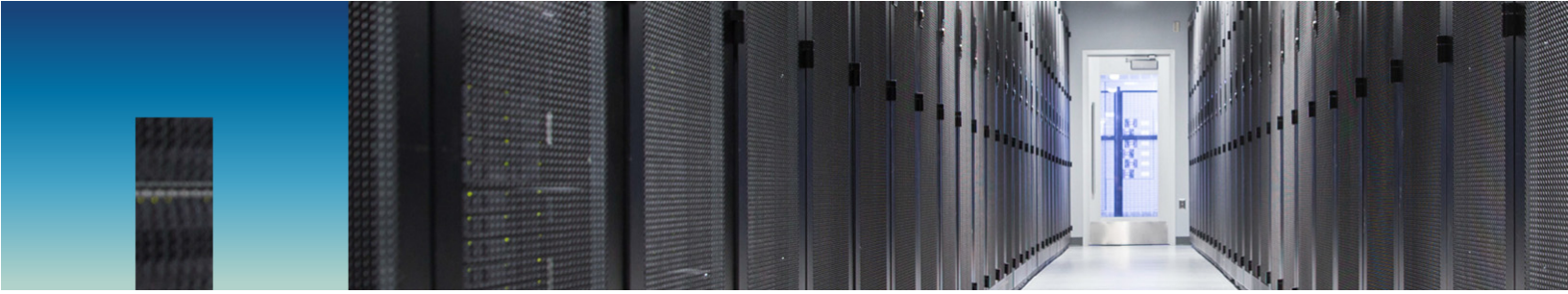


Technical Report

Build Your Data Fabric

With NetApp HCI, ONTAP, and Converged Infrastructure

Alan V. Cowles, Christopher Reno, Lindsey Street
March 2019 | TR-4748

Abstract

To enable data protection and mobility across the data fabric, including NetApp® converged systems, NetApp SnapMirror® replication technology provides disaster recovery and data transfer between NetApp Element® software and NetApp ONTAP® enabled systems. NetApp integration with VMware, when combined with VMware features, simplifies the administration of virtual environments. This report explores use cases related to infrastructure interoperability, disaster recovery, and data migration in the context of NetApp converged infrastructure and NetApp HCI.

NetApp®

TABLE OF CONTENTS

LIST OF FIGURES

1 Introduction

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 multiple cloud environments. These endpoints can include systems using NetApp® ONTAP® software or NetApp Element® software. The data fabric simplifies and integrates data management across cloud and on the premises to accelerate digital transformation.

For more information, see What Is a Data Fabric?

NetApp converged systems, including converged infrastructure, and NetApp HCI take advantage of robust data storage software. NetApp converged infrastructures include NFLEX™ Converged Infrastructure from Fujitsu and NetApp and FlexPod® data center solution from NetApp and Cisco, and use ONTAP for NAS (CIFS/NFS) and SAN (FC/FCoE/iSCSI) services. NetApp HCI is a hybrid cloud infrastructure solution that is capable of transforming and empowering organizations to move faster, drive operational efficiencies, and reduce costs. NetApp HCI systems are deployed with Element software, providing native SAN (iSCSI) services and file services through NetApp ONTAP Select. Because of the diversity of application requirements, both converged infrastructure and NetApp HCI are necessary in today's operational paradigm, provided that they can communicate and share data across a data fabric. The mobility between these systems helps eliminate data silos and allows customers to choose which solution is right for a given application, workload, or use case.

For more information about NetApp HCI and converged infrastructure, see NetApp Converged Systems.

1.1 Theory of Operations

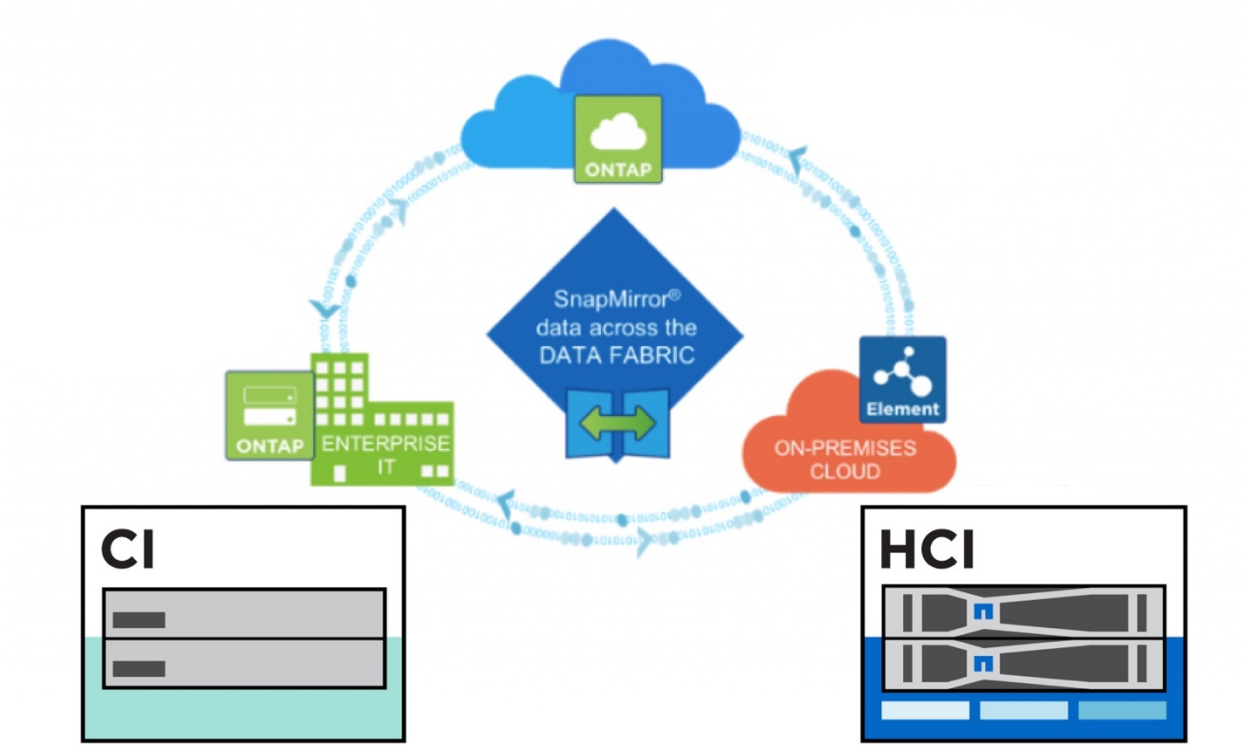
NetApp SnapMirror® replication technology provides disaster recovery and data transfer between Element software and ONTAP enabled systems, offering data protection for converged infrastructure and NetApp HCI systems across the data fabric. SnapMirror creates a replica, or mirror, of your working data 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 enables clusters and volumes to exchange data securely.

Beginning with 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 back to an Element volume. This replication is accomplished through the ONTAP CLI and the Element API and GUI.

Figure 1 illustrates two on-premises options for the data fabric with converged infrastructure and NetApp HCI.

Figure 1) Data fabric powered by NetApp.



SnapMirror is a NetApp Snapshot replication technology that facilitates disaster recovery and is designed for failover from primary storage to secondary storage at a geographically remote site. SnapMirror technology creates a replica, or mirror, of the working data in secondary storage from which you can continue to serve data if an outage occurs at the primary site.

SnapMirror runs natively on the ONTAP controllers and is now integrated into Element, which runs on NetApp HCI and NetApp SolidFire® clusters. The logic to control SnapMirror resides in ONTAP software; therefore all SnapMirror relationships must involve at least one ONTAP system to perform the coordination work. Relationships between Element and ONTAP clusters can be managed primarily through the Element UI; however, some management tasks reside in OnCommand® System Manager. You can also manage SnapMirror through the CLI and API, which are both available in ONTAP and Element.

In its simplest configuration, a mirror relationship is the relationship between a source volume and a destination volume. Data is replicated to the destination volume through NetApp Snapshot copies.

Typically, the source volume is a read/write volume that clients can access and modify. The destination volume is a read-only volume that can export a Snapshot copy to clients for read-only access.

Snapshot copies are used by the source volume to update destination volumes. The copies are transferred from the source volume to the destination volume through an automated or manual schedule, which means that mirror copies are updated asynchronously.

Updates are asynchronous and follow the schedule configured in the SnapMirror policy. You can activate the destination volume with minimal disruption if a disaster occurs at the primary site and reactivate the source volume after service is restored.

Because SnapMirror transfers Snapshot copies only after the baseline is created, replication is fast and nondisruptive. If comparable performance is the design objective, you must confirm that the FAS controllers on the ONTAP system are near-comparable equivalents to the primary Element based system.

Figure 2) NetApp SnapMirror.

High-level features supported by SnapMirror for Element include:

- Replication of a volume created with Element to an ONTAP LUN in an ONTAP volume
- Replication of a LUN created with ONTAP to an Element volume
- Baseline and incremental transfers
- Use of Element volumes on ONTAP as ONTAP LUNs
- Disaster recovery

For general technical information about NetApp SnapMirror, see TR-4015: SnapMirror Configuration and Best Practices Guide.

For more information about NetApp SnapMirror with Element and ONTAP, see TR-4651: NetApp SolidFire SnapMirror Architecture and Configuration (login required).

1.2 Architectural Design

There are various ways to deploy NetApp converged infrastructure and NetApp HCI systems based on varying customer needs. NetApp Converged Systems Advisor (CSA) verifies that the data center infrastructure is deployed according to best practices and in a supported manner. The NetApp Deployment Engine (NDE) eliminates most of the day zero manual steps that it takes to deploy the infrastructure, and the VMware VCP makes ongoing management simple and intuitive.

For more information about NetApp CSA, see the CSA Datasheet.

For more information about NetApp HCI, NDE, and Element integration with VMware, see WP: NetApp HCI Theory of Operations.

This report assumes the simultaneous and ongoing operational model of converged infrastructure and NetApp HCI coexisting in a shared VMware customer environment. Depending on the customer requirements and design, converged infrastructure storage and compute resources could be added to a NetApp HCI VMware vCenter Server environment, or vice versa. Also, both converged infrastructure and NetApp HCI resources could be joined to an external VMware vCenter Server environment or to a dedicated management infrastructure.

This guide uses the NetApp HCI system, vCenter Server environment, and NetApp Element Plug-In for VMware vCenter Server, which are deployed using NDE. Later, converged infrastructure resources are

added to this virtual infrastructure, including the Virtual Storage Console (VSC) 7.2 for VMware vSphere for management of ONTAP systems.

Figure 3 is an example high-level overview of the connectivity assumed in this technical report.

Figure 3) NetApp HCI and converged infrastructure.

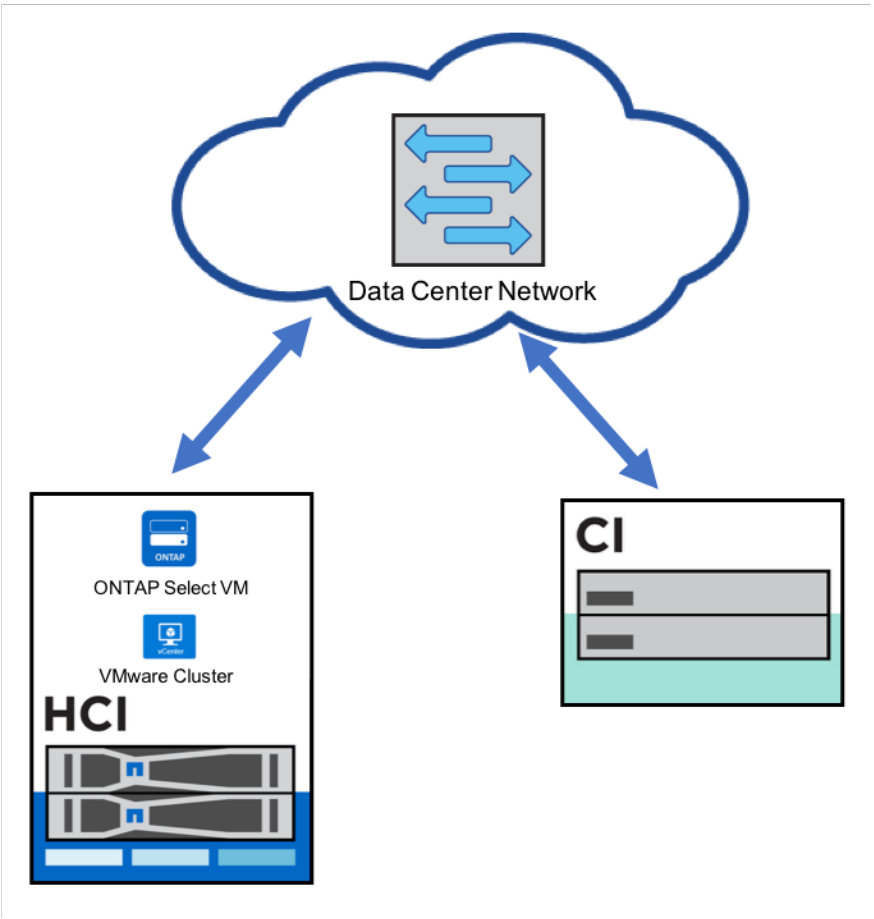


Figure 4 is an example of network connectivity for a NetApp converged infrastructure.

