

# **EMC Business Continuity for VMware View Enabled by EMC SRDF/S and VMware vCenter Site Recovery Manager**

*A Detailed Review*

## **EMC Global Solutions**

---

### ***Abstract***

This white paper demonstrates that business continuity can be enhanced by using custom scripts with VMware SRM recovery procedures. The scripts enable VMware linked clone virtual desktops, created with VMware View Composer, to be recovered in addition to the server infrastructure as part of the failover to a recovery site. This solution saves recovery time and demonstrates that user settings, data, and user data disks are all recovered.

May 2010

---

---

Copyright © 2010 EMC Corporation. All rights reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com

All other trademarks used herein are the property of their respective owners.

Part number: H6971.1

---

---

## Contents

---

Executive summary.....	4
Introduction.....	5
Key components .....	6
Component overview .....	6
Hardware from other vendors .....	6
EMC Symmetrix VMAX .....	6
VMware vSphere 4 update 1.....	6
VMware HA Cluster.....	7
VMware View Connection Server .....	7
VMware View Composer.....	7
EMC SRDF/S .....	7
VMware View Connection Replica Server .....	7
VMware vCenter Site Recovery Manager.....	7
EMC SRDF Adapter for VMware Site Recovery Manager.....	8
EMC Solutions Enabler .....	8
Physical architecture .....	9
Architecture diagram .....	9
Environment profile .....	10
Hardware resources.....	10
Virtual allocation of hardware resources.....	10
Software resources .....	11
Design and validation.....	12
Design overview .....	12
Validation overview .....	12
Interoperability.....	13
VMware View Connection Server .....	13
VMware View Composer Service.....	13
RSA key container migration.....	14
VMware View Agent.....	15
VMware View Client.....	15
Desktop pools.....	16
Functionality .....	20
Failback .....	20
Performance.....	20
Conclusion.....	21
References .....	22

---

---

## Executive summary

---

**Business case** Organizations cannot afford downtime in their key applications. Business continuity plans must handle service interruptions and recovery from disasters. Yet many organizations only consider the server environments in their business continuity plans.

Physical desktops make disaster recovery a challenge at the protected site. Re-creating the physical desktop environment at the recovery site takes considerable time, and users must adjust to the new environment. Using VMware View to virtualize the desktops allows organizations to use VMware vCenter Site Recovery Manager (SRM) to handle both the server and the desktop environment business continuity plans.

Protecting the virtual desktop along with the infrastructure makes disaster recovery transparent to the end users and has less effect on the business. Being able to recover critical applications — and the virtual desktops that access them — means that user productivity can be restored quickly and revenue-generating activities are minimally affected.

---

### Product solution

Users like to have their desktop preferences and data available from any desktop or handheld device. System administrators want to keep that data secure and be able to effectively manage those critical production desktop pools. VMware View protected with SRM satisfies both needs and allows organizations to

- retain the “look and feel” (desktop personality) of their production virtual desktop in both the protected and recovery sites,
- provide a means to retain this same desktop experience, post-disaster and failover in the recovery site, and
- improve end-user productivity by speeding the time to recovery for critical applications and the virtual desktops that provide access.

VMware View Composer uses linked clone technology to reduce the storage needs for the VMware View deployment. This white paper highlights the challenges involved in disaster recovery of linked clone virtual desktops and what is done to overcome those issues.

---

### Key results

This white paper demonstrates a method for recovering VMware View Composer linked clone virtual desktops on the recovery site with custom scripts added to the SRM recovery steps. The environment described in this solution:

- saves time on the research of how to recover a VMware View environment,
  - demonstrates that the user settings and data are not altered, and
  - demonstrates recoverability of virtual desktops with User Data Disks (UDD) configured.
-

---

## Introduction

---

### **Purpose**

This white paper explores the ability to recover VMware View Composer-based linked clone virtual desktops at a remote site replicated with EMC® SRDF®/S and managed by VMware vCenter Site Recovery Manager.

---

### **Scope**

This white paper discusses the EMC Symmetrix VMAX Business Continuity Enabled by EMC SRDF/S and VMware vCenter Site Recovery Manager solution at a high level. It is assumed the reader familiar with

- VMware vSphere 4
  - VMware vCenter Server 4
  - VMware vCenter Site Recovery Manager 4
  - EMC Symmetrix VMAX™
  - EMC SRDF/S
- 

### **Audience**

This white paper is intended for EMC employees, partners, and customers including IT planners, virtualization architects and administrators, and any other IT professionals involved in evaluating, acquiring, managing, operating, or designing a private cloud environment leveraging EMC technologies.

---

---

## Key components

---

### Component overview

The following topics briefly describe the major components of the business continuity solution described in this white paper, including:

- EMC Symmetrix VMAX
- VMware vSphere 4 update 1
- VMware HA Cluster
- VMware View Connection Server
- VMware View Composer
- EMC SRDF/S
- VMware View Connection Replica Server
- VMware vCenter Site Recovery Manager
- EMC SRDF Adapter for VMware Site Recovery Manager

---

### Hardware from other vendors

This white paper uses Cisco UCS B200-M blade servers, and Cisco Nexus 2104, 6120, 7010, and MDS-9509 switches, but hardware from other vendors can be substituted.

