NetApp

EBOOK

Disaster Recovery in the Cloud With

CLOUD VOLUMES ONTAP®

Executive Summary

Whether you are running NetApp ONTAP on-premises or already in the cloud using AWS or Azure, you need a good DR solution in place if you want to protect your data. AWS and Azure offer some native solutions and on-prem ONTAP users have their backup data centers, but both of these users could benefit from cloud-based DR using Cloud Volumes ONTAP. Disaster recovery allows you to ensure you can failover your business operations to a secondary location and later recover and failback to your primary copy reliably: Cloud Volumes ONTAP makes it possible to do that faster and more efficiently while paying less for updates and data storage.

Table of Content

Introduction

All enterprise platforms, whether on-premises or in the cloud, require a DR (Disaster Recovery) environment to ensure that business-critical services and applications can continue operating in the event of a major infrastructure outage. For example, a natural disaster such as a hurricane may cause outages at a primary site or even on a regional level. Security threats such as massive targeted malware attacks can also take sites completely out of action. In these circumstances, it is essential to bring services back online as quickly as possible, which requires having standby systems in a secondary location that can be failed over to.

Deploying disaster recovery environments is challenging for most organizations due to the requirement for infrastructure and site independence. There are huge costs involved in establishing and maintaining such sites physically—basically the same costs as the entire production environment but for a site that will sit idle for most of the time. This is where the cloud helps to lower the barrier to entry by providing scalable Infrastructure-as-a-Service solutions that can be used to build DR environments for both on-premises or cloud-based systems. After building out all DR services, the challenge then becomes to synchronize data from the production environment, and to keep it in synchronized going forward.

In this white paper, we examine in detail the challenges involved in setting up a DR environment, discuss the available services in AWS and Azure that can be used to build DR solutions, and look at how NetApp Cloud Volumes ONTAP provides cost-effective enterprise-grade support for data replication and disaster recovery both for existing NetApp storage system users and for cloud-based deployments on AWS and Azure.

Disaster Recovery Challenges

Effective disaster recovery requires a full complement of the applications and services used in production environments. Everything you need to run your primary workload has to be reproduced from the bottom up. The necessary infrastructure must be planned for and implemented in advance, and deploying physical infrastructure for the setup of a DR site increases operational costs significantly.

Making sure this all works is a paramount concern. The longer it takes a site or application to operate normally, the more business losses will be incurred. Getting the site up and running is so important in DR, it has its own metric. The time taken to bring services back online after a DR event is known as the RTO (Recovery Time Objective), and the aim should be to reduce this interval as much as possible.

Setting up a replica DR environment also requires having an independent, up-to-date copy of all enterprise data, including database systems, file services, iSCSI storage, etc. As data in the production environment will be constantly updated, these data changes must be transferred to the DR site on a regular basis. The frequency with which data in the DR site is updated will determine the period of time that data loss will be incurred for after a disaster. The amount of data that can acceptably be lost is known as the RPO (Recovery Point Objective). For some enterprises data is so important that in a DR event no data loss can be tolerated, which means their RPO will equal zero.

RPO
Recovery Point Objective
How much data in a time period a company can lose during a disaster event.

RTO
Recovery Time Objective
How long it takes to get back to normal operation after the disaster event.

Disaster Recovery Challenges

A fully-functioning DR site is useful for both unplanned and planned outages. For example, a DR site may be made live in order to perform updates to the primary production environment. This requires a failover to the DR site and then a failback after the updates have been performed. Failover and failback would also be used to make the DR site live after a disaster and to eventually restore services back to the primary site in the future, and so being able to perform these operations easily is a requirement for an effective DR solution.

Enterprise workloads and services are constantly evolving, and new software releases must be applied to both primary and DR environments. The primary site is used actively and so it will be possible to quickly verify that it is operating correctly. The DR site, however, may be left unchecked for a long period of time, and then may fail to come online when its actually needed. To prevent that from happening, it's essential to perform regular testing of DR services and ensure that they are functioning as expected.

Finally, after completing the deployment of a DR site, it may seem as though it simply remains idle for much of the time. In the interests of improving cost effectiveness, it would be ideal to make use of DR systems for peripheral requirements, such as read-only reporting or for setting up software development test environments.

DR Challenges at a Glance

SCHEDULED SYNCS

Data must be synchronized efficiently and regularly to the secondary location to ensure it is up to date.

FAILOVER AND FAILBACK

Provide the capability for data storage to be failed over to the DR site and then failed back to the primary site as required.

REGULAR TESTING

Ensure that DR systems work as expected in the case a DR failover is required.

CONTROLLING COSTS

DR compute and storage resources should be allocated in such a way to remain cost effective since the system is not normally in active use.

