happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

Exchange 2003 to Exchange 2010 Migration – Part -I

By Koteswararao Venigalla

Contents

Contents....2
Introduction....3
It a Migration or a Transition?....3
Exchange 2003 overviewIs....3
Features of exchange 2010....3
Flexibility and Reliability 5
Goals of the migration....6
Factors to consider before migration....6
Active Directory....7
Check the health of your Active Directory Site 7
before Upgrading....7
Summary....9

Introduction

With the release of Exchange Server 2010, Microsoft has expanded the existing functionality and introduced new concepts. Exchange Server 2010 still provides organizations a robust messaging and collaboration platform while continuing to broaden their focus to enhance the feature set.

Exchange 2000/2003 cannot be ‘‘upgraded’’ to Exchange 2010. One must perform a migration. The process of moving from Exchange 2003 to Exchange 2010 or from Exchange 2007 to Exchange 2010 is often referred to as an upgrade, but technically it is not. An upgrade occurs in-place; that is, it involves taking an existing server and installing the newer version of the software on that server. The server installation process then performs whatever changes it needs to, in order to convert the old software (and database) to the newest version.

This white paper describes the new features of Exchange Server 2010 and the goals of migration.

Is it a Migration or a Transition?

If you search through the Microsoft documentation and read books and articles on Exchange 2010 migration, you will see the term transition tossed around a lot. A transition is a type of migration that occurs when you install new Exchange servers in the same organization. The servers interoperate for some period of time, you move services and data over to the new servers and then you shut down the old server and remove them.

Most Exchange migrations are really transitions, because you usually install new servers and move the data over. However the term migration here is used in a more generic sense. Just to make things less complex you will often see migration guidelines giving you two upgrade strategies:

- Upgrade your existing organization, which Microsoft sometimes calls an ‘upgrade’, though here in places we will refer to it as a transition.
- Create a new organization and move your messaging data over. This is called a migration. Be aware that this use of migration refers only to the act of moving your data between the two organizations.

To be consistent with Microsoft usage and minimize confusion, we will use the term upgrade to refer to the process of moving from an existing Exchange 2003 organization to Exchange 2010, no matter which strategy you used to get there. Actual migrations from messaging systems other than earlier versions of Exchange (or from Exchange 5.5) are outside the scope of this document.

When we need to refer to moving data between organizations, we will explicitly say migration strategy. This helps us in being clear and staying consistent with the excellent documentation provided for Exchange 2010.

Exchange 2003 overview

Exchange 2003 cannot be ‘‘upgraded’’ to Exchange Server 2010. The services and data on Exchange 2003 must be migrated or moved to Exchange Server 2010.

There are a number of reasons for this.

- Exchange 2003 runs only on Windows 2003 x32.
- Exchange Server 2010 runs only Windows Server 2008 x64 or Windows Server 2008 R2.
- Exchange Server 2010’s database architecture is radically different. Exchange 2010 uses 1 MB transaction logs, a different database page size, and a single EDB file rather than Exchange 2003 EDB and STM files.
- Exchange Server 2010’s message transport and client access components are very different from those of Exchange 2010.

What you must do instead of an in-place upgrade is install new Exchange Server 2010 servers in the existing Exchange organization. To the existing Exchange 2003 servers, these new servers will appear similar to other Exchange 2003 servers. Once you start installing new Exchange 2010 servers in the organization, you can start transitioning messaging services over to these new services.

Features of exchange 2010

Exchange Server 2010 provides three high-level benefits:

- Anywhere access
- Protection and compliance
- Flexibility and reliability

These features were designed to meet the needs of today’s mobile workforce, help organizations protect and retain information according to policy, as well as ensure that e-mail services are available at all times.

Anywhere Access

Today, e-mail needs to be accessible from any location as end users are no longer tied to a single desktop computer that is used only during the work day. Microsoft considered this when designing Exchange 2010, and has made accessing and manipulating messaging data easier than ever.

Outlook Web Access

Internet-based e-mail access has been common for many years. It looks and feels like the standard Outlook client. The much-improved conversation view in OWA provides a quick way to browse through a thread of messages without having to change the focus to each individual message. This is a significant improvement over the threading capabilities in Microsoft Office Outlook 2007 that is at par with the conversation view in Microsoft Office Outlook 2010.