Figure 4) NetApp converged infrastructure network.

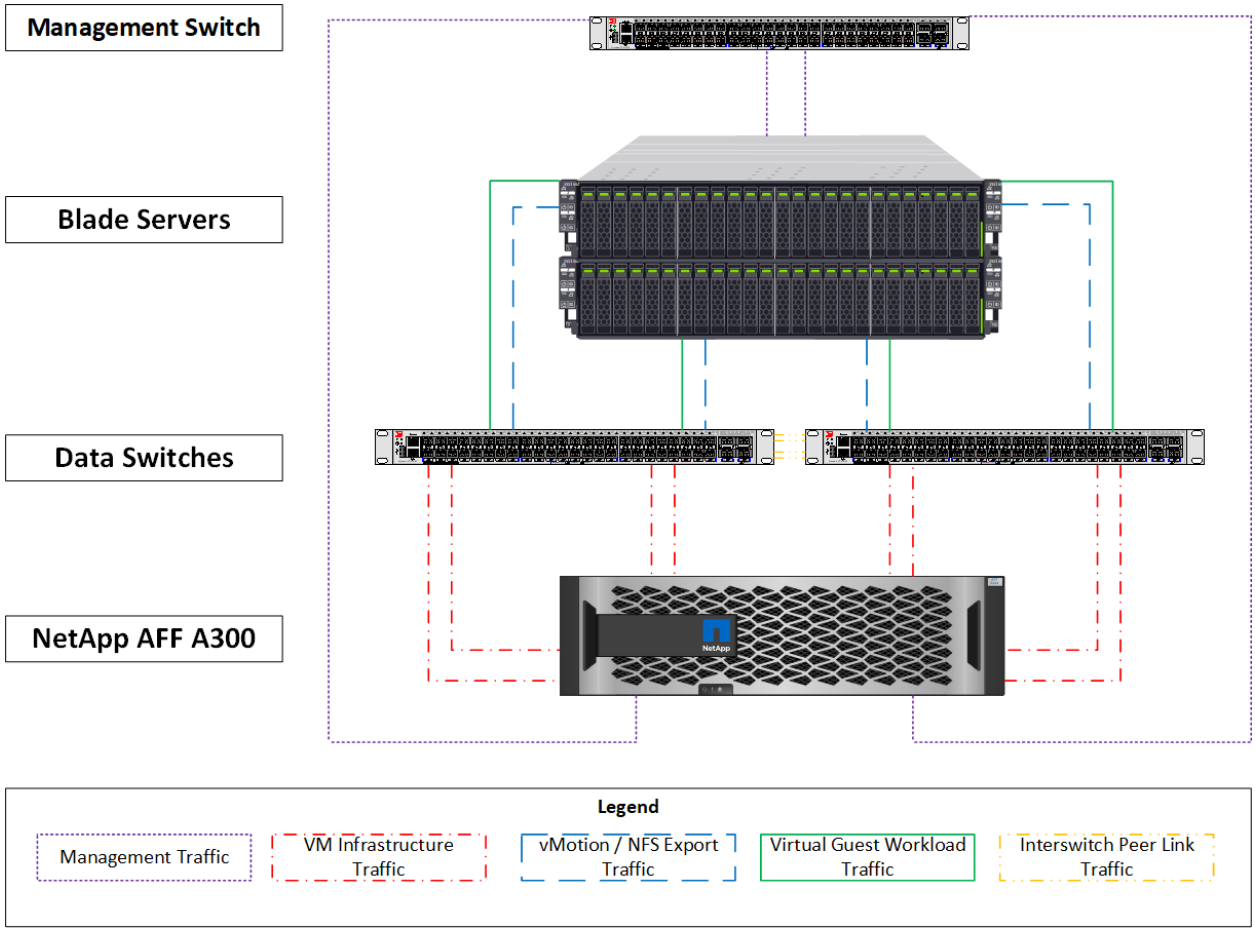


Figure 5 is an example of network connectivity for NetApp HCI with a two-compute cable design.

Figure 5) NetApp HCI network.

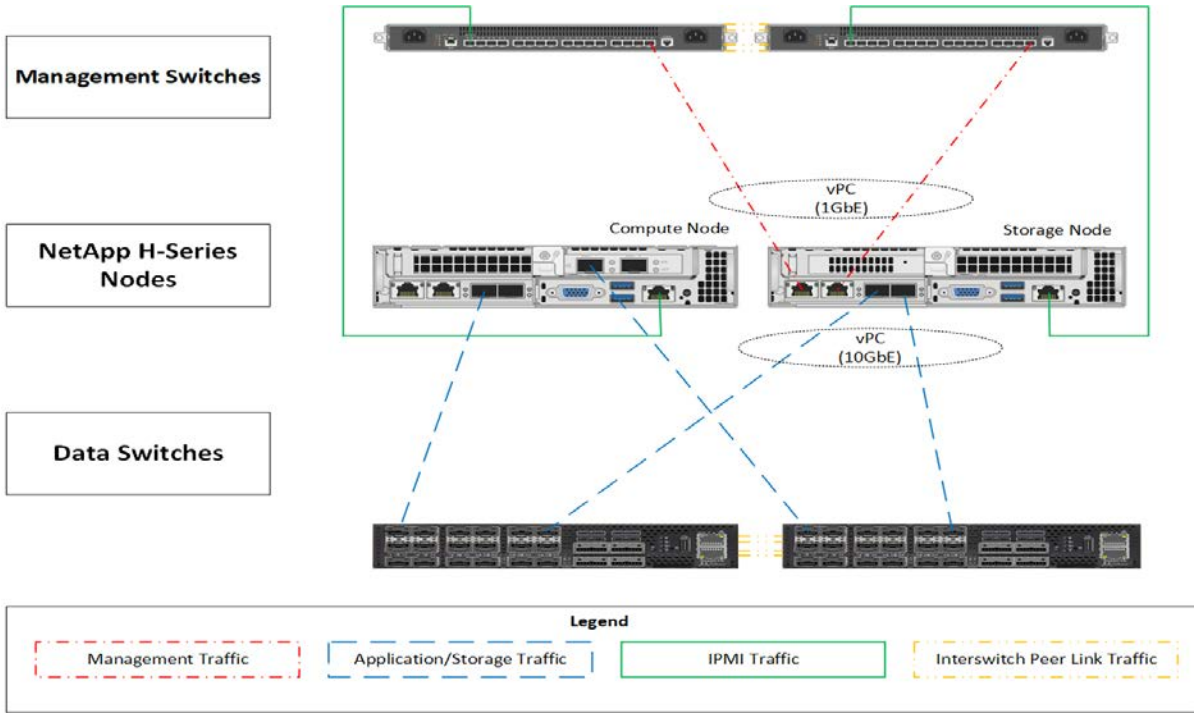


Figure 6 shows the logical design of a common vCenter Server for NetApp HCI and converged infrastructure systems.

Figure 6) Virtual infrastructure.

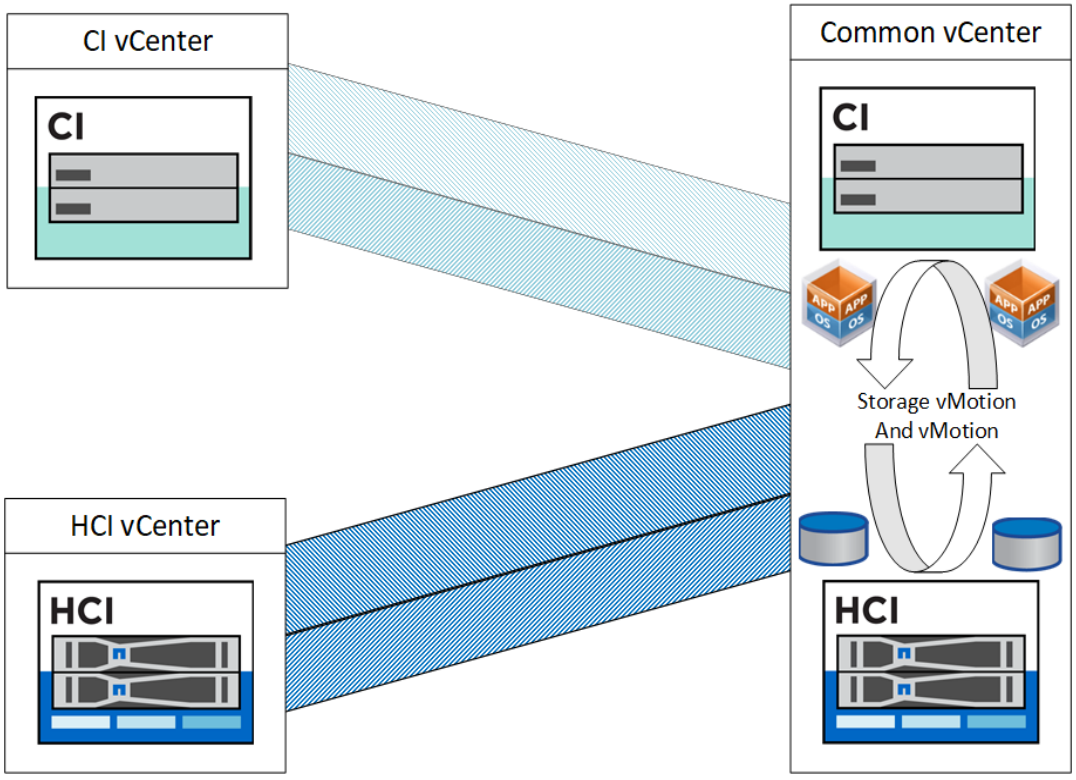
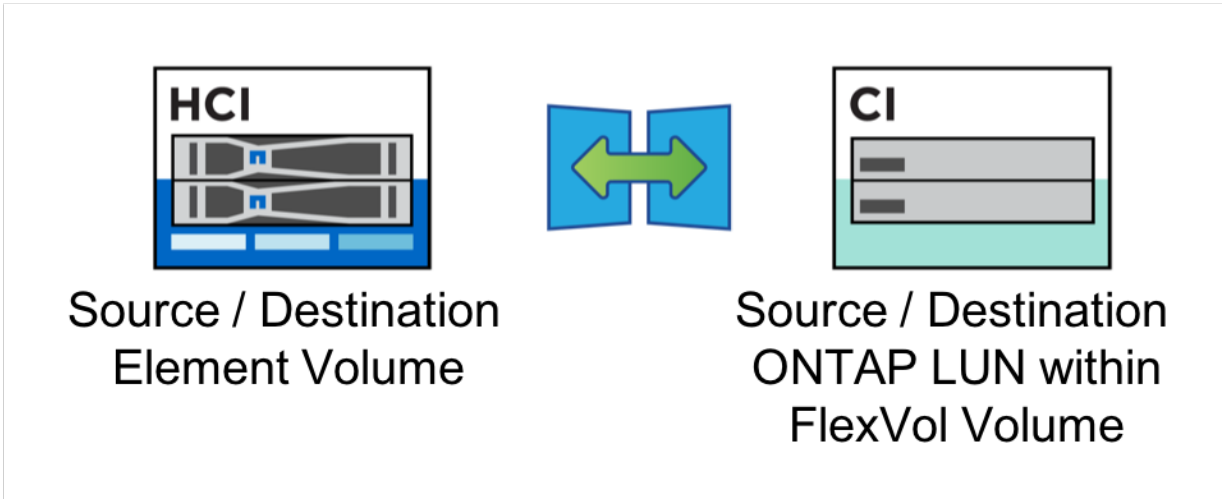


Figure 7 shows the logical design components of a SnapMirror peer relationship with ONTAP and Element systems.

Figure 7) SnapMirror peer relationship with Element and ONTAP systems.



2 Use Cases

There are various use cases in which NetApp converged infrastructure and NetApp HCI work together with the data fabric. This helps prevent data silos when compared with third-party HCI or converged infrastructure systems. On NetApp HCI, data can easily flow to and from NetApp converged infrastructure solutions. Also, converged infrastructure and NetApp HCI systems can be physically and virtually attached in the same data center. The use cases detailed in this technical report focus on infrastructure interoperability and data mobility.:

Infrastructure interoperability:

- NetApp HCI and converged infrastructure systems are supported by NetApp with a single call
- OS and legacy compute hosts storage access
- Bidirectional storage access and administration
- File services including virtual desktop infrastructure (VDI) considerations for end-user computing (EUC) environments

Data protection, disaster recovery, and mobility:

- Backups from NetApp HCI and converged infrastructure systems can be accomplished with each other, through integration with third-party backup software, and with cloud resources
- Data fabric SnapMirror data movement between converged infrastructure ONTAP based systems and NetApp HCI Element for failover and failback of NetApp HCI to converged infrastructure
- Data migration from converged infrastructure to NetApp HCI and from NetApp HCI to converged infrastructure

2.1 Infrastructure Interoperability

NetApp converged infrastructure provides high availability (HA) to applications and speeds time to deployment, especially for traditional workloads. NetApp HCI provides simple, scalable resources that allow you to confidently consolidate applications while controlling costs. NetApp converged infrastructure and NetApp HCI systems are supported in the same data center architecture to allow the deployment of various workloads and use cases.

