# Microsoft Exchange 2007—End-to-End Messaging Infrastructure Solution

## Abstract

A complete end-to end messaging solution in a virtualization-enabled platform for Microsoft Exchange 2007 can provide a number of technical and operational benefits. This document provides an overview of this end-to-end infrastructure that takes advantage of the best-of-class technologies from Cisco, EMC, and VMware. The reference architecture presented in this document enables customers that are considering a Microsoft Exchange 2007 deployment to capitalize on the benefits of a complete cooperation and integration from world leaders in IT solutions and services.

## Contents



**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Executive Summary

Microsoft Exchange messaging environments support a vital part of a company's operation where users expect to have access to the messaging system at all times. Microsoft Exchange messaging environments are also growing in complexity and user requirements are increasingly demanding. Additionally, the manner in which Microsoft Exchange is used to support business operations has changed and it is now even more business-critical than ever before.

Without a comprehensive plan for a Microsoft Exchange 2007 deployment, the company could face:

- Loss of revenue
- Missed business opportunities
- Compliance-related fines
- Loss of data

With these potential risks of a poorly implemented solution, our market analysis revealed the following critical business factors that affect Microsoft Exchange 2007 installations:

- Capital cost reduction through consolidation
- Operating expense reduction through streamlining operations management
- Risk reduction through validated compliance
- Risk reduction through security (including spam and virus filtering needs)

Cisco, EMC, and VMware developed a jointly validated foundation reference architecture for Microsoft Exchange 2007 to address these requirements, offering organizations the building blocks to take messaging to the next level. Implementing the joint reference architecture for Microsoft Exchange ensures the resiliency to meet the growing demands of today's rapidly changing business.

# About the Document

## Audience

This document is intended for Cisco, EMC, and VMware customers. In addition, this document benefits Microsoft Exchange administrators and architects, systems administrators, systems architects, and anyone involved in the design, decision making, and implementation of a Microsoft Exchange 2007 solution would find this paper useful.

## Document Objective

The objective of this document is to provide customers an overview of the joint Cisco, EMC, and VMware solution for Microsoft Exchange 2007 messaging infrastructures. It is not meant to introduce the reader to basic EMC, VMware, or Cisco data center; nor is it meant to be a resource to learn the details of Microsoft Exchange Server 2007.

# Introduction

Microsoft Exchange is considered the backbone of enterprise messaging environments and is growing at a rapid pace. As the number of users and departments grow, so does the requirement for a scalable, reliable, and cost effective Microsoft Exchange architecture to meet the new business requirements. While enterprises prepare to meet demands for greater collaboration, quicker access to applications and compliance with ever-stricter regulatory compliance, they are being crimped by issues relating to power and cooling, efficient asset utilization, escalating security and provisioning needs, and business continuance. Customers understand that unmanaged growth is no longer viable and appreciate the benefits that are gained from data center consolidation and virtualization. A virtualized data center infrastructure enables the customer to efficiently service an Microsoft Exchange collaborative environment.

Cisco, EMC, and VMware are jointly collaborating on a validated solution for an end-to-end messaging infrastructure in a fully virtualized architecture (see Figure 1). The design presented in this document enables customers considering a Microsoft Exchange 2007 deployment to capitalize on the benefits of a virtualized platform with VMware ESX 3.5, EMC storage and replication capabilities that provide disaster-recovery protection, and advanced server and storage connectivity through Cisco technology. The combination of these technologies provides a critical combination for *efficient*, *secure*, and *agile* deployments that achieve the business initiatives stated earlier under Executive Summary, page 2.

*Figure 1 Virtualized End-to-End Messaging Infrastructure*


# Efficiency

Enterprise customers need to support the continued growth in data while consolidating assets and reducing costs. Many customers today are also facing imposed or adopted "green" initiatives and are limited in the amount of power and cooling they can consume. At the same time, managing more information, providing sufficient application performance, and enabling access to information for competitive advantage means building infrastructures that are more efficient than ever before.

# Security

Due to recent high-profile security breaches and identity thefts, governments and security agencies world wide have introduced security regulations such as the the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, Basel II, and European Privacy Directive to protect sensitive data. The loss of sensitive data raised security concerns about how data has been stored or forwarded across the enterprise, including Microsoft Exchange email messages. The concerns include theft of disk drives, backup tapes lost during transportation, hacking, and access control. Nearly all customers today need to protect huge volumes of information from loss and from falling into the wrong hands. The next generation of the information infrastructure needs to provide end-to-end secure solutions.

# Agility

Customers demand high service velocity to adapt to their ever-changing business environments. A virtualized environment reduces the time to service customers, whether it is adding new storage or adding new servers to support growth. Efficiency and security are not enough. Customers need their information infrastructure to be agile enough to respond quickly to changing business needs and service levels.

## Other Business and Operations Challenges

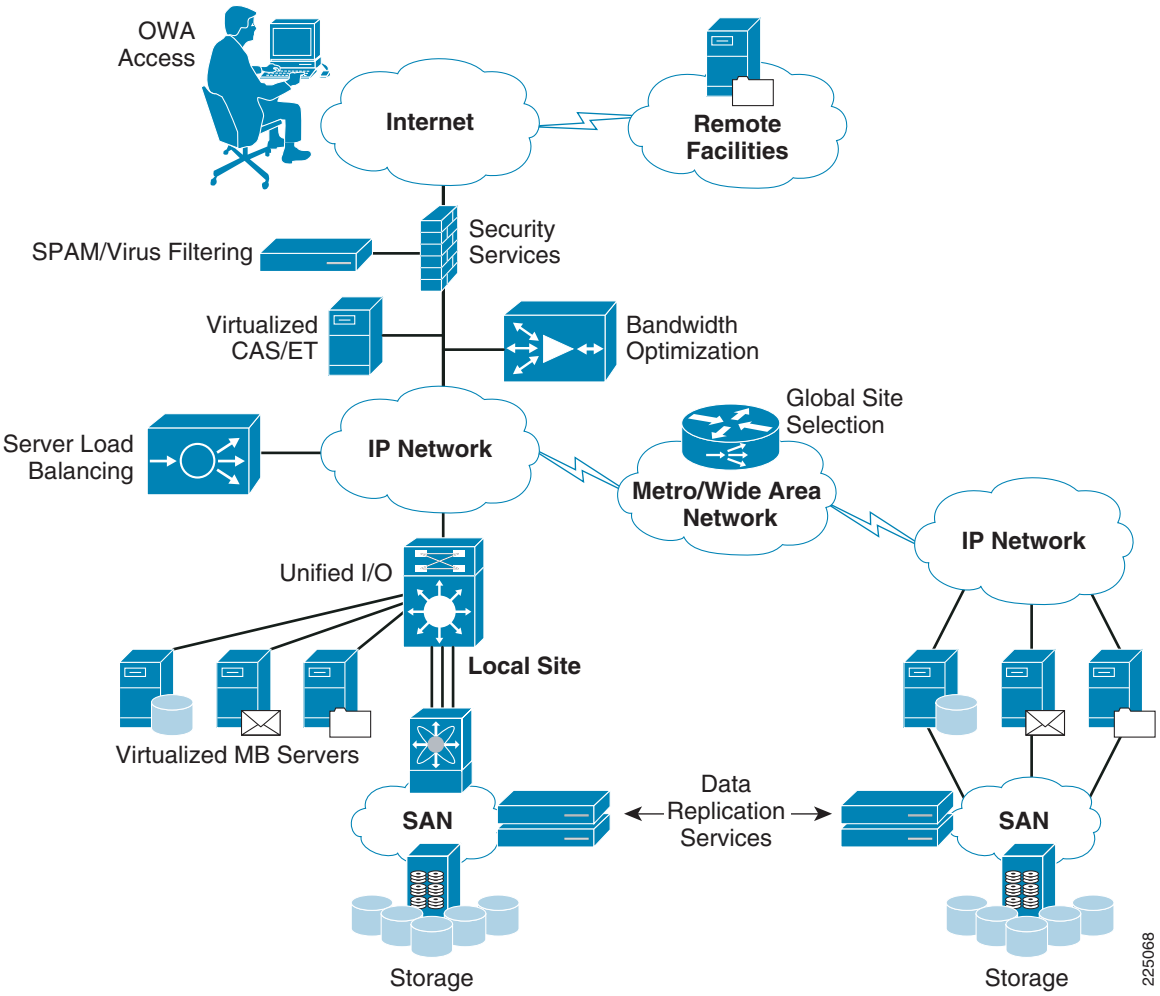
- Growth of information makes day-to-day information and infrastructure management more difficult and costly.
- Operational risks are increasing.
- Increasing data migration requirements necessitates the ability to move data between heterogeneous arrays nondisruptively, even in mission-critical environments.
- Businesses must optimally use the server resources already deployed without purchasing additional hardware.
- Customers need secure data, whether on a storage device or in real time.
- Regulatory requirements for data availability and data replication must be met.
- Businesses need a backup to remote business continuity sites more than 150 miles away.
- The cost for dark fiber connectivity is prohibitive.
- Businesses must protect their network application services.
- Large consolidated storage area networks (SANs) offer improved consolidation economics, but can be difficult to manage, secure, and keep available.
- Corporate information "at the edge" is difficult to manage, protect, and share.
- Local recovery must be simplified: These files can be backed up and restored in order to recover the server if a host fails or a system becomes corrupted. The backup is often performed through a SAN-based copy or snap technology that allows for very quick recovery of the server on the same or alternate hardware.

# Solution Overview

Microsoft Exchange 2007 provides a solid foundation for corporate messaging. However, due to high availability requirements of ever-increasing email data, the need to archive and provide mobility services, and protect email against intended or unintended threats makes it necessary to provide a holistic approach to a company's solution. A piecemeal approach can be overly complicated and difficult to maintain and manage. With EMC, VMware, and Cisco's foundation architecture for Microsoft Exchange 2007, organizations have the building blocks to ensure that the growing demands of today's rapidly changing landscape are met while protecting capital investments for years to come.

Figure 2 depicts the high level services that Cisco, VMware, and EMC provide.

