Automated Disaster Recovery

Simon Caruso
Senior Systems Engineer, VMware
What is a Disaster?

Complete loss of a data center for an extended period of time

- Declaration of a disaster usually requires consensus from multiple parts of the organization (at the C*O level)

What is not a disaster?

- Failure of an individual host
- A temporary service interruption
The Current State of Physical Disaster Recovery

<table>
<thead>
<tr>
<th>Tier</th>
<th>RPO</th>
<th>RTO</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Immediate</td>
<td>Immediate</td>
<td>$$$$</td>
</tr>
<tr>
<td>II</td>
<td>4 hrs.</td>
<td>8 hrs.</td>
<td>$$</td>
</tr>
<tr>
<td>III</td>
<td>24 hours</td>
<td>24 - 48 hours</td>
<td>$</td>
</tr>
</tbody>
</table>

DR services tiered according to business needs

Physical DR is challenging

- Maintain identical hardware at both locations
- Apply upgrades and patches in parallel
- Little automation
- Error-prone and difficult to test
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 VMware Site Recovery Manager

Site Recovery Manager leverages VMware Infrastructure to deliver advanced disaster recovery management and automation

- Simplifies and automates disaster recovery workflows:
  - Setup, testing, failover
- Turns manual recovery runbooks into automated recovery plans
- Provides central management of recovery plans from VirtualCenter

- Works with VMware Infrastructure to make disaster recovery rapid, reliable, manageable, affordable
Site Recovery Manager at a Glance

Protected Site

Site A

Recovery Site

Supported bi-directional site protection

Protected VMs powered on become unavailable online in Protected Site

Site B

Recovery Site

Protected Site

VirtualCenter

Site Recovery Manager

VirtualCenter

Site Recovery Manager

Protected VMs powered on

Array Replication

Datastore Groups

Virtualization Seminar Series

vmware
Server Side Components

Site 1
- VCMS 1 DB
- SRM 1 DB
- VC Server 1
- SRM Server 1
- Storage Replication Adapter
- Array 1
  - Block Replication SW

Site 2
- VCMS 2 DB
- SRM 2 DB
- VC Server 2
- SRM Server 2
- Storage Replication Adapter
- Array 2
  - Block Replication SW

* Note: Conceptual drawing only. Site Recovery Manager Server may run on another system than VCMS.
Key Concepts And Their Relationships

Datastore Group 1
LUN 1
VMFS 1

Protection Group 1
VMware applications

Datastore Group 2
LUN 2
VMFS 2

Protection Group 2
VMware applications

Datastore Group 3
LUN 3
VMFS 3
LUN 4
VMFS 4
LUN 5
VMFS 5

Protection Group 3
VMware applications

Recovery Plan 1 (Whole Site)
Protection Groups:
- Protection Group 1
- Protection Group 2
- Protection Group 3

Recovery Plan 2 (Subset)
Protection Groups:
- Protection Group 1

Protected Site

Recovery Site
Array Integration with Site Recovery Manager

Vendor-specific scripts support:

- Array discovery
- Replicated LUN discovery
- Test initiation (simulated failover in an isolated environment)
- Failover initiation (actual failover of services to the recovery site)

In cooperation with VMware and with the full support of VMware the storage vendors create the storage replication adapters for their respective storage arrays.
VMware Site Recovery Manager Licensing

**Protected Site**
- VirtualCenter
- Site Recovery Manager
- SRM Protected VMs

**Site 1**
- VirtualCenter
- Site Recovery Manager

**Site 2**
- VirtualCenter
- Site Recovery Manager
- SRM licensed per CPU socket on the ESX server that hosts the protected virtual machines in the Protected Site

