in the event of a server or even a datacenter outage.

3.1.3. Scaling on the Cloud: Single Server

While it's great to have multiple servers supporting a high availability environment, it's also expensive. Many mid-tier enterprises are seriously looking at deploying a single server solution in the cloud. And, why not? A single server in the cloud is quite different from a single on-premise server in terms of scalability and configuration. A best practice when choosing your cloud provider is to ask for redundancy built in with enterprise networking, multiple SAN's, daily backups and snapshots. In the cloud, it's not really just a single server after all. And, unlike a single server solution on-premise if you need to grow, you can dynamically increase processer, RAM and storage quickly and easily.

3.2. Configuration Best Practices

Exchange Server 2010 cloud configuration is where things can get interesting, and a little complicated, for email system managers. Exchange configuration has long been a bit of an art, and the cloud simply extends that art in a new direction. With configuration, proven best practices are absolutely essential for Exchange Server 2010 success in the cloud.

3.2.1. Client Configuration and Connection

Exchange Server 2010 increases the ability to stay connected. Outlook Web Access* has been rebranded as Outlook Anywhere* and more closely matches the feel and

functionality of Outlook. Exchange ActiveSync* has been improved and expanded to include support for more devices and more flexibility in the management of roles and features. This includes the ability to force a password and remotely wipe lost devices.

Autodiscover service and Outlook Anywhere can now more easily connect Outlook to Exchange Server securely and without having to know the name of the mail server. All that is required is the domain\username, email address and password.

Autodiscover service also helps ease the transition from older Exchange versions by automatically repointing Outlook to the new Exchange server after a mailbox move. This greatly reduces administration and makes the move seamless to the end user.

3.2.2. Current Configuration: User Count

Most hosted Exchange providers charge per mailbox. For a more cost effective solution, look for a service provider that only charges for the storage that is used. Often, client licensing is also available with this model, although you should be able to use your own Exchange licensing if you already have it. A good check of the current configuration is total database size, total number of mailboxes and any mailbox quotas. This way, the most accurate amount of storage can be allocated to meet the storage needs of the Exchange environment. The number of users is not relevant. This offers greater flexibility in environments of all sizes.

3.2.3. Current Configuration: Relay Needs

Your cloud service provider should offer the ability to use SMTP relay. SMTP relay may be needed in order to relay email messages sent from fax gateways, network appliances or custom applications (the most common type of relay). With a respectable SMTP relay, you will not be black-holed. An SMTP virtual server can be setup using IIS7 to relay these messages. For example, if a line-of-business application needs to send email alerts to a group of users, it can be relayed through your system and secured via Transport Layer Security (TLS)

3.2.4. Current Configuration: Active Directory

In order to install Exchange Server 2010 into a current infrastructure, certain Active Directory (AD) requirements must be met:

1. All AD servers must be at least Windows 2003 SP2.
2. Forest functional level must be set to at least Windows 2003 native.
3. Domain functional level must be set to at least Windows 2003 native.
4. A global catalog server must be in the same AD site as the first installed Exchange 2010 server.

These conditions must be must or the Exchange Server 2010 install will not begin. Once the above conditions are met, the forest, domain and schema must be prepared. This mostly involves running some Exchange setup command line tools to add some fields and functionality to the AD Schema. Once this is complete, Exchange installation can begin.

Note: In previous versions of Exchange the prepare schema, forest prep and domain prep were required to be run before running the Exchange installer. This can still be done before installing manually but Exchange Server 2010 SP1 setup will perform these steps for you.

3.2.5. Current Configuration: Public Folders

Public folder data can contain all sorts of data important to an organization – legal contracts, communities, HR data and so on. As a result, managing public folder data can be very resource intensive. However, this resource investment need not be replicated in the cloud. With the the ability to migrate all of your public folder data to the cloud, the data will be hosted from an Exchange mailbox as if it were still on–premise – make sure your service provider offers this ability if you are a user of public folders.

3.2.6. Current Configuration: Smart Hosts Inbound and Outbound

A smart host is an appliance or outsourced vendor that scans email for viruses and malware at the edge, stopping malicious code from entering your network and avoiding the use of Exchange server resources to perform the scans. Before choosing a smart host provider, consider these questions while looking for smart host services.