There are many variables to consider when deploying workloads in a customer data center. Instead of monolithic, application-centric servers, IT prefers the resource-sharing capabilities of public and private clouds deployed on NetApp converged infrastructure and NetApp HCI. Driven by the development of virtual machines (VMs), these clouds allocate compute, memory, and storage resources as needed.

When deploying workloads that require design simplification and cost control through true multitenancy and an incrementally scalable architecture, look to NetApp HCI. When considering workloads that need high performance and HA, look to NetApp converged infrastructure.

A data fabric is a way to manage data, both on the premises and in the cloud, using a common structure and architecture. A data fabric offers efficient data transport, software-defined management, and a consistent data format, allowing data to move more easily among clouds. This approach is what allows hybrid clouds to operate in enterprise application environments.

NetApp Support

The NetApp support organization works closely with customers to improve outcomes by using proven tools and processes. NetApp SupportEdge service mitigates support issues and helps achieve superior levels of availability for customer enterprise data environments. SupportEdge services combine the industry-leading advanced predictive intelligence of NetApp Active IQ® with 24/7/365 support. Active IQ can automatically identify problems before they affect your business, open cases, and even send out hardware. You can depend on NetApp SupportEdge services to increase uptime and availability, provide predictive risk analysis, and deliver advanced remote support. NetApp HCI is backed by this world-class support, with a single point of contact for both hardware and software. Support includes 24/7/365 worldwide availability, with 4-hour on-site response for critical system issues.

In addition to supporting NetApp hardware and software products, NetApp offers third-party support for a multiple offering from hardware and software partners. NetApp Solution Support is available for NetApp AFF and FAS arrays that are used as storage for NetApp converged infrastructure.

Solution Support builds on support from SupportEdge Premium by adding a single-point-of-contact support model that covers the infrastructure products and components of a converged infrastructure as defined by a reference architecture. The service also includes a license for the Converged System Advisor (CSA) for NetApp converged infrastructure solutions, which monitor the converged infrastructure and provide information relating to configuration and lifecycle management. The CSA cloud-based portal gives you a consolidated view of your converged infrastructure and, with NetApp Active IQ monitoring, is an efficient and time-saving support tool.

For more information about support options, see NetApp Support.

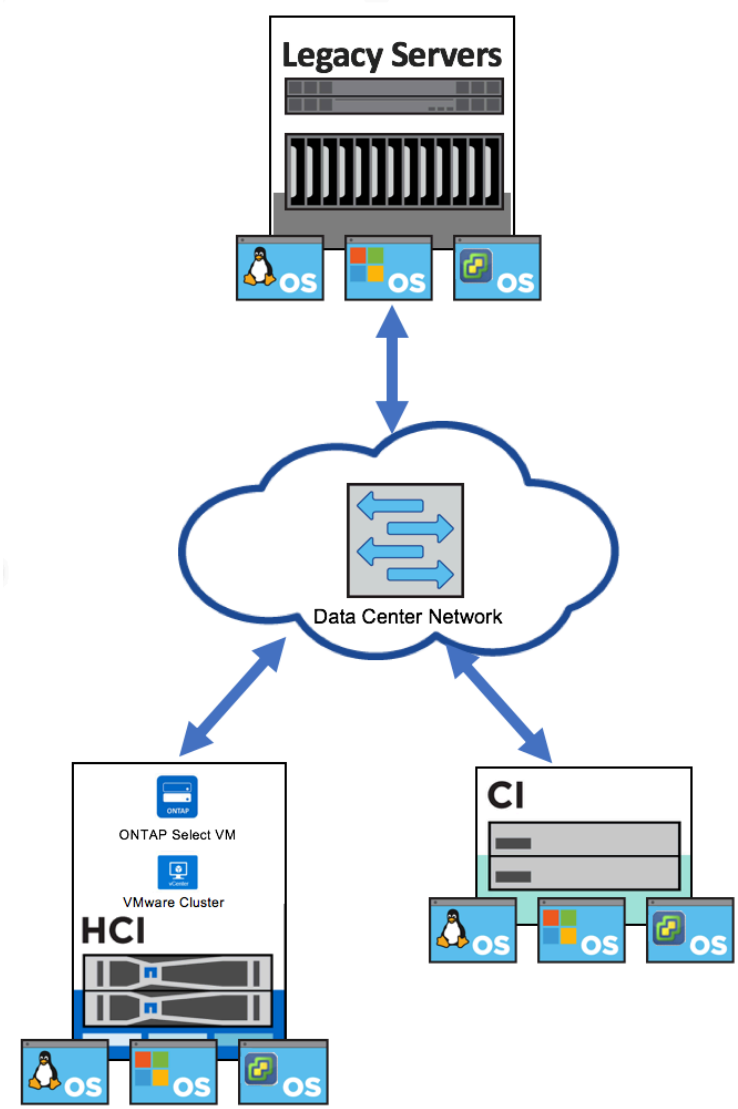
To learn more about actionable intelligence for your infrastructure, see NetApp Active IQ.

OS and Legacy Server Access

In addition to the flexibility and scalability of NetApp HCI and converged infrastructure systems, they both support an open ecosystem. Operating systems beyond vSphere ESXi and hosts outside of the converged systems for accessing the NetApp storage systems are supported.

Figure 8 is a high-level overview of legacy server and third-party OS access.

Figure 8) OS and legacy server access.



The NetApp Interoperability Matrix Tool (IMT) defines the qualified components and versions you can use to build FC/FCoE, iSCSI, NFS, and CIFS configurations with NetApp storage. For every supported ONTAP and Element release listed in the IMT, NetApp supports all subsequent patch releases in that maintenance release stream. NetApp supports all traditional (non-data- center bridging and enhanced 10GbE switches with iSCSI and NAS without specific model reference in the IMT. For FCoE configurations, the IMT lists supported 10GbE switches by specific model reference. NetApp fully supports various third party ecosystems.

For more information about supported components with NetApp storage systems, see the Interoperability Matrix Tool (login required).

For more information about supported components with VMware, see the VMware Compatibility Guide.

Note: For non-VMware OS support on NetApp HCI, consult your sales team.

Bidirectional Storage Access

In a shared VMware vCenter Server environment, customers can easily access converged infrastructure and NetApp HCI storage resources. By using the Element Plug-In for vCenter Server or the VSC for VMware, Element, and ONTAP, administrative tasks can be accomplished with a click of a button.

For more information about NetApp management options with VMware, see Virtual Infrastructure Management.

Converged infrastructure and NetApp HCI systems are the optimal foundation for a VMware virtualized infrastructure. With VMware environments, you can perform workload migrations with VMware vMotion and Storage vMotion. VMware vMotion allows you to change a host or both host and datastore while the VM is running. With Storage vMotion, you can migrate a virtual machine and its disk files from one datastore to another while the VM is running, including moving from disparate storage arrays. You must meet the resource and configuration requirements to perform vMotion and Storage vMotion activities.

For more information about VMware migration, see VMware Docs.

There are certain scenarios in which vMotion and Storage vMotion are not ideal, such as when hosts do not have common network settings, specific host processor configurations are in place, or hosts do not have adequate licensing. For these scenarios, array-based replication such as NetApp SnapMirror is preferable.

Note: Similar to how SnapMirror enables protected relationships for cluster peers that are geographically dispersed, long-distance vMotion enables live migration of workloads across distances of up to 100ms round-trip time. Long-distance vMotion was not tested as part of this technical report.

File Services

ONTAP Select is a virtual appliance that is deployed using NDE. It enables the entire suite of ONTAP features, including file services, to be run in your NetApp HCI environment. The ONTAP system running in the Select VM is fully functional for NetApp storage efficiencies and data protection capabilities. The ONTAP Select instance deployed using NDE is a single node, non-HA instance. ONTAP Select can also be deployed in multinode or HA instances that add support for HA and ONTAP nondisruptive operations, all within a shared-nothing environment.

ONTAP Select can be used for general file services for the NetApp HCI environment, and also with VDI use cases. Using NetApp converged infrastructure and NetApp HCI systems for EUC environments offers flexibility and delivers the experience that customers expect with their local system. Whether deploying with converged infrastructure or NetApp HCI, NetApp offers enterprise-grade features and functionalities to help reduce cost, increase utilization, and improve performance. The virtual infrastructure, virtual desktops, and system images take advantage of NetApp storage efficiencies when deployed on Element or ONTAP systems. In addition to the storage requirements of the infrastructure and the virtual desktops, the needs of end-user home directories, (VDI profiles, and general CIFs or NFS are part of an EUC deployment. These NAS requirements can be satisfied with a converged infrastructure ONTAP system or ONTAP Select with NetApp HCI systems. For example, NetApp storage systems running CIFS eliminate the need for Windows file servers, which improves overall performance and removes overhead.

When your environment expands beyond the capabilities of an ONTAP Select instance, converged infrastructure ONTAP resources can be used as a natural growth path.

For more information about ONTAP Select configurations, see TR-4517: ONTAP Select, Product Architecture and Best Practices.

2.2 Data Protection, Disaster Recovery, and Mobility

SnapMirror technology is a key part of disaster recovery plans. If critical data has been replicated to a different physical location, a serious disaster no longer results in extended periods of application

downtime. Clients can access replicated data across the network until the damage caused by the disaster is repaired. Application servers at the recovery site can access replicated data to restore operations for business-critical applications for as long as necessary to recover the production site. Recovery might include recovery from corruption, natural disaster at the production site, accidental deletion, and so on.

If a disaster requires failover and the primary storage is not lost, SnapMirror offers an efficient means of resynchronizing the primary and disaster recovery sites. When the primary site is back online, SnapMirror resynchronizes the two sites, transferring only changed or new data back to the primary site from the disaster recovery site by reversing the SnapMirror relationships. After the primary production site resumes normal application operations, SnapMirror transfers to the disaster recovery facility without requiring another complete data transfer.

SnapMirror technology can be used to distribute large amounts of data throughout the enterprise, enabling faster access to data at remote locations. It also allows more efficient and predictable use of expensive network and server resources because WAN usage occurs at a predetermined replication time. Storage administrators can replicate production data at a specific time to minimize overall network utilization.

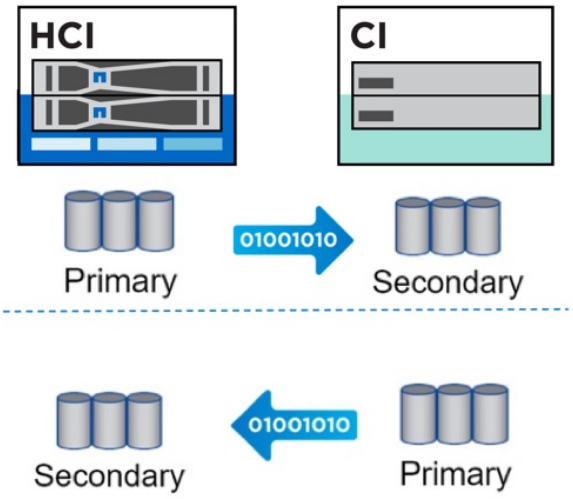
For more information about configuring SnapMirror relationships between converged infrastructure and NetApp HCI, see ONTAP 9: Replication between NetApp Element Software and ONTAP.

NetApp HCI and Converged Infrastructure Backups

NetApp SnapMirror enhances data protection options for NetApp customers who are using converged infrastructure and NetApp HCI systems. Here are some scenarios that customers can use with backup options:

- SnapMirror: NetApp HCI to converged infrastructure (SAN)
- SnapMirror: Converged infrastructure to NetApp HCI (SAN)
- SnapMirror: NetApp HCI to converged infrastructure (NAS) using ONTAP Select
- SnapMirror: Converged infrastructure and NetApp HCI to public cloud
- Third-party backup solutions support

Figure 9) <<Add caption and add a description in the text. I renumbered the rest of the figures in the document.>>



SnapMirror: NetApp HCI to Converged Infrastructure (SAN)

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 your more expensive solid-state drives (SSDs) can quickly become prohibitive. With NetApp SnapMirror Unified Replication, you can transfer data from the local Element system in your NetApp HCI environment to a remote ONTAP system in your converged infrastructure. This relationship can be configured by using SnapMirror for disaster recovery purposes, or by using SnapVault® for archival purposes to store these Snapshot copies for an extended period. With the SnapVault solution, the Snapshot copies can be removed from the source NetApp HCI system, resulting in storage space and infrastructure cost savings.

SnapMirror: Converged Infrastructure to NetApp HCI (SAN)

The ability to create a SnapMirror relationship that flows in the opposite direction is also a valuable asset. This is possible with a data fabric delivered by NetApp. NetApp HCI running Element can be used as a mirror target to transfer data from a production converged infrastructure system running NetApp ONTAP. Another advantage is realized when workloads currently running on converged infrastructure solutions, deployed with traditional or hybrid ONTAP systems, experience performance issues. The data in these environments can be rapidly mirrored to a NetApp HCI counterpart to take advantage of the increased performance provided by the all-flash Element cluster.