---

### EMC Symmetrix VMAX

The solution described in this white paper uses EMC Symmetrix VMAX storage system to

- provide high-end, multi-dimensional storage, and
- allow connections to multiple storage networks using Fibre Channel and iSCSI protocols.

In this white paper, the VMware vSphere servers use Fibre Channel storage. This high-end system provides a standalone solution that can consolidate multiple applications across multiple ESX servers.

---

### VMware vSphere 4 update 1

VMware vSphere is a data center operating system that virtualizes the entire IT infrastructure. It enables the most scalable and efficient use of server hardware in a robust fault-tolerant environment. VMware ESX:

- Abstracts server processor, memory, storage, and networking resources into multiple virtual machines (VMs), forming the foundation of the VMware Infrastructure 4 suite.
- Partitions physical servers into multiple VMs. Each VM represents a complete system with processors, memory, networking, storage, and BIOS.
- Can share single server resources across multiple virtual machines, and cluster ESX servers for further sharing of resources.

---

**VMware HA Cluster**

VMware HA provides cost-effective high availability for any application running in a virtual machine, regardless of its operating system or underlying hardware configuration.

---

**VMware View Connection Server**

VMware View Connection Server manages secure access to virtual desktops and works with vCenter server to provide advanced management capabilities. It is sometimes referred to as a connection broker.

---

**VMware View Composer**

VMware View Composer reduces storage cost for the deployment of virtual desktops by using linked clone technology. It installs as a service on the vCenter server.

A *clone* is a copy of an existing virtual machine (VM). Installing the OS and applications on a VM can be time-consuming. With clones, you can make copies of a VM from one master image.

A *linked clone* is a copy of a VM that shares virtual disks with its parent VM. This saves disk space and allows multiple VMs to use the same software installation.

Linked cloning makes it easy to

- provision many VM images,
  - deploy patches and updates, and
  - restore VMs to their original state.
- 

**EMC SRDF/S**

SRDF/S is a synchronous remote replication solution for the EMC Symmetrix® family. It provides host-independent, real-time data replication across one or more physically separate target Symmetrix systems.

---

**VMware View Connection Replica Server**

The VMware View Connection Replica Server contains a replica of the View Directory database. Replica servers are used in conjunction with other network load-balancing technology to balance the broker connection traffic.

---

**VMware vCenter Site Recovery Manager**

VMware vCenter Site Recovery Manager (SRM) automates the recovery process and reduces the complexity of managing and testing recovery plans. VMware vCenter Site Recovery Manager eliminates complex manual recovery steps and removes the risk and worry from disaster recovery.

---

---

**EMC SRDF  
Adapter for  
VMware Site  
Recovery  
Manager**

EMC SRDF Adapter is a storage replication adapter that extends the disaster restart management functionality of VMware Site Recovery Manager to the EMC Symmetrix VMAX storage environment. It allows SRM to automate storage-based disaster restart operations on VMAX arrays in a SRDF/S configuration.

For additional information please refer to the white paper *Using EMC SRDF Adapter Version 2 for VMware Site Recovery Manager*.