1. Can the provider queue incoming email while my mail system is down for maintenance or unexpected issues?
2. Can the provider provide detailed reporting of message flow, quarantine activities, etc

3. Can the provider provide a mechanism for automatic account creation and deletion based on Exchange users?
4. Does the provider have multiple independent datacenters and mechanisms to allow my incoming messages to be received when the smart host provider is having a local issue?
5. Does the provider provide an API for bulk account modification for whitelists, blackslists, SPAM protection levels, etc?
6. Does the provider SLA meet my organizations needs for uptime and availability?

These are just a few things to consider when looking for a smart host provider. For many organizations, email is the most critical application. Making a good choice for a smart host is an important decision. When making this decision ensure at a minimum your provider provides these critical services.

- A layer of protection and intelligence between your corporate Exchange email system and the Internet
- The ability to queue for future delivery incoming email destined to your organization during planned and unplanned outages
- SLA's that encompass your business needs

3.2.7. Current Configuration: Multi-Server

When analyzing the current environment it is key to identify not only every component of Exchange but also every system that connects to the mail server. This includes: Front End servers, Back End Mailbox servers, any systems that send email, such as the backup system, Anti-Spam, Anti-Virus, Faxing, et al. All these components must be analyzed and an upgrade road map must be established. The most important thing to consider when examining the current architecture is to ensure that the new environment is adequately provisioned to handle the load. Quite often companies will consolidate servers and run more roles on fewer servers to leverage the built-in advancements on performance and also to save on resources.

Location is a key function of how many servers will need to be deployed. Look not only at how many legacy Exchange servers there are but also in what locations. If moving to a cloud provider, determine the ability to scale by adding memory, processor and storage. Also examine how to best position Exchange servers across geographically dispersed locations.

3.2.8. Current Configuration: Backup, Retention Policies, Archiving

The ability to restore email data is critical to any organization. Email data can be preserved in Exchange Server 2010 through the use of backups, retention policies, and archiving. Users will delete important emails, calendar data, contacts, or other business critical information; intentionally or by accident. The need to recover data from these scenarios exists at every organization.

Any good cloud provider will be able to recover deleted email information. Backups should be done daily to prevent data loss and keep the RPO within 24 hours. Retention policies give administrators the ability to recover recent items from the deleted items location per user, or from the transport dumpster (all users). Retention policies can be set specifically for folders and deleted items.

Archiving is another great way to maintain access to older email data. A lot of organizations depend on the use of third party backup and storage solutions instead of archiving; this approach takes more money to maintain, more time to recover data from tapes, and can spiral costs when a legal hold requires older tapes to be maintained that would otherwise be retired. In addition, archived mailboxes reside on a separate tier of storage from a user's main mailbox. The duration of archiving can be set to an organization's specific requirements for having data available and searchable; this is an especially great benefit for situations requiring a legal discovery. Archive databases can also be set to different retention and quota policies than active databases.

A combination of backups, retention policies and archiving is typically the best approach to having email data recoverable, accessible and searchable. Backups prevent complete data loss; retention policies allow recently deleted data to be easily restored; and archiving allows for an organization to set the limit on how long data is searchable for their own legal requirements.

Five areas that need to be considered with your cloud provider:

1. How quickly can deleted email data be recovered?
2. What will their RPO be for lost email data?
3. Is your email data easily searchable and accessible for legal discovery?

4. How long do you require email data to be available for legal discovery?
5. Is the ability to archive email data available on cheaper disk available?

Best Practices:

1. Run Exchange backups daily so data loss can be easily recovered within an RPO of 24 hours.
2. Set retention policies to 35 days to easily recover items that were accidently deleted, especially for tasks such as month-end processing.
3. Use archiving to keep all of your email data easily searchable and accessible.
4. Have your archiving stored on separate tier of storage, preferably on less expensive disk, since it won't be in use 100% of the time.
5. Eliminate 3rd party backup programs that use tapes by switching to archiving. For example, set ar chiving to a year, and hard delete after that date. This will save money by not moving data to tape, and not paying for tape maintenance, storage and retrieval while keeping your email data easily accessible and searchable for any legal discovery requests.
6. Set different quota policies on archive databases, depending on your legal requirements.
7. A good overall strategy is to use a combination of backups, retention policies and archiving. Backups prevent complete data loss; retention policies allow recently deleted data to be easily restored; and ar chiving allows for easily accessible data, legal discovery, and lower maintenance costs.

3.3. Migration Steps

The actual migration to Exchange Server 2010 in the cloud is where your deployment and configuration options come to life in a real instantiation of the solution. There are several approaches to optimizing the migration process.