Building Cloud Based DR Environments in AWS & Azure

Disaster recovery environments must implement redundancy at the compute, network, and storage layers. In this section, we will look at how this can be done using the two major public cloud providers, AWS and Azure.

Cloud DR Environment Building Blocks

COMPUTE

The CPU processing power that runs applications.

Amazon EC2 and Azure Virtual Machines provide flexible cloud compute resources that can be used to build and scale the most demanding enterprise workloads. A range of different instance types makes it easy to find the right fit in terms of CPU processing power and memory capacity. For containerized applications, both AWS and Azure also offer native Kubernetes services, known as Amazon EKS and Azure AKS, respectively.

Some DR deployments make use of an architecture known Pilot Light, whereby only the most critical applications and services are active at the DR site. When a failover is performed, the rest of the infrastructure can be instantiated on demand, which can dramatically reduce the costs associated with the DR environment for regular day-to-day operation. AWS CloudFormation and Azure Resource Manager make it possible to recreate compute and other cloud resources from a predefined template.

NETWORK

How traffic is managed to the primary and secondary DR site.

In event that a failover is required, client hosts and applications must to be able to automatically find the active site that is hosting the services they need to access. This is usually performed through DNS, which allows a network name to be repointed to a different resource without requiring any client-side changes. Amazon Route 53 and Azure DNS can be used to manually failover services to a DR site when this is required. Amazon Traffic Flow and Azure Traffic Manager take this a step further, allowing for automatic failover when the primary site has been deemed to be unhealthy.

STORAGE

The repository for all the data, optimized for usage and costs.

Amazon and Azure provide a variety of data storage solutions, such as managed file services, block-level iSCSI devices, and low cost, highly durable object storage. Some of these services provide redundancy within an Availability Zone, such as Amazon EBS and Azure Disk, across Availability Zones, such as Amazon EFS and Azure Files, and even across regions with Amazon S3 and Azure Blob.

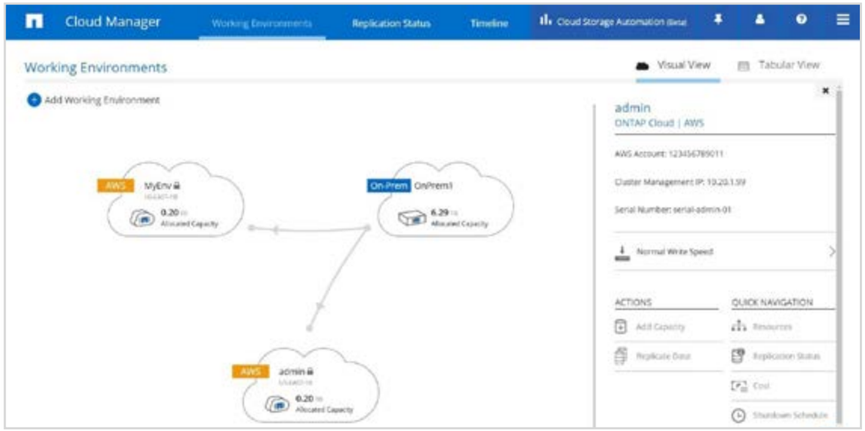
Each solution in use at the primary site would need to be catered for separately, and could require end-user administrators to set up additional processes and workflows. For example, Amazon EC2 compute instances using Amazon EBS would need the data being stored at the primary site available at the DR site as well. Amazon EBS snapshots could be used to create a solution for this, however the actual failover and failback processes would need to be manually developed and tested. That can be a difficult, risky, and costly process to carry out and maintain. In the next section we'll look at how NetApp's Cloud Volumes ONTAP helps solve those problems.

Cloud-Based DR with Cloud Volumes ONTAP

Cloud Volumes ONTAP is NetApp's solution for enterprise data management in AWS and Azure. Building on native cloud compute and storage resources, Cloud Volumes ONTAP offers a wide variety of data storage services from a single platform, including NFS, SMB/CIFS with Active Directory integration, and iSCSI. Any and all of this data can be efficiently replicated from on-premises NetApp ONTAP systems, or from AWS or Azure-based deployments of Cloud Volumes ONTAP, using NetApp's replication technology, SnapMirror®.

Cloud Volumes ONTAP provides SnapMirror as a solution for block-level data replication that keeps the destination up to date through incremental updates. Users can specify a synchronization schedule, for example, of every minute or every hour, at which time data changes from the source will be transferred over. Creating a new SnapMirror relationship is very easy: simply drag and drop the source system onto the destination in Cloud Manager. This is a process that the SnapMirror wizard will walk you through from start to finish. These are all central parts of the NetApp data fabric vision.

