Microsoft Exchange 2007 – Enhancing the Solution with Cisco, EMC and VMware

Mike Forbes
CCIE# 15389 R&S, Storage
Technical Marketing Engineer
Enterprise Solutions Engineering (ESE) – Data Center

Session Objectives

At the end of the session, the participants should be able to:

- Understand the basic roles of Exchange 2007 from a Cisco Perspective
- Understand the basic roles of VMware Virtualization
- Understand the basic roles of EMC Storage Replication
Agenda

- Business Drivers
- Cisco Solutions for Exchange 2007 Server Roles
- Cisco-EMC-VMware Exchange 2007 Joint Solutions
  - EMC Technology Overview
  - VMWare Overview
  - Design and Deployment
- Summary

Business Drivers
MS Exchange 2007 Challenges

- Microsoft Exchange is mission critical
  - Users expect to have access to the messaging system at all times
  - Messaging environments growing in size and complexity
- Without a comprehensive deployment plan, companies could face
  - Loss of revenue
  - Missed business opportunities
  - Compliance-related fines
  - Increased exposure to loss of data
- Key business drivers for a complete solution
  - Cost reduction and consolidation
  - Streamlined operations management
  - Compliance & Security

Advantages of EMC RecoverPoint and VMware SRM for Exchange 2007

- RecoverPoint + SRM replicate entire Virtual Machine and associated storage (DB, Log, Shares, etc...)
- Configurable “Lag” time can greatly reduce/eliminate out of sync replicated copies making the VM and storage at the replicated DC ready for production at a moments notice
- No need for complex cluster configurations or the risk of increased RPO/RTO times due to long Mailbox seeding or log file synchronization delays
Business Reasons for Virtualizing Exchange

- Flexibility gained by virtualizing Microsoft Exchange
- Less hardware required to install a virtualized Exchange
- Ability to move VM’s from one server to another based on server load without user outage
- Ability to move VM’s during maintenance windows, hardware/electric/cooling failures without user outage
- SAN attached storage allows leveraging of existing replication on SAN, whether Appliance, SRDF, or other
- Manage Exchange roles with Virtual Center
- Manage disaster recovery with Site Recovery Manager

Exchange 2007 from Cisco’s Perspective
Exchange 2007 Logical Layout

Unified Messaging Role not shown

Mailbox Protection Options – Microsoft Based

Local Continuous Replication (LCR)
- Replication to a second disk set
- Cluster Continuous Replication (CCR)
- Replication within a cluster

Standby Continuous Replication (SCR)
- Replication to a standby server
- Single Copy Cluster (SCC)
- DB Log Quorum
SAN vs. DAS vs. SAN-based Replication

- The essential argument is not really SAN vs. DAS but rather SAN-based replication vs. DAS with CCR

- Why is this happening?
  
  Why not DAS? Why not control their own storage and forget the SAN guys?

  Exchange 2007 now offers many more options to provide HA/DR with MSFT-based solutions vs. a shared storage (with SAN replication) model

- What most concerns Exchange Admins?
  
  - Server Performance (Disk I/O)
  - Message Store Availability and Backups
  - High Availability and Time to Recover

Mailbox Role

- Multiple HA/DR options
- CCR Requires “local” heartbeat for cluster
  
  Layer 2 extension of two VLANs if stretching CCR nodes
  
  CCR + SCR requires no L2 extension
  
  CCR nodes over L3 - Windows Server 2008 ONLY*
- CCR promotes locally attached storage, and independent data stores
- SCC is the only option if keeping shared storage AND a cluster

* Brand new capability
Continuous Cluster Replication

- Two-node Active/Passive failover cluster
  - File Share Witness (MNS Quorum)
  - No shared storage
  - Witness on Hub Transport
  - Automatic recovery
- Continuous data replication
- Full redundancy
- One or two datacenter solution

Single Copy Cluster (SCC)

- Shared Storage
- Relies on MSFT clusters (as does CCR)
- Functionally, the only difference between CCR and SCR is the SAN, specifically shared storage vs. log shipping
Single Active Directory Site
Active/Active

Data Center 1
- Microsoft offers several options for how to build an AD infrastructure with multiple sites
- The option used here is a single AD site between both DC locations in order to show how multiple Exchange roles can be A/A