3.3.1. Install Exchange Server 2010: Network Configuration Tips and Takeaways

Exchange Server 2010 is reliant on Active Directory (AD). Customers looking to transition should Before making the migration to Exchange Server 2010 in the cloud, carefully consider the health of your AD environment.. Replication issues, DNS configuration problems and other network related issues can very quickly disrupt your migration if you have not addressed them before you began the process. Before installing Exchange, run the latest version of the Microsoft Exchange Best Practices Analyzer. Pay special attention to the Exchange 2010 readiness test. This will scan the current Exchange, AD and DNS and network environment and report any issues that should be resolved before installing Exchange.

3.3.2. Extending Active Directory to the Data Center

In order to maintain a single sign on architecture, Active Directory must be extended and connected. Two ways to accomplish this are: AD Federation Services (AD FS) and AD Sites and Services. One option, AD FS, is a token based method of authenticating separate security realms through an extranet level trust. As another option, an additional AD server can be created in the same Data Center as the Exchange server. Then AD Sites and Services can be leveraged to reduce replication and ensure servers in the datacenter authenticate with their local AD server. Either method will work to ensure users are not prompted for credentials when logged into the domain and attempting to connect to their mailbox.

3.3.3. Client Configuration and Migration

Exchange Server 2010 increases the ability to stay connected and improves the ability to coexist during the migration. Once Exchange Server 2010 has been deployed, a few changes will need to be made for coexistence. A new Unified Communications certificate will have to be purchased, and a legacy namespace will need to be configured. When the legacy namespace is working, clients who still have mailboxes housed on Exchange 2003 will be able to access their mailbox through OWA without learning a new domain name. The front end Client Access server will automatically detect where the user's mailbox is and route OWA to the correct location.

The Autodiscover service also helps ease the transition from older Exchange versions by automatically repointing Outlook to the new Exchange server after a mailbox move. This greatly reduces administration and can make the move seamless to the end user. If moving from Exchange 2007, users can still use their mailbox while it is being moved. For clients with mailboxes on older version of Exchange their only downtime will be during the mailbox move. Public folders, Free/Busy, Offline Address Book,

and other client features can all coexist during the migration, serving clients on both Exchange 2010 and the older versions.

Migration Steps:

1. A separate namespace will be required for the legacy version of Exchange. The best practice for the namespace is to use a legacy URL such as: legacy.company.com
2. A new Unified Communications (UC) certificate will be required; it will use the existing names in the current Exchange UC certificate plus the name for the legacy URL
3. Assign services on 2010 CAS to the new UC certificate once installed
4. The legacy URL will need to be added to 2010 OWA with the commandlet Set-OWAVirtualDirectory using the -Exchange2003URL
5. The legacy Exchange system (2003/2007) will need it's OWA URL's changed to the legacy URL
6. A DNS record will need to be added to point the legacy URL legacy.company.com to the Exchange 2003/2007 servers that are hosting OWA
7. Firewall rules should be updated to route SMTP traffic to the new 2010 CAS servers instead of the legacy Exchange system

3.3.4. Planning for Namespace Changes

When implementing Exchange Server 2010, there are many names to keep track of and items that require SSLsecurity. With Exchange Server 2003, a single certificate with a single name was sufficient to secure the entire organization. With Exchange Server 2010 the following names must be secured on a single certificate:

1. External namespace for OWA and ActiveSync
2. The internal name for OWA and ActiveSync, if different
3. Autodiscover.
4. FQDN of each Client Access Server
5. If using load balancing, the name used for Client Access
6. Legacy - for coexistence to allow user with mailboxes still on 2003 to use OWA

This is a lot of complexity and therefore a great deal of planning needs to go into the namespace and all the different names that need to be included. All of these names must be on the same SAN (Subject Alternative Names) Certificate. These certificates are very flexible. In fact, even different domain names can be secured on the same certificate. This is useful and necessary if your internal domain is different from your external domain.

3.3.5. Server Validation: Namespace

A new namespace must be created for Exchange Server 2010 (internal and external) so both platforms can coexist at the same time. Configuring a new namespace will include DNS configuration; how certificates are created and named; and what URL's will be used for client access directories (Outlook Anywhere, , Offline Address Book, Exchange Web Services, Exchange Control Panel, and ActiveSync). This will allow users to continue to have uninterrupted access to their email regardless of which system they are on during the migration. Once the migration is complete, the old namespace can be removed.

3.3.6. User Migration Testing: Checklist of All Major Features

Major features to be tested on a user after a migration include:

Logging Into Outlook And OWA

OWA - Using a test mailbox account on the new Exchange system, go to the OWA url (I.E. https://mail.company.com/owa) and test logging in by using email address & password or domain/username & password.

