VMware® View™
Infrastructure Resiliency

VMware View 5 and VMware vCenter™ Site Recovery Manager™

WHITE PAPER
# Table of Contents

Introduction ................................................................. 3  
Target Audience ............................................................ 3  
Architectural Overview .................................................... 4  
  Management Block ....................................................... 5  
  Desktop Block ............................................................ 6  
Creating a Disaster Recovery Solution for VMware View .................... 6  
Logical Architecture Overview ........................................... 7  
Failover Procedure for Floating Linked Clone Desktops ...................... 9  
  Scenario-Specific Requirements ...................................... 9  
  Recovery Steps for Floating Linked Clone Desktops ................. 10  
  View Desktop Block Recovery Steps ................................ 11  
  Update Base Image and Pool Configuration .......................... 11  
  Scenario Summary ..................................................... 11  
Failover Procedure for Persistent Linked Clone Desktops .................. 11  
  Scenario-Specific Requirements ...................................... 12  
  Recovery Steps for Persistent Linked Clone Desktops .............. 12  
  View Desktop Block Recovery Steps ................................ 12  
  Scenario Summary ..................................................... 13  
Failover of Persistent Linked Clone Desktops with Persistent Disks ....... 13  
  Scenario-Specific Requirements ...................................... 13  
  Recovery Steps for Persistent Linked Clone Desktops with Persistent Disks .... 14  
  Scenario Summary ..................................................... 14  
Conclusion ........................................................................ 14  
About the Authors ............................................................ 15
Introduction

VMware® View™ offers a personalized, device-neutral, end-user computing experience with increased security and control. It enables agile desktop solutions that quickly meet changing business needs and proactively protect against planned and unplanned downtime.

This case study provides insight and information on how to increase availability and recoverability of a View infrastructure using VMware vCenter™ Site Recovery Manager™ (SRM) and common disaster recovery (DR) tools and methodologies. vCenter SRM automates the failover process of the VMware View management environment to enable fast, reliable recovery and meet specific Recovery Time Objectives (RTO).

The architecture described here is an active/passive design, in which the entire View infrastructure operates within one datacenter until the failover scenario is invoked. This solution does not satisfy every use case or requirement for virtual desktop disaster recovery. Total Cost of Ownership (TCO) and Return on Investment (ROI), for example, were not evaluated during testing and implementation. However, this study does demonstrate a successfully tested DR solution for a View infrastructure that is easy to implement and support. Among the environments that can benefit from this solution are those that already include SRM and those where a virtual desktop use case has a definitive DR requirement.

Other solutions are possible for DR with VMware View, but they may be more complicated and less reliable. Although vCenter SRM is required for this specific solution, it is not a requirement for VMware View disaster recovery in general.

Target Audience

This document is intended for readers with a technical background who plan to design, deploy, or manage a VMware View infrastructure—technical consultants, infrastructure architects, IT managers, implementation engineers, partner engineers, sales engineers, and customer staff. It does not replace or override existing, certified designs for VMware View, but it is meant to provide additional information about implementing a DR strategy.

The solution presented here addresses specific requirements. It assumes that the reader is familiar with VMware View, VMware vCenter Server™, vCenter Site Recovery Manager, and VMware vSphere® reference architectures, technology, and terminology.
VMware View should always be deployed according to VMware View architecture and deployment best practices. To facilitate your disaster recovery plan, deploy VMware View in conformance with the View pod and block design described in VMware View Architecture Planning.

The View architecture consists of a management block and a desktop block.

- The management block contains the infrastructure components required to operate and manage VMware View, including the View Connection Servers and one or more vCenter Server instances used to provision View desktops.

- The desktop block (desktop vSphere cluster) represents dedicated resources for hosting the desktops. Each vSphere cluster consists of a set of VMware ESXi hosts managed by the View vCenter Server and dedicated to hosting VMware View virtual desktops.
Management Block

The management block hosts all the necessary VMware View infrastructure components. In this scenario, the management block contains at least the following virtual machines:

- Two vCenter Servers
  - One vCenter Server for management
  - One vCenter Server for desktop resources
- One database server hosting VMware View and vCenter Server databases
- One VMware View Connection Server

The management vCenter Server runs as a virtual machine in the vSphere cluster it is managing, as indicated by the blue arrow in Figure 2.

