

Building a DR solution using VMWARE SRM and EMC Storage Platforms

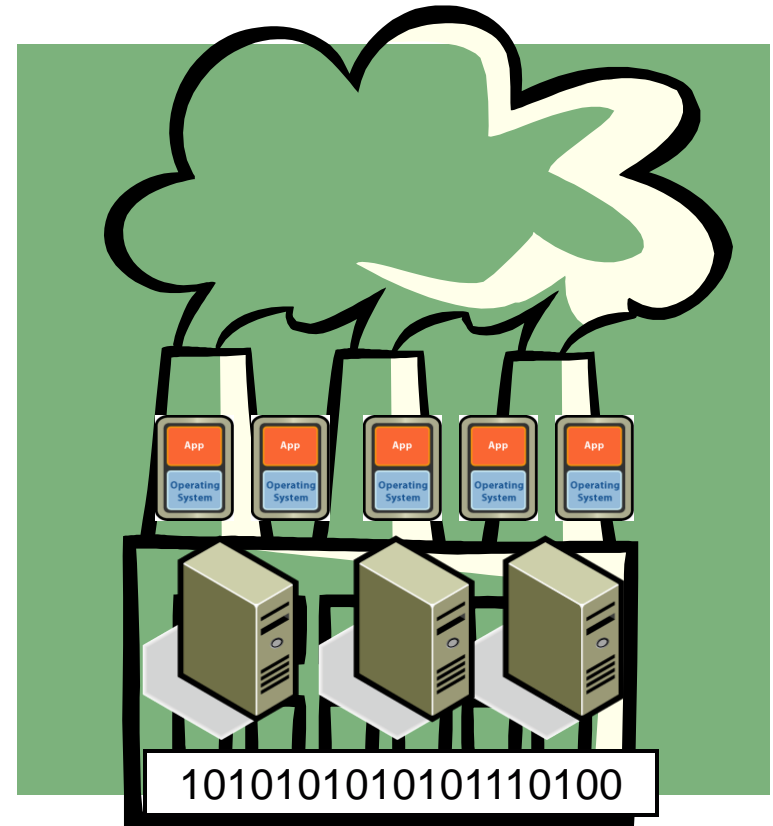
Itzik Reich
Solutions Architect
reich_itzik@emc.com



Availability Technology Taxonomy

Key elements of availability are

- DR (site protection)
- Data protection (protecting the bits)
- HA (continuously running apps)





The Current State of (Physical) DR

Tier	Recovery point objective (RPO)	Recovery Time objective (RTO)	Cost
I	Immediate	Immediate	\$\$\$
II	24+ hrs.	48+ hrs.	\$\$
III	7+ days	5+ days	\$

- * DR Services tiered according to business needs
- * Physical upgrades and patches in parallel
- * Little Automation
- * Error-prone and difficult to test

RPO = Recovery point objective (point in time to which data must be recovered, i.e. how old can the data be?)

RTO = Recovery Time objective (time required to complete recovery of application data)



Advantages of Virtual Disaster Recovery

VMware is a true enabler for 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

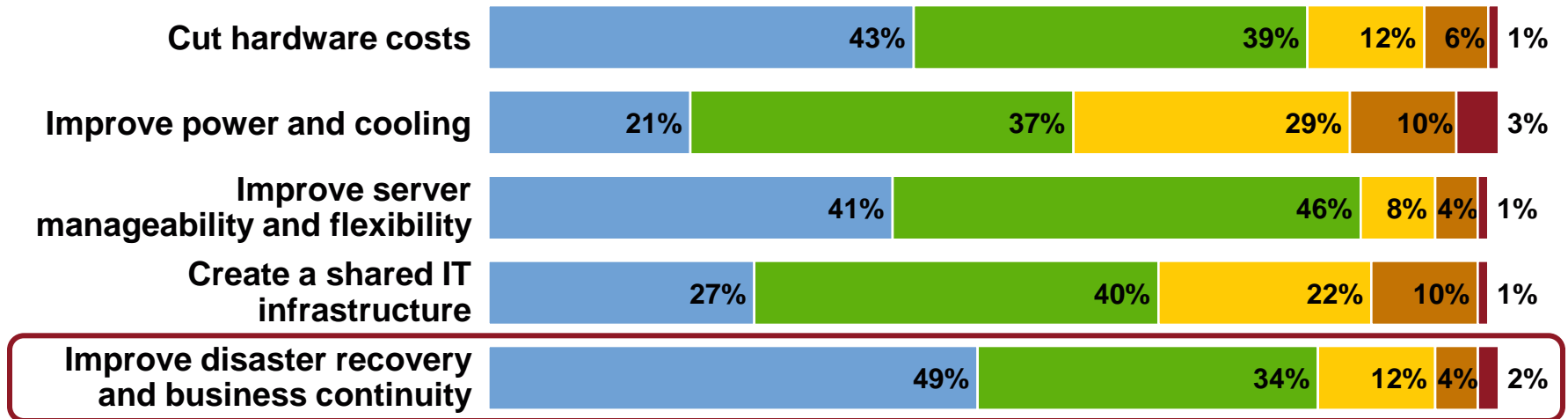




Disaster Recovery is a Top VMware Requirement

“How important are the following motivations for adopting server virtualization?”

