DR-to-the-Cloud Best Practices

HOW TO EFFECTIVELY CONFIGURE YOUR OWN SELF-MANAGED RECOVERY PLANS AND THE REPLICATION OF CRITICAL VMWARE® VIRTUAL MACHINES FROM ON-PREMISES TO A CLOUD SERVICE PROVIDER

rackspace

MANAGED VIRTUALIZATION
Powered By VMware®

CONTENTS

DR-to-the-Cloud Best Practices

HOW TO EFFECTIVELY CONFIGURE YOUR OWN SELF-MANAGED RECOVERY PLANS AND THE REPLICATION OF CRITICAL VMWARE® VIRTUAL MACHINES FROM ON-PREMISES TO A CLOUD SERVICE PROVIDER

Some IT initiatives are a natural fit for cloud computing. Disaster recovery (DR) is one of them. In this technical white paper, we'll explain how to help protect on-premises production virtual machines (VMs) with VMware recovery technologies and use EMC storage solutions to replicate VMs to an off-premises cloud service provider. Derived from years of managed virtualization experience, the following DR-to-the-Cloud best practices are designed to give organizations like yours insight into a validated architecture that helps minimize downtime.

EXAMPLE CONFIGURATION

The following products will be used throughout this paper to describe how a company with an existing production VMware environment located in its own data center can leverage a cloud service provider as a DR target site:

Company On-Premises

- Existing license and installation of VMware® vCenter Server™ 5.1 or higher with VMware® vCenter™ Site Recovery Manager™ 5.1 or higher for runbook automation and failover protection

- EMC® VNX™ series for dedicated storage area network (SAN) storage

- EMC RecoverPoint appliance or RecoverPoint as a virtual appliance (RPA or vRPA), 4.0 or higher, for bidirectional replication

Cloud Provider Off-Premises

- Rackspace® Dedicated VMware® vCenter Server™ offering for the hosted target environment with its capabilities to be managed directly using VMware vSphere® API-compatible tools such as the VMware vSphere® Web Client or Site Recovery Manager

- EMC® VNX™ series for dedicated storage area network (SAN) storage

- EMC RecoverPoint appliance (RPA), 4.0, for bidirectional replication

The solution described in the next sections will include these technology components, as well as the specific configurations, integrations, considerations, and recommendations required to successfully implement a self-managed DR-to-the-Cloud scenario using Rackspace's data center (DC) as the target site.

EXAMPLE RECOVERY SCENARIO

In this model of business continuance, complete restoration of business operations is made possible by replicating the enterprise private-cloud application environment in addition to replicating the data hosted by the applications running in that private cloud. In contrast to a backup model— where data must be restored to the original, running application environment because disaster prevents the data center from returning to normal operations—DR-to-the-Cloud enables the replicated data to be brought up at the service provider target site. There, replicated data temporarily runs on a replicated application environment to help ensure continuity of business operations until service at the original source site can be restored.

To provide DR services from the company source site to the cloud, both the customer and the cloud provider sites must have infrastructure components. In this case, Rackspace has Dedicated vCenter and the company has its on-premises VMware environment and license of Site Recovery Manager. For storage, the Rackspace and customer environments must be running the same array technology. In this validated scenario, the Rackspace environment is using a VNX array running the physical RecoverPoint appliance. The customer site must also have an EMC array and the option exists for the customer to run a physical RPA or the software-only, vRPA. Additionally, the required network segmentation must be implemented at both the company and Rackspace sites, along with a consistent addressing scheme between sites.
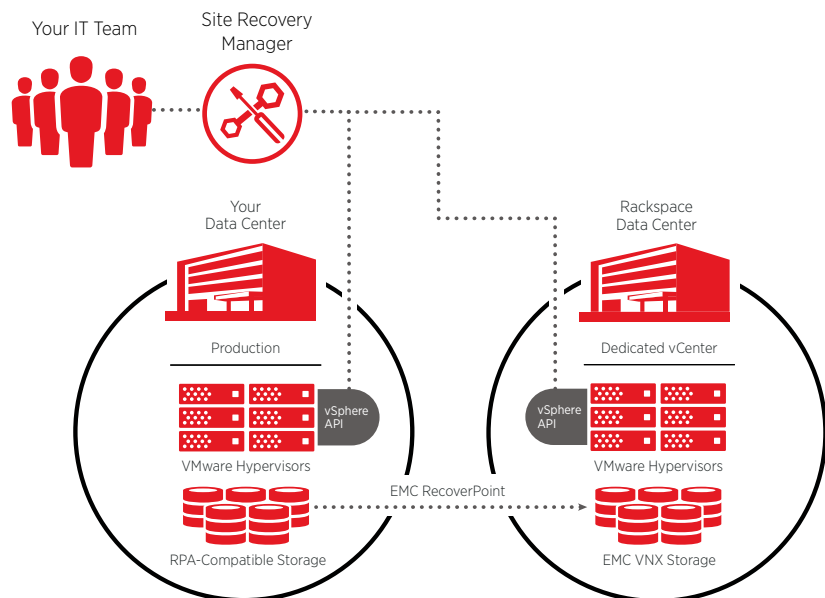

