



Technical Report

# NetApp HCI Reference Architecture with Veeam Backup and Replication 9.5 Update 4

Erik Kemp, NetApp; Adam Bergh, Veeam

July 2019 | TR-4634

In partnership with



## Abstract

This document outlines the reference architecture and best practices for using NetApp® HCI® in a Veeam Backup and Replication 9.5 Update 4 environment.



## TABLE OF CONTENTS

<b>1</b>	<b>Executive Summary.....</b>	<b>5</b>
1.1	The Challenge.....	5
1.2	The Solution.....	5
<b>2</b>	<b>Introduction .....</b>	<b>6</b>
2.1	About NetApp.....	6
2.2	About Veeam .....	6
<b>3</b>	<b>NetApp HCI Private Cloud - Running Demanding Workloads in a Multitenant Environment.....</b>	<b>7</b>
<b>4</b>	<b>Reference Architecture Overview.....</b>	<b>8</b>
4.1	Deployment Scenarios.....	8
<b>5</b>	<b>NetApp HCI and Veeam .....</b>	<b>9</b>
5.1	Predictable Quality of Service and Always-On Availability for Element Hybrid Cloud Infrastructures .....	9
5.2	NetApp HCI Key Features.....	9
<b>6</b>	<b>Veeam Backup and Replication 9.5 Update 4.....</b>	<b>10</b>
6.1	Overview.....	10
6.2	Solution Architecture.....	10
6.3	Veeam Backup and Replication 9.5 Update 4 VMware vSphere Requirements.....	13
6.4	Veeam Backup and Replication 9.5 Update 4 Hyper-V System Requirements .....	13
6.5	Veeam Sizing Requirements.....	13
<b>7</b>	<b>Universal Storage API for Element .....</b>	<b>13</b>
7.1	Adding Element Storage Infrastructure .....	16
7.2	Creating and Deleting Element snapshots .....	21
7.3	Performing Backup from Element Snapshots.....	22
7.4	Restoring VM data from Element Snapshots.....	29
<b>8</b>	<b>Veeam Backup and Replication 9.5 Components.....</b>	<b>30</b>
8.1	Veeam Backup and Replication 9.5 Components.....	30
<b>9</b>	<b>NetApp HCI Volume Configuration Guidelines .....</b>	<b>31</b>
9.1	NetApp HCI Quality of Service .....	31
9.2	NetApp HCI Storage Configuration Guidelines for Backup and Replication 9.5 Backup Repositories .....	31
9.3	NetApp HCI Volumes as VMware Datastores .....	32
<b>10</b>	<b>NetApp HCI Host Configuration Guidelines .....</b>	<b>32</b>
10.1	Host Connectivity.....	32
<b>11</b>	<b>Element Plug-in for vCenter Server .....</b>	<b>32</b>

<b>12 Active IQ .....</b>	<b>33</b>
<b>13 Summary.....</b>	<b>33</b>
<b>Where to Find Additional Information .....</b>	<b>33</b>
NetApp HCI Documentation .....	33
Veeam Backup and Replication 9.5 Update 4 Software Documentation.....	33
<b>Version History.....</b>	<b>33</b>

## LIST OF TABLES

Table 1) Veeam sizing requirements. ....	13
Table 2) Veeam Backup and Replication 9.5 components.....	30
Table 3) Veeam Backup and Replication 9.5 components.....	31
Table 4) NetApp HCI volume QoS for VMware datastores. ....	32

## LIST OF FIGURES

Figure 1) NetApp HCI Private Cloud with dedicated Veeam backup and Replication infrastructure. ....	7
Figure 2) NetApp HCI as repositories for backup and archiving. ....	8
Figure 3) NetApp HCI production storage to E-Series and EF-Series backup repositories. ....	8
Figure 4) NetApp HCI as the Veeam backup and Replication infrastructure for FAS production storage to an E-Series backup repository. ....	9
Figure 6) Veeam Explorer for Storage Snapshots. ....	29

# 1 Executive Summary

## 1.1 The Challenge

The enterprise IT landscape is going through a digital transformation as there is a shift from hand-crafted, single-purpose data center designs to embracing new technologies that deliver agility, scalability, and greater efficiency. The hybrid cloud relies on the availability and resiliency of data. Enterprises require a complete data protection solution that is reliable, flexible, and easy to use. Although virtualizing an environment provides an increased level of data availability; meeting aggressive recovery point objectives (RPOs) and recovery time objectives (RTOs) becomes increasingly difficult.

Traditional backup tools were not created for such virtualized environments. This fact makes it hard for many organizations to take full advantage of virtualization, and many IT managers struggle with the following issues:

- Unreliable backups
- Recovery that takes too long
- High costs associated with managing backup data and secondary storage
- An inability to provide reliable, true backups for compliance purposes
- Lost productivity because of managerial complexity
- The need to scale backup operations for growth

## 1.2 The Solution

To meet these challenges, Veeam and NetApp® HCI® have collaborated to offer high-performance storage with reliable data protection that is designed for virtualized environments. Veeam and NetApp HCI help you modernize your data protection strategy with a solution that is architected from the ground up to manage large amounts of data. The solution can also handle the increasing performance and availability demands of next-generation data centers.

Veeam Backup and Replication unifies backup and replication into a single solution, increasing the value of backup and reinventing data protection for VMware vSphere and Microsoft Hyper-V virtual environments. The Veeam agentless design provides multiple backup options to meet your needs. Features such as source-side deduplication and compression, changed block tracking, parallel processing, and automatic load balancing provide fast and efficient backups.

Together, Veeam and NetApp create an optimal staging area for backups, reducing backup ingest bottlenecks and providing faster backups through parallel processing.

Veeam Backup and Replication provides the following advantages:

- Granular recovery of virtual machines (VMs) and files, including Microsoft Exchange and SharePoint application items
- The ability to automatically verify every backup, VM, and replica
- Self-service recovery of virtual machines (VMs) and guest files without a direct network connection to the VM, user permissions, or the need to deploy costly agents
- Instant VM recovery in as little as two minutes
- A choice to back up and recover what you need, where you need it, and when you need it, whether it is on-site, on tape, or in the cloud

Veeam and NetApp offer the right solution for performance, flexibility, and reliability, providing an impressive, modern disaster recovery solution for your vSphere or Hyper-V environment.

This document is a reference architecture for creating a collaborative backup and recovery solution on NetApp HCI with Veeam Backup and Replication 9.5 data protection software.

## 2 Introduction

Veeam and NetApp jointly developed this reference architecture to guide successful Backup and Replication 9.5 deployments with NetApp HCI storage and to enable data and application availability.

This solution is optimized for virtual environments, providing all-flash backup and recovery on scalable, flexible, performance-oriented NetApp HCI storage arrays. This solution provides you with superior data management for virtual environments and high availability while also making your data highly available.

NetApp HCI arrays provide a high-performing backup repository to house Veeam-created backups. With this capability, the recovery technologies that are enabled through Veeam can satisfy stringent RTOs. Recovery technologies such as Instant VM Recovery, SureBackup, and On-Demand Sandbox can achieve their full potential by using backup repositories with high I/O.

These technologies allow you to restore from your backups faster and enable capabilities such as automated recovery verification. These technologies can also use backup data as a testing environment. This capability has changed the way that users have used backups in the past because there are more benefits associated with having backups. Backups no longer sit idle, waiting for an emergency restore; instead, you can use your backups in many creative ways.

This solution includes the following capabilities:

- Recovery of a failed VM in as little as two minutes
- Near-continuous data protection with built-in replication
- Fast, agentless item recovery and e-discovery for Microsoft Exchange, SharePoint, and Active Directory, along with transaction-level recovery of SQL Server databases
- Automatic recoverability testing of every backup and every replica
- Off-site backups made up to 50 times faster than the speed of standard file copy with built-in WAN acceleration
- Fast and secure cloud backups with Veeam Cloud Connect
- Deduplication and compression to minimize storage consumption
- Off-site recovery with one-click site failover and support for facilitated data center migrations with zero data loss

### 2.1 About NetApp

[NetApp](#) is the data authority for hybrid cloud. We provide a full range of hybrid cloud data services that simplify management of applications and data across cloud and on-premises environments to accelerate digital transformation. Together with our partners, we empower global organizations to unleash the full potential of their data to expand customer touchpoints, foster greater innovation, and optimize their operations.

### 2.2 About Veeam

[Veeam](#) recognizes the new challenges that companies across the globe face in enabling the always on business, one that must operate 24 hours a day, 7 days a week, and 365 days a year. To address this challenge, Veeam delivers availability for the modern data center by making sure that RTOs and RPOs are less than 15 minutes for all applications and data. Veeam corporate headquarters are located in Baar, Switzerland, and the main Americas office is located in Columbus, Ohio.

### 3 NetApp HCI Private Cloud - Running Demanding Workloads in a Multitenant Environment

Moving to the private cloud is a journey. Most organizations start small and grow the environment over time. NetApp has developed, in collaboration with VMware, a private cloud solution that starts with a small footprint and can grow compute and storage independently as workloads and performance expectations change.