■ Very important ■ Important ■ Slightly/somewhat important ■ Not important ■ Doesn't know or does not apply to me



Base: 197 server decision-makers at North American and European enterprises that are interested in, are implementing in the next 12 months, or have already implemented server virtualization for x86 servers (percentages may not total 100 because of rounding)

Introducing VMware Site Recovery Manager (SRM)



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



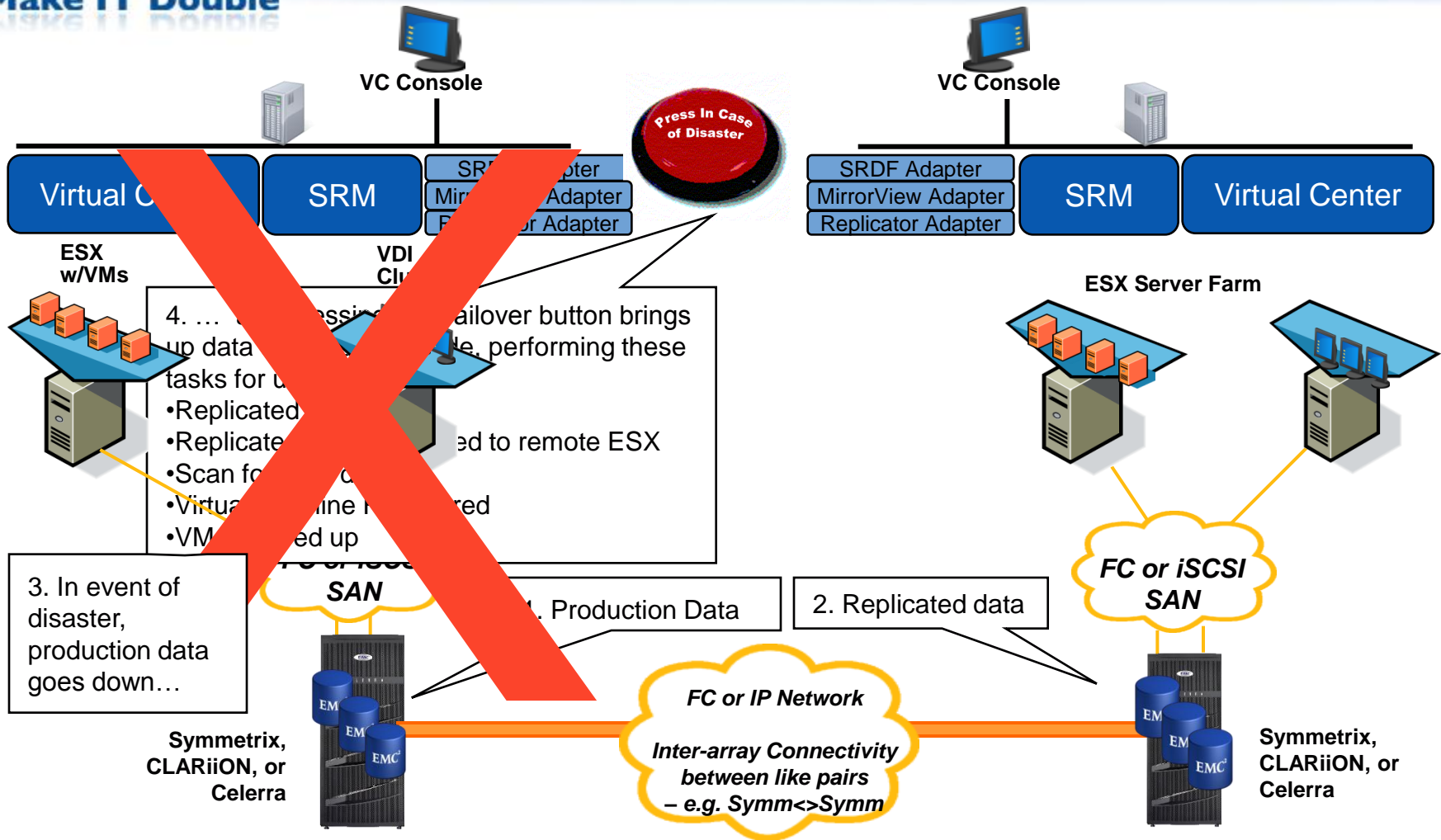
Site Recovery Manager works with VMware Infrastructure to enable faster, more reliable, affordable disaster recovery

- Turns manual recovery runbooks into automated recovery plans
- Provides central management of recovery plans from VirtualCenter

Site Recovery Manager leverages VMware infrastructure to transform disaster recovery

