Symantec Reference Architecture for Business Critical Virtualization

David Troutt
Senior Principal Program Manager

11/6/2012
Virtualization of Business Critical Applications

- Easy, department level systems already virtualized
- Next are the “Business Critical Applications”
- They are the last to be done because they are the “crown jewels” of the company
- They must be protected, they must meet SLA’s

Symantec is the Solution.

Symantec Reference Architecture for Business Critical Virtualization
Agenda

1. approach
2. overview
3. technology architecture domains
4. validation
5. conclusion
approach
Business Challenges

- Organizations are striving to leverage the benefits of virtualization:
  - Drive down cost
  - Improve business agility through consolidation
  - Improve resource utilization
  - Benefit from increased automation and efficiency

- Many business critical applications are considered too large, complex, or high risk, concerns center around:
  - Meeting enterprise level SLAs (Service Level Agreements) for “up time”
  - Maximizing continuity and recovery
  - Meeting enterprise level security and governance requirements
  - Achieving I/O performance requirements
  - Minimizing storage and related resource costs
  - Minimizing learning the curve by removing one-off point-solutions
Goal & Objectives

Goal:

To remove the barriers to virtualization, and provide proven capabilities to help businesses migrate their critical Microsoft® applications safely to virtual environments, while managing complexity and risk.

Objectives:

- Optimize I/O performance
- Provide business critical levels of availability
- Protect critical servers from security threats
- Reduce infrastructure costs
- Improve operations efficiency
Key Requirements Driving this Architecture

- Defines optimum configurations that ensure VMware, Microsoft®, and Symantec technologies work together for maximum benefit

- Optimized for large enterprises deploying business critical applications with high transaction rates

- Benefits of virtualization remain intact and improved upon

- Minimizing cost of implementation
  - Organizations can expand the scope of a specific implementation of the Symantec Reference Architecture to include multi-instance applications.

- Based on the most current generally available versions of software
Introducing the Symantec Reference Architecture

- Tested framework
- Meets the business critical application challenges
- A complete solution
- Combines key products from Symantec and VMware
- Enterprise Architecture based on TOGAF Standards
- Off the shelf products, *no custom software required*, low TCO, easy expansion
- Accelerates the design process, reduces costs & risk, speeds implementation
- Selected resources trained in architecting and implementing this solution
- Hardware platform flexibility (HP, Dell, EMC, etc.)

SymRA for Business Critical Virtualization is the **blueprint** to make it work.
overview
Common Architecture Overview

- Users
- Visibility, Audit & Reporting
- Operations Management
- Security & Compliance

Primary Site:
- Hypervisor
- Business Critical Application
  - Application Data
- Virtual Machine
- Enterprise Dynamic Storage (SAN)
- Clustering

Secondary Site:
- Hypervisor
- Business Critical Application
  - Application Data
- Virtual Machine
- Hypervisor
- Business Critical Application
  - Application Data
- Virtual Machine
- Enterprise Dynamic Storage (SAN)
- SAN/NAS
- Replication
- Off-Site Deduplication

Enterprise Backup

Symantec Reference Architecture
Symantec Reference Architectures for Business Critical Virtualization

The Reference Architectures within this series include supporting environments for:

- Security
- Archiving
- Data Protection
- Microsoft applications on VMware
- SharePoint 2010
- Exchange Server 2010
- SQL Server 2008
- High Availability
- Storage Management
technology architecture domains
# Requirements to Architecture Segment Mapping

<table>
<thead>
<tr>
<th>Concerns</th>
<th>High Availability Segment</th>
<th>Storage Segment</th>
<th>Data Protection Segment</th>
<th>Security Segment</th>
<th>Archiving Segment</th>
</tr>
</thead>
<tbody>
<tr>
<td>I/O Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Availability</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Recovery</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Application Visibility</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Infrastructure costs</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Management costs</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

Symantec Reference Architecture for Business Critical Virtualization
# Product to Technology Architecture Domain Map

<table>
<thead>
<tr>
<th>Technology / Product</th>
<th>Virtualization</th>
<th>High Availability</th>
<th>Storage Management</th>
<th>Data Protection</th>
<th>Security</th>
<th>Archiving</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vCenter</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vShield</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>HA</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRM</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRA Replication</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Array-Based Snapshots</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ApplicationHA</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage Foundation</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Veritas Operations Manager</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Veritas Operations Manager Advanced</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical System Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>NetBackup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Vault</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

1. Antivirus recommended for Exchange environment.
High Availability (& Disaster Recovery)

Objectives Achieved

- Protect systems at **ALL levels** (application through ESXi host and data center)
- Enable quick recovery
- Ensure live migration of complex systems
- Provide consolidated monitoring and report of system status and SLAs

