



VMware Site Recovery Manager: Technical Overview

Michael White
Senior System Engineer
VMware, Inc.

Agenda

- ▶ **Introduction and Key Concepts**
- ▶ **Site Recovery Manager 1.0 Prerequisites and SAN Integration**
- ▶ **Site Recovery Manager Workflows**
- ▶ **Site Recovery Manager Roles and Privileges**
- ▶ **Alarms and Site Status Monitoring**
- ▶ **Summary**

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 Traditional Disaster Recovery

Tier	RPO	RTO	Cost
I	Immediate	Immediate	\$\$\$
II	24+ hrs.	48+ hrs.	\$\$
III	7+ days	5+ days	\$

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

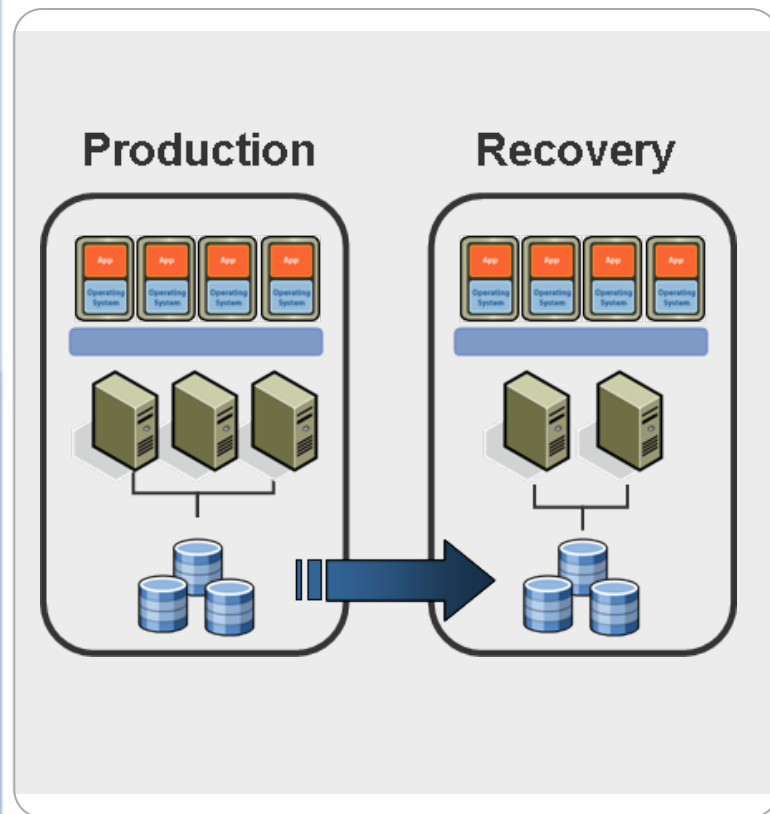
Advantages of Virtual Disaster Recovery

- > 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



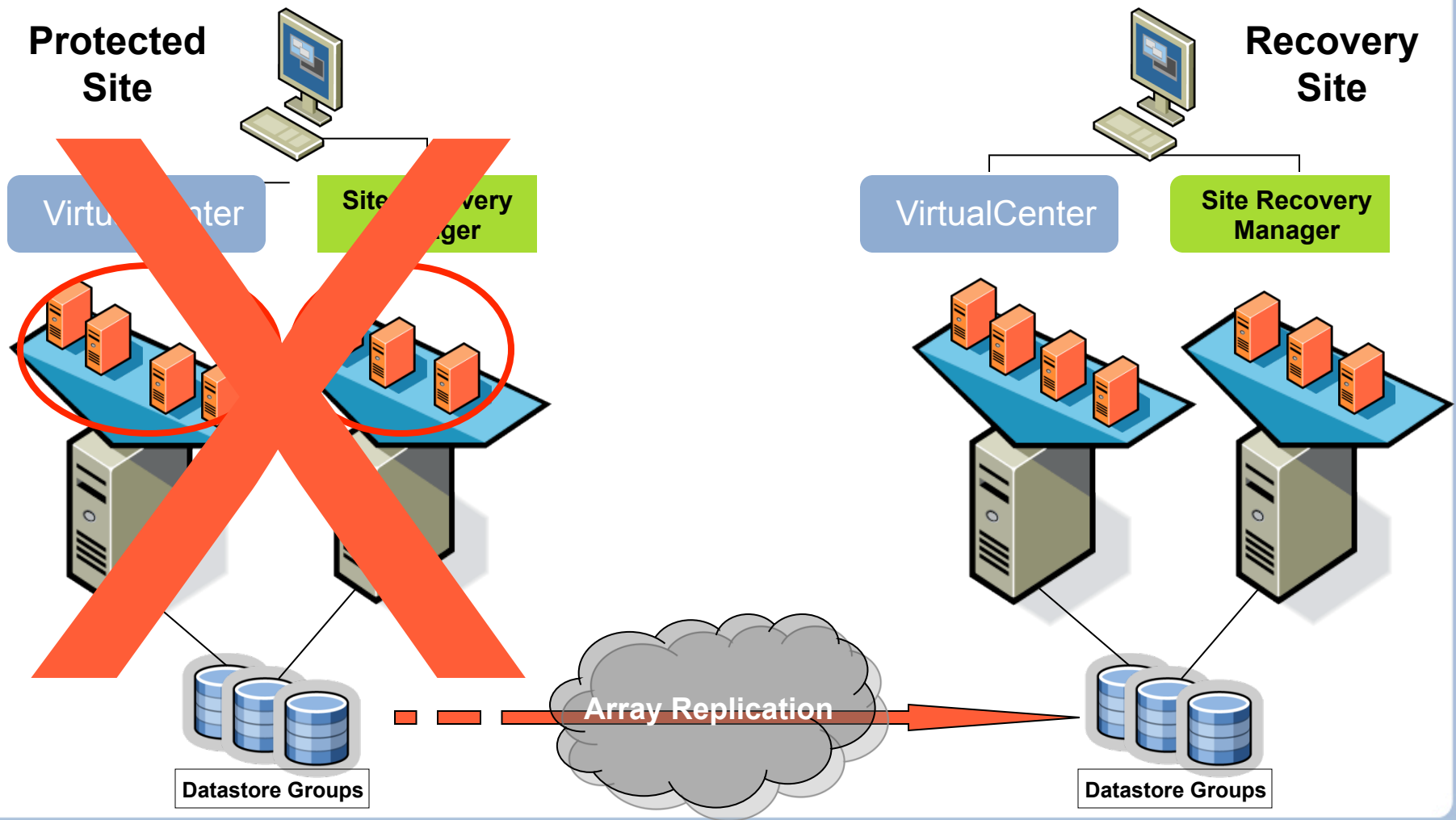
Introducing VMware Site Recovery Manager

