



## **NetApp Solutions**

NetApp Solutions

NetApp  
June 07, 2022

# Table of Contents

NetApp Solutions .....	1
NetApp Artificial Intelligence Solutions .....	2
AI Converged Infrastructures .....	2
Data Pipelines, Data Lakes and Management .....	2
Use Cases .....	84
NetApp Container Solutions .....	267
TR-4919: DevOps with NetApp Astra .....	267
NVA-1160: Red Hat OpenShift with NetApp .....	294
NVA-1165: Anthos with NetApp .....	457
Archived Solutions .....	498
Data Migration and Data Protection .....	508
Data Migration .....	508
Data Protection .....	592
Security .....	593
Enterprise Applications .....	594
NetApp Enterprise Database Solutions .....	595
Oracle Database .....	595
Microsoft SQL Server .....	639
Hybrid Cloud Database Solutions with SnapCenter .....	652
NetApp Modern Data Analytics Solutions .....	773
Big Data Analytics Data to Artificial Intelligence .....	773
Best practices for Confluent Kafka .....	817
NetApp hybrid cloud data solutions - Spark and Hadoop based on customer use cases .....	846
NetApp Hybrid Multi-Cloud Solutions .....	865
VMware for Public Cloud .....	865
VMware Hybrid Cloud Use Cases .....	997
NetApp Hybrid Multi-Cloud Solutions for AWS / VMC .....	1000
NetApp Hybrid Multi-Cloud Solutions for Azure / AVS .....	1002
NetApp Hybrid Multi-Cloud Solutions for GCP / GCVE .....	1002
NetApp Solutions for Virtualization .....	1067
Get Started With NetApp & VMware .....	1067
VMware Virtualization for ONTAP .....	1068
NetApp Hybrid Multi-Cloud Solutions .....	1138
VMware Hybrid Cloud Use Cases .....	1138
Virtual Desktops .....	1139
Demos and Tutorials .....	1178
Blogs .....	1181
Solution Automation .....	1182
NetApp Solution Automation .....	1182
Setup the Ansible control node (For CLI based deployments) .....	1182
NetApp Solution Automation .....	1182
Cloud Volumes Automation via Terraform .....	1185
NetApp Solutions Change Log .....	1187

About this Repository . . . . .	1195
Navigation of the Repository . . . . .	1195
Change Log . . . . .	1195
Feedback . . . . .	1196
Legal notices . . . . .	1197
Copyright . . . . .	1197
Trademarks . . . . .	1197
Patents . . . . .	1197
Privacy policy . . . . .	1197
Open source . . . . .	1197

# **NetApp Solutions**

# NetApp Artificial Intelligence Solutions

## AI Converged Infrastructures

### NetApp ONTAP AI with NVIDIA

Overview of ONTAP AI converged infrastructure solutions from NetApp and NVIDIA.

#### NetApp ONTAP AI with NVIDIA DGX A100 Systems

- [Design Guide](#)
- [Deployment Guide](#)

#### NetApp ONTAP AI with NVIDIA DGX A100 Systems and Mellanox Spectrum Ethernet Switches

- [Design Guide](#)
- [Deployment Guide](#)

### NetApp EF-Series AI with NVIDIA

Overview of EF-Series AI converged infrastructure solutions from NetApp and NVIDIA.

#### EF-Series AI with NVIDIA DGX A100 Systems and BeeGFS

- [Design Guide](#)
- [Deployment Guide](#)
- [BeeGFS Deployment Guide](#)

## Data Pipelines, Data Lakes and Management

### NetApp AI Control Plane

#### TR-4798: NetApp AI Control Plane

Mike Oglesby, NetApp

Companies and organizations of all sizes and across many industries are turning to artificial intelligence (AI), machine learning (ML), and deep learning (DL) to solve real-world problems, deliver innovative products and services, and to get an edge in an increasingly competitive marketplace. As organizations increase their use of AI, ML, and DL, they face many challenges, including workload scalability and data availability. This document demonstrates how you can address these challenges by using the NetApp AI Control Plane, a solution that pairs NetApp data management capabilities with popular open-source tools and frameworks.

This report shows you how to rapidly clone a data namespace. It also shows you how to seamlessly replicate data across sites and regions to create a cohesive and unified AI/ML/DL data pipeline. Additionally, it walks you through the defining and implementing of AI, ML, and DL training workflows that incorporate the near-instant creation of data and model baselines for traceability and versioning. With this solution, you can trace every model training run back to the exact dataset that was used to train and/or validate the model. Lastly, this document shows you how to swiftly provision Jupyter Notebook workspaces with access to massive datasets.

Note: For HPC style distributed training at scale involving a large number of GPU servers that require shared access to the same dataset, or if you require/prefer a parallel file system, check out [TR-4890](#). This technical report describes how to include [NetApp's fully supported parallel file system solution BeeGFS](#) as part of the NetApp AI Control Plane. This solution is designed to scale from a handful of NVIDIA DGX A100 systems, up to a full blown 140 node SuperPOD.

The NetApp AI Control Plane is targeted towards data scientists and data engineers, and, thus, minimal NetApp or NetApp ONTAP® expertise is required. With this solution, data management functions can be executed using simple and familiar tools and interfaces. If you already have NetApp storage in your environment, you can test drive the NetApp AI Control plane today. If you want to test drive the solution but you do not have already have NetApp storage, visit [cloud.netapp.com](#), and you can be up and running with a cloud-based NetApp storage solution in minutes. The following figure provides a visualization of the solution.



[Next: Concepts and Components.](#)

## Concepts and Components

### Artificial Intelligence

AI is a computer science discipline in which computers are trained to mimic the cognitive functions of the human mind. AI developers train computers to learn and to solve problems in a manner that is similar to, or even superior to, humans. Deep learning and machine learning are subfields of AI. Organizations are increasingly adopting AI, ML, and DL to support their critical business needs. Some examples are as follows:

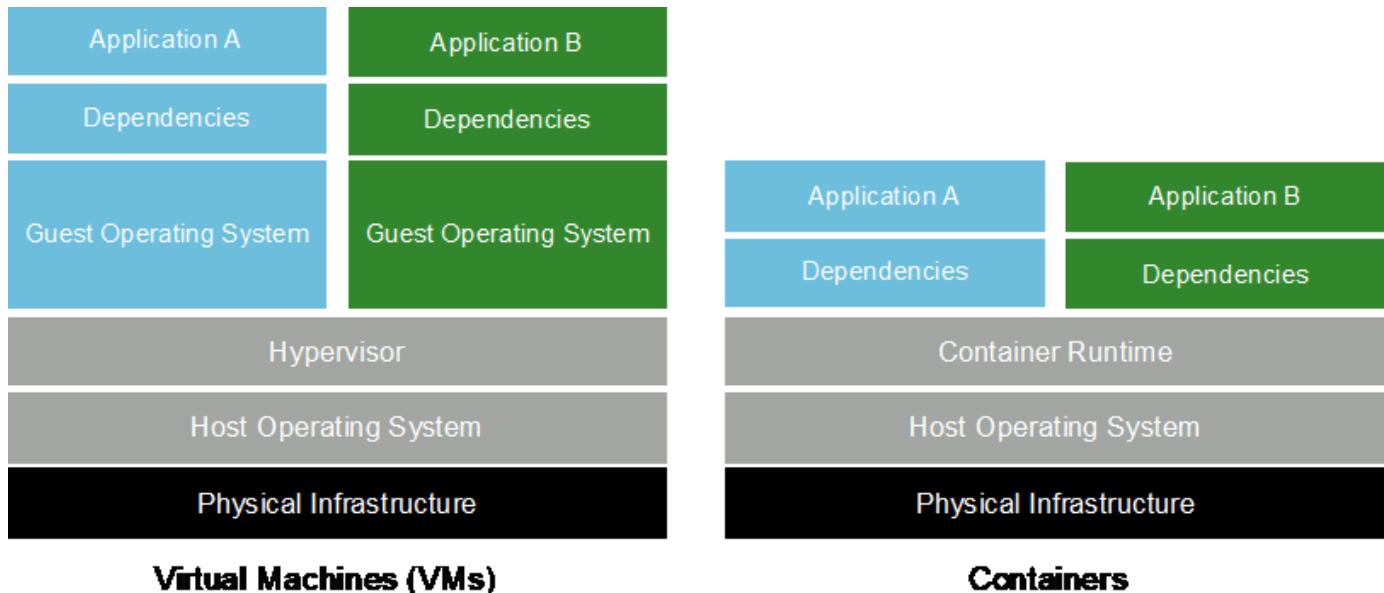
- Analyzing large amounts of data to unearth previously unknown business insights
- Interacting directly with customers by using natural language processing
- Automating various business processes and functions

Modern AI training and inference workloads require massively parallel computing capabilities. Therefore, GPUs are increasingly being used to execute AI operations because the parallel processing capabilities of GPUs are vastly superior to those of general-purpose CPUs.

### Containers

Containers are isolated user-space instances that run on top of a shared host operating system kernel. The adoption of containers is increasing rapidly. Containers offer many of the same application sandboxing benefits that virtual machines (VMs) offer. However, because the hypervisor and guest operating system layers that VMs rely on have been eliminated, containers are far more lightweight. The following figure depicts a visualization of virtual machines versus containers.

Containers also allow the efficient packaging of application dependencies, run times, and so on, directly with an application. The most commonly used container packaging format is the Docker container. An application that has been containerized in the Docker container format can be executed on any machine that can run Docker containers. This is true even if the application's dependencies are not present on the machine because all dependencies are packaged in the container itself. For more information, visit the [Docker website](#).



### Kubernetes

Kubernetes is an open source, distributed, container orchestration platform that was originally designed by Google and is now maintained by the Cloud Native Computing Foundation (CNCF). Kubernetes enables the

automation of deployment, management, and scaling functions for containerized applications. In recent years, Kubernetes has emerged as the dominant container orchestration platform. Although other container packaging formats and run times are supported, Kubernetes is most often used as an orchestration system for Docker containers. For more information, visit the [Kubernetes website](#).

### **NetApp Trident**

Trident is an open source storage orchestrator developed and maintained by NetApp that greatly simplifies the creation, management, and consumption of persistent storage for Kubernetes workloads. Trident, itself a Kubernetes-native application, runs directly within a Kubernetes cluster. With Trident, Kubernetes users (developers, data scientists, Kubernetes administrators, and so on) can create, manage, and interact with persistent storage volumes in the standard Kubernetes format that they are already familiar with. At the same time, they can take advantage of NetApp advanced data management capabilities and a data fabric that is powered by NetApp technology. Trident abstracts away the complexities of persistent storage and makes it simple to consume. For more information, visit the [Trident website](#).

### **NVIDIA DeepOps**

DeepOps is an open source project from NVIDIA that, by using Ansible, automates the deployment of GPU server clusters according to best practices. DeepOps is modular and can be used for various deployment tasks. For this document and the validation exercise that it describes, DeepOps is used to deploy a Kubernetes cluster that consists of GPU server worker nodes. For more information, visit the [DeepOps website](#).

### **Kubeflow**

Kubeflow is an open source AI and ML toolkit for Kubernetes that was originally developed by Google. The Kubeflow project makes deployments of AI and ML workflows on Kubernetes simple, portable, and scalable. Kubeflow abstracts away the intricacies of Kubernetes, allowing data scientists to focus on what they know best—data science. See the following figure for a visualization. Kubeflow has been gaining significant traction as enterprise IT departments have increasingly standardized on Kubernetes. For more information, visit the [Kubeflow website](#).



## Kubeflow Pipelines

Kubeflow Pipelines are a key component of Kubeflow. Kubeflow Pipelines are a platform and standard for defining and deploying portable and scalable AI and ML workflows. For more information, see the [official Kubeflow documentation](#).

## Jupyter Notebook Server

A Jupyter Notebook Server is an open source web application that allows data scientists to create wiki-like documents called Jupyter Notebooks that contain live code as well as descriptive text. Jupyter Notebooks are widely used in the AI and ML community as a means of documenting, storing, and sharing AI and ML projects. Kubeflow simplifies the provisioning and deployment of Jupyter Notebook Servers on Kubernetes. For more information on Jupyter Notebooks, visit the [Jupyter website](#). For more information about Jupyter Notebooks within the context of Kubeflow, see the [official Kubeflow documentation](#).

## Apache Airflow

Apache Airflow is an open-source workflow management platform that enables programmatic authoring, scheduling, and monitoring for complex enterprise workflows. It is often used to automate ETL and data pipeline workflows, but it is not limited to these types of workflows. The Airflow project was started by Airbnb but has since become very popular in the industry and now falls under the auspices of The Apache Software Foundation. Airflow is written in Python, Airflow workflows are created via Python scripts, and Airflow is

designed under the principle of "configuration as code." Many enterprise Airflow users now run Airflow on top of Kubernetes.

## Directed Acyclic Graphs (DAGs)

In Airflow, workflows are called Directed Acyclic Graphs (DAGs). DAGs are made up of tasks that are executed in sequence, in parallel, or a combination of the two, depending on the DAG definition. The Airflow scheduler executes individual tasks on an array of workers, adhering to the task-level dependencies that are specified in the DAG definition. DAGs are defined and created via Python scripts.