---

**EMC Solutions  
Enabler**

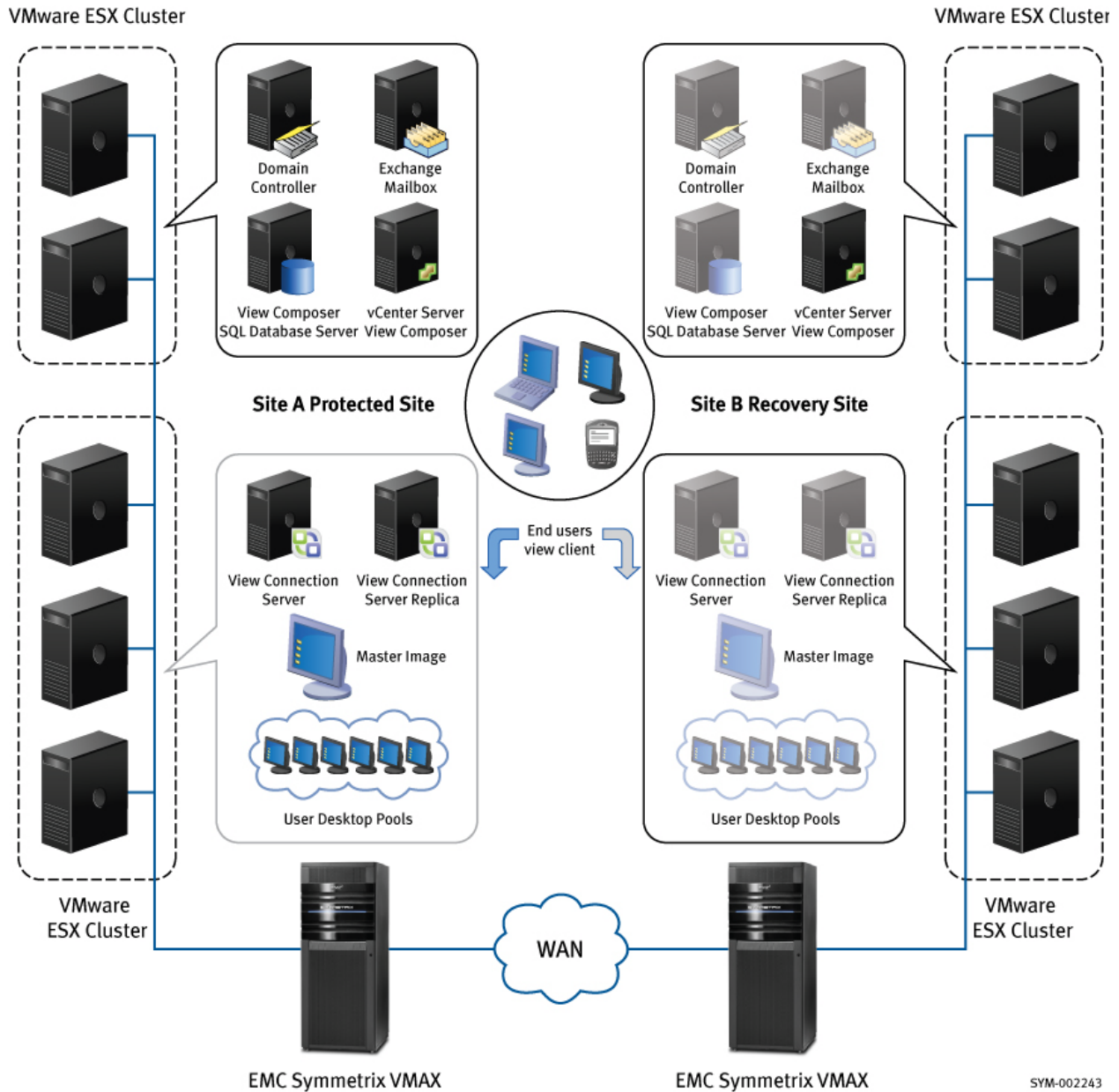
EMC Solutions Enabler contains all of the base management software that provides a host with SYMAPI-shared libraries and the basic Symmetrix command line interface SYMCLI.

---

## Physical architecture

### Architecture diagram

The following illustration depicts the overall physical architecture of the solution described in this white paper.



---

## Environment profile

---

### Hardware resources

The following table lists the hardware used in this white paper.

Equipment	Quantity	Configuration
Cisco UCS B200-M blade servers	5 x 2	<ul style="list-style-type: none"><li>• Dual-socket quad-core Intel Nehalem processors</li><li>• 48 GB RAM</li><li>• 2 QLogic CNA (10 Gb FCoE)</li></ul>
Cisco Nexus 2104	2 x 2	4 10Gb FCoE
Cisco Nexus 6120	1 x 2	20 10Gb Ethernet/FCoE and 8 1/2/4Gb FC ports
Cisco Nexus 7010	1 x 1	10Gb IP core
Cisco MDS 9509	1 x 2	6 24-port FC 1/2/4G blades
Symmetrix VMAX	1 x 2	FC connectivity, 450 GB/15k FC drives

---

### Virtual allocation of hardware resources

The following table lists the virtual allocation of hardware resources described in this solution. These are the virtual machine configurations.

Equipment	Quantity	Configuration
Domain Controller	2	2 vCPUs, 4 GB RAM, 1 vNIC, 30 GB VMDK
vCenter Server	1 x 2	2 vCPUs, 3 GB RAM, 1 vNIC, 30 GB VMDK
View SQL Server	1	2 vCPUs, 3 GB RAM, 1 vNIC, 20 GB VMDK
View Connection Server	1	2 vCPUs, 3 GB RAM, 2 vNICs, 20 GB VMDK
View Replica Server	1	2 vCPUs, 3 GB RAM, 1 vNIC, 20 GB VMDK
View Client	1	1 vCPU, 2 GB RAM, 1 vNIC, 20 GB VMDK
Virtual desktops	15	1 vCPU, 1 GB RAM, 1 vNIC, 20 GB (OS) +10 GB (UDD) VMDK

---

---

---

**Software resources**

The following table lists the software used in this solution.

<b>Software</b>	<b>Version</b>	<b>Configuration</b>
VMware vSphere	4 Update 1	Build 208167
VMware vCenter Server	4 Update 1	Build 208111
VMware View (with Composer)	4	
VMware vCenter Site Recovery Manager	4.0	Build 192921
VMware vSphere PowerCLI	4.0 Update 1	Build 208462
EMC SRDF Adapter for VMware Site Recovery Manager	2.1.0.7	
EMC Solutions Enabler	7.0.1	
EMC Symmetrix Management Console	7.1.15.0	
Microsoft Windows 2008	Enterprise Edition	64-bit
Microsoft Windows 2003	Enterprise Edition	32-bit
Microsoft Windows XP Professional	SP3	32-bit
Microsoft SQL Server 2005	SP2	
Microsoft PowerShell	1.0	
Quest ActiveRoles Management Shell for Active Directory	1.3.0	
PuTTY	0.60	

---

---

## Design and validation

---

### Design overview

The infrastructure for this solution is deployed in an EMC Virtual Information Infrastructure spanning two data center locations:

- Protected site – Site A
- Recovery site – Site B

Within the same data center, hosting is as follows:

- Infrastructure servers are hosted on a VMware high-availability (HA) cluster (see the section “Virtual allocation of hardware resources”).
- The VMFS datastores are created on a Symmetrix VMAX Fibre Channel array.
- In order to facilitate communication between vCenter and the storage array, a host must have direct access to the Symmetrix VMAX array through a gatekeeper device. In our case we’re using two separate vCenter servers, each with a single gatekeeper communicating with the VMAX arrays.