FIGURE 1

NETWORK REQUIREMENTS

While some organizations use a dedicated network connection to connect to the Rackspace DC and access their Dedicated vCenter environment, a more common approach is to use a secure VPN connection over the Internet. A VPN connection can also be used for non-protected systems such as Active Directory (AD) and database servers that have their own native replication. [See the Design Consideration Note on side.]

Site Recovery Manager uses specific network ports (e.g., SOAP and HTTP) to communicate with vCenter servers and the EMC storage solution. If these ports are used by other applications or blocked on your network, Site Recovery Manager must be reconfigured to use other ports. [For a detailed list of required Site Recovery Manager ports, see http://kb.vmware.com/kb/1009562.]

Firewalls should be configured to use all of the required network ports (or documented exceptions, if applicable). Rackspace will work with you to configure your firewalls to support the Site Recovery Manager protected segment traffic over a VPN.

To help ensure proper failover in the event of a disaster, a Rackspace target site must be configured to match the networks and settings in use by your VMware environment. These may include subnets, IP addresses, Access Control Lists (ACLs) and load balancing configurations. If the settings at your site don't match the target site settings for the servers being replicated, automated failover can't occur.

Once you establish network connectivity, setting up Site Recovery Manager is easy. A wizard guides you through the process of pairing your VMware environment and the Dedicated vCenter at Rackspace. You shouldn't have to adjust any additional network parameters to enable this connectivity. If pairing fails, a troubleshooting guide is available. [See http://kb.vmware.com/kb/1037682.]

STORAGE REQUIREMENTS

The next step is to configure the storage. You can match the Dedicated vCenter environment by first creating a vm_swap Logical Unit Number (LUN)—LUN sizing comes later. A VM swap file is created when a VM is brought online and requires the same amount of storage as memory that is assigned to the VM.

All hypervisors in a cluster with Site Recovery Manager protected VMs should be configured to place VM swap files on the non-replicated vm_swap datastore. Doing this prevents you from having to replicate constantly changing swap files that aren't required for recovery. VM swap file locations affect the compatibility of VMware vSphere® vMotion® and VMware vSphere®

Storage vMotion® with the hypervisor running at your site. This compatibility can vary depending on the version of VMware® ESXi™ you have installed. If you're using VMware® ESX™ or ESXi version 3.5 or later, hosts can be configured to store VM swap files with the VM configuration file or on a swap file datastore specified for that host. If the VM swap file location specified doesn't match and/or is not accessible across all hosts on a cluster, the speed of the migration may be impacted. [See http://kb.vmware.com/kb/1004082.]

Rightsizing and Managing Storage

As you prepare for DR-to-the-Cloud, you can plan for growth by keeping the following storage sizing and management recommendations in mind:

• The size of the vm_swap LUN should be at least equal to the total vRAM of all VMs configured to use the LUN. We recommend doubling the physical RAM in the entire cluster to support growth.

• You should create a vm_placeholder LUN to hold the placeholder VMs that Site Recovery Manager creates. Placeholder VM files are very small; for example, a fully populated Site Recovery Manager server with up to 1,500 VMs only requires a few gigabytes of storage.

• You should record which internal storage mappings and drives attached to VMs at your site aren't being replicated to the Rackspace target site. If they aren't available at the target site, VMs with any internal OS storage mappings (e.g., iSCSI, NFS, CIFS) may not have access to those resources in a failover situation. To help ensure proper failover during downtime, make sure all drives that you have mapped will be maintained.