Approach Taken

- Implement **ApplicationHA** on all application virtual machines
- Integrate with VMware’s HA and DR capabilities for local and site level failover
- Apply multi-tier application management and protection
- Provide data center level monitoring and reporting of application SLA’s

Products Used

- Symantec™ ApplicationHA
- VMware HA
- Veritas™ Operations Manager
- VMware SRM
- SRA (from HP) – Array based Site-to-Site replication
Achieving Service Level Agreements

<table>
<thead>
<tr>
<th>Failure Level</th>
<th>Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center</td>
<td>Symantec ApplicationHA detects and then attempts to restart application services. If services can’t be restarted, Application HA notifies VMwareHA.</td>
</tr>
<tr>
<td>Physical Server</td>
<td>VMware HA attempts to restart virtual server.</td>
</tr>
<tr>
<td>Virtual Server</td>
<td>ESXi Host is detected as being down by VMware HA which then moves applications to an alternate ESXi Host.</td>
</tr>
<tr>
<td>Application</td>
<td>VMware SRM detects the data center down, starts applications at DR site.</td>
</tr>
</tbody>
</table>
Managing Availability Across Application Tiers

Symantec Reference Architecture for Business Critical Virtualization

Symantec ApplicationHA

USE CASE
- Service Stop
- Disaster Recovery
- Security
- Service Start
- Status Summary
- High Availability
Disaster Recovery Logical Architecture

Primary Site
- SRM Server
- VM1 (EXCH) → VMware HA → ESXi
- VM2 (SQL) → VMware HA → ESXi
- VM3 (SP) → VMware HA → ESXi

Secondary Site
- SRM Server
- VM1 (EXCH) → VMware HA → ESXi
- VM2 (SQL) → VMware HA → ESXi
- VM3 (SP) → VMware HA → ESXi

SRM Protection Group
- Replicated Storage
  - VM Boot Vols
  - Data Vols
  - Log Vols

Array-based Replication
- Non-Replicated Storage
  - ESX Boot Vols
- Replicated Storage
  - VM Boot Vols
  - Data Vols
  - Log Vols

Symantec Reference Architecture for Business Critical Virtualization

High Availability

Symantec VISION 2012
Objectives achieved

- Provide for scalable and optimized I/O performance
- Reduced infrastructure and management costs
- Provide instant recovery via snapshots
- Ensure Disaster Recovery with data integrity

Approach taken

- Implement thin provisioning/reclamation to provide capacity on demand
- Deploy DMP (SFW) to eliminate single points of failure in the I/O path
- Utilize VOM/VOM Advanced to provide centralized storage management and reporting
- Use snapshots to facilitate instant point in time recovery

Products Used

- Veritas Storage Foundation™ for Windows® from Symantec
- Veritas™ Operations Manager
- Veritas™ Operations Manager Advanced
Storage Management Logical Architecture

Physical Server

VMware ESXi

VM1
EXCH
OS
SFW
VM2
SQL
OS
SFW
VM3
SP
OS
SFW

VMDK Local Storage

Non-Replicated Storage

ESX
Boot Vols
Snap-Shots

RDM SAN Shared Storage

SRM Protection Group
Replicated Storage

VM Boot Vols
Data Vols
Log Vols

Non-Replicated Storage

Snap-Shots
Benefits of Choosing Raw Device Mapped Storage

Benefits

• Breaks the 2 TB limit
• I/O Isolation
  o Minimize impact on other applications
  o More predictable performance
  o Separation of application files types (databases, log files, etc.)
• Supports advanced storage mgmt. capabilities (e.g. Thin Provisioning)
• Lower CPU overhead, 5% to 8%
Managing and Monitoring Storage
VOM and VOM Advanced

IMPROVE SERVICE LEVELS
- Monitoring, alerting, & built-in health checks
- Storage capacity planning & reporting
- Patch reporting & alerting
- File Systems & Volume Management Information

REDUCE COST AND COMPLEXITY
- Automated detection & mapping of virtual guests and related storage
- Thin-Pool Monitoring & reclamation reporting

Symantec Reference Architecture for Business Critical Virtualization
Data Protection

Objectives Achieved

- Enable fast recovery of data in the event of data loss or logical corruption
- Improve performance and scalability by offloading backup processing from application virtual machines
- Reduce infrastructure and storage costs by eliminating backups of duplicated data
- Allow for recovery of individual objects (files, mailboxes, etc.)