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

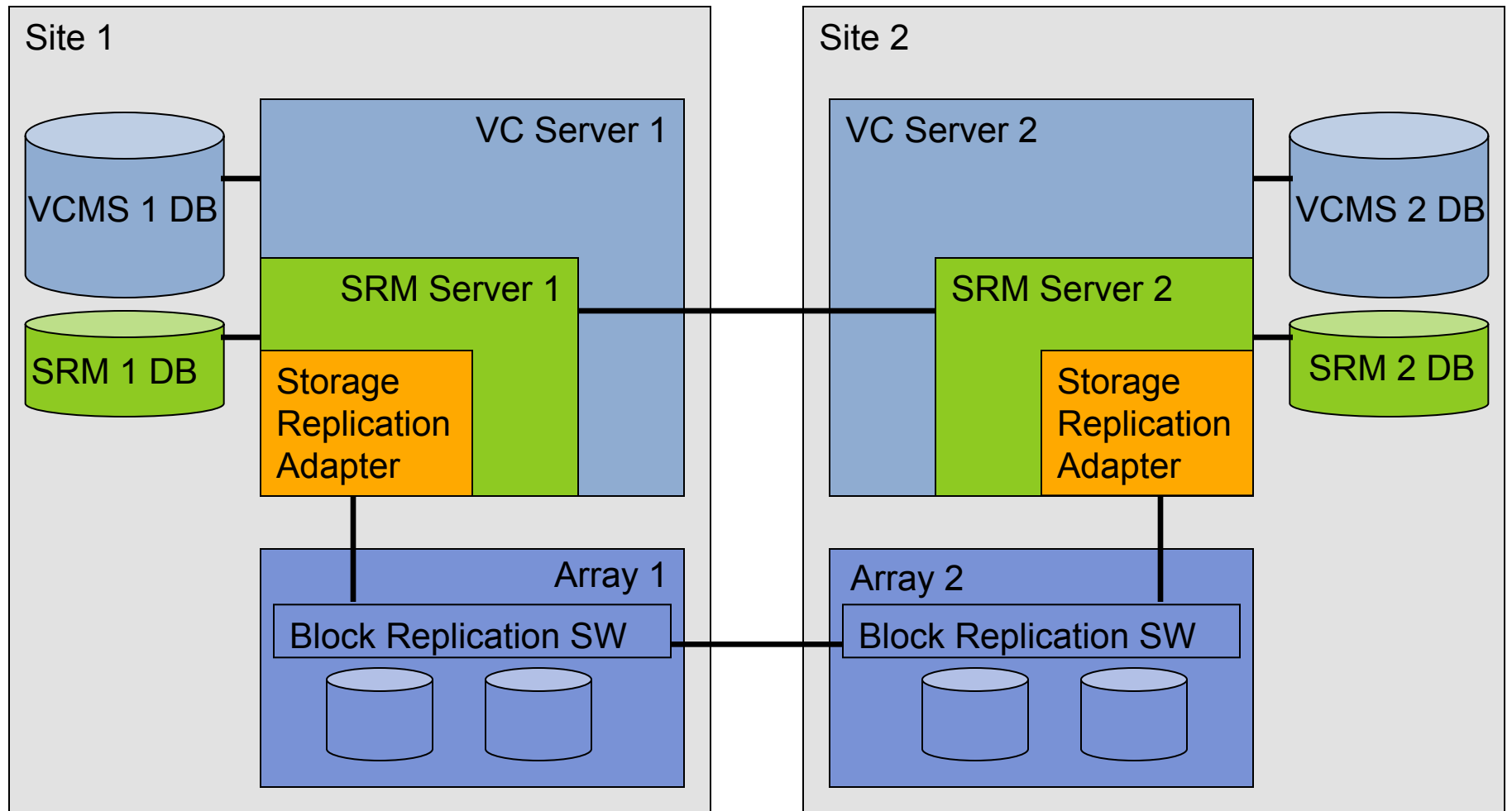


- > **Simplifies and automates disaster recovery workflows:**
 - Setup, testing, failover
 - > **Turns manual recovery runbooks into automated recovery plans**
 - > **Provides central management of recovery plans from VirtualCenter**
-
- > **Works with VMware Infrastructure to make disaster recovery **rapid, reliable, manageable, affordable****