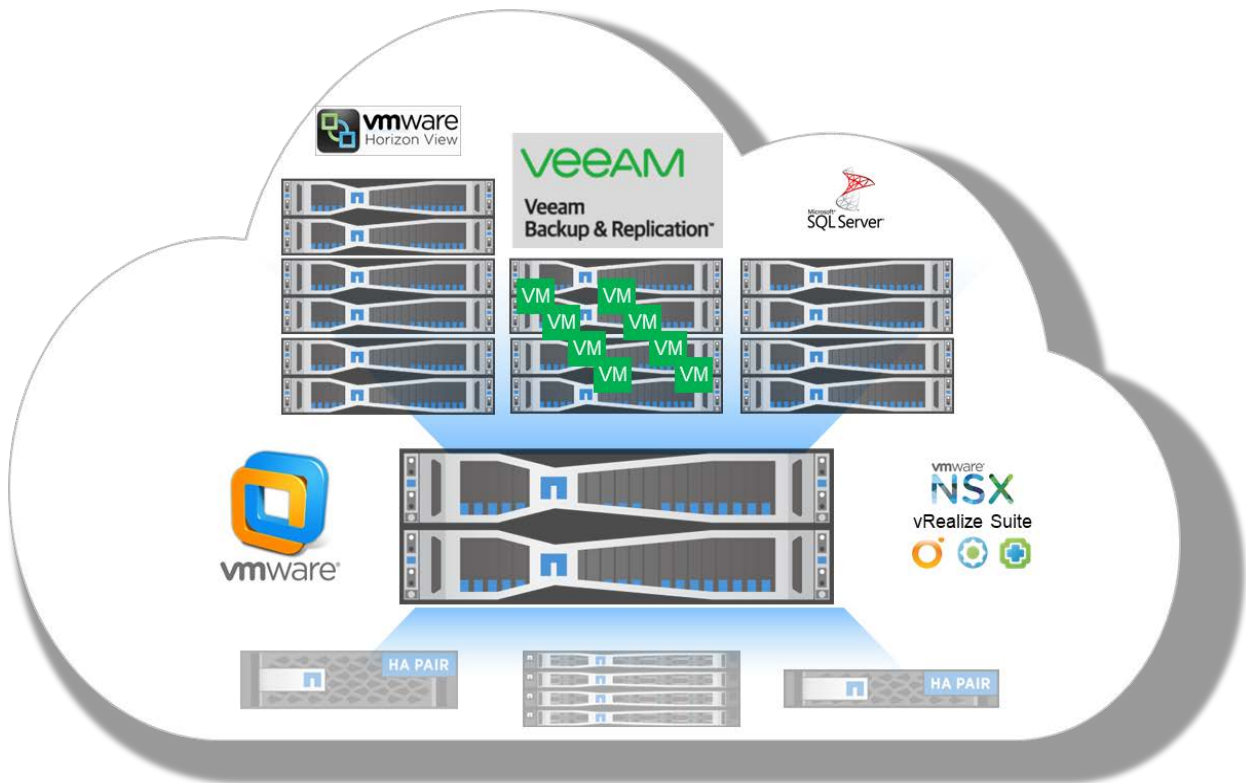
NetApp has multiple documents and deployment services describing how to deploy VMware Private Cloud on NetApp HCI. Two primary documents are [VMware Validated Design \(VVD\)](#) and the [NetApp Verified Architecture \(NVA\)](#) for VMware Private Cloud on NetApp HCI. These documents provide guidelines, best practices, and deployment documentation for a VMware private cloud, using the VMware vRealize Suite of products and NSX, with NetApp HCI.

With NetApp HCI, you can deploy and support multitenant environments running diverse applications and workloads in a single infrastructure. You can choose the most suitable storage for the application or workload and scale the compute and storage independently. Also, the NetApp Data Fabric enables users to connect their private cloud ecosystem on NetApp HCI to the hyperscalers to deliver a seamless hybrid multicloud experience.

For more information about the NetApp Data Fabric, see [What Is Hybrid Multicloud Experience?](#)

Figure 1 shows a NetApp HCI deployed with VMware private cloud running multiple workloads. Choose the NetApp storage that matches the application needs. In this example, Veeam can back up both the NetApp HCI environment and any other source in the data center.

Figure 1) NetApp HCI Private Cloud with dedicated Veeam backup and Replication infrastructure.



## 4 Reference Architecture Overview

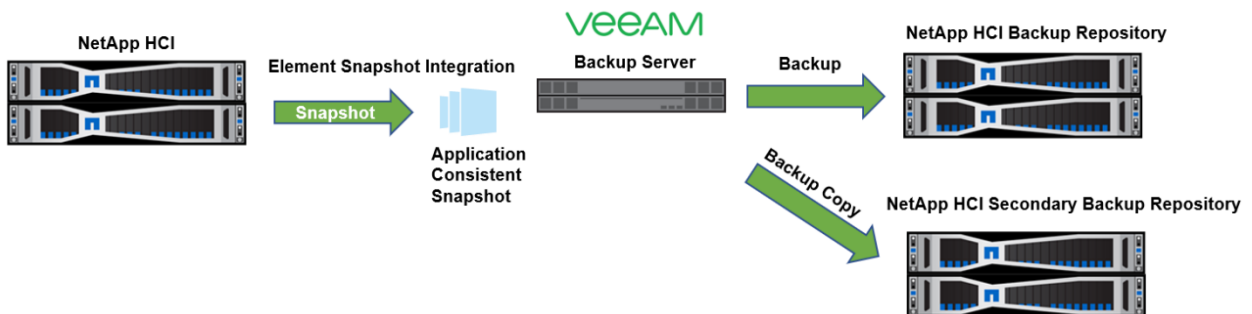
This section describes reference architectures that range from small environments that protect a few terabytes of data to large enterprise-size environments with petabytes of data under management.

### 4.1 Deployment Scenarios

#### NetApp HCI as Veeam Backup and Replication Repositories for Backup and Archiving

Figure 2 depicts a typical NetApp HCI and Veeam setup.

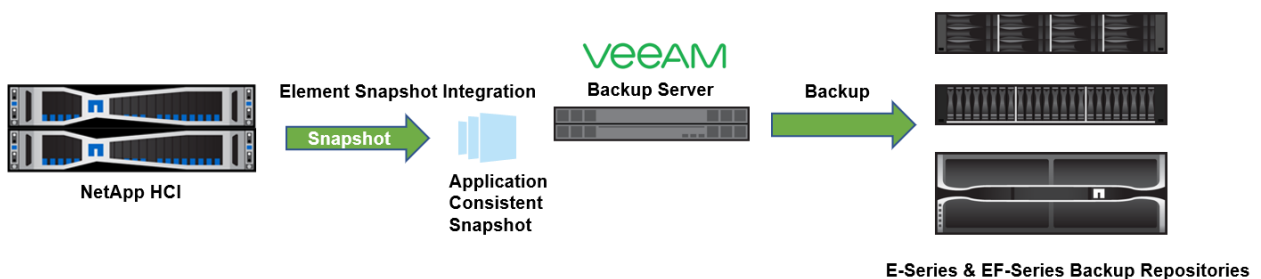
Figure 2) NetApp HCI as repositories for backup and archiving.



#### NetApp HCI Production Storage with Veeam Backup and Replication to E-Series and EF-Series Backup Repositories

Figure 3 depicts NetApp HCI production storage with to NetApp E-Series and EF-Series backup repositories.

Figure 3) NetApp HCI production storage to E-Series and EF-Series backup repositories.

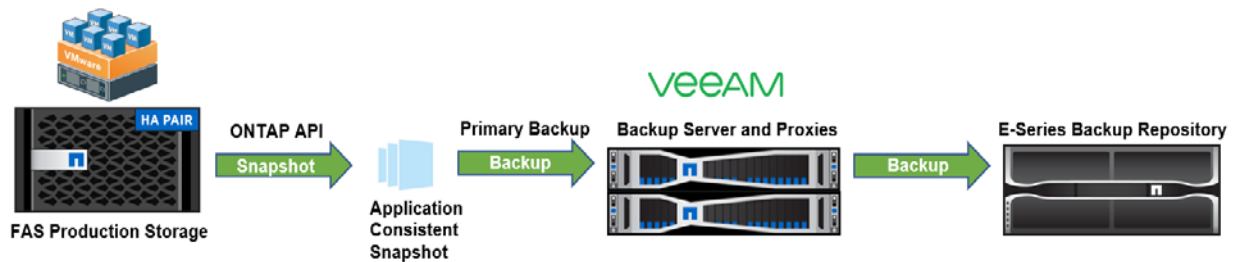


#### NetApp HCI as a Veeam Backup and Replication Backup Repository for FAS Production Storage

Figure 4 depicts Veeam integration with a NetApp FAS-series production storage array, with newly created backups going to a NetApp HCI array for storage. To provide disaster recovery, backups can also be sent off the premises to another backup repository (another NetApp HCI system). Veeam provides a backup copy job for such scenarios. This job can be used for backups off the premises or for long-term archiving by using Veeam's built-in Grandfather-Father-Son (GFS)-type retention.



Figure 4) NetApp HCI as the Veeam backup and Replication infrastructure for FAS production storage to an E-Series backup repository.



## 5 NetApp HCI and Veeam

### 5.1 Predictable Quality of Service and Always-On Availability for Element Hybrid Cloud Infrastructures

Veeam availability solutions combined with fully scalable, predictable, and automated NetApp HCI enable organizations to achieve predictable application performance and availability while simplifying IT operational management, enhancing agility, lowering costs, and advancing their digital transformation initiatives.

NetApp Element<sup>®</sup> software enables NetApp HCI to power cloud environments by allowing administrators to consolidate workloads onto a single infrastructure without sacrificing performance. Element provides enterprise-grade reliability, all-flash performance, and secure multitenancy in an innovative architecture that delivers unmatched agility through scalability, predictability, and automation.

Through its fine-grained performance control, Element delivers predictable storage quality of service (QoS) for every workload to ensure consistent application performance, regardless of the number of applications or the size of the cluster. Each storage volume within a NetApp HCI cluster can be allocated a precise amount of capacity and performance, both of which can be changed spontaneously without migrating data or interrupting I/O.