SnapMirror: NetApp HCI to Converged Infrastructure and ONTAP Select (NAS)

Volumes created on the ONTAP Select system, running as virtual guests in a NetApp HCI solution, can establish a replication relationship with another ONTAP system provisioned in a NetApp converged infrastructure. The volumes can be a destination for either mirror or vault purposes, enabling easy and rapid data transfer between the two environments.

SnapMirror: Converged infrastructure and NetApp HCI to Public Cloud

With NetApp Cloud Volumes ONTAP, you can create an ONTAP compatible cloud volume in either Amazon Web Services (AWS) or Microsoft Azure cloud and configure those volumes as disaster recovery

destinations. Using NetApp OnCommand Cloud Manager, you can provision the cloud volume and also establish a protection relationship with the ONTAP system in a converged infrastructure deployment, or an Element system in a NetApp HCI deployment. The ability to integrate NetApp Cloud Volumes ONTAP with both converged infrastructure and NetApp HCI systems as an on-demand disaster recovery solution is very appealing if you have a dedicated disaster recovery site, and especially if you do not.

For more information about NetApp Cloud Volumes ONTAP, see https://cloud.netapp.com/home.

For more information about NetApp OnCommand Cloud Manager, see www.netapp.com/us/products/data-infrastructure-management/cloud-manager.aspx.

Third-Party Backup Solutions Support

In addition to the full set of data protection and migration features offered in the data fabric, NetApp has partnered with several third-party vendors, including Commvault and Veeam, to increase the data protection options available to our customers. These third-party applications add an extra layer of functionality to the backup, restore, and disaster recovery processes by enabling more granular management of the converged infrastructure or NetApp HCI environment. This functionality includes specific virtual machines or individual files, all from a centralized dashboard.

With the IntelliSnap solution from Commvault, you can create specific policies that enable you to use the local Snapshot copy functionality on either converged infrastructure or NetApp HCI. From the CommCell Console you can create individualized backup and retention policies for LUNS, volumes, specific VMs, and applications. You can also establish relationships with remote systems that enable data transfer between source and destination. You can do this by using native tools configured either for disaster recovery operations or for simple workload migrations. Commvault IntelliSnap has integration points with NetApp HCI and converged infrastructure systems.

For more information about Commvault integration with ONTAP, see TR-3920: Commvault IntelliSnap for NetApp.

For more information about Commvault integration with Element, see TR-4636: NetApp SolidFire Reference Architecture with Commvault Data Platform v11.

The Veeam backup and replication system solution allows you to select specific files for backup and restore through direct SAN access. The Veeam backup server can mount data LUNs presented by the storage systems used in either converged infrastructure or NetApp HCI deployments. You can then copy individual VMs or individual files from the mounted LUNs to a remote system for disaster recovery. This functionality can also be applied to transfer a workload from one environment to another. As the data center scales up and out, more Veeam backup proxies can be added to handle the additional workload required to protect the entire environment at scale, and to continue to provide rapid backup and restore operations. Veeam has integration points with NetApp HCI and converged infrastructure systems.

For more information about Veeam integration with ONTAP, see Veeam Availability Solutions for Data Protection.

For more information about Veeam integration with Element, see TR-4634: NetApp SolidFire Reference Architecture with Veeam Backup and Replication 9.5.

Disaster Recovery Failover and Failback: NetApp HCI to Converged Infrastructure

NetApp SnapMirror enhances disaster recovery options by using converged infrastructure and NetApp HCI systems. SnapMirror helps provide business continuity on an Element system by replicating Snapshot copies of an Element volume to an ONTAP destination. If there is a disaster at the Element site, you can serve data to clients from the ONTAP system, and then reactivate the Element system when service is restored.

Starting with ONTAP 9.4, you can replicate Snapshot copies of a LUN created on an ONTAP node back to an Element system. You might have created a LUN during an outage at the Element site, or you might be using a LUN to migrate data from ONTAP to Element software.

There are several scenarios that you can use if a disaster occurs:

- **SnapMirror.** NetApp HCI to converged infrastructure (SAN) in the event of a disaster at the NetApp HCI site
- **SnapMirror.** Converged infrastructure to NetApp HCI (SAN) when service is restored
- **Data migration.** Converged infrastructure to NetApp HCI and NetApp HCI to converged infrastructure

SnapMirror technology can be used to distribute large amounts of data throughout the enterprise, enabling faster access to data for clients in remote locations. It also allows more efficient and predictable use of expensive network and server resources because WAN usage occurs at a predetermined replication time. Storage administrators can replicate production data at a specific time to minimize overall network usage. Storage can be added nondisruptively to both converged infrastructure and NetApp HCI and when data migration is not required for adding storage.

Reasons to migrate data from one array to another include:

- Data center outages, data center moves, moving data to another system
- Application migrations and releasing storage on another system
- DevOps or software application development and test cycles
- Desire to take advantage of cheaper storage and even spinning media
- Desire to deliver submillisecond latency for performance-intensive workloads
- Desire to take advantage of Element quality of service (QoS) or linear scaling of workloads such as VDI
- Remote office or branch office use cases with NetApp HCI in smaller deployments with converged infrastructure at the main data center

3 Configuration

In considering converged systems and the cooperation of NetApp HCI and converged infrastructure, it's important to review all layers of the infrastructure. With converged infrastructure, compute, network, and storage are configured according to best practices and sized according to the anticipated workload requirements. With NetApp HCI, compute and storage are deployed but network is considered outside the scope of the deployment because the requirements placed on the network infrastructure are limited.

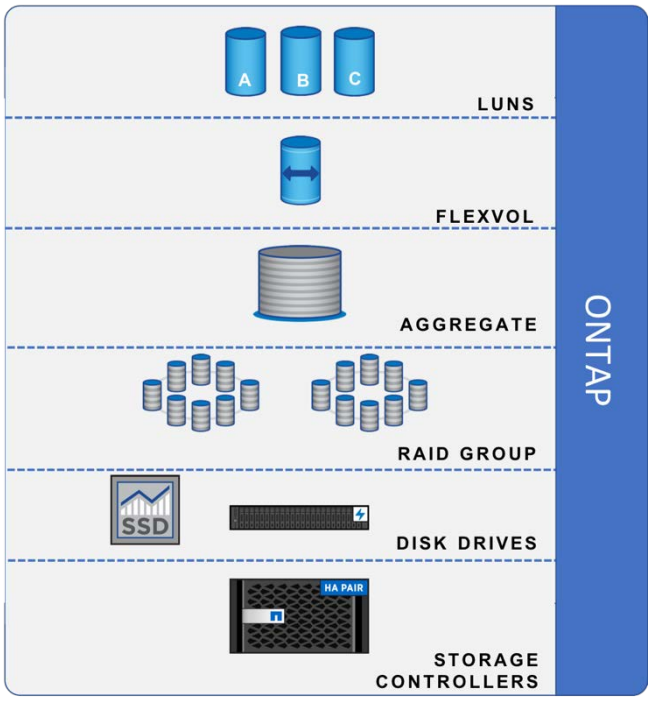
3.1 Storage Considerations

NetApp HCI and converged infrastructure offer enterprise-grade storage with various capabilities that are based on workload demands. Enabling replication between these systems requires an understanding of the components and datastores.

NetApp AFF and FAS take advantage of ONTAP, a highly available and performance-optimized system with NetApp RAID DP® technology. Storage controllers serve as the brains of the cluster; they are connected to disks. These drives are organized into RAID groups, which constitute the foundation of an aggregate. Aggregates can be created from one or many RAID groups, depending on size requirements. FlexVol® volumes are logical volumes that can contain LUNs or file-based datastores.

Figure 10 shows the components of ONTAP software.

Figure 10) ONTAP software components.

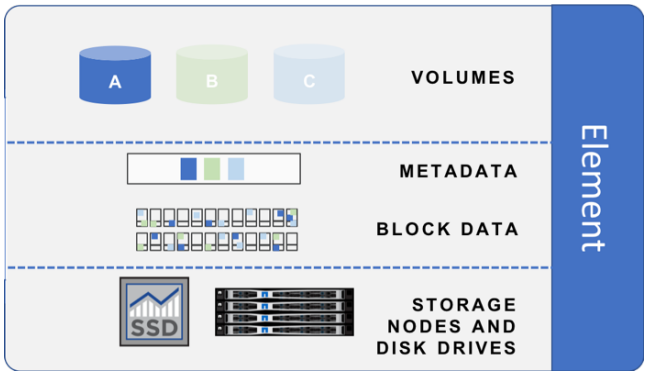


NetApp HCI and SolidFire flash nodes use Element software, which is a shared-nothing, RAID-less architecture. As nodes are added to the Element cluster, incremental performance and capacity are added to the system. Two instances of the file system are placed on the drives, spread across the system.

For more information about Element, see the Element Software Product Library.

Figure 11 shows the components of Element software.

Figure 11) Element software components.



When you are using SnapMirror between converged infrastructure and NetApp HCI systems, consider that a SolidFire volume is roughly equivalent to an ONTAP LUN. SnapMirror creates a LUN with the name of the database in the destination volume when an Element to ONTAP data protection relationship is initialized. You must also consider the following points:

- An ONTAP LUN in a FlexVol volume can contain data from only one Element volume.
- SnapMirror replication between Element and ONTAP is supported only for SAN volumes.
- SnapMirror replication between Element and ONTAP is supported only for iSCSI and FC volumes; however, NetApp HCI does not support Fibre Channel (FC).

- SnapMirror replication is supported between ONTAP Select on NetApp HCI and ONTAP for NAS-based volumes.
- An Element source volume can be replicated to only one ONTAP destination volume.
- Data cannot be replicated from an ONTAP volume to multiple Element volumes.

Scale and support limits of SnapMirror for Element as of Element 11.x include:

- Element supports up to 30 Snapshot copies per volume for SnapMirror (the system limit is typically 32).
- You can replicate up to 32 Element clusters to a single ONTAP cluster.
- ONTAP 9.3 supports up to 251 Snapshot copies per volume
- In ONTAP 9.4 and later, a destination volume can contain up to 1,019 Snapshot copies.
- SnapMirror supports a maximum of 500 protected volumes replicating from one Element cluster to ONTAP.
- SnapMirror supports a maximum of 32 SolidFire clusters replicating to a single ONTAP array.
- SnapMirror supports a maximum of 2,000 volumes replicating to a single ONTAP array.
- You can have up to 100 concurrent transfers per SolidFire node.

Note: Review the Element release notes to get the latest scale and support limits.

3.2 Storage Efficiencies Guidelines

The ONTAP storage systems used in the NetApp converged infrastructure and the Element systems that are core components of the NetApp HCI solution use various storage efficiencies. Storage efficiency enables you to store the maximum amount of data for the lowest cost and accommodates rapid data growth while consuming less space. Element and ONTAP offer various technologies that can be combined to increase storage utilization and decrease storage costs. This section reviews the data flow, inline, and postprocess storage efficiencies applied to the working set, thin provisioning considerations, and projected space savings.

Dataflow

Both the NetApp WAFL® file system and the Element file system used in converged infrastructure and NetApp HCI receive user data and commit it to NVRAM on multiple nodes in 4KB blocks to avoid data loss if a node fails before the data is committed to the disk. Many of the storage efficiency strategies are first implemented on each storage system after the data is secured in NVRAM but before the data is written to disk.

Inline Deduplication, Compression, and Compaction

Both NetApp AFF systems and Element systems can deduplicate, compress, and compact data inline before the data is committed to the system SSDs. In most workloads, clients write data to storage systems, where it is analyzed for its ability to be compressed, so that larger chunks of data can be broken down into the 4KB blocks as required. A compression-friendly workload results in significant space savings at the block level on both ONTAP and Element storage systems used in NetApp converged infrastructure and NetApp HCI solutions. Because both storage systems write data in 4KB blocks, regardless of the incoming data size, larger writes that are not evenly divisible by 4, and smaller writes, have their 4KB blocks filled out with zeros to meet the size requirements for a block to be written to disk. Compaction of data blocks removes these zeros and completes the 4KB blocks by using data from other uneven write requests to complete full data blocks. From this point, both Element and ONTAP AFF systems perform an inline deduplication process, examining each of these blocks. If another identical block is found, the system updates metadata to point to the original block and does not write the duplicate to disk, thus saving space in the environment.

Postprocess Deduplication and Compression

After inline deduplication is complete, an extra layer of deduplication and compression is run postwrite. This storage efficiency action is run globally across all SolidFire nodes in an Element deployment and against other volumes in the same aggregate on AFF ONTAP systems. It is also run against data in the same volume on hybrid and traditional ONTAP arrays. These storage efficiencies help to extend the life of SSDs by limiting the number of committed writes and by using only the necessary data blocks for the storage system, helping you to get the most value from your solution.

Thin Provisioning

Both systems also enable increased usage of your storage system by thin provisioning the volumes that you allocate. When a volume is created in ONTAP with thin provisioning enabled, it displays its full allocated size to client machines, but in ONTAP it uses only the amount of aggregate disk space it needs for the data that the volume contains. In Element, when a volume is created it dedicates only the amount of space used for data in the volume and grows the volume as needed in 4KB blocks. This minimizes writes to the SSDs and enables you to gain significant value from the storage efficiencies used in your environment.