**Recovery Site**
- VMs not protected by Site Recovery Manager
Site Recovery Manager 1.0 Prerequisites

- ESX 3.0.2, ESX 3.5 or ESXi
- VirtualCenter (VC) server version 2.5 installed at the **protected site** and at the **recovery site**
- Site Recovery Manager server installed at the **protected** and at the **recovery site**
- Site Recovery Manager plug-in installed on the VMware Infrastructure Clients that will access the protected and recovery site
- Network configuration that allows TCP connectivity between VC servers and SRM servers
- An Oracle or SQL Server database that uses ODBC for connectivity in the **protected site** and in the **recovery site**
- A Site Recovery Manager license file installed on the VC license server at the **protected site** and at the **recovery site**
- **Pre-configured array-based replication between the protected site and the recovery site**
Site Recovery Manager Installation Workflow

At the **protected site** the following activities are completed:

- Installation of the SRM server
- Installation of the SRM Plugin into the VI Client
- Installation of the Storage Replication Adapter (SRA)

At the **recovery site** the following activities are completed:

- Installation of the SRM server
- Installation of the SRM Plugin into the VI Client *
- Installation of the Storage Replication Adapter (SRA)

**It is important to complete the workflows in the order detailed in this presentation**

* Note: Optional step, only required if a different instance of the VI Client is used to access the recovery site
Site Recovery Manager User Interface

VMware Infrastructure Client

Site Recovery

Local and Paired Site

Protection Setup

Recovery Setup

Virtualization Seminar Series
Setup Workflow – Protection Site

At the **protection site** the following setup activities are completed:

- The user pairs the SRM servers at the protected and recovery sites
- Security certificates are established between the SRM servers and the VC servers
  - Certificates that are not properly signed will result in the Yellow Warnings Signs.
  - Reciprocity will still be established allowing you to continue to the next step in the workflow.

Certificates that are properly signed will result in the Green Check Mark.

Reciprocity will still be established allowing you to continue to the next step in the workflow.
Setup Workflow – Protection Site (continued)

Array Managers Configuration

➢ Select the correct Manager Type from the Manager type drop down box

Storage Partner Participation

➢ VMware provides the SRA specification
➢ Storage Partners create the SRA
➢ Storage Partners test the SRA
➢ VMware review the SRA test results
➢ SRA support with SRM granted if all test are passed
SRM identifies available arrays in the Protection and Recovery Side and the replicated datastores and determines the datastore groups.
Setup Workflow – Protection Site (continued)

Using the Inventory Preferences Mapper, the user maps resources in the protected site to their counterparts in the recovery site.

![Inventory Preferences Mapper](image)

Configure mappings between resources on the protection and recovery sites. Resources used by a VM on the protection site will be replaced by mapped resources on the recovery site when the VM is recovered.
A protection group is a group of VMs that will be failed over together to the recovery site.

Working through the Protection Group wizard you will need to select a temporary location for placeholder VM configuration files for the protected VMs at the recovery site.
Setup Workflow – Protection Site (continued)

> Working through the Protection Group wizard a user selects which VMs need to be protected and assigns them to a protection group.

> The creation of a protection group results in VC inventory updates in the recovery site.
Setup Workflow – Recovery Site

At the recovery site the following setup activity is completed:

- The user creates a recovery plan which is associated to a single or multiple protection groups.
Site Recovery Manager Recovery Plan

1. Shutdown Protected Virtual Machines at Protected Site "vm22"
   - 1. Shutdown Low Priority Protected Virtual Machines
   - 2. Shutdown Normal Priority Protected Virtual Machines
   - 3. Shutdown Primary Site VM "app_vm7"
     - 1. Shutdown Guest OS for Remote VM "app_vm7"
     - 2. Wait for Guest OS Shutdown
     - 3. Power off VM "app_vm7"
   - 4. Shutdown Primary Site VM "app_vm8"
   - 5. Shutdown Primary Site VM "app_vm9"
   - 6. Shutdown Primary Site VM "app_vm10"
   - 7. Shutdown Primary Site VM "app_vm11"
   - 8. Shutdown High Priority Protected Virtual Machines
     - 1. Shutdown Primary Site VM "app_vm12"