![Figure 2. Management Block](image-url)
Desktop Block

A vSphere resource cluster is a set of resources dedicated to end-user workloads and managed by a single vCenter Server. VMware View controls all the desktop vSphere clusters and the virtual desktops running within them. This logical grouping is called a desktop block.

As shown in Figure 3, a desktop block contains only virtual desktops instantiated by VMware View. The vCenter Server instance that manages this environment resides within the management block and is not depicted in this figure but is shown in Figure 1.

Creating a Disaster Recovery Solution for VMware View

VMware vCenter Site Recovery Manager 5.1 and earlier versions do not include native support for the protection of VMware View. To facilitate disaster recovery of a VMware View environment, the solution proposed here uses

- Standard DR concepts to leverage standard replication technologies and vSphere features for VMware View virtual desktops
- vCenter SRM to orchestrate failover of the VMware View management infrastructure

vCenter SRM is designed to manage rapid failover of virtual machines to the recovery site by controlling the destination vCenter Server. To control failover of one vSphere environment to another, SRM requires vCenter objects, such as resource pools, folders, and port groups, to be pre-created on the destination site. These objects have unique identifiers that make it difficult for VMware View to understand the changes on the vSphere layer.

When replication stops during failover, standard procedure is to have SRM resignature the datastores and present the replicated volume to the hosts in the recovery site. This is a common DR best practice. Resignaturing provides the recovery volume with a unique ID to avoid the possibility of two volumes with the same unique ID being presented to the same host. However, resignaturing a datastore requires all virtual machines within the vCenter to re-register. The proposed solution therefore requires that volumes not be resignatured. In this way, it avoids changes to any of the vCenter objects. This, in turn, simplifies the recovery of the View infrastructure and increases the resiliency of the management infrastructure.
Logical Architecture Overview

VMware View disaster recovery can be implemented with various scenarios and configurations. This case study focuses on three scenarios that cover the most commonly deployed architectures.

1. Floating linked clone desktop pool – Floating linked clones are used when there is no requirement for a relationship between the user and the desktop. In effect, the desktop becomes disposable—the user is issued a fresh desktop instance at each login—and any persistent data is saved outside the desktop (on the H drive). This use case is best suited for environments that already contain SRM and require a DR solution that is easy to build and implement. (See Failover Procedure for Floating Linked Clone Desktops.)

2. Persistent linked clone desktop pool – This type of pool provides a convenient way to deploy and refresh linked clone desktops when applications or users require OS persistency. There is a mapping between the user and the desktop. (See Failover Procedure for Persistent Linked Clone Desktops.)

3. Persistent linked clone desktops with persistent disks pool – This type of pool also provides user-to-desktop mapping, but any persistency in this case is kept on the persistent disk, not on the OS disk. (See Failover of Persistent Linked Clone Desktops with Persistent Disks.)

These scenarios all rely on the same architecture for the VMware View management environment and use SRM to orchestrate the failover by restarting management components in the correct order and in the shortest time. Each site must contain a management vCenter server and an SRM server, as shown in Figure 4.

![Diagram showing the logical architecture overview](image-url)
The full VMware Infrastructure™ architecture used for this case study is depicted in Figure 5.

The protected and recovery sites each have a management block with a vCenter Server and an SRM server. This arrangement facilitates the DR procedures for the other components in the management block by including them in an SRM protection group. When you create an SRM recovery plan, you can make the virtual machines in this protected group fail over to the recovery site. For more information on the creation of recovery plans, protection groups, and SRM configuration, see the VMware vCenter Site Recovery Manager documentation.

In this environment, storage is replicated, not stretched, so hosts in the desktop vSphere cluster at the recovery site cannot see the storage at the protected site or run VMware View workloads in a normal—that is, a non-disaster, non-failover—situation.
The recovery site is not required to have the same number of hosts as the protected site, and it may contain fewer, depending on the resources available. Also, it is possible to add standalone hosts to the View desktop vSphere cluster during failover.

Logical unit numbers (LUNs) are replicated from the protected site to the recovery site with storage replication technology. You can choose asynchronous or synchronous replication. This choice typically depends on the Recovery Point Objective (RPO) determined in the Service Level Agreement (SLA) and the distance between the protected site and the recovery site. This case study uses synchronous replication.

