Exploring Options for Virtualized Disaster Recovery

Ranganath GK
Solution Architect
6th Nov 2008
Defining Disaster Recovery

What is a “disaster”?
- Extended outage that requires an organization to recover IT services using alternate or rebuilt infrastructure

What is not a disaster?
- Failure of an individual server
- A short service interruption

Network failure
Server failure
Disk failure
Power failure
Storage failure
Flood
Earthquake
Hurricane
Fire

VIRTUALIZATION FORUM 2008
Business continuity and disaster recovery planning includes people, facilities, and technology.

Assessing requirements is a necessary first step before planning technology.

Questions:
- Risk tolerance?
- Recovery objectives?
- Application criticality?
- Application dependencies?
- Compliance requirements?
Disaster Recovery Planning

Business Impact Analysis
- Outage assessment
- Risk assessment
- Cost of downtime
- Application criticality
- Compliance requirements

Disaster Recovery Requirements
- Application assessment
- Recovery site strategy
- Recovery tiers
- Recovery time objective (RTO)
- Recovery point objective (RPO)

Technology
- Configuration management
- Backup and recovery
- Replication
- Process automation
Recovery versus $$$

- **Tier 7**: Highly automated, business wide solution
  - Zero or near Zero data lost

- **Tier 6**: Disk Mirroring, Tape Mirroring

- **Tier 5**: Hot Site w/ two phase commit
  - Minutes to Hours with data recreation

- **Tier 4**: Batch & Online data base shadowing
  - Up to 24 Hours with significant data recreation

- **Tier 3**: Remote Electronic Tape Vault
  - 24 Hours to several days with significant lost data

- **Tier 2**: PTAM + Hot Site

- **Tier 1**: PTAM

Recovery Time:

- < 5 min
- 1-4 Hr.
- 4-12 Hr.
- 12+ Hr.
- 24 Hrs.
- + Days

VIRTUALIZATION FORUM 2008
Challenges of DR with Physical Infrastructure

**Require identical hardware for recovery**
- Because of hardware dependencies
- Double costs, increases complexity

**Idle hardware**
- Need standby hardware for faster RTO
- Repurposing servers at time of disaster is labor-intensive and time-consuming

**Slow, complex recovery process**
- Different solutions for different availability tiers
- Separate procedures for system and data disks
- Separate procedures for desktop PC’s
- Multi-step recovery processes
Challenges of Traditional DR: Infrastructure

Prod

Application

OS

x86

OS files

local storage

Storage

DR

Application

OS

x86

OS files

local storage

Storage

- Bound to HW
- 5-10% utilized

Expensive and Complex
Challenges of Traditional DR: Recovery Process

- OS & applications have dependencies on hardware configuration
- Tier 2 & 3 applications left unprotected, adding to Tier 1 RTO risk
- Slow and Unreliable Process

"Boot & Pray"

Slow and Unreliable Process
Our Disaster Recovery Plan Goes Something Like This...

HELP! HELP!

DILBERT
By Scott Adams
Data Protection with VMware Consolidated Backup
### VMware Infrastructure: The Safest Place To Run Applications

<table>
<thead>
<tr>
<th>Component</th>
<th>Prevent Planned Outages</th>
<th>Minimize Downtime from Unplanned Outages</th>
<th>Prevent Unplanned Outages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server</strong></td>
<td>DRS Maintenance Mode, VMotion</td>
<td>HA</td>
<td>Fault Tolerance</td>
</tr>
<tr>
<td><strong>Storage</strong></td>
<td>Storage VMotion</td>
<td>VCB + Backup ISV products, Data Recovery</td>
<td></td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td>N/A</td>
<td>VCB + Backup ISV products, Data Recovery</td>
<td></td>
</tr>
<tr>
<td><strong>Site</strong></td>
<td>Site Recovery Manager</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All available across physical hardware, operating systems, and applications.
Data and System Protection – Physical vs. Virtual

Data and system protection with Physical infrastructure
- Separate processes for protecting data and system disks
- Require identical hardware for guaranteed restore
- Complex processes to ensure protection

Data and system protection with VMware infrastructure
- Same process for data and system disks
- Entire system stored as data
- Hardware-independent virtual machines are easy to restore to any hardware
Enterprise Data Protection Overview

VMware Infrastructure provides:
- Hardware-independent image encapsulation
- Simplified backup of VM images
- System level restore without the complexity of traditional bare metal recovery solutions

Additional Benefits from VMware Consolidated Backup:
- Eliminates agents in VM’s as points of mgmt
- Eliminates backup windows
- Higher consolidation ratio for 24x7 IT shops
- Off-host and LAN free backup with industry-leading backup and restore products
Backup Options for Virtual Machines

**In-VM**
- Agent in each VM
  - Same architecture as physical system backup
  - File-level incremental backup possible
  - Any storage

**In-Console**
- Agent in Service Console
  - Simplified backup of full-disk images
  - Any storage
  - Not available for ESXi a.k.a. ESX Server 3i

**VCB**
- Consolidated Backup - Agent on Proxy Server
  - Move backup out of VM
  - Provide LAN-free backup
  - Eliminate backup windows
  - Requires FC SAN
  - Pre-integrated with 3rd party backup products
VMware Consolidated Backup

Centralized file and image level backup

1. Take VM Snapshot
2. Mount SAN Snapshot
3. Backup files or disk images with leading backup tools

Move backup out of the virtual machine
Run midday backups – LAN Free
Integrated with 3rd party backup
VCB: How it Works - SAN

SAN

VM1
VM2
VM3
vmkernel
Service Console
vmkernel
ESX

Backup Proxy

VLUN

VMDK

VMFS

VMDK

REDO

BLOCK LIST
VCB: How it Works - NBD

ESX

Backup Proxy

NAS/Local Storage
VCB Recommendations

Maximum of 14 VM’s per physical Datastore (LUN)
> 14 VM’s can be a tremendous amount of I/O
> Keep in mind the I/O profile of VCB