The newest version of OWA includes many other useful features. The nickname cache provide users with a familiar drop-down listing of possible name matches as they type a name or e-mail address into the To, Cc, or Bcc fields of a message. Searches have more flexibility, and users can filter searches quickly by typing qualifiers directly into the search field using an easy-to-understand format. For example, to search for messages with the word 'operations' in the Subject field, you simply type subject: operations in the search box.

Windows Mobile

Anywhere access is also enhanced by functionality that allows mobile device users, including those with Windows Mobile 6.1, to access messaging data. Outlook Mobile is being updated to include the features available in Windows Mobile 6.5. The conversation view available in Outlook 2010 and OWA 2010 is also available in the latest version of Outlook Mobile. Free/busy calendaring information for users within an organization can be obtained through Outlook Mobile, simplifying the process of scheduling meetings from mobile devices.

Multi-Mailbox Search

One of the most useful features of Exchange Server 2010 is the multi-mailbox search, which allows users with appropriate permissions to search the entire organization for messages containing specific keywords or characteristics. This capability is designed to simplify e-discovery. However, it can also be helpful in other situations, such as when confidential information has been leaked from an organization or a new virus is spreading. Administrators or other named parties can easily search for information and extract the results to a mailbox for inspection. Unfortunately, search results cannot be exported directly to a PST file. Administrators or compliance officers need to manually export the search results to a PST file when they need to provide search results to others.

Information Rights Management

Preventing information leaks has become a serious concern for many organizations. In Exchange Server 2010, Microsoft has improved some of the existing mechanisms in Exchange Server 2007 and introduced new ways of protecting messaging data. Information Rights Management (IRM), which restricts access and makes data accessible only to specifically named parties, has been expanded to work with Outlook Web Access (OWA) in addition to the Outlook client. This enables users to create and access messages that have been protected using IRM, even when they are not at their workstations. The rich OWA client, including IRM support, works not only in Microsoft Internet Explorer, but also in Apple Safari and Mozilla Firefox browsers. Many organizations are attracted to the idea of encrypting specific data using IRM but are concerned about the long-term ramifications, since encrypted messages cannot be read easily by anyone other than the sender and the intended recipients. Accordingly, Microsoft enabled the Exchange 2010 transport agents to decrypt messages for inspection by anti-spam and antivirus programs when they are being bifurcated and sent to the message journaling mailbox.

MailTips

MailTips is expected to be a popular new feature especially with end users who have made the mistake of sending a message to a large distribution group instead of a few recipients. MailTips is based on a simple idea, giving users hints about what they are about to do before a message is actually sent. MailTips includes preconfigured options and can also be tailored by the user. For example, the user can change the number of recipients in a distribution list that will result in the presentation of a MailTips hint. One of the most useful features of MailTips is that it indicates when intended recipients of a message have their Out of Office (OOF) message set, a preview of the OOF is even displayed in the draft message to enable the sender to re-address the message more appropriately. While MailTips is not natively supported by Outlook 2007, a plug-in is available to extend MailTips to this legacy client. Both the Outlook 2010 client and OWA 2010 include native support for MailTips.

Message Transport Rules

Microsoft keeps making huge strides in message transport rules. These rules continue to become more flexible and meet diverse criteria. The standard transport rules have been expanded to cover additional message characteristics, such as information from a user's Active Directory account. For example, rules can be created to block, IRM-protect, or force moderation of messages from a group of users (such as the Marketing department) to a specific domain or e-mail address. They can also scan messages (including those with any Microsoft Office-based attachments) for certain keywords or phrases and then take specific action against those messages, such as sending the message to a supervisor for moderation.

Active Directory Rights Management Services

With Windows Server 2008, Active Directory Rights Management Services (AD RMS) become much simpler to deploy and manage, and AD RMS is well integrated into Exchange 2010. The new transport protection rules can apply AD RMS templates to messages (and attachments) without the need for end users to get involved in the decision-making process. Just a few AD RMS templates are included with Exchange 2010, and the 'Do Not Forward' template will likely prove to be the most popular. When the 'Do Not Forward' template is applied to a message, the recipient can perform only limited actions on the message. For example, recipients can be prevented from printing or copying message data. This provides an additional measure of protection for organizations that are concerned about information leaks.

Flexibility and Reliability

In addition to the enhanced anywhere access and protection and compliance, Exchange Server 2010 also offers improved flexibility and reliability. Keeping messaging data available at all times has become a necessity for most organizations and it is a big focus for Microsoft in Exchange 2010. The new clustering functionality in Exchange 2010 is a giant leap forward from the continuous clustering options available with Exchange 2007, and much improved from the single copy clustering available in Exchange 2003 and earlier versions.