## NetApp ONTAP 9

NetApp ONTAP 9 is the latest generation of storage management software from NetApp that enables businesses like yours to modernize infrastructure and to transition to a cloud-ready data center. With industry-leading data management capabilities, ONTAP enables you to manage and protect your data with a single set of tools regardless of where that data resides. You can also move data freely to wherever you need it: the edge, the core, or the cloud. ONTAP 9 includes numerous features that simplify data management, accelerate and protect your critical data, and future-proof your infrastructure across hybrid cloud architectures.

## Simplify Data Management

Data management is crucial for your enterprise IT operations so that you can use appropriate resources for your applications and datasets. ONTAP includes the following features to streamline and simplify your operations and reduce your total cost of operation:

- **Inline data compaction and expanded deduplication.** Data compaction reduces wasted space inside storage blocks, and deduplication significantly increases effective capacity.
- **Minimum, maximum, and adaptive quality of service (QoS).** Granular QoS controls help maintain performance levels for critical applications in highly shared environments.
- **ONTAP FabricPool.** This feature provides automatic tiering of cold data to public and private cloud storage options, including Amazon Web Services (AWS), Azure, and NetApp StorageGRID object-based storage.

## Accelerate and Protect Data

ONTAP delivers superior levels of performance and data protection and extends these capabilities with the following features:

- **High performance and low latency.** ONTAP offers the highest possible throughput at the lowest possible latency.
- **NetApp ONTAP FlexGroup technology.** A FlexGroup volume is a high-performance data container that can scale linearly to up to 20PB and 400 billion files, providing a single namespace that simplifies data management.
- **Data protection.** ONTAP provides built-in data protection capabilities with common management across all platforms.
- **NetApp Volume Encryption.** ONTAP offers native volume-level encryption with both onboard and external key management support.

## Future-Proof Infrastructure

ONTAP 9 helps meet your demanding and constantly changing business needs:

- **Seamless scaling and nondisruptive operations.** ONTAP supports the nondisruptive addition of

capacity to existing controllers and to scale-out clusters. You can upgrade to the latest technologies, such as NVMe and 32Gb FC, without costly data migrations or outages.

- **Cloud connection.** ONTAP is one of the most cloud-connected storage management software, with options for software-defined storage (ONTAP Select) and cloud-native instances (NetApp Cloud Volumes Service) in all public clouds.
- **Integration with emerging applications.** By using the same infrastructure that supports existing enterprise apps, ONTAP offers enterprise-grade data services for next-generation platforms and applications such as OpenStack, Hadoop, and MongoDB.

### NetApp Snapshot Copies

A NetApp Snapshot copy is a read-only, point-in-time image of a volume. The image consumes minimal storage space and incurs negligible performance overhead because it only records changes to files created since the last Snapshot copy was made, as depicted in the following figure.

Snapshot copies owe their efficiency to the core ONTAP storage virtualization technology, the Write Anywhere File Layout (WAFL). Like a database, WAFL uses metadata to point to actual data blocks on disk. But, unlike a database, WAFL does not overwrite existing blocks. It writes updated data to a new block and changes the metadata. It's because ONTAP references metadata when it creates a Snapshot copy, rather than copying data blocks, that Snapshot copies are so efficient. Doing so eliminates the seek time that other systems incur in locating the blocks to copy, as well as the cost of making the copy itself.

You can use a Snapshot copy to recover individual files or LUNs or to restore the entire contents of a volume. ONTAP compares pointer information in the Snapshot copy with data on disk to reconstruct the missing or damaged object, without downtime or a significant performance cost.



*A Snapshot copy records only changes to the active file system since the last Snapshot copy.*

#### NetApp FlexClone Technology

NetApp FlexClone technology references Snapshot metadata to create writable, point-in-time copies of a volume. Copies share data blocks with their parents, consuming no storage except what is required for metadata until changes are written to the copy, as depicted in the following figure. Where traditional copies can take minutes or even hours to create, FlexClone software lets you copy even the largest datasets almost instantaneously. That makes it ideal for situations in which you need multiple copies of identical datasets (a development workspace, for example) or temporary copies of a dataset (testing an application against a production dataset).



*FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.*

#### NetApp SnapMirror Data Replication Technology

NetApp SnapMirror software is a cost-effective, easy-to-use unified replication solution across the data fabric. It replicates data at high speeds over LAN or WAN. It gives you high data availability and fast data replication for applications of all types, including business critical applications in both virtual and traditional environments. When you replicate data to one or more NetApp storage systems and continually update the secondary data, your data is kept current and is available whenever you need it. No external replication servers are required. See the following figure for an example of an architecture that leverages SnapMirror technology.

SnapMirror software leverages NetApp ONTAP storage efficiencies by sending only changed blocks over the network. SnapMirror software also uses built-in network compression to accelerate data transfers and reduce network bandwidth utilization by up to 70%. With SnapMirror technology, you can leverage one thin replication data stream to create a single repository that maintains both the active mirror and prior point-in-time copies, reducing network traffic by up to 50%.



### NetApp Cloud Sync

Cloud Sync is a NetApp service for rapid and secure data synchronization. Whether you need to transfer files between on-premises NFS or SMB file shares, NetApp StorageGRID, NetApp ONTAP S3, NetApp Cloud Volumes Service, Azure NetApp Files, AWS S3, AWS EFS, Azure Blob, Google Cloud Storage, or IBM Cloud Object Storage, Cloud Sync moves the files where you need them quickly and securely.

After your data is transferred, it is fully available for use on both source and target. Cloud Sync can sync data on-demand when an update is triggered or continuously sync data based on a predefined schedule. Regardless, Cloud Sync only moves the deltas, so time and money spent on data replication is minimized.

Cloud Sync is a software as a service (SaaS) tool that is extremely simple to set up and use. Data transfers that are triggered by Cloud Sync are carried out by data brokers. Cloud Sync data brokers can be deployed in AWS, Azure, Google Cloud Platform, or on-premises.

### NetApp XCP

NetApp XCP is client-based software for any-to-NetApp and NetApp-to-NetApp data migrations and file system insights. XCP is designed to scale and achieve maximum performance by utilizing all available system resources to handle high-volume datasets and high-performance migrations. XCP helps you to gain complete visibility into the file system with the option to generate reports.

NetApp XCP is available in a single package that supports NFS and SMB protocols. XCP includes a Linux binary for NFS data sets and a windows executable for SMB data sets.

NetApp XCP File Analytics is host-based software that detects file shares, runs scans on the file system, and provides a dashboard for file analytics. XCP File Analytics is compatible with both NetApp and non-NetApp systems and runs on Linux or Windows hosts to provide analytics for NFS and SMB-exported file systems.

### NetApp ONTAP FlexGroup Volumes

A training dataset can be a collection of potentially billions of files. Files can include text, audio, video, and other forms of unstructured data that must be stored and processed to be read in parallel. The storage system must store large numbers of small files and must read those files in parallel for sequential and random I/O.

A FlexGroup volume is a single namespace that comprises multiple constituent member volumes, as shown in the following figure. From a storage administrator viewpoint, a FlexGroup volume is managed and acts like a NetApp FlexVol volume. Files in a FlexGroup volume are allocated to individual member volumes and are not striped across volumes or nodes. They enable the following capabilities:

- FlexGroup volumes provide multiple petabytes of capacity and predictable low latency for high-metadata workloads.
- They support up to 400 billion files in the same namespace.
- They support parallelized operations in NAS workloads across CPUs, nodes, aggregates, and constituent FlexVol volumes.



Next: [Hardware and Software Requirements](#).

### Hardware and Software Requirements

The NetApp AI Control Plane solution is not dependent on this specific hardware. The solution is compatible with any NetApp physical storage appliance, software-defined instance, or cloud service, that is supported by Trident. Examples include a NetApp AFF storage system, Azure NetApp Files, NetApp Cloud Volumes Service, a NetApp ONTAP Select software-defined storage instance, or a NetApp Cloud Volumes ONTAP instance. Additionally, the solution can be implemented on any Kubernetes cluster as long as the Kubernetes version used is supported by Kubeflow and NetApp Trident. For a list of Kubernetes versions that are supported by Kubeflow, see the [official Kubeflow documentation](#). For a list of Kubernetes versions that are supported by Trident, see the [Trident documentation](#). See the following tables for details on the environment that was used to validate the solution.

Infrastructure Component	Quantity	Details	Operating System
Deployment jump host	1	VM	Ubuntu 20.04.2 LTS

Infrastructure Component	Quantity	Details	Operating System
Kubernetes master nodes	1	VM	Ubuntu 20.04.2 LTS
Kubernetes worker nodes	2	VM	Ubuntu 20.04.2 LTS
Kubernetes GPU worker nodes	2	NVIDIA DGX-1 (bare-metal)	NVIDIA DGX OS 4.0.5 (based on Ubuntu 18.04.2 LTS)
Storage	1 HA Pair	NetApp AFF A220	NetApp ONTAP 9.7 P6

Software Component	Version
Apache Airflow	2.0.1
Apache Airflow Helm Chart	8.0.8
Docker	19.03.12
Kubeflow	1.2
Kubernetes	1.18.9
NetApp Trident	21.01.2
NVIDIA DeepOps	Trident deployment functionality from master branch as of commit <a href="#">61898cdfda</a> ; All other functionality from version 21.03

## Support

NetApp does not offer enterprise support for Apache Airflow, Docker, Kubeflow, Kubernetes, or NVIDIA DeepOps. If you are interested in a fully supported solution with capabilities similar to the NetApp AI Control Plane solution, [contact NetApp](#) about fully supported AI/ML solutions that NetApp offers jointly with partners.

[Next: Kubernetes Deployment.](#)

## Kubernetes Deployment

This section describes the tasks that you must complete to deploy a Kubernetes cluster in which to implement the NetApp AI Control Plane solution. If you already have a Kubernetes cluster, then you can skip this section as long as you are running a version of Kubernetes that is supported by Kubeflow and NetApp Trident. For a list of Kubernetes versions that are supported by Kubeflow, see the [see the official Kubeflow documentation](#). For a list of Kubernetes versions that are supported by Trident, see the [Trident documentation](#).

For on-premises Kubernetes deployments that incorporate bare-metal nodes featuring NVIDIA GPU(s), NetApp recommends using NVIDIA's DeepOps Kubernetes deployment tool. This section outlines the deployment of a Kubernetes cluster using DeepOps.

## Prerequisites

Before you perform the deployment exercise that is outlined in this section, we assume that you have already

performed the following tasks:

1. You have already configured any bare-metal Kubernetes nodes (for example, an NVIDIA DGX system that is part of an ONTAP AI pod) according to standard configuration instructions.
2. You have installed a supported operating system on all Kubernetes master and worker nodes and on a deployment jump host. For a list of operating systems that are supported by DeepOps, see the [DeepOps GitHub site](#).

## Use NVIDIA DeepOps to Install and Configure Kubernetes

To deploy and configure your Kubernetes cluster with NVIDIA DeepOps, perform the following tasks from a deployment jump host:

1. Download NVIDIA DeepOps by following the instructions on the [Getting Started page](#) on the NVIDIA DeepOps GitHub site.
2. Deploy Kubernetes in your cluster by following the instructions on the [Kubernetes Deployment Guide page](#) on the NVIDIA DeepOps GitHub site.

Next: [NetApp Trident Deployment and Configuration Overview](#).

## NetApp Trident Deployment and Configuration

This section describes the tasks that you must complete to install and configure NetApp Trident in your Kubernetes cluster.

### Prerequisites

Before you perform the deployment exercise that is outlined in this section, we assume that you have already performed the following tasks:

1. You already have a working Kubernetes cluster, and you are running a version of Kubernetes that is supported by Trident. For a list of supported versions, see the [Trident documentation](#).
2. You already have a working NetApp storage appliance, software-defined instance, or cloud storage service, that is supported by Trident.

### Install Trident

To install and configure NetApp Trident in your Kubernetes cluster, perform the following tasks from the deployment jump host:

1. Deploy Trident using one of the following methods:
  - If you used NVIDIA DeepOps to deploy your Kubernetes cluster, you can also use NVIDIA DeepOps to deploy Trident in your Kubernetes cluster. To deploy Trident with DeepOps, follow the [Trident deployment instructions](#) on the NVIDIA DeepOps GitHub site.
  - If you did not use NVIDIA DeepOps to deploy your Kubernetes cluster or if you simply prefer to deploy Trident manually, you can deploy Trident by following the [deployment instructions](#) in the Trident documentation. Be sure to create at least one Trident Backend and at least one Kubernetes StorageClass. For more information about Backends and StorageClasses, see the [Trident documentation](#).



If you are deploying the NetApp AI Control Plane solution on an ONTAP AI pod, see [Example Trident Backends for ONTAP AI Deployments](#) for some examples of different Trident Backends that you might want to create and [Example Kubernetes Storageclasses for ONTAP AI Deployments](#) for some examples of different Kubernetes StorageClasses that you might want to create.

Next: [Example Trident Backends for ONTAP AI Deployments](#).

### NetApp Trident Deployment and Configuration

This section describes the tasks that you must complete to install and configure NetApp Trident in your Kubernetes cluster.

#### Prerequisites

Before you perform the deployment exercise that is outlined in this section, we assume that you have already performed the following tasks:

1. You already have a working Kubernetes cluster, and you are running a version of Kubernetes that is supported by Trident. For a list of supported versions, see the [Trident documentation](#).
2. You already have a working NetApp storage appliance, software-defined instance, or cloud storage service, that is supported by Trident.