Site Recovery Manager at a Glance



Server Side Components *

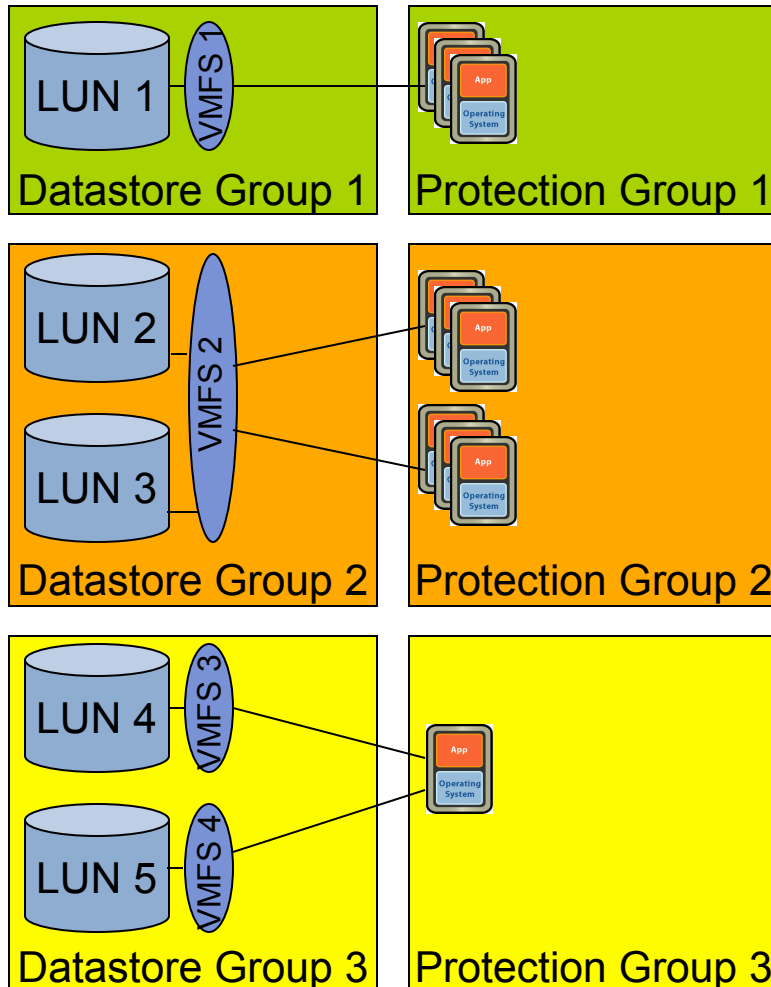


* Note: Conceptual drawing only. SRM Server may run on another system than VCMS

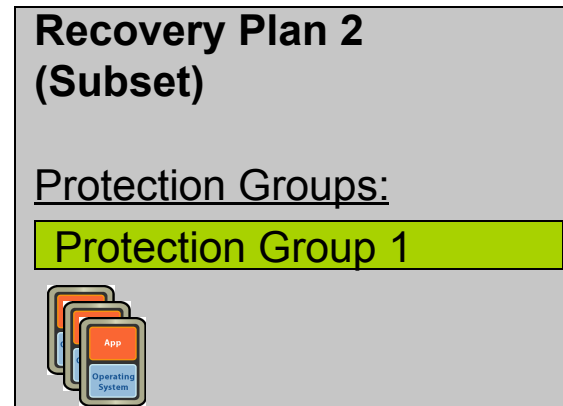
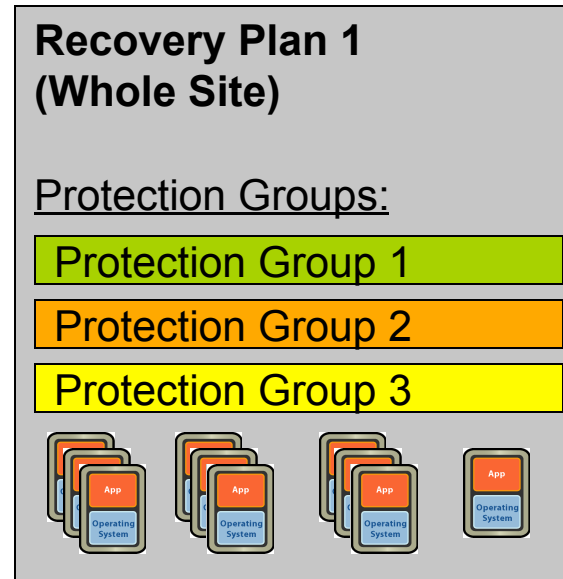
Site Recovery Manager Concept Relationship “Cheat Sheet”

Site	Concept	Relationship
Protected	LUN	Indivisible unit of storage that can be replicated
Protected	Datastore	Contains one or more LUNs (i.e. VMFS)
Protected	Datastore Groups	Auto-generated collection of one or more datastores. Indivisible unit or storage failover.
Protected	Protection Group	Collection of all VMs stored in a datastore group
Recovery	Recovery Plan	Contains one or more protection groups

Key Concepts And Their Relationships

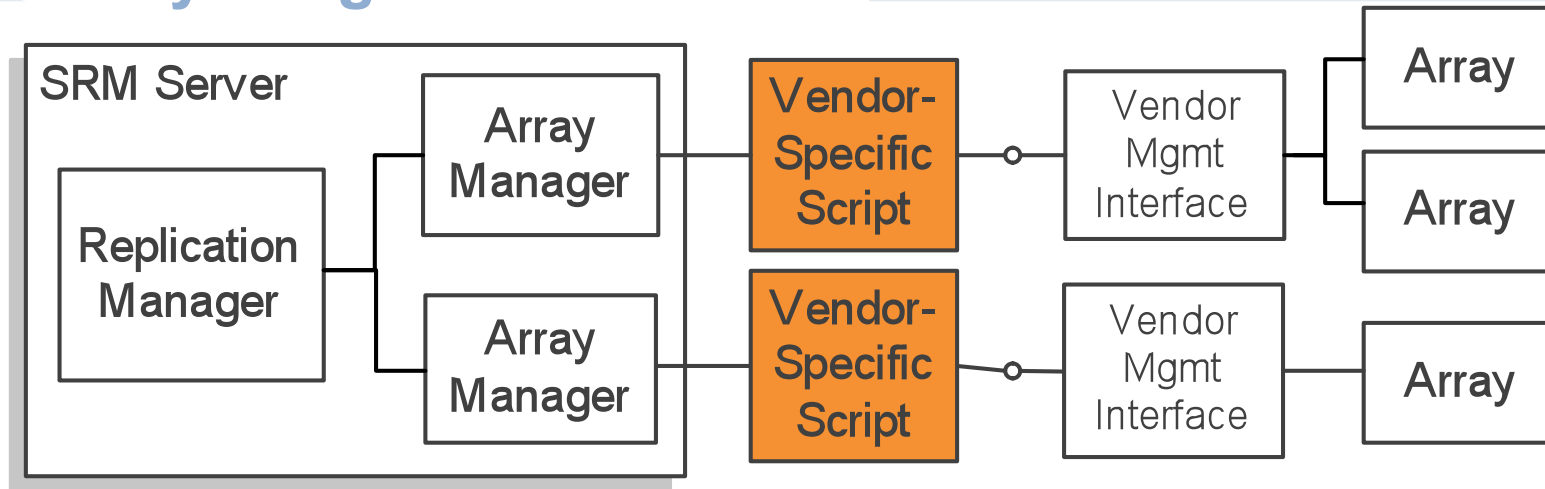


Protected Site



Recovery Site

Array Integration with SRM



Vendor-specific scripts support:

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

Array vendors will be responsible for creating the scripts for their arrays to enable the integration with Site Recovery Manager

Safety Tip: DNS Validation – The Rule of ‘Four’

Validate DNS is working as expected and by performing the following DNS lookups for the VC,SRM and ESX servers

- > Short name
- > Long name
- > Reverse
- > Forward

```
C:\>nslookup dr-vc-vim22
Server:
Address:

C:\>nslookup dr-vc-vim22.eng.vmware.com
Name:
Address:
Server:
Address:

C:\>nslookup 10.17.195.184
Name:
Address:
Server: vmc-ns1.eng.vmware.com
Address: 10.17.193.1

C:\>nslookup dr-vc-vim22.eng.vmware.com
Name: dr-vc-vim22.eng.vmware.com
Address: 10.17.195.184
Server:
Address:

C:\>nslookup 10.17.195.234
Name:
Address:
Server: vmc-ns1.eng.vmware.com
Address: 10.17.193.1

C:\>nslookup dr-vim22.eng.vmware.com
Name: dr-vim22.eng.vmware.com
Address: 10.17.195.234
Server:
Address:

C:\>nslookup 10.17.195.106
Name:
Address:
Server: vmc-ns1.eng.vmware.com
Address: 10.17.193.1

C:\>nslookup vim22.eng.vmware.com
Name: vim22.eng.vmware.com
Address: 10.17.195.106
Server:
Address:

C:\>nslookup eng.vmware.com
Name: eng.vmware.com
Address: 10.17.0.20
Server: vmc-ns1.eng.vmware.com
Address: 10.17.193.1
```