**Note** Gatekeepers must be presented to the host as a raw device or RDM in physical compatibility mode for Solutions Enabler to function properly.

- The data is replicated to another site using SRDF/S and managed by VMware vCenter Site Recovery Manager.

---

### Validation overview

The following is an overview of steps involved to validate business continuity of VMware View using SRM.

Step	Action
1	Set up the protected site virtual infrastructure environment
2	Deploy the View environment at the protected site
3	Verify virtual desktop operations
4	Set up the recovery site virtual infrastructure environment
5	Configure FC LUN replication between sites using Symmetrix Management Console (SMC)
6	Configure the protection group at the protected site
7	Configure the recovery plan with any custom scripts at the recovery site
8	Upon failover, execute the recovery plan
9	Verify the functionality at the recovery site

---

---

**Interoperability**

The VMware View Composer environment consists of:

- VMware View Connection Server
- VMware View Composer Service
- VMware View Agent
- VMware View client
- Desktop pools
- Base image

For a successful VMware View recovery, all of these components must be recovered properly.

---

**VMware View Connection Server**

VMware View clients connect to entitled virtual desktops through the VMware View Connection Server. This server hosts the ADAM database, which contains the configuration of VMware View.

To make the Connection Server available on the recovery site, the following must take place for the VM:

- the VMs are configured for protection in the SRM protection group,
- the IP addresses may be changed,
- DNS registration, and
- update of network load balancing (if used) in the recovery step.

Some modifications are required on the Microsoft ADAM database, which is detailed in the “Desktop pools” section. For more information on Microsoft ADAM refer to <http://www.microsoft.com/windowsserver2003/adam/default.mspx>.

---

**VMware View Composer Service**

VMware View Composer Service on the vCenter server

- uses an ODBC connection to a SQL database, and
- has SQL Server 2005 installed on a virtual machine that is configured to fail over.

VMware View Composer Service is also installed on the recovery site vCenter server and configured to use the same database

- having an ODBC with the same name, and
- having an RSA public-private key pair exported from SviKeyContainer from the protected site and imported into the recovery site.

---

**RSA key  
container  
migration**

Perform the following steps to migrate an RSA key container between systems:

Step	Action
1	<p>Export the RSA keys associated with the earlier instance of the View Composer from their local key container by entering the following from a command line on the source system:</p> <pre>Aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri</pre> <p>The RSA public-private key pair is exported from SviKeyContainer to a file called keys.xml that is saved locally to the ASP.NET IIS registry.</p>
2	<p>Copy the keys.xml file to the system on which you want to install a new of the View Composer Service.</p>
3	<p>Import the key pair data into the local key container by entering the following from the command prompt on the target system, where &lt;path&gt; is the path to the exported file:</p> <pre>Aspnet_regiis -pi "SviKeyContainer" "&lt;path&gt;\keys.xml"</pre>

A DNS alias is created for the active vCenter server that has access to the View SQL database. VMware View Connection Manager is configured to use this DNS alias for the vCenter server. Additionally both vCenter servers should have the same username and password.

Each site will have its own vCenter server that hosts the View Composer Service. During failover of the SQL database server:

- The IP of the server is changed and registered on DNS.
- The vCenter alias is updated to point to the recovery site vCenter.

Some modifications are required on the SQL database that are detailed in the "Desktop pools" section.

---

The following figure shows the VirtualCenter configuration settings.

**VirtualCenter Settings** \* Required

Server address:  \*

User name:  \*

Password:  \*

Description:

Connect using SSL

Port:

[Basic <<](#)

Specify the virtual machine behavior for desktops that use this VirtualCenter Server.

Maximum number of concurrent provisioning operations:

Maximum number of concurrent power operations:

---

**VMware View Agent**

View Agent is installed on the base image that interacts with VMware View Connection Server. No special steps are needed for recovery.

---

**VMware View Client**

The VMware View Client is an application that is used to launch the virtual desktops hosted on VMware View.

This application is installed on the end-user devices. It must be installed and connected to the recovery site. Users also have the option to access using a web browser pointing to the active View Connection Server.

---

## Desktop pools

Desktop pools are collections of virtual machines that have the desktop OS installed on them.