#### Install Trident

To install and configure NetApp Trident in your Kubernetes cluster, perform the following tasks from the deployment jump host:

1. Deploy Trident using one of the following methods:
  - If you used NVIDIA DeepOps to deploy your Kubernetes cluster, you can also use NVIDIA DeepOps to deploy Trident in your Kubernetes cluster. To deploy Trident with DeepOps, follow the [Trident deployment instructions](#) on the NVIDIA DeepOps GitHub site.
  - If you did not use NVIDIA DeepOps to deploy your Kubernetes cluster or if you simply prefer to deploy Trident manually, you can deploy Trident by following the [deployment instructions](#) in the Trident documentation. Be sure to create at least one Trident Backend and at least one Kubernetes StorageClass. For more information about Backends and StorageClasses, see the [Trident documentation](#).



If you are deploying the NetApp AI Control Plane solution on an ONTAP AI pod, see [Example Trident Backends for ONTAP AI Deployments](#) for some examples of different Trident Backends that you might want to create and [Example Kubernetes Storageclasses for ONTAP AI Deployments](#) for some examples of different Kubernetes StorageClasses that you might want to create.

Next: [Example Trident Backends for ONTAP AI Deployments](#).

### Example Trident Backends for ONTAP AI Deployments

Before you can use Trident to dynamically provision storage resources within your Kubernetes cluster, you must create one or more Trident Backends. The examples that follow represent different types of Backends that you might want to create if you are

deploying the NetApp AI Control Plane solution on an ONTAP AI pod. For more information about Backends, see the [Trident documentation](#).

1. NetApp recommends creating a FlexGroup-enabled Trident Backend for each data LIF (logical network interface that provides data access) that you want to use on your NetApp AFF system. This will allow you to balance volume mounts across LIFs

The example commands that follow show the creation of two FlexGroup-enabled Trident Backends for two different data LIFs that are associated with the same ONTAP storage virtual machine (SVM). These Backends use the `ontap-nas-flexgroup` storage driver. ONTAP supports two main data volume types: FlexVol and FlexGroup. FlexVol volumes are size-limited (as of this writing, the maximum size depends on the specific deployment). FlexGroup volumes, on the other hand, can scale linearly to up to 20PB and 400 billion files, providing a single namespace that greatly simplifies data management. Therefore, FlexGroup volumes are optimal for AI and ML workloads that rely on large amounts of data.

If you are working with a small amount of data and want to use FlexVol volumes instead of FlexGroup volumes, you can create Trident Backends that use the `ontap-nas` storage driver instead of the `ontap-nas-flexgroup` storage driver.

```
$ cat << EOF > ./trident-backend-ontap-ai-flexgroups-iface1.json
{
    "version": 1,
    "storageDriverName": "ontap-nas-flexgroup",
    "backendName": "ontap-ai-flexgroups-iface1",
    "managementLIF": "10.61.218.100",
    "dataLIF": "192.168.11.11",
    "svm": "ontapai_nfs",
    "username": "admin",
    "password": "ontapai"
}
EOF
$ tridentctl create backend -f ./trident-backend-ontap-ai-flexgroups-
iface1.json -n trident
+-----+
+-----+-----+
|           NAME           |   STORAGE DRIVER   |
UUID          | STATE  | VOLUMES |
+-----+-----+
+-----+-----+
| ontap-ai-flexgroups-iface1 | ontap-nas-flexgroup | b74cbddb-e0b8-40b7-
b263-b6da6dec0bdd | online |      0 |
+-----+
+-----+-----+
$ cat << EOF > ./trident-backend-ontap-ai-flexgroups-iface2.json
{
    "version": 1,
    "storageDriverName": "ontap-nas-flexgroup",
    "backendName": "ontap-ai-flexgroups-iface2",
```

```

    "managementLIF": "10.61.218.100",
    "dataLIF": "192.168.12.12",
    "svm": "ontapai_nfs",
    "username": "admin",
    "password": "ontapai"
}
EOF
$ tridentctl create backend -f ./trident-backend-ontap-ai-flexgroups-
iface2.json -n trident
+-----+-----+
+-----+-----+-----+
|           NAME          |   STORAGE DRIVER   |
UUID          | STATE   | VOLUMES  |
+-----+-----+
+-----+-----+-----+
| ontap-ai-flexgroups-iface2 | ontap-nas-flexgroup | 61814d48-c770-436b-
9cb4-cf7ee661274d | online |      0 |
+-----+-----+
+-----+-----+-----+
$ tridentctl get backend -n trident
+-----+-----+
+-----+-----+-----+
|           NAME          |   STORAGE DRIVER   |
UUID          | STATE   | VOLUMES  |
+-----+-----+
+-----+-----+-----+
| ontap-ai-flexgroups-iface1 | ontap-nas-flexgroup | b74cbddb-e0b8-40b7-
b263-b6da6dec0bdd | online |      0 |
| ontap-ai-flexgroups-iface2 | ontap-nas-flexgroup | 61814d48-c770-436b-
9cb4-cf7ee661274d | online |      0 |
+-----+-----+
+-----+-----+-----+

```

2. NetApp also recommends creating one or more FlexVol- enabled Trident Backends. If you use FlexGroup volumes for training dataset storage, you might want to use FlexVol volumes for storing results, output, debug information, and so on. If you want to use FlexVol volumes, you must create one or more FlexVol- enabled Trident Backends. The example commands that follow show the creation of a single FlexVol- enabled Trident Backend that uses a single data LIF.

```

$ cat << EOF > ./trident-backend-ontap-ai-flexvols.json
{
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "ontap-ai-flexvols",
    "managementLIF": "10.61.218.100",
    "dataLIF": "192.168.11.11",
    "svm": "ontapai_nfs",
    "username": "admin",
    "password": "ontapai"
}
EOF
$ tridentctl create backend -f ./trident-backend-ontap-ai-flexvols.json -n
trident
+-----+
+-----+-----+
|           NAME          |   STORAGE DRIVER   |           UUID
| STATE  | VOLUMES |
+-----+-----+
+-----+-----+
| ontap-ai-flexvols      | ontap-nas          | 52bdb3b1-13a5-4513-
a9c1-52a69657fabe | online | 0 |
+-----+-----+
+-----+-----+
$ tridentctl get backend -n trident
+-----+
+-----+-----+
|           NAME          |   STORAGE DRIVER   |           UUID
| STATE  | VOLUMES |
+-----+-----+
+-----+-----+
| ontap-ai-flexvols      | ontap-nas          | 52bdb3b1-13a5-4513-
a9c1-52a69657fabe | online | 0 |
| ontap-ai-flexgroups-iface1 | ontap-nas-flexgroup | b74cbddb-e0b8-40b7-
b263-b6da6dec0bdd | online | 0 |
| ontap-ai-flexgroups-iface2 | ontap-nas-flexgroup | 61814d48-c770-436b-
9cb4-cf7ee661274d | online | 0 |
+-----+-----+
+-----+-----+

```

[Next: Example Kubernetes Storageclasses for ONTAP AI Deployments.](#)

#### **Example Kubernetes StorageClasses for ONTAP AI Deployments**

Before you can use Trident to dynamically provision storage resources within your

Kubernetes cluster, you must create one or more Kubernetes StorageClasses. The examples that follow represent different types of StorageClasses that you might want to create if you are deploying the NetApp AI Control Plane solution on an ONTAP AI pod. For more information about StorageClasses, see the [Trident documentation](#).

1. NetApp recommends creating a separate StorageClass for each FlexGroup-enabled Trident Backend that you created in the section [Example Trident Backends for ONTAP AI Deployments](#), step 1. These granular StorageClasses enable you to add NFS mounts that correspond to specific LIFs (the LIFs that you specified when you created the Trident Backends) as a particular Backend that is specified in the StorageClass spec file. The example commands that follow show the creation of two StorageClasses that correspond to the two example Backends that were created in the section [Example Trident Backends for ONTAP AI Deployments](#), step 1. For more information about StorageClasses, see the [Trident documentation](#).

So that a persistent volume isn't deleted when the corresponding PersistentVolumeClaim (PVC) is deleted, the following example uses a `reclaimPolicy` value of `Retain`. For more information about the `reclaimPolicy` field, see the official [Kubernetes documentation](#).

```

$ cat << EOF > ./storage-class-ontap-ai-flexgroups-retain-iface1.yaml
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-ai-flexgroups-retain-iface1
  provisioner: netapp.io/trident
parameters:
  backendType: "ontap-nas-flexgroup"
  storagePools: "ontap-ai-flexgroups-iface1:.*"
reclaimPolicy: Retain
EOF
$ kubectl create -f ./storage-class-ontap-ai-flexgroups-retain-
iface1.yaml
storageclass.storage.k8s.io/ontap-ai-flexgroups-retain-iface1 created
$ cat << EOF > ./storage-class-ontap-ai-flexgroups-retain-iface2.yaml
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-ai-flexgroups-retain-iface2
  provisioner: netapp.io/trident
parameters:
  backendType: "ontap-nas-flexgroup"
  storagePools: "ontap-ai-flexgroups-iface2:.*"
reclaimPolicy: Retain
EOF
$ kubectl create -f ./storage-class-ontap-ai-flexgroups-retain-
iface2.yaml
storageclass.storage.k8s.io/ontap-ai-flexgroups-retain-iface2 created
$ kubectl get storageclass
NAME                      PROVISIONER          AGE
ontap-ai-flexgroups-retain-iface1   netapp.io/trident   0m
ontap-ai-flexgroups-retain-iface2   netapp.io/trident   0m

```

2. NetApp also recommends creating a StorageClass that corresponds to the FlexVol-enabled Trident Backend that you created in the section [Example Trident Backends for ONTAP AI Deployments](#), step 2. The example commands that follow show the creation of a single StorageClass for FlexVol volumes.

In the following example, a particular Backend is not specified in the StorageClass definition file because only one FlexVol-enabled Trident backend was created. When you use Kubernetes to administer volumes that use this StorageClass, Trident attempts to use any available backend that uses the `ontap-nas` driver.

```

$ cat << EOF > ./storage-class-ontap-ai-flexvols-retain.yaml
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-ai-flexvols-retain
  provisioner: netapp.io/trident
parameters:
  backendType: "ontap-nas"
  reclaimPolicy: Retain
EOF
$ kubectl create -f ./storage-class-ontap-ai-flexvols-retain.yaml
storageclass.storage.k8s.io/ontap-ai-flexvols-retain created
$ kubectl get storageclass
NAME                      PROVISIONER          AGE
ontap-ai-flexgroups-retain-iface1   netapp.io/trident   1m
ontap-ai-flexgroups-retain-iface2   netapp.io/trident   1m
ontap-ai-flexvols-retain           netapp.io/trident   0m

```

3. NetApp also recommends creating a generic StorageClass for FlexGroup volumes. The following example commands show the creation of a single generic StorageClass for FlexGroup volumes.

Note that a particular backend is not specified in the StorageClass definition file. Therefore, when you use Kubernetes to administer volumes that use this StorageClass, Trident attempts to use any available backend that uses the `ontap-nas-flexgroup` driver.

```

$ cat << EOF > ./storage-class-ontap-ai-flexgroups-retain.yaml
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-ai-flexgroups-retain
  provisioner: netapp.io/trident
parameters:
  backendType: "ontap-nas-flexgroup"
  reclaimPolicy: Retain
EOF
$ kubectl create -f ./storage-class-ontap-ai-flexgroups-retain.yaml
storageclass.storage.k8s.io/ontap-ai-flexgroups-retain created
$ kubectl get storageclass
NAME                      PROVISIONER          AGE
ontap-ai-flexgroups-retain           netapp.io/trident   0m
ontap-ai-flexgroups-retain-iface1   netapp.io/trident   2m
ontap-ai-flexgroups-retain-iface2   netapp.io/trident   2m
ontap-ai-flexvols-retain           netapp.io/trident   1m

```

Next: Kubeflow Deployment Overview.

## Kubeflow Deployment

This section describes the tasks that you must complete to deploy Kubeflow in your Kubernetes cluster.

### Prerequisites

Before you perform the deployment exercise that is outlined in this section, we assume that you have already performed the following tasks:

1. You already have a working Kubernetes cluster, and you are running a version of Kubernetes that is supported by Kubeflow. For a list of supported versions, see the [official Kubeflow documentation](#).
2. You have already installed and configured NetApp Trident in your Kubernetes cluster as outlined in [Trident Deployment and Configuration](#).

### Set Default Kubernetes StorageClass

Before you deploy Kubeflow, you must designate a default StorageClass within your Kubernetes cluster. The Kubeflow deployment process attempts to provision new persistent volumes using the default StorageClass. If no StorageClass is designated as the default StorageClass, then the deployment fails. To designate a default StorageClass within your cluster, perform the following task from the deployment jump host. If you have already designated a default StorageClass within your cluster, then you can skip this step.

1. Designate one of your existing StorageClasses as the default StorageClass. The example commands that follow show the designation of a StorageClass named `ontap-ai-flexvols-retain` as the default StorageClass.