Approach Taken

- Use VMware and array-based snapshots for off host backups of OS, applications, and data
- Deploy NetBackup agents on all application virtual machines for granular recovery
- Utilize NetBackup deduplication to minimize storage and network bandwidth requirements
- Deploy Granular Restore Technology (NetBackup GRT) for individual object level restores

Products Used

- Symantec NetBackup™ Enterprise Server
- Symantec NetBackup™ 5000 and MSDP (Deduplication)
- VMware vStorage APIs for Data Protection (VADP)
- VMware Snapshots
- Array-based Snapshots (from HP)
NetBackup Logical Architecture

- OpsCenter Reporting and Management Server
- NetBackup Media Server
- Third-Party Storage Appliance
- SAN Storage
- Tape Library
- NetBackup Dedupe Media Server (MSDP)
- Ethernet
- NetBackup Master Server
- NetBackup Dedupe Appliance
- SAN Storage
- NetBackup Client Hosts (Virtual Machines)
- VMware ESXi Host
- SAN Storage
- Snapshots

Symantec Reference Architecture for Business Critical Virtualization
Offhost Backup Using vStorage API and Snapshots
Protecting I/O Performance via Off-host Backups

NetBackup Media Server or Appliance

ESXi Host

NBU Agent

Guest

“Alternate Host”

RDM

ESXi Host

NBU Agent

Guest

Application

RDM

Backup Storage

Snapshot

SAN Storage

Shared Storage

Symantec Reference Architecture for Business Critical Virtualization

Data Protection

SYMANTEC VISION 2012
Security

Objectives Achieved

- Protect a virtualized environment against intrusion and unauthorized changes
- Protect against network security threats
- Lower security management costs
- Keep security policies relevant to new threats

Approach Taken

- Multiple layers of protection
- Utilize Symantec™ Critical System Protection (SCSP) to monitor file systems and processes for unauthorized changes
- Lockdown system configuration settings, file settings, and use of removable media using SCSP
- Implement VMware vShield App to enforce firewall security policies
- Centralize security administration and management via SCSP
- Implement LiveUpdate™ to keep security policies current

Products Used

- Symantec™ Critical System Protection, Symantec LiveUpdate™
- VMware vShield App
## Security Capability Map by Application

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Microsoft Applications *</th>
<th>Symantec CSP**</th>
<th>VMware vShield</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control to Applications and Data</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>In Place Data Encryption</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tamper Protection (no unauthorized modification)</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SSL Certificate Protection (no unauthorized access)</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>System Hardening (Prevent 0 day attacks and unauthorized software installation)***</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Built in compliance reports</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Firewall</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Hypervisor Level Firewall (Application &amp; System Aware)</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

* Referring specifically to Microsoft SQL Server, Exchange Server and SharePoint

** Symantec Critical System Protection (SCSP) protects physical & virtual systems. Security groups, policy management, logging, and auditing can cross both physical and virtual environments.

*** SCSP follows best practices for hardening an ESX server from VMware and ensuring your ESX systems settings are set to be secure and remain secure.
Hardening Virtual and Physical Systems Efficiently

- Shield critical physical and virtual systems
- Apply Isolation Trust Zones
- Unified Policy and Control

Key Functions:
- System hardening
- User access control
- Change monitoring/prevention
- Guest isolation
- Network access control
- IPS / IDS
- Log retention
- Removable media control
- User and application behavior control
- File integrity monitoring
Lock Down All of the Virtual Environment with CSP

Threats
- Rogue Clients
- Client Hijacking
- Disgruntled Admin
- Mis-configurations
- SSL certificate
- Malware
- Unauthorized Access

Symantec Reference Architecture for Business Critical Virtualization
Archiving

Objectives Achieved

• Offload aging data and duplicated data from infrastructure, optimizing I/O performance
• Reduce cost of Tier 1 storage and related infrastructure
• Provides capability to quickly locate messages and documents for compliance requirements

Approach Taken

• Deploy Enterprise Vault to archive Microsoft® Exchange Server and Microsoft® SharePoint® information
• Implement eDiscovery using Discovery Accelerator to allow for quick searches of archived content
• Define expiration policies to remove old messages and content from archive stores

Products Used

• Symantec Enterprise Vault™
• Symantec Enterprise Vault™ Discovery Accelerator
Archiving Physical Architecture

1. Migrate information to archive
2. Reduce information stores
3. Apply deduplication
4. Discover against archived data
5. Expire data over time
validation
Validation Approach

- **Testing Methodology**
  - Focus on Interoperability
  - Placed applications under load during functional testing

- **Use Cases Tested**
  - High Availability – Recovery at each tier (*Application to Data Center*)
  - Disaster Recovery
  - Data protection
  - Thin provisioning / reclamation
  - Security
  - Reporting / tracking of events
conclusion
Conclusion

Symantec’s Reference Architecture solves the problems facing the virtualization of common Microsoft® business applications.

- Improved Availability & Performance
- Improved Application & Data Protection
- Reduced Infrastructure & Management Costs
Next Steps

• Review the associated white paper:
  – White Paper: *Accelerating Virtualization of Tier 1 Applications*


• Schedule a meeting with a Symantec technical sales specialist to discuss suitability of this solution.
Questions
Thank you!

David Troutt
david_troutt@symantec.com
949-836-1174