Site Recovery Manager 1.0 Prerequisites

- > ESX Server 3.0.2 Patch 1, ESX Server 3.5 Update 1
- > VirtualCenter (VC) server version 2.5 Update 1 installed at the **protected site** and at the **recovery site**
- > SRM server installed at the **protected** and at the **recovery site**
- > SRM plug-in installed on the VI 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 SRM license 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**

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:

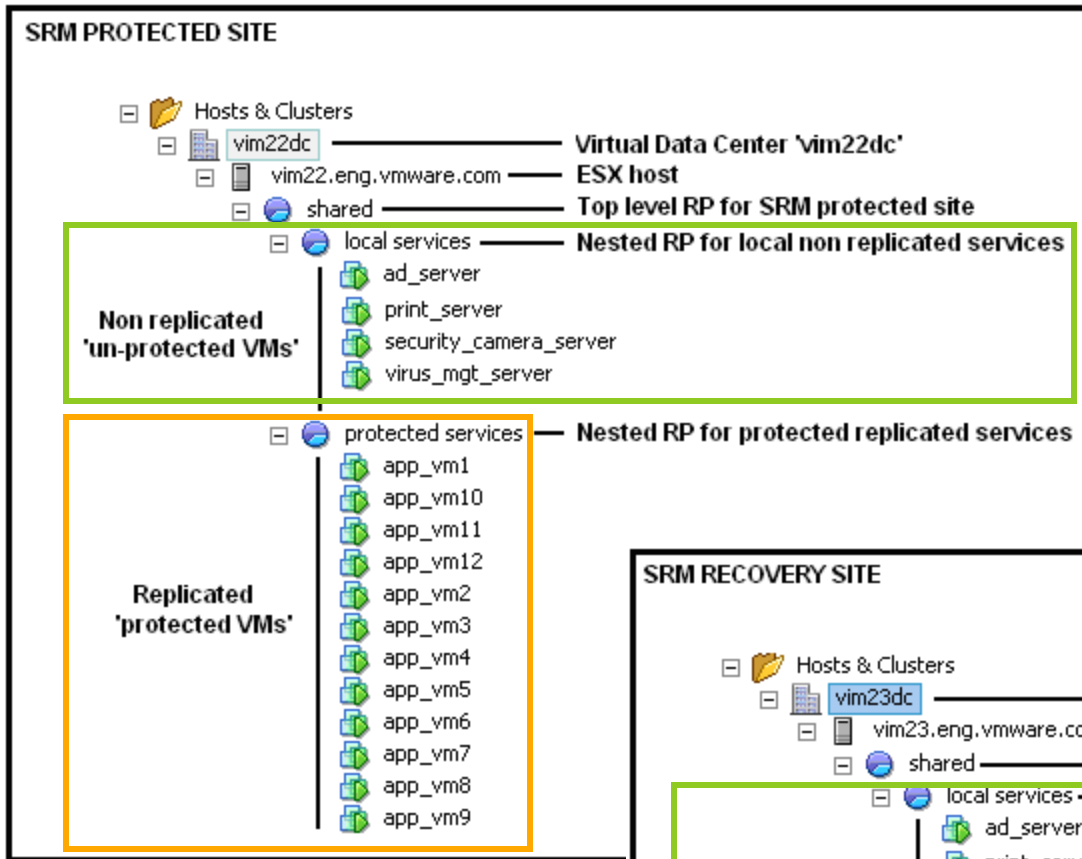
- > Installation of the SRM server
- > Installation of the SRM Plugin into the VI Client *
- > Installation of the Storage Replication Adapter (SRA)

It is important to complete the Site Recovery Manager workflows in the order detailed in this presentation

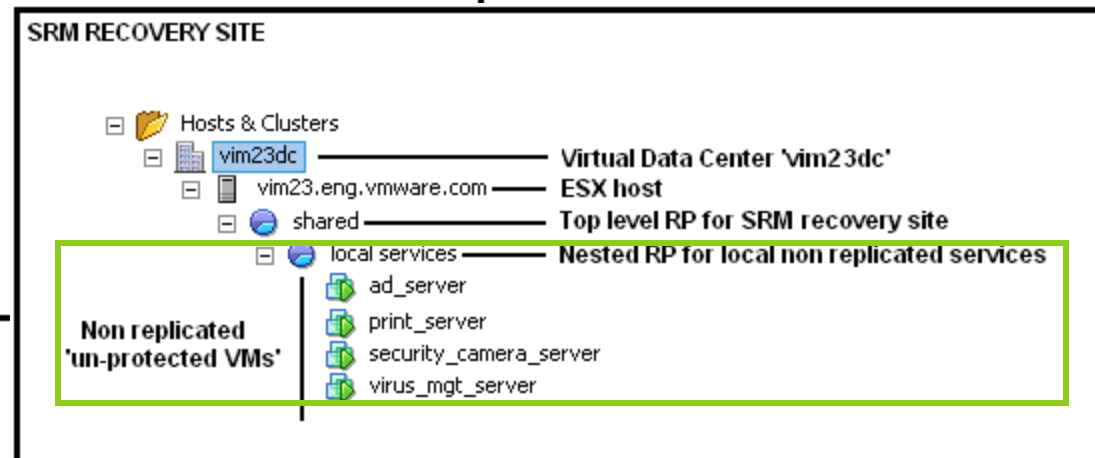
* Note: Optional step, only required if a different instance of the VI Client is used to access the recovery site

Protected and Recovery Site Datacenters

PROTECTED SITE



RECOVERY SITE



Site Recovery Manager User Interface

The screenshot displays the VMware Infrastructure Client interface for Site Recovery Manager. The top navigation bar includes 'Events', 'Administration', 'Maps', 'Consolidation', and 'Site Recovery' (highlighted with a red box). Below this, the 'dr-vim22' instance is shown with tabs for 'Summary', 'Alarms', and 'Permissions'. The 'Summary' tab is active, displaying two columns: 'Local Site' and 'Paired Site', both with fields for 'VC Server:', 'DR Server:', and 'Site Name:'. A 'Setup' section below contains a message: 'This server has not completed set up for disaster recovery. To complete configuration, follow the steps below.' This section is also highlighted with a red box and contains a table of configuration items:

Item	Status	Action
Connection:	Not Configured	Configure Break
Array Managers:	Not Configured	Configure
Inventory Preferences:	Not Configured	Configure
Protection Groups:	0 Group(s) Created	Create
Recovery Plans:	0 Plan(s) Created	Create

Setup Workflow – Protection Site

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

- > The user
- > Security
- VC serv

Primary sites
Servers and the

Connect to Remote Site

Remote Site Information
Connect to a remote site.

Remote Site Information
Authentication
Complete Connections

VMware Site Recovery Manager

Certificate Type Selection

Choose a certificate method for authentication.