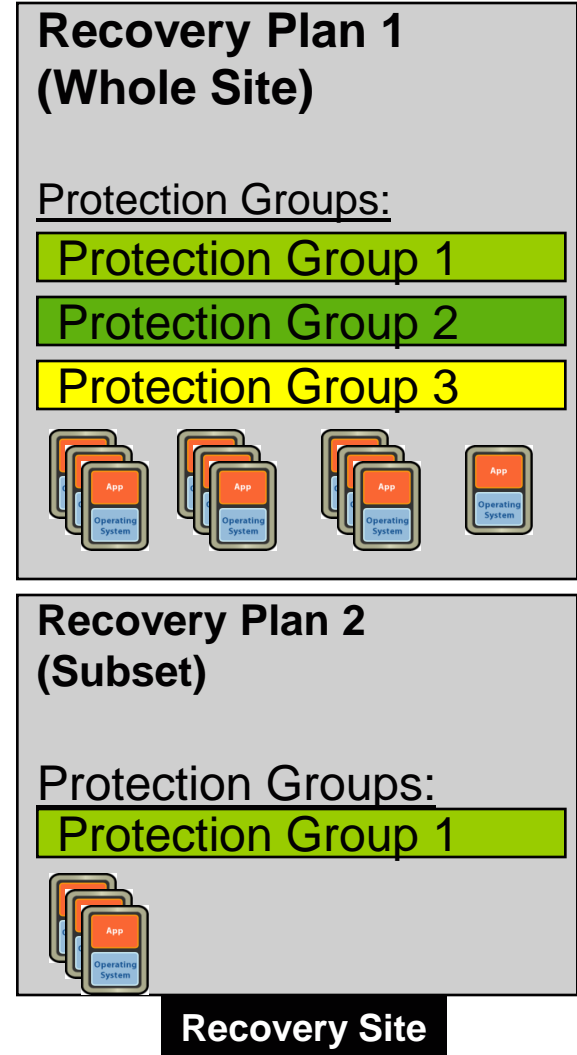
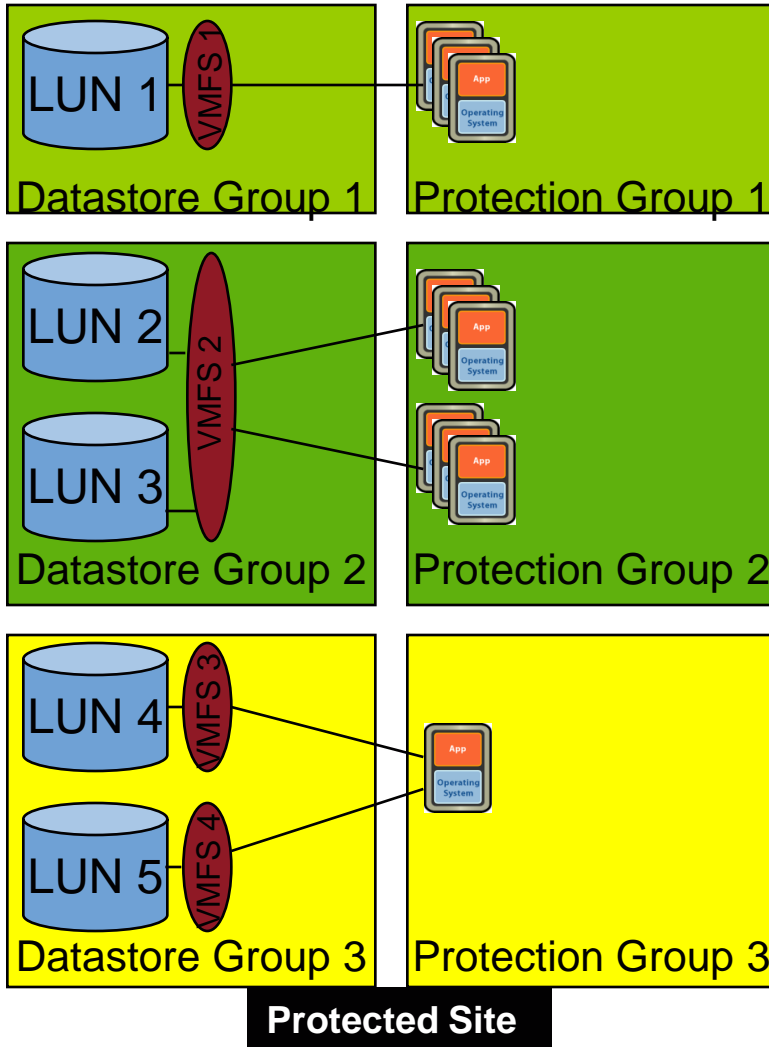