Projected Efficiencies

Combining these storage efficiencies results in a reduced storage footprint. The actual savings vary, because workloads differ from infrastructure to infrastructure and application to application. Databases can often show efficiencies of about 3:1; VDI environments about 8:1; and workloads about 4:1, depending on the specifics of the workload. NetApp Fusion, a unified sizing application, allows engineers to design recommended solutions for AFF, FAS, Element, NetApp E-Series storage systems, and NetApp HCI, based on performance and capacity requirements. Because workload requirements can vary based on several factors, NetApp recommends consulting with our sales team about planning your workload to specify the most appropriate storage efficiencies on both converged infrastructure and NetApp HCI systems.

For information about the NetApp storage efficiency guarantees, see NetApp All-Flash Guarantee for AFF, SolidFire and NetApp HCI.

For more information about ONTAP storage efficiencies, see TR-4476: NetApp Data Compression, Deduplication, and Data Compaction.

For more information about Element storage efficiencies, see How SolidFire Data Efficiencies Work (login required).

3.3 Network Considerations

Both NetApp HCI and converged infrastructure solutions have specific networking best practices that should be considered. Converged infrastructure systems use Cisco Nexus or Extreme switches, while NetApp HCI systems are often deployed with Mellanox, Cisco Extreme switches, or any 10/25GbE-capable switch. This section reviews the networking best practices for NetApp converged infrastructure solutions using ONTAP and NetApp HCI solutions using Element.

Converged infrastructure and NetApp HCI systems offer a choice of Ethernet speeds for the data path, including 10, 25, or 40GbE. To find the appropriate option, review the solution-specific documentation.

Switch Requirements for NetApp HCI

- All switch ports connected to NetApp HCI nodes must be configured to allow the Spanning Tree Protocol (STP) to enter the forwarding state immediately. (On Cisco switches, this functionality is known as PortFast.) Ports connected to NetApp HCI nodes should not receive STP Bridge Protocol Data Units.

- The switches handling storage, VM, and vMotion traffic must support speeds of at least 10GbE per port. Up to 25GbE per port is supported.
- The switches handling management traffic must support speeds of at least 1GbE per port.
- The maximum transmission unit (MTU) size on the switches handling storage traffic must be 9216 bytes end to end for a successful installation. (MTU size is configured on the storage node interfaces automatically.)
- Cisco virtual port channel (vPC) or the equivalent switch stacking technology for your switches must be configured on the switches that are handling the storage network for NetApp HCI. Switch stacking technology makes configuration of LACP and port channels easier and provides a loop-free topology between switches and the 10/25GbE ports on the storage nodes.
- The switch ports connected to the 10/25GbE interfaces on NetApp HCI storage nodes must be configured as LACP port channels.
- The LACP timers on the switches handling storage traffic must be set to `fast mode (1s)` for optimal failover detection time. During deployment, the Bond1G interface on all NetApp HCI storage nodes is automatically configured for active-passive mode.
- Round-trip network latency between all storage and compute nodes should not exceed 2ms.
- To prepare your network for NetApp HCI deployment, implement the following best practices:
  - Install as many switches as needed to meet HA requirements.
  - Balance 1/10GbE port traffic between at least two 1/10GbE-capable management switches.
  - Balance 10/25GbE port traffic between two 10GbE-capable switches.

Switch Requirements for NetApp Converged Infrastructure

- A separate 100Mbps Ethernet/1Gb Ethernet out-of-band management network is required for all components.
- NetApp recommends that you enable jumbo frame support throughout the environment, although it is not required.
- When using Cisco UCS, NetApp recommends the fabric interconnect appliance ports only for iSCSI and NAS connections.
- No additional equipment can be placed in line between the core converged infrastructure components.
- The uplink ports on the NetApp storage controllers must be connected to the converged infrastructure switches to enable support for vPCs or similar functionality.
- vPCs or similar functionality is required from the converged infrastructure switch uplink ports to the NetApp storage controllers.
- vPCs or similar functionality is required from converged infrastructure switches to the UCS fabric interconnects, where appropriate.
- NetApp storage controller ports that are directly connected to the fabric interconnects can be grouped to enable a port channel. vPC is not supported for this configuration.
- FCoE port channels are recommended for end-to-end direct connect FCoE designs.

For more information about NetApp HCI networking best practices, see TR-4679: NetApp HCI Network Setup Guide.

For more information about NetApp HCI with Mellanox switches, see TR-4735-1218: NetApp HCI with Mellanox SN2010 Switch Quick Cabling Guide.

For more information about the NetApp converged infrastructure networking best practices, see TR-4036: FlexPod Technical Specification.

3.4 VMware Considerations

As previously mentioned, NetApp has proven various integration points with VMware for NetApp HCI and converged infrastructure systems, as documented in NetApp Verified Architectures (NVAs). These integration points include storage plug-ins for VMware vCenter Server, tight integration with VMware storage policy-based management (SPBM), and management packs for VMware vRealize Operations (vROps).

NVAs, including validations with VMware products and solutions, can be found in the NetApp NVA library.

The NetApp Element Plug-In for VMware vCenter Server (4.2) allows you to manage the storage of your NetApp HCI environment from the vSphere web client on the vCenter Server. This plug-in is installed automatically with NDE. If you have performed a custom deployment of your NetApp HCI solution, the plug-in is still available for download and can be installed to enable the additional functionality.

For more information about Element integration with VMware, see the Element Plug-in for vCenter Server landing page in the documentation center.

The NetApp VSC Plug-In for VMware vSphere enables you to manage your storage systems in your converged infrastructure environment from within VMware vSphere. It also allows you to fine-tune your environments by managing device settings on ESXi hosts in the environment to conform to best practices. The software is available to download as an OVA file from NetApp and can be deployed as a guest in vSphere. The plug-in can then be activated in vCenter Server, enabling you to manage your ONTAP systems from within the vSphere web client.

For more information about ONTAP integration with VMware, see Virtual Storage Console for VMware vSphere in the product library.

Element has tight integration with VMware SPBM using Virtual Volumes (VVols). When VVols is enabled on the NetApp HCI cluster, VMware SPBM policies can be set on VMs created on VVols storage. This enables granular, direct manipulation of the QoS settings for each VM and each virtual disk associated with each VM. This SPBM integration means that you can create and assign vRealize Automation (vRA) property definitions for single or multiple disks for VMs created through the Blueprint and Catalog Services. You can then select your predefined storage policies in vCenter Server.

NetApp has partnered with Blue Medora to deliver comprehensive management packs for ONTAP and Element based systems. These management packs provide visibility into storage systems and workloads from within vROps. This visibility helps optimize performance and eliminate potential resource constraints.

For more information about the ONTAP integration with vROps, see VMware vRealize Operations Management Pack for NetApp Storage from Blue Medora.

For more information about the Element integration with vROps, see VMware vRealize Operations Management Pack for NetApp HCI and SolidFire from Blue Medora.

Deploying the Virtual Appliance for VSC

It's important to understand the sequence of steps for deploying the virtual appliance for VSC, vSphere API for Storage Awareness (VASA) Provider, and VMware Storage Replication Adapter (SRA) in your environment, because the tasks that you can perform depend on the deployment model that you select.

Before you deploy a VSC, follow these steps.

1. Confirm that you are running a supported version of vCenter Server.

   Note: The virtual appliance for VSC, VASA Provider, and SRA can be deployed on either a Windows deployment of vCenter Server or a VMware vCenter Server Virtual Appliance (vCSA) deployment.

2. Verify that your vCenter Server environment is configured.
3. Verify that an ESXi host was set up for your virtual machine.

4. Download the OVA file.
5. Have the login credentials for your vCenter Server instance ready.
6. To avoid any browser cache issues during the deployment of the virtual appliance for VSC, VASA Provider, and SRA, log out and close all browser sessions of vSphere Web Client, and delete the browser cache.
7. Enable Internet Control Message Protocol (ICMP).

Note: If ICMP is disabled, then the initial configuration of the virtual appliance for VSC, VASA provider, and SRA fails. In that case, VSC cannot start the VSC and VASA Provider services after deployment. You must manually enable the VSC and VASA Provider services after deployment.

Deploying VSC

1. Log in to the vSphere web client.
2. Select Home > Host and Clusters.
3. Right-click the required data center and then click Deploy OVA Template.
4. Select one of the following methods to provide the deployment file for VSC, VASA Provider, and SRA, and then click Next.
   - URL: Provide the URL for the OVA file for the virtual appliance for VSC, VASA Provider, and SRA.
   - Folder: Select the OVA file for the virtual appliance for VSC, VASA Provider, and SRA from the saved location.
5. Enter the following details to customize the deployment wizard:
   - Name for your deployment
   - Destination data center to apply permissions to
   - Host on which the virtual appliance for VSC, VASA Provider, and SRA is to be deployed
   - Virtual disk format, VM storage policies, storage location, and network
   - Administrator username and password

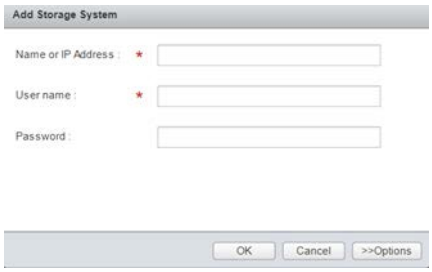
   Note: While you are configuring the static IP address for the virtual appliance for VSC, VASA Provider, and SRA, you must provide a host name that includes only the following characters: hyphen (-), English uppercase characters (A through Z), English lowercase characters (a through z), and base digits (0 through 9).

   Note: Do not use any spaces in the administrator password.
6. View the progress of the deployment from the Tasks tab and wait for the deployment to complete.
7. Right-click the deployed virtual appliance for VSC, VASA Provider, and SRA and then click Install VMware tools.
8. Log in to the web CLI by using the administrator username and password that you set during deployment.

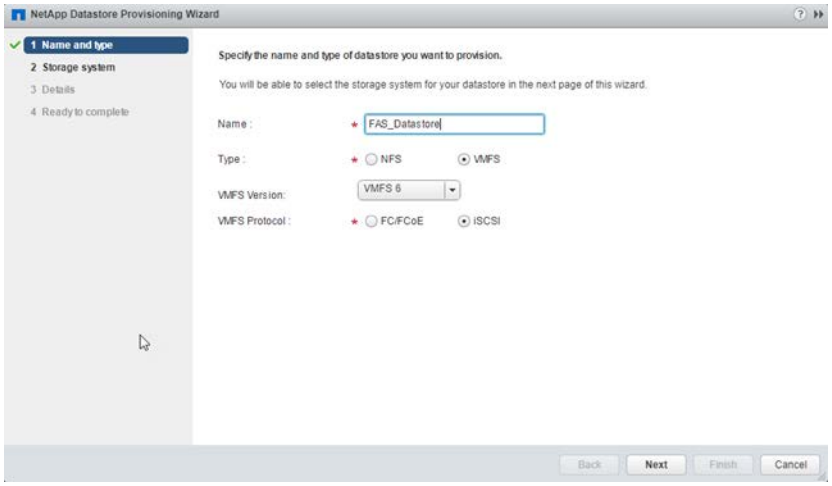
   Note: Use https://<UA_APPLIANCE_IP>:9083 to access the web CLI.
9. Use https://<appliance_ip>:8143/Register.html to register the VSC instance after deployment only if the virtual appliance for VSC, VASA Provider, and SRA is not registered with any vCenter Server.

Adding ONTAP Storage Controller to VSC

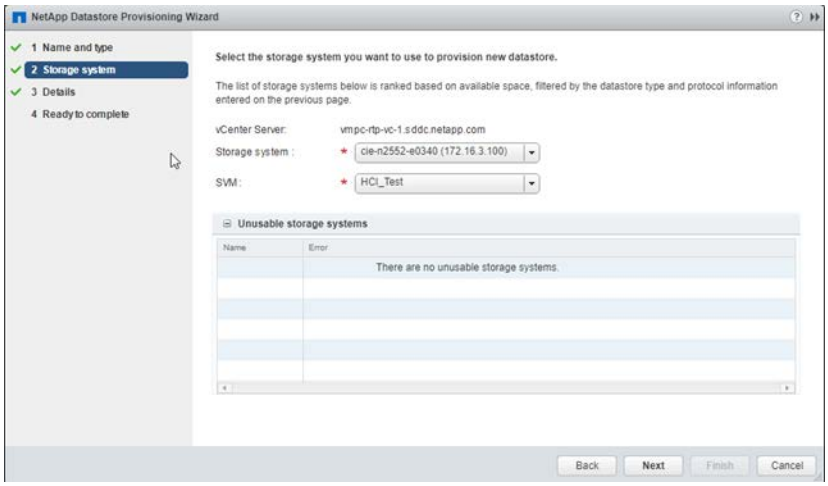
1. Log in to the vSphere web client.
2. Select Home > Virtual Storage Console.
3. Select Storage Systems.
4. Click the Add icon to add a storage system and enter the name, username, and password of the FAS system, then click OK.