Although Element provides flexibility to scale your data when you need it most, it does so without compromising protection. Designed for tomorrow's applications and data demands, native data protection delivers ironclad data assurance through a resilient, self-healing architecture that reduces operational overhead and risk. Local snapshots enable space-efficient, point-in-time copies of your data for rapid restore. With the built-in synchronous and asynchronous replication of Element, data can be copied quickly between multiple sites, regardless of where the NetApp HCI clusters physically sit.

### 5.2 NetApp HCI Key Features

Following are some of the important features of NetApp HCI:

- **Guaranteed performance**
  - Allocate storage performance independent of capacity
  - Manage performance in real time without affecting other volumes
  - Guarantee performance to every volume with fine-grain quality-of-service (QoS) settings
- **Global efficiency**
  - Inline and post-compression
  - Automatic distribution of data (no hot spots) with always-on deduplication
  - Global thin provisioning
- **Data assurance**

- NetApp HCI Helix® RAID-less data protection
- Real-time replication (synchronous and asynchronous)
- Integrated backup and recovery (cloud)
- Complete data and performance availability regardless of system condition or application activity
- Data safeguarded with 256-bit encryption

## Enterprise Reliability and Availability

NetApp HCI also provides the following features that support enterprise reliability and availability:

- Data assurance
  - To provide data redundancy, NetApp HCI maintains two copies of every data block on two separate nodes through a technology called Helix that is built into Element. This feature allows a cluster to sustain application performance even after failures occur. It also takes away the need to have separate storage shelves with shared drive access, making the hardware less complex and less expensive.
- Self-healing from failures
  - **Active pool.** All resources in the system are always in the active pool. There is no need to have spare drives or spare nodes sitting idle if there is a failure.
  - **Drive failure.** If a drive fails, the system automatically restores full redundancy by redistributing copies of data by using a meshed rebuild process. There is no degraded mode operation and no performance penalty during a rebuild. The process typically completes in five minutes or less. Because of the speed with which full redundancy is restored, this feature provides a level of data protection that exceeds RAID 6 in a typical system.
  - **Node failure.** Because data copies are distributed on separate nodes, all data remains accessible if a node fails. Connections to the failed node are automatically redirected to other nodes. As with a drive failure, full redundancy is restored quickly and automatically by making sure that there are two copies of each block.

Regardless of the failure mode—drive, node, backplane, network failure, or software failure—the recovery process is the same. Because the recovery workload is distributed across all nodes in the cluster, redundancy is restored quickly, and no single node or application workload takes a performance hit. The more nodes in the cluster, the faster the activity occurs and the lower the overall affect.

- Active support
  - Element provides all the features you demand from primary storage—total reliability, all-flash performance, end-to-end security, and more—plus all five criteria for delivering agile, predictable storage performance.

## 6 Veeam Backup and Replication 9.5 Update 4

### 6.1 Overview

Veeam Backup and Replication is a data protection and disaster recovery solution for VMware vSphere and Microsoft Hyper-V virtual environments of any size or complexity. By combining all the necessary functions in one intuitive interface, Veeam Backup and Replication solves the most critical problems of virtualized infrastructure management. The solution also protects mission critical VMs from both hardware and software failures.

### 6.2 Solution Architecture

Veeam Backup and Replication is composed of the following three elements:

- Backup server
- Backup proxy
- Backup repository

## Veeam Backup Server

The Veeam backup server is the Windows-based physical machine or VM on which Veeam Backup and Replication is installed. It is the core component in the backup infrastructure that fills the role of the configuration and control center. The Veeam backup server performs all types of administrative activities, including the following tasks:

- It coordinates backup, replication, recovery verification, and restore tasks.
- It controls job scheduling and resource allocation.
- It is used to set up and manage backup infrastructure components and to specify global settings for the backup infrastructure.

In addition to its primary functions, a newly deployed Veeam backup server also acts as a default backup proxy and the backup repository (it manages data handling and data storing tasks).

The Veeam backup server uses the following services and components:

- **Veeam backup Service.** A Windows service that coordinates all the operations that Veeam Backup and Replication performs, such as backup, replication, recovery verification, and restore tasks. The Veeam Backup Service runs under the local system account or an account that has the local administrator permissions on the backup server.
- **Veeam broker service.** Interacts with the virtual infrastructure to collect and cache the virtual infrastructure topology. Jobs and tasks query information about the virtual infrastructure topology from the broker service, which accelerates job and task performance.
- **Veeam backup catalog/guest catalog service.** Manages guest OS file system indexing for VMs and replicates system index data files to enable search through guest OS files. Index data is stored in the Veeam backup catalog, which is a folder on the backup server. The Veeam guest catalog service running on the backup server works with search components that are installed on Veeam Backup Enterprise Manager and (optionally) a dedicated Microsoft Search Server.
- **Veeam mount service.** Mounts backups and replicas for file-level access, browsing the VM guest file system, and restoring VM guest OS files and application items to the original location.
- **Veeam backup proxy services.** In addition to dedicated services, the backup server runs a set of data-mover services. For details, see the section “Backup Proxy.”
- **Veeam backup and replication configuration database.** Stores data about the backup infrastructure, jobs, sessions, and so on. The database instance can be on a SQL Server that is installed either locally on the same machine where the backup server is running or remotely.
- **Veeam backup and replication console.** Provides the application UI and allows user access to the application’s functionality.
- **Veeam backup Windows PowerShell snap-in.** An extension for Microsoft Windows PowerShell 2.0. Veeam Backup PowerShell adds cmdlets that enable you to perform backup, replication, and recovery tasks through the PowerShell CLI or run custom scripts. In this way, you can fully automate Veeam Backup and Replication operation.

## Backup Proxy

When Veeam Backup and Replication is first installed, the Veeam backup server coordinates all job activities and handles data traffic. Therefore, when you perform a backup, replication, VM copy, or VM migration job or perform restore operations, VM data is moved from the source to the target through the Veeam backup server. This scenario is acceptable for virtual environments in which few backup jobs are

performed. In large-scale environments, however, the workload on the Veeam backup server is significant.

To take the workload off the Veeam backup server, Veeam Backup and Replication uses backup proxies. A backup proxy is an architecture component that sits between the data source and the target and is used to process jobs and deliver backup traffic. Backup proxy tasks include retrieving VM data from production storage. Tasks also include compressing the data and sending it to the backup repository (for example, if you run a backup job) or to another backup proxy (for example, if you run a replication job). As a data handling task is assigned to the backup proxy, the Veeam backup server becomes the point of control for dispatching jobs to proxy servers.

The role of a backup proxy can be assigned to a dedicated Windows Server (physical or virtual) in your virtual environment. You can deploy backup proxies in both the primary site and remote sites. To optimize the performance of several concurrent jobs, you can use multiple backup proxies. In this case, Veeam Backup and Replication distributes the backup workload between available backup proxies.

By using backup proxies, you can easily scale your backup infrastructure up and down according to your demands. Backup proxies run lightweight services that take a few seconds to deploy, and deployment is fully automated. Veeam Backup and Replication installs the necessary components on a Windows-based server when you add it to the product console. When you assign the role of a backup proxy to the added server, Veeam Backup and Replication starts the required services on it.

The primary role of the backup proxy is to provide an optimal route for backup traffic and to enable efficient data transfer. Therefore, when deploying a backup proxy, you must analyze the connection between the backup proxy and the storage with which it is working. Depending on the type of connection, the backup proxy can be configured in one of the following ways (starting with the most efficient):

- A machine used as a backup proxy should have direct access to the storage on which VMs reside or to the storage to which VM data is written. In this way, the backup proxy retrieves data directly from the datastore, bypassing the LAN.
- The backup proxy can be a VM with HotAdd access to VM disks on the datastore. This type of proxy also enables LAN-free data transfer.
- If neither of the preceding scenarios is possible, you have alternatives. You can assign the role of the backup proxy to a machine on the network that is closer to the source or closer to the target storage with which the proxy works. In this case, VM data is transported over the LAN by using the Network Block Device (NBD) protocol.

Depending on the type of backup proxy and your backup architecture, the backup proxy can use one of the following data transport modes: direct SAN access, virtual appliance, or network. If the VM disks are on the SAN storage and the SAN storage is added to the Veeam Backup and Replication console, the backup proxy can also use the backup from storage snapshots mode. You can select the transport mode or let Veeam Backup and Replication automatically choose it.

The backup proxy uses the following services and components:

- **Veeam installer service.** An auxiliary service that is installed and started on any Windows Server after it is added to the list of managed servers in the Veeam Backup and Replication console. This service analyses the system and installs and upgrades necessary components and services depending on the role that is selected for the server.
- **Veeam transport.** Responsible for deploying and coordinating executable modules that act as data movers and that perform the main job activities on behalf of Veeam Backup and Replication. These activities include communicating with VMware Tools, copying VM files, performing data deduplication and compression, and so on.

## Backup Repository

A backup repository is a location that Veeam Backup and Replication jobs use to store backup files, copies of VMs, and metadata for replicated VMs. Technically, a backup repository is a folder on the

backup storage. By assigning different repositories to jobs and by limiting the number of parallel jobs for each one, you can balance the load across your backup infrastructure.

### 6.3 Veeam Backup and Replication 9.5 Update 4 VMware vSphere Requirements

For more information about Veeam backup and replication requirements for VMware, see the [Guide for VMware vSphere - Planning and Preparation](#).

### 6.4 Veeam Backup and Replication 9.5 Update 4 Hyper-V System Requirements

For more information about Veeam backup and replication requirements for Hyper-V, see the [Guide for Hyper-V - Planning and Preparation](#).