VM Failover with SRM and EMC Replication



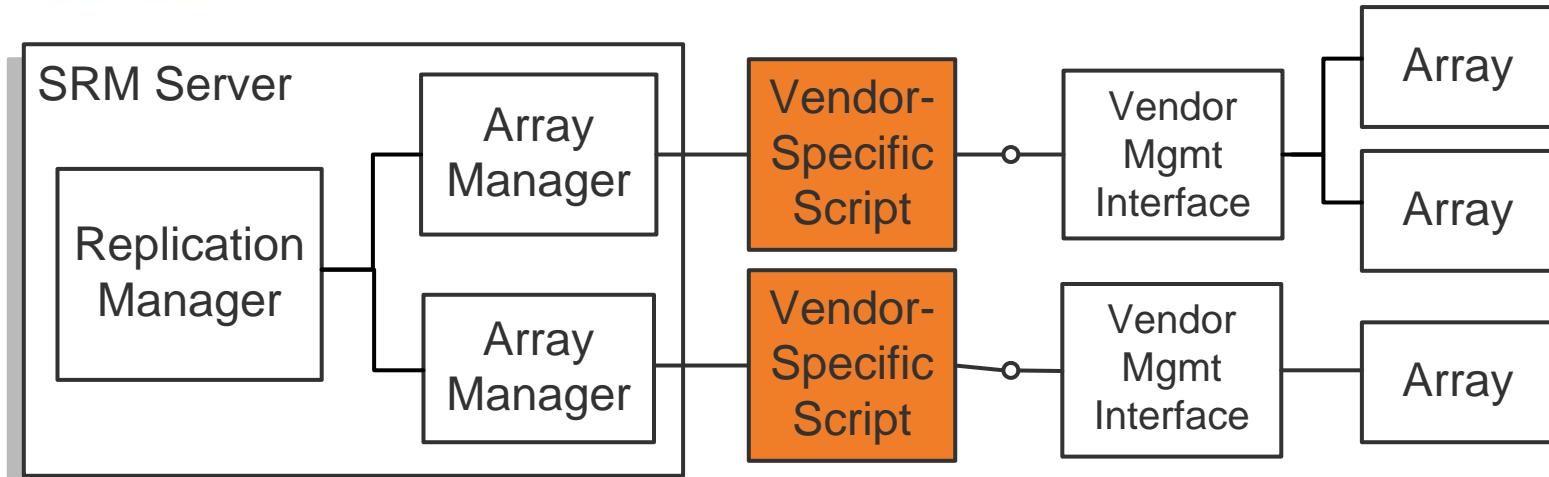


SRM Concepts and their Relationships





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 SRM



SRM 1.0 Prerequisites

- ESX Server 3.0.2, ESX Server 3.5 or ESXi Server 3.5
- VirtualCenter Server version 2.5 U1 installed at the **protected site** and the **recovery site**
- SRM server installed at the protected and 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 the **recovery site**.
- A SRM License file installed on the VC license server at the **protected site** and **the recovery site**.
- **Pre-configured array-based replication between the protected site and the recovery site**

SRM Compatability Matrixes:

http://www.vmware.com/pdf/srm_10_compat_matrix.pdf



SRDF SAN Replication Adapter

- DMX storage arrays
 - DMX-1/2 running Enginuity code 5671
 - DMX-3 and DMX-4 running Enginuity code 5771 or later.
- Management of Symmetrix array is done in-band
 - **Solutions Enabler version 6.5.0 or later**
- Host running Solutions Enabler is required at each site
 - Can be the Virtual Center Server if it has connection to the storage array.
- Solutions Enabler not required on Virtual Center Server However, strongly recommended
- Solutions Enabler in a client/server configuration
 - Host providing management service needs to be configured to provide service
 - Solutions Enabler on Virtual Center Server needs to be configured to access server
 - SSL connections between client and server recommended
- Solutions Enabler can be run on the ESX Server Console
 - Port 2707 has to be opened



SRDF SAN Replication Adapter

- SRDF/S and SRDF/A modes are supported
 - No support for SRDF/S consistency groups
 - No support for MSC
 - Provides consistency across multiple SRDF/A groups
 - No support for advanced configurations
 - SRDF/AR, SRDF/STAR etc.
- TimeFinder/Snap is not supported for testing recovery plans
 - No support for “splitting” SRDF link for testing recovery plans
 - TimeFinder/Mirror is required for testing recovery plans using non-grouped devices



Mirrorview SAN Replication Adapter

Requirements

- MirrorView /Synchronous and **Asynchronous** (was recently announced)
- Clariion CX3-10,20,40,80 (FC and iSCSI) with Flare 3.26
- Clariion CX4-120,240,480,960 (FC and iSCSI) with Flare 4.28
- AX4-5 (FC) with Flare 2.23
- All LUNs must be in consistency groups (replicated LUNs not in consistency groups will not be returned to SRM)



Celerra SAN Replication Adapter

Celerra software requirements

- DART operating system 5.6.36 or later
- Enabled licenses
- iSCSI (**NFS is not** supported in SRM 1.0)
- SnapSure
- Replicator v2

Local system software requirements

- Java Runtime Environment 1.6

Capabilities

- iSCSI lun replication for VMware SRM purposes
- No FC lun replication support

Gotchas

- Not every command returns to STDOUT
- It may be difficult to determine if a command succeeded



RecoverPoint SAN Replication Adapter

- **Hardware Prerequisites**

- **EMC RecoverPoint appliances running 3.0_g60 or above**
- One or more consistency groups configured, initialized and replicating between local and remote VMware environments.
 - Supported Array's (see RecoverPoint ESM for VMware)
 - Supported Splitting Technology (CX Splitter, Cisco SANTap and Brocade FAP)

Gotchas - RecoverPoint

- When a consistency group is being controlled by SRM there is no identifying flags
- CLR and CDP consistency groups are not supported
 - When doing a failover test we only support virtual access mode

Gotchas - VMware SRM

- No built-in failback
- This can be worked around by creating a new recovery plan or through a manual failover in RecoverPoint.
 - Does not support RecoverPoint point-in-time recovery

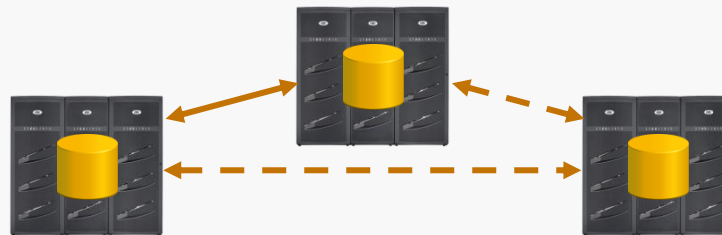


Enabling Technology - EMC Advanced Replication Technologies



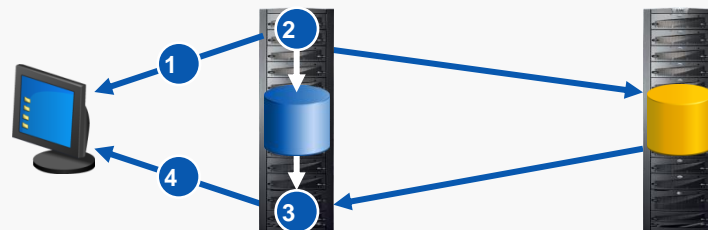
SRDF Family

The ultimate business continuity and disaster recovery solution for the broadest range of use cases