SRM uses a Storage Replication Adapter (SRA) to manage the LUNs and datastores that host the VMware View management infrastructure. With an SRA, you can fully automate and orchestrate a failover for the VMware View management infrastructure. However, SRM does not support the LUNs or datastores where the View desktops are running, so manual steps may be required during the failover. Depending on the type of storage used, it may be possible to automate these steps with storage system API calls.

**Failover Procedure for Floating Linked Clone Desktops**

This section describes the steps required for a successful failover of a VMware View floating linked clone desktop environment. In this scenario, the Layer-2 segment is not stretched, and the IP addresses of the Infrastructure change in the recovery site.

It is essential that each component of the VMware View management stack be started in the correct order (see Recovery Steps for Floating Linked Clone Desktops), which you can configure in an SRM recovery plan and initiate with a single SRM button.

To minimize the number of recovery steps needed, storage replication is required only for the base image virtual machine. All other components are rebuilt. With a floating pool, users can log in to any machine after recovery and, with the infrastructure servers managed by SRM, recovery is automated. This arrangement allows one pool to “virtually” exist in two datacenters during failover scenarios. After recovery, however, the pool must be updated with the recovery site’s network and storage configurations.

**Scenario-Specific Requirements**

This scenario has the following specific requirements:

<table>
<thead>
<tr>
<th>REQUIREMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNAME/FQDN</td>
<td>All View components must be configured to use CNAME/FQDN rather than IP addresses to minimize the reconfiguration footprint when failover occurs.</td>
</tr>
<tr>
<td>Linked Mode</td>
<td>Linked mode must be disabled because an IP change on the vCenter adversely affects the linked mode ADAM database.</td>
</tr>
<tr>
<td>Networking</td>
<td>DHCP must be configured in both datacenters to allow for a minimum number of failover steps.</td>
</tr>
<tr>
<td>Virtual IP</td>
<td>Users should connect to the View connection servers with a Virtual IP, not directly to the connection server.</td>
</tr>
<tr>
<td>Data Replication</td>
<td>The base Image virtual machine must be replicated to the recovery datacenter.</td>
</tr>
</tbody>
</table>

Table 1. Floating Linked Clone Desktop Environment
**Recovery Steps for Floating Linked Clone Desktops**

These procedures represent a combination of steps performed through the Site Recovery Manager workflow and manual steps. The use of manual wait steps between the different priorities may be necessary. This practice is highly recommended. Even with manual steps, some servers may require rebooting to reconnect to dependent machines, as in the case of vCenter Server.

1. Power on SQL Server (Priority 1 group).
2. SRM updates IP address.
   a. Update DNS (Dynamic?), Validate IP Address and DNS change.
   b. Validate.
3. Power on vCenter (Priority 2 group).
   You cannot update IP addresses with SRM on a vCenter Server. Use the following manual steps to reset the IP address of the Desktop vCenter Server:
   a. Remove the NIC from vCenter.
   b. Power on the vCenter virtual machine.
   c. Change all vCenter and Composer services to Manual.
   d. Add the NIC to the vCenter virtual hardware.
   e. Configure static IP in Windows.
   f. Reboot vCenter.
   g. Validate.
   h. (OPTIONAL) Set services back to Automatic.
   i. Update DNS, Validate IP Address and DNS Change.
4. Power on VMware View Manager™ (Priority 2 group).
5. SRM updates IP address.
   a. Validate IP and DNS changes and connectivity.
   b. Check vCenter connection.
   This connection should use a Fully Qualified Domain Name (FQDN).
   c. Verify that View Composer setup is still enabled in View Manager server settings.
   d. Validate.
6. Update CNAME for NFS.
   (Step in SRM workflow for a manual step and pause.)
7. Switch over replicated LUN(s) backing the View block to READ/WRITE.
8. Connect to vSphere and View Manager to verify connectivity to View components.
   The status of View desktops displays as “Missing” in the View Manager console.
9. Mount the replicated View LUN(s) from the standby hosts in the View desktop block from the command line on all ESXi hosts.
   
   ```bash
   esxcfg-volume --m <volume ID or vmfs name>
   ```
10. (OPTIONAL) List all current volumes.
    ```bash
        esxcfg-volume --l
    ```
    If this command does not provide any output, perform a rescan to attach the replicated volumes.
At this point, the Site Recovery Manager and manual DR steps are completed, and all IP addresses for the management virtual machines are changed. The View pool is now accessible and manageable.