 The `ontap-nas-flexgroup` Trident Backend type has a minimum PVC size that is fairly large. By default, Kubeflow attempts to provision PVCs that are only a few GBs in size. Therefore, you should not designate a StorageClass that utilizes the `ontap-nas-flexgroup` Backend type as the default StorageClass for the purposes of Kubeflow deployment.

```
$ kubectl get sc
NAME                      PROVISIONER          AGE
ontap-ai-flexgroups-retain   csi.trident.netapp.io  25h
ontap-ai-flexgroups-retain-iface1  csi.trident.netapp.io  25h
ontap-ai-flexgroups-retain-iface2  csi.trident.netapp.io  25h
ontap-ai-flexvols-retain      csi.trident.netapp.io  3s

$ kubectl patch storageclass ontap-ai-flexvols-retain -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
storageclass.storage.k8s.io/ontap-ai-flexvols-retain patched

$ kubectl get sc
NAME                      PROVISIONER          AGE
ontap-ai-flexgroups-retain   csi.trident.netapp.io  25h
ontap-ai-flexgroups-retain-iface1  csi.trident.netapp.io  25h
ontap-ai-flexgroups-retain-iface2  csi.trident.netapp.io  25h
ontap-ai-flexvols-retain (default)  csi.trident.netapp.io  54s
```

## Use NVIDIA DeepOps to Deploy Kubeflow

NetApp recommends using the Kubeflow deployment tool that is provided by NVIDIA DeepOps. To deploy Kubeflow in your Kubernetes cluster using the DeepOps deployment tool, perform the following tasks from the deployment jump host.



Alternatively, you can deploy Kubeflow manually by following the [installation instructions](#) in the official Kubeflow documentation

1. Deploy Kubeflow in your cluster by following the [Kubeflow deployment instructions](#) on the NVIDIA DeepOps GitHub site.
2. Note down the Kubeflow Dashboard URL that the DeepOps Kubeflow deployment tool outputs.

```
$ ./scripts/k8s/deploy_kubeflow.sh -x
...
INFO[0007] Applied the configuration Successfully!
filename="cmd/apply.go:72"
Kubeflow app installed to: /home/ai/kubeflow
It may take several minutes for all services to start. Run 'kubectl get
pods -n kubeflow' to verify
To remove (excluding CRDs, istio, auth, and cert-manager), run:
./scripts/k8s_deploy_kubeflow.sh -d
To perform a full uninstall : ./scripts/k8s_deploy_kubeflow.sh -D
Kubeflow Dashboard (HTTP NodePort): http://10.61.188.111:31380
```

3. Confirm that all pods deployed within the Kubeflow namespace show a STATUS of Running and confirm that no components deployed within the namespace are in an error state. It may take several minutes for all pods to start.

```
$ kubectl get all -n kubeflow
NAME                                         READY
STATUS    RESTARTS   AGE
pod/admission-webhook-bootstrap-stateful-set-0   1/1
Running   0          95s
pod/admission-webhook-deployment-6b89c84c98-vrtbh   1/1
Running   0          91s
pod/application-controller-stateful-set-0        1/1
Running   0          98s
pod/argo-ui-5dcf5d8b4f-m2wn4                   1/1
Running   0          97s
pod/centraldashboard-cf4874ddc-7hcr8           1/1
Running   0          97s
pod/jupyter-web-app-deployment-685b455447-gjhh7   1/1
Running   0          96s
pod/katib-controller-88c97d85c-kgq66            1/1
Running   1          95s
```

pod/katib-db-8598468fd8-5jw2c	1/1
Running 0 95s	
pod/katib-manager-574c8c67f9-wtrf5	1/1
Running 1 95s	
pod/katib-manager-rest-778857c989-fjbzn	1/1
Running 0 95s	
pod/katib-suggestion-bayesianoptimization-65df4d7455-qthmw	1/1
Running 0 94s	
pod/katib-suggestion-grid-56bf69f597-98vwn	1/1
Running 0 94s	
pod/katib-suggestion-hyperband-7777b76cb9-9v6dq	1/1
Running 0 93s	
pod/katib-suggestion-nasrl-77f6f9458c-2qzxq	1/1
Running 0 93s	
pod/katib-suggestion-random-77b88b5c79-164j9	1/1
Running 0 93s	
pod/katib-ui-7587c5b967-nd629	1/1
Running 0 95s	
pod/metacontroller-0	1/1
Running 0 96s	
pod/metadata-db-5dd459cc-swzkm	1/1
Running 0 94s	
pod/metadata-deployment-6cf77db994-69fk7	1/1
Running 3 93s	
pod/metadata-deployment-6cf77db994-mpbjt	1/1
Running 3 93s	
pod/metadata-deployment-6cf77db994-xg7tz	1/1
Running 3 94s	
pod/metadata-ui-78f5b59b56-qb6kr	1/1
Running 0 94s	
pod/minio-758b769d67-11vdr	1/1
Running 0 91s	
pod/ml-pipeline-5875b9db95-g8t2k	1/1
Running 0 91s	
pod/ml-pipeline-persistenceagent-9b69ddd46-bt9r9	1/1
Running 0 90s	
pod/ml-pipeline-scheduledworkflow-7b8d756c76-7x56s	1/1
Running 0 90s	
pod/ml-pipeline-ui-79ffd9c76-fcwpd	1/1
Running 0 90s	
pod/ml-pipeline-viewer-controller-deployment-5fdc87f58-b2t9r	1/1
Running 0 90s	
pod/mysql-657f87857d-15k9z	1/1
Running 0 91s	
pod/notebook-controller-deployment-56b4f59bbf-8bvnr	1/1
Running 0 92s	

pod/profiles-deployment-6bc745947-mrdkh			2/2
Running 0	90s		
pod/pytorch-operator-77c97f4879-hmlrv			1/1
Running 0	92s		
pod/seldon-operator-controller-manager-0			1/1
Running 1	91s		
pod/spartakus-volunteer-5fdfddb779-17qkm			1/1
Running 0	92s		
pod/tensorboard-6544748d94-nh8b2			1/1
Running 0	92s		
pod/tf-job-dashboard-56f79c59dd-6w59t			1/1
Running 0	92s		
pod/tf-job-operator-79cbfd6dbc-rb58c			1/1
Running 0	91s		
pod/workflow-controller-db644d554-cwrnb			1/1
Running 0	97s		
NAME			TYPE
CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
service/admission-webhook-service			ClusterIP
10.233.51.169	<none>	443/TCP	97s
service/application-controller-service			ClusterIP
10.233.4.54	<none>	443/TCP	98s
service/argo-ui			NodePort
10.233.47.191	<none>	80:31799/TCP	97s
service/centraldashboard			ClusterIP
10.233.8.36	<none>	80/TCP	97s
service/jupyter-web-app-service			ClusterIP
10.233.1.42	<none>	80/TCP	97s
service/katib-controller			ClusterIP
10.233.25.226	<none>	443/TCP	96s
service/katib-db			ClusterIP
10.233.33.151	<none>	3306/TCP	97s
service/katib-manager			ClusterIP
10.233.46.239	<none>	6789/TCP	96s
service/katib-manager-rest			ClusterIP
10.233.55.32	<none>	80/TCP	96s
service/katib-suggestion-bayesianoptimization			ClusterIP
10.233.49.191	<none>	6789/TCP	95s
service/katib-suggestion-grid			ClusterIP
10.233.9.105	<none>	6789/TCP	95s
service/katib-suggestion-hyperband			ClusterIP
10.233.22.2	<none>	6789/TCP	95s
service/katib-suggestion-nasrl			ClusterIP
10.233.63.73	<none>	6789/TCP	95s
service/katib-suggestion-random			ClusterIP
10.233.57.210	<none>	6789/TCP	95s

NAME	READY	UP-
TO-DATE	AVAILABLE	AGE
deployment.apps/admission-webhook-deployment	1/1	1
1 97s		
deployment.apps/argo-ui	1/1	1
1 97s		
deployment.apps/centraldashboard	1/1	1
1 97s		
deployment.apps/jupyter-web-app-deployment	1/1	1
1 97s		
deployment.apps/katib-controller	1/1	1
1 96s		

deployment.apps/katib-db		1/1	1
1	97s		
deployment.apps/katib-manager		1/1	1
1	96s		
deployment.apps/katib-manager-rest		1/1	1
1	96s		
deployment.apps/katib-suggestion-bayesianoptimization		1/1	1
1	95s		
deployment.apps/katib-suggestion-grid		1/1	1
1	95s		
deployment.apps/katib-suggestion-hyperband		1/1	1
1	95s		
deployment.apps/katib-suggestion-nasrl		1/1	1
1	95s		
deployment.apps/katib-suggestion-random		1/1	1
1	95s		
deployment.apps/katib-ui		1/1	1
1	96s		
deployment.apps/metadata-db		1/1	1
1	96s		
deployment.apps/metadata-deployment		3/3	3
3	96s		
deployment.apps/metadata-ui		1/1	1
1	96s		
deployment.apps/minio		1/1	1
1	94s		
deployment.apps/ml-pipeline		1/1	1
1	94s		
deployment.apps/ml-pipeline-persistenceagent		1/1	1
1	93s		
deployment.apps/ml-pipeline-scheduledworkflow		1/1	1
1	93s		
deployment.apps/ml-pipeline-ui		1/1	1
1	93s		
deployment.apps/ml-pipeline-viewer-controller-deployment		1/1	1
1	93s		
deployment.apps/mysql		1/1	1
1	94s		
deployment.apps/notebook-controller-deployment		1/1	1
1	95s		
deployment.apps/profiles-deployment		1/1	1
1	92s		
deployment.apps/pytorch-operator		1/1	1
1	95s		
deployment.apps/spartakus-volunteer		1/1	1
1	94s		

deployment.apps/tensorboard			1/1	1
1	94s			
deployment.apps/tf-job-dashboard			1/1	1
1	94s			
deployment.apps/tf-job-operator			1/1	1
1	94s			
deployment.apps/workflow-controller			1/1	1
1	97s			
NAME				
DESIRED	CURRENT	READY	AGE	
replicaset.apps/admission-webhook-deployment-6b89c84c98				1
1	1	97s		
replicaset.apps/argo-ui-5dcf5d8b4f				1
1	1	97s		
replicaset.apps/centraldashboard-cf4874ddc				1
1	1	97s		
replicaset.apps/jupyter-web-app-deployment-685b455447				1
1	1	97s		
replicaset.apps/katib-controller-88c97d85c				1
1	1	96s		
replicaset.apps/katib-db-8598468fd8				1
1	1	97s		
replicaset.apps/katib-manager-574c8c67f9				1
1	1	96s		
replicaset.apps/katib-manager-rest-778857c989				1
1	1	96s		
replicaset.apps/katib-suggestion-bayesianoptimization-65df4d7455				1
1	1	95s		
replicaset.apps/katib-suggestion-grid-56bf69f597				1
1	1	95s		
replicaset.apps/katib-suggestion-hyperband-7777b76cb9				1
1	1	95s		
replicaset.apps/katib-suggestion-nasrl-77f6f9458c				1
1	1	95s		
replicaset.apps/katib-suggestion-random-77b88b5c79				1
1	1	95s		
replicaset.apps/katib-ui-7587c5b967				1
1	1	96s		
replicaset.apps/metadata-db-5dd459cc				1
1	1	96s		
replicaset.apps/metadata-deployment-6cf77db994				3
3	3	96s		
replicaset.apps/metadata-ui-78f5b59b56				1
1	1	96s		
replicaset.apps/minio-758b769d67				1
1	1	93s		

```

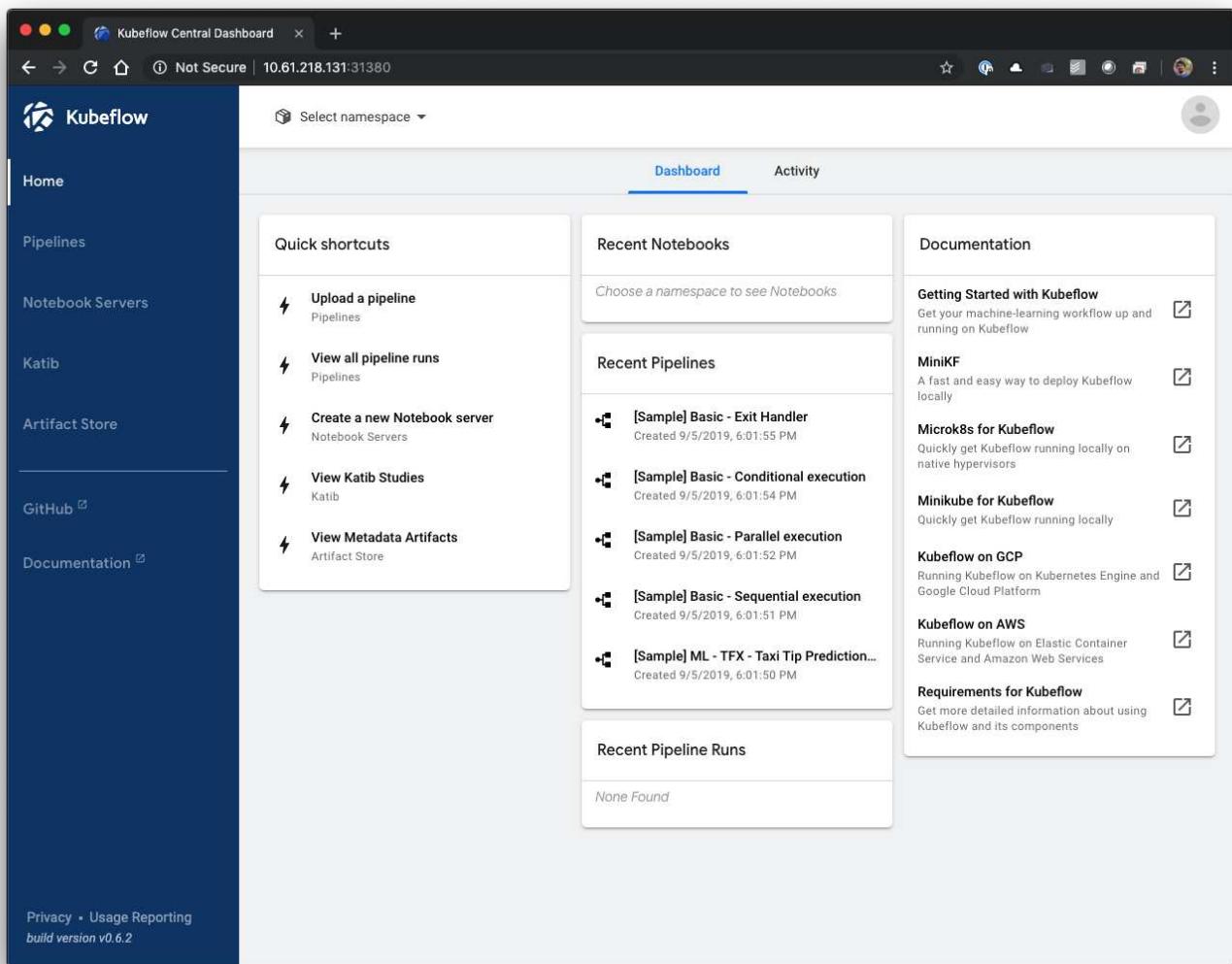
replicaset.apps/ml-pipeline-5875b9db95 1
1 1 93s
replicaset.apps/ml-pipeline-persistenceagent-9b69ddd46 1
1 1 92s
replicaset.apps/ml-pipeline-scheduledworkflow-7b8d756c76 1
1 1 91s
replicaset.apps/ml-pipeline-ui-79ffd9c76 1
1 1 91s
replicaset.apps/ml-pipeline-viewer-controller-deployment-5fdc87f58 1
1 1 91s
replicaset.apps/mysql-657f87857d 1
1 1 92s
replicaset.apps/notebook-controller-deployment-56b4f59bbf 1
1 1 94s
replicaset.apps/profiles-deployment-6bc745947 1
1 1 91s
replicaset.apps/pytorch-operator-77c97f4879 1
1 1 94s
replicaset.apps/spartakus-volunteer-5fdfddb779 1
1 1 94s
replicaset.apps/tensorboard-6544748d94 1
1 1 93s
replicaset.apps/tf-job-dashboard-56f79c59dd 1
1 1 93s
replicaset.apps/tf-job-operator-79cbfd6dbc 1
1 1 93s
replicaset.apps/workflow-controller-db644d554 1
1 1 97s
NAME READY AGE
statefulset.apps/admission-webhook-bootstrap-stateful-set 1/1 97s
statefulset.apps/application-controller-stateful-set 1/1 98s
statefulset.apps/metacontroller 1/1 98s
statefulset.apps/seldon-operator-controller-manager 1/1 92s
$ kubectl get pvc -n kubeflow
NAME STATUS VOLUME
CAPACITY ACCESS MODES STORAGECLASS AGE
katib-mysql Bound pvc-b07f293e-d028-11e9-9b9d-00505681a82d
10Gi RWO ontap-ai-flexvols-retain 27m
metadata-mysql Bound pvc-b0f3f032-d028-11e9-9b9d-00505681a82d
10Gi RWO ontap-ai-flexvols-retain 27m
minio-pv-claim Bound pvc-b22727ee-d028-11e9-9b9d-00505681a82d
20Gi RWO ontap-ai-flexvols-retain 27m
mysql-pv-claim Bound pvc-b2429afcd-d028-11e9-9b9d-00505681a82d
20Gi RWO ontap-ai-flexvols-retain 27m