*Figure 2 Cisco, VMware, and EMC Services*




This Microsoft Exchange messaging infrastructure solution is built upon elements of virtualization including server, storage, and network components that can simplify management and enable consolidation of physical assets and rapid provisioning of heterogeneous resources. It can also address other applications such as Structured Query Language (SQL) and Microsoft Office SharePoint Services (MOSS), because the solution can decouple applications from the hardware infrastructure. Within this solution Cisco, EMC, and VMware also address high availability and disaster-recovery requirements.

EMC offers a variety of storage products and capabilities that enable highly scalable solutions for every size deployment from very small mailboxes to enterprise-level environments in various topologies and capacity options, enabling you to plan for any size mailbox deployment and absorb unpredictable mail growth that is a growing challenge. Advance storage capability is an essential part for the design of Microsoft Exchange mailbox and database architectural components.

As mentioned previously, Cisco, EMC, and VMware can achieve asset usage at various levels and components. From a server perspective and consolidation point of view, VMware's capability in server consolidation can achieve compelling usage ratios by enabling the creation of multiple virtual machines within one physical server and aligning the right resources with the projected workload, such as CPU or memory draining services from specific server roles in the infrastructure.

In Exchange 2007, Microsoft introduced multiple server roles that provide different functions. In some cases some of these server roles require more resources to run their function than others. With VMware server virtualization, we can provide a methodology of server consolidation into fewer physical server entities, eliminating much needed real state within the data center and alleviating cooling, energy, and environmental data center requirements. This methodology is also ideal for the various Microsoft Active Directory servers.

High availability (HA) is another aspect being addressed through server virtualization. With VMware HA if a host fails, the host's virtual machines are brought back online by another host in the environment. VMware HA is an ideal way to protect the virtual server farm because this functionality can be extended to any Exchange server role, whereas in the past the traditional approach was to protect only the mailbox server.

In addition to server high availability, this solution also addresses information availability and mail store recovery with Virtual Switching System (VSS) technology. The EMC Replication Manager is EMC's leading VSS requestor; it provides online replication for Microsoft Exchange 2007 and an automated recovery process. Both the replication and recovery process fully adhere to an application programming interface (API) framework provided by Microsoft, which ensures proper mechanisms of replication and recovery.

With array-based replication, the recovery of Exchange databases can be performed in just minutes. Regardless of the size of the mailbox database, customers are able to provide server uptime within very strict service-level agreements (SLAs). In this solution, the storage has been designed to hold two full days worth of data on disk at all times. This means that 48 hours of data is available on high-speed disk at all times. When data older than 48 hours is required, restore from tape is used. The Replication Manager is primarily used for mailbox database recovery purposes, where corruption may have been the cause for the down condition.

EMC's Replication Manager can replicate Exchange environments in a physical environment as well as in a virtual configuration. A functionality like Vmotion provides the ability to move virtual machines from one physical server to another physical server. Replication Manager is able to adjust its replication policies and continue to replicate these environments regardless of the virtual machine movement.

As mentioned previously, email messaging has become a mission-critical application, and this solution provides an advance disaster-recovery capability by combining EMC's RecoverPoint, which provides array-to-array replication across extended distances, taking advantage of the Cisco MDS 9000 Storage Services Module (SSM). The SSM module provides compelling capability in data-splitting technology, allowing a customer to capture data in both the source and target sites.

RecoverPoint introduces two options of protection:

- Continuous Data Protection (CDP), which allows customers to capture frequent snapshots bookmarks ) of their environment for local data recovery
- Continuous Remote Replication (CRR) , which replicates data from array to array across extended distance

These two modes can be combined and, for the first time, customers are able to provide restart of services at a disaster-recovery location as well as recovery of data in case of corruption or data loss. Furthermore, RecoverPoint has extended its compelling data replication capability by integrating its replication engine with VMware's Site Recovery Manager, which provides full automation of the restart process at the disaster-recovery site for all virtual machines and applications being failed over. This key feature of automation provides additional value by removing human-error factors in a disaster event, as all policies have been predefined and can be tested by simulating these events before a disaster occurs.

Many of the components mentioned in the solution so far rely heavily on a solid infrastructure that can provide advance connectivity regardless of the topology and protocol. Cisco Fiber Channel directors provide all the high-performance connectivity needed for these critical environments.

# Technologies

- Cisco, EMC, and VMware continue to partner closely to develop key network-storage capabilities in support of virtualized environments
- Cisco is also a major investor in VMware and such continues to partner closely to develop key network-server capabilities in support of virtualized environments.
- Cisco and EMC: Technology collaboration and integration into Cisco MDS platform
- Cisco Server Load Balancing (SLB), Secure Sockets Layer (SSL) Offload, and connection management
- Cisco: VN-Link, Virtual Switch for enhanced VM capabilities, and management
- Cisco: Fibre Channel over Ethernet for enhanced server flexibility
- Cisco: MDS/SSM/SANTap
- Cisco perimeter and application security solutions such as ASA Firewalls and Cisco/IronPort spam, Malware, and Data Loss Prevention (DLP) filtering
- Cisco: MDS VSAN technology
- Cisco: Wide Area Application Services (WAAS)
- EMC CLARiiON CX3-80 storage technology
- EMC VSS requestor Replication Manager
- EMC RecoverPoint which provides for advanced data replication
- RSA: Key Manager
- EMC: Connectrix MDS
- EMC: Qualification and support
- EMC: RecoverPoint
- VMware Infrastructure with VMotion, high availability (HA), business continuity (BC), and Dynamic Resource Scheduler (DRS)

# Solution Components

This section describes the objectives and characteristics of the architecture.  Cisco, EMC, and VMware have developed a reference architecture that addresses the following business needs:

- Reduction of cost with virtualized end-to-end infrastructure and unified I/O
- Increased operational efficiencies through rapid storage provisioning services, bandwidth optimization services, and intelligent SLB services
- Meeting or exceeding compliance mandates with security services and clearly defined and achievable Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs)
- Drastic reduction in unwanted spam and viruses

This section discusses the Microsoft Exchange Server 2007 roles and provides high-level information about the EMC, VMware, and Cisco product and solution components that provide an *efficient*, *secure*, and *agile* messaging environment.

## Microsoft Exchange 2007 Server Roles

Microsoft Exchange Server 2007 uses a variety of roles to provide services. Some roles are the same or slightly different from the roles in Microsoft Exchange Server 2003, whereas others are new. Each role serves a unique purpose within the Microsoft Exchange architecture and is flexible enough to be deployed in various sizes of organizations with varying requirements.

Some roles can be installed together on a single platform or deploy them completely independent of one another. Small and medium-sized businesses can take advantage of the diverse number of Microsoft Exchange Server 2007 features while limiting the amount of hardware required for deployment. Large organizations can take advantage of the ability to deploy multiple roles in a redundant fashion on independent hardware platforms in geographically dispersed locations.

The following Microsoft Exchange Server 2007 roles are discussed in this document:

- Client Access Server (CAS) provides messaging access to a variety of client endpoints to include Outlook Web Access (OWA), Outlook Anywhere, and ActiveSync clients.
- Hub Transport (HT) performs the central role for all intelligent message routing, delivery, and control within and outside of the organization.
- Mailbox Server (MBX) ) is the database for all user messaging data; it provides access to Messaging Application Programming Interface (MAPI)-based clients such as Outlook.
- Edge Transport (ET) provides Internet Simple Mail Transport Protocol (SMTP) relay and simple message hygiene services.

## Solution Components—Efficient Environments

An efficient messaging infrastructure is achieved in this solution by taking advantage of the end-to-end virtualization, consolidation, and server offloading. Key efficiency features include:

- VMware VMotion allows clients to move running virtual machines from one physical host to another with no impact to end users. Vmotion can easily move under- or overused Microsoft Exchange servers to meet the increasing demands of businesses and end users.
- The solution is designed around VMware Site Recovery Manager to accelerate recovery and ensure successful recovery of a Microsoft Exchange Server by automating the recovery process and eliminating the complexity of managing and testing recovery plans. VMware Site Recovery Manager enables this solution to provide disaster recovery for Microsoft Exchange that is rapid, reliable, and manageable so that businesses can meet recovery objectives. By eliminating complex manual recovery steps and enabling nondisruptive testing of recovery plans, Site Recovery Manager removes the risk and worry from disaster recovery, helping businesses protect all of their important systems and applications.
- VMware Distributed Resource Scheduler (DRS) and High Availability (HA)—VMware DRS tracks the performance of virtual machines and, depending on the configuration, recommends target hosts for best performance or actually migrates hosts based on policy. VMware HA automatically restarts virtual machines that run on hosts that experience a failure; for example, if a motherboard fails or the host panics.
- Virtual machine templates can speed deployment times by eliminating repetitive operating system installation and patching tasks. New virtual machines can have their core configuration deployed in a matter of minutes, allowing rapid provisioning of applications into production and reduction of manual work required during their deployment. Organizations using virtual machine templates have reported a significant reduction in server deployment times, from as much as several weeks to provision and deploy physical servers to a matter of minutes in the VMware virtual machine environment.