### 6.5 Veeam Sizing Requirements

For Veeam sizing requirements, see Table 1

Table 1) Veeam sizing requirements.

Veeam Sizing Requirements		
Veeam backup proxy	<b>Virtual.</b> 1 vCPU for every 200 VMs (recommended minimum: 2 vCPUs), 4GB RAM, 300MB disk space for installed components, and a VMXNET3 network interface card (NIC). No CPU or memory reservations are required.	<b>Physical.</b> 1 CPU core for every 250 VMs, 2GB of RAM for each concurrent Virtual Machine Disk (VMDK) backup.
Veeam backup server	4GB of RAM plus 500MB of RAM for each concurrent job. Disk space: 2GB for the product, plus 10GB per 100 VMs for a guest file system catalog and at least 10GB for a VM recovery cache folder. No CPU or memory reservations are required. More sizing considerations should be applied if the back-end SQL Server is deployed on this server. For more guidance, see the Veeam documentation.	
Veeam repository	The Veeam repository can be collocated with the backup server role for small deployments or on a dedicated server (physical or virtual Windows or Linux server, NAS device, or dedicated backup appliance). The repository requires sufficient free space to store all backup job data. If a VM is used, NetApp recommends using the VMware Para virtual SCSI (PVSCSI) controller for the disk or disks that store backup data. vSphere 5.5 enables the use of disks larger than 2TB, which might be advantageous for a repository server.	

## 7 Universal Storage API for Element

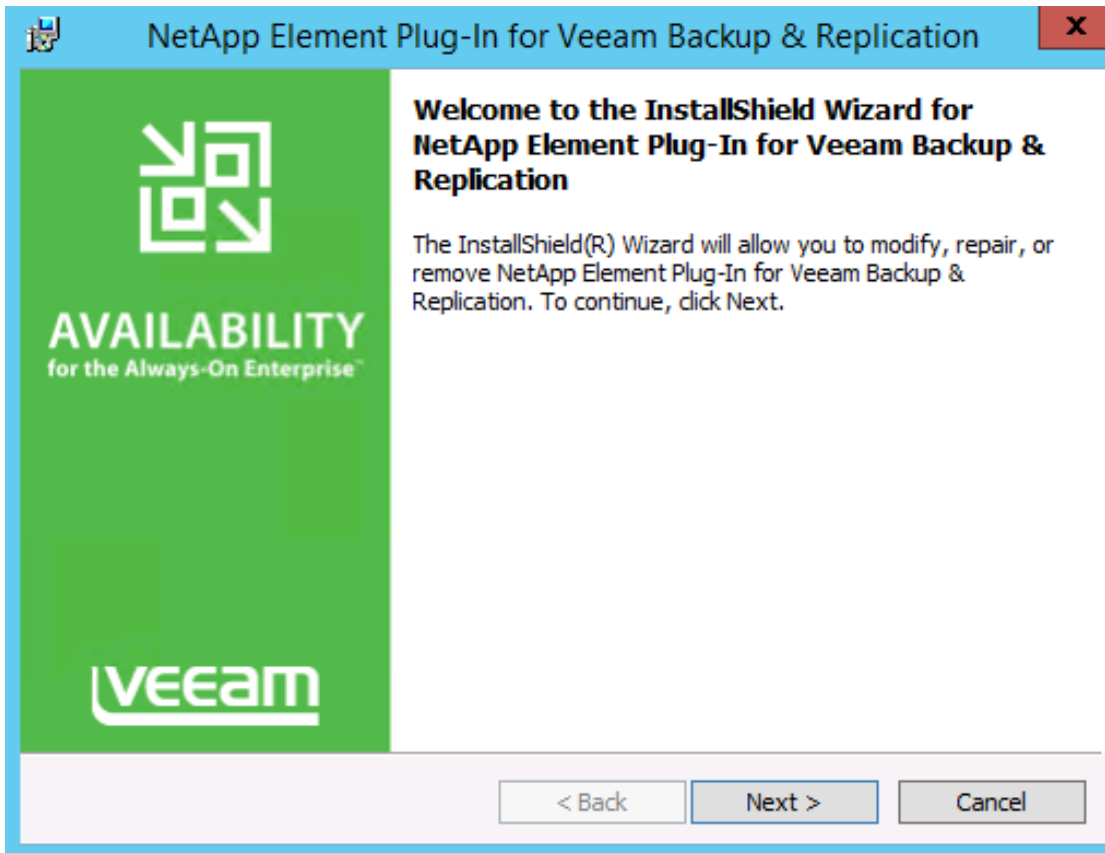
Veeam Backup and Replication offers built-in integration with Element to help decrease the impact on the production environment and significantly improve RPOs. With this integration, you can use Element snapshots to perform backup and restore operations for VMware environments.

To start working with the Universal Storage API for Element, you must perform the following steps:

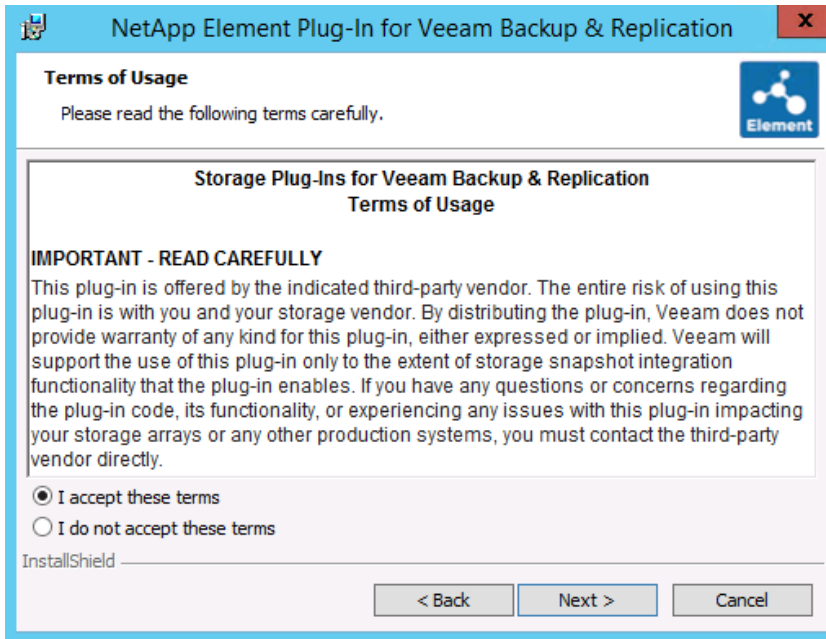
1. Download the Element plug-in from the [Veeam Download page](#)

<b>NetApp Element Plug-In for Veeam Backup &amp; Replication (for HCI/SolidFire storage)</b>  Requires: NetApp HCI (Element 10.0 or later), NetApp Solidfire (Element 9.0 or later), iSCSI models only Veeam Backup & Replication 9.5 Update 4 or later	Offered by <a href="#">NetApp, Inc.</a>  Subject to NetApp, Inc. T&C.	Version: 1.0.9  <b>DOWNLOAD</b>  January 23, 2019
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------	---------------------------------------------------------------

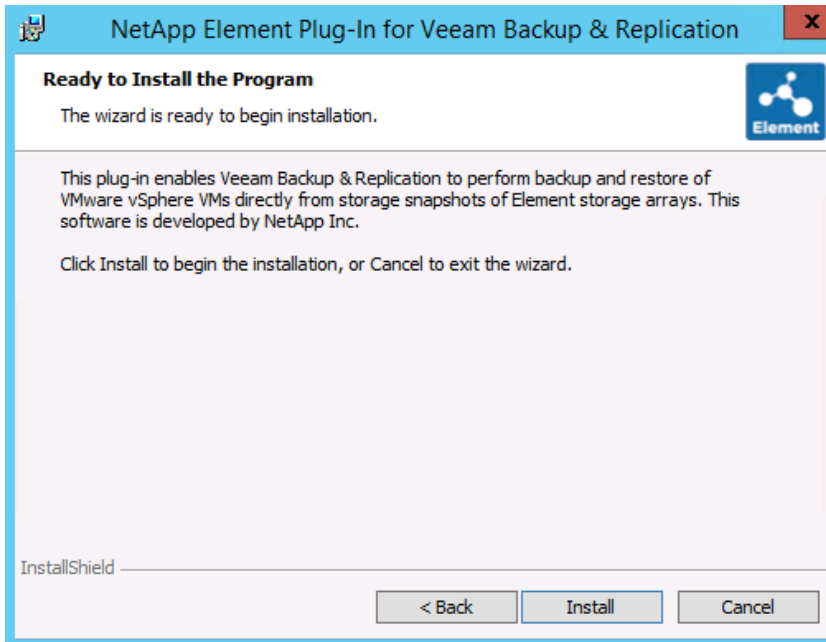
2. Run the setup wizard to install the plug-in.
  - a. Install the Element software Plugin. Run the .exe and click Next to begin installation.



- b. Accept the Terms of Usage and click Next to continue.