• To be sure only replicated data stores are imported into Site Recovery Manager, you should include "srm" in the file name. When you are using the vCenter console, this naming convention will also help you more easily identify the specific VMs being replicated.

Sizing the EMC RPA Journal

After determining the requirements and configuring storage, you'll need to size your RPA journal, a key component of the RPA solution. As one or more volumes, a journal is stored at the target site to hold images (snapshots) that are either waiting to be distributed or that have already been distributed to the storage array. Snapshots preserve the state of the VM data at a specific point in time. Capacity sizing of your journal or journals is important because RPA provides LUN replication at both your site and the Rackspace target site. It also controls replication through consistency groups, which are collections of LUNs used to ensure that write-order consistency for replicated volumes can span multiple heterogeneous storage systems and servers. Capacity sizing of your journals can be done per consistency group and you can also define the protection window or how far back in time a rollback can be performed.

Your journal volume should have the correct performance characteristics to handle the total write performance required, as well as the capacity to store all the writes by the LUN(s) being protected.
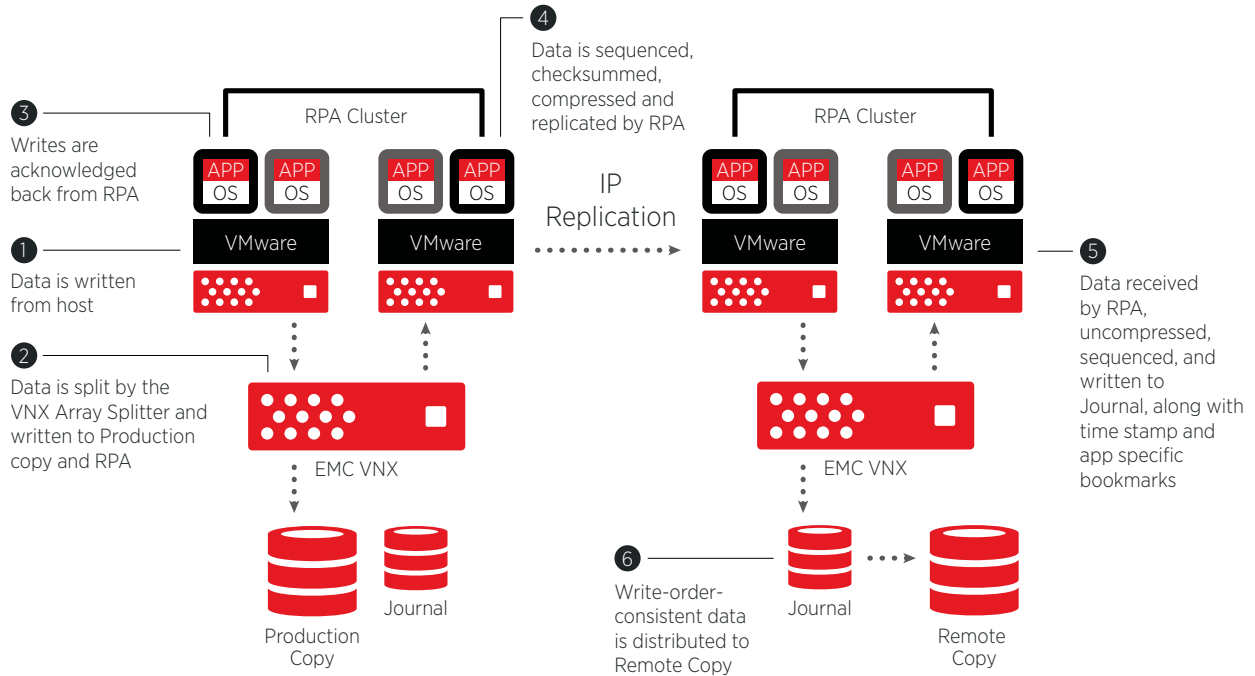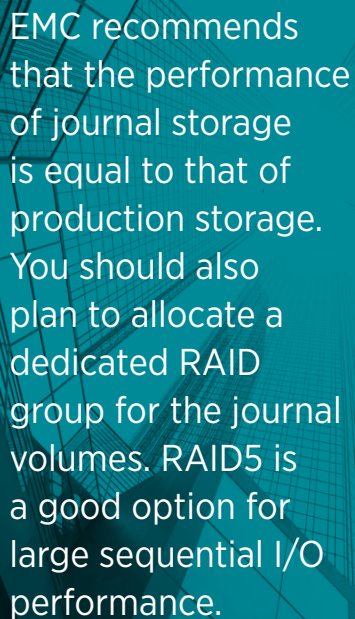