Before updating the base image and pool configuration, verify that the hosts and datastores are online and available.

**View Desktop Block Recovery Steps**

Assuming the failover hosts have been in maintenance mode, they need to be taken out of maintenance mode before provisioning can be enabled in any pools.

1. Take recovery datacenter hosts out of maintenance mode.
2. Verify that datastores are online and have the necessary disk space available.
3. Check the base image virtual machine(s) on replicated View LUN(s).

**Update Base Image and Pool Configuration**

Take the following steps to update the base image and the desktop pool:

1. Verify that Virtual IP points to the new IP address of the connection servers.
2. Edit the base image virtual hardware.
   a. Update virtual NIC to reflect the recovery datacenter port group.
   b. Validate.
   c. (OPTIONAL) Power on the base image to validate the NIC driver.
3. Take new snapshot of the base image.
4. Update the pool configuration.
   a. Change the base image snapshot.
   b. Update the datastore configuration to recovery site datastores.
   c. Enable pool and provisioning.
   d. Validate.

**Scenario Summary**

Some automation considerations still need to be addressed, particularly with the base image and pool configurations. With PowerShell (and PowerCLI) scripts, these steps can be completely automated to reduce the number of steps in a failover scenario. This study uses manual steps to validate each individual step.

**Failover Procedure for Persistent Linked Clone Desktops**

This section describes the steps required for a successful failover of a VMware View persistent linked clone desktop environment. This scenario is based on the assumption that a stretched, Layer-2 network is available and that there are no requirements for changing IP addresses on any of the components.
Scenario-Specific Requirements
Specific requirements for this scenario are listed in Table 2.

<table>
<thead>
<tr>
<th>REQUIREMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNAME/FQDN</td>
<td>Use CNAME/FQDN instead of IP address to simplify management and troubleshooting.</td>
</tr>
<tr>
<td>Networking</td>
<td>DHCP must be configured in both datacenters to allow for a minimum number of failover steps.</td>
</tr>
<tr>
<td>Data Replication</td>
<td>Both persistent disks and base image virtual machines must be replicated to the recovery datacenter.</td>
</tr>
</tbody>
</table>

Table 2. Persistent Linked Clone Desktop Environment

Recovery Steps for Persistent Linked Clone Desktops
Each component of the View management stack must be started in the correct order. You can configure the order in which the components should be started in an SRM recovery plan and initiate the plan a single SRM button. The following order was used to power on the VMware View management virtual machines:

1. Database Server providing VMware View and vCenter Server Databases
2. Desktop vCenter Server
3. VMware View

After the failover of the View management virtual machines in the management block succeeds, the View persistent linked clone desktops can be failed over. You can describe the necessary steps manually or automate them using PowerCLI or VMware vCenter Orchestrator™.

View Desktop Block Recovery Steps
Failing over the linked clone mechanism used by persistent desktops can be complicated because of the on-disk structure and associated unique identifiers. You can use the following steps to avoid having to alter identifiers and database entries manually.

1. Verify that all VMware View management virtual machines are powered on.
2. Using your storage management utility, break replication for the datastores connected to the View desktop block, and set the datastores to READ/WRITE, if required by storage platform.
3. Mask the datastores to the recovery site, if required by storage platform.
4. Using ESXi command line tools, mount the volumes of the VMware View desktop block on each host in the vSphere cluster:
   ```bash
   esxcfg-volume -m <volume ID>
   ```
5. Using vCenter Server for the VMware View desktop block, rescan the storage, and verify that all volumes are available.
6. Either take the hosts out of maintenance mode for the VMware View desktop block, or add the hosts to your vSphere cluster, depending on the chosen strategy.

In this study, the virtual desktops were automatically powered on by VMware vSphere High Availability (HA). vSphere HA is aware of a disaster situation before the failover and powers on the virtual machines according to the last known state stored on the mounted datastores.
Scenario Summary
At this point, the failover of the VMware View environment, including the virtual desktops, has been successfully completed. All View management components are virtualized, so the virtual machines are moved over to the recovery site with all currently managed unique identifiers maintained. Leveraging the standard vSphere CLI to avoid the need to re-register all the virtual machines eliminates the need to resignature the datastore.