- Cisco Application Control Engine (ACE) provides intelligent Server Load Balancing (SLB) for Microsoft Exchange 2007 Server components, which reside on the edge network and within the data center. Cisco ACE optimizes server resources (both physical and virtual) by ensuring these resources are load balanced intelligently with advanced algorithms and user-tunable parameters. These services increase application availability and optimize server resources. The Cisco ACE also provides SSL and TCP offload capabilities for the CAS role.
- With multiple data centers, the Cisco ACE Global Site Selectors (GSSs) are used in conjunction with Cisco ACE SLB to provide workload distribution, disaster recovery, failover protection, and Domain Name System (DNS) offloading. Optimal site load balancing is achieved by having the Cisco ACEs within the data center in active communications with the GSSs (outside the data center) to ensure optimal access across data centers. Cisco ACE also has very robust virtualization capabilities known as contexts. Each context can be configured to support very specific SLAs that allow for greater flexibility on a per-application or per-network service basis.
- Server virtualization is rapidly accelerating server use to new levels. As server use increases, so does the business-critical nature of the servers and the applications they support. One important trend is the need to add additional network interface cards (NICs) and host bus adapters (HBAs) to handle the increased LAN and SAN usage. Although the LAN interfaces have typically been increasing, the Fibre Channel side frequently has not grown at the same rate, often relying upon direct attached storage for applications such as Microsoft Exchange. For this solution, a simplified approach is proposed, combining the HBA and NIC functions. The cost associated with multiple network interfaces is multifold and includes not just capital expenditures (CapEx), but also network infrastructure, management complexity, and server resources. The ready availability of 10 Gigabit Ethernet is increasingly leading to a lessened need for as many interfaces, instead relying upon the virtualized use of common 10 Gigabit Ethernet interfaces. The logical progression has since led to the incorporation of all SAN and LAN traffic onto a common interface, thus allowing for the benefits of the EMC SAN in what has become known as Unified I/O.
- Cisco has partnered closely with VMware to introduce a new generation of server virtualization technologies known as VN-Link. Cisco VN-Link provides improved mobility for virtual machines through tight integration between the Hypervisor, virtual machines, and the network. As VMware Distributed Resource Scheduler dynamically moves virtual machines around, their network and security policies can potentially become unsynchronized with those of the network infrastructure. With VN-Link, the virtual and network infrastructures remain in a consistent state throughout. Customers can rapidly deploy virtual machines without sacrificing security, network consistency, or operational manageability.

## Solution Components —Secure Environments

Unwanted or virus-infected email messages not only distract end users, but also can reduce their productivity while placing a large processing and storage load on the messaging system. Cisco IronPort security appliances with Adaptive ASA technology provide a best-of-class email security solution, while also protecting the infrastructure as a whole. User productivity and experience are maximized by deploying these products.

Key security features of the Cisco IronPort appliance with the ASA include:

- Cisco IronPort C Series appliances are incorporated into the solution; they reside at the edge of the network behind an ASA firewall. These devices protect Microsoft Exchange servers from virus attacks, spam, and other malware before the email message is injected into the corporate network by ensuring that unwanted email messages are automatically filtered without user intervention. They significantly improve network efficiency by accurately blocking up to 80 percent of incoming spam and malware at the connection level.

- Cisco ASA provides application-aware advanced firewall and VPN security services for the Microsoft Exchange ET and CAS roles at two places in the network, the network edge (perimeter) and the data center.

## Solution Components—Agile Environments

Symmetrix and Cisco MDS storage switches with SSM provide the foundation for intelligent SAN services for the Microsoft Exchange 2007 solution.

Key agility features include:

- Virtual SAN (VSAN) provides multiple virtual SAN networks on the same physical hardware. VSANs consolidate multiple islands into a larger SAN network. They can share the physical infrastructure while retaining separate management, security, and quality-of-service (QoS) policies.
- EMC CLARiiON CX is the world's largest, most powerful midrange networked storage array. Based on the CLARiiON CX3 UltraScale architecture, CLARiiON CX3 model 80 provides high-performance, high-capacity networked storage that enables businesses to handle the most data-intensive Microsoft Exchange workloads and large consolidation projects. The CX3 model 80 provides compelling performance characteristics for Microsoft Exchange 2007 and can scale seamlessly into large deployments.
- Deploying Microsoft Exchange 2007 with VMware Infrastructure provides additional options to meet specific business and technical requirements of an organization's messaging environment. For example, using virtual machines allows the user population to be split into multiple smaller Exchange mailbox virtual machines without requiring additional server hardware. Each mailbox virtual machine can then be configured with its own unique design requirements.

Additionally, replication-enabling products such as EMC's RecoverPoint continue to provide agility in case of a planned or unplanned outage. Combined with Cisco SANTap intelligent I/O splitting, RecoverPoint enables Continuous Data Protection and Continuous Remote Replication (CRR) application (Exchange Server and Active Directory) disaster recovery for local and remote sites. For Microsoft Exchange 2007, the advanced features of RecoverPoint provide capabilities in recovering Exchange data stores from possible corruption scenarios in just minutes rather than hours and allow multiple RPO and RTP options. This seamless integration with Microsoft Exchange Server 2007 provides both an integrated approach to application protection and recovery and advance restart capability for disaster-recovery requirements.

In this solution, RecoverPoint offers the following benefits:

- It provides continuous data protection and continuous remote replication for on-demand protection and recovery at any time. Its advanced capabilities and integration with Microsoft's Virtual Shadow Copy Services VSS include policy-based management, application integration, and WAN acceleration.
- It allows the implementation of a single, unified solution to protect and replicate data across heterogeneous storage, simplifying management, reducing costs, allowing for the recovery of data at a local or remote site at any time, and ensuring continuous replication to a remote site without affecting performance.

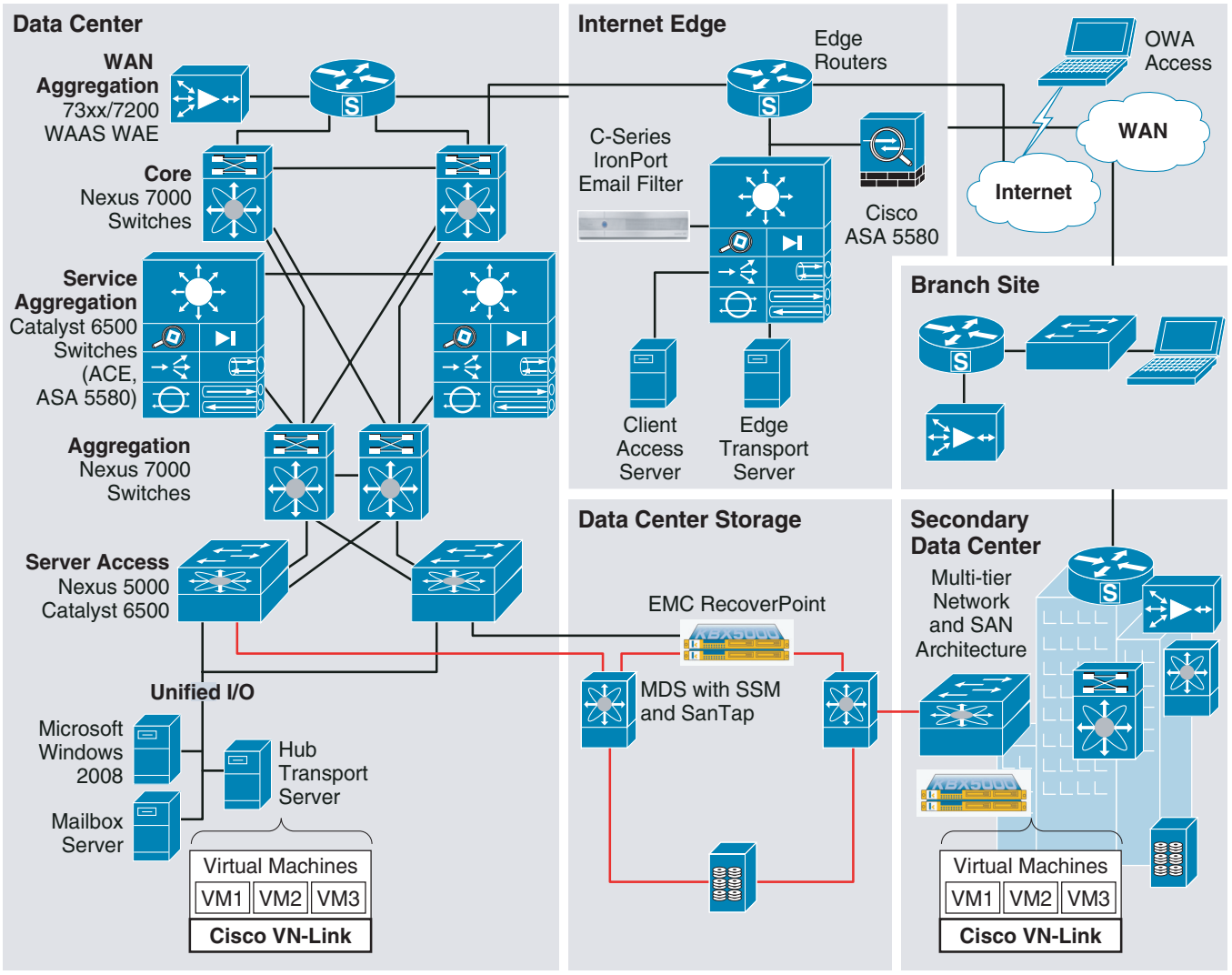
# Solution Details

## Solutions for Microsoft Exchange 2007

In order to fulfill the demanding business and technical objectives for a Microsoft Exchange 2007 environment, individual products, technologies, and an architectural approach need to be combined to build an overall solution.

Figure 3 illustrates the architectural components used in the Cisco, EMC, and VMware solution for Microsoft Exchange 2007.