FIGURE 2

Because each journal holds as many images as its capacity allows, the oldest image will be removed to make room for the newest one. This "first in, last out" operation works only when the images have already been distributed to the storage array at both sites. The actual number of images in the journal varies and depends on the size of the images and the storage capacity.

While a minimum journal size is 10 GB, each journal in a consistency group must be large enough to support your business requirements for that group. EMC recommends using the following minimum journal calculation when not using snapshot consolidation:

- Minimum journal size = 1.05 * [(data per second)*(required rollback time in seconds) / (1 – image access log size)] + (reserved for marking)
  Note: To determine the value of your data per second, use ostat (UNIX) or Perfmon (Windows).

- [For more information about snapshot consolidation, see http://kb.vmware.com/kb/1015180.]

- Rackspace recommends the following journal storage calculation when using Site Recovery Manager: Calculate your daily % change rate (15% if not known) and how many days you'll run a DR test (we use up to 7 days)

- Usable data store size * change rate * days of testing = journal LUN
  The generic calculation is: Usable data store size * 15% * 7 = journal size

EMC recommends that the performance of journal storage is equal to that of production storage. You should also plan to allocate a dedicated RAID group for the journal volumes. RAID5 is a good option for large sequential I/O performance.

Another consideration in sizing the journal is the percent of journal space allocated for image access. The default use of the journal LUN is 80% for incoming data replication and 20% for image access. To run VMs in a Site Recovery Manager test, the image access portion of the journal is used for temporary write access to disks. To allow your Site Recovery Manager test to run long enough to validate your DR plan, we recommend changing the image access allocation to 40% of the journal LUN. This will leave 60% of the journal available to receive incoming data replication.

IDENTIFYING PROTECTION GROUPS

You'll need to create protection groups to specify which on-premises VMs should be included in the failover to a Rackspace target site. A protection group encompasses one or more data stores and all VMs that are located on them.

Protection groups are the smallest, logical grouping of VMs possible in Site Recovery Manager and they map to your array-based storage and must contain at least one replicated data store. All LUNs in a single consistency group need to be in the same protection group. Data stores and VMs can only be members of one protection group.

DOCUMENTING RECOVERY PLANS

After you create protection groups for your site, documenting recovery plans is next. A list of steps establishes a process that specifies which assets will failover from your data center operations to the Rackspace site. The list will also include the prioritization of those assets in the event of a disaster or test. Recovery plans can be configured as a single recovery plan or multiple recovery plans.

Recovery plans created in Site Recovery Manager can be associated with one or more protection groups. Multiple recovery plans for a protection group can be applied depending on different recovery priorities. With Site Recovery Manager, you have a variety of recovery options.

During a test, Site Recovery Manager creates a test environment—including network and storage infrastructure—that is isolated from the production environment. It rescans the ESX servers at the recovery site to find iSCSI and

Fibre Channel (FC) devices, and mounts replicas of NFS volumes. (Note: NFS mounts do not require that the host be scanned to be located). Site Recovery Manager registers the replicated VMs. It suspends nonessential VMs, if specified, at the recovery site to free up resources for the protected VMs being failed over. It then completes the power-up of replicated protected VMs in accordance with the recovery plan before providing a report of test results.

During test cleanup, Site Recovery Manager automatically deletes temporary files and resets the storage configuration in preparation for a failover or the next scheduled Site Recovery Manager test.

Site Recovery Manager supports two modes for failover—planned migration mode and disaster recovery mode. In planned migration mode, both sites are running normally and no errors are expected in the failover process. In disaster recovery mode, one site is offline due to a failure and errors are expected during the failover, but the process must continue.