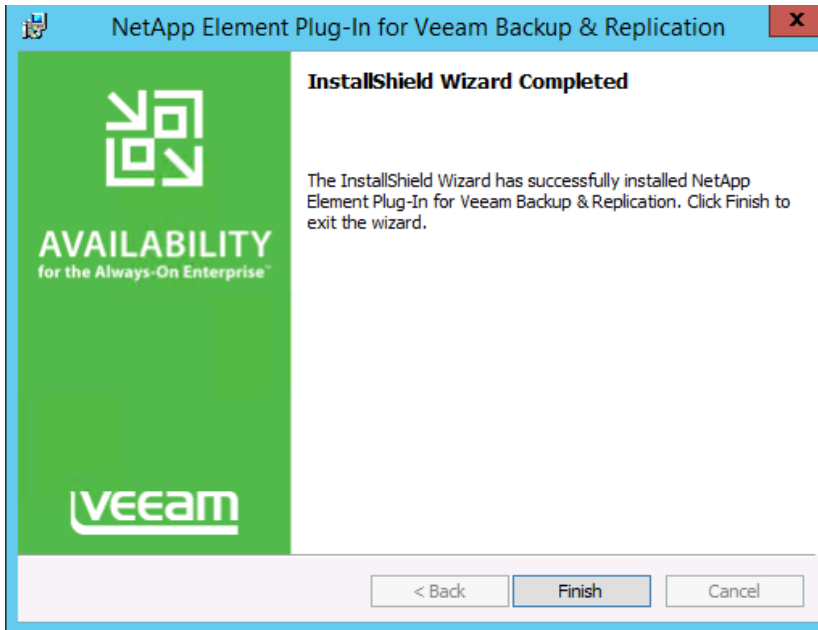


- c. Click Install to begin the installation process.



- d. After the installation complete, click Finish and continue to the next section.





3. Configure the backup infrastructure for storage snapshots.

## 7.1 Adding Element Storage Infrastructure

Veeam Backup and Replication lets you apply NetApp Element software Storage snapshots as a part of a comprehensive backup and recovery strategy, where storage hardware-based snapshots and image-level backups complement each other. With Veeam Backup and Replication, you can:

- Perform backups from Element Storage snapshots
- Restore data directly from Element Storage snapshots
- Perform snapshots-only backups (Snapshot™ Orchestration)

Before working with Element Storage snapshots in Veeam Backup and Replication, the backup infrastructure must be properly configured. The Veeam backup server's proxy component is used for re-scanning VMware Virtual Machine File System (VMFS) on Element Storage volumes and for performing backup from Element Storage snapshots. For the proxy component to perform these functions, it must have a Microsoft iSCSI Software initiator enabled. Backup from storage snapshots requires the Microsoft iSCSI initiator. iSCSI traffic between the backup proxy and storage system must be allowed.

1. To start using storage snapshots for backup and restore, the Element Storage system must be added to Veeam. To do so, open the SAN Infrastructure view, click Add Storage.



2. From the storage vendors list, select Element Storage.





## ELEMENT

Adds support for NetApp HCI and Element storage clusters. iSCSI connectivity is supported

3. In the Name step of the wizard, specify the name and description for the Element Storage system in the DNS name or IP address field.

4. In the Description field, provide a description for future reference. After the description is complete, click Next.

**Note:** The default description contains information about the user who added the Element Storage system and the date and time when the storage system was added.

**New Element Storage**

**Credentials**  
Type in storage administrator credentials.

Name

**Credentials**

Access Options

Summary

Select credentials with Local Administrator privileges on the server you are adding

Credentials: admin (admin, last edited: 6 days ago) Add...

Port: 443

[Manage accounts](#)

< Previous Next > Finish Cancel

- Next, from the Credentials list, select the credentials for the user account to connect to the Element Storage system. If the necessary credentials are not set up beforehand, click the Add button to the right or the Manage accounts link to add the necessary credentials.

**Note:** The account selected must have administrative privileges on the Element Storage system.

**New Element Storage**

**Access Options**  
Specify how this storage can be accessed by Veeam.

Name

Credentials

**Access Options**

Summary

Protocol to use:

☐ Fibre Channel (FC)

☒ iSCSI

☐ NFS

Volumes to scan:

Automatic detection (all VMFS volumes found with the initial scan) Choose...

Backup proxies to use:

Automatic selection Choose...

< Previous Next > Finish Cancel

6. From the Protocol to use list, check the protocol type that Veeam should use to back up data from the Element Storage system.

Choose Volumes

Choose storage volumes which should be scanned periodically to detect and catalog newly added VMs. Limiting the amount of volumes to scan reduces storage load.

☒ Automatic detection (all VMFS volumes found with the initial scan)

☐ All volumes except:

Name
------

Add... Remove

☐ Only these volumes:

Name
------

Add... Remove

OK Cancel

7. The Volumes to scan option enables customization of the volumes that Veeam should scan for VMs and existing snapshots.

**Note:** NetApp recommends this selection be made if you have volumes that contain non-VM data.

Backup Proxy

Choose backup proxies servers for this job. For redundancy, we recommended to select at least two proxies. When multiple proxies are available, selection will be performed on per-VM basis, taking into account proxy connectivity and current load.

☒ Automatic selection  
The job will automatically select the most suitable backup proxy server from all available backup proxy servers.

☐ Use the selected backup proxy servers only  
The job will automatically select the most suitable backup proxy server from the following list of proxy servers.

Name
<input type="checkbox"/> VMware Backup Proxy

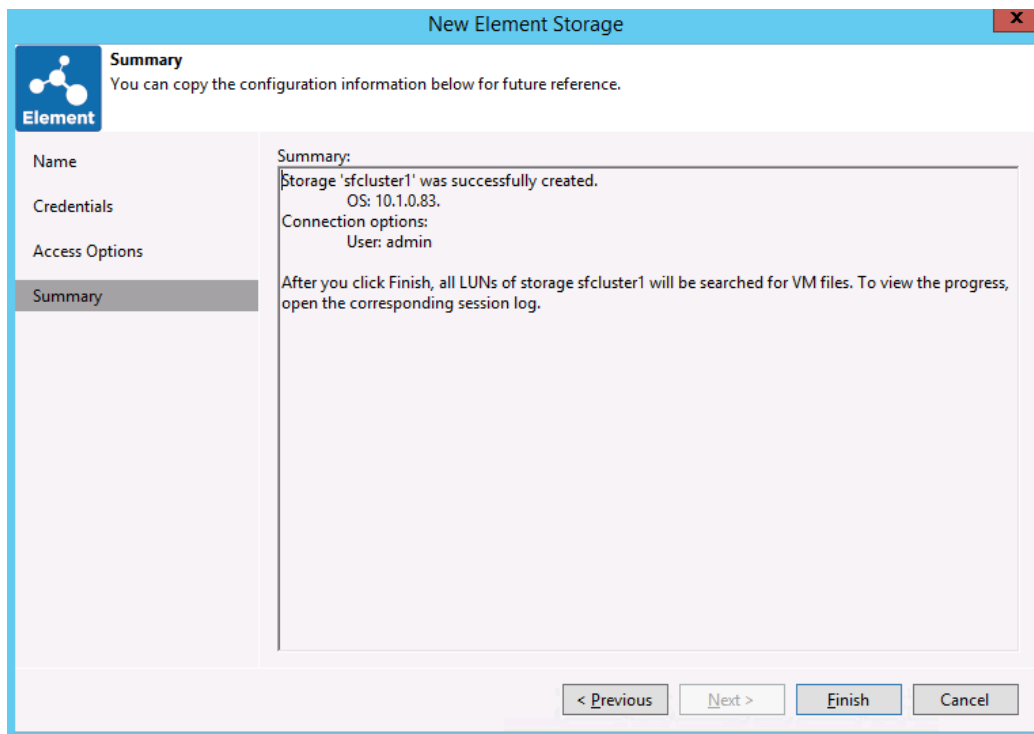
Select All

Clear All

OK Cancel

**Note:** The Backup Proxy selection is also important if you have multiple locations and multiple Element Storage arrays to manage. Proxies can be assigned to specific Element Storage arrays to keep volume rescans and other management operations local to the storage.

8. Review the summary information and click Finish.
9. After you click Finish, Veeam performs the Element Storage discovery operation; it rescans the storage LUNs and locate VM files on them.



10. The details of the rescan process are displayed in the System window. This window can be closed and a review of the rescan details can be accessed later in the History view of Veeam Backup and Replication. Click Close after the discovery is completed.
11. Storage rescans are performed automatically. Veeam discovers new volumes and snapshots or remove deleted volumes and snapshots from the storage system hierarchy. If necessary, a storage rescan can also be initiated manually.
12. To perform a manual, rescan of the storage system, follow these 4 steps:
  - a. Open the SAN Infrastructure view.
  - b. In the inventory pane, expand a tree of the storage system to rescan.
  - c. Select the necessary node in the storage system hierarchy: storage system, volume and so on.
  - d. Click Rescan on the ribbon. Alternatively, you can right-click the necessary node in the hierarchy and select Rescan.

Now you can use Universal Storage API for Element snapshots for data protection and disaster recovery operations.

## 7.2 Creating and Deleting Element snapshots

Creating and deleting storage snapshots can be performed from the Veeam Backup and Replication interface. Create and delete snapshot copy operations do not differ from create/delete snapshot operations performed through the Element Storage cluster management dashboard, and any snapshots created manually are crash-consistent.

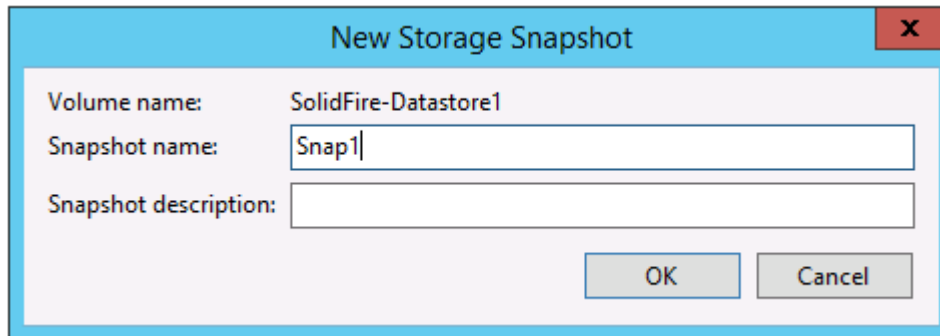
Creating a volume snapshot:

1. Open the SAN Infrastructure view.
2. In the inventory pane, expand a tree of the necessary storage system.
3. Right-click the necessary volume and select Create Snapshot.