*Figure 3 Cisco, EMC, and VMware Solution for Microsoft Exchange 2007*



This section provides more details about the technologies used to create the overall solution and addresses the most important aspects of a Microsoft Exchange 2007 environment, including the following:

- Sizing and performance management
  - SLB, SSL Offload, and server connection management.
  - WAN optimization.
  - Specific Exchange 2007 advanced I/O, capacity, scalability, and performance sizing: All these methodologies are published in Microsoft's Exchange Storage Reviewed Program (ESRP) and follow very strict standards of testing, taking advantage of the native Microsoft performance tools.
  - Validation of extended distance replication: Within ESRP, EMC has validated extended distance replication, with RecoverPoint reaching compelling performance characteristics and savings by using advanced data-compression ratios, reducing the operating cost of the solution.
  - Optimal performance: With the Cisco and EMC Connectrix MDS offering, best practices for SAN zoning allow Microsoft Exchange Server 2007 to perform optimally at all stages of the day.
- Resiliency and availability
  - Application availability through DNS or routing (Interior Gateway Protocol [IGP] or Border Gateway Protocol [BGP] and Cisco Route Health Injection Protocol [RHI]).
  - Site selection.
  - SAN virtualization and alternate paths in mirror fabric topologies: This feature allows for any deployment to have fully redundant and fault-tolerant connection to all servers and data. These topologies integrate with and facilitate a variety of connectivity requirements from Microsoft, such as clustering and native topology requirements.
  - Storage virtualization services and mobility: Cisco and EMC realize the critical interaction with VMware ESX server mobility requirements, and both Cisco and EMC provide end-to-end SAN virtualization so when any of the Microsoft Exchange Server roles need to be moved from physical host to physical host, the data that is accessed by that role is available.
  - EMC advanced CLARiiON array technology and Cisco technology such as redundancy in storage, power, cooling and processing: These technologies bring five-nines uptime availability, a key factor in designing this messaging infrastructure.
- Disaster recovery
  - SANTap with Continuous Data Protection and CRR services can provide the best combination for restart of services as well as data-recovery tools fully integrated with Microsoft's VSS technology. Because disaster restart and data recovery are two very different challenges, both Cisco and EMC have developed best-of-class technology within one single product offering to address these uptime requirements.
- Security
  - Application and network security for Microsoft Exchange Server roles located anywhere in the network to include the perimeter and data center.
  - SAN N Port Identifier Virtualization (NPIV) capabilities, which allow each virtual machine to have its own data path to the SAN.
  - EMC's RSA capabilities: With RSA, EMC can secure access to disk technology by requiring authenticated access to the array.
  - Cisco IronPort C Series Email spam and virus filtering appliance.

- Management
  - Rapid provisioning with deployment wizard and virtual machine templates reduces the time and effort for creating and deploying virtual machines to a few mouse clicks.
  - Performance-monitoring capabilities, including usage graphs of CPU, memory, disk I/O, and network I/O, provide the detail needed to analyze the performance of physical servers and the virtual machines they are running.
  - Operational automation through task scheduling and alerting improves responsiveness to business needs and prioritizes actions needing the most urgent attention.
  - Secure access control, robust permissions mechanisms, and integration with Microsoft Active Directory provides centralized user and permissions management.
  - Resource optimization through performance monitoring, multiserver resource pools, and dynamic workload balancing delivers a very high virtual machine-to-physical server ratio while improving service levels to software applications. Automated data center-wide resource optimization with VMware DRS aligns available resources with predefined business priorities while streamlining labor- and resource-intensive operations across disparate hardware, operating system, and software applications.
  - Migration of live virtual machines across entirely separate physical servers with VMware VMotion makes the maintenance of IT environments nondisruptive.
  - Migration of live virtual machines across entirely separate storage arrays with VMware Storage VMotion allows nondisruptive maintenance and optimization of storage environments.
  - High availability provided by VMware HA enables broad-based, cost-effective application failover independent of hardware and operating systems.

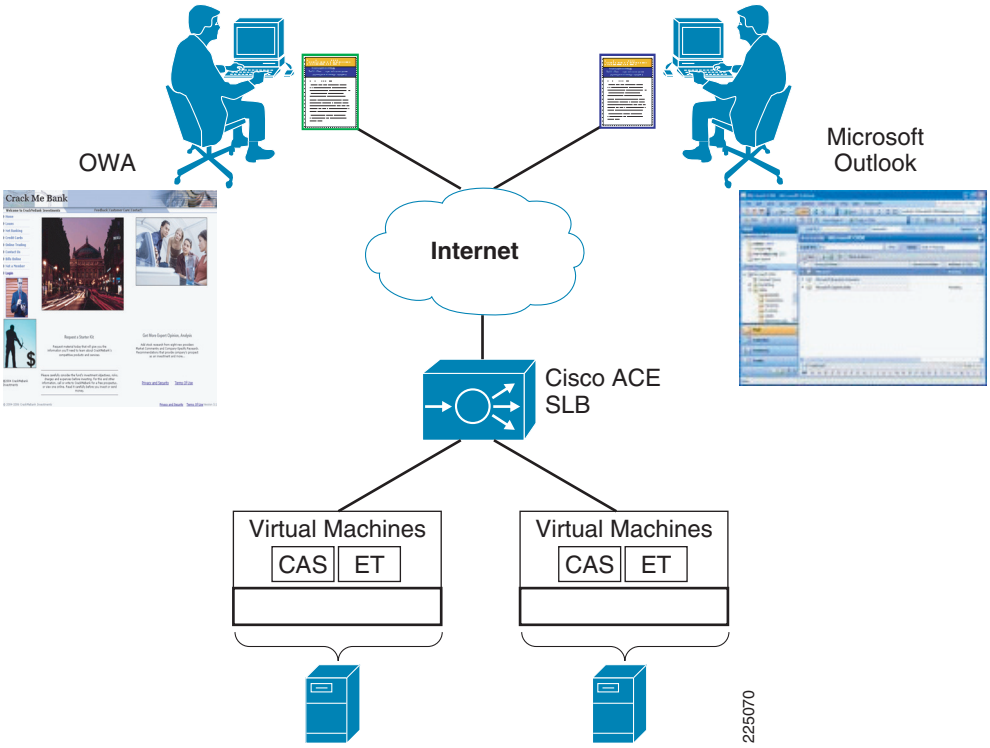
## Sizing and Performance Management for Exchange

The sizing of Microsoft Exchange components incorporates not only the server and SAN hardware (memory, CPU, bus, and disk), but also the size of the load on the system itself based on the role it performs. The following subsections discuss the Cisco solution components used to ensure that the appropriate Microsoft Exchange roles have as much traffic and processing offloaded as possible, while maintaining service availability as seen by the end user.

## Cisco Sizing and Performance Management for Microsoft Exchange 2007

Figure 4 shows a high-level diagram of the Cisco ACE load balancing ET and CAS roles in a virtual machine environment.

***Figure 4 Cisco ACE Server Load Balancing***




The only server roles in Microsoft Exchange 2007 that can be effectively load balanced are the CAS and Edge Transport roles. The Cisco ACE module or appliance can be used to load balance connections from OWA, Outlook Anywhere, and SMTP to the "best" or most appropriate server. The Cisco ACE is configured to front-end multiple CASs, and a single VIP is configured on the ACE to represent all CASs behind it. The single VIP is added to DNS for the clients to use. The ACE monitors the health of the CAS through a range of health probes to ensure not only that each individual server is available through the IP address, but also that the CAS services such as OWA are available. If a probe fails, the ACE removes the failed server out of its rotation list and sends an alert to the administrator. The ACE supports the following health probes (only the probes appropriate for Microsoft Exchange 2007 are listed):

- ICMP
- TCP
- UDP
- HTTP
- HTTPS (SSL probes)
- DNS
- SMTP
- IMAP

- Post Office Protocol (POP)
- Scripted (Tool Command Language [Tcl] support)

A similar approach is taken with the Edge Transport (ET) role. The ACE front-ends the ET and has a virtual IP (VIP) that is registered in DNS as an Mail Exchanger (MX) record. SMTP messages are forward to the VIP based on the DNS MX record entry and the ACE forwards the SMTP connection on to the most appropriate server based on a variety of configurable metrics such as basic availability, load, site preference, etc.

### SSL Offload

The Cisco ACE is capable of providing secure transport services to applications residing in the data center. It implements its own SSL stack and does not rely on any version of OpenSSL. The Cisco ACE supports Transport Layer Security (TLS) 1.0 and SSLv2 and v3 hybrid protocols. Three SSL relevant deployment models are available to each ACE virtual context:

- *SSL termination*—This feature allows for the secure transport of data between the client and ACE virtual context. The Cisco ACE operates as an SSL proxy, negotiating and terminating secure connections with a client and a nonsecure or plaintext connection to an application server in the data center. The advantage of this design is that the ACE offloads the demands of SSL processing from the CAS CPU and memory, allowing the CAS to focus strictly on processes related directly to Exchange and not those of SSL.
- *SSL initiation*—This feature provides secure transport between the Cisco ACE and the CAS server. The client initiates an unsecure HTTP connection with the ACE virtual context, and the Cisco ACE acting as a client proxy negotiates an SSL session to an SSL server.
- *SSL end-to-end*—This feature provides a secure transport path for all communications between a client and the CAS server residing in the data center. The Cisco ACE uses SSL termination and SSL initiation techniques to support the encryption of data between the client and the CAS server. Two completely separate SSL sessions are negotiated, one between the ACE context and the client, the other between the ACE context and the CAS. In addition to the intelligent load-balancing services the Cisco ACE provides in an end-to-end SSL model, the system administrator can alter the intensity of data encryption to reduce the load on either the front-end client connection or back-end application server connection to reduce the SSL resource requirements on either entity.

### SSL URL Rewrite Offload

The Cisco ACE can insert or delete HTTP header information for connections it is sustaining. This capability is highly useful when a CAS server responds with a HTTP 302 or "Moved Temporarily" response to a client's HTTP GET or HEAD request. The HTTP 302 response usually indicates a new HTTP LOCATION URL for the client to access. Modifying the HTTP LOCATION value for a secure connection is known as SSL URL Rewrite, a feature that allows the system administrator to alter the HTTP LOCATION value returned to the client, resulting in granular control of session flow and persistence of the application in the data center.

### SSL Session ID Reuse

SSL Session ID Reuse allows the client and server to reuse the secret key negotiated during a previous SSL session. This feature generally improves the volume of SSL sessions that a CAS can effectively maintain. Clients residing with remote connectivity, for instance across a WAN, generally benefit from this feature. The SSL negotiation load is effectively reduced on the SSL proxy server while simultaneously improving the user experience because key negotiation is a rather lengthy process. The Cisco ACE may maintain the SSL session ID indefinitely or up to 20 hours with a timeout configuration.

Note that SSL Session ID Reuse does not compromise the security of the data center. The feature only acknowledges that a secret key already exists between the client and server. Nevertheless the client must use this key for the application server to receive data from the client. The security resides in the secret key, not the SSL session ID.

### Allowed Server Connections

Enterprise data centers should perform due diligence on all deployed server and network devices, determining the performance capabilities to create a more deterministic, robust, and scalable application environment. The Cisco ACE allows the system administrator to establish the maximum number of active connections values on a per-server basis or globally to the server farm. This function protects the end device, whether it is an application server or network application-optimization device such as the Cisco Wide Area Application Engine (WAE).