- If logging in fails:
- Check the URL's set on the OWA Virtual Directory on each CAS server
- Make sure services are started on each CAS server
- Verify the mail certificate has the correct names on it
- Verify certificate has SMTP/IIS/IMAP/POP services as signed to it

Outlook - Using a test mailbox account on the new Exchange system, open Outlook and follow the prompts to create an Outlook profile. Use the published name of the new Exchange system (I.E. mail.company.com), and then email address & password or domain/username & password to create a profile.

- If you can't create a profile:
- Make sure services are started on each CAS server
- Verify the mail certificate has the correct names on it

- Verify certificate has SMTP/IIS/IMAP/POP services assigned to it
- Validate autodiscover is working (you can use testexchangeconnectivity.com)
- If using basic authentication, make sure it is set under More Settings when creating a new Outlook profile
- Create/send/receive Outlook items such as email and calendar items

Verify certificate has SMTP/IIS/IMAP/POP services assigned to it

Verify all Exchange services are started

- Use Outlook to connect internally (on the network), and externally (off the network)

Use a test mailbox account

- If internal works, but external fails:
- Check that Exchange is published correctly externally
- Verify DNS records are created correctly and published externally
- If external works, then internal will work too
- Free/Busy information shows up correctly

Check calendar in Outlook for OWA for another person's schedule

- If free/busy information does not show up correctly:
- Verify all Exchange services are started
- User lookups in the global address list work correctly, and the offline address book (OAB) generates and downloads successfully

Look for a user that you know is in Active Directory in the Address book. Use either OWA or Outlook.

- If the lookup fails:
- Check event logs on the OAB generation server for errors
- Validate OAB distribution points are set correctly; especially web distribution for OAB on the CAS servers

Use Outlook to manually download the OAB.

- If the download fails:
- Check event logs on the OAB generation server for errors
- Validate OAB distribution points are set correctly; especially web distribution for OAB on the CAS servers

3.3.7. User Migration Testing: Validation

Begin to test a successful user migration by creating a test account to validate the Exchange experience. This test account will be created on the legacy system. To complete a full test, make sure the account can be accesses through OWA. Also, connect a test phone to the account and make sure Microsoft ActiveSync works. A new Outlook profile for the account will be created and populated with test email and calendar data before migrating it to the new system. Once the user is migrated, Autodiscover will provide a seamless login to the test account on the new system without the user having to manually enter in server names to connect to the new Exchange system. After Outlook is connected, next test access to OWA and ActiveSync. Using a test account with access to Outlook, OWA and ActiveSync will expose any connectivity issues that can be remedied before moving and impacting production users.

3.3.8. Server Validation: Creation of Test User on New Platform

Once all major components for the Exchange server have been deployed and validated as functional, new user account creation can occur. Following validation of the availability of all major Exchange components, one of two methods can be utilized to create and test a user mailbox: Either via the typical Exchange system tools or through new user creation on the Active Directory domain.

3.3.9. Using the Exchange Management Console in Exchange Server 2010:

Open Exchange Management Console (EMC) -> Organization configuration – > Mailbox -> Right Click and Click on New Mailbox.

Continue through the new mailbox creation wizard answering steps for the type of mailbox, the appropriate user data, the database to be used, additional options like ActiveSync and archiving and completion.

3.3.10. Test User Creation via Shell Commands

Creation of a test user can be done from a shell command on the Exchange system. The below example creates the mail user Test User with the external e-mail address testuser@company.com.

New-MailUser -Name Test -FirstName Test -LastName User -ExternalEmailAddress testuser@company.com -UserPrincipalName test@contoso.com -Password Pass@word1

Once the test user is created, next steps would include validation of mail delivery, calendar functions, address book functions, OWA, ActiveSync and any other necessary Exchange functionality.

3.3.11. Recovery and Maintenance: RPO, RTO, SLA or Mailbox Restore on a Given Mailbox/Mail Item

When choosing a cloud service provider, it is important to have 24 hours or less RPO on your Exchange data. Depending on when a disaster occurs, data should at least be restored and brought back online to the data from the night before. Backups of Exchange databases should be taken daily by your cloud provider. Your Exchange instantiation should constantly be monitored, so any issues with backups are responded to immediately, and the restore process should frequently be tested.

4. The Tier 3 Exchange Solution

Tier 3 supports a full implementation of Exchange and Windows that can be built, deployed and customized to the customer's need.