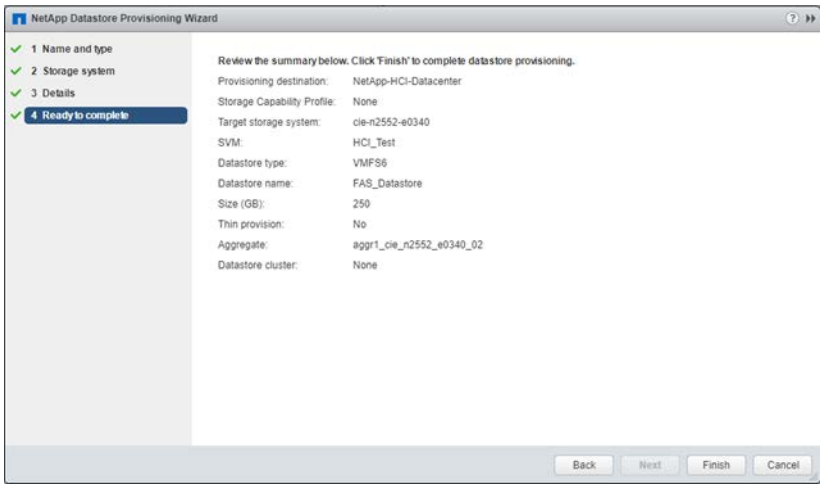
5. Enter the name and type of the new datastore and then click Next.

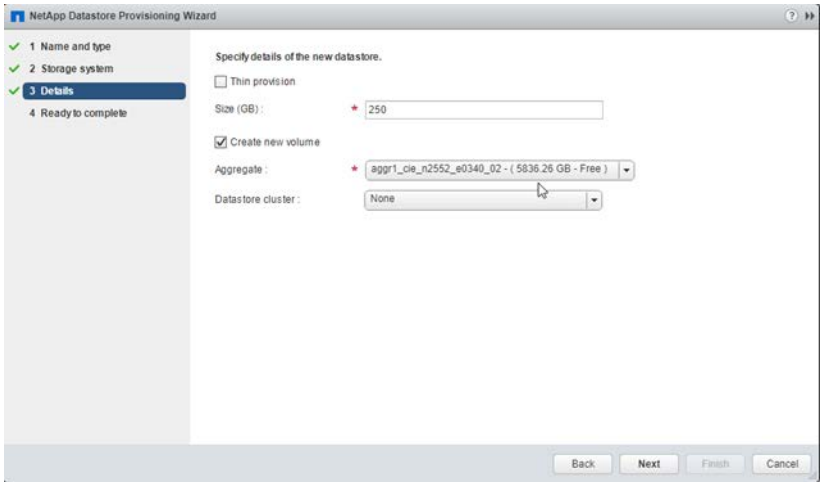


6. Select the vCenter Server, SVM, and then click Next.



7. Enter the size of the datastore, select the correct aggregate, and then click Next.





8. Review the summary and then click Finish.

Reviewing VMware Plug-In Information

Once the Element and ONTAP related plug-ins are installed, NetApp recommends that you launch the flash-enabled client for improved functionality. Simple administrative tasks are available with a click of a button from a common location in vCenter Server.

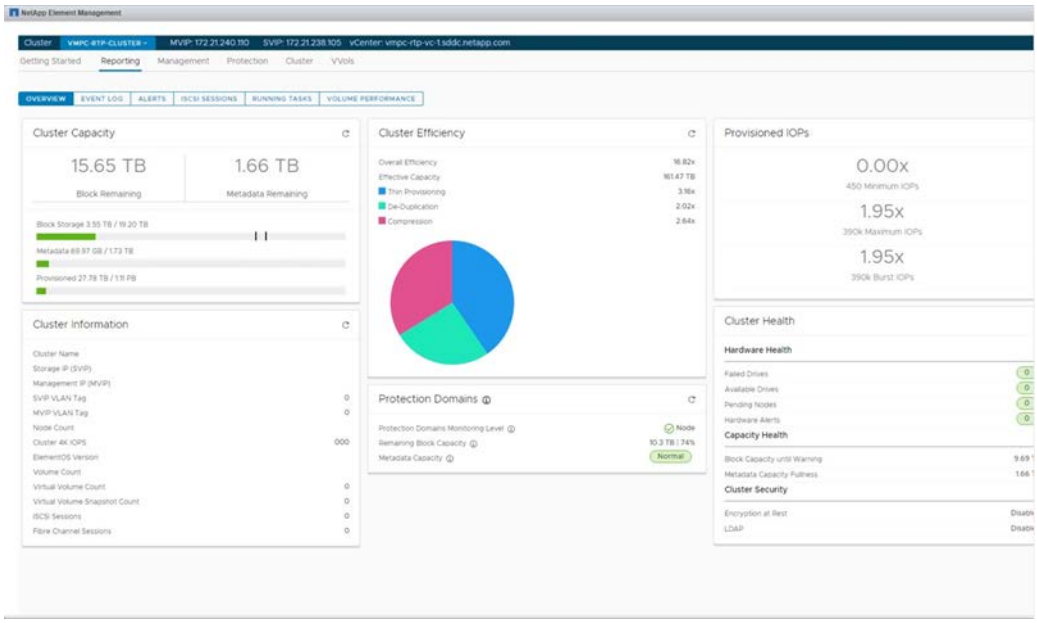
1. Log in to the vSphere web client.
2. Click the Home icon and notice that the Element (Element Configuration and Element Management) and the ONTAP (Virtual Storage Console) integration are visible.

Figure 12 shows the availability of Element and ONTAP plug-ins in vCenter Server.

Figure 12) NetApp plug-ins for VMware vCenter Server.

The Element overview displays the overall cluster health, storage efficiencies, and provisioned IOPS. Figure 13 shows the Element plug-in in vCenter Server.

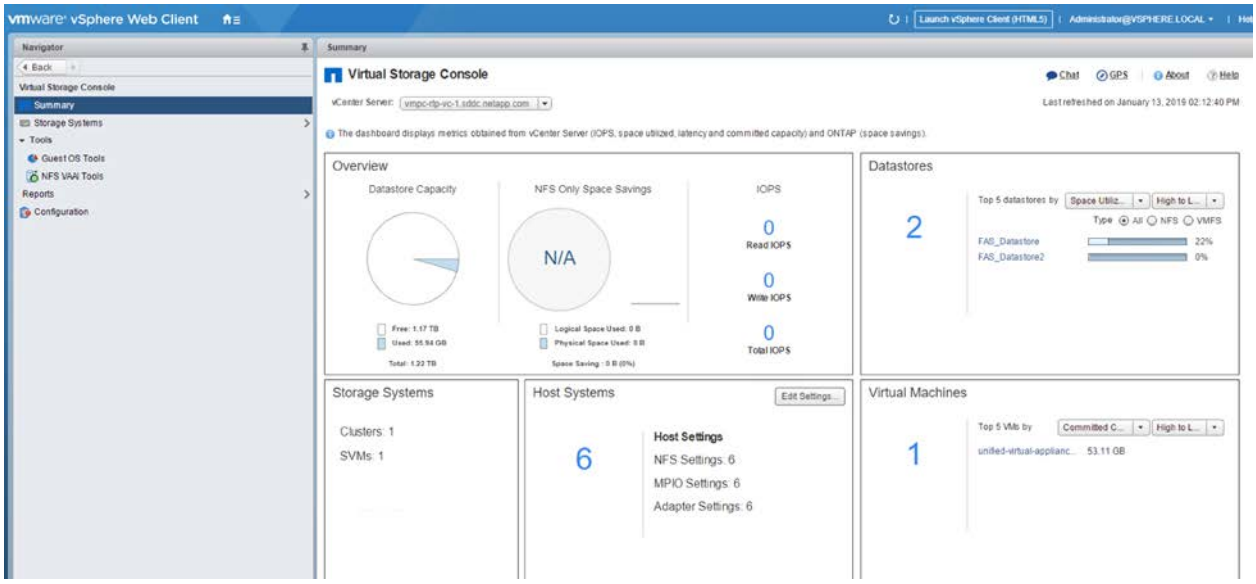
Figure 13) NetApp Element software management plug-in.



The VSC plug-in presents SVM, performance, VM, and capacity information of ONTAP systems.

Figure 14 shows the Element plug-in in vCenter Server.

Figure 14) NetApp ONTAP management plug-in.

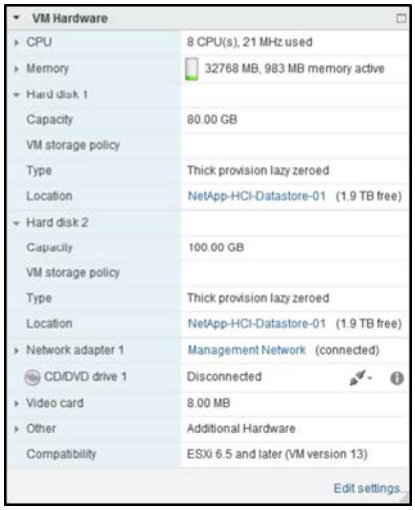


vMotion Across Converged Infrastructure and NetApp HCI

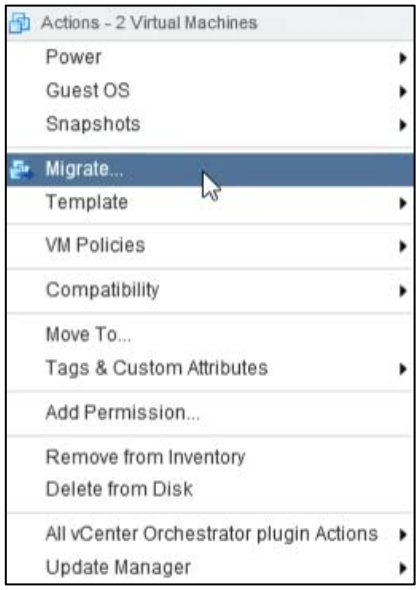
Although the data fabric presents several options to enable easy migration of data between the storage systems in both NetApp HCI and converged infrastructure solutions, it is also possible to approach this migration from the application as an end user. An example of this functionality is Storage vMotion, provided in VMware vSphere. Using NetApp tools such as VSC, the remote storage system deployed in a converged infrastructure solution can be added as a storage resource to the vCenter Server that has been deployed by NDE with a NetApp HCI solution. Doing so enables almost effortless, live migrations of virtual guests from one storage infrastructure to the other with no perceivable downtime.

Performing a Storage vMotion Migration Across Converged Infrastructure and NetApp HCI

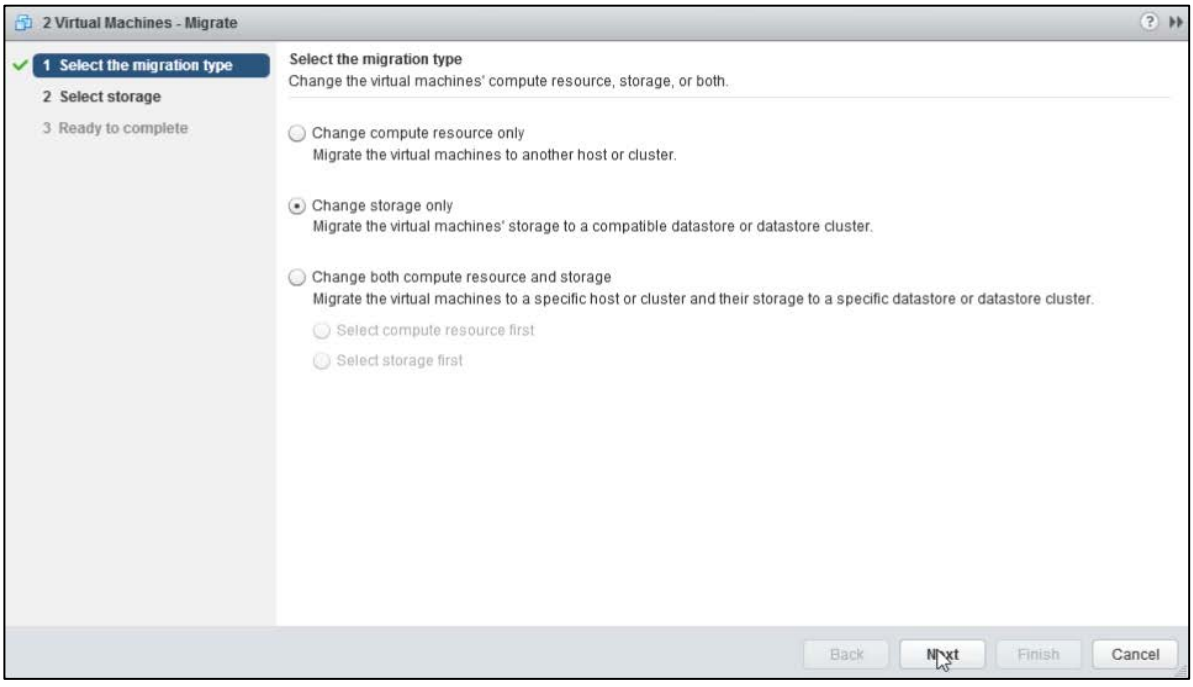
1. Log in to the vSphere web client.
2. Select the virtual guest to migrate and verify its storage location.