Data Center 2

Exchange 2007 Roles and Cisco Services
Active/Active

- CAS
  - Active at both DC sites using site load-balancing with GSS/DNS
  - Active within each DC using server load-balancing with ACE
- IronPort Secure Email Appliance
  - Active at both DC sites using site LB with GSS/DNS or DNS Round-Robin
  - Active within each DC using server LB with ACE
- Hub Transport
  - Internal LB mechanism (round-robin) used to LB between:
    - Hub-to-Hub and Hub-to-Edge
- Mailbox role does NOT support active/active in Exchange 2007 – however, the MBX role can LB towards Hub Transport servers via round-robin
Services for CAS

IronPort Email Appliance Traffic Flow

1. DNS round-robin or site selection used for SMTP
2. Perimeter security and server LB services are provided
3. IronPort provides message filtering/security and then relays to HT
What Can Cisco Load-Balance?

- LB works great against Edge and CAS roles
- Mailbox role cannot be load-balanced as each user is “homed” to a specific server or cluster instance
- Hub role has proprietary LB mechanism

<table>
<thead>
<tr>
<th>Component</th>
<th>Load Balancing</th>
<th>Fault Tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailbox Server</td>
<td>N/A</td>
<td>Clustering (CCR)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NIC Teamin</td>
</tr>
<tr>
<td>Hub Transport Server</td>
<td>MBX -&gt; HUB: Built in</td>
<td>Clustering (CCR)</td>
</tr>
<tr>
<td></td>
<td>Edge -&gt; HUB: Send Connector – multiple bridgeheads</td>
<td>NIC Teamin</td>
</tr>
<tr>
<td>Edge Transport Server</td>
<td>Internet -&gt; Edge: MX equal cost &amp; DNS Round Robin</td>
<td>Clustering (CCR)</td>
</tr>
<tr>
<td></td>
<td>hub -&gt; Edge: Edge Subscriptions</td>
<td>NIC Teamin</td>
</tr>
<tr>
<td>Client Access Server</td>
<td>External: Network Load Balancing + ISA 2006 WPPLB</td>
<td>Clustering (CCR)</td>
</tr>
<tr>
<td></td>
<td>Internal: Network Load Balancing</td>
<td>NIC Teamin</td>
</tr>
<tr>
<td>Unified Messaging</td>
<td>UM -&gt; IP Gateway: Multiple IP Gateways per dial plan</td>
<td>Clustering (CCR)</td>
</tr>
<tr>
<td></td>
<td>IP Gateway -&gt; UM: Built In (Round Robin between UM)</td>
<td>NIC Teamin</td>
</tr>
</tbody>
</table>

Exchange 2007 on Cisco - Summary

<table>
<thead>
<tr>
<th>Component</th>
<th>ACE Module / Appliance</th>
<th>ACE GSS</th>
<th>Firewall</th>
<th>WAAS</th>
<th>SAN</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge Transport</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>Replace with IronPort</td>
</tr>
<tr>
<td>Client Access Server (CAS)</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X*</td>
<td>X**</td>
<td></td>
</tr>
<tr>
<td>Mailbox</td>
<td></td>
<td></td>
<td></td>
<td>X***</td>
<td>X****</td>
<td>L2 Extension for clusters</td>
</tr>
<tr>
<td>Hub Transport</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Firewall external connections – internal are all encrypted and dynamic port ranges
** WAAS for un-encrypted OWA/Outlook Anywhere sessions (HTTP, MAPI over RPC) from Branch
*** WAAS for clustered log shipping connections
**** SAN – other than basic MDS connectivity – SANTap and other SAN-based replication solution can be used instead of leveraging MSFT-based log shipping solution for HA/DR
EMC Storage and Replication Overview

EMC RecoverPoint

- Network-Based Data Protection
  - Support heterogeneous storage and servers
  - Integrated with Cisco MDS9000 SANTap
  - Supports VMMware Virtual Machines (VDM)
- Heterogeneous Replication
  - Works with EMC and third-party storage
  - True Any to Any Volume Replication
- CDP Recovery at Local or CRR at Remote Site
  - Tracks all data changes to every protected LUN
  - Utilizes bookmarks for application-aware recovery
  - Enables Read/Write processing of replicated LUNs
- Advanced WAN functionality
  - WAN data reduction and compression
  - FC to TCP/IP conversion
  - TCP Optimization
Hardware Components

MDS Switch:
- MDS 9200 or MDS 9500
- Minimum of 1 SSM per fabric
- Support for dual physical fabrics