4. In the New SAN Snapshot window, specify a name for the created snapshot and provide a snapshot description.

Deleting a volume snapshot:

1. Open the SAN Infrastructure view.
2. In the inventory pane, expand a tree of the necessary storage system.
3. Right-click the necessary snapshot and select Delete Snapshot.



The screenshot shows a 'New Storage Snapshot' dialog box. It has a blue title bar with the text 'New Storage Snapshot' and a red close button. The dialog contains three input fields: 'Volume name' with the value 'SolidFire-Datastore1', 'Snapshot name' with the value 'Snap1', and 'Snapshot description' which is empty. At the bottom right are 'OK' and 'Cancel' buttons.

### 7.3 Performing Backup from Element Snapshots

Backup jobs can be configured to use Veeam Backup from Storage Snapshot technology, which uses Element Storage system snapshots for backup operations. Instead of reading data from VMware VM snapshots, Veeam reads data from storage snapshots, which speeds up backup operations and improves recovery point objectives (RPOs). Veeam is also able to orchestrate snapshots between Element Storage arrays without taking a backup. Combining snapshot orchestration along with backups can offer more aggressive RPOs.

#### Back up from Storage Snapshots: Backup Job Creation

1. To create a backup from storage snapshots job, select Backup and Replication under the Home tab. Click the Backup Job button to begin.
2. When the New Backup Job wizard displays, enter a name for the backup job. Click Next.

**Note:** Below the job name is the Description box. By default, this box is populated with the user who created the job along with a date and time stamp. Optionally, more text can be added.

**New Backup Job**

**Name**  
Type in a name and description for this backup job.

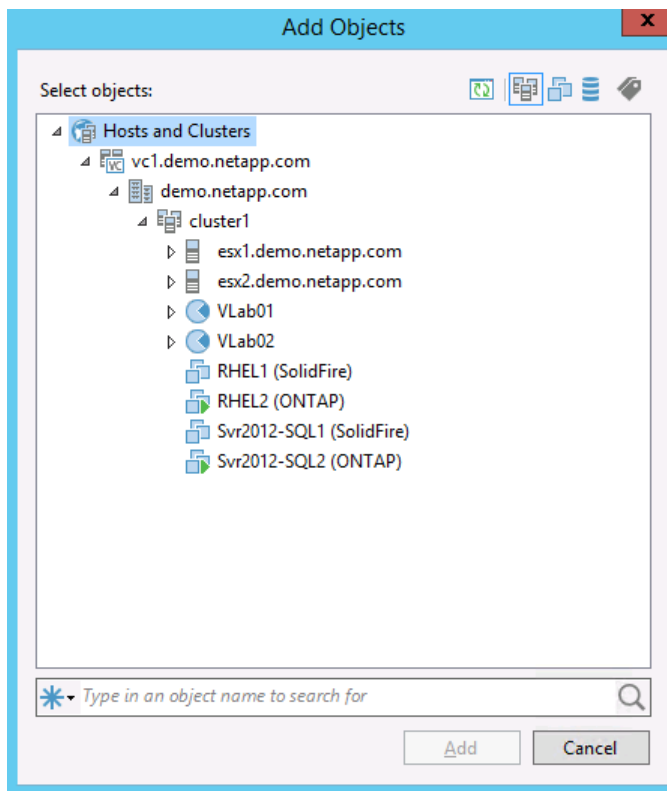
**Name:**  
Backup from Storage Snapshots

**Description:**  
Created by DEMO\Administrator at 12/20/2018 9:13 AM.

< Previous   Next >   Finish   Cancel

3. Click Add to add VMs to the job. The Add Objects window opens.

**Note:** There are multiple options for adding virtual machines into the backup job. Virtual machines can be selected individually, or an entire container can be selected. Some of the options are entire hosts, clusters, datastores, folders, and VM tags. Because this job uses volume snapshots on the Element Storage array, a recommendation is based on the datastore. Click Next to move on.



4. Using Storage options, you can select a specific proxy to use for the backup, but by default the Backup proxy is selected automatically. You can select Backup repository by clicking on the drop-down button for the location where the newly created backup files are stored. Retention policy enables you to specify the desired number of restore points to retain.

**Note:** There is also an option to Configure secondary destinations for this job, if this option is selected, a new menu is available for selecting the secondary destination. Secondary destinations can include a backup copy job, tape job, or an Element Storage snapshot. Click the Advanced button in the lower right-hand corner to see where the integration settings for the job are located. Keep in mind that if you want to perform backups from snapshots on the secondary array, the Configure secondary destinations for this job box needs to be checked and the Backup repository should be located local to the secondary array. Click Next to continue.



**New Backup Job**

**Storage**  
Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

**Name**

**Virtual Machines**

**Storage**

**Guest Processing**

**Schedule**

**Summary**

Backup proxy: Automatic selection Choose...

Backup repository: Backup2Disk (Created by Veeam Backup) 372 GB free of 399 GB Map backup

Retention policy

Restore points to keep on disk: 14 i

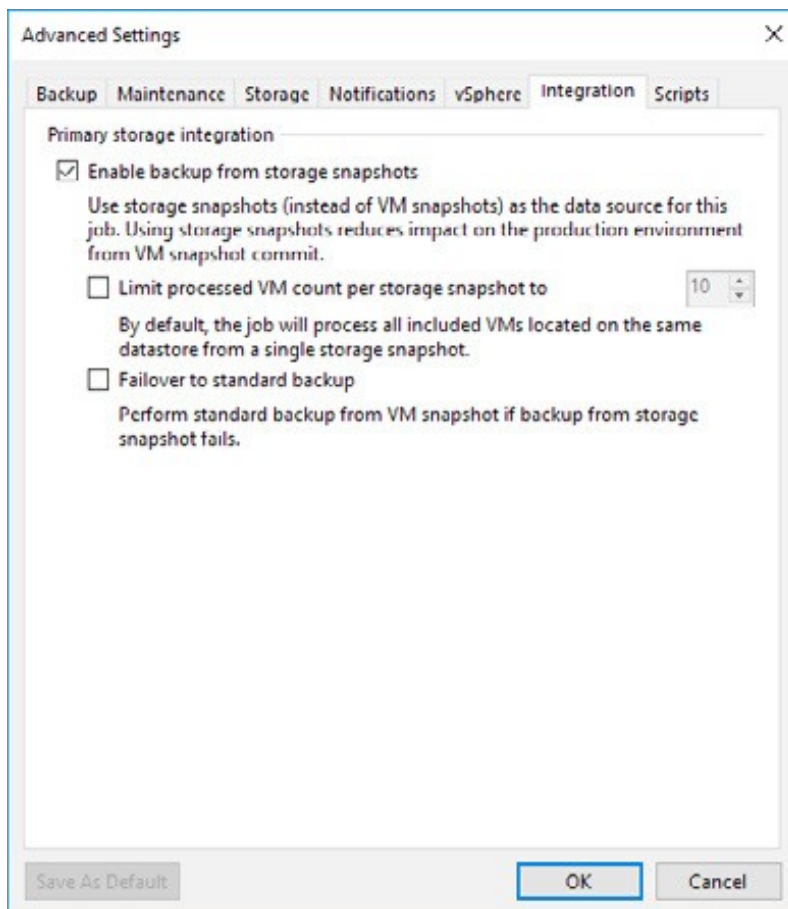
☐ Configure secondary destinations for this job  
Copy backups produced by this job to another backup repository, or to tape. Best practices recommend maintaining at least 2 backups of production data, with one of them being off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings. Advanced

< Previous Next > Finish Cancel

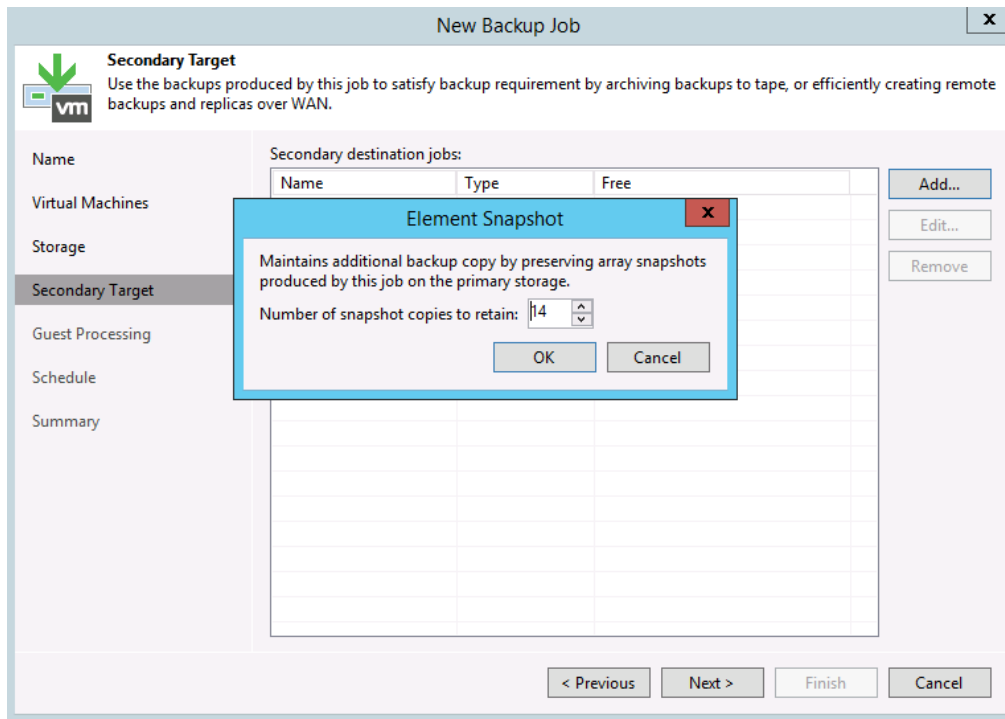
5. Click the Integration tab when the Advanced setting window is available. On the Integration tab, the Enable backup from storage snapshots box should already be checked by default. If it is not checked, then check it.

