Solution Brief

Managing VMware Disaster Recovery for ONTAP Systems

Using the ONTAP Storage Replication Adapter with VMware Site Recovery Manager

Disaster Recovery for VMware

VMware customers are making significant investments in transforming their data center operations to support the growth of their digital enterprise initiatives. With all this investment, it is critical to also determine how to protect environments from significant outages that could be caused by natural causes, equipment failure, or cyberattack. Virtualization is a key component to the modern ecosystem, and for VMware users, VMware vCenter Site Recovery Manager (SRM) enables testing and orchestration of recovery plans for VMware virtual machines. To integrate an enterprise shared storage platform to use its storage data services with the SRM management layer requires the use of a Storage Replication Adapter (SRA). After being installed, the SRM interacts with the NetApp® ONTAP® cluster using SRA to discover and replicate storage logical unit numbers (LUNs), or virtual disks, between DR sites. In managing DR policies, SRM provides failover and test failover capabilities that allow for automated failover between DR sites, using SRA to leverage data services from the storage array to perform tasks when available.

NetApp makes the ONTAP SRA component available for users to download and quickly integrate with their SRM instance. After the SRM is installed, you can use it to configure protected and recovery sites in your environment that perform disaster recovery during failures leveraging ONTAP storage data services. A key feature of ONTAP storage software is found in the SnapMirror® capabilities.

With SnapMirror, users can transport data seamlessly and efficiently between NetApp storage systems to support both backup and disaster recovery with the same target volume and I/O stream. The replication can be done between ONTAP devices, regardless of host protocol or media type, as well as between disparate ONTAP versions. Users are also able to shrink network traffic by preserving data reduction benefits on the primary storage during transport, including deduplication, compression, and compaction.

Using SRM with NetApp ONTAP SRA for Disaster Recovery

There are some key steps to implementing an effective disaster recovery strategy and implementation using SRM and SRA. After completing the initial SRA configuration, you must set up disaster recovery workflows that can be executed. To configure disaster recovery workflows, you must create protection groups and then create a recovery plan.

Before you begin, you must have configured SRA and performed a replication operation for the primary site to the recovery site. To do this, you will have configured the network mappings, folder mappings, and resource mappings and configured placeholder datastores. Each replicated virtual machine must be assigned to an existing resource pool, folder, and network on the recovery site using inventory mappings. More about

■ NetApp®

performing these functions can be found in the *Virtual Storage Console, VASA Provider, and Storage Replication Adapter 7.0 for VMware vSphere Administration Guide*. With those tasks complete, you are ready to begin creating your disaster recovery workflows.

Step 1: Building protection groups
In creating your SRM disaster recovery method, you start by creating protection groups. A protection group is a way of identifying sets of virtual machines that will be recovered together during recovery. The virtual machine data will be replicated to the recovery site using the array-based replication of the NetApp storage platforms. Because each virtual machine is replicated on an individual basis, protection groups provide a way to identify the collection of VMs that support a single application, such as e-mail, and then recover all the group VMs together to get an application running on the recovery site.

Step 2: Creating a recovery plan
The recovery plan is the automated set of steps required to perform the recovery to return to normal operations at the recovery site. This plan defines which virtual machines get started, the startup order of each VM, and which scripts need to be run. If you have properly defined a protection group to include all the required virtual machines to be replicated together, the recovery plan can be defined in parallel to describe how each protection group is to be recovered.

Step 3: Testing
The most important part of having a disaster recovery plan is to know that it will work in the case of an outage. With the recovery plan test, you need to function as close as possible to running an actual recovery plan, but without disrupting the running VMs or interfering with the storage replication process. To help to protect the test from a recovery, there is an SRM test administrator role that will help to minimize the chances of performing a recovery instead of a test.

Step 4: Performing a recovery
Because you have regularly tested your DR processes, you should be ready to execute the DR plan in the case of a true outage. The storage platforms will have performed the replication between sites as the replication policy has defined, and the data will be ready at the recovery site. SRM will orchestrate your recovery plan and bring up the virtual machines at the recovery site according to plan. Your operations will be ready to resume using resources at your recovery site.

Improve the Efficiency of Your Disaster Recovery Operations
By using SRM to manage your DR process, your VMware environment can be restored to a state that will allow your operations to restart after an outage at your DR site. With SRA, VMware has given SRM users the ability to leverage the replication capabilities of their storage platforms to improve the efficiency of data movement between sites. For NetApp ONTAP customers, the advanced capabilities of SnapMirror deliver replication features beyond data movement for a wider set of replication options. This ties together the management of SRM with the data management of SnapMirror to deliver an efficient model for VMware disaster recovery operations.

About NetApp
NetApp is the data authority for hybrid cloud. We provide a full range of hybrid cloud data services that simplify management of applications and data across cloud and on-premises environments to accelerate digital transformation. Together with our partners, we empower global organizations to unleash the full potential of their data to expand customer touchpoints, foster greater innovation and optimize their operations. For more information, visit www.netapp.com. #DataDriven