RecoverPoint Appliance (RPA):
- Minimum of 1 RPA per site
- Typically 2 dual-port Qlogic HBA (connecting 1 HBA per fabric)

Server (Initiator ports):
- Application Server utilizing RP solution

Storage (Target ports):
- Storage port(s) used with RP solution

SANTap Deployment – Before/After

BEFORE

Exchange Server

PRODUCTION VSAN

Storage Array

AFTER

Exchange Server

RecoverPoint Front-End VSAN

9 Virtual Initiators

CVTs

AVTs

Storage Array

RecoverPoint Back-End VSAN

DVTs

CVTs

AVTs

DVTLUNs

CVTLUNs

DVTLUNs
VMware Overview

ESX Server Architecture

- SDK Agent
- VirtualCenter Agent
- 3rd Party Agents
- Service Console
- VM
- VMM
- VM
- VMM
- VM
- VMM

Resource Management
- Clustered VM File System
- Virtual NICs & Switches
- Storage Stack
- Network Stack
- Device Drivers

VMkernel

Physical Hardware

Device Drivers
Storage

- An ESX Server can connect to SAN arrays via iSCSI, Fiber Channel, or FCoE and connect to NAS devices via NFS
  - Storage options in addition to Fibre Channel SAN and local disk
  - Either/Both can be used to hold VM files, templates, ISO files
  - ESX Server can boot from iSCSI SAN using HW initiator

Four Key Properties of Virtual Machines

- Partitioning
  - Run multiple operating systems on one physical machine
  - Divide system resources between virtual machines
  - ESX is the special operating system that abstracts the HW from the GUEST OS/Application
  - Industry Term “The Hypervisor”
Four Key Properties of Virtual Machines

- **Partitioning**
  - Run multiple operating systems on one physical machine
  - Divide system resources between virtual machines

- **Isolation**
  - Fault and security isolation at the hardware level
  - Advanced resource controls preserve performance

- **Encapsulation**
  - Entire state of the virtual machine can be saved to files
  - Move and copy virtual machines as easily as moving and copying files
Four Key Properties of Virtual Machines

- **Partitioning**
  - Run multiple operating systems on one physical machine
  - Divide system resources between virtual machines

- **Isolation**
  - Fault and security isolation at the hardware level
  - Advanced resource controls preserve performance

- **Encapsulation**
  - Entire state of the virtual machine can be saved to files
  - Move and copy virtual machines as easily as moving and copying files

- **Hardware-Independence**
  - Provision or migrate any virtual machine to any similar or different physical server

### VMotion

- VMotion is a migration technique for virtual machines
- VMotion improves hardware utilization & uptime
- Requires identical hardware and software
- Requires shared storage
- Scripted or scheduled
- **CANNOT** have internal switch connectivity or a cluster relationship with another VM
Resource Optimization with VMware DRS

DRS = Dynamic Resource Scheduler

- What is it?
  - Dynamic balancing of computing resources across resource pools
  - Intelligent resource allocation based on pre-defined rules

- Customer Impact
  - Align IT resources with business priorities
  - Operational simplicity; dramatically increase system administrator productivity
  - Add hardware dynamically to avoid over-provisioning to peak load
  - Automate hardware maintenance

Advantages of Virtual Disaster Recovery

- Virtual machines are portable
- Virtual hardware can be automatically configured
- Test and failover can be automated (minimizes human error)
- The need for idle hardware is reduced
- Costs are lowered, and the quality of service is raised
Introducing Site Recovery Manager (SRM)

Site Recovery Manager leverages VMware Infrastructure to transform disaster recovery

- What it is:
  - Site Recovery Manager is a new VMware product for disaster recovery

- What it does:
  - Simplifies and automates disaster recovery processes
    - Setup
    - Testing
    - Failover
    - Failback

- Site Recovery Manager works with VMware Infrastructure to enable faster, more reliable, affordable disaster recovery

SRM Server Side Components *

* Note: Conceptual drawing only. SRM Server may run on another system than VCMS
Key Concepts — VMware Site Recovery Manager

Recovery Plan
Complete set of steps needed to recover (or test the recovery of) the protected virtual machines in one or more protection groups.

Protection Group
Collection of protected virtual machines that will be failed over to the recovery site together. Protection groups are mapped to datastore groups.

Datastore Groups
Replicated datastores containing the complete set of virtual machines you wish to protect via SRM.