Certificate Source

Select a certificate source.

Use a PKCS#12 certificate file.
You will be prompted to select a PKCS#12 certificate and optional password.

Automatically generate a certificate.
Select this option if you wish to use an automatically generated certificate.

InstallShield

< Back Next > Cancel

Certificates that result in the Yes/No Reciprocity will allow you to continue the workflow.

✓ Reciprocity is established.

Setup Workflow – Protection Site

Add Array Manager

Array Manager Information

Display Name:

Manager Type:

SP-A IP:

SP-B IP:

Username:

Password:

Array ID	Model
From the Manager Type drop down box select the correct Manager Type for the SAN in your environment	

Array Managers Configuration

- > Select the correct **Manager Type** from the Manager type drop down box

Setup Workflow – Protection Site

- > SRM identifies available arrays and replicated datastores and determines the datastore groups.

Configure Array Managers
Protection Side Array Managers
Enter the location and credentials for array managers on the protection side.

Protection Side Array Manager:
Recovery Side Array Managers
Review Mirrored LUNs

Display Name	Manager Type	Address
vim22dc SAN	Symmetrix Native	vim22

Protection Arrays:

Array ID	Model	Peer Array	LUN Count
000190102189	DMX3-24	000187461516	38

Configure Array Managers
Recovery Side Array Managers
Enter the location and credentials for array managers on the recovery side.

Protection Side Array Managers
Recovery Side Array Managers
Review Mirrored LUNs

Display Name	Manager Type	Address
vim23dc SAN	Symmetrix Native	vim23

Protection Arrays:

Array ID	Model	Peer Array	LUN Count
000190102189	DMX3-24	000187461516	0

Review Mirrored LUNs
Review the list of mirrored datastores and RDMs.

Protection Side Array Managers
Recovery Side Array Managers
Review Mirrored LUNs

- SAN Array 000190102189
 - LUN Group: [shared-san-1]
 - LUN Group: [shared-san-2]

Setup Workflow – Protection Site

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

Protection Groups

Summary | Protection Groups | **Inventory Preferences** | Permissions

This diagram indicates mappings between resources on the primary site and its secondary site. Resources used by a protected virtual machine on the primary site will be replaced by the mapped resources in the shadow virtual machines on the secondary site.

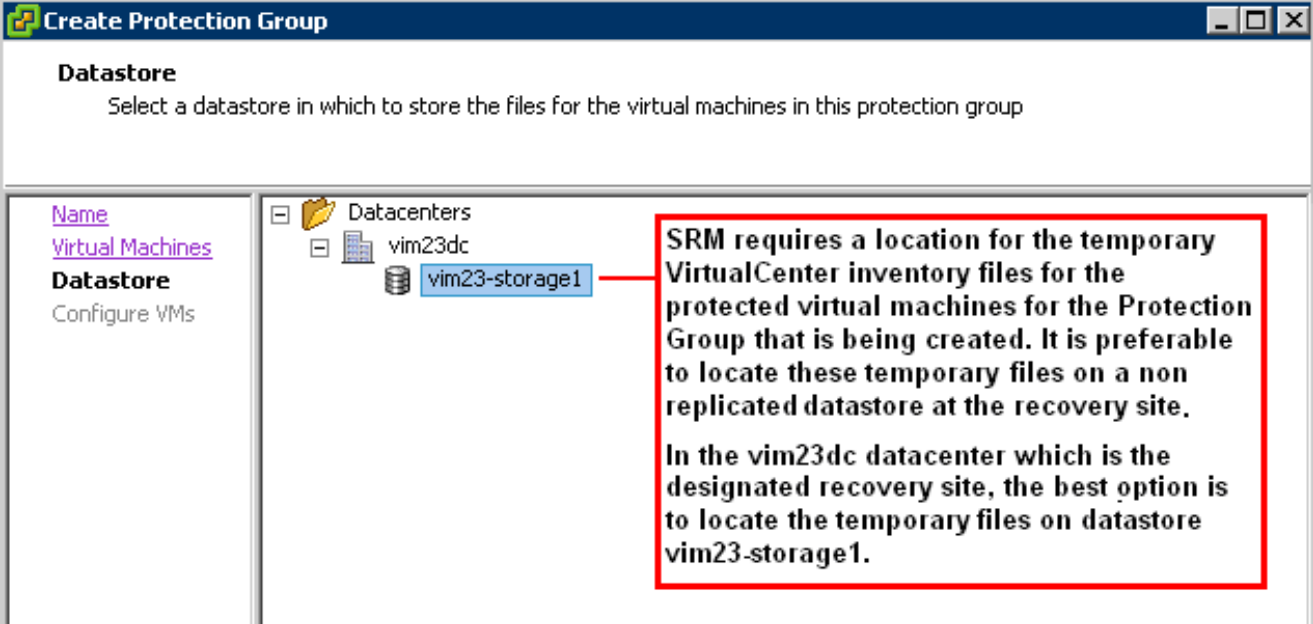
[Refresh](#) [Edit...](#) [Remove](#)

Primary Site Resources	Secondary Site Resources	Secondary Site Path
Networks		
vim22dc	---	
VM Network	VM Network	/Networks/vim23dc/
Compute Resources		
vim22dc	---	
vim22.eng.vmware.com	None Selected	
shared	None Selected	
local services	None Selected	
protected services	recovery	/Hosts & Clusters/vim23dc/vim23.eng.vmware.com/shared/
Virtual Machine Folders		
vim22dc	None Selected	
shared	recovery	/Hosts & Clusters/vim23dc/shared/

Setup Workflow – Protection Site

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 location for temporary VirtualCenter Inventory files for the protected VMs at the recovery site.



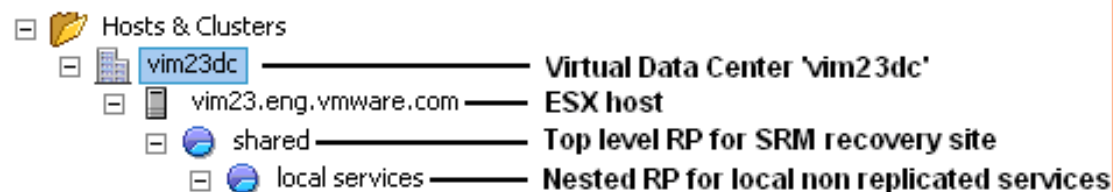
SRM requires a location for the temporary VirtualCenter inventory files for the protected virtual machines for the Protection Group that is being created. It is preferable to locate these temporary files on a non replicated datastore at the recovery site.

In the vim23dc datacenter which is the designated recovery site, the best option is to locate the temporary files on datastore vim23-storage1.