Storage Options

With 32-bit versions of Microsoft Exchange Server (i.e., Exchange Server 2003 and earlier versions), using a storage area network (SAN) for data storage was often the optimal solution. When Exchange Server 2007 was introduced, the expanded application access to memory provided by the 64-bit platform reduced disk I/O by up to 70 percent, so the disk subsystem was no longer a bottleneck in Exchange environments. With Exchange 2010, disk I/O is further reduced. Microsoft put a lot of effort into reconfiguring the database structure, and the result is impressive. Disk I/O is reduced by up to 50 percent of Exchange 2007 levels, which is a reduction of up to 85 percent from Exchange 2003 levels. Microsoft began recommending the use of direct attached storage (DAS) for Exchange data with the introduction of Exchange 2007 and continues to do so with Exchange 2010. With Exchange 2010, there is no need to use an expensive SAN to hold messaging data. Exchange 2010 was designed to work well with serial advanced technology attachment (SATA) disks. Disk writes do not come in bursts with Exchange 2010, which enables SATA disks to easily support the messaging infrastructure's storage needs.

Although using a SAN for Exchange-related storage is not prohibited, it seems like Exchange 2010 can perform consistently and reliably on less expensive storage. Microsoft has long recommended specific RAID configurations for Exchange Server implementations. RAID 10 (mirroring plus striping) or RAID 5 (striped with parity) for the mailbox databases, and RAID 1 (mirroring) for the transaction logs. But with Exchange Server 2010, RAID configuration is no longer necessary because database availability groups (DAGs) (a new type of continuous clustering introduced in Exchange 2010) provide enough redundancy that disks become disposable. If a disk fails, the mailbox database can switch over to another DAG instance, and administrators can simply pull the disk, replace it, and rebuild the database instance. Therefore, Exchange 2010 can use just a bunch of disks (JBOD) for storage, eliminating the need for RAID configurations.

Clustering with Database Availability Groups

Clustering Exchange 2003 and prior versions were complicated processes that did not offer a lot of protection against serious failures in the environment. Continuous replication clustering technologies were introduced in Exchange 2007, removing much of the complexity of managing clustered Exchange servers. The legacy method of clustering, single copy clustering (SCC) did not provide a second copy of the mailbox databases. Continuous clustering created additional copies of each storage group and kept the copies up to date by using log shipping.

With the introduction of the DAG, Exchange 2010 has gone beyond the initial promise of continuous clustering and finally offers a solid clustering solution that provides a level of assurance that has too long been absent from Exchange Server.

A DAG is a set of up to 16 Exchange 2010 servers assigned the Mailbox role, where each server that is a member of the DAG can contain a copy of the mailbox databases assigned to that DAG. Initial database instance seeding is done through ESE (the database technology behind the Exchange database itself) streaming, and each database instance is kept up to date through log file shipping using TCP raw sockets.

Microsoft has also eliminated storage groups in Exchange 2010. One reason was the aggregation of transaction log files for a storage group in a single folder hierarchy. With the DAG, storage groups and their associated combined transaction logs could have complicated database failure, so Microsoft has chosen to simplify the architecture to allow quick recovery and return to operations.

One of the most impressive characteristics of the DAG architecture is that DAGs can be created on the fly; there is no need to commit to DAG membership during the installation process. If there is more than one Exchange 2010 mailbox server running with live mailboxes, a DAG can be created with ease and the existing mailbox databases can be assigned to it. DAGs can easily span

sites to provide geographic clustering without any special configuration, eliminating the tedious configuration process required with earlier releases of Exchange clustering. A few additional items of note; the client access server (CAS) and hub transport server (HUB) roles can be co-located on servers that are joined to a DAG, and public folder replication is incompatible with the replication technology used by the DAG. Public folders being replicated from servers that are members of a DAG should be isolated. While the DAG architecture provides more mailbox database protection than was previously available, making regular, quick volume shadow copy service (VSS) snapshots of the databases should still be considered a best practice.

goals of the migration

Higher Availability

Organizations and users depend upon stable e-mail access. Component failure, power failures, and natural disasters can affect email system availability or level of service. Highly available email systems have minimal downtime, provide acceptable performance, and aid user productivity. In addition, they can recover quickly from hardware or network failures. Microsoft Exchange Server 2010 provides high availability through Database Availability Groups (DAG), which essentially provide continuous background replication.