Cisco-EMC-VMware Solutions
Design and Deployment
Site Selection

- Basic DNS-based Round-Robin
- GSS can be used to offer higher level of scalability, availability and site selection intelligence
- Examples discussed are:
  - DNS-based Round-Robin for SMTP mail flow for IronPort Appliances
  - GSS with intelligent site selection for CAS access
DNS-based Round-Robin for SMTP

- Very popular deployment method for many customers
- Allows for equal cost MX record entries or ‘weighted’ based on MX record preference values

| e.se.com MX preference = 10, mail exchanger = ironyport1.e.se.com |
| e.se.com MX preference = 10, mail exchanger = ironyport2.e.se.com |
| ironyport1.e.se.com internet address = 10.5.25.11 |
| ironyport2.e.se.com internet address = 10.6.25.11 |

- Note, for an example deployment using Cisco GSS with Cisco Network Registrar to provide intelligent site selection for MX records check out: http://www.cisco.com/en/US/docs/solutions/Verticals/mstdcmsftex.html

GSS Request Flow for CAS

1. OWA user issues a DNS query for owa.e.se.com
2. Router forwards to the GSS.
3. GSS receives the DNS request
4. GSS responds with owa.e.se.com entry which resolves in DNS to the ACE VIP
5. The router forwards the packet
6. OWA user receives record GSS
CAS Roles with ACE

- CAS roles are “independent”
  Basically a web server
- ACE leveraging
  SSL Offload (Terminal/bridging)
  SSL/TCP Reuse
  HTTP/s Probes
  SYN Cookie

Configuring the CAS Server for SSL-Offload

- Note
  - The CAS role is aware of the SSL-offload functionality of the ACE. To configure support for SSL-offloading on a CAS role, refer to:
Redirect Server

http://---/iowa

https://---/iowa/

https://---/iowa

- For use in SSL only environments

TCP Reuse Optimization

ACE-TCP1 Pool1

ACE-TCP2 Pool2

- Reduction of Active TCP Connections to OWA Server

Applied to multi-match policy

policy-map multi-match multi-match OWA-POLICY-MAP
class OWA-VIP-443
app1-parameter http advanced-options TCP-REUSE

parameter-map type tcp TCP-REUSE
server-conn reuse

serverfarm redirect REDIRECT-SERVERFARM
in-service

class-map multi-match OWA-VIP
2 match virtual-address 11.5.103.11 tcp eq www

policy-map type loadbalance first-match
REDIRECT-PM

class class-default

serverfarm REDIRECT-SERVERFARM

policy-map multi-match OWA-POLICY-MAP

class OWA-VIP
loadbalance vip inservice
loadbalance policy REDIRECT-PM
loadbalance vip_icmp-reply active

server redirect REDIRECT-TO-HTTPS
webhost-redirection https://owa,ese.com/owa 302
in-service

serverfarm redirect REDIRECT-SERVERFARM
server redirect REDIRECT-TO-HTTPS
in-service
Application Optimizers

HTTP Benefits
- This eliminates the latency caused by establishing multiple connections between clients and servers
- Tuned to offset connection "bursts"
- Transparency is maintained
- Compliments and preserves http application pipelining

Mapi Benefits
- Reduced send and receive time and improves response time of interactive control operations – very important for Outlook 2000 users
- Cleans up the outbox faster – important for cached mode users
- Faster downloads of OAB, while significantly reducing BW consumption as this is a redundant transfer across user population
- Optimizes native Outlook 2007 operations (Note: requires encryption to be disabled on server)
- Transparent, automatic optimization. Simple enable/disable control. no requirement for modification of MAPI ports as Riverbed does. Integrated with EPM adapter for classification
- No reverse engineering (MSFT licensing) - Full protocol compliance with the different protocol versions –
- No security hole of keeping sessions open even after users have logged out
Replication Acceleration Mode Overview

– WAEs in Replication Accelerator mode have
– TFO tuned to **address TCP issues for high speed** WAN links
– DRE tuned for **low latency processing** requirements for DC to DC Replication
– Default policy in Replication Accelerator mode is tuned for Replication Applications

Combined Power of TCP Optimization and Advanced Compression

- LAN-Like Throughput
- Bandwidth Savings
- Fewer Roundtrips
- No WAAS
- WAAS enabled with Replication Accelerator Mode
Cisco WAAS Solution Topology