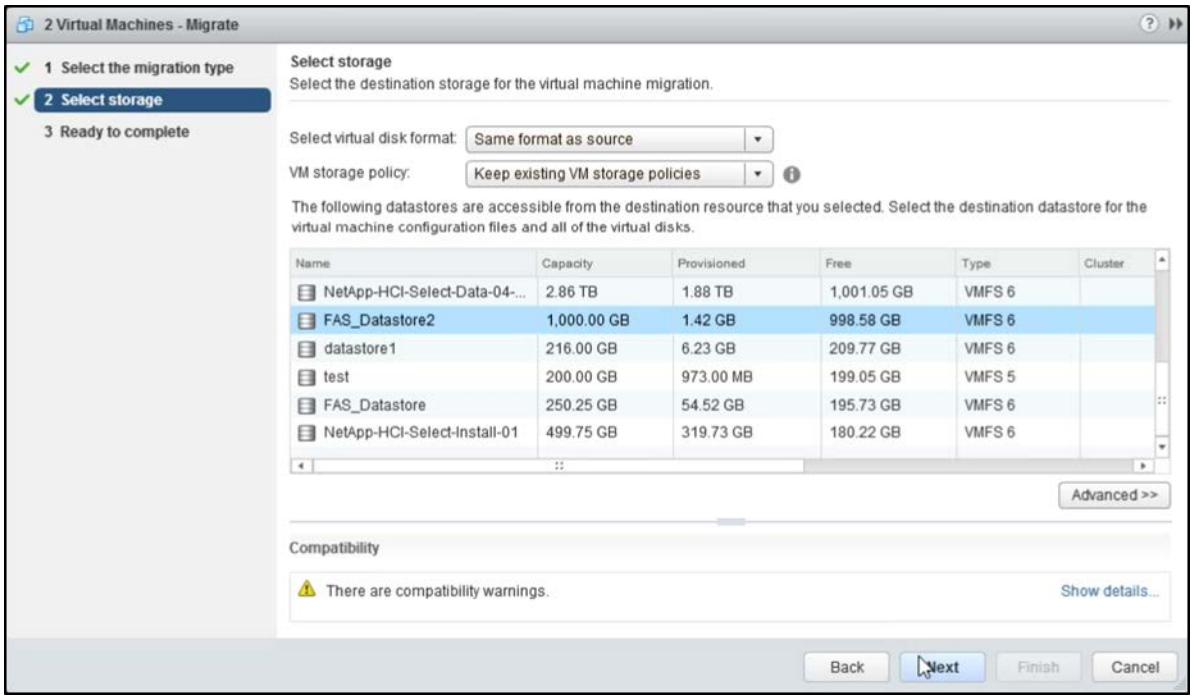
3. Right-click the guest and select Migrate from the pop-up menu.



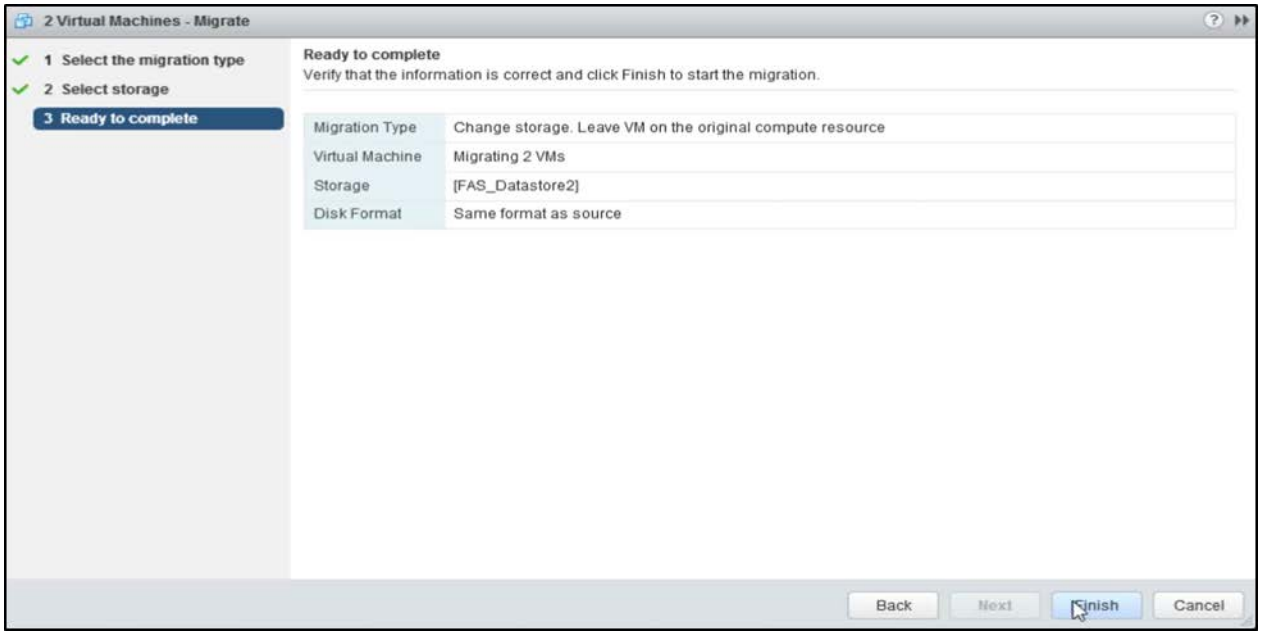
4. In the migration wizard, choose the second option, Change Storage Only.



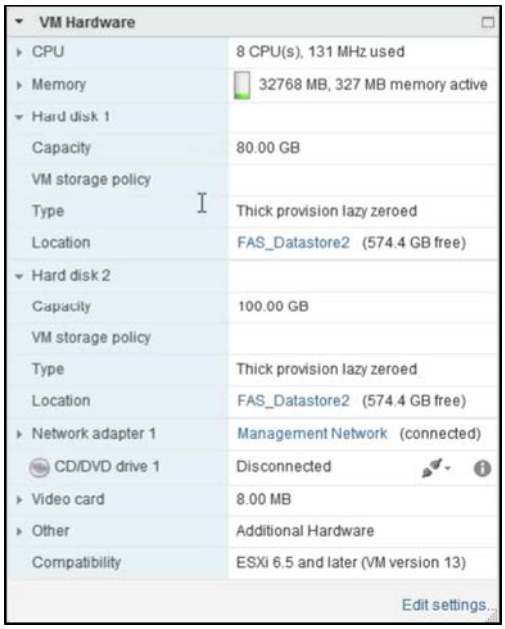
5. Choose the remote datastore to migrate your guest to.



6. Confirm the settings in the migration wizard and click Finish.



7. Confirm that the virtual guest now resides on the remote FAS storage system in your converged infrastructure.



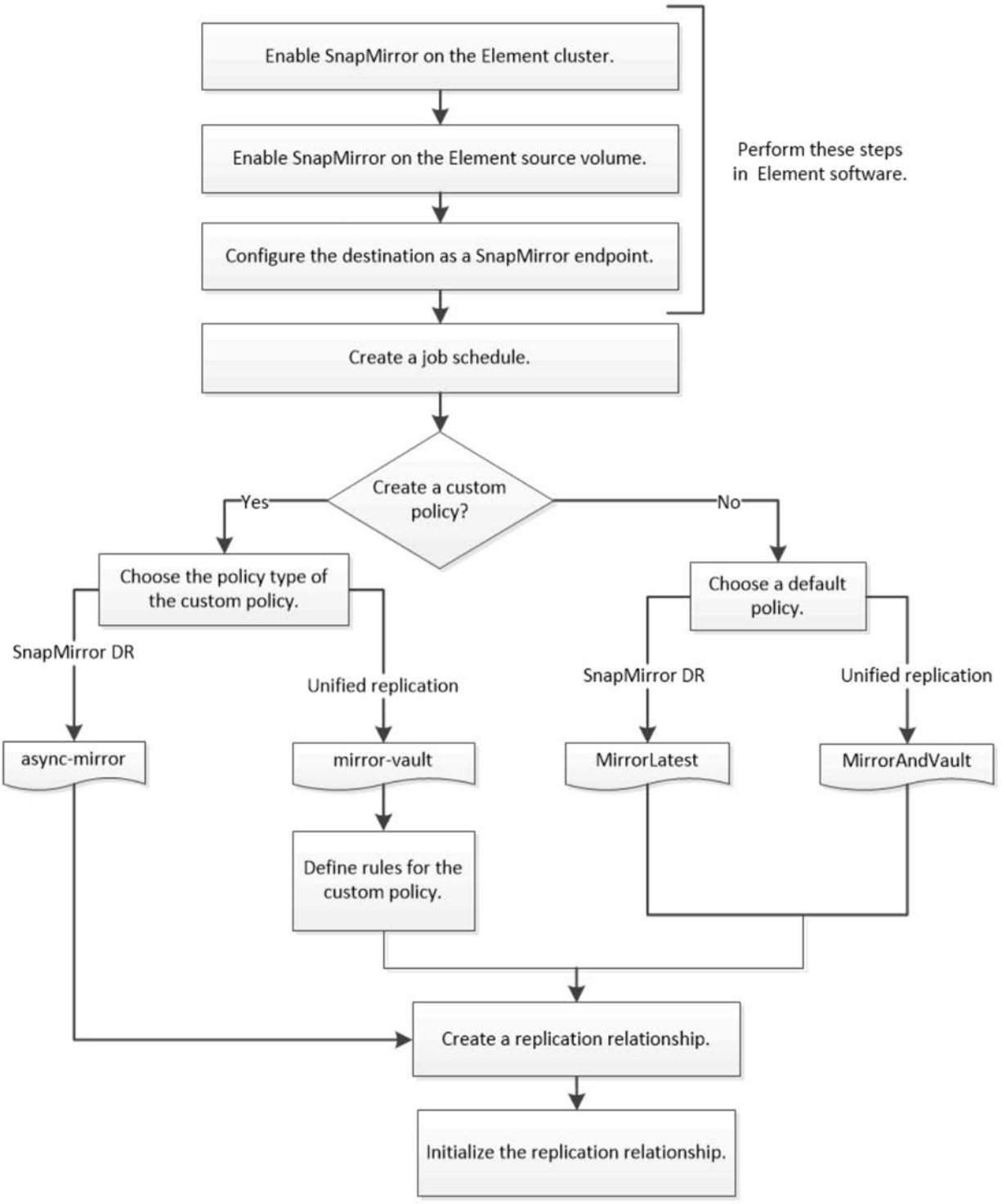
3.5 SnapMirror Configuration Deployment

This section documents the steps to enable SnapMirror for Element. Figure 15 details the workflow for establishing the data protection relationship between Element and ONTAP.

For full information about the prerequisites to configure the data protection relationship between Element and ONTAP, see Understanding Replication between Element and ONTAP in the documentation center.

The workflow in Figure 15 assumes that you have completed the prerequisite tasks.

Figure 15) SnapMirror workflow.



For complete background information about SnapMirror policies, including guidance on which policy to use, see the ONTAP Data Protection Power Guide.

Enabling SnapMirror in Element Software

You must enable SnapMirror on the Element cluster before you can create a replication relationship. You can perform this task in the Element software web UI or by using the API.

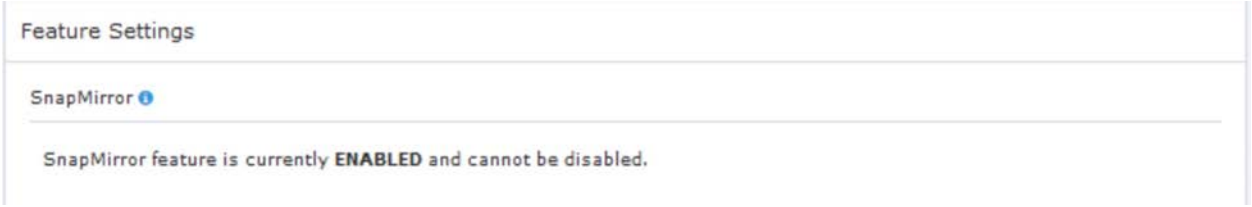
Note: After SnapMirror is enabled on the Element cluster, it cannot be disabled.

To configure using the API:

```
{
  "id": 106,
  "method": "EnableFeature",
  "params": {
    "feature": "snapMirror"
  }
}
```

To configure using the GUI:

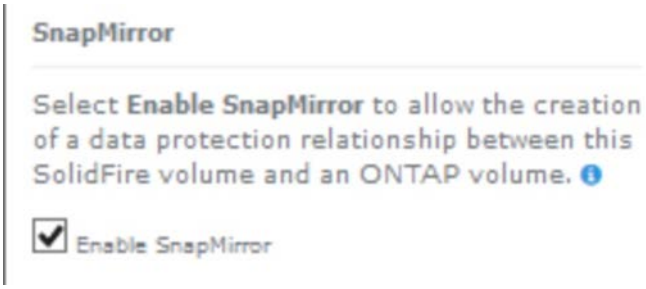
1. Enable SnapMirror on the Element cluster.
2. In the SolidFire UI, select Cluster > Settings.
3. Find the cluster-specific settings for SnapMirror.
4. Click Enable SnapMirror.



5. Enable SnapMirror on the Element source volume.

   Note: You must enable SnapMirror on the Element source volume before you can create a replication relationship. You can perform this task only in the Element software web UI.

6. In the SolidFire UI, select Management > Volumes.
7. Click the # button for the volume.
8. Select Edit from the menu.
9. In the Edit Volume dialog box, select Enable SnapMirror.
10. Click Save Changes.