2. Prepare Storage
   - 1. Attach Disks for Protection Group "Protection Group 2"
   - 2. Suspend Non-critical Virtual Machines
   - 3. Recover High Priority Virtual Machines
     - 1. Recover VM "app_vm12"
       - 1. Change Network Settings
       - 2. Pre-Power On
       - 3. Power On
       - 4. Wait for OS Heartbeat
       - 5. Post Power On
   - 4. Recover Normal Priority Virtual Machines
     - 1. Recover VM "app_vm7"
     - 2. Recover VM "app_vm8"
     - 3. Recover VM "app_vm9"
     - 4. Recover VM "app_vm10"
     - 5. Recover VM "app_vm11"

During an actual failover using SRM the Protected Site VMs are shutdown starting with Low Priority VMs, followed by Normal Priority VMs (app_vm7 to app_vm11) and ending off with the High Priority VMs (app_vm12).

It is worth noting that during a simulated failover test using SRM the Protected VMs (app_vm7 to app_vm12) are not shutdown in the Protected Site.

The datastore group (shared-san-2) which is associated with Protection Group 2 is prepared at the recovery site for the failover of the protected VMs (app_vm7 to app_vm12)

If required designated non-critical VMs at the recovery site can be shutdown to provide more resources for the VMs that will need to be powered on to complete the execution of the Recovery Plan at the recovery site.

VMs are restarted at the recovery site starting with the High Priority VMs first (app_vm12) followed by the Normal Priority VMs (app_vm7 to app_vm11)
Site Recovery Manager Recovery Plan Benefits:

- Turn manual **BC/DR run books** into an automated process
- Specify the steps of the recovery process in VirtualCenter
- Provide a way to test your BC/DR plan in an isolated environment at the recovery site without impacting the protected VMs in the protected site
Testing a Recovery Plan

SRM enables you to ‘Test’ a recovery plan by simulating a failover with zero downtime to the protected VMs in the protected site.

Storage configuration during a SRM Test failover from Site A to Site B for datastore ‘shared-san-2’

- **Source LUN (shared-san-2)**: Read Write Enabled
- **Target LUN (shared-san-2)**: Write Disabled (read only)
- **Clone LUN (shared-san-2)**: Read Write Enabled

Note: Datastore ‘shared-san-1’ will be in the same configuration state as ‘shared-san-2’.

Protected VMs: (app_vm7 to app_vm12)

Protected VMs powered on in Site B during the SRM Test failover.
Testing a Recovery Plan (continued)

<table>
<thead>
<tr>
<th>Recovery Step</th>
<th>Status</th>
<th>Task Started</th>
<th>Task Completed</th>
<th>Mode</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>Plan</th>
<th>Mode</th>
<th>Result</th>
<th>Execution Time</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/4/2008 12:52:22 PM</td>
<td>Recovery Plan 2</td>
<td>Test</td>
<td>Success</td>
<td>00:31:01</td>
<td>View</td>
</tr>
</tbody>
</table>
Executing an Actual Failover

WARNING - Executing an actual failover will permanently alter virtual machines and infrastructure of both the protected and recovery sites

Site A - Protected Site
Source LUN (shared-san-2)
Protected VMs (app_vm7 to app_vm12)
All powered off by SRM
At start of SRM Recovery

Site B - Recovery Site
Target LUN (shared-san-2)
Protected VMs (app_vm7 to app_vm12)
All powered on by SRM
during the SRM Recovery

Note: A Clone LUN is not used during an actual failover in SRM.

Data Replication is suspended
Executing an Actual Failover (continued)

WARNING - Executing an actual failover will permanently alter virtual machines and infrastructure of both the protected and recovery sites.