No more than 4 simultaneous backups per LUN
> This is a good number
> Be sure to spread out the I/O load of backups across Datastores

Limit the number of sim backups per Backup Proxy to 8
> An important part of this number is I/O capacity of staging area
> Snapshot creation, vmdk mapping and transfer to disk/tape happen simultaneously

Keep in mind these figures are just guidelines!
> There are environments where these limits could be much too high
> There are environments where these limits could be much too low
VCB 1.5 – What’s New

1. Better Security
   - SSPI support on interacting with VC host; run backup engine in the context of a user instead of SYSTEM account
   - Store password in the registry instead of config.js

2. More Reliable Recovery - VSS support (comes from ESX 3.5 U2)
   - VSS requestor in VMware tools runs before snapshots
   - Better Windows application integration (e.g. SQL, Exchange)
   - Replaces synch driver for NTFS quiescing on W2K3 (W2K8 coming later)

3. Better Performance
   - VM proxy performance using new hot-add transport mode on par with physical proxy LAN backups
VSS Integration

- **File System Level Quiescing**
  - Vista, W2K8, W2K3 (32 and 64 bit versions)

- **Application Level Quiescing (Exchange, SQL)**
  - W2K3 (32 and 64 bit versions)

- VMware VSS requestor and VMware VSS provider in VMware tools used to create quiesced snapshot

- **NOTE:** Location and method of pre-freeze and post-thaw script has changed
Leveraging VMware Converter For Quick, Simple Recovery
## Migrating from Physical to Virtual (P2V)

Simpler than Physical Hardware replacement process …

<table>
<thead>
<tr>
<th>Examples</th>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Free VMware Converter (for Windows)</td>
<td>Retain all OS &amp; Application settings.</td>
<td>Clean up required (e.g. H/W agents</td>
</tr>
<tr>
<td>• Commercial 3rd-party tool (e.g. Platespin, Leostream)</td>
<td>Clean build, install only component</td>
<td>Knowledge to rebuild a server may be</td>
</tr>
<tr>
<td></td>
<td>required.</td>
<td>lost, e.g. staff attrition.</td>
</tr>
<tr>
<td><strong>Guest OS/Apps reinstallation + Data migration</strong></td>
<td>Fully documented procedures</td>
<td>Application specific process.</td>
</tr>
<tr>
<td>• Install fresh Windows OS and SQL Server, restore and attach database.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Leverage standard application migration process</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Domino Replication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Add Domain Controllers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VIRTUALIZATION FORUM 2008
Protecting Physical Machines with Virtual Machines

- Convert physical machines to VMs using VMware Converter
  - Can use to protect against local physical server/storage failures
- Consider when physical servers in production are in “lock-down” mode
  - No need to reinstall and rebuild
- Costs significantly less to build your DR

VIRTUALIZATION FORUM 2008
Addressing Site Failures for Physical Machines: Physical to Virtual Disaster Recovery

- Convert images to virtual machines
- Or use hardware-independent images

Primary Site

- Back up images
- Tape array

Disaster Recovery Site

- Import virtual machines to ESX Servers with VMware Converter

- Convert images to virtual machines
- Or use hardware-independent images
Simplifying the Disaster Recovery Process

Eliminate recovery steps
- No operating system re-install or bare-metal recovery
- No time spent reconfiguring hardware

Standardize recovery process
- Consistent process independent of operating system and hardware
Replication Options
Replication Options with Virtual Infrastructure

- **Server-based replication**
- **Storage network-based replication**
- **Array-based replication**

PRIMARY ↔ DR SITE
Server Based Replication

Considerations

- Some provide agents for quiescing key applications
- Higher performance impact on host
- Generally do not provide consistency across systems
- Storage independent
Server Based Replication Options

Running in guest OS
- Filter driver sends writes to remote system
- Requires running “catcher”
- May have agents for application quiescing

Running below virtual machines in Service Console
- Agent monitors virtual disk files and sends changes to remote host
- Replicated image is at best filesystem consistent
Server Based Replication Options

Running below virtual machines in Service Console
- Vizioncore esxReplicator

Running in Windows guest OS
- CA XOsoft WANSync
- Doubletake
- EMC Replistor
- NetApp TDPS (Topio)
- Symantec Veritas Volume Replicator
Storage Network Based Replication

Storage network-based replication products:

- EMC RecoverPoint (Kashya)
- F5 Acopia (for NAS)
- NetApp TPDS (Topio)
- FalconStor CDP Virtual Appliance

Considerations

- Common architectures use software running on storage network switches and replication appliances
- Low performance impact on host
- Often array-independent
Array Based Replication

Considerations

- Minimal performance impact on host
- Can leverage consistency groups for multi-tier applications
- May be able to use agents for quiescing important applications
- Tied to specific storage platform
Summary: Why Virtual is Better than Physical

Faster recovery
- Eliminate need for many manual recovery steps
- Eliminate complexity of different hardware

More reliable recovery
- Eliminate failures due to hardware dependencies
- Eliminate human error by simplifying processes

Affordable disaster recovery
- Consolidating servers and eliminating idle equipment slashes infrastructure costs
- Simplicity and uniformity reduce management costs

Virtual machines are an inherently safer container for your applications than physical machines!
VMware BCDR References

Download VMbook on BCDR at:

Download Virtual Machine Backup Guide at:

Visit the VMware Consolidated Backup site to learn more at:

Backup Software Compatibility Guide for ESX Server 3.5 and ESX Server 3i

Download the Site Recovery Manager Compatibility Matrix, which is available at: