NetApp Verified Architecture

NetApp HCI for Multicloud Data Protection with Cloud Volumes ONTAP

James Bradshaw III, Arvind Ramakrishnan, Chris Reno, NetApp
June 2019 | NVA-1137

Abstract

This document describes a NetApp® Verified Architecture (NVA) for data protection with NetApp HCI that uses Cloud Volumes ONTAP®, Red Hat OpenShift, and the NetApp Kubernetes Service (NKS).

NetApp®

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Executive Summary

As organizations increasingly rely on data for their daily operations, building a data protection solution is more important than ever. Whether applications reside on the premises or in the cloud, it's increasingly important to protect against events that might cause data loss or service failure. The need to back up applications, operate from a disaster recovery location to ensure business continuity, and develop and test efficiently has never been greater.

The data fabric delivered by NetApp is an architecture and set of data services that provides consistent capabilities across a choice of endpoints spanning on-premises and multicloud environments. These endpoints can include systems that use NetApp® ONTAP® software or NetApp Element® software. NetApp HCI, a fully provisioned virtual hybrid cloud infrastructure, takes advantage of robust data storage software with Element through native SAN (iSCSI) services and file services through NetApp ONTAP Select. For public cloud services, NetApp offers a wide variety of options that integrate seamlessly into a customer's IT practices and are designed to reduce overall cloud spending. Cloud Volumes ONTAP is a powerful, cost-effective, and easy-to-use data management solution for cloud workloads. NetApp Kubernetes Service (NKS) helps dramatically simplify the management and deployment of Kubernetes clusters.

This NetApp Verified Architecture (NVA) demonstrates backup, disaster recovery, and test and development use cases with a workload spanning NetApp HCI, Red Hat OpenShift, NKS, and Cloud Volumes ONTAP. This document details the design choices and technical requirements to achieve a flexible, predictable, and reliable hybrid multicloud infrastructure that scales independently with your application demands, as demonstrated with various use cases.

For more information about the data fabric, see What Is a Data Fabric?

2 Program Summary

2.1 NetApp Verified Architecture Program

The NetApp Verified Architecture program offers customers a verified, referenceable architecture for NetApp solutions. With a NetApp Verified Architecture, you get a NetApp solution architecture that:

- Is thoroughly tested
- Is prescriptive in nature
- Minimizes deployment risks
- Accelerates time to market

2.2 NetApp HCI with Cloud Volumes ONTAP and SnapMirror

NetApp SnapMirror® replication technology provides disaster recovery and data transfer between Element software and ONTAP enabled systems, offering data protection for NetApp HCI systems across your data fabric. SnapMirror creates a replica, or mirror, of your working data in secondary storage, from which you can serve data if a catastrophe occurs at the primary site. In addition to disaster scenarios, SnapMirror can be used to migrate data between systems as requirements change, allowing you to choose the most appropriate system to satisfy organizational growth needs.

With SnapMirror, data is mirrored at the volume level. The relationship between the source volume in primary storage and the destination volume in secondary storage is called a *data protection relationship.* The clusters (referred to as endpoints) in which the volumes reside and the volumes that contain the replicated data must be peered. A peer relationship allows clusters and volumes to exchange data securely.

Beginning in Element 10.1 and ONTAP 9.3, these peer relationships include systems beyond NetApp AFF and FAS, enabling replication of NetApp Snapshot™ copies between Element and ONTAP. Starting with Element 10.3 and ONTAP 9.4, you can replicate Snapshot copies of a LUN that was created in ONTAP, including ONTAP Select, back to an Element volume. SnapMirror replication of Element to Cloud Volumes ONTAP is supported starting with ONTAP 9.5 and Element 11.0. This replication capability is seamless whether you are using a physical AFF or FAS cluster or Cloud Volumes ONTAP in the public clouds of Amazon Web Services (AWS) or Microsoft Azure.

For more information about SnapMirror, see the SnapMirror Data Replication landing page.

2.3 Assumptions

This document assumes that the reader has working knowledge of the following areas:

- AWS and Microsoft Azure
- NetApp storage administration
- Network administration
- Windows and/or Linux administration
- Kubernetes

3 Solution Overview

This NetApp HCI solution gives customers a fully validated multicloud solution that integrates NetApp public cloud offerings with NetApp HCI, as demonstrated with a containers workload. By integrating on-premises and cloud products, this solution enables organizations to improve the productivity of infrastructure engineers, DevOps engineers, and cloud teams to provide a robust data protection solution.

3.1 Business Challenges

Flexibility, efficiency, and data protection are at the core of a modern data center design that spans on the premises and the cloud. When customers deploy new services or run applications with varying usage needs, the public cloud offers a level of flexibility that allows an “as-a-service” consumption model.

Applications with fixed usage patterns are often still deployed in a more traditional fashion due to the economics of on-premises data centers. This situation creates a multicloud environment for applications based on the model that best fits the application.

Regardless of where application data resides, the ability to protect it, back it up, and develop and test it on a secondary instance is still a business challenge that must be addressed. Managing resources deployed in the cloud presents its own challenges and sets of tools. NetApp HCI provides the foundation for on-premises resources, Cloud Volumes ONTAP offers a familiar management plane for storage in the cloud, and NKS delivers Kubernetes clusters with just a few clicks.

3.2 NetApp and the Public Cloud

Customers purchase raw server and storage resources for many functions, including infrastructure as a service, from public cloud providers such as AWS, Microsoft Azure, and Google Cloud Platform. Customers can use server or virtual server environments to run their applications and cloud storage for their data. For customers to use storage in a way that is consistent with their on-premises data center, it’s important for their data to be controlled and protected.

NetApp has embraced the public cloud like no other storage vender. By offering software or services, NetApp allows customers to choose whether to fully control their own storage system in the cloud or to go full service and control performance levels, SLAs, and SLOs. Customers can decide where to deploy primary workloads and develop disaster recovery strategies and development and test scenarios while reducing cloud costs. They benefit from data management capabilities that were previously unavailable in

public clouds. Some of the products and services that NetApp offers in the public clouds include the following:

- Azure NetApp Files
- Cloud Volumes Service for AWS
- Cloud Volumes Service for Google Cloud
- Cloud Volumes ONTAP
- Cloud Sync
- NetApp Kubernetes Service
- Cloud Manager
- Cloud Insights

NetApp offers this collection of resources to help customers navigate the journey to the public cloud. NetApp Cloud Central provides a landing page for deployment of a variety of NetApp Cloud resources with the click of button. NetApp Cloud Central allows customers to try Cloud Volumes ONTAP, Cloud Volumes Service, NKS, and Cloud Insights on a variety of public cloud providers.

For more information about NetApp cloud resources, see the following resources:

- NetApp Microsoft Azure Partner Page
- NetApp Google Cloud Platform Partner Page
- NetApp AWS Partner Page

3.3 NetApp HCI with Cloud Volumes ONTAP

NetApp HCI for multicloud data protection with Cloud Volumes ONTAP is a prevalidated, best-practice data center architecture that uses an enterprise multicloud model. This NVA offers guidance for deploying microservice workloads at an enterprise scale, including backup to the cloud, disaster recovery in the cloud, and test and development of container workloads in the cloud. The design described in this document is built on the VMware private cloud and uses the NetApp Verified Architecture program and product documentation. It provides the advantages of open-source innovation with enterprise robustness coupled with data protection in the cloud. NetApp SnapMirror is an integral component of the design, tying the data fabric together with NetApp HCI and Cloud Volumes ONTAP.

For full information about NetApp HCI and the Red Hat OpenShift Container Platform, see NVA-1124: Red Hat OpenShift Container Platform with NetApp HCI NVA Design Guide.

For full information about NetApp HCI and the VMware Private Cloud, see NVA-1122: NetApp HCI for VMware Private Cloud Design Guide.

For full information about NetApp HCI and SnapMirror use cases, see TR-4748: Build your Data Fabric with NetApp HCI, ONTAP and Converged Infrastructure.

3.4 Target Audience

This document is for NetApp and partner solutions engineers and customer strategic decision makers. It describes the architecture design considerations that were used to determine the specific equipment, cabling, and configurations that are required for a particular environment.

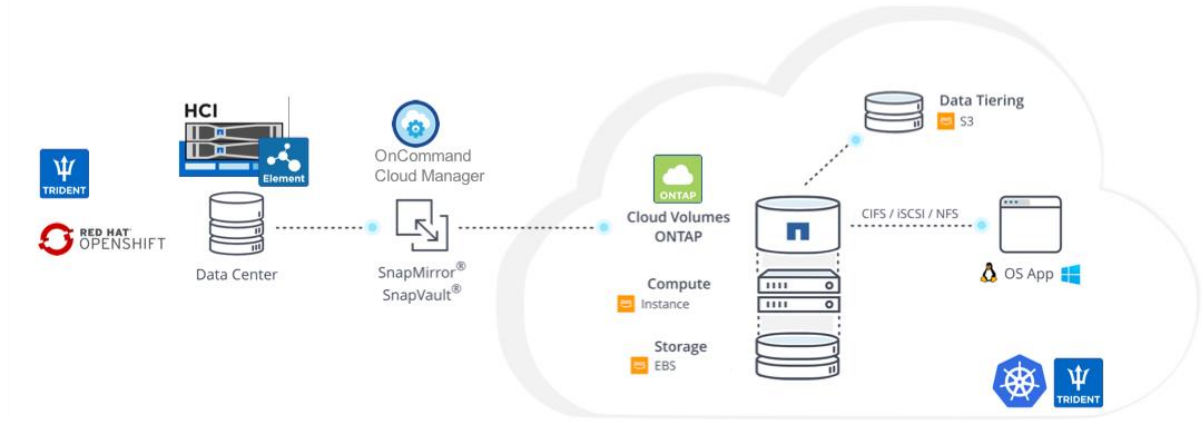
4 Solution Technology

The key technology elements of this design include:

- NetApp HCI with on-premises Element storage
- Red Hat OpenShift for containers workload on the premises
- NetApp Cloud Volumes ONTAP in the public cloud

- NKS in the public cloud
- Data fabric with SnapMirror
- NetApp Cloud Manager
- NetApp Trident

Figure 1) Solution architecture with AWS.



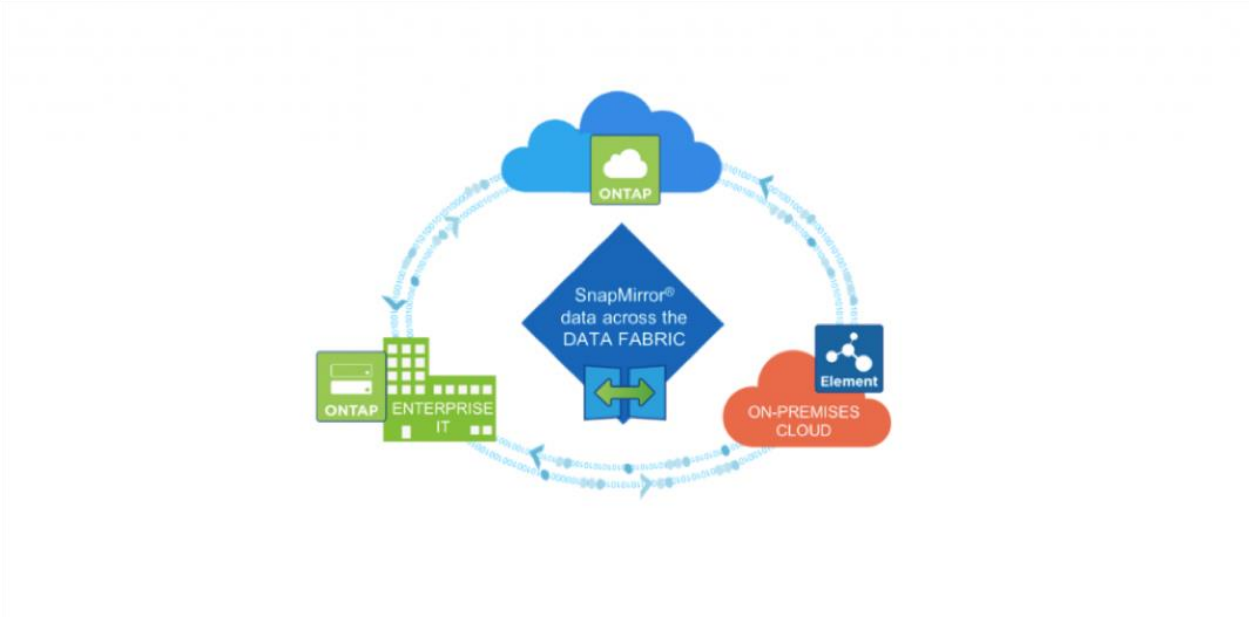
4.1 The Data Fabric

The data fabric helps organizations unleash the power of data to meet business demands and gain a competitive edge by putting data at the heart of the business beyond physical boundaries, applications, and infrastructures. The data fabric provides efficient data transport, software-defined management, and a consistent data format, allowing data to move more easily among clouds, all made possible with NetApp SnapMirror.

The data fabric architecture helps accelerate digital transformation by providing the following capabilities:

- **Data visibility and insights.** Insights into performance, capacity, and cost for resources and application planning, along with analytics application integrations.
- **Data access and control.** Migration to and from on-premises and cloud environments, replication, business continuity, data tiering for efficiency, and access across locations and applications.
- **Data protection and security.** Data backup and recovery, archiving and retention, copy data management, encryption, and application integration.

Figure 2) Data fabric and NetApp SnapMirror.



4.2 NetApp Cloud Central

NetApp Cloud Central is a centralized location to access and manage NetApp cloud data services. These services enable you to run crucial applications in the cloud, create automated disaster recovery sites, back up your SaaS data, and migrate and control data across multiple clouds.

Cloud Manager and NetApp Kubernetes Service (NKS) integration with NetApp Cloud Central offers a simplified deployment experience, a single location to view and manage multiple Cloud Manager systems, and centralized user authentication.

For more information about NetApp Cloud Central, see the NetApp Cloud Central landing page.

4.3 NetApp Cloud Manager

NetApp Cloud Manager, provisioned from NetApp Cloud Central, is the single-pane console for Cloud Volumes ONTAP resources. Cloud Manager offers the following capabilities:

- Centralized management for controlling multiple ONTAP systems both on the premises and in the AWS and Azure clouds.
- Simplified provisioning of storage capacity with automatic capacity scaling.
- Data fabric enablement through automation and orchestration of cloud storage operations with RESTful API support and integration with NetApp cloud management systems across hybrid and multicloud environments.

For more information about NetApp Cloud Manager, see the NetApp Cloud Manager product page.

4.4 NetApp Cloud Volumes ONTAP

Cloud Volumes ONTAP combines data control with enterprise-class storage features for various use cases, including:

- File share and block-level storage serving NAS and SAN protocols (NFS, SMB/CIFS, and iSCSI)
- Disaster recovery
- Backup and archive

- DevOps
- Databases (SQL, Oracle, and NoSQL)
- Any other enterprise workload in AWS and Azure

Cloud Volumes ONTAP runs in a public cloud environment, bringing intelligence and data fabric connectivity to public cloud storage. It offers customers the following benefits:

- Nondisruptive operations
- Seamless workloads migration
- Low-cost disaster recovery
- Reduced storage footprint
- Grow-as-you-go file shares
- Automated DevOps environments
- Cloud Volumes ONTAP managed encryption at rest
- Cost-effective data protection
- Cloud write once, read many (WORM) data protection

Cloud Volumes ONTAP supports the following features in AWS and Azure:

- Highly available storage
- iSCSI and NFS/CIFS file services
- Thin provisioning, deduplication, and compression
- Data tiering
- Data encryption
- NetApp FlexClone® technology
- NetApp SnapMirror and SnapVault® replication
- NetApp Snapshot copy, NetApp SnapCenter®, and NetApp SnapRestore® technologies
- NetApp SnapLock® technology

For more information about NetApp Cloud Volumes ONTAP, see the Cloud Volumes ONTAP product page.

4.5 NetApp Kubernetes Service

NetApp Kubernetes Service is an advanced Kubernetes-as-a-service platform that directly supports the application orchestration capabilities of the data fabric. NKS allows users to quickly build production-ready Kubernetes clusters on their cloud of choice. NKS makes management of Kubernetes clusters easy from a single pane of glass. and it allows multiple clusters to be managed as one across cloud providers.

For more information about NetApp Kubernetes, see the NKS product page.

4.6 NetApp Element Software

NetApp Element, the storage foundation of NetApp HCI, is designed for data centers in which rapid, modular growth or contraction is required for diverse workloads. Element is the storage infrastructure of choice for service providers because of its flexible handling of permanent and transient workloads with various throughput and capacity requirements. Element provides enterprise-grade storage efficiencies while also being easy to administer, whether from the GUI or VMware plug-in, or through automation with available APIs.

For more information about NetApp Element Software, see the Element product page.

4.7 NetApp HCI

NetApp HCI with Element software and VMware vCenter are the foundation for a multicloud infrastructure. NetApp HCI is designed to deliver a public cloud consumption experience with simplicity, dynamic scaling, and operational efficiency for hybrid multiclouds. Each Element storage node added to a NetApp HCI environment provides a set amount of IOPS and capacity, allowing predictable, plannable growth. QoS for each workload can be guaranteed because each node provides a set volume of throughput (IOPS) to the storage cluster. Minimum SLAs are assured with Element because the total throughput of the cluster is known.

For more information about NetApp HCI, see the HCI product page.

4.8 NetApp Deployment Engine

The NetApp Deployment Engine (NDE) enables the quick deployment of NetApp HCI, including a NetApp Element software cluster and VMware virtualized infrastructure. NDE simplifies day-0 deployment by reducing the number of manual steps from over 400 to fewer than 30. Preinstallation checklists, consistent credential application, and auto-IP address assignment enable successful deployments while reducing user errors. NDE optimally configures data and management networks, configures the cluster, and sets up VMware ESXi and vCenter and other required configurations. The virtualized environment becomes operational in a risk-free process.

For more information about NDE and the deployment of NetApp HCI, see the NetApp HCI Deployment Guide.

4.9 NetApp ONTAP Select

As part of NetApp HCI deployment, administrators can optionally install a single-node ONTAP Select cluster as a virtual machine (VM). ONTAP Select builds on NetApp HCI capabilities, adding a rich set of file and data services to the HCI platform while extending the data fabric.

The primary use cases for ONTAP Select on NetApp HCI include departmental file services, VM template storage over NFS, and home directories for midsized virtual desktop deployments. ONTAP Select is not positioned as a primary storage platform for VMs hosted on NetApp HCI.

For more information, see the ONTAP Select product page.

4.10 NetApp Trident

Trident, a fully supported open-source project maintained by NetApp, enables microservices and containerized applications to use enterprise-class storage services such as QoS, storage efficiencies, and cloning to meet the persistent storage demands of applications. Trident makes use of StorageClass objects, introduced in Kubernetes 1.4, to dynamically provision a Persistent Volume when a Persistent Volume Claim object is created. Depending on an application's requirement, Trident can dynamically provision storage from the following sources:

- NetApp ONTAP data management software (AFF, FAS, Select, or the cloud)
- NetApp Element software (HCI or SolidFire)
- NetApp SANtricity® software (E-Series or EF-Series)

For more information, see the Trident documentation.

Note: Following the migration of a data set to the public cloud, the import functionality of Trident is used to import the volume to the destination Kubernetes cluster.

4.11 Red Hat OpenShift Container Platform

The Red Hat OpenShift Container Platform provides enterprise Kubernetes bundled CI/CD pipelines, automated builds, and deployment, allowing developers to focus on application logic while using a best-in-class enterprise infrastructure. The platform includes an enterprise-grade Linux operating system, container runtime, networking, monitoring, a container registry, authentication, and authorization.

For more information, see the Red Hat OpenShift product page.

5 Primary Use Case

NetApp HCI is targeted at a variety of use cases for enterprise customers, including:

- **Hybrid cloud.** NetApp HCI accelerates delivery of private cloud services with an enterprise-scale hyperconverged infrastructure while being an integral part of the data fabric.
- **End-user computing.** NetApp HCI with VMware Horizon delivers an optimal user experience through ease of management and seamless scalability.
- **Workload consolidation.** NetApp HCI helps eliminate silos and allows predictable operations with multiple applications.

This NVA validates the hybrid cloud use case in multiple public clouds. It details the following use cases with a containers workload on the premises and in the public cloud:

- Backup of Element volumes to Cloud Volumes ONTAP
- Disaster recovery of HCI volumes onto AWS or Azure by using Cloud Volumes ONTAP
- Test and development of a Kubernetes workload in the cloud following replication
- Replication of file services from ONTAP Select to Cloud Volumes ONTAP

6 Technology Requirements

This section covers the technology requirements for the NetApp HCI for Multicloud Data Protection with Cloud Volumes ONTAP validated solution. Individual customer requirements might vary.

For more information about the technical requirements and for installation guidance on NetApp HCI, see the NetApp HCI Resources page.

6.1 Hardware Requirements

Table 1 lists the hardware components that were used to implement the solution. The hardware components that are used in any particular implementation of the solution might vary based on customer requirements.

Table 1) Hardware requirements.

Layer	Product Family	Quantity	Details
Compute	NetApp H500E	4	2 x Intel E5-2650 v4; 12 cores; 2.2GHz 512GB RAM
Storage	NetApp H500S	4	6 x 960GB encrypting/nonencrypting

6.2 Software Requirements

Table 2 lists the software components that were used to implement the solution. The software components that are used in any particular implementation of the solution might vary based on customer requirements.

Table 2) Software requirements.

Software	Software	Version
Storage	NetApp Element software	11
	NetApp ONTAP Select	9.5
	NetApp Trident	19.04
	NetApp Deployment Engine	1.4
On-Premises Compute	VMware vSphere ESXi	6.5 U2
	VMware vCenter Server	6.5
	Red Hat Enterprise Linux	7.6
	Red Hat OpenShift Container Platform	3.11
Public Cloud Resources	Kubernetes deployed via NKS	1.14
	NetApp Cloud Volumes ONTAP	9.5
	Debian Linux	9.9
	NetApp Cloud Manager	3.7

6.3 Licensing Requirements

The following components in the solution have license requirements:

- VMware vSphere
- VMware vCenter Server Enterprise Plus
- Red Hat OpenShift Container Platform subscription
- NetApp ONTAP Select
- NetApp Cloud Volumes ONTAP
- NetApp Kubernetes Service

6.4 NetApp Cloud Manager and Public Cloud Considerations

NetApp Cloud Manager is used to manage your data fabric resources across on-premises and multiple cloud environments, including Cloud Volumes ONTAP, Cloud Volumes ONTAP High Availability, NetApp AFF, and NetApp FAS storage systems.

When deploying Cloud Volumes ONTAP, Cloud Manager uses your cloud credentials to run the instance of your choice with either Elastic Computer Cloud (EC2) resources and Elastic Block Storage (EBS) in AWS or VM and Blob storage in Azure.

For AWS deployments, NetApp Cloud Manager is delivered as an Amazon machine image (AMI) by EC2 on the Red Hat Enterprise Linux operating system. When deploying NetApp Cloud Manager, you can select the region to implement the AMI and optionally use AWS Identity and Access Management to provide access control to NetApp Cloud Manager.

For Azure deployments, NetApp Cloud Manager is delivered as an Azure virtual machine by Azure compute on the Red Hat Enterprise Linux operating system. When deploying NetApp Cloud Manager, you must download and modify the NetApp Cloud Central policy for Azure. This JSON file is used to create a custom role in Azure, allowing the deployment of Cloud Manager from Cloud Central onto Azure resources.

The general networking requirements are:

- **Outbound internet access.** Used to connect NetApp Cloud Manager to Cloud Volumes ONTAP and communicate with NetApp AutoSupport® support tool.
- **Virtual Private Cloud (VPC).** Virtual network dedicated to your AWS account, logically isolated from other virtual networks in the AWS cloud.
- **Virtual Network (VNet).** Virtual network dedicated to your Azure account, logically isolated from all other virtual networks in the Azure cloud.
- **Virtual Private Network (VPN).** Used to extend on-premises networks and communicate between Cloud Volumes ONTAP instances, NKS, and others.

For more information about NetApp Cloud Manager ONTAP and Cloud Volumes ONTAP deployment prerequisites and detailed steps, see the NetApp Cloud Manager Documentation.

For more information about networking in AWS, see the Amazon Virtual Private Cloud product page.

For more information about networking in Azure, see the Microsoft Azure networking product page.

6.5 Red Hat OpenShift Container Platform Components

Red Hat OpenShift Container Platform uses Kubernetes to manage containerized applications across a set of hosts. Table 3 lists the components that are required for a successful Red Hat OpenShift Container Platform deployment.

Table 3) Red Hat OpenShift Container Platform components.

Type	Component	Details
Master nodes	API server	The Kubernetes API server acts as a front end for the Kubernetes control plane. It accepts the desired cluster state (YAML or JSON configuration files). Examples of the cluster state include but are not limited to: • Applications or other workloads to run • Container images for your applications and workloads • Allocation of network and disk resources
	Etcd	Etcd stores the cluster state information persistently.
	Controller manager server	The controller manager includes: • **Node controller.** Notices and responds when nodes go down. • **Replication controller.** Maintains the correct number of pods for every replication controller object in the system. • **Endpoints controller.** Populates the endpoints object (that is, joins services and pods). • **Service account and token controllers.** Create default accounts and API access tokens for new namespaces.

Worker nodes	Kubelet	• A kubelet is an agent that runs on each node in the cluster. It makes sure that containers are running in a pod. • The kubelet takes a set of PodSpecs that are provided through various mechanisms and makes sure that the containers that are described in those PodSpecs are running and healthy. The kubelet does not manage containers that were not created by Kubernetes.
	Kube-proxy	Kube-proxy is a service proxy that enables the Kubernetes service abstraction by maintaining network rules on the host and by performing connection forwarding.
Infrastructure nodes	OCR	OCR adds the ability to automatically provision new image repositories on demand. Includes a preprovisioned endpoint to push the application build images.
	OpenShift Container Platform router	This router enables routes that are created by developers to be used by external clients. The routing layer in the OpenShift Container Platform router is pluggable, and several router plug-ins are provided and are supported by default.

6.6 Design Considerations for Deploying Red Hat OpenShift Container Platform with NetApp HCI

NetApp HCI leverages VMware ESXi as the hypervisor and VMware vCenter Server for centralized management of VMs, ESXi hosts, and other dependent components. All the OpenShift nodes are deployed as Red Hat Enterprise Linux 7.5 VMs on NetApp HCI.

6.7 Storage Elements in Red Hat OpenShift Container Platform

Trident enables dynamic provisioning of enterprise-class storage from NetApp Element software-based NetApp HCI all-flash storage nodes. Kubernetes 1.4 introduced support for storage classes, which allow you to specify the provisioner and additional details such as QoS levels and media types.

Consider the following details with Trident:

- Deploy Trident on OpenShift infrastructure nodes along with other OpenShift services such as OCR or OpenShift Platform router.
- Create a Trident user in Element with access privileges to read, volumes, accounts, and ClusterAdmins resource types.
- Use CHAP authentication to provide access to PVs in the nodes. Set UseCHAP to True in the Trident storage back end.
- Consider storage pools to create different storage classes that correspond to different QoS bands.
- For generic use cases with no specific QoS requirements, create a default storage class that specifies Trident as the storage provisioner and uses the default QoS settings in Element software.

6.8 NetApp Cloud Central Considerations

Each Cloud Manager system is associated with a NetApp Cloud Central account. A Cloud Central account is a container for your Cloud Manager systems and the workspaces in which users deploy Cloud Volumes ONTAP. A single Cloud Central account can include multiple Cloud Manager systems that serve

different business needs. You can get started with Cloud Volumes ONTAP in AWS or Azure from NetApp Cloud Central.

6.9 NetApp Cloud Volumes ONTAP

The Cloud Manager intuitive wizard creates the necessary logical constructs, networking details, and client access settings to enable an administrator to create a working environment with a few clicks.

When you deploy Cloud Volumes ONTAP, you can choose a preconfigured system that matches your workload requirements, or you can create your own configuration. If you choose your own configuration, you should understand the options available to you.

Cloud Volumes ONTAP License Type

Cloud Volumes ONTAP is available in AWS and Azure in two pricing options: pay-as-you-go and Bring Your Own License (BYOL). For pay-as-you-go, you can choose from three licenses: Explore, Standard, or Premium. Each license offers different capacity and compute options. Users are also provided a free trial with full functionality to get a first-hand experience of the offerings.

Cloud Volumes ONTAP Storage Limits

The raw capacity limit for a Cloud Volumes ONTAP system is tied to the license. Additional limits affect the size of aggregates and volumes. You should be aware of these limits as you plan your configuration. See Storage limits for Cloud Volumes ONTAP 9.5 for storage limits for different Cloud Volumes ONTAP versions.

Note: SnapMirror replication of Element to Cloud Volumes ONTAP is supported starting with ONTAP 9.5 and Element 11.0.

Cloud Volumes ONTAP Sizing

Sizing your Cloud Volumes ONTAP system helps you meet requirements for performance and capacity. You should be aware of a few key points when choosing an instance type, disk type, and disk size.

Table 4) Cloud Volumes ONTAP sizing considerations.

Public Cloud	Consideration	Details
AWS	Instance type	• Match your workload requirements to the maximum throughput and IOPS for each EC2 instance type. • If several users write to the system at the same time, choose an instance type that has enough CPUs to manage the requests. • If you have an application that is mostly reads, then choose a system with enough RAM.
	EBS disk type	• General purpose SSDs are the most common disk type for Cloud Volumes ONTAP.

Public Cloud	Consideration	Details
	EBS disk size	• All disks in an aggregate must be the same size. • The performance of EBS disks is tied to disk size. The size determines the baseline IOPS and maximum burst duration for SSDs and the baseline and burst throughput for HDDs. • Choose the disk size that gives you the sustained performance that you need. • EC2 instance bandwidth limits can affect the actual IOPS available to the instance.
Microsoft Azure	Virtual machine type	• Review release notes of the Cloud Volumes ONTAP version you want to deploy for information about the supported VM type. • Each VM type supports a specific number of data disks.
	Azure disk type	• HA Cloud Volumes ONTAP instances use premium page blobs. • Single-node Cloud Volumes ONTAP instances can use three types of Azure Managed disks: Premium SSD managed disks, Standard SSD managed disks, and Standard HDD managed disks.
	Azure disk size	• All disks in an aggregate must be the same size. • The performance of Azure Premium Storage is tied to the disk size. Larger disks provide higher IOPS and throughput. • There are no performance differences between disk sizes for Standard storage. Choose a disk size based on the capacity that you need.

Cloud Volumes ONTAP Write Speed

Cloud Manager enables you to choose either normal write speed or high write speed for single-node Cloud Volumes ONTAP systems. With normal write speed, data is written directly to disk, thereby reducing the likelihood of data loss in the event of an unplanned system outage. With high write speed, data is buffered in memory before it is written to disk, which provides faster write performance. Due to this caching, there is the potential for data loss if an unplanned system outage occurs. High write speed is a good choice if fast write performance is required for your workload and you can withstand the risk of data loss in the event of an unplanned system outage.

Note: If you enable high write speed, you should provide write protection at the application layer.

Cloud Volumes ONTAP Volume Usage Profile

ONTAP includes several storage efficiency features that can reduce the total amount of storage needed. When you create a volume in Cloud Manager, you can choose a profile that enables these features or a profile that disables them.

Table 5) ONTAP storage efficiency features.

Feature	Details
Thin provisioning	Presents more logical storage to hosts or users than you actually have in your physical storage pool. Instead of preallocating storage space, storage space is allocated dynamically to each volume as data is written.
Deduplication	Improves efficiency by locating identical blocks of data and replacing them with references to a single shared block. This technique reduces storage capacity requirements by eliminating redundant blocks of data that reside in the same volume.
Compression	Reduces the physical capacity required to store data by compressing data within a volume on primary, secondary, and archive storage.

Cloud Volumes ONTAP Networking Information

When you deploy Cloud Volumes ONTAP in a public cloud, you need to specify details about your virtual network. You can use the worksheet in Table 6 to collect the information from your administrator.

Table 6) Cloud Volumes ONTAP networking information.

Public Cloud	Consideration	Details
AWS	Region	
	VPC	
	Subnet	
	Security group (if using your own)	
Microsoft Azure	Region	
	VNet	
	Subnet	
	Security group (if using your own)	

Note: Review AWS documentation for deploying Cloud Volumes ONTAP in an HA pair across multiple availability zones.

Outbound Internet Access for Cloud Volumes ONTAP Nodes

Cloud Volumes ONTAP nodes require outbound internet access to send messages to NetApp AutoSupport, which proactively monitors the health of your storage.

Routing and firewall policies must allow AWS HTTP and HTTPS traffic to the following endpoints so that Cloud Volumes ONTAP can send AutoSupport messages:

- https://support.netapp.com/aods/asupmessage
- https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.hw-metrocluster-tiebreaker%2FGUID-EB722A3D-C181-42CB-BBF7-5AEC4AEBD92C.html

If you have an NAT instance, you must define an inbound security group rule that allows HTTPS traffic from the private subnet to the internet.

7 Networking Topology

7.1 Necessary VLANs

NetApp HCI deployment requires multiple logical network segments, one for each of the following types of traffic:

- Management
- VMware network
- VMware vMotion
- iSCSI Storage

Table 7 lists the necessary VLANs for deployment, as outlined in this validation. NetApp recommends configuring these VLANs on the network switches before executing the NDE.

Table 7) Required VLANs.

Network	Details	VLAN ID
Out-of-band management network	Network for HCI terminal user interface (TUI)	16
In-band management network	Network for accessing management interfaces of nodes, hosts, and guests	3496
VMware vMotion	Network for live migration of VMs	3495
SAN storage	Network for iSCSI storage traffic	3494
NAS storage	Network for NFS storage traffic	3493
VM network	Network for VM traffic	3490

7.2 Network Design Considerations for Red Hat OpenShift Container Platform

OpenShift uses virtual extensible LAN (VXLAN) overlay networking for pod networks. This deployment was validated with the ovs-multitenant plug-in that enables project-level isolation between pods and services.

The different network traffic types in OpenShift are isolated by using VLANs. The following port groups with corresponding VLAN tags are created:

- **Management.** In-band management network.
- **Storage network.** iSCSI network for persistent storage.
- **Intracluster traffic.** The overlay OpenShift network.
- **Cluster egress traffic.** External traffic for services.

7.3 AWS Network Considerations

The networking of the AWS environment must be set up so that the Cloud Volumes ONTAP and NKS instances in AWS can operate properly with the on-premises HCI resources.

Connections to Storage Systems in Other Networks

To replicate data between a Cloud Volumes ONTAP system in AWS and storage systems in other networks, you must have a VPN connection between the AWS VPC and the other network—for example, an Azure VNet or your corporate network.

For instructions, see the AWS documentation: Setting Up an AWS VPN Connection.

This VPC configuration is a hybrid cloud configuration in which Cloud Volumes ONTAP becomes an extension of your private environment. The configuration includes a private subnet and a virtual private gateway with a VPN connection to your network. Routing across the VPN tunnel allows EC2 instances to access the internet through your network and firewalls. You can run Cloud Manager in the private subnet or in your data center. You would then launch Cloud Volumes ONTAP in the private subnet.

A VPC with this configuration includes public and private subnets, an internet gateway that connects the VPC to the internet, and a NAT gateway or NAT instance in the public subnet that enables outbound internet traffic from the private subnet. In this configuration, you can run Cloud Manager in a public subnet or a private subnet, but NetApp recommends the public subnet because it allows access from hosts outside the VPC. You can then launch Cloud Volumes ONTAP instances in the private subnet.

7.4 Azure Network Considerations

The networking of the Azure environment must be set up so that the Cloud Volumes ONTAP and NKS instances in Azure can operate properly with the on-premises HCI resources.

Connections to Storage Systems in Other Networks

To replicate data between a Cloud Volumes ONTAP system in Azure and storage systems in other networks, you must have a VPN connection between the Azure VNet and the other network—for example, an AWS VPC or your corporate network.

For instructions, see Microsoft Azure Documentation: Create a Site-to-Site connection in the Azure portal.

This VNet configuration is a hybrid cloud configuration in which Cloud Volumes ONTAP becomes an extension of your private environment. The configuration would be defined as a site-to-site VPN gateway connection from your on-premises network to the VNet.

8 Deployment

The steps to deploy the NetApp HCI with Cloud Volumes ONTAP and NKS solution are beyond the scope of this document. The high-level steps include:

- Virtual infrastructure implementation with the NDE HCI
- Containers implementation on the premises
- Configuration of data protection relationships

Virtual infrastructure implementation with the NDE has these high level-steps:

- NDE execution prerequisites
- NDE execution
- Post-NDE configuration

Container implementation on the premises has these high level-steps:

- Deploy and configure Red Hat Enterprise Linux VMs for OpenShift
- Deploy the Red Hat OpenShift Container Platform
- Deploy and configure NetApp Trident
- Deploy other OpenShift components

Cloud resource configuration has these high level-steps:

- Review cloud deployment prerequisites for AWS and Microsoft Azure
- Deploy Cloud Volumes ONTAP with Cloud Central in AWS and Microsoft Azure

- Deploy NKS with Cloud Central in AWS and Microsoft Azure
- Deploy and configure NetApp Trident

Data protection relationship configuration has these high level-steps:

- Enablement of SnapMirror
- Creation of SnapMirror endpoints
- Creation of destination volumes
- Initialization of the SnapMirror relationship

9 Solution Operations

NetApp SnapMirror integration with NetApp HCI and Cloud Volumes ONTAP allows a variety of use cases that add value for customers with respect to hybrid multicloud deployments. These use cases include:

- Backup and restore HCI storage to Cloud Volumes ONTAP
- Disaster recovery to the public cloud
- Development and test in the public cloud
- Backup and restore ONTAP Select to Cloud Volumes ONTAP

9.1 Backup and Restore HCI Storage to Cloud Volumes ONTAP

Keeping local Snapshot copies of volumes in your NetApp HCI deployment is the first line of protection against unexpected data loss. However, the cost of storing many idle Snapshot copies on more expensive SSDs can quickly become prohibitive. NetApp SnapMirror allows you to transfer data from the on-premises Element cluster in your NetApp HCI environment to a remote ONTAP system in the public cloud. This relationship can be configured as a SnapVault volume for archival purposes to store these Snapshot copies for an extended period on Cloud Volumes ONTAP. This enables the removal of the Snapshot copies on the source NetApp HCI system, resulting in saving storage space and infrastructure costs. After Snapshot copies are moved to the cloud, the ability to make copies instantly, operate without retention limits, and support single-file recovery are differentiators of Cloud Volumes ONTAP.

9.2 Disaster Recovery to the Public Cloud

By offering efficient data replication and a rich set of data management tools and partnerships, NetApp helps businesses recover from unplanned IT outages. NetApp SnapMirror enhances disaster recovery options by using converged infrastructure and NetApp HCI. SnapMirror improves business continuity on an Element system by replicating Snapshot copies of an Element volume to a Cloud Volumes ONTAP instance when an on-site application is not accessible. If there is a disaster at the Element site, you can serve data to clients from the Cloud Volumes ONTAP instance and then reactivate the Element system when service is restored.

9.3 Development and Test in the Public Cloud

SnapMirror technology can be used to distribute large amounts of data throughout the enterprise and to the public cloud, enabling access to data at remote locations. Having datasets in the public cloud allows clients in the cloud to access copies of the production workload. These copies consume minimal space because they are cloned with FlexClone technology and modified as developers continue to work with persistent volumes imported with Trident in NKS.

The replication of datasets enables the efficient and predictable use of network and server resources, because SnapMirror operations can be scheduled at a predetermined replication time. Storage administrators can replicate production data at a specific time to minimize overall network usage. After

data is in the public cloud, development and test of Kubernetes applications can occur on cloud resources, mirrored back to the on-premises data center, and then moved into production when ready. Cloud Volumes ONTAP delivers the storage efficiencies of ONTAP, such as thin provisioning, deduplication, and compression, which allows you to consume fewer cloud resources as development continues.

9.4 Backup of and Restore of ONTAP Select to Cloud Volumes ONTAP

In addition to the Element operations described previously, file services in NetApp HCI can be protected with Cloud Volumes ONTAP. Volumes created on the ONTAP Select system, running as a virtual guest in a NetApp HCI solution, can establish a replication relationship with another ONTAP system provisioned on the premises or in the cloud. The volumes can be a destination for either mirror or vault purposes, enabling data to be easily and rapidly transferred between the two environments.

10 Conclusion

NetApp has embraced the customer's need for a hybrid multicloud strategy. The data fabric powered by NetApp SnapMirror allows customers to gain control of their data whether it resides on the premises or in the public cloud. SnapMirror functionality between Element and ONTAP extends the data fabric with NetApp HCI systems for both SAN and NAS datasets. NetApp SnapMirror provides increased data protection options for Element while using the robust data management capabilities of ONTAP with Cloud Volumes ONTAP in the cloud. You can also take advantage of these new data mobility options to enable backup, disaster recovery, and development and test of a variety of workloads.

Where to Find Additional Information

To learn more about the information that is described in this document, review the following documents and/or websites.

Product Documentation

- What is the Data Fabric?
  www.netapp.com/us/info/what-is-data-fabric.aspx
- NetApp Cloud Central
  https://cloud.netapp.com
- NetApp Cloud Manager
  https://cloud.netapp.com/cloud-manager
- NetApp Cloud Volumes ONTAP
  https://cloud.netapp.com/ontap-cloud
- NetApp Kubernetes Service
  https://cloud.netapp.com/kubernetes-service
- NetApp Element Software
  https://www.netapp.com/us/products/data-management-software/element-os.aspx
- NetApp HCI
  https://www.netapp.com/us/products/converged-systems/hyper-converged-infrastructure.aspx
- NetApp ONTAP Software
  https://www.netapp.com/us/products/data-management-software/ontap.aspx
- NetApp ONTAP Select
  https://www.netapp.com/us/products/data-management-software/ontap-select-sds.aspx
- NetApp SnapMirror Data Replication
  https://www.netapp.com/us/products/backup-recovery/snapmirror-data-replication.aspx

- NetApp Trident
  https://www.netapp.com/us/media/ds-netapp-project-trident.pdf

Technical Documentation

- TR-4015: SnapMirror Configuration and Best Practices Guide
  www.netapp.com/us/media/tr-4015.pdf
- TR-4651: NetApp SolidFire SnapMirror Architecture and Configuration
  https://fieldportal.netapp.com/content/616239
- ONTAP 9: Replication between NetApp Element Software and ONTAP
  https://library.netapp.com/ecm/ecm_download_file/ECMLP2834698
- TR-4517: ONTAP Select, Product Architecture and Best Practices
  www.netapp.com/us/media/tr-4517.pdf
- ONTAP 9 Documentation Center
  http://docs.netapp.com/ontap-9/index.jsp
- ONTAP Data Protection Power Guide
  https://library.netapp.com/ecm/ecm_download_file/ECMLP2811525
- NetApp Converged Systems
  www.netapp.com/us/products/converged-systems/index.aspx
- NetApp HCI Theory of Operations
  www.netapp.com/us/media/wp-7261.pdf
- Element Software Product Library
  https://mysupport.netapp.com/documentation/productlibrary/index.html?productID=62480
- NetApp Trident Documentation
  https://netapp-trident.readthedocs.io/en/stable-v18.07/index.html

Support and Partner Documentation

- NetApp Azure partner page
  https://cloud.netapp.com/azure-partners
- NetApp Google Cloud Platform partner page
  https://cloud.netapp.com/google-partners
- NetApp AWS partner page
  https://cloud.netapp.com/aws-partners
- NetApp Interoperability Matrix Tool
  https://mysupport.netapp.com/matrix/#welcome
- NetApp Support
  https://mysupport.netapp.com/
- NetApp Active IQ
  www.netapp.com/us/products/data-infrastructure-management/active-iq-predictive-technology.aspx

Version History

Version	Date	Document Version History
Version 1.0	June 2019	Initial release

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.

Copyright Information

Trademark Information

NVA-1137-0619