```

4. In your web browser, access the Kubeflow central dashboard by navigating to the URL that you noted

down in step 2.

The default username is `admin@kubeflow.org`, and the default password is `12341234`. To create additional users, follow the instructions in the [official Kubeflow documentation](#).



Next: [Example Kubeflow Operations and Tasks](#).

## Example Kubeflow Operations and Tasks

This section includes examples of various operations and tasks that you may want to perform using Kubeflow.

Next: [Provision a Jupyter Notebook Workspace for Data Scientist or Developer Use](#).

## Example Kubeflow Operations and Tasks

This section includes examples of various operations and tasks that you may want to perform using Kubeflow.

Next: [Provision a Jupyter Notebook Workspace for Data Scientist or Developer Use](#).

## Provision a Jupyter Notebook Workspace for Data Scientist or Developer Use

Kubeflow is capable of rapidly provisioning new Jupyter Notebook servers to act as data scientist workspaces. To provision a new Jupyter Notebook server with Kubeflow, perform the following tasks. For more information about Jupyter Notebooks within the Kubeflow context, see the [official Kubeflow documentation](#).

1. From the Kubeflow central dashboard, click Notebook Servers in the main menu to navigate to the Jupyter Notebook server administration page.

The screenshot shows the Kubeflow Central Dashboard interface. The left sidebar has a dark blue background with white text. It lists several options: Home, Pipelines, **Notebook Servers** (which is highlighted with a yellow box), Katib, Artifact Store, GitHub, and Documentation. The main content area has a light gray background. At the top, it shows the title "Kubeflow Central Dashboard" and the URL "10.61.218.131:31380/?ns=kubeflow-anonymous". Below the title, there's a dropdown menu showing "kubeflow-anonymous". A "Quick shortcuts" box is open, containing five items with icons and text: "Upload a pipeline" (Pipelines), "View all pipeline runs" (Pipelines), "Create a new Notebook server" (Notebook Servers), "View Katib Studies" (Katib), and "View Metadata Artifacts" (Artifact Store).

2. Click New Server to provision a new Jupyter Notebook server.

The screenshot shows a web browser window titled "Kubeflow Central Dashboard". The URL is "Not Secure | 10.61.218.131:31380/\_/jupyter/?ns=kubeflow-anonymous...". The page header includes the Kubeflow logo and the namespace "kubeflow-anonymous". The main content area is titled "Notebook Servers" and features a table with columns: Status, Name, Age, Image, CPU, Memory, and Volumes. A yellow-bordered button labeled "+ NEW SERVER" is located in the top right corner of the table header.

3. Give your new server a name, choose the Docker image that you want your server to be based on, and specify the amount of CPU and RAM to be reserved by your server. If the Namespace field is blank, use the Select Namespace menu in the page header to choose a namespace. The Namespace field is then auto-populated with the chosen namespace.

In the following example, the `kubeflow-anonymous` namespace is chosen. In addition, the default values for Docker image, CPU, and RAM are accepted.

Kubeflow Central Dashboard Not Secure | 10.61.218.131:31380/\_jupyter/?ns=kubeflow-anonym...

**Name**

Specify the name of the Notebook Server and the Namespace it will belong to.

Name: mike

Namespace: kubeflow-anonymous

**Image**

A starter Jupyter Docker Image with a baseline deployment and typical ML packages.

Custom Image

Image: gcr.io/kubeflow-images-public/tensorflow-1.13.1-notebook-cpu:v0.5.0

**CPU / RAM**

Specify the total amount of CPU and RAM reserved by your Notebook Server. For CPU-intensive workloads, you can choose more than 1 CPU (e.g. 1.5).

CPU: 0.5

Memory: 1.0Gi

4. Specify the workspace volume details. If you choose to create a new volume, then that volume or PVC is provisioned using the default StorageClass. Because a StorageClass utilizing Trident was designated as the default StorageClass in the section [Kubeflow Deployment](#), the volume or PVC is provisioned with Trident. This volume is automatically mounted as the default workspace within the Jupyter Notebook Server container. Any notebooks that a user creates on the server that are not saved to a separate data volume are automatically saved to this workspace volume. Therefore, the notebooks are persistent across reboots.

 **Workspace Volume**

Configure the Volume to be mounted as your personal Workspace.

**Don't use Persistent Storage for User's home**

Type	Name	Size	Mode	Mount Point
New	workspace-mike	10Gi	ReadWriteOnce	/home/jovyan

5. Add data volumes. The following example specifies an existing PVC named 'pb-fg-all' and accepts the default mount point.

## Data Volumes

Configure the Volumes to be mounted as your Datasets.

[+ ADD VOLUME](#)

Type

Existing

Name

pb-fg-all

Size

10Gi

Mode

ReadWriteOnce

Mount Point

/home/jovyan/data-vol-1



6. **Optional:** Request that the desired number of GPUs be allocated to your notebook server. In the following example, one GPU is requested.

## Configurations

Extra layers of configurations that will be applied to the new Notebook. (e.g. Insert credentials as Secrets, set Environment Variables.)

Configurations

## Extra Resources

Specify extra resources that might be needed in the Notebook Server.

Enable Shared Memory

Extra Resources \*

{"nvidia.com/gpu": 1}

Extra Resources available in the cluster (ex. NVIDIA GPUs)

[LAUNCH](#)

[CANCEL](#)

7. Click Launch to provision your new notebook server.

8. Wait for your notebook server to be fully provisioned. This can take several minutes if you have never provisioned a server using the Docker image that you specified because the image needs to be downloaded. When your server has been fully provisioned, you see a green check mark in the Status column on the Jupyter Notebook server administration page.

Notebook Servers

Status	Name	Age	Image	CPU	Memory	Volumes
Running	mike	12 mins ago	tensorflow-1.13.1-notebook-cpu:v0.5.0	0.5	1.0Gi	⋮

+ NEW SERVER

CONNECT

9. Click Connect to connect to your new server web interface.
10. Confirm that the dataset volume that was specified in step 6 is mounted on the server. Note that this volume is mounted within the default workspace by default. From the perspective of the user, this is just another folder within the workspace. The user, who is likely a data scientist and not an infrastructure expert, does not need to possess any storage expertise in order to use this volume.

jupyter

Files    Running    Clusters

Select items to perform actions on them.

Upload    New    Quit

0	/	Name	Last Modified	File size
<input type="checkbox"/>	<input type="checkbox"/> data-vol-1		a day ago	



11. Open a Terminal and, assuming that a new volume was requested in step 5, execute `df -h` to confirm that a new Trident-provisioned persistent volume is mounted as the default workspace.

The default workspace directory is the base directory that you are presented with when you first access the server's web interface. Therefore, any artifacts that you create by using the web interface are stored on this Trident-provisioned persistent volume.



```
$ df -h
Filesystem              Size  Used Avail
overlay                  439G  34G  382G
/
tmpfs                   64M   0    64M
/dev/sda2                439G  34G  382G
/etc/hosts                9%
/home/jovyan
192.168.11.11:/trident_pvc_3dcfe7e5_d5a9_11e9_9b9d_00505681a82d  10G  320K  10G
1% /home/jovyan
tmpfs                   252G  0    252G
0% /dev/shm
192.168.11.11:/pb_fg_all          10T  10T  47G
100% /home/jovyan/data-vol-1
tmpfs                   252G  12K  252G
1% /run/secrets/kubernetes.io/serviceaccount
tmpfs                   252G  12K  252G
1% /proc/driver/nvidia
tmpfs                   51G   4.9M  51G
1% /run/nvidia-persistenced/socket
udev                   252G  0    252G
0% /dev/nvidia5
tmpfs                   252G  0    252G
0% /proc/acpi
tmpfs                   252G  0    252G
0% /proc/scsi
tmpfs                   252G  0    252G
0% /sys/firmware
$
```

12. Using the terminal, run nvidia-smi to confirm that the correct number of GPUs were allocated to the notebook server. In the following example, one GPU has been allocated to the notebook server as requested in step 7.

```
$ nvidia-smi
Fri Sep 13 13:52:15 2019
+-----+
| NVIDIA-SMI 410.104      Driver Version: 410.104      CUDA Version: N/A |
+-----+
| GPU  Name     Persistence-M| Bus-Id     Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap| Memory-Usage | GPU-Util  Compute M. |
|-----+
| 0  Tesla V100-SXM2... On   | 00000000:86:00.0 Off   |          0 |
| N/A   38C    P0    46W / 300W |      0MiB / 32480MiB |     0%      Default |
+-----+
+-----+
| Processes:                               GPU Memory |
| GPU  PID  Type  Process name        Usage        |
|-----+
| No running processes found            |
+-----+
$
```

Next: Example Notebooks and Pipelines.

## Example Notebooks and Pipelines

The [NetApp Data Science Toolkit for Kubernetes](#) can be used in conjunction with Kubeflow. Using the NetApp Data Science Toolkit with Kubeflow provides the following benefits:

- Data scientists can perform advanced NetApp data management operations directly from within a Jupyter Notebook.
- Advanced NetApp data management operations can be incorporated into automated workflows using the Kubeflow Pipelines framework.

Refer to the [Kubeflow Examples](#) section within the NetApp Data Science Toolkit GitHub repository for details on using the toolkit with Kubeflow.

Next: [Apache Airflow Deployment](#).

## Apache Airflow Deployment

NetApp recommends running Apache Airflow on top of Kubernetes. This section describes the tasks that you must complete to deploy Airflow in your Kubernetes cluster.