Setup Workflow – Protection Site

- > 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

SRM RECOVERY SITE AFTER THE CONFIGURATION OF SRM PROTECTION GROUPS



```
root@vim23:/vmfs/volumes/vim23-storage1/app_vm12
[root@vim23 vim23-storage1]# cd app_vm12
[root@vim23 app_vm12]# ls -al
total 1216
drwxr-xr-x  1 root  root    700 Feb  6 21:58 .
drwxrwxrwt  1 root  root   4760 Feb 11 16:03 ..
-rw-----  1 root  root     0 Feb  6 21:58 app_vm12.vmsd
-rw-r--r--  1 root  root    911 Feb  6 21:58 app_vm12.vmx
-rw-----  1 root  root    263 Feb  6 21:58 app_vm12.vmxfs
[root@vim23 app_vm12]#
```

- app_vm2
- app_vm3
- app_vm4
- app_vm5
- app_vm6
- app_vm7
- app_vm8
- app_vm9

'recovery' RP specified during the SRM Inventory Preferences configuration.

The VMs are registered in the VC inventory during the configuration of the SRM Protection Groups.

Setup Workflow – Recovery Site

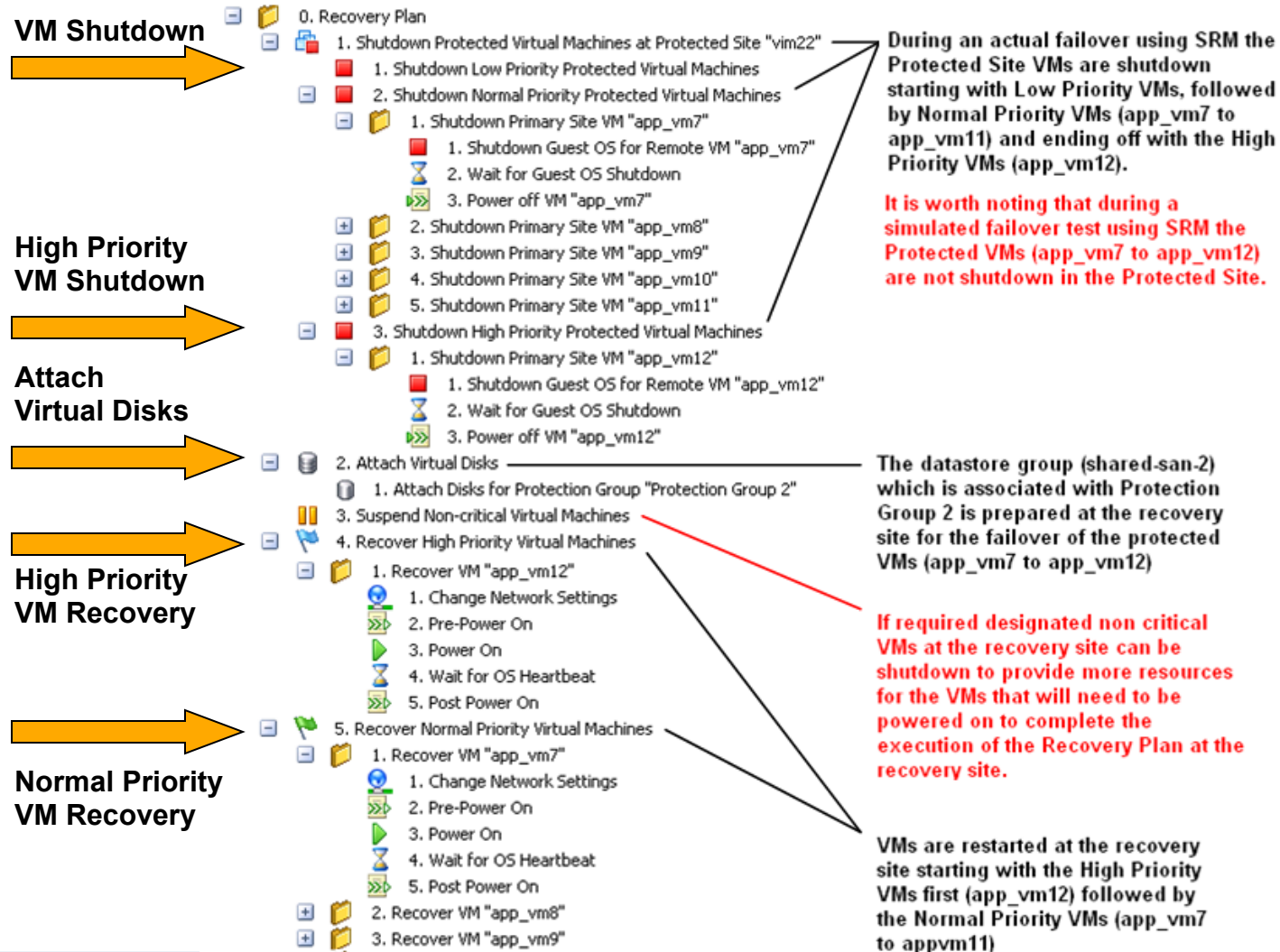
At the **recovery site** the following setup activity is completed:

- > The user creates a recovery plan which is associated to a single or multiple protection groups

Recovery Plans are added via the VI Client connected to the VC server in the recovery site.

Click on the Add button on the toolbar above or click on the Add Recovery Plan under the Commands section to launch the Recovery Plan wizard

Site Recovery Manager Recovery Plan



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 appvm11)

Site Recovery Manager Recovery Plan

Low Priority VM Recovery



Post Test Cleanup

Virtual Disk Reset



- 4. Recover VM "app_vm10"
- 5. Recover VM "app_vm11"
- 6. Recover Low Priority Virtual Machines
- 7. Recover No Power On Virtual Machines
- 8. Cleanup Virtual Machines Post Test
- 1. Remove Test VM "app_vm7"
- 2. Remove Test VM "app_vm8"
- 3. Remove Test VM "app_vm9"
- 4. Remove Test VM "app_vm10"
- 5. Remove Test VM "app_vm11"
- 6. Remove Test VM "app_vm12"
- 9. Cleanup DRS Clusters
- 10. Resume Non-critical Virtual Machines
- 11. Reset Virtual Disks Post Test
- 1. Reset Disks for Protection Group "Protection Group 2"

VMs that are powered up at the recovery site during a 'Test' of the Recovery Plan are powered down at the recovery site as part of the post test procedures.