During failover in planned migration mode, it is assumed that there is connectivity between sites and that they are online. When run in this mode, Site Recovery Manager shuts down the protected VMs. It synchronizes any final data changes between sites. It then suspends data replication and read/write enables the replica storage devices. Site Recovery Manager rescans the ESX servers at the recovery site to find iSCSI and FC devices, and mounts replicas of NFS volumes (Note: NFS mounts do not require that the host be scanned to be located). Site Recovery Manager registers the replicated VMs. It also suspends nonessential VMs, if specified, at the recovery site to free up resources for the protected VMs being failed over. Site Recovery Manager then completes the power-up of replicated protected VMs in accordance with the recovery plan before providing a report of failover results.

During failover in disaster recovery mode, Site Recovery Manager performs the same actions as it does during a planned migration, but it doesn't abort the process if one step fails. Site Recovery Manager continues the failover process to recover at the target site. If any errors are encountered, due to the production site being down, for example, you will have to re-run the failover when the source site is available or the errors are resolved so that Site Recovery Manager can bring the source and target environments into a consistent state.

Once a failover is complete it is necessary to have Site Recovery Manager perform a re-protect process, reversing the direction of replication after a failover, then automatically re-protecting protection groups.

Multiple recovery plans are typically in place at companies that need to recover individual departments in their business. Departments can be configured to have their own protection groups and plans that recover designated protection groups and applicable VMs. Site Recovery Manager supports 10 concurrent recoveries and 150 recovery plans.

TESTING RECOVERY PLANS

Unlike traditional DR systems, Site Recovery Manager allows you to test recovery scenarios without interrupting production environments. A test network uses a copy of replicated data at the target site. Recovery tests perform the steps documented in your recovery plan with the exception of steps labeled "recovery only," which would power down VMs at your data center and likely disrupt production services.

To implement one or more recovery plans and begin the failover process requires the use of the Site Recovery Manager console plugin in the vCenter client. A warning message will prompt you for execution validation. Once you confirm the process, in this example a planned migration failover, Site Recovery Manager will perform the following steps:

• Shut down the protected VMs if there is connectivity between sites and they are online

• Synchronize any final data changes between sites

• Suspend data replication and read/write enable the replica storage devices

• Rescan the ESX servers at the recovery site to find iSCSI and FC devices and mount replicas of NFS volumes

• Register the replicated VMs

• Suspend nonessential VMs (if specified) at the recovery site, to free up resources for the protected VMs being failed over

• Complete power-up of replicated protected VMs in accordance with the recovery plan

• Provide a report of failover results

At this point, the VMs at the Rackspace target site will be operational. Should you choose to failback to your original site, you must perform a re-protect. Because array-based replication will have been halted during the failover, the re-protect operation will restart—in reverse order—the process to replicate data from the target site to your source site. Moreover, a recovery plan in migration mode will need to be executed to return the replicated VMs to your site. Once this second migration is completed, replication will be disabled again and you'll need to perform another re-protect so that your site will once again be protected at the Rackspace site.

DR ROLES AND RESPONSIBILITIES

Implementing DR-to-the-Cloud requires careful planning. You must identify and document every process, as well as individual roles and responsibilities to help ensure success. The following is a table of recommended roles and responsibilities:

INITIAL CONFIGURATION

	CUSTOMER	RACKSPACE
Business Continuity (BC)/ Disaster Recovery (DR)	• Creates, maintains, and manages BC/DR plan and procedure using existing license of Site Recovery Manager for runbook automation and failover protection.	• Offers Dedicated vCenter Server for the hosted target environment with its capabilities to be managed directly using vSphere API-compatible tools such as the VMware vSphere® Web Client or the Site Recovery Manager plugin to the vCenter client. • Maintains EMC VNX series for dedicated SAN storage. • Maintains EMC RPA for bidirectional replication.
Networking	• Defines target network for VMs during test and failover.	• Configures target networks.
Monitoring	• Ensures recovery plan consistency. • Monitors replication operations at the source site. • Monitors replication space utilization at the source site.	• Monitors replication operations at the target site. • Monitors replication space utilization at the target site.
Data Replication	• Defines and configures replication frequency.	• Matches storage replication frequency defined by the customer.
Recovery Time Objective (RTO)	• Defines desired RTO. • Requests appropriate hardware to support RTO.	• Recommends appropriate hardware to support RTO.
Recovery Point Objective (RPO)	• Defines desired RPO. • Requests appropriate hardware to support RPO. • Configures replication.	• Recommends appropriate hardware to support RPO. • Matches customer-defined replication configuration.
Define/Change Recovery Plan	• Creates, maintains, and manages recovery plan. • Implements recovery plan.	
Customer Applications	• Configures applications for recoverability at target site.	