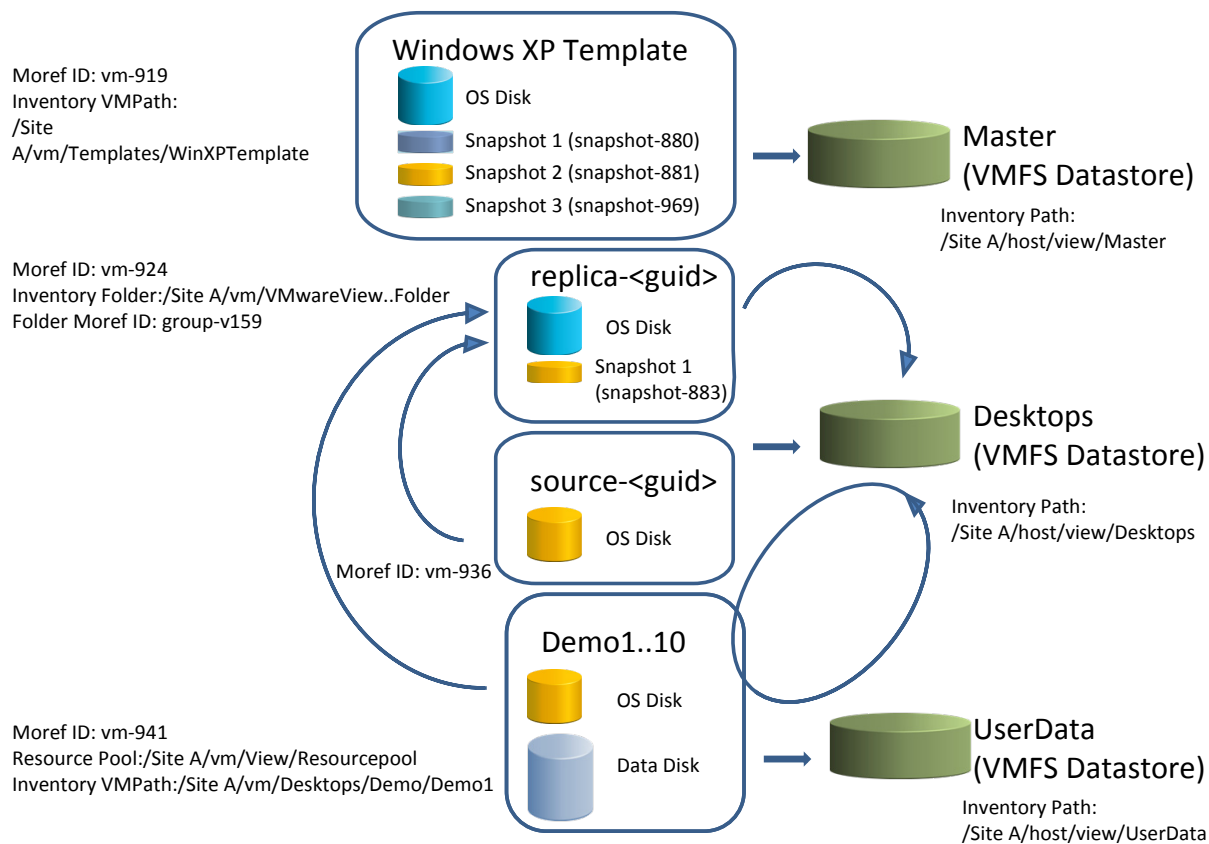
When a linked clone desktop pool is created from the base image

- the OS disk and its snapshot are copied to the replica folder on every datastore that is selected to deploy,
- a new snapshot is created and presented as an OS disk to the source VM, and
- the source VM is cloned to create additional virtual desktops.

The following figure shows all the virtual desktops pointing to the replica OS disk as the parent.