It is possible to deploy Airflow on platforms other than Kubernetes. Deploying Airflow on platforms other than Kubernetes is outside of the scope of this solution.

## Prerequisites

Before you perform the deployment exercise that is outlined in this section, we assume that you have already performed the following tasks:

1. You already have a working Kubernetes cluster.
2. You have already installed and configured NetApp Trident in your Kubernetes cluster as outlined in the section “[NetApp Trident Deployment and Configuration](#).”

## Install Helm

Airflow is deployed using Helm, a popular package manager for Kubernetes. Before you deploy Airflow, you must install Helm on the deployment jump host. To install Helm on the deployment jump host, follow the [installation instructions](#) in the official Helm documentation.

## Set Default Kubernetes StorageClass

Before you deploy Airflow, you must designate a default StorageClass within your Kubernetes cluster. The Airflow deployment process attempts to provision new persistent volumes using the default StorageClass. If no StorageClass is designated as the default StorageClass, then the deployment fails. To designate a default StorageClass within your cluster, follow the instructions outlined in the section [Kubeflow Deployment](#). If you have already designated a default StorageClass within your cluster, then you can skip this step.

## Use Helm to Deploy Airflow

To deploy Airflow in your Kubernetes cluster using Helm, perform the following tasks from the deployment jump host:

1. Deploy Airflow using Helm by following the [deployment instructions](#) for the official Airflow chart on the

Artifact Hub. The example commands that follow show the deployment of Airflow using Helm. Modify, add, and/or remove values in the `custom-values.yaml` file as needed depending on your environment and desired configuration.

```
$ cat << EOF > custom-values.yaml
#####
# Airflow - Common Configs
#####
airflow:
    ## the airflow executor type to use
    ##
    executor: "CeleryExecutor"
    ## environment variables for the web/scheduler/worker Pods (for
airflow configs)
    ##
    #
#####
# Airflow - WebUI Configs
#####
web:
    ## configs for the Service of the web Pods
    ##
    service:
        type: NodePort
#####
# Airflow - Logs Configs
#####
logs:
    persistence:
        enabled: true
#####
# Airflow - DAGs Configs
#####
dags:
    ## configs for the DAG git repository & sync container
    ##
    gitSync:
        enabled: true
        ## url of the git repository
        ##
        repo: "git@github.com:mboglesby/airflow-dev.git"
        ## the branch/tag/sha1 which we clone
        ##
        branch: master
        revision: HEAD
        ## the name of a pre-created secret containing files for ~/.ssh/
```

```

## 
## NOTE:
## - this is ONLY RELEVANT for SSH git repos
## - the secret commonly includes files: id_rsa, id_rsa.pub,
known_hosts
## - known_hosts is NOT NEEDED if `git.sshKeyscan` is true
##
sshSecret: "airflow-ssh-git-secret"
## the name of the private key file in your `git.secret`
##
## NOTE:
## - this is ONLY RELEVANT for PRIVATE SSH git repos
##
sshSecretKey: id_rsa
## the git sync interval in seconds
##
syncWait: 60
EOF
$ helm install airflow airflow-stable/airflow -n airflow --version 8.0.8
--values ./custom-values.yaml
...
Congratulations. You have just deployed Apache Airflow!
1. Get the Airflow Service URL by running these commands:
   export NODE_PORT=$(kubectl get --namespace airflow -o
   jsonpath=".spec.ports[0].nodePort" services airflow-web)
   export NODE_IP=$(kubectl get nodes --namespace airflow -o
   jsonpath=".items[0].status.addresses[0].address")
   echo http://$NODE_IP:$NODE_PORT/
2. Open Airflow in your web browser

```

2. Confirm that all Airflow pods are up and running. It may take a few minutes for all pods to start.

NAME	READY	STATUS	RESTARTS	AGE
airflow-flower-b5656d44f-h8qjk	1/1	Running	0	2h
airflow-postgresql-0	1/1	Running	0	2h
airflow-redis-master-0	1/1	Running	0	2h
airflow-scheduler-9d95fcdf9-clf4b	2/2	Running	2	2h
airflow-web-59c94db9c5-z7rg4	1/1	Running	0	2h
airflow-worker-0	2/2	Running	2	2h

3. Obtain the Airflow web service URL by following the instructions that were printed to the console when you deployed Airflow using Helm in step 1.

```
$ export NODE_PORT=$(kubectl get --namespace airflow -o jsonpath=".spec.ports[0].nodePort" services airflow-web)
$ export NODE_IP=$(kubectl get nodes --namespace airflow -o jsonpath=".items[0].status.addresses[0].address")
$ echo http://$NODE_IP:$NODE_PORT/
```

#### 4. Confirm that you can access the Airflow web service.

	<b>DAG</b>	<b>Schedule</b>	<b>Owner</b>	<b>Recent Tasks</b>	<b>Last Run</b>	<b>DAG Runs</b>	<b>Links</b>
<input checked="" type="checkbox"/>	Off ai_training_run	None	NetApp	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●
<input checked="" type="checkbox"/>	Off create_data_scientist_workspace	None	NetApp	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●
<input checked="" type="checkbox"/>	Off example_bash_operator	0 0 * * *	Airflow	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●
<input checked="" type="checkbox"/>	Off example_branch_dop_operator_v3	*/1 * * * *	Airflow	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●
<input checked="" type="checkbox"/>	Off example_branch_operator	@daily	Airflow	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●
<input checked="" type="checkbox"/>	Off example_complex	None	airflow	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●
<input checked="" type="checkbox"/>	Off example_external_task_marker_child	None	airflow	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●
<input checked="" type="checkbox"/>	Off example_external_task_marker_parent	None	airflow	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●
<input checked="" type="checkbox"/>	Off example_http_operator	1 day, 0:00:00	Airflow	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●
<input checked="" type="checkbox"/>	Off example_kubernetes_executor_config	None	Airflow	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●
<input checked="" type="checkbox"/>	Off example_nested_branch_dag	@daily	airflow	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●
<input checked="" type="checkbox"/>	Off example_passing_params_via_test_command	*/1 * * * *	airflow	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●
<input checked="" type="checkbox"/>	Off example_pig_operator	None	Airflow	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●
<input checked="" type="checkbox"/>	Off example_python_operator	None	Airflow	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●
<input checked="" type="checkbox"/>	Off example_short_circuit_operator	1 day, 0:00:00	Airflow	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●
<input checked="" type="checkbox"/>	Off example_skip_dag	1 day, 0:00:00	Airflow	○○○○○○○○○○○○		○○○○	○●●●●●●●●●●●●

Next: [Example Apache Airflow Workflows](#).

### Example Apache Airflow Workflows

The [NetApp Data Science Toolkit for Kubernetes](#) can be used in conjunction with Airflow. Using the NetApp Data Science Toolkit with Airflow enables you to incorporate NetApp data management operations into automated workflows that are orchestrated by Airflow.

Refer to the [Airflow Examples](#) section within the NetApp Data Science Toolkit GitHub repository for details on using the toolkit with Airflow.

Next: Example Trident Operations.

## Example Trident Operations

This section includes examples of various operations that you may want to perform with Trident.

### Import an Existing Volume

If there are existing volumes on your NetApp storage system/platform that you want to mount on containers within your Kubernetes cluster, but that are not tied to PVCs in the cluster, then you must import these volumes. You can use the Trident volume import functionality to import these volumes.

The example commands that follow show the importing of the same volume, named `pb_fg_all`, twice, once for each Trident Backend that was created in the example in the section [Example Trident Backends for ONTAP AI Deployments](#), step 1. Importing the same volume twice in this manner enables you to mount the volume (an existing FlexGroup volume) multiple times across different LIFs, as described in the section [Example Trident Backends for ONTAP AI Deployments](#), step 1. For more information about PVCs, see the [official Kubernetes documentation](#). For more information about the volume import functionality, see the [Trident documentation](#).

An `accessModes` value of `ReadOnlyMany` is specified in the example PVC spec files. For more information about the `accessMode` field, see the [official Kubernetes documentation](#).

 The Backend names that are specified in the following example import commands correspond to the Backends that were created in the example in the section [Example Trident Backends for ONTAP AI Deployments](#), step 1. The StorageClass names that are specified in the following example PVC definition files correspond to the StorageClasses that were created in the example in the section [Example Kubernetes StorageClasses for ONTAP AI Deployments](#), step 1.

```
$ cat << EOF > ./pvc-import-pb_fg_all-iface1.yaml
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pb-fg-all-iface1
  namespace: default
spec:
  accessModes:
    - ReadOnlyMany
  storageClassName: ontap-ai-flexgroups-retain-iface1
EOF
$ tridentctl import volume ontap-ai-flexgroups-iface1 pb_fg_all -f ./pvc-import-pb_fg_all-iface1.yaml -n trident
+-----+-----+
+-----+-----+
+-----+-----+-----+
|          NAME          |  SIZE   |      STORAGE CLASS      |
| PROTOCOL |           BACKEND UUID           | STATE   |
MANAGED  |
+-----+-----+
```

```

+-----+
+-----+-----+-----+
| default-pb-fg-all-iface1-7d9f1 | 10 TiB | ontap-ai-flexgroups-retain-
iface1 | file      | b74cbddb-e0b8-40b7-b263-b6da6dec0bdd | online | true
|
+-----+-----+
+-----+-----+
+-----+-----+-----+
$ cat << EOF > ./pvc-import-pb_fg_all-iface2.yaml
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pb-fg-all-iface2
  namespace: default
spec:
  accessModes:
    - ReadOnlyMany
  storageClassName: ontap-ai-flexgroups-retain-iface2
EOF
$ tridentctl import volume ontap-ai-flexgroups-iface2 pb_fg_all -f ./pvc-
import-pb_fg_all-iface2.yaml -n trident
+-----+
+-----+
+-----+-----+-----+
|           NAME          |   SIZE   |        STORAGE CLASS
| PROTOCOL |           BACKEND UUID           | STATE |
MANAGED |
+-----+
+-----+
+-----+-----+-----+
| default-pb-fg-all-iface2-85aee | 10 TiB | ontap-ai-flexgroups-retain-
iface2 | file      | 61814d48-c770-436b-9cb4-cf7ee661274d | online | true
|
+-----+
+-----+
+-----+-----+-----+
$ tridentctl get volume -n trident
+-----+
+-----+
+-----+-----+-----+
|           NAME          |   SIZE   |        STORAGE CLASS
| PROTOCOL |           BACKEND UUID           | STATE | MANAGED |
+-----+
+-----+
+-----+-----+-----+
| default-pb-fg-all-iface1-7d9f1 | 10 TiB | ontap-ai-flexgroups-retain-

```

```

iface1 | file      | b74cbddb-e0b8-40b7-b263-b6da6dec0bdd | online | true
|
| default-pb-fg-all-iface2-85aee   | 10 TiB  | ontap-ai-flexgroups-retain-
iface2 | file      | 61814d48-c770-436b-9cb4-cf7ee661274d | online | true
|
+-----+
+-----+
+-----+-----+
$ kubectl get pvc
NAME           STATUS    VOLUME                                     CAPACITY
ACCESS MODES   STORAGECLASS                               AGE
pb-fg-all-iface1   Bound     default-pb-fg-all-iface1-7d9f1
10995116277760   ROX       ontap-ai-flexgroups-retain-iface1   25h
pb-fg-all-iface2   Bound     default-pb-fg-all-iface2-85aee
10995116277760   ROX       ontap-ai-flexgroups-retain-iface2   25h

```

## Provision a New Volume

You can use Trident to provision a new volume on your NetApp storage system or platform. The following example commands show the provisioning of a new FlexVol volume. In this example, the volume is provisioned using the StorageClass that was created in the example in the section [Example Kubernetes StorageClasses for ONTAP AI Deployments](#), step 2.

An `accessModes` value of `ReadWriteMany` is specified in the following example PVC definition file. For more information about the `accessMode` field, see the [official Kubernetes documentation](#).

```

$ cat << EOF > ./pvc-tensorflow-results.yaml
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: tensorflow-results
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-ai-flexvols-retain
EOF
$ kubectl create -f ./pvc-tensorflow-results.yaml
persistentvolumeclaim/tensorflow-results created
$ kubectl get pvc
NAME                      STATUS        VOLUME
CAPACITY      ACCESS MODES   STORAGECLASS          AGE
pb-fg-all-iface1           Bound       default-pb-fg-all-iface1-7d9f1
10995116277760   ROX          ontap-ai-flexgroups-retain-iface1 26h
pb-fg-all-iface2           Bound       default-pb-fg-all-iface2-85aee
10995116277760   ROX          ontap-ai-flexgroups-retain-iface2 26h
tensorflow-results         Bound       default-tensorflow-results-
2fd60      1073741824     RWX          ontap-ai-flexvols-retain
25h

```

[Next: Example High-Performance Jobs for ONTAP AI Deployments Overview.](#)

### Example High-performance Jobs for ONTAP AI Deployments

This section includes examples of various high-performance jobs that can be executed when Kubernetes is deployed on an ONTAP AI pod.

[Next: Execute a Single-Node AI Workload.](#)

### Example High-performance Jobs for ONTAP AI Deployments

This section includes examples of various high-performance jobs that can be executed when Kubernetes is deployed on an ONTAP AI pod.