Failover of Persistent Linked Clone Desktops with Persistent Disks
This section describes the steps required for a successful failover of a VMware View persistent linked clone desktop environment with persistent disks. This scenario is based on the assumption that the Layer-2 segment is not stretched and that IP addresses of the Infrastructure will change in the recovery site.

In this scenario, persistent disks maintain user data and profiles. Replicating the persistent disks to the secondary site provides a cost saving by not replicating the linked clones. The only items replicated from the primary site to the recovery site are the base image virtual machine and the persistent disks.

The failover steps are almost identical to those for the floating desktop scenario, except that where floating desktops require only the base image be replicated to the recovery site, this scenario also requires that the persistent disks be replicated. There are a few manual steps that must be performed to enable the persistent disks.

Scenario-Specific Requirements
In addition to the general solution requirements previously identified, this scenario also has the following specific requirements:

<table>
<thead>
<tr>
<th>REQUIREMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNAME/FQDN</td>
<td>All View components must be configured to use CNAME/FQDN rather than IP addresses to minimize reconfiguration footprint when failover occurs.</td>
</tr>
<tr>
<td>Linked Mode</td>
<td>Linked mode must be disabled because an IP change on the vCenter adversely affects the linked mode ADAM database.</td>
</tr>
<tr>
<td>Networking</td>
<td>DHCP must be configured in both datacenters to allow for a minimum number of failover steps.</td>
</tr>
<tr>
<td>Virtual IP</td>
<td>Users should connect to the View connection servers with a Virtual IP, not directly to the connection server.</td>
</tr>
<tr>
<td>Data Replication</td>
<td>Both persistent disks and base image virtual machines must be replicated to the recovery datacenter.</td>
</tr>
</tbody>
</table>

Table 3. Persistent Linked Clone Desktop Environment with Persistent Disks
Recovery Steps for Persistent Linked Clone Desktops with Persistent Disks
The initial recovery steps are the same as those listed in Recovery Steps for Floating Linked Clone Desktops. In addition, use the following steps for pool and disk configuration:

**Update Base Image and Pool Configuration**
1. Verify that the virtual IP address points to the IP address of the connection servers.
2. Edit the base image virtual hardware.
   a. Update virtual NIC to reflect recovery datacenter port group.
   b. Validate.
   c. (OPTIONAL) Power on the base image to validate NIC driver.
3. Take new snapshot of base image.
4. Update View pool configuration.
   a. Change base image snapshot.
   b. Update datastore configuration to recovery site datastores.
   c. Enable pool and provisioning.
   d. Validate.

**Detach/Attach Persistent Disk**
The persistent disks must first be detached from their primary site virtual machines so that they can be attached to a virtual machine in the recovery site.
1. Edit pool inventory to verify that all persistent disks are detached from desktops.
2. Review pool inventory to make sure all missing desktops are deleted.
3. Manually re-attach all persistent disks to newly provisioned desktops.

**Scenario Summary**
The order of the steps of the recovery process is of the utmost importance. If you delete desktops before detaching the persistent disks, it is impossible to complete a successful recovery. VMware recommends automating these steps to minimize the risks.

**Conclusion**
This case study shows how to achieve VMware View resiliency by leveraging basic vSphere High Availability and vCenter Site Recovery Manager functionality. This solution allows for disaster recovery of floating virtual desktops, linked clone persistent desktops, and persistent linked clone desktops with persistent user data disks. By virtualizing all management components and following the described procedures, you can implement a simple and effective disaster recovery strategy.

For more details about VMware View Resiliency, contact your local VMware sales representative.
About the Authors

Kristopher Boyd is a Technical Solutions Architect in the VMware Global Technology Solutions organization.

Matt Coppinger is Group Product Marketing Manager in the UK focusing on Strategic Advisory Services for VMware End User Computing.

John Dodge is Director, EUC Technical Enablement, managing a team of EUC architects and engineers focused on developing technical product collateral at VMware.

Duncan Epping, Principal Architect, VCDX works in the Technical Marketing group at VMware and is focused on cloud infrastructure management architecture.

Simon Richardson is a Solutions Architect, working in the UK with the largest public and private sector customers.