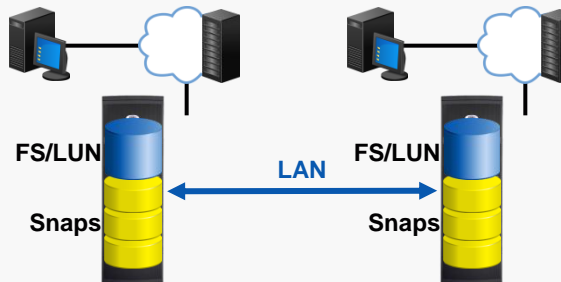
MirrorView

Synchronous & Asynchronous replication for flexible recovery-point and recovery-time objective requirements



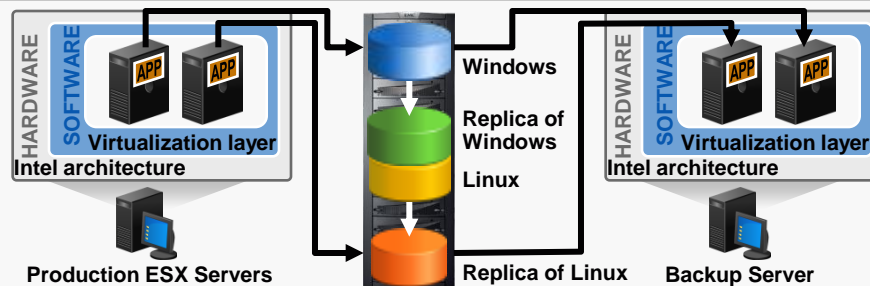
Celerra Replicator

IP replication with Quality of Service to optimize LAN/WAN bandwidth utilization



RecoverPoint

Host, array, fabric continuous data protection (CDP), continuous remote replication (CRR), concurrent local and remote (CLR) data protection; and compression





SRM Installation Workflow

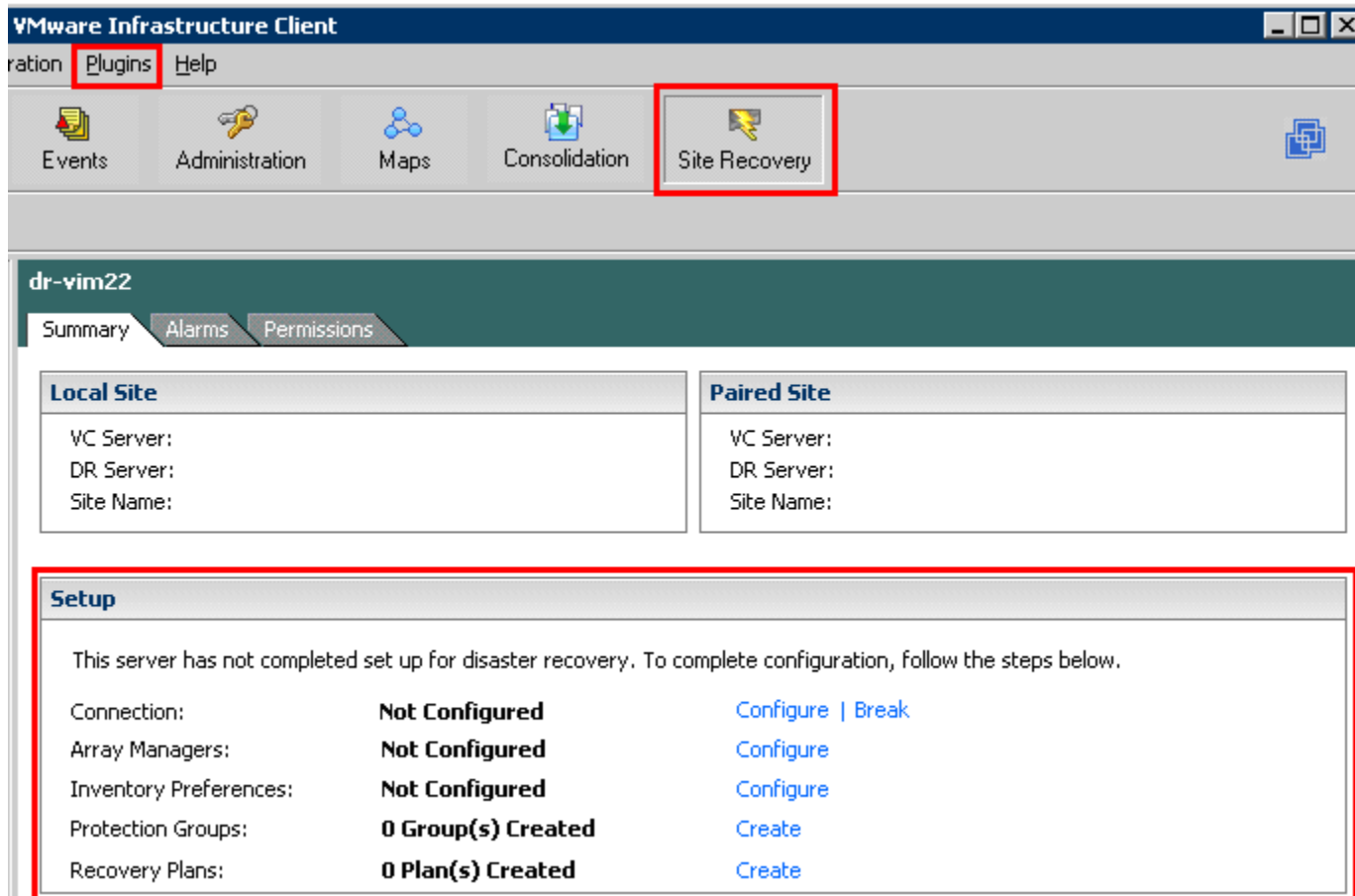
- At the protected site the following activities are completed:
 - installation of the SRM server
 - Installation of the SRM Plug-in into the VI Client
 - Installation of the Storage Replication Adapter (SRA)
- At the recovery site the following activities are completed:
 - Installation of the SRM server.
 - Installation of the SRM Plug-in into the VI Client
 - Installation of the Storage Replication Adapter (SRA)