**Note** For more information about these enhanced services, refer to the *Cisco Wide Area Application Services (WAAS) V4.0 Technical Overview* at the following URL: http://www.cisco.com/en/US/products/ps6870/products_white_paper0900aecd8051d5b2.shtml

### Microsoft Exchange 2007 Storage Sizing

With storage technology, EMC introduces an easy approach to sizing and configuring storage for use with Microsoft Exchange Server (mailbox servers). This process is complicated, affected by many variables and factors that vary from organization to organization. One method often used to simplify the sizing and configuration of large numbers of mailboxes is to define a unit of measure. EMC developed this unit-of-measure "building block" (see Figure 5), which needs to be scalable for unpredictable growth, a frequent challenge in many organizations. In that way, an organization can simply take this block of work and multiply it by some factor until the desired number of Microsoft Exchange Server users (that is, Microsoft MAPI Outlook users) has been properly met or configured to satisfy the Microsoft Exchange Server-recommended performance metrics. If each unit is properly configured, it will match the Microsoft Exchange Server recommendations for a healthy-performing system from both disk and end-user perspectives.

This methodology also allows for a highly efficient work distribution in the disk array activity and the path used in the SAN. With multiple disk configuration features within the Symmetrix and CLARiiON, this well-balanced configuration for Microsoft Exchange Server 2007 meets and exceeds I/O latency requirements.

*Figure 5 Building Blocks*

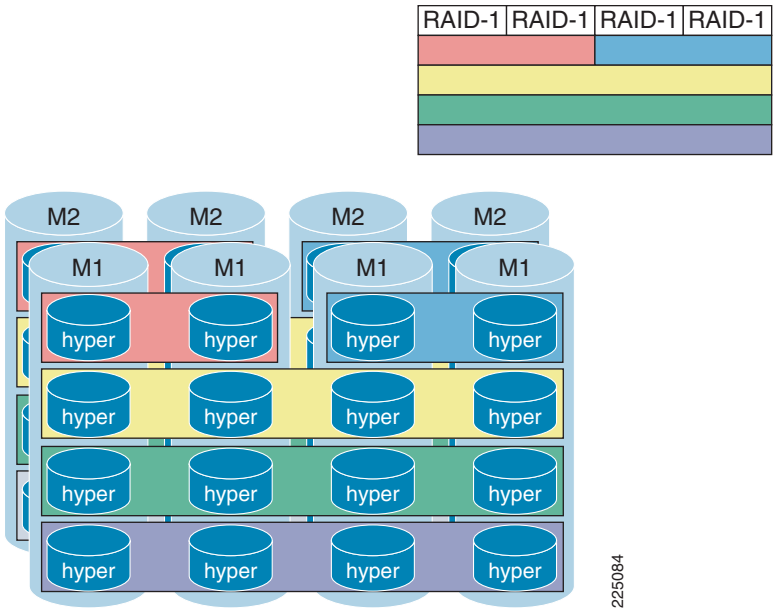



Figure 5 represents the basic concept of the storage building block. A given number of disks are associated with a given workload associated with Microsoft Exchange databases and log files.

A building block offers the following benefits:

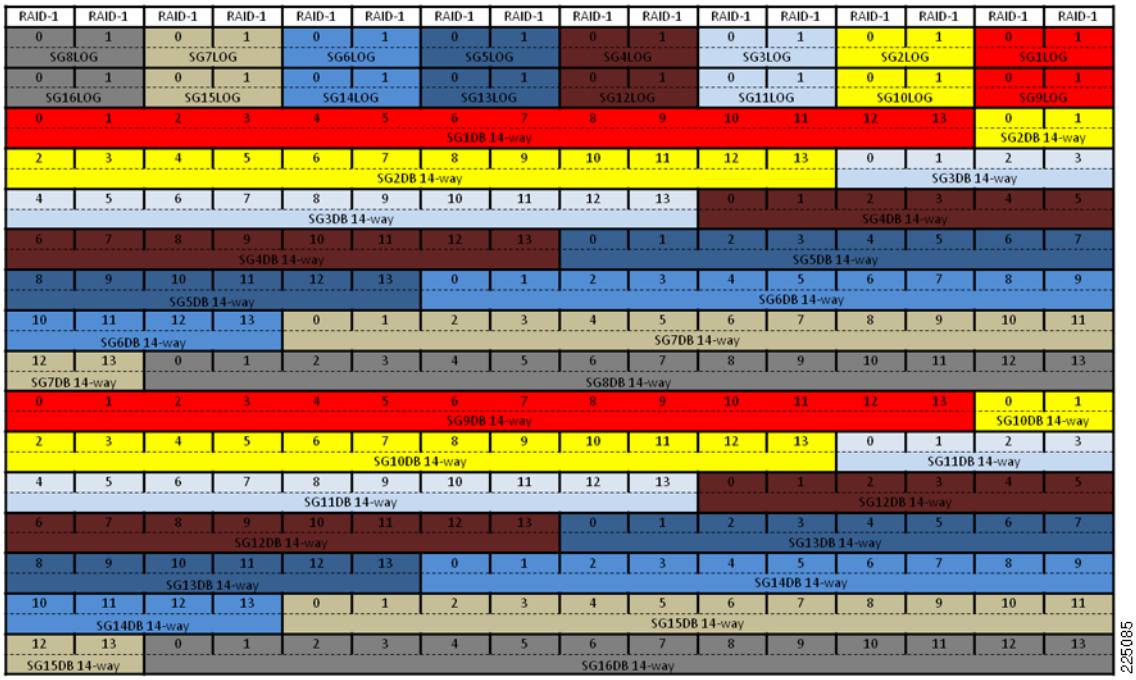
- The design is simple.
- I/O is balanced over physical disks.
- Stroke distance is independent of mailbox database size.
- Some designs will only half stroke the disk, with 50 percent of the capacity used.
- Building blocks provide worst-case seeking distance from day 1.
- Disk performance will not get any worse because of the seek distance.
- If user activity increases, only the I/O rate will go up, not the seek-related response time.
- Building-block performance capability is specified in Exchange 2003 or 2007 I/O.
- Each server has its own building block.
- Other servers or applications introduce no interference.
- Scalability testing is easy.

When testing scalability for a given component, ensure that all other components do not create a bottleneck. Table 1 provides a sample of CLARiiON storage building blocks, and Figure 6 shows how the Microsoft Exchange 2007 storage group building block is applied.

*Table 1 CLARiiON Storage Building Blocks Sample*

| Number of Virtual Machine Building Blocks | Number of Users | Production Disks | Backup Clone Disks |
|---|---|---|---|
| 1 | 2,000 | 12 disks (8 database and 4 log) | 6 disks |
| 2 | 4,000 | 22 disks (16 database and 6 log) | 12 disks |
| 3 | 6,000 | 32 disks (24 database and 8 log) | 18 disks |
| 4 | 8,000 | 44 disks (32 database and 12 log) | 24 disks |
| 5 | 10,000 | 54 disks (40 database and 14 log) | 30 disks |
| 6 | 12,000 | 64 disks (48 database and 16 log) | 36 disks |

*Figure 6 Exchange 2007 Storage Group Building Block Applied*




## VMware Host Sizing

Using VMware virtual machines for a Microsoft Exchange 2007 deployment avoids costly overprovisioning of Exchange server computing resources. Organizations can size their infrastructure based on current requirements and use excess capacity on their 64-bit servers to run other virtual machine workloads. CPU and RAM resources can be monitored and fine-tuned at any time to meet changing performance requirements. The ability to adjust resources in this manner provides new levels of flexibility for Exchange virtual machines running on a VMware Infrastructure 3 platform that are not possible without virtualization. In a physical server-based Exchange deployment, there is a tendency to overprovision server resources, because resources typically remain static until the next upgrade cycle of hardware provisioning. Projected increases in the number of Exchange end users through growth or

acquisition can be difficult to estimate, but still must be factored into server provisioning and sizing decisions. In an attempt to avoid problems associated with moving an Exchange Server to a newer physical machine, many system implementers oversize physical server CPU and memory resources during the design of the system infrastructure to account for future growth. This oversizing can result in wasted computing capacity, because the resources of these servers are rarely fully used. This problem can be avoided using VMware virtual machines. CPU and memory allocated to the virtual machine can be increased at any time with a simple reboot of the virtual machine. Moreover, the CPU and memory allocated to a virtual machine can be sized more realistically based on current workloads and adjusted at any time as the workload increases.

## Resiliency and Availability

Each data center site provides a highly available and robust network and network-based services for the local Exchange environment. The introduction of multiple data centers extends the n-tier Exchange application model between sites. Therefore, the network must address the state of the application tier at each site to provide user, application, and data-recovery services. To this end, the availability design takes advantage of the following technologies:

- Site selection technologies combining DNS with high availability services such as Keep Alive-Application Protocol (KAL-AP)—These technologies are available on the GSS to ensure proper name resolution exists for the Internet-facing Exchange roles such as CAS and ET.
- Route Health Injection (RHI)—Available on the Cisco ACE, RHI is used to ensure that individual CAS and ET servers are taken out of load-balancing rotation if they become unavailable.
- Fabric availability—Fabric availability provides redundant access to storage and storage services through dual fabric connections.

### Site Selection

Site selection (or content routing) provides user recovery services associating a single user with an application instance. The use of Cisco ACE GSS offers the following benefits to Microsoft Exchange:

- Workload distribution
- Disaster recovery and failover protection
- Improved user experience
- DNS offload

The GSS appliances are the external DNS authoritative name servers for the enterprise providing “A” and Mail Exchanger (MX) records for the domain. The GSS appliances are deployed at the edge of the network as a cluster. Clustering the GSS boxes across multiple enterprise sites provides for a highly available and scalable DNS solution. It is important to note that each GSS houses an instance of Cisco's Network Registrar (CNR) that supplies the MX resource records to properly route Internet mail into the enterprise.

