Implementing cost-effective disaster recovery

A Dell technical white paper

By Fabian Salamanca, Javier Jiménez, and Leopoldo Orona
Implementing cost-effective disaster recovery

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Copyright © 2011 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

Dell, the Dell logo, the Dell badge, Dell Compellent, Data Instant Replay, Fluid Data, PowerConnect, PowerEdge, Remote Instant Replay, and Storage Center are trademarks of Dell Inc. Microsoft is a registered trademark and Hyper-V is a trademark of Microsoft Corporation in the United States and/or other countries. Red Hat and Enterprise Linux are registered trademarks of Red Hat, Inc. VMware is a registered trademark and vSphere is a trademark of VMware, Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

November 2011
Implementing cost-effective disaster recovery

Contents

Introduction .......................................................................................................................... 1
Accelerating storage area network-based replication .......................................................... 2
Changing workloads dynamically....................................................................................... 2
Leveraging a foundation for efficient business continuity ................................................. 3
Managing storage replication ............................................................................................. 3
Configuring persona management ..................................................................................... 4
Simulating the disaster recovery process ........................................................................ 6
Summary ............................................................................................................................ 11

Figures

Figure 1. Implementing a disaster recovery time line for enhanced business continuity .......... 1
Figure 2. Configuring a dual-site disaster recovery simulation ........................................... 4
Figure 3. Creating a volume using the main site storage view ............................................. 5
Figure 4. Viewing storage at the disaster recovery site ...................................................... 5
Figure 5. Creating a disaster recovery persona ................................................................. 6
Figure 6. Confirming disaster recovery persona image details ............................................ 7
Figure 7. Stopping the replication process to simulate a failure .......................................... 7
Figure 8. Listing site volume Replay history ..................................................................... 8
Figure 9. Verifying a site persona is running properly ....................................................... 8
Figure 10. Executing the disaster recovery script ............................................................. 10
Figure 11. Confirming workload recovery in a persona startup log .................................... 10
Implementing cost-effective disaster recovery

Introduction
Today's working environment requires the availability of business-critical applications to ensure the successful operation of the organization, and IT departments are seeking innovative, cost-effective ways to provide business continuity. As a result, IT organizations are escalating their efforts to protect mission-critical applications such as e-mail, Internet presence, enterprise resource planning (ERP), and customer relationship management (CRM) from sudden disruption or downtime.

Although high availability clustering provides local protection, critical applications also require geographical protection. The stakes for preserving business continuity are high: among organizations that experience a major loss of business data, a significant number face critical problems, and only a few are able to overcome them.

Organizations creating a business continuity plan should begin by identifying critical applications and functions requiring protection. Next, they should delineate the recovery time objective (RTO), which specifies the maximum allowable time to restore each critical process after an adverse event occurs. Then they should define the recovery point objective (RPO), which targets the maximum acceptable amount of data that is at risk of loss after an adverse event occurs. Time to data (TTD) is the time required for retrieving backup data and delivering it to the recovery site (see Figure 1).

RTO and RPO are key measures that drive the configuration of a disaster recovery implementation, which also affect its cost. Reduced RTO and RPO translate into an enhanced business continuity response and a cost-effective disaster recovery implementation.

Figure 1. Implementing a disaster recovery time line for enhanced business continuity

Organizations taking an approach to deploy cost-effective business continuity and data replication can leverage Dell™ Advanced Infrastructure Manager (AIM)—a component of the Dell Virtual Integrated System (VIS) portfolio—with Dell Compellent™ Storage Center™ storage area network (SAN) arrays. This
Implementing cost-effective disaster recovery

architecture is designed to provide reliable data replication, OS image integrity, and efficient workload provisioning. The configuration referenced in this document implements Fiber Channel for OS image and data access, IP and Ethernet networks for long-distance, WAN-based replication using Internet SCSI (iSCSI) connectivity, and AIM to manage the provisioning of workload identities and network configuration.