11. Create a SnapMirror endpoint.

Note: You must create a SnapMirror endpoint before you can create a replication relationship. You can perform this task only in the Element software web UI.

12. Select Data Protection > SnapMirror Endpoints.
13. Click Create Endpoint.
14. In the Create a New Endpoint dialog box, enter the IP address of the ONTAP cluster management.
15. Enter the user ID and password of the ONTAP cluster administrator.
16. Click Create Endpoint.

Configuring a Replication Relationship

To configure a replication relationship, follow these steps.

1. Create a replication job schedule.

   Note: You can use the `job schedule cron create` command to create a replication job schedule. The job schedule determines when SnapMirror automatically updates the data protection relationship to which the schedule is assigned.

2. Create a job schedule.

```
job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -
hour hour -minute minute
For -month, -dayofweek, and -hour, you can speCIfy all to run the job every month, day of the
week, and hour, respectively.
Example
The following example creates a job schedule named my_weekly that runs on Saturdays at 3:00 a.m.:
cluster_dst::> job schedule cron create -name my_weekly -dayofweek "Saturday" -hour 3 -minute 0
```

3. Optional: Create a customized replication policy.

   Note: You can use a default or custom policy when you create a replication relationship. For a custom unified replication policy, you must define one or more rules that determine which Snapshot copies are transferred during initialization and update.

4. Create a replication relationship. For Element to ONTAP, see step 5. For ONTAP to Element, see step 6.

   Note: The relationship between the source volume in primary storage and the destination volume in secondary storage is called a *data protection relationship.* You can use the `snapmirror create` command to create a data protection relationship from an Element source to an ONTAP destination, or from an ONTAP source to an Element destination.

5. Create a replication relationship from an Element source to an ONTAP destination:

```
snapmirror create -source-path hostip:/lun/name -destination-path SVM:volume|cluster://SVM/volume
-type XDP -schedule schedule -policy policy
The following example creates a SnapMirror DR relationship using the default MirrorLatest policy:
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005 -destination-path
svm_backup:volA_dst -type XDP -schedule my_daily -policy MirrorLatest
```

6. Create a replication relationship from an ONTAP source to an Element destination:

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume -destination-path hostip:/lun/name
-type XDP -schedule schedule -policy policy
The following example creates a SnapMirror DR relationship using the default MirrorLatest policy:
```

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst -destination-path
10.0.0.11:/lun/0005 -type XDP -schedule my_daily -policy MirrorLatest
```

Initializing a Replication Relationship

For all relationship types, initialization performs a baseline transfer; it makes a Snapshot copy of the source volume, then transfers that copy and all the data blocks it references to the destination volume.

1. Initialize a replication relationship:

```
snapmirror initialize -source-path hostip:/lun/name -destination-path
SVM:volume|cluster://SVM/volume
```

Note: For complete command syntax, see the man page.

The following example initializes the relationship between the source volume 0005 at IP address 10.0.0.11 and the destination volume volA_dst on svm_backup:

```
cluster_dst::> snapmirror initialize -source-path 10.0.0.11:/lun/0005 -destination-path
svm_backup:volA_dst
```

2. Use the `snapmirror show` command to verify that the SnapMirror relationship was created.

4 Management and Monitoring Tools

Active IQ is a web-based application that is based on AutoSupport® information from your NetApp systems, providing predictive and proactive insights to help improve availability, efficiency, and performance.

Things that are new with Active IQ include:

- Storage efficiency and risk advisor powered by community wisdom
- Customizable, responsive dashboard
- Capacity trending and forecasting so that you know when you need more storage
- One-click lookup for your systems, sites, groups, and clusters
- Workload tagging
- Improved visibility for case tracking and trending

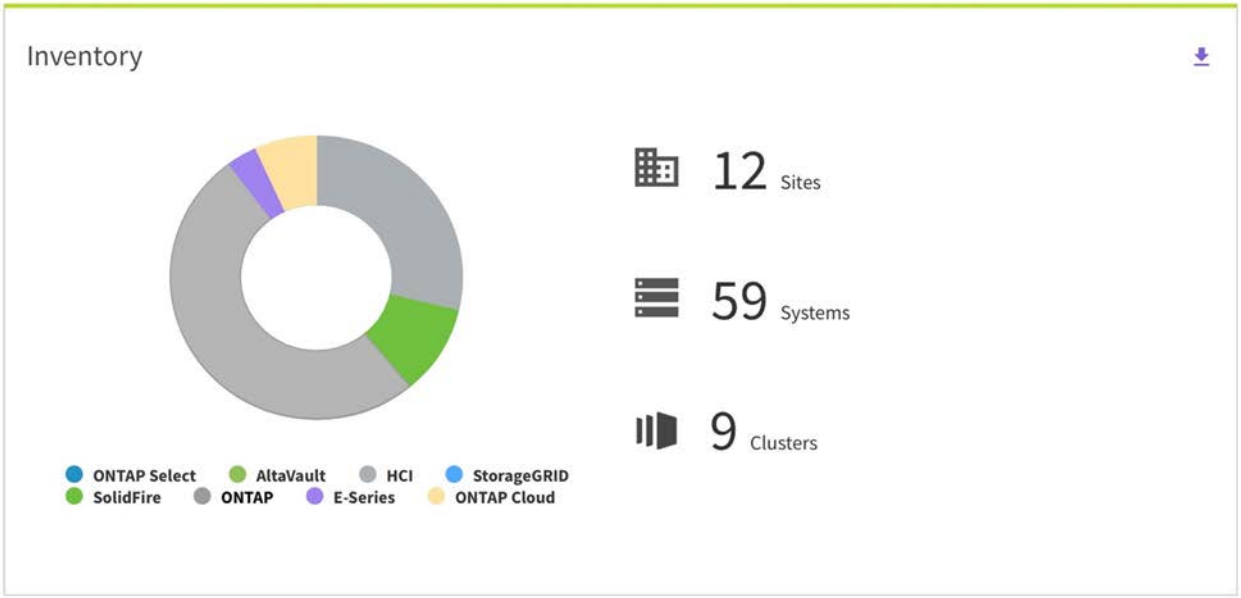
Benefits of Active IQ include:

- Predicts storage capacity growth to identify more requirements
- Recommends upgrade requirements for ONTAP systems and provides upgrade plans
- Proactively identifies system risks related to a configuration issue or known bugs
- Provides configuration, capacity, efficiency, and performance views and reports for better management of your NetApp systems

Active IQ allows customers and partners to dive into the resources deployed by the customer. By selecting any resource, you can view specifics for that storage system. For example, when choosing ONTAP systems, options such as AFF and FlexPod are visible.

Figure 16 shows an Active IQ customer dashboard.

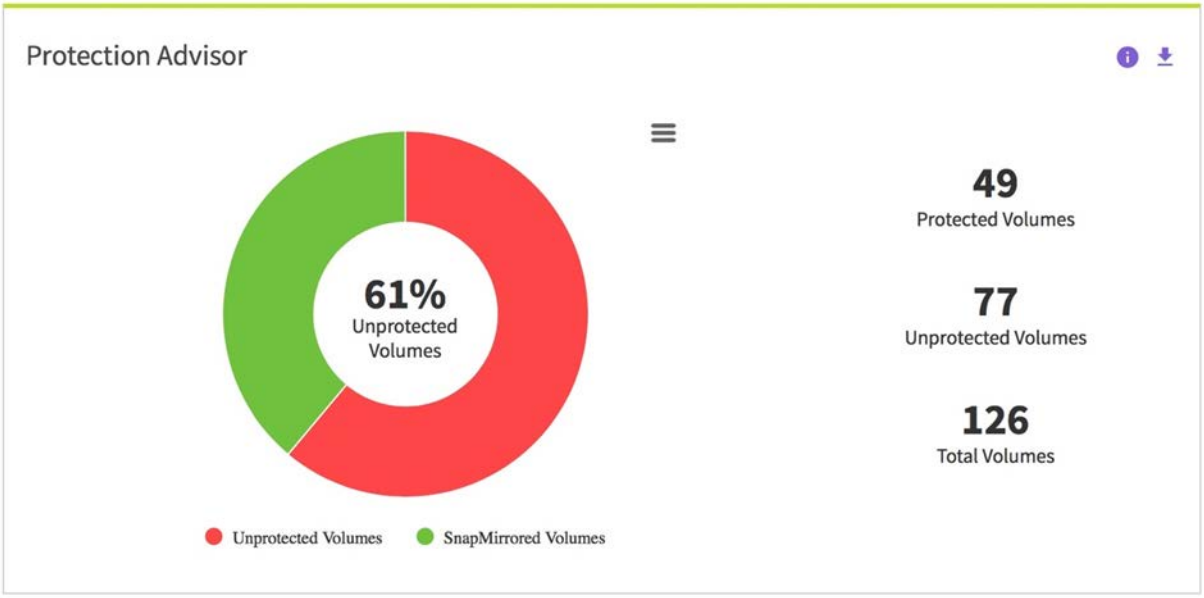
Figure 16) NetApp Active IQ customer dashboard.



AutoSupport also allows you to customize the widgets that are present when logging in. Protection Advisor displays the number of SnapMirror protected and unprotected volumes. A detailed list of the protected and unprotected volumes can be found in the widget. The detailed list can also be downloaded from the widget, so that you can easily view your NetApp HCI and converged infrastructure protected volumes.

Figure 17 shows the NetApp Protection Advisor, which provides guidance for protected and unprotected volumes.

Figure 17) NetApp Protection Advisor.



5 Summary

NetApp SnapMirror functionality between Element and ONTAP extends the data fabric with this disaster recovery architecture for NetApp converged infrastructure and NetApp HCI systems. SnapMirror offers increased data protection options for Element while using the robust data management capabilities of ONTAP. You can also take advantage of these new data mobility options to enable centralized backup and analytics and maximize the value and flexibility of your critical data. In addition to the SnapMirror capabilities, the integration of Element and ONTAP with VMware offers benefits to VMware administrators beyond disaster and data migration use cases.

Acknowledgments

The team would like to acknowledge the following team members for their contributions:

- James Bradshaw III
- Sam Sassorossi
- Erik Kemp

Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents and/or websites.

NetApp Technologies

- What Is a Data Fabric?
  www.netapp.com/us/info/what-is-data-fabric.aspx
- 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
- NetApp CSA Datasheet
  www.netapp.com/us/media/ds-3896.pdf
- NetApp Support
  https://mysupport.netapp.com/
- NetApp Active IQ
  www.netapp.com/us/products/data-infrastructure-management/active-iq-predictive-technology.aspx
- 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
- TR-4476: NetApp Data Compression, Deduplication, and Data Compaction
  www.netapp.com/us/media/tr-4476.pdf
- TR-4036: FlexPod Datacenter Technical Specification
  www.netapp.com/us/media/tr-4036.pdf
- Element Plug-in for vCenter Server landing page
  https://mysupport.netapp.com/documentation/productlibrary/index.html?productID=62701

- Virtual Storage Console for VMware vSphere
  https://mysupport.netapp.com/documentation/productlibrary/index.html?productID=30048
- 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
- ONTAP 9: Replication between NetApp Element Software and ONTAP
  https://library.netapp.com/ecm/ecm_download_file/ECMLP2834698
- Element Software Product Library
  https://mysupport.netapp.com/documentation/productlibrary/index.html?productID=62480
- NetApp All-Flash Guarantee for AFF, SolidFire and NetApp HCI
  www.netapp.com/us/media/netapp-aff-efficiency-guarantee.pdf
- How SolidFire Data Efficiencies Work
  https://fieldportal.netapp.com/content/777062
- Understanding replication between Element and ONTAP
  https://docs.netapp.com/ontap-9/topic/com.netapp.doc.pow-sdbak/GUID-723A9AB0-8565-4F65-B39E-B1B7B16ABA5F.html#GUID-723A9AB0-8565-4F65-B39E-B1B7B16ABA5F__SECTION_F0C7A7CFEE584B2CBB4E52D02402DD94

Third-Party Integrations with NetApp

- NetApp Interoperability Matrix Tool
  https://mysupport.netapp.com/matrix/#welcome
- VMware Compatibility Guide
  www.vmware.com/resources/compatibility/search.php?action=base&deviceCategory=san
- Virtual Infrastructure Management
  www.netapp.com/us/products/data-infrastructure-management/virtual-infrastructure.aspx
- VMware Migration
  https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vcenterhost.doc/GUID-AB266895-BAA4-4BF3-894E-47F99DC7B77F.html
- TR-3920: Commvault IntelliSnap for NetApp
  www.netapp.com/us/media/tr-3920.pdf
- TR-4636: NetApp SolidFire Reference Architecture with Commvault Data Platform v11
  www.netapp.com/us/media/tr-4636.pdf
- Veeam Availability Solutions for Data Protection
  www.veeam.com/netapp-use-cases-availability-solutions_wpp.pdf?ad=netapp-hub
- TR-4634: NetApp SolidFire Reference Architecture with Veeam Backup and Replication 9.5
  www.netapp.com/us/media/tr-4634.pdf

Version History

Version	Date	Document Version History
Version 1.0	February 2019	Initial release of TR

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