Typically, enterprise deployments take advantage of DNS-based round-robin and multiple MX records to distribute load across multiple Internet mail servers. This method provides redundancy and scalability but relies heavily on the client mail application to resolve DNS and MX records for mail delivery. MX preferences of equal value are the equivalent of round-robin load balancing. Lower MX preference values receive higher priority from the clients' mail applications.

The Cisco GSS includes the following factors prior to responding to a DNS request such as an MX record:

- Availability (of server and/or VIP)
- Proximity
- Load
- Source of the request (DNS proxy)
- Preference

To provide a higher-level of scalability and availability for inbound and outbound mail processing, administrators can load-balance across multiple ET roles. A load-balancer, such as the Cisco ACE, provides high availability and scalability within a single data center and can communicate the state of the ET roles to the Cisco GSS that are globally aware. The GSS may probe the ACE VIP at each site using multiple probe types. Combining these probes allows the GSS to gain better insight into the state of the ET roles located at each data center, providing a more intelligent form of SMTP server (i.e., site selection).

In addition to using a more intelligent traffic routing scheme with DNS, the ability for the Cisco ACE GSS to track the availability of a CAS or ET server through the GSS and ACE load balancer with KAL-AP probes allows for the "best" or available servers to be selected. If one or all of the CAS or ET servers are unavailable at a site, the system can make decisions about where to redirect traffic (either within a site or between sites). The Cisco ACE GSS is configured to "track" a VIP on the ACE load balancer or even the server IP directly through the KAL-AP probes. If the probe fails then the GSS takes that server or VIP out of rotation (if load balancing) or service (if actively forwarding requests to that service) and redirects requests to the other available sites. When the probe recovers (service comes back online), the GSS begins forwarding requests to that site or server again. This process is automatic based on defined policies.

For more information about the Cisco Global Site Selector, refer to the following URL:

http://www.cisco.com/en/US/products/hw/contnetw/ps4162/tsd_products_support_series_home.html

### Route Health Injection

RHI on the Cisco ACE module or appliance can announce to the network whether or not the VIP that is associated with a group of servers such as CAS and ET is available. RHI works with the health probes, as discussed previously, to ensure that at least one server (a threshold can be defined for RHI) is available for the service that is associated with the VIP. If all available servers behind the VIP are unavailable (or an administrator decides to take it out of service), RHI takes the VIP out of service, resulting in removal of the route for the VIP from the network. Traffic destined for the VIP either sees the address as unreachable or the network can reroute the traffic to another active VIP somewhere else (such as the other data center).

### Session Persistence

Session persistence is the ability to forward client requests to the same server for the duration of a session. Microsoft recommends session persistence for its Microsoft Exchange environment through the following methods:

- Source IP sticky
- Cookie sticky

The Cisco ACE supports each of these methods, but given the presence of proxy services in the enterprise, Cisco recommends using the cookie sticky method to guarantee load distribution across the server farm wherever possible as session-based cookies present unique values to use for load balancing.

In addition, the Cisco ACE supports the replication of sticky information between devices and their respective virtual contexts. This provides a highly available solution that maintains the integrity of each client's session.

### SAN Virtualization with Cisco MDS

Most if not all SAN deployments use dual-fabric SAN design. Cisco added another level of protection with VSANs, which provide SAN virtualization on the Cisco MDS platform. VSANs are similar to VLANs on an IP network. Microsoft Exchange Servers and storage can be segregated to their own VSAN for added protection and reliability. Changes on VSANs associated with enterprise resource planning (ERP) or engineering do not affect hosts and storage on the Microsoft Exchange VSAN sharing the same physical SAN. VSANs also provide additional security features such as SAN segregation for back- and front-end disk access in a virtualized storage environment.

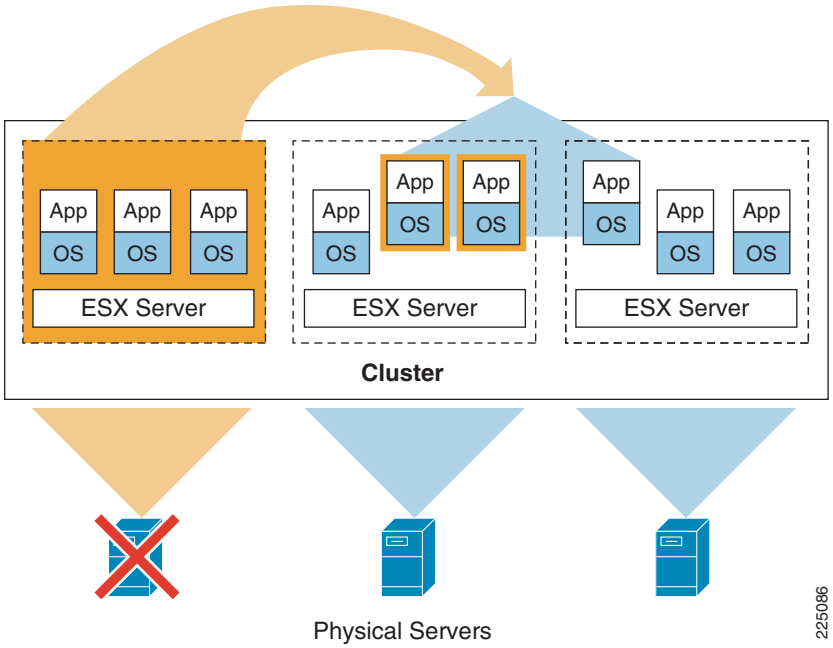
### VMware High Availability with Minimal Complexity

The VMware Infrastructure platform can be leveraged to provide a wide-range of availability options. VMware HA provides protection from server hardware failure that is independent of the operating system or applications and works for every virtual machine running on VMware Infrastructure. To aid in dynamic load balancing of Exchange virtual machines, VMware DRS can be used to balance workloads automatically. Base solutions built on VMware HA and DRS can be deployed with minimal configuration changes and provide a robust availability solution. These solutions can also be enhanced to provide higher levels of availability by combining them with more traditional clustering and replication options.

By taking advantage of the inherent benefits of a virtualization-based platform, an Exchange deployment using VMware Infrastructure offers a variety of availability options. Each of these options provides different levels of both protection and cost, capable of meeting the unique high availability requirements of any Exchange environment. Many of the tools available from EMC and Cisco can be used to facilitate both in-site and remote-site availability and recovery. The VMware Infrastructure platform uses two powerful features as the basis for building high availability solutions:

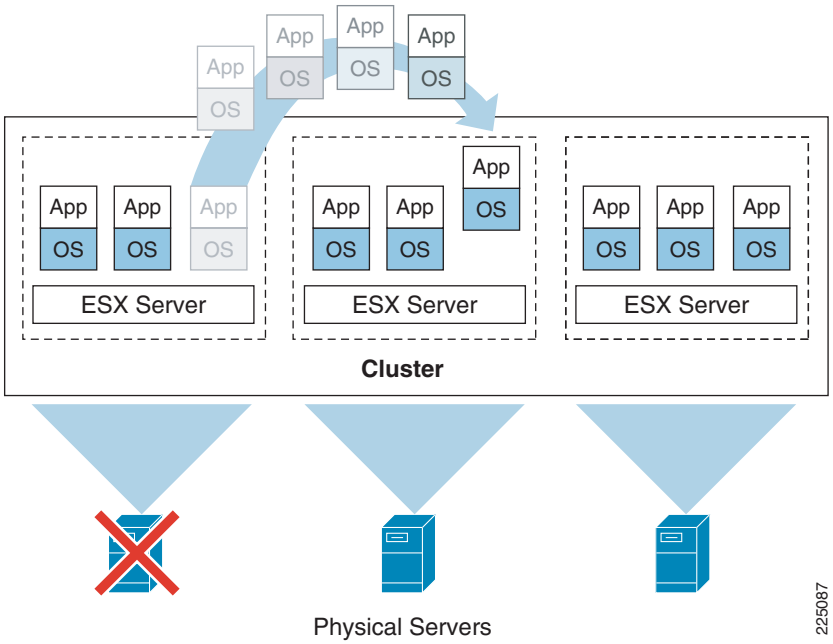
- *VMware High-Availability (HA)*—This solution provides simple, low-cost protection for virtual machines by guarding them against physical host failure. If a server hardware outage occurs, VMware HA automatically restarts all virtual machines on another VMware ESX server, minimizing disruption to the Exchange environment. Simple to set up, VMware HA protects every virtual machine without requiring complex clustering software. See Figure 7.

*Figure 7 VMware HA*




- *VMware Dynamic Resource Scheduler (DRS)*—With VMware DRS, virtual machines are dynamically load-balanced across an entire pool of server resources. DRS collects resource usage information for all hosts and virtual machines and generates recommendations for virtual-machine placement. These recommendations can be applied manually or automatically. DRS can dynamically load balance all virtual machines in the environment by shifting workloads across the entire pool of ESX servers, ensuring that critical Exchange virtual machines in the environment always have the CPU and RAM resources they need to maintain optimal performance. See Figure 8.

*Figure 8 VMware DRS*




Solutions built using VMware HA and VMware DRS combined with EMC and Cisco technologies provide out-of-the-box high availability for the entire Exchange environment without requiring any Microsoft or other third-party clustering software. A critical weakness in most clustered Exchange architectures is their coverage of mailbox servers only, leaving critical supporting server roles (DNS, domain controllers, Exchange Hub, CAS servers, etc.) vulnerable to outages due to hardware failure. Cisco provided the necessary redundancy through the Cisco Nexus® 1000v.

For Exchange environments deployed with Cisco, EMC, and VMware Infrastructure, the joint solution provides a new alternative that takes advantage of the simplicity of standalone virtual machines while providing complete server hardware redundancy for every virtual machine, not just the mailbox server. VMware HA focuses on hardware failure, not on operating system or software failure. If you need greater levels of protection and guarantees of availability for the Exchange mailbox server to handle those situations, you can combine VMware HA with traditional cluster solutions such as Windows Server Failover Clusters (WSFC).