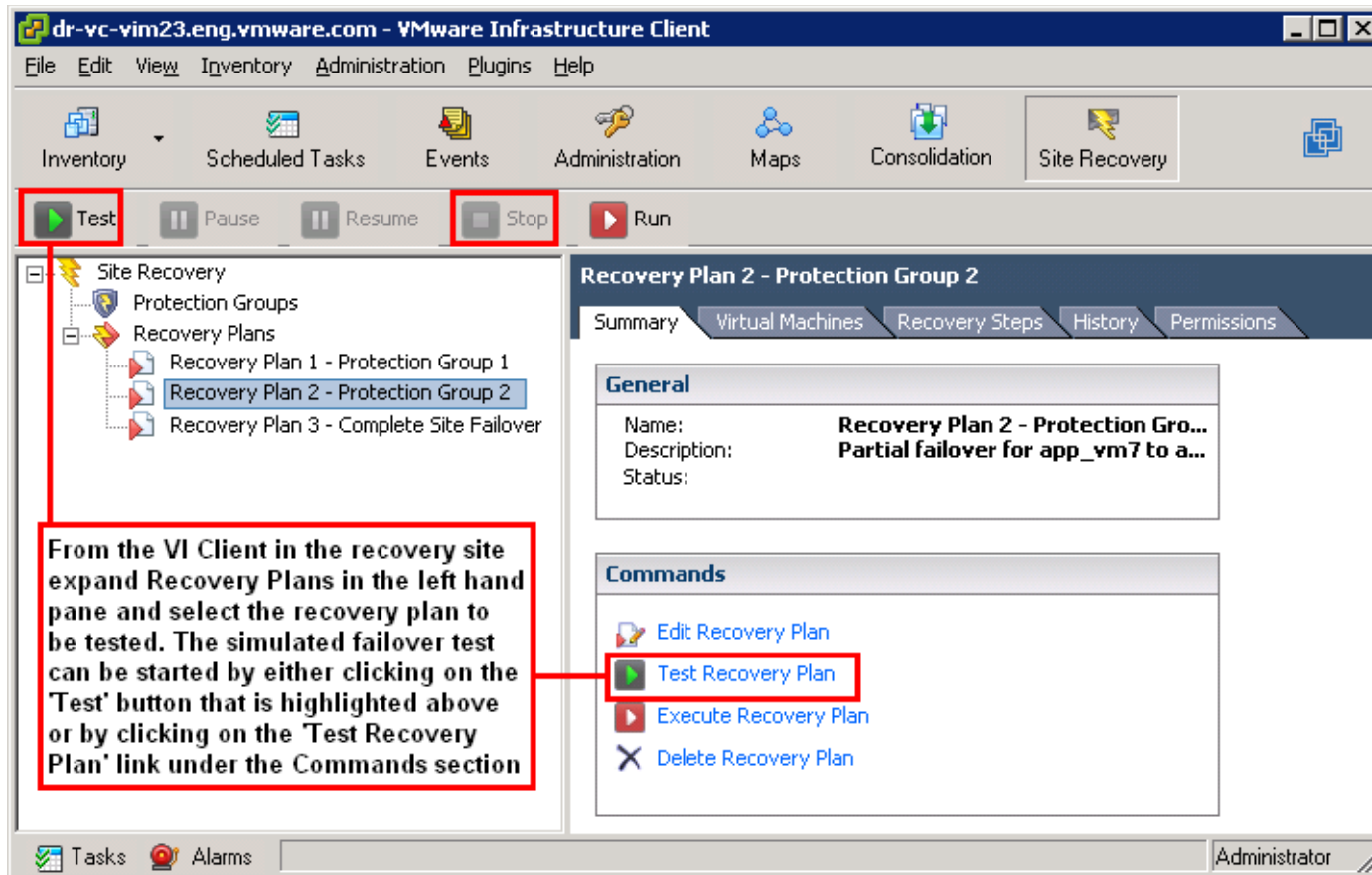
SRM Recovery Site is reset and left in a ready state for the next SRM Test or Failover event due to a disaster being declared.

Site Recovery Manager Recovery Plans:

- > 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

'Test' a recovery plan by simulating a failover of protected VMs with zero downtime to the protected VMs in the protected site



The screenshot displays the VMware Infrastructure Client interface. At the top, the title bar reads "dr-vc-vim23.eng.vmware.com - VMware Infrastructure Client". Below the title bar is a menu bar with "File", "Edit", "View", "Inventory", "Administration", "Plugins", and "Help". A toolbar contains icons for "Inventory", "Scheduled Tasks", "Events", "Administration", "Maps", "Consolidation", and "Site Recovery". Below the toolbar is a control bar with buttons for "Test", "Pause", "Resume", "Stop", and "Run". The "Test" button is highlighted with a red box. The main area is divided into two panes. The left pane shows a tree view under "Site Recovery" with "Protection Groups" and "Recovery Plans". "Recovery Plan 2 - Protection Group 2" is selected and highlighted. The right pane shows the details for "Recovery Plan 2 - Protection Group 2" with tabs for "Summary", "Virtual Machines", "Recovery Steps", "History", and "Permissions". The "General" tab is active, showing "Name: Recovery Plan 2 - Protection Gro...", "Description: Partial failover for app_vm7 to a...", and "Status:". Below this is the "Commands" section with links for "Edit Recovery Plan", "Test Recovery Plan", "Execute Recovery Plan", and "Delete Recovery Plan". The "Test Recovery Plan" link is highlighted with a red box. A red text box on the left side of the screenshot contains the following text: "From the VI Client in the recovery site expand Recovery Plans in the left hand pane and select the recovery plan to be tested. The simulated failover test can be started by either clicking on the 'Test' button that is highlighted above or by clicking on the 'Test Recovery Plan' link under the Commands section".

From the VI Client in the recovery site expand Recovery Plans in the left hand pane and select the recovery plan to be tested. The simulated failover test can be started by either clicking on the 'Test' button that is highlighted above or by clicking on the 'Test Recovery Plan' link under the Commands section

Testing a Recovery Plan

Recovery Plan 2 - Protection Group 2

Summary Virtual Machines **Recovery Steps** History Permissions

tree

Status	Task Started	Task Completed	Mode
Success	1/10/2008..	1/10/2008 8:27:56 PM	Recovery only
Success	1/10/2008..	1/10/2008 8:27:56 PM	Recovery only
Success	1/10/2008..	1/10/2008 8:27:56 PM	Recovery only
Success	1/10/2008..	1/10/2008 8:27:56 PM	Recovery only
Success	1/10/2008..	1/10/2008 8:33:15 PM	
Success	1/10/2008..	1/10/2008 8:33:15 PM	
Success	1/10/2008..	1/10/2008 8:33:15 PM	
Running	1/10/2008..	60	
Running	1/10/2008..	60	
Success	1/10/2008..	1/10/2008 8:33:31 PM	
Success	1/10/2008..	1/10/2008 8:33:31 PM	
Success	1/10/2008..	1/10/2008 8:33:55 PM	
Running	1/10/2008..	7	

1. Shutdown Primary Site VM "app_vm12"

1. Shutdown Guest OS for Remote VM "app_vm12"

2. Wait for Guest OS Shutdown

3. Power off VM "app_vm12"

2. Attach Virtual Disks

1. Attach Disks for Protection Group "Protection Group 2"

3. Suspend Non-critical Virtual Machines

4. 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

5. Recover Normal Priority Virtual Machines

1. Recover VM "app_vm7"

1. Change Network Settings

2. Pre-Power On

3. Power On

4. Wait for OS Heartbeat

5. Post Power On

2. Recover VM "app_vm8"

Each step that is executed in the recovery plan can be monitored via the Recovery Steps window while the simulated failover test is running.