SRM User Interface

Disaster recovery management is another view of environment

- Viewed from VirtualCenter management client
- One central point of management for virtual infrastructure and disaster recovery



VMware Infrastructure Client

ration **Plugins** Help

Events Administration Maps Consolidation **Site Recovery**

dr-vim22

Summary Alarms Permissions

Local Site	Paired Site
VC Server:	VC Server:
DR Server:	DR Server:
Site Name:	Site Name:

Setup

This server has not completed set up for disaster recovery. To complete configuration, follow the steps below.

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



Make IT Double

Configuring the SRDF Adapter for VMware SRM

- Visual Ch...
- Uses
- Configure
- Replicated determined

Configure Array Managers

Review Replicated Datastores
Review the list of replicated datastores and RDMs.

[Protection Side Array Managers](#)
[Recovery Side Array Managers](#)
Review Replicated Datastores

SAN Array 000190101906

- Datastore Group: [srm_sync_span]
 - Datastores
 - LUN 'A5C' replicated to remote LUN 'A5C'
 - LUN 'A5E' replicated to remote LUN 'A5E'
- Datastore Group: [srm_async]
 - Datastores
 - LUN 'A60' replicated to remote LUN 'A60'
- Datastore Group: [srm_async_2], [srm_async_1]
 - Datastores
 - LUN 'A66' replicated to remote LUN 'A66'
 - LUN 'A64' replicated to remote LUN 'A64'
- Datastore Group: [srm_sync]

Help ≤ Back Finish

Extents of spanned VMFS are grouped

Datastores grouped due to consistency definitions or VM configurations

cally



Simplified DR Setup: Resource Mapping

Maps production resources to resources available at recovery site

- * Virtual machine hierarchy
- * Resource pools
- * Network connections

Eliminates complexity of Managing recovery Site resources

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... Remo...

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/



The SRM Scenario ("Script") Based Model

VM Shutdown



High Priority VM Shutdown



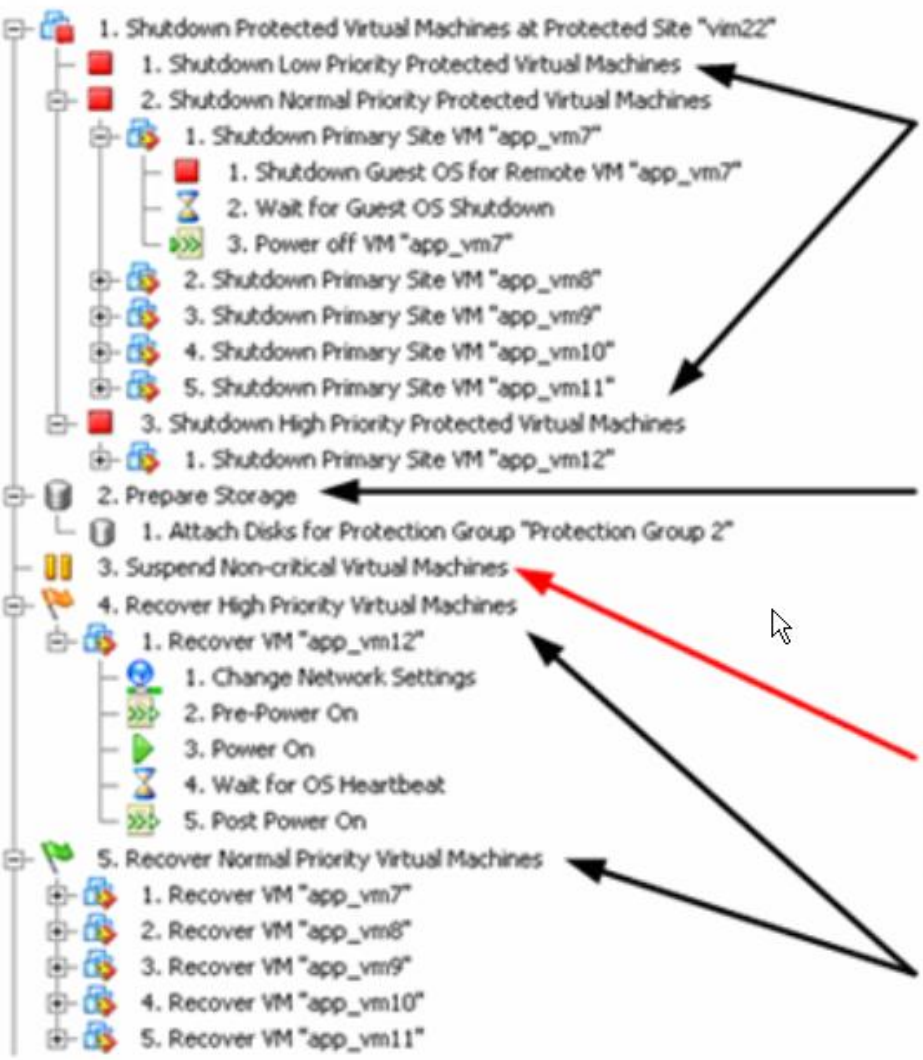
Prepare Storage



High Priority VM Recovery



Normal Priority VM Recovery



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)



Testing a SRM Recovery Plan

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

The screenshot shows the VMware Infrastructure Client interface. The title bar reads "dr-vc-vim23.eng.vmware.com - VMware Infrastructure Client". The menu bar includes "File", "Edit", "View", "Inventory", "Administration", "Plugins", and "Help". The toolbar contains icons for "Inventory", "Scheduled Tasks", "Events", "Administration", "Maps", "Consolidation", and "Site Recovery". Below the toolbar is a row of action buttons: "Test" (highlighted with a red box), "Pause", "Resume", "Stop" (highlighted with a red box), and "Run".