## Disaster Recovery

### SANTap with Continuous Data Protection and CRR Services

Cisco SANTap is an API that provides storage application access to the Cisco intelligent storage network. The SANTap service uses the storage network intelligence on a Cisco SSM card. The EMC RecoverPoint appliance uses SANTap to provide two types of replication services, Continuous Data Protection and CRR. Continuous Data Protection is for local continuous data protection, whereas CRR is for continuous remote replication. Because SANTap with SSM is a copy of the I/O between the Microsoft Exchange Servers and the disks, there is no latency or effect on the I/O requests from the Microsoft Exchange Servers. Even long-distance EMC RecoverPoint CRR services will have no delayed disk I/O on primary Microsoft Exchange Servers. Because SANTap takes advantage of network intelligence on the SSMs, no additional host drivers are required on the Exchange Servers, resulting in seamless integration of the Microsoft Exchange recovery process with EMC RecoverPoint.

## Disaster Recovery and Remote Replication with RecoverPoint and VMware SRM

Data replication for the purposes of disaster recovery should always be evaluated based on customer business requirements and needs. In many cases, these requirements will determine the best replication technology based on distance, disaster-recovery compliance requirements, customer budget, ability for the business to function with or without email messaging, and other factors.

Before examining the technology applied in this solution, it is important to know the differences between the following terms:

- *Restart*, as defined by EMC, is a point-in-time recovery.
- *Restore* is the act of bringing data back to disk for an application.
- *Recovery* ensures logical integrity while applying newer data
- *Resiliency* is the ability to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation.

Typically, most clients require all of these factors in their business continuance and disaster-recovery requirements. They are all required with RecoverPoint and its integration with Microsoft's Volume Shadow Copy Services.

### What is Volume Shadow Copy Service (VSS)?

Volume Shadow Copy Service (VSS) is a Microsoft framework introduced in Windows 2003 that allows the online replication of Exchange databases. This mechanism guarantees consistency of the replicas for recovery purposes if a failure or corruption occurs. It is a coordination service by which writers (i.e., applications such as Exchange and SQL), providers (i.e., storage hardware drivers for CLARiiON and Symmetrix), and requesters (RecoverPoint) communicate with one another.

RecoverPoint offers a variety of functions that address Exchange data recovery through VSS database replication through consistency groups that will ensure proper paring of devices when being replicated on extended distances. This combination yields:

- Recovery of data
- Restartability of services at the remote site
- Backup and restore enablement through VSS

This section details the following functions:

- RecoverPoint is a comprehensive data-protection solution providing integrated continuous remote replication and Continuous Data Protection, allowing users to recover applications remotely to any point in time.
- RecoverPoint Continuous Data Protection offered as a standalone solution or combined with CRR enables rollback to any point in time for effective local recovery from events such as database corruption at either site.
- RecoverPoint supports VSS replication and supports storage arrays from EMC and other vendors, and can be easily managed from a GUI or a command-line interface (CLI).

VSS provides a great integration point with Microsoft Exchange 2007, because the replication process taking place in RecoverPoint is through Microsoft's VSS integrated API framework. This framework allows Exchange databases to be recovered in a highly efficient way and the management is done at the Exchange object level. The VSS framework also integrates additional steps to validate replicas (ESEUTIL checks) to ensure this replication cycle is successful every time.

Through VSS and RecoverPoint Continuous Data Protection and CRR, it is possible to maintain consistent copies of your environment that can be used to recover, restart or provide backup capability through these idle VSS snapshots, taking the backup overhead completely away from the production servers. With VSS, all replication is done 100 percent online and the production server never needs to be taken down.

When using VSS as means of replication, it is possible to secure backup windows easily and offload these processes during business hours. In addition, recovery is extremely compelling, because with disk-to-disk replication and recovery the data recovery occurs, in some cases, within just minutes. RecoverPoint also can replicate the Exchange logs and databases together in consistency groupings, so a disaster-recovery restart process can be done consistently.

RecoverPoint also integrates with VMware's Site Recovery Manager, a pioneering new product for disaster-recovery management and automation. VMware Site Recovery Manager, which is part of VMware's suite of management and automation products for the data center, takes advantage of virtualization to simplify business continuity planning and testing, and reduces the risk and complexity associated with executing disaster recovery.

Traditional recovery plans leave organizations exposed to significant risk of extended downtime because they are laborious to set up, time-consuming to maintain, and extremely difficult to test. As a result, only a subset of important systems can be adequately protected. For example, traditional disaster-recovery plans for data centers require extensive documentation consisting of hundreds of pages of instructions contained in runbooks that are nearly impossible to keep accurate and up-to-date. The complexity of the manual recovery processes in these runbooks makes it difficult for organizations to reliably recover within their recovery-time objectives. Traditional nonvirtualized systems have extensive dependencies on hardware configurations, making consistent automation of the process extremely difficult, if not impossible.

Site Recovery Manager works seamlessly with VMware Infrastructure, VMware VirtualCenter, and replication software from storage partners to provide integrated disaster-recovery management and automation. It provides:

- Integrated management of disaster-recovery plans—Create, update, and document nondisruptive testing of disaster-recovery plans. Execute automated tests of recovery plans in an isolated testing environment using the recovery plan that would be used in an actual failover. Hardware configuration dependencies are eliminated and testing can occur without affecting production systems.
- Automated failover and recovery—Automate execution of the recovery process, eliminating many of the slow and unreliable manual processes common in traditional disaster recovery.

### VMware Simple and Reliable Exchange Disaster Recovery

VMware Infrastructure 3 simplifies Exchange disaster recovery by reducing hardware compatibility constraints and, through consolidation, the number of servers required at the disaster-recovery site. Combined with the Exchange Transportable Database feature in Microsoft Exchange 2007, recovery from both hardware and software failure is greatly improved, reducing the time to restore essential mail services to the end users. Hardware independence allows the Exchange virtual machines to be restarted on any supported ESX server and Exchange server replication is simplified using virtual machine encapsulation.

An important benefit of virtualization is abstraction of the operating system and application from the underlying physical server hardware. This abstraction is extremely useful in disaster-recovery scenarios because it eliminates the traditional requirement of physical server-based disaster recovery to provide identical hardware at the disaster-recovery site. Any virtual machine can be brought online on any supported ESX server without worrying about hardware or software compatibility. The ability to run multiple virtual machines on a single server also reduces the costs of a disaster-recovery solution through

consolidation of Exchange components and services on fewer physical servers than would normally be required. Thus, all the necessary Exchange server roles and Active Directory components can be run in virtual machines at a disaster-recovery site with minimal hardware to speed recovery in a disaster situation.

Regardless of the make and model of the physical server hosting the virtual machines in production, virtual machines can be brought online on any VMware-supported ESX server at the disaster-recovery site. Older servers freed from other VMware Infrastructure consolidation projects are commonly repurposed to host a disaster-recovery site, minimizing the overall lifecycle costs of hardware.

When used in conjunction with VMware Infrastructure 3, the Exchange 2007 "database portability" feature creates additional options for disaster recovery. Standby virtual machines can be configured with the Exchange mailbox role and made available at both the production and disaster-recovery sites. These virtual machines can be easily configured to connect to existing Exchange databases during a recovery.

Finally, virtual machine encapsulation means that an entire Microsoft Exchange 2007 server can be contained in a small set of files, simplifying replication to disaster-recovery sites. Moving an entire virtual machine can be accomplished with a simple file copy.

## Security

### SAN NPIV

NPIV is used with VMware ESX servers.  In a virtual machine deployment of the Microsoft Exchange environment, there is no way to assign a logical unit number (LUN)  WWN directly to a virtual machine without NPIV.  With NPIV, each virtual machine in the Microsoft Exchange environment obtains its own WWN.  Disk access and SAN zoning are granted at the virtual machine level.

With NPIV, SAN administrators see the virtual machines and can identify their traffic and add a redundant layer of LUN masking and QoS controls, but the virtual machines are still isolated as before, and they have no additional visibility into the SAN. They still do not see the Fibre Channel HBAs and cannot see the Fibre Channel targets or scan for LUNs that are not explicitly assigned to them by the ESX Server administrator. Using NPIV, a WWN can be uniquely associated with a virtual machine, and it remains associated with that virtual machine even as the virtual machine is dynamically transferred, using VMotion, across physical ESX Server hosts in a virtualized environment.

### Cisco IronPort Security

The Cisco IronPort C Series contains a powerful multilayered approach to email security -- providing advanced threat prevention, blocking spam and viruses, and enabling corporate data loss prevention and remediation. Key features include:

- Spam protection
  - Cisco IronPort Senderbase Reputation Filtering typically rejects more than 80 percent of all incoming connections that are from senders known through Senderbase to be malicious. Senderbase, as with all Cisco IronPort technologies, strives for and maintains the lowest false-positive rates in the industry. Rejecting connections from known malicious senders is highly effective in combating spam, and greatly increases the effective performance of the platform.
  - Cisco IronPort antispam provides best-in-class spam protection with the lowest false-positive rate in the industry while maintaining very high spam catch rates; Cisco IronPort antispam uses a suite of cutting-edge technologies and strategies that consistently outperform competitive solutions.

- Virus protection
  - Cisco IronPort security appliances provide a choice of anti-virus vendor, all of which provide effective anti-virus protection.
- Data loss prevention and business class email
  - Cisco IronPort Business-Class Email (BCE) provides a cutting-edge solution to on-demand and policy-based email encryption. BCE uses Cisco IronPort PXE encryption, which is based on strong industry-standard encryption technologies, supports envelope-based use policies such as secure forward and secure reply, and provides guaranteed delivery and read receipts.
  - Cisco IronPort DLP augments IronPort BCE with a growing set of rules and policy templates to detect and manage outbound content, helping to protect your organization from unintended data and intellectual property loss.

For more information, refer to the following URL:

http://www.ironport.com/products/email_security_appliances.html

### EMC SAN Security

EMC's RSA SecurID provides a great element of OWA remote-access authentication. Because it is critical that remote access to your enterprise messaging environments is "anytime and anywhere", EMC's RSA SecureID has a two-factor authentication process based on a known variable (something the end user knows such as a password or personal identification number [PIN]) and something you have (an authenticator), providing a much more reliable level of user authentication than reusable passwords.