**Note:** Other options include limiting the number of process VMs per storage snapshot and failover options for the job. There are many other tabs available that change different aspects of the backup job. For this guide, the other tabs are not covered. See the Veeam user guide for details about other tabs. Click OK and click Next back at the Storage menu to proceed.



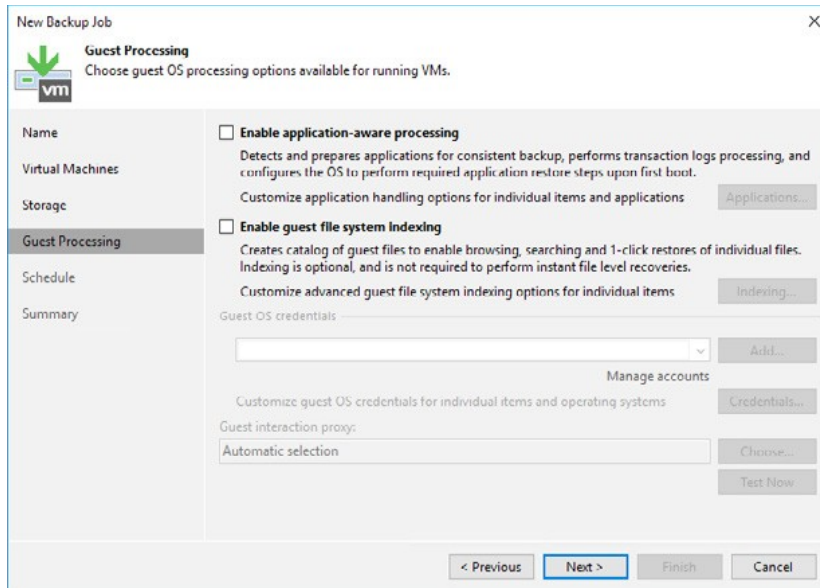
6. If the secondary target option was checked, the next step includes the Secondary Target options. Click Add on the right side of the window and a selection box opens. Here, you can retain the storage snapshot and apply a specified retention policy. Jobs allow you to add a backup copy job or tape job. Element Storage Snapshot enables you to set retention for the snapshot on the primary Element Storage array.

**Note:** By default, when Veeam completes the backup, it removes the storage snapshot. This option needs to be selected if Element Storage snapshot retention is desired on the primary array. Click OK and then click Next to continue.



7. Guest Processing is the next step in the backup job wizard. This is an important step if application consistency is desired for both the snapshot and backup files.
  - a. To enable, check the Enable application-aware image processing box. This option requires Guest OS credentials.
  - b. Click Add next to the Guest OS credentials to add a set of credentials or choose credentials from the drop-down box.
  - c. There is also an Applications button. The enable application-aware processing button opens a new window where you can select a VM or object you are backing up and Edit the way it is processed.
  - d. Editing a VM or object opens the Processing settings window with multiple tabs. These tabs include General, SQL Server, Oracle, File Exclusions, and Scripts.

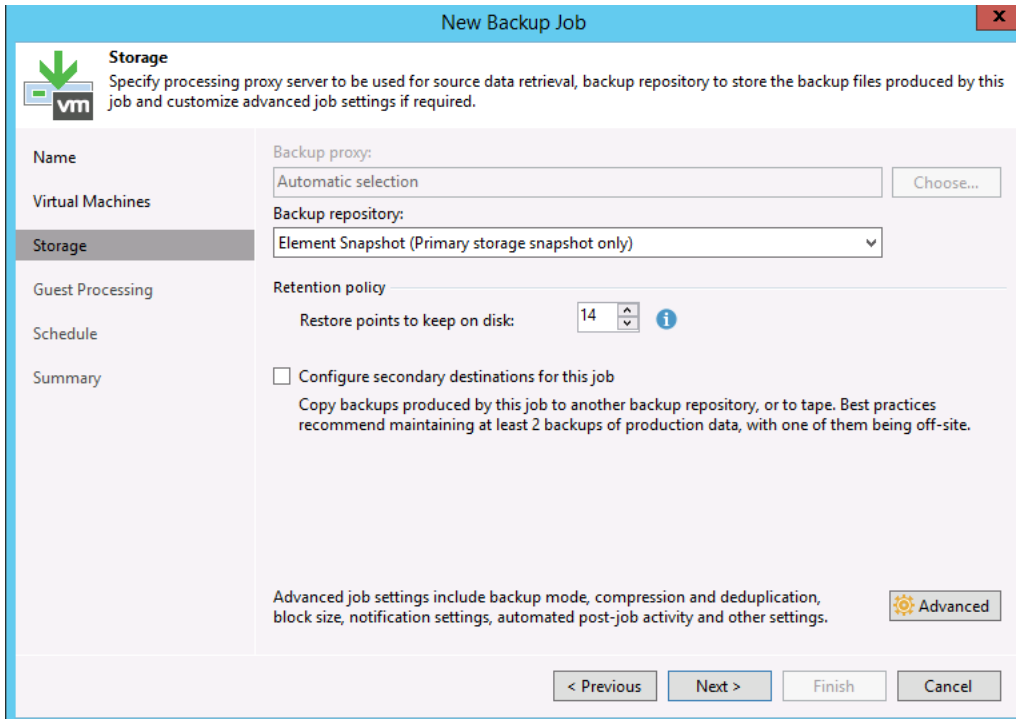
**Note:** If you would like more detail about these options, refer to the Veeam user guide. Under Guest Processing, there is also an option to Enable guest file system indexing. Enabling this option enables Veeam to create a searchable catalog of the guest files. It also enables features such as 1-click restores. To use the catalog, the optional Veeam Backup Enterprise Manager should be installed. File system indexing also requires Guest OS credentials. There is an Indexing button next to the setting that allows for customization of the indexing that Veeam performs. The last setting in this section is the Guest interaction proxy. By default, Veeam selects an appropriate proxy to perform this interaction, but you can explicitly select the desired proxy or number of proxies. There is also a Test Now button near the bottom. You can use this to test the settings before running the backup job. Testing the settings prior to running the job can help prevent job failures due to incorrect or insufficient credentials. When finished with these settings, click Next to proceed.



8. Next up is the Schedule, which is where you can specify when and how often the newly created backup job should run. There are many options to accommodate your business needs. Automatic retry allows for setting the number of times to retry a failed attempt to back up a VM and how long Veeam should wait in between retry attempts. Backup window is optional and enables termination of a job if it runs outside of a specified window. Click Next when complete.
9. The final screen on the backup job wizard displays a Summary of all the job settings configured throughout the wizard. If these settings are all acceptable, click Finish to exit the wizard.

## Snapshot Copy-Only Job Orchestration

1. The snapshot orchestration job is the exact same Backup Job wizard used earlier. This section only identifies the differences when creating the backup job to perform snapshot orchestration. Please refer to the section above if more information is needed on specific parts of the backup job creation.
2. Using the Backup Job wizard to perform snapshot orchestration on Element Storage arrays can be done within a single job.
  - a. To accomplish this, create a backup job, add VMs or objects into the job and when you get to the Storage options, it differs slightly. Since the Element Storage is already added into the Veeam storage infrastructure, Veeam automatically creates a repository called Element Snapshot.
  - b. To let Veeam know that this is a snapshot orchestration job, select the Element Storage Snapshot (Primary storage snapshot only) option from the Backup repository drop-down. Set the desired Retention and click Next to continue.



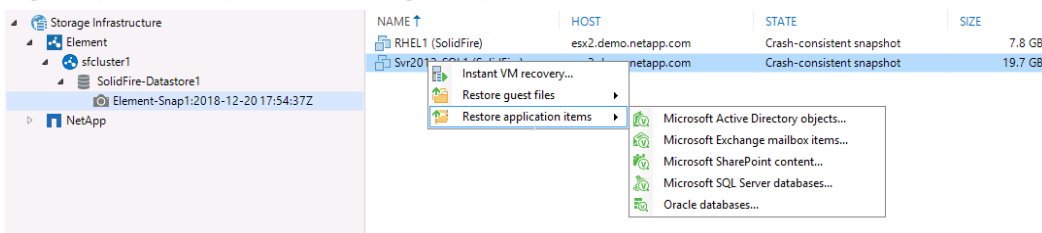
3. Guest Processing is identical to the standard backup job, minus the guest file indexing option. Veeam only offers guest file indexing for backups. Enable application-aware image processing if an application consistent snapshot is desired. If not, Veeam simply orchestrates crash-consistent snapshot copies.
4. Scheduling options are identical to the standard backup job. After the schedule is set, click Finish.

## 7.4 Restoring VM data from Element Snapshots

VM data can be restored directly from Element snapshots if important data is accidentally lost or corrupted. The restore process is like a restore from image-level backups of VMs. Veeam Backup and Replication offers the following restore options for Element Storage snapshots:

- Instant VM Recovery®
- Restoring VM guest OS files (Windows, Linux and others)
- Restoring application items (Exchange, Active Directory, SQL Server, SharePoint and Oracle)

Figure 5) Veeam Explorer for Storage Snapshots.