[Next: Execute a Single-Node AI Workload.](#)

### Execute a Single-Node AI Workload

To execute a single-node AI and ML job in your Kubernetes cluster, perform the following tasks from the deployment jump host. With Trident, you can quickly and easily make a data volume, potentially containing petabytes of data, accessible to a Kubernetes

workload. To make such a data volume accessible from within a Kubernetes pod, simply specify a PVC in the pod definition. This step is a Kubernetes-native operation; no NetApp expertise is required.



This section assumes that you have already containerized (in the Docker container format) the specific AI and ML workload that you are attempting to execute in your Kubernetes cluster.

1. The following example commands show the creation of a Kubernetes job for a TensorFlow benchmark workload that uses the ImageNet dataset. For more information about the ImageNet dataset, see the [ImageNet website](#).

This example job requests eight GPUs and therefore can run on a single GPU worker node that features eight or more GPUs. This example job could be submitted in a cluster for which a worker node featuring eight or more GPUs is not present or is currently occupied with another workload. If so, then the job remains in a pending state until such a worker node becomes available.

Additionally, in order to maximize storage bandwidth, the volume that contains the needed training data is mounted twice within the pod that this job creates. Another volume is also mounted in the pod. This second volume will be used to store results and metrics. These volumes are referenced in the job definition by using the names of the PVCs. For more information about Kubernetes jobs, see the [official Kubernetes documentation](#).

An `emptyDir` volume with a `medium` value of `Memory` is mounted to `/dev/shm` in the pod that this example job creates. The default size of the `/dev/shm` virtual volume that is automatically created by the Docker container runtime can sometimes be insufficient for TensorFlow's needs. Mounting an `emptyDir` volume as in the following example provides a sufficiently large `/dev/shm` virtual volume. For more information about `emptyDir` volumes, see the [official Kubernetes documentation](#).

The single container that is specified in this example job definition is given a `securityContext > privileged` value of `true`. This value means that the container effectively has root access on the host. This annotation is used in this case because the specific workload that is being executed requires root access. Specifically, a clear cache operation that the workload performs requires root access. Whether or not this `privileged: true` annotation is necessary depends on the requirements of the specific workload that you are executing.

```
$ cat << EOF > ./netapp-tensorflow-single-imagenet.yaml
apiVersion: batch/v1
kind: Job
metadata:
  name: netapp-tensorflow-single-imagenet
spec:
  backoffLimit: 5
  template:
    spec:
      volumes:
        - name: dshm
          emptyDir:
            medium: Memory
        - name: testdata-iface1
          persistentVolumeClaim:
```

```

        claimName: pb-fg-all-iface1
      - name: testdata-iface2
        persistentVolumeClaim:
          claimName: pb-fg-all-iface2
      - name: results
        persistentVolumeClaim:
          claimName: tensorflow-results
      containers:
      - name: netapp-tensorflow-py2
        image: netapp/tensorflow-py2:19.03.0
        command: ["python", "/netapp/scripts/run.py", "--dataset_dir=/mnt/mount_0/dataset/imagenet", "--dgx_version=dgx1", "--num_devices=8"]
      resources:
        limits:
          nvidia.com/gpu: 8
      volumeMounts:
      - mountPath: /dev/shm
        name: dshm
      - mountPath: /mnt/mount_0
        name: testdata-iface1
      - mountPath: /mnt/mount_1
        name: testdata-iface2
      - mountPath: /tmp
        name: results
      securityContext:
        privileged: true
      restartPolicy: Never
EOF
$ kubectl create -f ./netapp-tensorflow-single-imagenet.yaml
job.batch/netapp-tensorflow-single-imagenet created
$ kubectl get jobs
NAME                               COMPLETIONS   DURATION   AGE
netapp-tensorflow-single-imagenet   0/1           24s        24s

```

2. Confirm that the job that you created in step 1 is running correctly. The following example command confirms that a single pod was created for the job, as specified in the job definition, and that this pod is currently running on one of the GPU worker nodes.

```

$ kubectl get pods -o wide
NAME                               READY   STATUS
RESTARTS   AGE
IP          NODE          NOMINATED NODE
netapp-tensorflow-single-imagenet-m7x92   1/1     Running   0
3m       10.233.68.61    10.61.218.154   <none>

```

3. Confirm that the job that you created in step 1 completes successfully. The following example commands confirm that the job completed successfully.

```
$ kubectl get jobs
NAME                      COMPLETIONS   DURATION
AGE
netapp-tensorflow-single-imagenet      1/1          5m42s
10m

$ kubectl get pods
NAME                      READY   STATUS
RESTARTS     AGE
netapp-tensorflow-single-imagenet-m7x92   0/1    Completed
0           11m

$ kubectl logs netapp-tensorflow-single-imagenet-m7x92
[netapp-tensorflow-single-imagenet-m7x92:00008] PMIX ERROR: NO-
PERMISSIONS in file gds_dstore.c at line 702
[netapp-tensorflow-single-imagenet-m7x92:00008] PMIX ERROR: NO-
PERMISSIONS in file gds_dstore.c at line 711
Total images/sec = 6530.59125
===== Clean Cache !!! =====
mpirun -allow-run-as-root -np 1 -H localhost:1 bash -c 'sync; echo 1 >
/proc/sys/vm/drop_caches'
=====
mpirun -allow-run-as-root -np 8 -H localhost:8 -bind-to none -map-by
slot -x NCCL_DEBUG=INFO -x LD_LIBRARY_PATH -x PATH python
/netapp/tensorflow/benchmarks_190205/scripts/tf_cnn_benchmarks/tf_cnn_be
nchmarks.py --model=resnet50 --batch_size=256 --device=gpu
--force_gpu_compatible=True --num_intra_threads=1 --num_inter_threads=48
--variable_update=horovod --batch_group_size=20 --num_batches=500
--nodistortions --num_gpus=1 --data_format=NCHW --use_fp16=True
--use_tf_layers=False --data_name=imagenet --use_datasets=True
--data_dir=/mnt/mount_0/dataset/imagenet
--datasets_parallel_interleave_cycle_length=10
--datasets_sloppy_parallel_interleave=False --num_mounts=2
--mount_prefix=/mnt/mount_%d --datasets_prefetch_buffer_size=2000
--datasets_use_prefetch=True --datasets_num_private_threads=4
--horovod_device=gpu >
/tmp/20190814_105450_tensorflow_horovod_rdma_resnet50_gpu_8_256_b500_im
agenet_nodistort_fp16_r10_m2_nockpt.txt 2>&1
```

4. **Optional:** Clean up job artifacts. The following example commands show the deletion of the job object that was created in step 1.

When you delete the job object, Kubernetes automatically deletes any associated pods.

```

$ kubectl get jobs
NAME                                COMPLETIONS   DURATION
AGE
netapp-tensorflow-single-imagenet      1/1          5m42s
10m

$ kubectl get pods
NAME                                READY   STATUS
RESTARTS   AGE
netapp-tensorflow-single-imagenet-m7x92  0/1    Completed
0          11m

$ kubectl delete job netapp-tensorflow-single-imagenet
job.batch "netapp-tensorflow-single-imagenet" deleted

$ kubectl get jobs
No resources found.

$ kubectl get pods
No resources found.

```

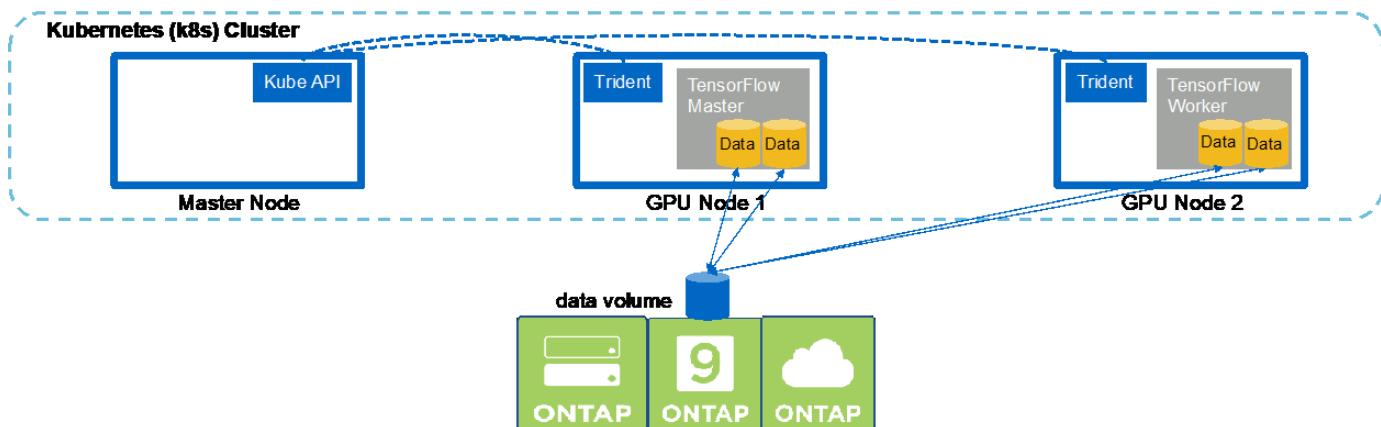
[Next: Execute a Synchronous Distributed AI Workload.](#)

#### Execute a Synchronous Distributed AI Workload

To execute a synchronous multinode AI and ML job in your Kubernetes cluster, perform the following tasks on the deployment jump host. This process enables you to take advantage of data that is stored on a NetApp volume and to use more GPUs than a single worker node can provide. See the following figure for a depiction of a synchronous distributed AI job.



Synchronous distributed jobs can help increase performance and training accuracy compared with asynchronous distributed jobs. A discussion of the pros and cons of synchronous jobs versus asynchronous jobs is outside the scope of this document.



1. The following example commands show the creation of one worker that participates in the synchronous distributed execution of the same TensorFlow benchmark job that was executed on a single node in the example in the section [Execute a Single-Node AI Workload](#). In this specific example, only a single worker

is deployed because the job is executed across two worker nodes.

This example worker deployment requests eight GPUs and thus can run on a single GPU worker node that features eight or more GPUs. If your GPU worker nodes feature more than eight GPUs, to maximize performance, you might want to increase this number to be equal to the number of GPUs that your worker nodes feature. For more information about Kubernetes deployments, see the [official Kubernetes documentation](#).

A Kubernetes deployment is created in this example because this specific containerized worker would never complete on its own. Therefore, it doesn't make sense to deploy it by using the Kubernetes job construct. If your worker is designed or written to complete on its own, then it might make sense to use the job construct to deploy your worker.

The pod that is specified in this example deployment specification is given a `hostNetwork` value of `true`. This value means that the pod uses the host worker node's networking stack instead of the virtual networking stack that Kubernetes usually creates for each pod. This annotation is used in this case because the specific workload relies on Open MPI, NCCL, and Horovod to execute the workload in a synchronous distributed manner. Therefore, it requires access to the host networking stack. A discussion about Open MPI, NCCL, and Horovod is outside the scope of this document. Whether or not this `hostNetwork: true` annotation is necessary depends on the requirements of the specific workload that you are executing. For more information about the `hostNetwork` field, see the [official Kubernetes documentation](#).

```
$ cat << EOF > ./netapp-tensorflow-multi-imagenet-worker.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: netapp-tensorflow-multi-imagenet-worker
spec:
  replicas: 1
  selector:
    matchLabels:
      app: netapp-tensorflow-multi-imagenet-worker
  template:
    metadata:
      labels:
        app: netapp-tensorflow-multi-imagenet-worker
    spec:
      hostNetwork: true
      volumes:
        - name: dshm
          emptyDir:
            medium: Memory
        - name: testdata-iface1
          persistentVolumeClaim:
            claimName: pb-fg-all-iface1
        - name: testdata-iface2
          persistentVolumeClaim:
            claimName: pb-fg-all-iface2
EOF
```

```

- name: results
  persistentVolumeClaim:
    claimName: tensorflow-results
  containers:
  - name: netapp-tensorflow-py2
    image: netapp/tensorflow-py2:19.03.0
    command: ["bash", "/netapp/scripts/start-slave-multi.sh",
"22122"]
    resources:
      limits:
        nvidia.com/gpu: 8
  volumeMounts:
  - mountPath: /dev/shm
    name: dshm
  - mountPath: /mnt/mount_0
    name: testdata-iface1
  - mountPath: /mnt/mount_1
    name: testdata-iface2
  - mountPath: /tmp
    name: results
  securityContext:
    privileged: true
EOF
$ kubectl create -f ./netapp-tensorflow-multi-imagenet-worker.yaml
deployment.apps/netapp-tensorflow-multi-imagenet-worker created
$ kubectl get deployments
NAME                                DESIRED   CURRENT   UP-TO-DATE
AVAILABLE   AGE
netapp-tensorflow-multi-imagenet-worker   1         1         1
1           4s

```

2. Confirm that the worker deployment that you created in step 1 launched successfully. The following example commands confirm that a single worker pod was created for the deployment, as indicated in the deployment definition, and that this pod is currently running on one of the GPU worker nodes.

```

$ kubectl get pods -o wide
NAME                                READY
STATUS     RESTARTS   AGE
IP          NODE          NOMINATED NODE
netapp-tensorflow-multi-imagenet-worker-654fc7f486-v6725   1/1
Running     0          60s   10.61.218.154   10.61.218.154   <none>
$ kubectl logs netapp-tensorflow-multi-imagenet-worker-654fc7f486-v6725
22122

```

3. Create a Kubernetes job for a master that kicks off, participates in, and tracks the execution of the

synchronous multinode job. The following example commands create one master that kicks off, participates in, and tracks the synchronous distributed execution of the same TensorFlow benchmark job that was executed on a single node in the example in the section [Execute a Single-Node AI Workload](#).