Accelerating storage area network-based replication

Dell Compellent Storage Center SANs are designed to actively and effectively manage enterprise data throughout its life cycle, giving organizations the agility to constantly adapt in a dynamic business environment. Together, the Dell Fluid Data™ architecture, storage virtualization, advanced software, and modular hardware deliver enhanced efficiency, ease of use, and security. Built-in intelligence and automation help ensure that data is available when and where it is needed, and an open, persistent hardware platform scales in line with business needs to help protect storage infrastructure over the long term.

Dell Compellent Storage Center SANs are also designed to improve RTO and RPO while accelerating replication and recovery operations, helping reduce time consumed by management tasks as well as capacity and bandwidth costs, and increasing business continuity. Its thin replication feature allows for multisite replication that is more cost-efficient than traditional approaches to replication. Thin replication allows IT organizations to realize performance benefits using built-in bandwidth simulation and shaping. This feature helps align bandwidth procurement with estimated requirements based on actual data traffic flow, and transfer rates can be customized based on link speed, time of day, and priority.

Thin provisioning in Dell Compellent Storage Center SANs is designed to reduce the disk space that organizations consume and free their bandwidth resources. Volumes are created based on only written data, and thin replication enables intelligent transfer of only changed blocks of data thereafter. Dell Compellent Storage Center SANs also offer a technology-agnostic approach that provides the flexibility and scalability to support synchronous or asynchronous replication, Fibre Channel or iSCSI connectivity, and bidirectional, point-to-point, or multipoint configurations.

With the ability to create continuous snapshots—Replays created with Dell Compellent Data Instant Replay™ software—between local and remote sites, Dell Compellent Storage Center SANs provide unlimited recovery points and block-level management that allows for very rapid recovery. Remote replication can be tested with just a few mouse clicks, without disrupting production environments.

Changing workloads dynamically

Dell AIM enables data centers to react in real time to changing business needs by dynamically changing which servers are running and how those servers are connected to the network and storage. IT services can be dynamically provisioned or reconfigured in minutes, helping increase the utilization of existing assets, recover quickly if problems occur, and rapidly scale services to support business processes. AIM creates dynamic workloads that can leverage a flexible, cable-once data center infrastructure by coordinating end-to-end network, storage, and computing resources.

A dynamic workload, or persona, is a server environment captured on disk. It comprises the OS, the optional AIM agent software, application software, and storage and networking settings—including either iSCSI or Fibre Channel. A persona can also include other settings required to run an application on a server, either a virtual server or a physical server. This personality includes persistent
Implementing cost-effective disaster recovery

identification settings to help ensure the persona has access to the same resources no matter which changes in an AIM-managed data center may occur.

One type of persona, the network-booted persona, is a workload that is able to boot on any validated component, using its personality to always access the same resources. For example, at any given time, a network-booted persona can run on a physical server such as a Dell PowerEdge™ R610 server, and after business hours it can run on either a VMware® vSphere™-based or Microsoft® Hyper-V™-based virtual machine to save power and cooling costs. This dynamic capability enables the workload to use resources as needed on demand—for example, using low-cost hardware or virtual machines when load is expected to be minimal and retargeting to high-performance gear when load is expected to be high.

All data related to a network-booted persona resides in a SAN, enabling IT organizations to leverage the management benefits associated with SANs. For example, if a network-booted persona resides within a Dell Compellent virtual storage array, it benefits from the Dell Fluid Data architecture by using Data Instant Replay software for backup and recovery and Dell Compellent Remote Instant Replay™ software for long-distance replication.

Leveraging a foundation for efficient business continuity

Dell AIM and Dell Compellent Storage Center SANs offer a rich set of complementary features that together form a cost-effective foundation for an efficient approach to business continuity. In September 2011, Dell engineers configured a disaster recovery scenario utilizing two simulated sites that support production operation of workloads, replication, and disaster recovery. Two racks of equipment were used for this example infrastructure. One simulated the main site in Mexico City, Mexico, and the other simulated the disaster recovery site in Round Rock, Texas.