Change Management	• Maintains a change management program for all protected VMs and the supporting environment. Requests appropriate changes be made at BOTH the source and target sites.	• Collaborates with the customer to verify environment consistency prior to scheduled test or planned failover events. Updates customer if inconsistencies are found.

SITE RECOVERY MANAGER OPERATIONS

	CUSTOMER	RACKSPACE
Test Recovery Plan	• Develops scope and objectives. • Tests the recovery plan using Rackspace Dedicated vCenter Server. • Verifies functionality and conduct testing at the target site.	• Facilitates and monitors tests.
Recovery Test Cleanup	• Confirms conclusion of test. Backs up or documents changes needed in production systems. • Performs cleanup operation.	• Facilitates and monitors cleanup operations.
Planned Migration	• Develops scope and objectives. Initiates a planned failover of the recovery plan using Rackspace Dedicated vCenter Server. • Initiates failover of any additional resiliency services. • Performs re-protect process, reversing protection from the target back to the source site. Verifies functionality at the target site. • Initiates migration back to source site.	• Monitors planned migration. Reconfigures Rackspace services for VMs at target site, if needed.

NEXT STEPS

Cloud computing is ideal for DR and by following these best practices, your organization can easily and affordably self-manage DR using a validated DR-to-the-Cloud solution. As one of the largest VMware Service Provider Program (VSPP) partners, Rackspace has expert VMware Certified Professionals available and experience that comes with managing over 45,000 VMs. To get started, contact Rackspace or read more about DR-to-the-Cloud at http://www.rackspace.com/blog/tag/disaster-recovery.

ABOUT RACKSPACE

Rackspace® (NYSE: RAX) is the global leader in hybrid cloud and founder of OpenStack®, the open-source operating system for the cloud. Hundreds of thousands of customers look to Rackspace to deliver the best-fit infrastructure for their IT needs, leveraging a product portfolio that allows workloads to run where they perform best—whether on the public cloud, private cloud, dedicated servers, or a combination of platforms. The company's award-winning Fanatical Support® helps customers successfully architect, deploy and run their most critical applications. Headquartered in San Antonio, TX, Rackspace operates data centers on four continents. Rackspace is featured on Fortune's list of 100 Best Companies to Work For.

For more information, visit www.rackspace.com

ADDITIONAL RESOURCES

Rackspace

- Dedicated VMware vCenter Server: http://www.rackspace.com/managed-virtualization/dedicated-vcenter/

EMC

- Enterprise DR solutions: http://www.emc.com/backup-and-recovery/disaster-recovery.htm

- DR-as-a-Service Whitepaper: http://www.emc.com/collateral/white-papers/h12031-wp-disaster-recovery-as-a-service.pdf

- VNX with VMware vSphere Techbook: http://www.emc.com/collateral/hardware/technical-documentation/h8229-vnx-vmware-tb.pdf

VMware

- VMware vCenter Site Recovery Manager documentation: https://www.vmware.com/support/pubs/srm_pubs.html

- VMware vCenter Site Recovery Manager product site: http://www.vmware.com/products/site-recovery-manager

- VMware vCenter Site Recovery Manager 5.5 release notes: https://www.vmware.com/support/srm/srm-releasenotes-5-5-0.html

- VMware vCenter Site Recovery Manager 5.0 Evaluation Guide: http://www.vmware.com/files/pdf/products/SRM/VMware-vCenter-Site-Recovery-Manager-Evaluation-Guide.pdf

- Configuring VMware vSphere on VNX Storage: http://www.emc.com/collateral/hardware/technical-documentation/h8229-vnx-vmware-tb.pdf

Support: +44 (0)208 734 2700 | Sales: +44 (0)20 3553 3141 | Or Visit Us www.rackspace.co.uk
Rackspace Limited | 5 Millington Road | Hyde Park | Hayes | Middlesex | UB3 4AZ | UK