Improved fault tolerance

Fault tolerance is the ability of a solution to continue operating even after any part of the solution fails. Fault tolerance requires a high degree of redundancy. If any single component fails, the redundant component takes its place with no appreciable downtime. The clustered Microsoft Exchange 2003 solution would be able to provide fault tolerance in case of many server problems because a second server maintains access to the database and could be activated in response to problems on the active server. Microsoft Exchange 2010 solution improves fault tolerance.

Improved regulatory compliance

Exchange Server 2010 includes integrated e-mail retention and discovery features aimed at meeting regulatory requirements related to preventing information leaks and preserving business emails. Centrally managed emails and information control capabilities such as multi-mailbox search and immediate hold gives IT the ability to store and query email across the organization more effectively.

Improved IT productivity

Exchange Server 2010 includes features designed to reduce the cost of managing e-mail infrastructure. New role-based permissions functionality enables administrators to delegate permissions to other administrators and users based on the Exchange tasks each performs and to define what users can configure on their mailboxes. The Web-based Exchange Control Panel (ECP) provides self-service options for tasks that might otherwise require a help desk call. The role-based access control model ensures users can only access the functions to which they have authorized access to.

Improved End user satisfaction and productivity

Additional features address end-user productivity problems and disaster recovery. Features such as the ignore conversation option and conversation view options give users more control over mailbox content and organization. If the organization adds mobile and Web access capability, users can access all their centrally managed emails from PC, mobile, and web access devices using a consistent interface on Outlook on the PC, Outlook Mobile, and Outlook Web access.

Factors to consider before migration

Before you pull the trigger and pop the Exchange 2010 installation media into the drive, you must take into account a few factors. Let us go over them in detail so that your upgrade is successful.

Prerequisites

Before you can begin upgrading your Exchange organization, you have to ensure that it meets the necessary prerequisites. We've gone over some of these in this document, from the context of a fresh installation of Exchange 2010, but let us look at them again, this time keeping in mind how your existing Exchange deployment may affect your ability to meet them.

Hardware and Operating System

For production use, you must have x64-compatible hardware — systems with one of the following types of processors.

- The Opteron processor line, made by AMD, found in high-end server hardware
- Athlon 64 processors, also by AMD, meant for inexpensive servers and high-end workstations
- Intel Xeon and Pentium line of processors with the Extended Memory 64 Technology (EM64T) extensions.

The Xeon family is typically found in high-end servers, whereas the Pentiums are found in low-end servers and workstations.

The Intel Itanium processor line is not compatible with Exchange 2010. Unlike some other Microsoft restrictions, this isn't just a case of being an unsupported configuration. The Itanium processors are not compatible with the x64 specification and Exchange 2010 has not been compiled to run on the Itanium family of CPUs. Nowadays, multicore processors are increasingly common — both Intel and AMD. Although Windows recognizes multiple cores as separate processors when managing processes and threads,

Microsoft licensing does not make a distinction between single-core and dual-core processors. This fact is to your benefit because Exchange will certainly benefit from additional cores.

You can run Exchange 2010 on any of the following versions of Windows Server 2008 SP2 or R2.

- Windows Server 2008 x64 Standard Edition with SP2 or R2
- Windows Server 2008 x64 Enterprise Edition with SP2 or R2 This doesn't mean you are completely off the hook on the hardware front.

Even if your current Exchange 2003 servers are running on 64-bit hardware, you cannot just pop the Exchange 2010 DVD in and do an in-place upgrade. You may ask, why not?

- Previous versions of Exchange are all 32-bit only and cannot be run on Windows Server 2003 x64. Note that this is not a matter of support. Exchange 2003 simply will not run on 64-bit Windows
- You cannot upgrade from Windows Server 2003 x86 to Windows Server 2008 x64. You have to perform a clean installation.
- There is no x32 bit version of Exchange Server 2010. All this means that to reuse existing server hardware, you are going to have to have at least one spare server and be prepared to reinstall Windows and Exchange on your servers as you go.

Active Directory

Because Exchange 2010 depends on Active Directory, you should take a good look at the domain controllers and global catalog servers in your Active Directory forest before starting the upgrade process.

Unlike Exchange 2003, which could use domain controllers running either Windows 2000 Server with the appropriate service pack or Windows Server 2003, Exchange 2010 requires that all of the following domain controllers be running Windows Server 2003 + SP1.