- Application Acceleration mode from Branch to Data Center
  - Branch WAES inline for simplicity
  - Data Center WAES inline for flexibility
  - SW version 4.1.1
- Replication Acceleration mode from Primary DC to Backup DC
  - Both WAES deployed inline
  - SW version 4.0.19
- Central Manager ver 4.4.1 manages overall environment

WAAS Performance for Recover Point

Traffic Summary (Dec/22/0Z 02:52:48 - Dec/23/0Z 01:52:06) (GMT-08:00)

<table>
<thead>
<tr>
<th>Device</th>
<th>Original Traffic</th>
<th>Optimized Traffic</th>
<th>Reduction inBandwidth Capacity</th>
<th>Reduction/Single-Day Point-to-Point</th>
<th>Effective Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCAS1-WAEX-2000</td>
<td>1,349 MB</td>
<td>67,614 KB</td>
<td>90.0%</td>
<td>7.04X</td>
<td>1.4 X</td>
</tr>
<tr>
<td>DCAS1-WM1-WM2</td>
<td>3,375 GB</td>
<td>1,002 GB</td>
<td>72.0%</td>
<td>72.0%</td>
<td>3.6 X</td>
</tr>
<tr>
<td>DCAS1-WM2-WM3</td>
<td>56.6 GB</td>
<td>0 KB</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>DCAS1-WM3-WM4</td>
<td>3,087 GB</td>
<td>1,002 GB</td>
<td>72.0%</td>
<td>72.0%</td>
<td>3.6 X</td>
</tr>
</tbody>
</table>

Last Updated: 23-05-00 22-12-2000
Iron Port

IronPort Gateway Security Products

APPLICATION-SPECIFIC SECURITY GATEWAYS

BLOCK Incoming Threats

ENCRYPTION Appliance

EMAIL Security Appliance

WEB Security Appliance

CENTRALIZE Administration

PROTECT Corporate Assets

Data Loss Prevention

CLIENTS

Web Security | Email Security | Security Management | Encryption
The IronPort SenderBase® Network
Global Reach Yields Benchmark Accuracy

- 30B+ queries daily
- 150+ Email and Web parameters
- 25% of the World’s Traffic
- Cisco Network Devices

View into both email & Web traffic dramatically improves detection
80% of spam contains URLs
Email is a key distribution vector for Web-based malware
Malware is a key distribution vector for Spam zombie infections

Combines Email & Web Traffic Analysis

IronPort Consolidates the Network Perimeter
For Security, Reliability and Lower Maintenance
Fiber Channel over Ethernet

**FC over Ethernet (FCoE) – Quick Overview**

- Mapping of FC Frames over Ethernet
- Enables FC to Run on a Lossless Ethernet

Ethernet

Fibre Channel Traffic

CNA = Converged Network Adapter
FCoE Extends FC SAN Connectivity Pervasively and Cost Effectively

- Increases SAN-attach rate of servers
- Preserves FC investments
- No change to operational and management models

FCoE Physical Layout
Site Recovery Manager

RecoverPoint CRR Physical Layout
Site Recovery Manager Disaster Recovery Setup

Create recovery plans
- For virtual machines, applications, business units

Integrate with replication
- Identify which virtual machines are protected by replication configuration

Map recovery resources
- Server resources, network resources, management objects

Specify recovery process
- Convert manual runbook to pre-programmed response
- Customizable with scripting and callouts