**Note** The term Moref ID refers to the management object reference identifier (also referred to as the MOID).

## VMware Linked Clone on Site A



The following figure is a sample file output showing the hardcoded datastore ID.

```
[root@esxc Lab5]# cat replica-c984ecc3-92cc-424b-96ed--cl1.vmdk
# Disk DescriptorFile
version=1
CID=809888fb
parentCID=75a502c7
createType="vmfsSparse"
parentFileNameHint="/vmfs/volumes/4a53e8ca-44bffa94-55ff-001b211f4358/replica-c984ecc3-92cc-424b-96ed-/replica-c984ecc3-92cc-424b-96ed-.vmdk"
# Extent description
RW 41943040 VMFSSPARSE "replica-c984ecc3-92cc-424b-96ed--cl1-delta.vmdk"

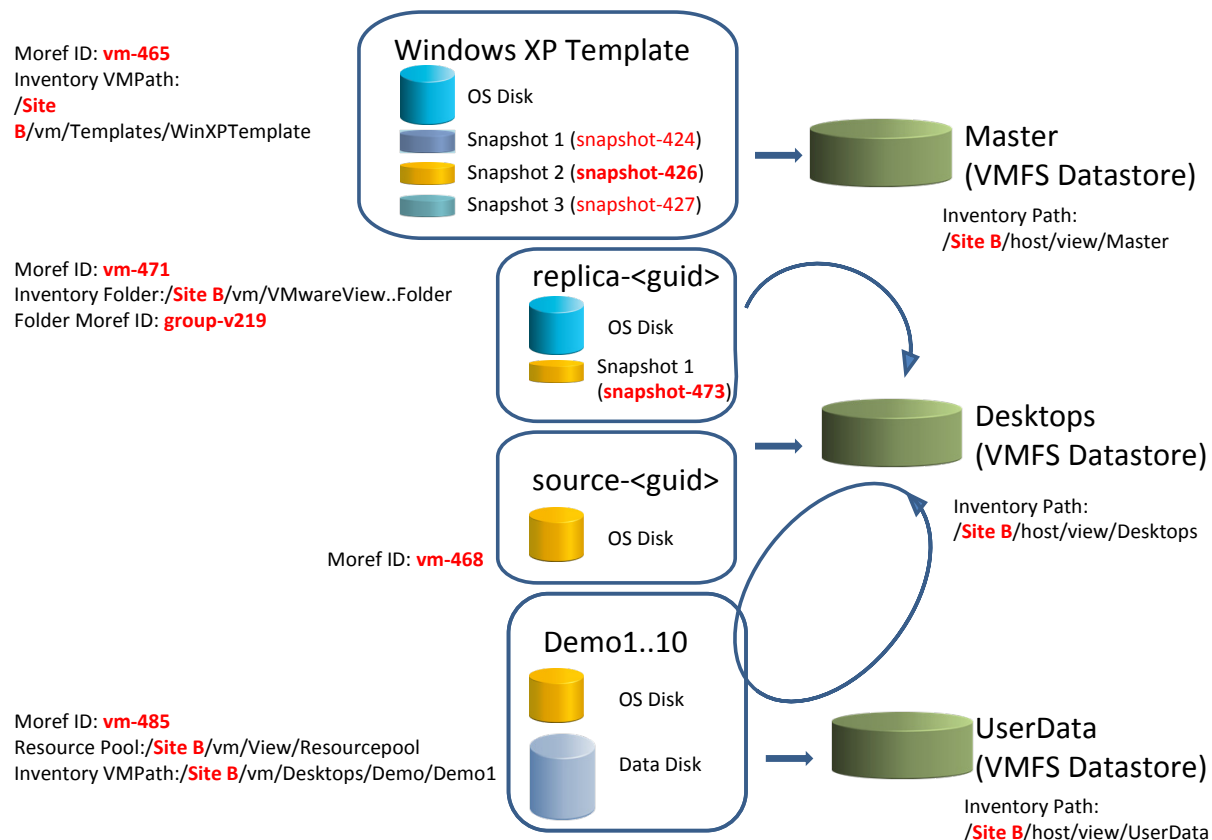
# The Disk Data Base
#DDB

ddb.toolsVersion = "7303"
```

When the recovery plan is executed, that link is broken because the virtual machine cannot access the datastore with that ID and it fails to power on with the message “file not found”. Updating the file to point to the valid path makes the virtual machines power on successfully.

The statuses of the linked clone desktops are shown in the following figure.

### VMware Linked Clone on Site B



Note that because the objects are managed by different vCenter servers, the Moref ID (MOID) is changed between the vCenter servers. This makes the virtual desktops not accessible from the View Client because the ADAM database and SQL database reference that information.

The following two figures show the ADAM and View SQL database changes.