The left-hand pane shows a tree view under "Site Recovery":

- Site Recovery
 - Protection Groups
 - Recovery Plans
 - Recovery Plan 1 - Protection Group 1
 - Recovery Plan 2 - Protection Group 2 (highlighted)
 - Recovery Plan 3 - Complete Site Failover

The right-hand pane displays details for "Recovery Plan 2 - Protection Group 2". It has tabs for "Summary", "Virtual Machines", "Recovery Steps", "History", and "Permissions". The "General" section shows:

Name: Recovery Plan 2 - Protection Gro...
Description: Partial failover for app_vm7 to a...
Status:

The "Commands" section lists:

- Edit Recovery Plan
- Test Recovery Plan (highlighted with a red box)
- Execute Recovery Plan
- Delete Recovery Plan

A red box at the bottom left 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

The bottom status bar shows "Tasks", "Alarms", and the user role "Administrator".



Testing a SRM Recovery Plan - continued

Recovery Plan 2

Summary Virtual Machines **Recovery Steps** History Permissions

Recovery Step	Status	Task Started	Task Completed	Mode
1. Shutdown Protected Virtual Machines at Protected Site "vm22"				Recovery only
1. Shutdown Low Priority Protected Virtual Machines				Recovery only
2. Shutdown Normal Priority Protected Virtual Machines				Recovery only
3. Shutdown High Priority Protected Virtual Machines				Recovery only
1. Shutdown Primary Site VM "app_vm12"				Recovery only
2. Prepare Storage				
1. Attach Disks for Protection Group "Protection Group 2"	Success	4/4/2008 3:11:11 PM	4/4/2008 3:28:15 PM	
3. Suspend Non-critical Virtual Machines	Success	4/4/2008 3:11:11 PM	4/4/2008 3:28:15 PM	
4. Recover High Priority Virtual Machines	Error: Failed to connect NFC service.	4/4/2008 3:28:15 PM	4/4/2008 3:35:10 PM	
1. Recover VM "app_vm12"	Error: Failed to connect NFC service.	4/4/2008 3:28:17 PM	4/4/2008 3:35:10 PM	
5. Recover Normal Priority Virtual Machines	Success	4/4/2008 3:35:10 PM	4/4/2008 3:40:28 PM	
1. Recover VM "app_vm7"	Success	4/4/2008 3:35:19 PM	4/4/2008 3:36:26 PM	
2. Recover VM "app_vm8"	Success	4/4/2008 3:36:26 PM	4/4/2008 3:37:28 PM	
3. Recover VM "app_vm9"	Success	4/4/2008 3:37:28 PM	4/4/2008 3:38:26 PM	
4. Recover VM "app_vm10"	Success	4/4/2008 3:38:26 PM	4/4/2008 3:39:27 PM	
5. Recover VM "app_vm11"	Success	4/4/2008 3:39:27 PM	4/4/2008 3:40:28 PM	
6. Recover Low Priority Virtual Machines	Success	4/4/2008 3:40:28 PM	4/4/2008 3:40:28 PM	
7. Recover No Power On Virtual Machines	Success	4/4/2008 3:40:28 PM	4/4/2008 3:40:28 PM	
8. Message: Test recovery complete. Please verify the success of the...	Waiting for Input	4/4/2008 3:40:28 PM	0%	Test only
9. Cleanup Virtual Machines Post Test				Test only
10. Resume Non-critical Virtual Machines				Test only
11. Reset Storage Post Test				Test only
1. Reset Disks for Protection Group "Protection Group 2"				Test only

Message

[Continue](#) Message: Test recovery complete. Please verify the success of the test. When done, click Continue to clean up the test and return to a ready state.



Testing a SRM Recovery Plan – Recovery Site Cleanup

Low Priority VM Recovery

Post Test Cleanup

Storage Reset

- 6. Recover Low Priority Virtual Machines
- 7. Recover No Power On Virtual Machines
- 8. Message: Test recovery complete. Please verify the success of the test.
- 9. Cleanup Virtual Machines Post Test
 - 1. Remove Test VM "app_vm12"
 - 2. Remove Test VM "app_vm7"
 - 3. Remove Test VM "app_vm8"
 - 4. Remove Test VM "app_vm9"
 - 5. Remove Test VM "app_vm10"
 - 6. Remove Test VM "app_vm11"
- 10. Resume Non-critical Virtual Machines
- 11. Reset Storage 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.