---

RecoverPoint and SRM Integration

Production

Disaster Recovery

Automated VM Failover

Non-disruptive DR Testing

Common Interface to VMware SRM

Heterogeneous storage

Replica Journal

Remote Replicas
RecoverPoint GUI Before SRM Failover

RecoverPoint GUI after SRM failover
# Site Recover Manager after failover

**Win-2003**

**VMWare Site Recovery Manager**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Result</th>
<th>Completion Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Shutdown Low Priority Virtual Machines</td>
<td>Success</td>
<td>08:01:21</td>
</tr>
<tr>
<td>1.2</td>
<td>Shutdown Normal Priority Protected Virtual Machines</td>
<td>Success</td>
<td>08:01:21</td>
</tr>
<tr>
<td>1.2.1</td>
<td>Shutdown Normal Protected Site VM &quot;Svr0187-Work&quot;</td>
<td>Success</td>
<td>08:01:21</td>
</tr>
<tr>
<td>1.2.1.1</td>
<td>Shutdown Steady State Remote VM &quot;Svr0187-MRSC&quot;</td>
<td>Success</td>
<td>08:01:03</td>
</tr>
<tr>
<td>1.2.1.2</td>
<td>Wait for Steady State Shutdown</td>
<td>Success</td>
<td>08:01:20</td>
</tr>
<tr>
<td>1.2.1.3</td>
<td>Power off VM &quot;Svr0187-MRSC&quot;</td>
<td>Success</td>
<td>08:01:00</td>
</tr>
<tr>
<td>1.2.2</td>
<td>Shutdown High Priority Protected Virtual Machines</td>
<td>Success</td>
<td>08:01:00</td>
</tr>
<tr>
<td>2.1</td>
<td>Prepare Storage</td>
<td>Success</td>
<td>08:04:05</td>
</tr>
<tr>
<td>2.1.1</td>
<td>Attach/Ports for Production Group &quot;Win2003&quot;</td>
<td>Success</td>
<td>08:04:05</td>
</tr>
<tr>
<td>2.1.2</td>
<td>Prepare High Priority Virtual Machines</td>
<td>Success</td>
<td>08:01:00</td>
</tr>
<tr>
<td>3.1</td>
<td>Prepare Normal Priority Virtual Machines</td>
<td>Success</td>
<td>08:01:20</td>
</tr>
<tr>
<td>4.1</td>
<td>Prepare Normal Priority Virtual Machines</td>
<td>Success</td>
<td>08:01:45</td>
</tr>
<tr>
<td>4.1.1</td>
<td>Remote VM &quot;Svr0187-MRSC&quot;</td>
<td>Success</td>
<td>08:01:45</td>
</tr>
<tr>
<td>4.1.1.1</td>
<td>Remote VM &quot;Svr0187-MRSC&quot;</td>
<td>Success</td>
<td>08:01:20</td>
</tr>
<tr>
<td>4.1.1.2</td>
<td>Wait for Steady State Shutdown</td>
<td>Success</td>
<td>08:01:20</td>
</tr>
<tr>
<td>4.1.1.3</td>
<td>Power on VM &quot;Svr0187-MRSC&quot;</td>
<td>Success</td>
<td>08:01:00</td>
</tr>
<tr>
<td>4.1.1.4</td>
<td>Wait to OS Preheat</td>
<td>Success</td>
<td>08:03:45</td>
</tr>
<tr>
<td>4.1.1.5</td>
<td>Post Power On</td>
<td>Success</td>
<td>08:03:00</td>
</tr>
<tr>
<td>5.1</td>
<td>Prepare Low Priority Virtual Machines</td>
<td>Success</td>
<td>08:01:00</td>
</tr>
<tr>
<td>6.1</td>
<td>Prepare No Priority Virtual Machines</td>
<td>Success</td>
<td>08:01:00</td>
</tr>
<tr>
<td>6.1.1</td>
<td>Power off VMs &quot;Svr0187-Work&quot;</td>
<td>Success</td>
<td>08:01:00</td>
</tr>
</tbody>
</table>

**Summary**

- Task summary complete. Please verify the outcome of the test. When done, click Continue to clean up the test and return to a ready state.
Understand the Pain Points

- Migration issues abound from 2003 to 2007 – Routing groups vs. AD-based routing with Hub Transport, Public Folders, many more

- CAS and Mailbox design are the most challenging for Admins
  - DR/HA of Mailbox – Clusters, SRDF or SRM/RecoverPoint
  - HA/SLB for CAS and security for CAS (placement and Firewall vs. Proxy)

- 2007 offers more application security options

- Msg. routing is completely dependent on AD
  - AD clean-up may be required before deployment

- Archiving/snapshots are required for journaling purposes in order to meet HR/Legal/Industry compliance

Key Takeaways

The Key Takeaways of this presentation are:

- There are three (of five) Exchange 2007 roles that we need to fully understand – CAS, ET and MBX

- Cisco insertion points in the Exchange 2007 environment include site selection, load balancing, & security

- Cisco, EMC and VMware are working together on a validated architecture for MS Exchange 2007
Resources

- Microsoft Exchange Server 2007—Cisco, EMC, and VMware Multisite Data Center Design

- EMC Solutions for Microsoft Exchange:

- Deploying Exchange on a VMware platform:

- VMware Site Recovery Manager with EMC Recover Point Implementation Guide

- Microsoft Exchange Server 2007:
  http://www.microsoft.com/exchange/default.mspx