## ADAM Changes

### Pae-serverpool object

Pae-SVIVmDatastore

Pae-SVIVmParentVM

Pae-SVIVmSnapshotMOID

Pae-VmDatastore

Pae-VmPath

Pae-VmResourcepool

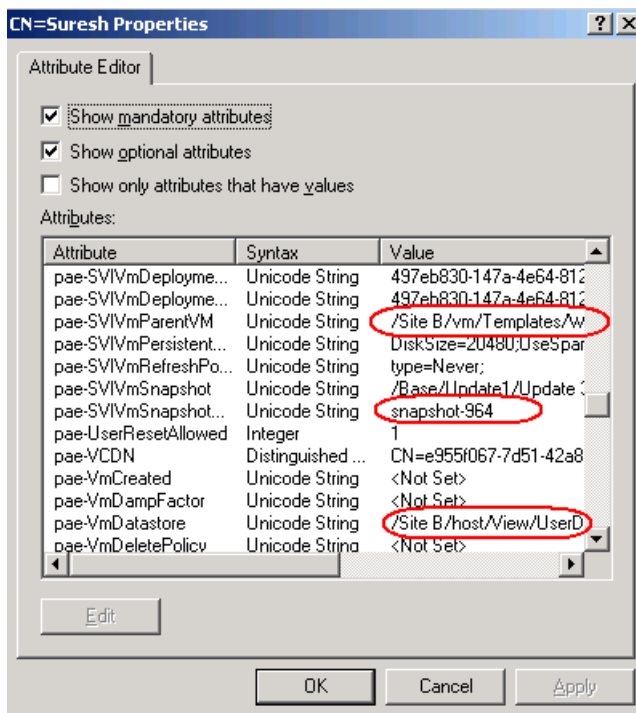
### Pae-VM object

Pae-MOID

Pae-SVIVmSnapshotMOID

Pae-VmPath

Pae-SVIVmParentVM



## View SQL DB Changes

### SVI\_REPLICA

REPLICA_MOID
REPLICA_SS_MOID
FOLDER_MOID
SOURCE_LC_MOID

### SVI\_SIM\_CLONE

SIM_CLONE_MOID
GOLDEN_MASTER_VM_MOID
GOLDEN_MASTER_VM_SS_MOID

### SVI\_DEPLOYMENT\_GROUP

VM_MO_REF
VM_SS_MO_REF

ID	SIM_CLONE...	DEPLOYMENT...	STATE	VM_NAME	GUEST...	REPLICA_ID	GOLD...	GOLDEN_MAST...	LAST_SYNC_TIME	AD_CONFIG_ID	CONTAINER_P...	P...	P...	GOS_POLICY...	VM_UUID
29878...	vm-1203	497eb830-147a...	0	Suresh3	Suresh3	a50b11ee-b9f4...	vm-878	snapshot-964	7/27/2009 8:28:...	3fd83117-611d...	CN=Computers			1087188372	50146fb1-6b65...
332e1...	vm-980	1d7eb819-021b...	0	Lab8	Lab8	a50b11ee-b9f4...	vm-878	snapshot-964	7/22/2009 3:26:...	3fd83117-611d...	CN=Computers			1087188372	50145415-6cc9...
46495...	vm-941	9e87743f-e03a...	0	WinXP3	WinXP3	6db4a00f-c553...	vm-878	snapshot-881	7/27/2009 7:45:...	3fd83117-611d...	CN=Computers			1087188372	5014d12c-0df4...
48d89...	vm-984	1d7eb819-021b...	0	Lab10	Lab10	a50b11ee-b9f4...	vm-878	snapshot-964	7/22/2009 3:27:...	3fd83117-611d...	CN=Computers			1087188372	5014304b-f15c...
4a043...	vm-945	9e87743f-e03a...	0	WinXP4	WinXP4	6db4a00f-c553...	vm-878	snapshot-881	7/27/2009 7:45:...	3fd83117-611d...	CN=Computers			1087188372	501467a5-7ad4...
50f80...	vm-972	1d7eb819-021b...	0	Lab1	Lab1	a50b11ee-b9f4...	vm-878	snapshot-964	7/22/2009 3:22:...	3fd83117-611d...	CN=Computers			1087188372	50143c07-4373...
53e38...	vm-974	1d7eb819-021b...	0	Lab4	Lab4	a50b11ee-b9f4...	vm-878	snapshot-964	7/22/2009 3:24:...	3fd83117-611d...	CN=Computers			1087188372	5014c6b7-d3c3...
6d170...	vm-921	1d7eb819-021b...	0	Lab5	Lab5	a50b11ee-b9f4...	vm-878	snapshot-964	7/22/2009 3:22:...	3fd83117-611d...	CN=Computers			1087188372	5020be0c-d204...
71dfe...	vm-976	1d7eb819-021b...	0	Lab6	Lab6	a50b11ee-b9f4...	vm-878	snapshot-964	7/22/2009 3:24:...	3fd83117-611d...	CN=Computers			1087188372	5014d993-d8e0...
7eb1c...	vm-943	9e87743f-e03a...	0	WinXP5	WinXP5	6db4a00f-c553...	vm-878	snapshot-881	7/27/2009 7:45:...	3fd83117-611d...	CN=Computers			1087188372	50149fb1-6904...
96019...	vm-939	9e87743f-e03a...	0	WinXP2	WinXP2	6db4a00f-c553...	vm-878	snapshot-881	7/27/2009 7:45:...	3fd83117-611d...	CN=Computers			1087188372	50146145-5327...
971ad...	vm-937	9e87743f-e03a...	0	WinXP1	WinXP1	6db4a00f-c553...	vm-878	snapshot-881	7/27/2009 7:45:...	3fd83117-611d...	CN=Computers			1087188372	5014b336-cbe6...
9ce90...	vm-906	1d7eb819-021b...	0	Lab2	Lab2	a50b11ee-b9f4...	vm-878	snapshot-964	7/22/2009 3:22:...	3fd83117-611d...	CN=Computers			1087188372	502082e3-52e1...
a2338...	vm-982	1d7eb819-021b...	0	Lab9	Lab9	a50b11ee-b9f4...	vm-878	snapshot-964	7/22/2009 3:26:...	3fd83117-611d...	CN=Computers			1087188372	50140dc8-d83b...
bd6a9...	vm-1207	497eb830-147a...	0	Suresh5	Suresh5	a50b11ee-b9f4...	vm-878	snapshot-964	7/27/2009 8:30:...	3fd83117-611d...	CN=Computers			1087188372	5014aede-9817...
cdf70...	vm-1205	497eb830-147a...	0	Suresh4	Suresh4	a50b11ee-b9f4...	vm-878	snapshot-964	7/27/2009 8:29:...	3fd83117-611d...	CN=Computers			1087188372	50148fa3-1c7d...
ce62b...	vm-1199	497eb830-147a...	0	Suresh2	Suresh2	a50b11ee-b9f4...	vm-878	snapshot-964	7/27/2009 8:26:...	3fd83117-611d...	CN=Computers			1087188372	5014b20e-b233...
e926d...	vm-978	1d7eb819-021b...	0	Lab7	Lab7	a50b11ee-b9f4...	vm-878	snapshot-964	7/22/2009 3:25:...	3fd83117-611d...	CN=Computers			1087188372	5014906d-479b...
f4945...	vm-986	1d7eb819-021b...	0	Lab3	Lab3	a50b11ee-b9f4...	vm-878	snapshot-964	7/22/2009 3:59:...	3fd83117-611d...	CN=Computers			1087188372	501439d9-bc19...
f93ba...	vm-1201	497eb830-147a...	0	Suresh1	Suresh1	a50b11ee-b9f4...	vm-878	snapshot-964	7/27/2009 8:27:...	3fd83117-611d...	CN=Computers			1087188372	501487e6-d029...
*	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	N...	N...	NULL	NULL