WARNING - Failback to the protected site is a not an automated process in SRM 1.0.
SRM will automatically perform a re-signature on the **Datastores** in the **Recovery Site** that were replicated from the SRM Protected Site

- **LVM.EnableResignature=1**
- With a typical re-signature - **Datastore** names will change to `snapxxxxx_datastorename`, for example
  - `snap-00000002-shared-san-1`
  - `snap-00000002-shared-san-2`
- With a SRM initiated re-signature - **Datastore** will maintain the original datastore name
  - `shared-san-1`
  - `shared-san-2`

**WARNING** - The re-signature of the target datastore has implications during a failback (resync) of data back to the SRM Protected Site
Failback Options with Site Recovery Manager 1.0

SRM 1.0 does not provide a push-button automated failback process

Failback Options

- **Without SRM (no Recovery Plan, no Testing capabilities, no audit trail):**
  - Unregister the protected virtual machines in the Protected Site VC
  - Work with your storage team, reverse data replication
  - VM re-inventory in Protected Site VC, restart and re-ip (manual or scripted)

- **With SRM (Recovery Plan, Test before Recovery, built-in audit trail):**
  - Delete the protection groups in the Protected Site VC
  - Unregister the protected virtual machines in the Protected Site VC
  - Work with your storage team, reverse data replication
  - Leverage SRM, complete SRM workflows in the reverse direction from Recovery Site back to the Protected Site
  - Repeat the above steps from the Protected Site back to the Recovery Site to complete the re-protection of the virtual machines in the Protected Site
Default Roles and Privileges in Site Recovery Manager

- Protection Administrator
- Recovery Administrator
- Protection Groups Administrator
- Protection SRM Administrator
- Protection Virtual Machine Administrator
- Recovery Datacenter Administrator
- Recovery Host Administrator
- Recovery Inventory Administrator
- Recovery Plans Administrator
- Recovery SRM Administrator
- Recovery Virtual Machine Administrator

- Site Recovery Manager
  - Inventory Preferences
    - Create Mapping
    - Remove Mapping
  - Protection Group
    - Create
    - Remove
    - Modify
    - Run
  - Recovery Plan
    - Create
    - Remove
    - Modify
  - Remote Site
    - Create
    - Remove
    - Modify
  - Array Manager
    - Configure
  - Recovery Virtual Machine
    - Modify
Alarms and Site Status Monitoring

SRM will support the following alarm notification actions:

- Send e-mail to specified address
- Send SNMP trap to VC trap receivers
- Execute specified command on VC host

We recommend you complete setup of alarm notifications for:

- Remote Site Down
- Remote Site Ping Failed
- Replication Group Removed
- Recovery Plan Destroyed
- License Server Unreachable
Site Recovery Manager Server Monitoring

SRM will raise VC events for the following conditions:

- Disk Space Low
- CPU use exceeded limit
- Memory low
- Remote Site not responding
- Remote Site heartbeat failed
- Recovery Plan Test started, ended, succeeded, failed, or cancelled
- Virtual Machine Recovery started, ended, succeeded, failed, or reports a warning
Site Recovery Manager Core Benefits

Expand disaster recovery protection
> Now any workload in a VM can be protected with minimal incremental effort and cost

Reduce time to recovery
> As soon as disaster is declared, a single button kicks off recovery sequence for hundreds of VMs

Increase reliability of recovery
> Replication of system state ensures a VM has all it needs to startup
> Hardware independence eliminates failures due to different hardware
> Easier testing based off of actual failover sequence allows more frequent and more realistic tests
Summary

Site Recovery Manager Leverages VMware Infrastructure to Make Disaster Recovery

➤ **Rapid**
- Automate disaster recovery process
- Eliminate complexities of traditional recovery

➤ **Reliable**
- Ensure proper execution of recovery plan
- Enable easier, more frequent tests

➤ **Manageable**
- Centrally manage recovery plans
- Make plans dynamic to match environment

➤ **Affordable**
- Utilize recovery site infrastructure
- Reduce management costs