In this scenario, the main site runs a SAN-booted persona using the Red Hat® Enterprise Linux® 5 64-bit OS on a Dell PowerEdge R610 server (see Figure 2). The volume where this persona resides is to be replicated to the disaster recovery site using Dell Compellent Remote Instant Replay.

At the disaster recovery site this persona will be booted on a VMware ESX 4.1 virtual machine. Configurations at both sites include the following components:

- Dell Compellent Series 40 controller
- A 3.5-inch Serial Attached SCSI (SAS) disk array enclosure (DAE)
- Dell PowerConnect™ 6224 switch for local area network (LAN) and wide area network (WAN) access
- Brocade Silkworm 300 Fibre Channel switch
- ESX virtual machine running Dell AIM release 3.4.1

Primary challenges to achieving a successful disaster recovery configuration include the following:

- Data replication
- Physical-to-virtual (P2V) migration on the fly—also known as retargeting
- Virtual LAN (VLAN) management
- SAN access management

Managing storage replication

A 20 GB volume was created at the main site using Dell Compellent Enterprise Manager software (see Figure 3). An easy-to-use wizard allows administrators to create the replication volume at the disaster
Implementing cost-effective disaster recovery

recovery site automatically and at exactly the same time. This feature is available for any single volume created using the Dell Compellent Enterprise Manager software.

Figure 2. Configuring a dual-site disaster recovery simulation

The volume created at the main site is presented to a physical server using 8 Gbps Fibre Channel connectivity and its World Wide Port Number (WWPN). Proper zoning was configured at the Brocade Silkworm Fibre Channel switch (see Figure 4).

In this scenario, iSCSI connectivity, and not Fibre Channel connectivity, is deployed at the disaster recovery site. As a result, when the disaster recovery volume has been created through the automated process and first replication of data has completed, the disaster recovery volume is mapped to the original persona using iSCSI—after stopping the replication process momentarily. Then, a unique iSCSI Qualified Name (IQN), which was previously configured in the persona image at the main site, is already present at the disaster recovery volume. AIM can then be used to manage the replicated persona’s access to the SAN. The replication process then begins anew to keep transferring new data.

Configuring persona management

The persona to be replicated is created and located at both sites, and the protected workload runs the Red Hat Enterprise Linux 5 64-bit OS. Note: Because the scope of this scenario is related to data replication and disaster recovery, local persona retargeting is not shown in this disaster recovery example.
SAN zoning had already been implemented using the WWPN of the host bus adapter (HBA) and WWPN and World Wide Node Name (WWNN) of the Dell Compellent Storage Center SAN. Both servers—the Dell PowerEdge R610 running the persona at the main site and the VMware ESX-based virtual server at the remote site—have already been discovered.¹

¹ For information on discovering physical servers, VMRacks, and VMware virtualized servers, please refer to the “Dell Advanced Infrastructure Manager Release 3.4.1 User’s Guide” that is provided with the AIM software.
Implementing cost-effective disaster recovery

The persona at the main site was created by installing the OS directly on the master volume, with SAN booting previously configured in the HBA and BIOS. The LAN on Motherboard (LOM) on the server was connected to the Dell AIM control VLAN. The persona appears on the AIM console after installing the AIM agent software, which enables AIM to stop the persona and then start it successfully.

The VMRack and an AIM-managed virtual machine should be created and discovered by the AIM controller at the remote site. This virtual machine is intended to host the disaster recovery persona, which boots from an iSCSI volume. The disaster recovery persona was created using the Add Persona Wizard (see Figure 5).

The persona was configured with the following settings:

- Network mode: auto
- Networking enabled: yes
- Agent exists: yes
- iSCSI boot image

The disaster recovery persona is assigned to the VMRack—an ESX-based—virtual machine (see Figure 6).