This solution is the only one that automatically changes your password every 60 seconds. With SecureID, this solution offers a wide range of user authentication options to help positively identify users before they interact with your mission-critical data and applications through VPNs and wireless LANs (WLANs), email messages, intranets and extranets, Microsoft Windows desktops, web servers, and other network resources, making your application 100-percent available regardless of your location.

## Management

### Improved Flexibility with Exchange 2007 Server Roles

VMware Infrastructure 3 allows each server role to be deployed in its own virtual machine. These virtual machines may all run on the same system initially, or be spread across multiple systems, depending on requirements (see Figure 8). Flexibility is maximized because virtual machines can be distributed in any combination across available server resources, at any time, and can easily be moved around in the virtual infrastructure as required to meet changing service levels.

Exchange 2007 has evolved toward a more modular architecture that includes distinct server roles. These roles include the following:

- Mailbox
- Edge Transport
- Hub Transport
- Client Access
- Unified Messaging

In smaller deployments (generally 500 or fewer users), it may be possible to run multiple server roles such as Hub or CAS on a single physical server to maximize use of the required 64-bit server hardware. The trade-off of this approach is concentrated risk, increasing the chance that some problem on the

server could result in an outage to multiple server roles. Larger environments should run supporting server roles on separate physical machines. This approach increases the amount of hardware required for the solution, however, and typically results in less use of physical servers and increased overall cost.

The design approach using VMware Infrastructure 3 to host an Exchange 2007 installation deploys each Exchange 2007 server role in its own virtual machine to provide maximum flexibility (see Figure 1). As hardware requires maintenance or workloads change, roles can be moved to other servers at any time using VMware VMotion™, which allows migration of live, running virtual machines from one physical server to another, with no loss of service.

### ACE Virtualization

The Cisco ACE supports device partitioning where a single physical device may provide multiple logical devices. This virtualization function allows system administrators to assign a single virtual ACE device to a business unit or application to achieve application performance goals or SLAs. The flexibility of virtualization allows the system administrator to deploy network-based services according to the individual business requirements of the customer and technical requirements of the application. Service isolation is achieved without purchasing another dedicated appliance that consumes more space and power in the data center.

Using ACE virtualization, the CAS and ET SLB, SSL offload, and other optimization policies can be separated from other applications, business units, or user services. This allows for the Exchange-only polices to be created, managed, and monitored independently as though the Exchange services were being handled by a dedicated device when, in fact, a single ACE is handling multiple application environments simultaneously and virtualizing each application.

**Note** For more information about ACE virtualization, refer to the *Application Control Engine Module Virtualization Configuration Guide* at the following URL: http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A2/configuration/virtualization/guide/virtgd.html

# Conclusion

The Cisco, EMC, and VMware virtual solution provides for a scalable Microsoft Exchange Server 2007 environment brought together by the industry leaders in server virtualization, networking and data storage that address common challenges facing IT professionals. By virtualizing the Exchange Server 2007 environment using the VMware Infrastructure 3 (VI3) platform and EMC CLARiiON storage arrays, organizations can simplify disaster recovery and build a more flexible and reliable infrastructure with reduced complexity that makes email messaging highly available. The solution also simplifies management, diminishes a variety of IT expenditures, helps IT professionals take full advantage of existing IT assets, and improves performance of an Exchange deployment as a whole. Cisco, EMC, and VMware have all come together to ensure that Microsoft Exchange 2007 is an efficient, secure, and agile messaging environment.

# References

For further information about virtualizing an Exchange 2007 environment, refer to the VMware webpage (http://www.vmware.com/landing_pages/exchange_solution.html) for Exchange virtualization, which includes the following technical documentation:

- *SAN System Design and Deployment Guide*

  http://www.vmware.com/resources/techresources/772
- *Performance Tuning Best Practices for ESX Server 3*

  http://www.vmware.com/resources/techresources/707
- *CLARiiON Integration with VMware ESX Server*

  http://www.vmware.com/resources/techresources/241
- *VMware Certified Compatibility Guides*

  http://www.vmware.com/resources/guides.html
- *Deploy Exchange on a VMware Platform*

  http://www.vmware.com/landing_pages/exchange_resources.html
- *Virtual Solution for Microsoft® Exchange Server 2007 Using VMware® Infrastructure 3 and EMC CLARiiON® CX3-20 iSCSI Storage*

  http://www.vmware.com/files/pdf/exchange_solution_overview.pdf
- *Integrating Microsoft Exchange Server in a Cisco Multisite Data Center Desig*n

  http://www.cisco.com/en/US/docs/solutions/Verticals/mstdcmsftex.html
- *IronPort Secure Email Appliances*

  http://www.ironport.com/products/email_security_appliances.html
- *Cisco SAN and MDS Design*

  http://www.cisco.com/en/US/products/ps5990/prod_white_papers_list.html
- *Cisco Application Performance and Site Selection Solutions*

  http://www.cisco.com/en/US/products/ps5719/Products_Sub_Category_Home.html

  http://www.cisco.com/en/US/products/hw/contnetw/ps4162/index.html
- *Cisco ASA Security Solutions*

  http://www.cisco.com/en/US/products/ps6120/prod_brochure_list.html

# Appendix A—Microsoft Exchange Server 2007 Overview

The Microsoft Exchange Server 2007 offers many advantages to customers in the form of built-in protection, flexible access methods, and operational efficiency. Customers are looking for ways to cut cost and increase productivity while ensuring high availability. Microsoft Exchange Server 2007 was designed to offer solutions to these most demanding customer messaging requirements and do so for a variety of endpoints, from any location, and to provide access to messaging resources securely.

Some of these customer requirements are met by enabling the following:

- Business continuance through several clustering and disaster recovery options
- Endpoint security for a variety of access methods to include web, Outlook, mobile, and other access types
- Flexible policy creation, management, and reporting for legal compliancy needs
- Easier setup, administration and management through the Microsoft Exchange Management Console, Shell, and Systems Center products
- Scalability and performance improvements due to the increased memory support, more intelligent routing and extensive x64-based architecture

## Microsoft Exchange 2007 Server Roles

Microsoft Exchange Server 2007 uses a variety of roles to provide services. Some roles are the same or slightly different from the roles in Microsoft Exchange Server 2003, whereas others are new. Each role serves a unique purpose within the Microsoft Exchange architecture and is flexible enough to be deployed in various sizes of organizations with varying requirements.

The following sections describes the roles at a high-level and is not meant to be a full tutorial on the architecture, design, and operation of each role. Detailed information on the Microsoft Exchange Server 2007 product, architecture, and design is found at: http://www.microsoft.com/exchange or http://technet.microsoft.com/en-us/library/bb124558.aspx

### Client Access Server

The Client Access Server (CAS) provides access for a variety of client endpoints. The CAS role was formerly known as the Exchange front-end server. The CAS role supports access through the following methods:

- Microsoft Outlook Web Access (OWA)
- Post Office Protocol Version 3 (POP3)
- Internet Message Access Protocol Version 4 (IMAP4)
- Microsoft Exchange ActiveSync client
- Microsoft Outlook Anywhere

The CAS role also supports various other web services such as the offline address book (OAB) distribution and the autodiscover service. The list shows that the CAS role can provide access to messaging services through many different endpoint types such as computers with web browsers, email clients using POP3 or IMAP4, and even mobile devices. Endpoints using another method of access such as Messaging Application Programming Interface (MAPI) most often connect directly to the mailbox server (MBX) role.

In the simplest terms, the CAS role provides a front-end service for the MBX role for non-MAPI-enabled connections. The CAS communicates directly with the MBX. The CAS role is optional if there are no requirements to use non-MAPI clients.

## Hub Transport Server

The Hub Transport (HT) role, formerly known as the Bridgehead server, is the central role for intelligent message routing delivery and policy control. Unlike the CAS and Edge Transport (ET) roles, the HT role is mandatory.

All mail flow external to the organization and internal within the organization is handled by the HT role. The HT role can use the ET as an SMTP relay for messages going to/from the Internet or it can handle the SMTP relay role on its own. The HT communicates directly with the MBX, other HT roles, and the ET.

As was the case with the CAS role, Microsoft recommends deploying multiple HT roles for performance, scalability, and availability purposes. Microsoft Exchange Server 2007 fully supports for the HT role to have multiple servers active simultaneously.

## Mailbox Server

The mailbox server (MBX) role is the database for all user messaging data. Users are homed to a particular MBX and associated storage group. As mentioned before, MAPI-based clients such as those running Microsoft Outlook connect directly to the MBX. The MBX role is a mandatory component of an Exchange Server 2007 deployment.

The MBX communicates directly with the CAS, HT and, if deployed, the standby node in a clustered mailbox server (CMS).

The *Integrating Microsoft Exchange Server 2007 in a Cisco Multisite Data Center Design* (http://www.cisco.com/en/US/docs/solutions/Verticals/mstdcmsftex.html) describes in detail the deployment of Microsoft Exchange Server 2007 with a variety of MBX cluster solutions. This document focuses on providing business continuance and availability of the MBX role by taking advantage of joint EMC and Cisco solutions that are designed for maximum uptime.

## Edge Transport Server

The Edge Transport (ET) role is used as a dedicated Internet SMTP relay as well as a means to provide simple message hygiene. If the ET is deployed at the network edge, it should be deployed as securely as possible. In an effort to secure the internal Active Directory (AD) information, the ET has a one-way connection with the internal HT roles and uses an EdgeSync subscription as a method to replicate internal AD information with the ET. Alternatively, Cisco IronPort email security appliances (ESA) can be deployed at the network edge, providing a significantly enhanced email security solution relative to the Microsoft ET capability in terms of both efficacy and performance. In that case, the ET is still deployed at the Exchange edge, and the ESA is deployed at the network edge.

Microsoft recommends deploying multiple ET roles for performance, scalability, and availability purposes. Microsoft Exchange Server 2007 fully supports for the ET role to have multiple servers active simultaneously.