Recovery Plan Reports

Recovery Plan 2									
Summary		Virtual Machines		Recovery Steps		History		Permissions	
Date & Time	Plan	Mode	Result	Execution Time	Actions				
4/4/2008 3:11:10 PM	Recovery Plan 2	Test	Error	01:09:46	View	Export			
4/4/2008 12:52:22 PM	Recovery Plan 2	Test	Success	00:31:01	View	Export			

Recovery Site Recovery Plan

Description

Start Time: 5/28/2008 3:10:13 PM
Finish Time: 5/28/2008 3:23:03 PM
Total Execution Time: 00:12:50
Mode: Test
Overall Result: Success

Recovery Step	Result	Execution Time
1. Shutdown Protected Virtual Machines at Protected Site "Site Recovery for vc1sitea.usvbc.local"		
1.1. Shutdown Low Priority Protected Virtual Machines		
9.6.1. PowerOff VM "demovm7"	Success	00:00:07
9.7. Remove Test VM "demovm9"	Success	00:00:11
9.7.1. PowerOff VM "demovm9"	Success	00:00:11
9.8. Remove Test VM "demovm1"	Success	00:00:16
9.8.1. PowerOff VM "demovm1"	Success	00:00:16
9.9. Remove Test VM "demovm10"	Success	00:00:11
9.9.1. PowerOff VM "demovm10"	Success	00:00:11
9.10. Remove Test VM "demovm2"	Success	00:00:16
9.10.1. PowerOff VM "demovm2"	Success	00:00:16
10. Resume Non-critical Virtual Machines	Success	00:00:00
11. Reset Storage Post Test	Success	00:00:53
11.1. Reset Disks for Protection Group "Site A Protection Group"	Success	00:00:53

Accessible compliance

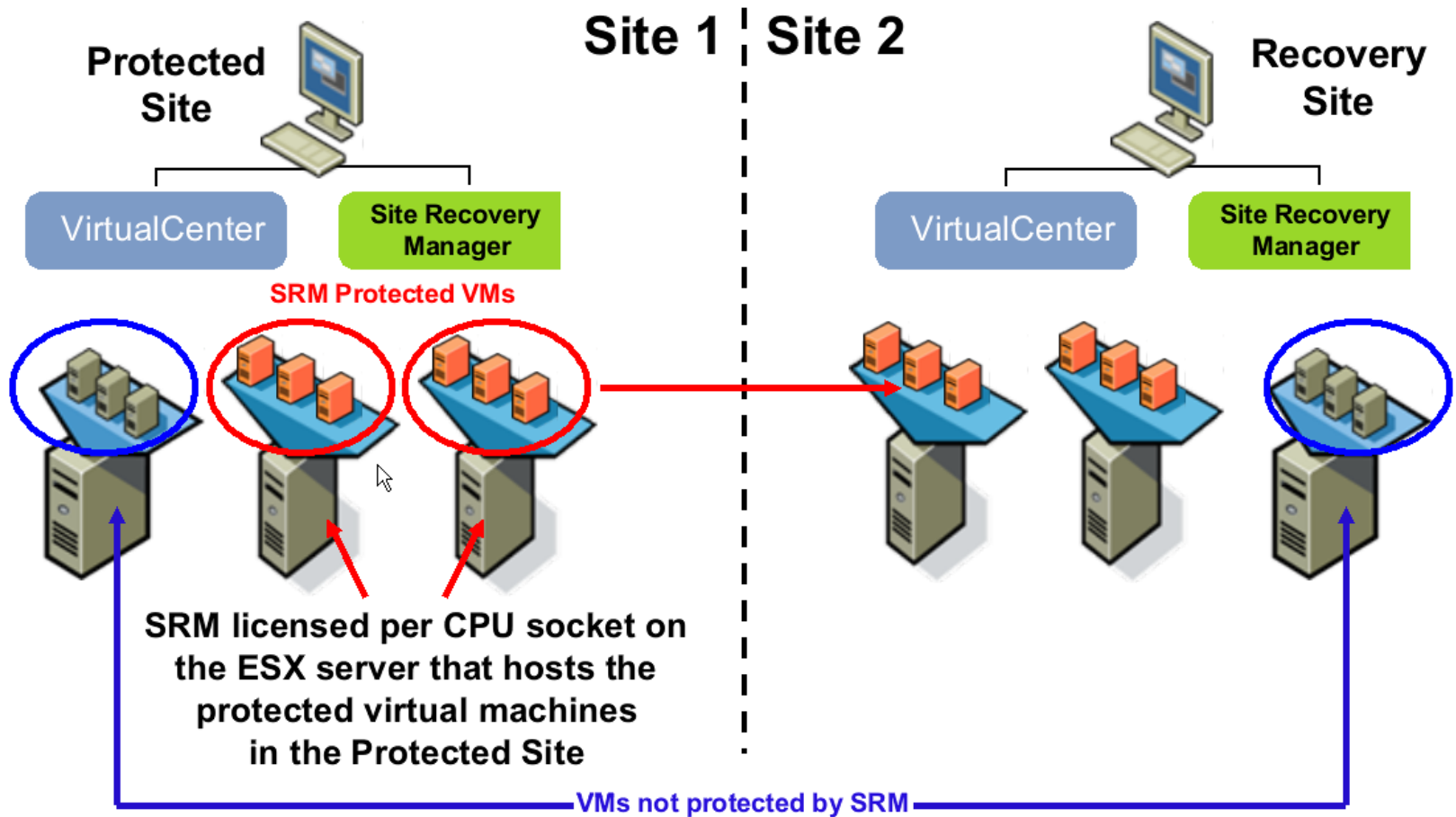
- Exportable recovery plan
- Exportable recovery results
- Maintained history



- ▶ **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**



Vmware SRM Licensing



EMC²[®]

where information lives[®]