Recovery Plan steps identified by 'Recover Only' are only executed during an actual failover.

Recovery Plan 2 - Protection Group 2

Summary Virtual Machines Recovery Steps **History** Permissions

Date & Time	Plan	Mode	Result	Execution Time	Actions
1/10/2008 8:27:55 PM	Recovery Plan 2 - Protection Group 2	Test	Success	00:15:24.23	View Export
1/10/2008 2:20:42 PM	Recovery Plan 2 - Protection Group 2	Test	Success	00:17:35.81	View Export

Executing Failover

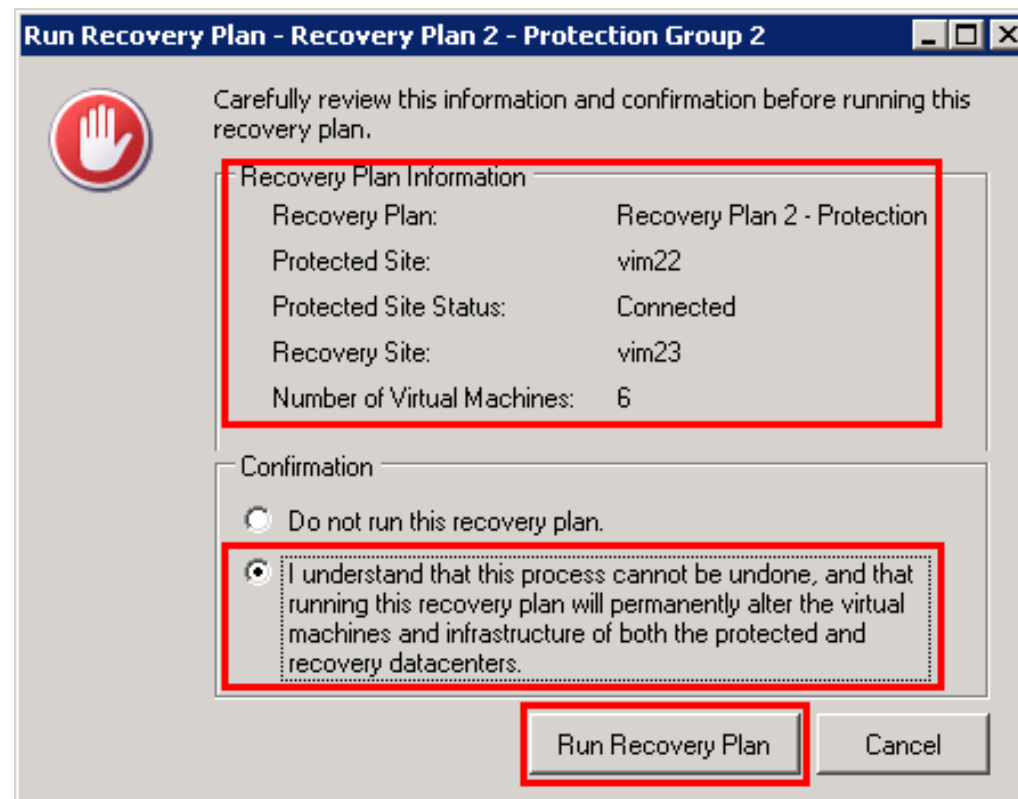
The screenshot displays the VMware Infrastructure Client interface. The top menu bar includes File, Edit, View, Inventory, Administration, Plugins, and Help. Below the menu is a toolbar with icons for Inventory, Scheduled Tasks, Events, Administration, Maps, Consolidation, and Site Recovery. A secondary toolbar contains buttons for Test, Pause, Resume, Stop, and Run. The main workspace is divided into two panes. The left pane shows a tree view under 'Site Recovery' with 'Recovery Plans' expanded, listing 'Recovery Plan 1 - Protection Group 1', 'Recovery Plan 2 - Protection Group 2', and 'Recovery Plan 3 - Complete Site Failover'. The right pane shows the details for 'Recovery Plan 2 - Protection Group 2', with tabs for Summary, Virtual Machines, Recovery Steps, History, and Permissions. The 'Recovery Steps' tab is active, showing a 'General' section with Name, Description, and Status fields, and a 'Commands' section with links for Edit, Test, Execute, and Delete Recovery Plan. Red boxes highlight the 'Run' button in the top toolbar, the 'Recovery Steps' tab, and the 'Execute Recovery Plan' link in the Commands section. A text box with a red border provides instructions on how to execute the failover.

From the VI Client in the recovery site expand Recovery Plans in the left hand pane and select the recovery plan to execute the failover against. The failover can be started by either clicking on the 'Run' button that is highlighted above or by clicking on the 'Execute Recovery Plan' link under the Commands section

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

Executing Failover

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



Failback Options in Site Recovery Manager 1.0

- ▶ Site Recovery Manager 1.0 does not provide a push-button automated failback process.
- ▶ Failback Options:
 - > Without SRM (**no startup order, no failback history reports**)
 - Work with your storage team, reverse data replication
 - VM re-inventory*, restart and re-ip (manual or scripted)
 - > With SRM (**start up order in recovery plan with failback history**)
 - Work with your storage team, reverse data replication
 - Leverage SRM, complete all SRM workflows in the reverse direction from Recovery Site back to the Protected Site
 - Repeat the above two steps from the Protected Site back to the recovery Site.

* Note: VM re-inventory in VC may not be necessary in the Protected site.

Default Roles and Privileges

dr-vc-vim23.eng.vmware.com - VMware Infrastructure Client

File Edit View Inventory Administration Plugins Help

Inventory Scheduled Tasks Events Administration

Add Role Clone R

Roles Sessions Licenses

Roles

Name
Virtual Machine Administrator
Datacenter Administrator
Virtual Machine Power User
Virtual Machine User
Resource Pool Administrator
VMware Consolidated Backup User
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

- 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
 - Recovery Plan
 - Create
 - Remove
 - Modify
 - Run
 - Remote Site
 - Create
 - Remove
 - Modify
 - Array Manager
 - Configure
 - Recovery Virtual Machine
 - Modify
 - Recovery Group
 - Modify

Alarms and Site Status Monitoring

Site Recovery Manager 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

Site Recovery Manager will raise VirtualCenter 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



Questions?