- The schema master domain controller, which is usually the first domain controller that you installed in the orest, unless you have moved the schema master flexible single master of operations (FSMO) role to another domain controller
- At least one global catalog server in each Active Directory site Our recommendation is to upgrade all your domain controllers to at least Windows Server 2003 SP2, especially if you still have Windows 2000 Server domain controllers.

The Active Directory improvements in Windows Server 2003 can vastly reduce the bandwidth required for Active Directory replication, and several Exchange 2010 features (such as address book browsing in OWA) rely on features in Windows Server 2003 SP1.

By making sure you have upgraded all your domain controllers, you increase the redundancy and resiliency of your Exchange/Active Directory integration.

Check the health of your Active Directory Site before Upgrading

It is extremely important for the Active Directory be healthy before you upgrade to Exchange 2010. Exchange 2010 relies directly on your Active Directory site structure for message-routing information.

Whether you upgrade all your domain controllers or just the minimum number, you need to list all the domains in which you will either install Exchange 2010 or create Exchange 2010 recipient objects such as users, contacts, and mail-enabled groups. For each of these domains, ensure that the domain functional level is set to the Windows Server 2003 native level or higher. Doing so ensures that you have no lingering Windows NT 4.0 servers acting as down-level domain controllers via the primary domain controller (PDC) emulator. The Active Directory forest must be Windows Server 2003 Forest Functional mode or higher.

Officially, you need to have only a single Windows Server 2003 SP2 global catalog server in each site, but Windows Server 2003 SP2 domain controllers offer many advantages to your organization above and beyond their benefits to Exchange Server 2010.

For Windows 2003 Active Directory forests, the minimum forest functional level must be Windows Server 2003.

A few additional things that we need to keep in mind :

- If you plan on using OWA and any of your domain control lers are using a non-English version of Windows 2003 SP1, you must install the hotfix in Knowledge Base article 919166 on each non-English domain controller.
- You may want to use 64-bit Windows Server 2003 or 2008 on your domain controllers for performance benefits; however, doing so is not required.
- Assuming similar speeds and models of processor, you should still plan to meet the long-standing recommendation of ensuring a proper ratio of Exchange Mailbox processor cores to global catalog processor cores in a given site. If

you are using x86 domain controllers, the ratio is 4:1; while using x64 domain controllers, the ratio is 8:1. Note that the x64 ratio is assuming that you have enough RAM on the domain controllers to cache the entire NTDS.DIT database. This helps ensure that global catalog lookups happen quickly enough to keep Exchange responding in a timely fashion.

- Avoid installing Exchange 2010 on a domain controller. Although it is technically possible, such a combined server is much less resilient to service outages or configuration changes and is much harder to restore in the event of a disaster.

Exchange Version

The final prerequisite you must consider is what mode your legacy Exchange organization is in. By default, these versions of Exchange install in mixed mode even when you did not upgrade from Exchange 5.5. You must upgrade the organization to Exchange 2000/2003 native mode. Note that in order to do this, you must ensure the following points.

- No Exchange 5.5 or Exchange 2000 servers remain in the organization.
- No legacy Exchange Site Replication Service (SRS) instances remain in the organization.
- No configured connection agreements in the Active Directory Connector (ADC) remain in the organization. In fact, if you still have the ADC in your organization and you have no more Exchange 5.5 servers or legacy Exchange SRS instances, remove the ADC from the organization.

Once you have verified that your Active Directory domains and forest and Exchange organization meet these prerequisites, you can begin the process of installing Exchange 2010 by preparing Active Directory.

Setting the Legacy Routing Server Parameter

When you install Exchange 2010 in an existing legacy Exchange organization, you should address some architectural differences. We said earlier that Exchange 2010 does not use administrative groups or routing groups, and that is completely true. Although Exchange 2010 servers don not make use of them, the legacy Exchange servers do require them; in a mixed organization, you are going to have the administrative groups and routing groups created for the older Exchange servers. The Exchange 2010 servers use the new Active Directory site-based architecture and the legacy Exchange servers use the administrative groups and routing groups. Under these conditions, everything is happy until the new Exchange 2010 server tries to interact with a legacy Exchange server.