Cloud Manager is the web-based UI used for deploying Cloud Volumes ONTAP and also managing hybrid cloud ONTAP storage environments. Existing on-premises and cloud-based ONTAP deployments can be discovered and added to the main dashboard, making it possible to set up replication relationships in any direction. Cloud Manager gives users the ability to failover data storage to the SnapMirror destination, as well as facilitating efficient failback to the source through a reverse re-synchronization operation.



Cloud Volumes ONTAP Features

HIGH AVAILABILITY

Ensures zero data loss and minimizes downtime

STORAGE EFFICIENCIES

Reducing overall storage space cuts DR costs

STORAGE TIERING

Automatically shift DR environments to performant disks only when needed, reducing costs

SNAPMIRROR

Data replication technology keeps DR sites up to date

FLEXCLONE DATA CLONES

For fast and space-efficient DR testing

CLOUD MANAGER

Easy management of all primary and DR systems

BACK

NEXT

Benefits of using Cloud Volumes ONTAP

Reliable Data Protection

Cloud Volumes ONTAP provides reliable data protection in the cloud within an Availability Zone, across Availability Zones using Cloud Volumes ONTAP HA, and across regions using SnapMirror replication. This comprehensive coverage of data protection capabilities is easily accessible from the Cloud Manager UI, which reduces the complexity of protecting cloud, hybrid cloud, and multicloud storage environments.

Cost Efficiency: Save Space, Save Costs

When using Cloud Volumes ONTAP, storage space requirements can be significantly reduced, in some cases by as much as 70%, through the use of built-in ONTAP technologies such as data compression, thin provisioning, and data deduplication. These storage efficiency solutions are applied transparently at the block-level, and so require no changes to client applications. In fact, SnapMirror replicates data in its compressed and deduplicated form, improving the speed at which transfers complete and reducing network bandwidth usage.

Data tiering is another compelling storage efficiency feature provided by Cloud Volumes ONTAP that automatically and seamlessly shifts data between performance and capacity tiers as required. The capacity tier uses Amazon S3 or Azure Blob, which are extremely cost effective for data that is not currently in active use, such as that of a DR environment. Cloud Volumes ONTAP provides fast on-demand access to this data by automatically bringing it back into the performance tier when it needs to be accessed, such as in a DR scenario. As with syncs, SnapMirror integrates with data tiering by sending data received at the destination directly to the capacity tier.

THIN PROVISIONING

Allocates storage only as it needs to be used, not ahead of time.

COMPRESSION

Compresses block groups to reduce the amount of storage space used.

DEDUPLICATION

Reduces storage space by automatically removing duplicate blocks.

COMPACTION

Consolidates data from blocks that are not full, which drives up storage utilization.

Seamless Failover and Failback

When a disaster actually occurs, storage administrators need a quick, easy, and reliable process for bringing storage online at a DR site, and SnapMirror provides this through intrinsic support for failing over to destination volumes. If the primary site is later recovered successfully, the new data created in the DR storage volumes can be efficiently synchronized back to the source volumes, which enables the normal flow of data replication between source and destination to be re-established without requiring a full baseline copy of the data to be copied over. Cloud Manager provides an easy-to-use graphical user interface for performing these failover and failback operations.

Benefits of using Cloud Volumes ONTAP

Efficient and Instant Testing Environment through Data Cloning

Software applications are continuously being developed and updated, which necessitates releasing new versions to production, as well as to DR environments. As a DR site is not normally active, this creates a risk of latent problems in the deployment that may not manifest themselves until after a failover, which would seriously affect the time taken to recover from an outage. Cloud Volumes ONTAP helps tackle these issues through its NetApp FlexClone® functionality, which can be used to instantly create zero-capacity cost, writable clones of a SnapMirror destination volume of any size. These volume clones can be used to execute DR platform test suites that mutate the data they operate on without interrupting the active replication of data from source systems. Clones can also be used to gain greater benefit from idle resources at the DR site by providing data for software development test environments or DevOps CI/CD pipelines.

Orchestration and Automation with a Click

Cloud Manager provides a modern, easy-to-use GUI interface for managing Cloud Volumes ONTAP, which includes setting up SnapMirror replication and creating FlexClone volumes. All of these tasks can also be performed through Cloud Manager's RESTful API, which allows for them to be automated or performed as part of a wider disaster recovery orchestration plan.

Conclusion

DR environments are crucial for ensuring data protection and the continued operation of software applications and services when physical infrastructure has been seriously compromised, such as from server failures, power outages, security threats, and natural disasters, to name a few. As shown in this white paper, Cloud Volumes ONTAP provides a reliable, cost-effective, and flexible solution for both on-premises and cloud-based ONTAP storage environments to leverage AWS and Azure for disaster recovery.

Visit us online to find out more about the enterprise data protection and DR capabilities of Cloud Volumes ONTAP, or start a free 30-day trial today in AWS or Azure.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific
environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's
installation in accordance with published specifications.

NA-287-0218

BACK