Before performing restoration, the following requirements must be met:

- Access to the Element Storage system over an iSCSI connection.

- The host is added to the list of servers having access to storage snapshots from which VM data is to be restored. An initiator group must be created on the Element Storage system. The initiator group must contain an iSCSI Qualified Name (IQN) of the ESXi host to which the storage snapshot is mounted.

## 8 Veeam Backup and Replication 9.5 Components

### 8.1 Veeam Backup and Replication 9.5 Components

Table 2 describes each component in Veeam Backup and Replication 9.5.

Table 2) Veeam Backup and Replication 9.5 components.

Component	Description
Veeam backup server	The Veeam backup server is a Windows-based physical machine or VM on which Veeam Backup and Replication is installed. It is the core component in the backup infrastructure that fills the role of the configuration and control center. The Veeam backup server performs all administrative activities: Coordinates backup, replication, recovery verification, and restore tasks Controls job scheduling and resource allocation Is used to set up and manage backup infrastructure components and to specify global settings for the backup infrastructure In addition to its primary functions, a newly deployed Veeam backup server also performs the roles of the default backup proxy and the backup repository. (It manages data handling and data storing tasks.)
Veeam Backup Service	This Windows service coordinates all the operations that are performed by Veeam Backup and Replication, such as backup, replication, recovery verification, and restore tasks. Veeam Backup Service runs under the local system account or the account that has the local administrator permissions on the Veeam backup server.
Veeam Backup Shell	Veeam Backup Shell provides the application UI and enables user access to the application's functionality.
Veeam Backup Catalog/Guest Catalog Service	This Windows service manages guest OS file system indexing for VMs and replicates system index data files to enable search through guest OS files. Index data is stored in the Veeam Backup Catalog, a folder on the Veeam backup server. The Veeam Backup Catalog/Guest Catalog Service running on the Veeam backup server works with search components that are installed on Veeam Backup Enterprise Manager and (optionally) a dedicated Microsoft Search Server.
Veeam Backup SQL Server database	This database is used by Veeam Backup Service, Veeam Backup Shell, and Veeam Backup Catalog Service to store data about the backup infrastructure, jobs, sessions, and so on. The database instance can be on a SQL Server installed either locally (on the same machine where the Veeam backup server runs) or remotely.
Veeam Backup PowerShell snap-in	This snap-in is an extension for Windows PowerShell 2.0. Veeam Backup PowerShell adds a set of cmdlets to enable you to perform backup, replication, and recovery tasks through the PowerShell CLI or run custom scripts. In this way, you can fully automate Veeam Backup and Replication operation.
Backup proxy services	In addition to dedicated services, the Veeam backup server runs a set of data-mover services.

Component	Description
Backup proxy	A backup proxy is an architecture component that sits between the data source and the target and is used to process jobs and deliver backup traffic. The backup proxy retrieves VM data from the production storage. It also compresses the retrieved data and sends it to the backup repository (for example, if you run a backup job) or to another backup proxy (for example, if you run a replication job). As the data handling task is assigned to the backup proxy, the Veeam backup server becomes the point of control for dispatching jobs to proxy servers.
Backup repository	A backup repository is a location that Veeam Backup and Replication jobs use to store backup files, copies of VMs, and metadata for replicated VMs. Technically, a backup repository is a folder on the backup storage. By assigning different repositories to jobs and by limiting the number of parallel jobs for each one, you can balance the load across your backup infrastructure.

## 9 NetApp HCI Volume Configuration Guidelines

### 9.1 NetApp HCI Quality of Service

NetApp HCI QoS guarantees an unprecedented level of control over performance through Min IOPS, Max IOPS, and Burst IOPS. QoS delivers specific IOPS and bandwidth.

- **Minimum IOPS.** The minimum number of IOPS that an administrator grants to a volume. When an application requests an IOPS value of at least the Min IOPS, the NetApp HCI cluster designates resources to fill the request. The minimum IOPS level is the guaranteed IOPS and is the focus of most SLA provisions. This control is imperative to enable performance-sensitive applications to run in multitenant cloud environments.
- **Maximum IOPS.** The maximum number of sustained IOPS that a volume is allowed to process over an extended period. With this control, noisy neighbors (applications that steal performance from other applications) are eliminated.
- **Burst IOPS.** The maximum number of IOPS that is allowed in a short-burst scenario. If a volume has been running below the Max IOPS, burst credits are accumulated. When performance levels become high and are pushed to maximum levels, short bursts of IOPS are allowed on the volume. This functionality is useful during VM reboots, database flushes, and large file transfers.

### 9.2 NetApp HCI Storage Configuration Guidelines for Backup and Replication 9.5 Backup Repositories

NetApp HCI volumes make excellent Veeam backup repositories because of their inherent speed and control.

For optimal performance, NetApp recommends that you follow these QoS guidelines:

- Run multiple backup jobs to each repository.
- Use multiple volumes per repository for maximum performance.

For NetApp HCI volume QoS information for backup repositories, see Table 3.

**Table 3) Veeam Backup and Replication 9.5 components.**

Parameter	Suggested Tune
Volume QoS	Low Min IOPS that is sufficient to cover throughput requirements during peak load times, and high Max IOPS and Burst IOPS. Tuning the volume in this manner permits

Parameter	Suggested Tune
	large volumes that do not consume many of the usable IOPS of your NetApp HCI system but permits the volume to burst its usage as backups are executed. Example: (Min:Max:Burst—4,000:25,000:25,000)
Multipath I/O (MPIO)	You should connect NetApp HCI volumes used as backup repositories to the backup server through MPIO by following the instructions in the <a href="#">NetApp HCI Storage for Microsoft Windows Configuration Guide</a> . This configuration permits maximum throughput to the volume.

### 9.3 NetApp HCI Volumes as VMware Datastores

NetApp HCI volumes applied as VMware (or other hypervisor) datastores function exactly as any other datastore volumes backed up by Veeam. However, some tuning can be performed on both the NetApp HCI volume and the systems used for Veeam.

For NetApp HCI volume QoS for VMware datastores, see Table 4.

Table 4) NetApp HCI volume QoS for VMware datastores.

Parameter	Suggested Tune
Volume QoS	<p><b>Full backups.</b> Increase the Max IOPS and Burst IOPS to 100,000 during the backup. You should return Max IOPS and Burst IOPS to their normal levels after the backup completes.</p> <p><b>Incremental backups.</b> Increase the Max IOPS and Burst IOPS by a multiple of four (for example: 1,000:5,000:5,000 becomes 1,000:20,000:20,000). You should return Max IOPS and Burst IOPS to their normal levels after the backup completes.</p> <p>These changes can be performed automatically by scripts at the beginning and end of the backup job.</p>

## 10 NetApp HCI Host Configuration Guidelines

### 10.1 Host Connectivity

#### iSCSI

All hosts connect to a NetApp HCI cluster through the storage virtual cluster IP address. After the connection is established, a redirector service passes the connection to the node that contains the primary metadata copy for the volume the host is requesting access to. During the node removal process, great care is taken to prevent a host from losing connection to its volume. If there is an active connection from the host to a node that is being removed, the secondary copy is promoted to primary and a new secondary copy is created. A seamless iSCSI redirect then occurs, and the application remains connected to its volume.

A similar process occurs when you add a node to a cluster. The newly added node takes on its share of volumes to help evenly distribute load and capacity on the system. As volumes are rebalanced to provide optimal placement, a seamless iSCSI redirect occurs if the active connection is moved to one of the new nodes added to the system.

## 11 Element Plug-in for vCenter Server

The NetApp Element Plug-in for vCenter Server is a web-based tool integrated with the VMware vSphere® Web Client. The Plug-in is an extension for VMware vSphere users who have deployed



NetApp HCI or Element storage. The plug-in provides a scalable interface to manage and monitor NetApp HCI or Element storage clusters.

By managing NetApp HCI within vCenter Server, you can:

- Discover and manage multiple NetApp HCI clusters.
- Perform vSphere datastore create, extend, clone, share, and delete operations.
- Perform NetApp HCI account create, edit, and delete operations.
- Perform NetApp HCI volume create, edit, clone, delete, and access group add and remove operations.
- Perform NetApp HCI access group create, edit, and delete operations.

For the latest download and details, see the [NetApp support site](#).

## 12 Active IQ

NetApp Active IQ is a web-based tool that provides continually updated historical views of cluster-wide statistics. Data for volumes, nodes, drives, and entire clusters is stored for five years and is updated at regular intervals depending on the data being monitored. You can set up notifications about specified events, thresholds, or metrics on a cluster so that you can address them when they arise. The Active IQ tool makes monitoring capacity, performance, and cluster health easy and accessible from anywhere.

## 13 Summary

The combination of Veeam Backup and Replication and NetApp HCI brings simplicity to operating and protecting highly virtualized, multitenant environments, while delivering powerful and cutting-edge capabilities. NetApp HCI arrays offer the performance that you need when recovering your applications and give you confidence that the data that you backed up is protected and is available when you need it.

## Where to Find Additional Information

### NetApp HCI Documentation

- NetApp HCI Element support  
<https://www.netapp.com/us/documentation/hci.aspx>
- NetApp Support Portal  
<https://mysupport.netapp.com>

### Veeam Backup and Replication 9.5 Update 4 Software Documentation

- Veeam documentation, guides, and datasheets  
<http://www.veeam.com/documentation-guides-datasheets.html>

## Version History

Version	Date	Document Version History
1.0	July 2019	First 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**

Copyright © 2019 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

### **Trademark Information**

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.