To deal with this, the Exchange 2010 installer takes several actions to ensure compatibility with legacy Exchange servers. To facilitate communication with legacy Exchange servers, the Exchange 2010 installer creates a special administrative group the first time it is run in a legacy organization. All Exchange 2010 servers are placed into this special administrative group, which is named Exchange Administrative Group (FYDIBOHF23SPDLT). If you have previously installed Exchange 2007, this administrative group will already exist. The Exchange 2010 servers don't use this group, but it will show up, along with all the Exchange 2010 servers, in the legacy Exchange System Manager

- The installer also creates a special routing group for Exchange 2010 servers, named Exchange Routing Group (DWBGZM FD01QNBJR). As with the administrative group, all Exchange 2007 servers are placed into this routing group, even though they use the native Exchange 2010 and Active Directory site-based routing mechanisms; the group and servers are visible in the legacy Exchange System Manager. The only purpose of this routing group is to force the legacy Exchange
  servers to use a routing group connector to communicate with Exchange 2010 servers.
- The installer also creates a universal security group named ExchangeLegacyInterop in Active Directory. Exchange 2010 servers use this group to determine which legacy servers are permitted to submit messages to the default SMTP receive connectors on the Exchange 2010 Hub Transport instances. By default, these connectors require successful authentica tion and permit message submission only from legacy servers whose computer accounts are in this group, such as the legacy Exchange bridgehead server.
- When the first Exchange 2010 Hub Transport role is installed, the installer creates a two-way routing group connector between the Exchange 2010 routing group and a user-selected legacy Exchange bridgehead server. If you use the command-line installer, you use the /LegacyRouting Server switch to specify which legacy Exchange server to use. You can add additional bridgehead servers to these routing group connectors after the installation is complete, and we talk about that in more detail later in this chapter. As with the administrative and routing groups, this connector is visible in the legacy Exchange System Manager.

About Exchange 2003/2010 Administrative and Routing Groups

The names of the Exchange 2007/2010 administrative and routing groups are designed to be unique, something that is not likely to be already present in any legacy organization. Do not rename these groups.

The Exchange 2007/2010 administrative group and routing group are intended only for Exchange 2007/2010 servers. Do not place legacy Exchange servers in these groups thinking that it will somehow improve interoperability or remove the need for the routing group connector. You will break mail flow because there is no other mechanism for translating between the legacy Exchange routing mechanism and the Exchange 2010 routing mechanism.

Once you have specified the legacy bridgehead server and successfully added the first Exchange 2010 Hub Transport instance to the organization, you can later configure the default routing group connector with additional legacy Exchange bridgehead servers or even create new routing group connectors to simplify the message routing paths in your organization.

However, you are going to have to perform these tasks from the Exchange Management Shell; you will not see the legacy routing group connectors listed in the Exchange Management Console.

To see the existing legacy routing group connectors, use the Get-RoutingGroupConnector cmdlet. To add a new legacy bridgehead to an existing legacy routing group connector, use the Set-RoutingGroupConnector cmdlet.

Suppressing Link State Updates

One of the interesting features included with Exchange Server 2000/2003 was link state updates. This feature allowed an Exchange 2000/2003 server to notify other bridgehead servers in the organization in the event of a connector failure. The intent was to ensure that messages did not get bounced back and forth between connectors and bridgehead servers. Exchange Server 2010 does not use or require link state updates, so this feature should be disabled on all Exchange 2003 servers.

To create a new routing group connector, use the New-RoutingGroupConnector cmdlet.

When you use the New-RoutingGroupConnector and Set-RoutingGroupConnector cmdlets to specify the TargetTransportServers and SourceTransportServers parameters, you need to specify all the servers you wish to be bridgeheads for the connector. Each invocation of the cmdlet will overwrite the existing parameter.

Summary

Exchange 2010 offers many important new functionalities, including the ability to closely integrate on-premise and online deployments. For this reason, migrating from Exchange Server 2003 to Exchange Server 2010 can offer significant benefits. Understanding the common challenges of migration and following the migration procedures will ensure that your project is successful.

About the Author

10 years of IT experience, including 4 years of experience in Active Directory, 2.5 years in Exchange, Lync 2013 and Hyper V. He has worked in different roles such as System Analyst, Senior System Analyst, Team Lead and now as a Tech Lead. Past key projects that he worked includes, Exchange migrations, Designing and deploying Lync 2013 and Server Virtualization using Hyper V. He is certified MCITP Enterprise Admin (Windows Server) and certified Citrix Xen Mobile Admin.

Koteswara Venigalla

Happiest Minds

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

To know more about our offerings. Please write to us at business@happiestminds.com

E-mail: business@happiestminds.com
Visit us: www.happiestminds.com

Follow us on