- Such features as unlimited mailbox and message sizes aresupported.

- Integration with existing systems such as Microsoft Lync* and Microsoft SharePoint* is supported.

- Implementation of the latest technologies such as multiple backend database servers, Data Availability Groups, load balanced client access and hub transport servers.

- Tier 3 can support DAG across multiple physical zones in order to maintain high availability, disaster recovery as well as low latency for localized users.

- Spam and virus protection is seamlessly integrated with the Tier 3 Exchange implementation through industry leading offerings such as Postini*.

With its team of Exchange experts on staff, Tier 3 can take on as much of the initial planning, deployment and ongoing management of the Exchange transition. The team constitutes decades of combined experience in implementation, transition, management and ongoing operational support. There are thousands of mailboxes and dozens of Exchange implementations managed by this team on a daily basis handling everything from complete hands off solutions to ongoing partnering with customers to ensure their solutions continually meet their needs.

Using the Tier 3 solution, the requirement for large capital expenditures is greatly reduced – no need for hardware, software or staff to run it. In addition, there is no need to plan for major upfront licensing costs. Customers have the flexibility to utilize their own purchased licensing models or leverage SPLA (Service Provider Licensing Agreement) models through Tier 3. In all cases, the customer takes advantage of utility-based pricing where only consumption is paid for.

Many cloud and hosted Exchange solutions can't or won't support such Exchange technologies as Public Folders. For example, if the client wants to retain legacy workflows or custom solutions based on the Public Folder systems, the Tier 3 solution allows the customer to retain these without costly upgrade requirements.

Tier 3 supports permanent point-to-point VPN solutions allowing the customer to have complete access and control of their environment whenever and wherever they want it. By using this channel, customers can also securely support their Active Directory configuration by extending their corporate domain implementation to their Tier 3 infrastructure. This provides a seamless authentication experience for the entire corporate user base.

Unlike a hardware-based model, resources for Exchange on the Tier 3 systems have the ability to scale up and down with usage and load characteristics. This is key to managing the infrastructure in a way that is flexible and dynamic.

Given the critical nature of corporate email systems, Tier 3's standard implementations for business continuity and disaster recovery is unmatched in cloud-based Exchange Server 2010. With every install, Tier 3 provides 14 days of snapshots should a rollback be required. The infrastructure supports SLAs and uptime models of 99.999% availability. Data is replicated to remote facilities in the event of full data center outage. And finally, additional backup models such as Windows-based shadow copy services and DPM (Data Protection Manager) are offered for specific Exchange-based requirements.

About the Authors - Tier 3 Exchange Deployment Experts

Kelly Malloy, Director of Operations

Over the past decade, Kelly has managed countless Microsoft Exchange Server environments, starting with Exchange 5.0. He has overseen dozens of migrations from Exchange 5.5 to 2003, 2003 to 2007, and then to 2010. Kelly's experience has shown him that an Exchange team must have significant knowledge of the configuration and process for backup and restore. When the client needs a backup or restore, they expect it to work. He enjoys being responsible for creating and managing email solutions, the client's most vital business application.

Eric Schubert, Senior Consultant

Eric's experience installing, administering and transitioning email systems goes back 15 years, starting with Microsoft Mail. He specializes in project planning and new environment sizing and architecture. His accomplishments in the Exchange arena include scoping, architecting and performing numerous Exchange transitions, from 2000 to 2003, 2003 to 2007 and 2007 to 2010. Eric has implemented single server solutions, supported a Continuous Cluster Replication with 7 servers, configured a dual site, 4 server Standby Continuous Replication solution and configured Exchange 2010 Database Availability Groups. He enjoys working closely with and mentoring in-house IT to empower them to manage their new email environment.

Mark Turpin, Senior System Engineer

Mark has more than 5 years' experience managing large, complex instances of Exchange Server. In some cases, the Exchange environments he oversees have more than 14,000 users. He's overseen numerous migrations of Exchange 2003 to 2007 and more recently, from 2007 to the 2010 edition. Mark specializes in design for disaster recovery, configuring backup and continuity

Tier 3 goes beyond traditional cloud offerings to provide an agile, self-optimizing enterprise cloud platform. Innovative technologies deliver predictive optimization for unprecedented performance. Enterprises large and small depend on the Tier 3 secure, intelligent platform to run their mission-critical, production applications and services so they can focus on their core business.

Contact Information

email: info@tier3.com

phone: 1.877.388.4373

www.tier3.com