After making the changes to the ADAM and SQL databases so they reference the current vCenter MOIDs, the virtual desktops are able to be accessed and look the same as in the protected site. Administration of VMware View also remains the same.

---

---

**Functionality** For this solution, the following actions were taken:

Step	Action
1	We created a protected site environment with <ul style="list-style-type: none"><li>• an automated desktop pool having virtual desktops, and</li><li>• the virtual desktops had the linked clone and user data disk hosted on a separate datastore.</li></ul>
2	The users connect to their virtual desktops to <ul style="list-style-type: none"><li>• create files and folders on the desktop and My Documents, and</li><li>• log in to Outlook to send and receive e-mail as usual.</li></ul>
3	The SRM recovery plan was executed, with custom scripts added to the recovery steps to <ul style="list-style-type: none"><li>• update the IP address of the virtual machines,</li><li>• register on DNS,</li><li>• run a comand line script to change the path of VMDK files, and</li><li>• update the ADAM and the Composer SQL databases with information collected on the recovery site vCenter server.</li></ul>
4	The users connect to their virtual desktops without any modification to their normal procedure and <ul style="list-style-type: none"><li>• access and update the files and folders created on the protected site, and</li><li>• log in to Outlook to retrieve the e-mails and reply to those e-mails.</li></ul>
5	View administrators are able to recompose, refresh, and deploy new pools.

---

**Failback** The failback process is performed manually and is the same as for the failover, except the operations are performed on the opposite site. The steps that were taken on Site A during failover are now taken on Site B for failback.

---

**Performance** For this specific configuration, the entire recovery took approximately 30 minutes for 15 virtual desktops. The script's updating of the ADAM and View SQL databases took less than 3 minutes.

Note that actual operation times will vary depending on your specific environment. The number of LUNs, desktop pools, and virtual machines all affect the operation time.

---

---

## Conclusion

---

### Summary

This white paper demonstrates that there is a method for recovering VMware linked clone virtual desktops on the recovery site with custom scripts added to the SRM recovery steps. This method of virtual desktop recovery provides a rapid, reliable, and cost-effective solution that replaces tedious error-prone manual steps with automated processes that reduce recovery time from hours, even days, to minutes.

---

### Key points

The table below summarizes the key points that this solution addresses.

Key Point	Solution objective
Recovery of desktop pools and images	<ul style="list-style-type: none"><li>• With no database changes, we are still able to deploy new desktop pools.</li><li>• With ADAM changes, we are able to recompose the image on protected site pools.</li><li>• With ADAM and View SQL DB changes, we are able to recompose, and refresh the image on protected site pools.</li></ul>
Environment validation	<p>In this solution, the recovery of 15 virtual desktops was validated within a 30-minute timeframe. (The recovery time depends on the size of the deployment.)</p> <p>The solution is also applicable in cases where the vCenter server needs to be replaced for the VMware View environment.</p>
Solution benefits	<ul style="list-style-type: none"><li>• Saves time on the research of how to recover a VMware View environment.</li><li>• Demonstrates that the user settings and data are not altered.</li><li>• Demonstrates recoverability of virtual desktops with User Data Disks (UDD) configured.</li></ul>

---

---

## References

---

### Other documentation

The following resources may also be useful in understanding and evaluating this solution:

- *Site Recovery Manager Evaluator Guide:*  
[http://www.vmware.com/pdf/srm\\_10\\_eval\\_guide.pdf](http://www.vmware.com/pdf/srm_10_eval_guide.pdf)
  - *VMware vCenter Site Recovery Manager Performance and Best Practices:*  
<http://www.vmware.com/resources/techresources/10057>
  - *Automating Network Setting Changes and DNS Updates on Recovery Site Using VMware vCenter Site Recovery Manager:*  
<http://viops.vmware.com/home/docs/DOC-1491>
  - *VMware View Composer — Advanced Image Management and Storage Optimization for your VMware View Environment:*  
<http://www.vmware.com/files/pdf/VMware-View-4-Composer-DS-EN.pdf>
  - *Using EMC SRDF Adapter Version 2 for VMware Site Recovery Manager — Best Practices Planning:*  
<http://www.emc.com/collateral/software/white-papers/h6368-using-emc-srdf-adapter-v2-vmware-srm-wp.pdf>
  - Windows Server 2003 Active Directory Application Mode Microsoft (ADAM) page on Microsoft's website:  
<http://www.microsoft.com/windowsserver2003/adam/default.mspx>
-