Figure 5. Creating a disaster recovery persona

Simulating the disaster recovery process

A failure test at the main site can be simulated by stopping the replication process between both sites from the same Dell Compellent Enterprise Manager interface (see Figure 7). All replicas configured on the Dell Compellent Storage Center SAN can be tested using the Test Recovery Site Tool without disruption to help improve disaster recovery testing times and processes.
Implementing cost-effective disaster recovery

Figure 6.  Confirming disaster recovery persona image details

![Boot Image Details](image)

Figure 7.  Stopping the replication process to simulate a failure

![Stopping Replication Process](image)

The disaster recovery volume at the remote site can be activated by using the Dell AIM disaster recovery persona iSCSI login process, which is part of its previously configured booting process.

Using Dell Compellent Enterprise Manager features helps simplify creating one or several recovery points using available disaster recovery tools to meet specific needs (see Figure 8).
Implementing cost-effective disaster recovery

Figure 8. Listing site volume Replay history

To simulate a failure at the main site, the server running the persona can simply be powered off directly, circumventing a clean shutdown process. The first step following the failure is to get to the data restoration point (see Figure 1). Figure 9 shows the main site persona up and running properly just prior to the simulated failure.

Figure 9. Verifying a site persona is running properly

Tackling the RTO issue requires using AIM to easily implement a disaster recovery script. For example, the following generic command-line interface (CLI) wrapper and AIM shell script help simplify the development and execution of AIM CLI scripting, and a separate text file containing AIM-related commands is the only input necessary for this wrapper.
Implementing cost-effective disaster recovery

#!/bin/bash
#
# **************************************
# # (C) 2011 Dell
# # **************************************

SDK=/opt/dell/aim/bin/sdk
ACCOUNT=admin
PASS=admin
SCRIPT=$1

if [ "$SCRIPT" == "" ]; then
    echo "Usage: $0 [script filename]"
    exit 1
fi

echo "=====================================
", echo "DELL AIM SDK wrapper"
", echo "Running script $SCRIPT"
", echo "=====================================

echo "$SDK account=$ACCOUNT password=$PASS ifile=$SCRIPT"

Many tools can be leveraged to implement similar functionality, which facilitates efficient integration with several open platforms. Figure 10 shows execution of the disaster recovery script.

Although this script represents a simple start persona, additional tasks can be included to restore the operating environment of a production workload. For example, test and development environments can be gracefully shut down to make room for business-critical applications that require the additional compute capacity. In addition, creating, configuring, and virtually cabling new networks may be automated before starting hundreds of personas, which can follow a specific order to correctly sequence the start of dependent workloads (see Figure 11).
Implementing cost-effective disaster recovery

Figure 10. Executing the disaster recovery script

```
[root@aimgdl src] ./aimcli.sh start.txt

DELL AIM SDK wrapper
Running script start.txt

>> open
>> start persona id=PR.4.1
>> save
>> exit
[root@aimgdl src]$
```

Figure 11. Confirming workload recovery in a persona startup log
Implementing cost-effective disaster recovery

Summary
Using Dell AIM workload mobility, Dell Compellent Storage Center SANs, and Dell Fluid Data Architecture, this approach to automated replication for remote disaster recovery demonstrates how several steps in the process can be simplified. In a manner representing an efficient variation to industry standards, managing the comprehensive set of activities required for disaster recovery from the storage point of view in a single interface—Dell Compellent Enterprise Manager—is now possible.

RTO is an important measure in the operations necessary for restoration after data has been restored. Dell AIM helps reduce this target by automating and validating several resource management, virtual and physical synchronization, workload assignment, networking, and storage access tasks.

Restoring the workload in this simulation took 1 minute, 27 seconds plus an additional 56 seconds to manually trigger and execute the disaster recovery script to yield a total recovery time of 2 minutes, 23 seconds. Using an integrated monitoring tool instead of a manually executed script may reduce the RTO.

Several personas can be configured using the same steps and controlled by the same disaster recovery script. As a result, organizations can gain similar benefits when working with several workloads at one time.