This example master job requests eight GPUs and thus can run on a single GPU worker node that features eight or more GPUs. If your GPU worker nodes feature more than eight GPUs, to maximize performance, you might want to increase this number to be equal to the number of GPUs that your worker nodes feature.

The master pod that is specified in this example job definition is given a `hostNetwork` value of `true`, just as the worker pod was given a `hostNetwork` value of `true` in step 1. See step 1 for details about why this value is necessary.

```
$ cat << EOF > ./netapp-tensorflow-multi-imagenet-master.yaml
apiVersion: batch/v1
kind: Job
metadata:
  name: netapp-tensorflow-multi-imagenet-master
spec:
  backoffLimit: 5
  template:
    spec:
      hostNetwork: true
      volumes:
        - name: dshm
          emptyDir:
            medium: Memory
        - name: testdata-iface1
          persistentVolumeClaim:
            claimName: pb-fg-all-iface1
        - name: testdata-iface2
          persistentVolumeClaim:
            claimName: pb-fg-all-iface2
        - name: results
          persistentVolumeClaim:
            claimName: tensorflow-results
      containers:
        - name: netapp-tensorflow-py2
          image: netapp/tensorflow-py2:19.03.0
          command: ["python", "/netapp/scripts/run.py", "--dataset_dir=/mnt/mount_0/dataset/imagenet", "--port=22122", "--num_devices=16", "--dgx_version=dgx1", "--nodes=10.61.218.152,10.61.218.154"]
          resources:
            limits:
              nvidia.com/gpu: 8
      volumeMounts:
        - mountPath: /dev/shm
```

```

        name: dshm
      - mountPath: /mnt/mount_0
        name: testdata-iface1
      - mountPath: /mnt/mount_1
        name: testdata-iface2
      - mountPath: /tmp
        name: results
    securityContext:
      privileged: true
  restartPolicy: Never
EOF
$ kubectl create -f ./netapp-tensorflow-multi-imagenet-master.yaml
job.batch/netapp-tensorflow-multi-imagenet-master created
$ kubectl get jobs
NAME                               COMPLETIONS   DURATION   AGE
netapp-tensorflow-multi-imagenet-master   0/1          25s        25s

```

4. Confirm that the master job that you created in step 3 is running correctly. The following example command confirms that a single master pod was created for the job, as indicated in the job definition, and that this pod is currently running on one of the GPU worker nodes. You should also see that the worker pod that you originally saw in step 1 is still running and that the master and worker pods are running on different nodes.

```

$ kubectl get pods -o wide
NAME                                     READY
STATUS      RESTARTS      AGE
IP           NODE          NOMINATED NODE
netapp-tensorflow-multi-imagenet-master-ppwwj   1/1
Running      0            45s     10.61.218.152   10.61.218.152   <none>
netapp-tensorflow-multi-imagenet-worker-654fc7f486-v6725   1/1
Running      0            26m     10.61.218.154   10.61.218.154   <none>

```

5. Confirm that the master job that you created in step 3 completes successfully. The following example commands confirm that the job completed successfully.

```

$ kubectl get jobs
NAME                               COMPLETIONS   DURATION   AGE
netapp-tensorflow-multi-imagenet-master   1/1          5m50s     9m18s
$ kubectl get pods
NAME                                     READY
STATUS      RESTARTS      AGE
netapp-tensorflow-multi-imagenet-master-ppwwj   0/1
Completed    0            9m38s
netapp-tensorflow-multi-imagenet-worker-654fc7f486-v6725   1/1
Running      0            35m
$ kubectl logs netapp-tensorflow-multi-imagenet-master-ppwwj

```

```

[10.61.218.152:00008] WARNING: local probe returned unhandled
shell:unknown assuming bash
rm: cannot remove '/lib': Is a directory
[10.61.218.154:00033] PMIX ERROR: NO-PERMISSIONS in file gds_dstore.c at
line 702
[10.61.218.154:00033] PMIX ERROR: NO-PERMISSIONS in file gds_dstore.c at
line 711
[10.61.218.152:00008] PMIX ERROR: NO-PERMISSIONS in file gds_dstore.c at
line 702
[10.61.218.152:00008] PMIX ERROR: NO-PERMISSIONS in file gds_dstore.c at
line 711
Total images/sec = 12881.33875
===== Clean Cache !!! =====
mpirun -allow-run-as-root -np 2 -H 10.61.218.152:1,10.61.218.154:1 -mca
pml ob1 -mca btl ^openib -mca btl_tcp_if_include enp1s0f0 -mca
plm_rsh_agent ssh -mca plm_rsh_args "-p 22122" bash -c 'sync; echo 1 >
/proc/sys/vm/drop_caches'
=====
mpirun -allow-run-as-root -np 16 -H 10.61.218.152:8,10.61.218.154:8
-bind-to none -map-by slot -x NCCL_DEBUG=INFO -x LD_LIBRARY_PATH -x PATH
-mca pml ob1 -mca btl ^openib -mca btl_tcp_if_include enp1s0f0 -x
NCCL_IB_HCA=mlx5 -x NCCL_NET_GDR_READ=1 -x NCCL_IB_SL=3 -x
NCCL_IB_GID_INDEX=3 -x
NCCL_SOCKET_IFNAME=enp5s0.3091,enp12s0.3092,enp132s0.3093,enp139s0.3094
-x NCCL_IB_CUDA_SUPPORT=1 -mca orte_base_help_aggregate 0 -mca
plm_rsh_agent ssh -mca plm_rsh_args "-p 22122" python
/netapp/tensorflow/benchmarks_190205/scripts/tf_cnn_benchmarks/tf_cnn_be
nchmarks.py --model=resnet50 --batch_size=256 --device=gpu
--force_gpu_compatible=True --num_intra_threads=1 --num_inter_threads=48
--variable_update=horovod --batch_group_size=20 --num_batches=500
--nodistortions --num_gpus=1 --data_format=NCHW --use_fp16=True
--use_tf_layers=False --data_name=imagenet --use_datasets=True
--data_dir=/mnt/mount_0/dataset/imagenet
--datasets_parallel_interleave_cycle_length=10
--datasets_sloppy_parallel_interleave=False --num_mounts=2
--mount_prefix=/mnt/mount_%d --datasets_prefetch_buffer_size=2000 --
datasets_use_prefetch=True --datasets_num_private_threads=4
--horovod_device=gpu >
/tmp/20190814_161609_tensorflow_horovod_rdma_resnet50_gpu_16_256_b500_im
agenet_nodistort_fp16_r10_m2_nockpt.txt 2>&1

```

6. Delete the worker deployment when you no longer need it. The following example commands show the deletion of the worker deployment object that was created in step 1.

When you delete the worker deployment object, Kubernetes automatically deletes any associated worker pods.

```

$ kubectl get deployments
NAME                                DESIRED   CURRENT   UP-TO-DATE
AVAILABLE   AGE
netapp-tensorflow-multi-imagenet-worker   1         1         1
1           43m

$ kubectl get pods
NAME                                         READY
STATUS      RESTARTS   AGE
netapp-tensorflow-multi-imagenet-master-ppwwj   0/1
Completed   0          17m
netapp-tensorflow-multi-imagenet-worker-654fc7f486-v6725   1/1
Running     0          43m

$ kubectl delete deployment netapp-tensorflow-multi-imagenet-worker
deployment.extensions "netapp-tensorflow-multi-imagenet-worker" deleted
$ kubectl get deployments
No resources found.

$ kubectl get pods
NAME                                READY   STATUS
RESTARTS   AGE
netapp-tensorflow-multi-imagenet-master-ppwwj   0/1     Completed   0
18m

```

7. **Optional:** Clean up the master job artifacts. The following example commands show the deletion of the master job object that was created in step 3.

When you delete the master job object, Kubernetes automatically deletes any associated master pods.

```

$ kubectl get jobs
NAME                                COMPLETIONS   DURATION   AGE
netapp-tensorflow-multi-imagenet-master   1/1          5m50s    19m
$ kubectl get pods
NAME                                READY   STATUS
RESTARTS   AGE
netapp-tensorflow-multi-imagenet-master-ppwwj   0/1     Completed   0
19m

$ kubectl delete job netapp-tensorflow-multi-imagenet-master
job.batch "netapp-tensorflow-multi-imagenet-master" deleted
$ kubectl get jobs
No resources found.

$ kubectl get pods
No resources found.

```

[Next: Performance Testing.](#)

## Performance Testing

We performed a simple performance comparison as part of the creation of this solution. We executed several standard NetApp AI benchmarking jobs by using Kubernetes, and we compared the benchmark results with executions that were performed by using a simple Docker run command. We did not see any noticeable differences in performance. Therefore, we concluded that the use of Kubernetes to orchestrate containerized AI training jobs does not adversely affect performance. See the following table for the results of our performance comparison.

Benchmark	Dataset	Docker Run (images/sec)	Kubernetes (images/sec)
Single-node TensorFlow	Synthetic data	6,667.2475	6,661.93125
Single-node TensorFlow	ImageNet	6,570.2025	6,530.59125
Synchronous distributed two-node TensorFlow	Synthetic data	13,213.70625	13,218.288125
Synchronous distributed two-node TensorFlow	ImageNet	12,941.69125	12,881.33875

[Next: Conclusion.](#)

## Conclusion

Companies and organizations of all sizes and across all industries are turning to artificial intelligence (AI), machine learning (ML), and deep learning (DL) to solve real-world problems, deliver innovative products and services, and to get an edge in an increasingly competitive marketplace. As organizations increase their use of AI, ML, and DL, they face many challenges, including workload scalability and data availability. These challenges can be addressed through the use of the NetApp AI Control Plane solution.

This solution enables you to rapidly clone a data namespace. Additionally, it allows you to define and implement AI, ML, and DL training workflows that incorporate the near-instant creation of data and model baselines for traceability and versioning. With this solution, you can trace every single model training run back to the exact dataset(s) that the model was trained and/or validated with. Lastly, this solution enables you to swiftly provision Jupyter Notebook workspaces with access to massive datasets.

Because this solution is targeted towards data scientists and data engineers, minimal NetApp or NetApp ONTAP expertise is required. With this solution, data management functions can be executed using simple and familiar tools and interfaces. Furthermore, this solution utilizes fully open-source and free components. Therefore, if you already have NetApp storage in your environment, you can implement this solution today. If you want to test drive this solution but you do not have already have NetApp storage, visit [cloud.netapp.com](http://cloud.netapp.com), and you can be up and running with a cloud-based NetApp storage solution in no time.

## MLRun Pipeline with Iguazio

### TR-4834: NetApp and Iguazio for MLRun Pipeline

Rick Huang, David Arnette, NetApp  
Marcelo Litovsky, Iguazio

This document covers the details of the MLRun pipeline using NetApp ONTAP AI, NetApp AI Control Plane,

NetApp Cloud Volumes software, and the Iguazio Data Science Platform. We used Nuclio serverless function, Kubernetes Persistent Volumes, NetApp Cloud Volumes, NetApp Snapshot copies, Grafana dashboard, and other services on the Iguazio platform to build an end-to-end data pipeline for the simulation of network failure detection. We integrated Iguazio and NetApp technologies to enable fast model deployment, data replication, and production monitoring capabilities on premises as well as in the cloud.

The work of a data scientist should be focused on the training and tuning of machine learning (ML) and artificial intelligence (AI) models. However, according to research by Google, data scientists spend ~80% of their time figuring out how to make their models work with enterprise applications and run at scale, as shown in the following image depicting model development in the AI/ML workflow.



To manage end-to-end AI/ML projects, a wider understanding of enterprise components is needed. Although DevOps have taken over the definition, integration, and deployment of these types of components, machine learning operations target a similar flow that includes AI/ML projects. To get an idea of what an end-to-end AI/ML pipeline touches in the enterprise, see the following list of required components:

- Storage
- Networking
- Databases
- File systems
- Containers
- Continuous integration and continuous deployment (CI/CD) pipeline
- Development integrated development environment (IDE)
- Security
- Data access policies
- Hardware

- Cloud
- Virtualization
- Data science toolsets and libraries

In this paper, we demonstrate how the partnership between NetApp and Iguazio drastically simplifies the development of an end-to-end AI/ML pipeline. This simplification accelerates the time to market for all of your AI/ML applications.

### Target Audience

The world of data science touches multiple disciplines in information technology and business.

- The data scientist needs the flexibility to use their tools and libraries of choice.
- The data engineer needs to know how the data flows and where it resides.
- A DevOps engineer needs the tools to integrate new AI/ML applications into their CI/CD pipelines.
- Business users want to have access to AI/ML applications. We describe how NetApp and Iguazio help each of these roles bring value to business with our platforms.

### Solution Overview

This solution follows the lifecycle of an AI/ML application. We start with the work of data scientists to define the different steps needed to prep data and train and deploy models. We follow with the work needed to create a full pipeline with the ability to track artifacts, experiment with execution, and deploy to Kubeflow. To complete the full cycle, we integrate the pipeline with NetApp Cloud Volumes to enable data versioning, as seen in the following image.



[Next: Technology Overview](#)

## Technology Overview

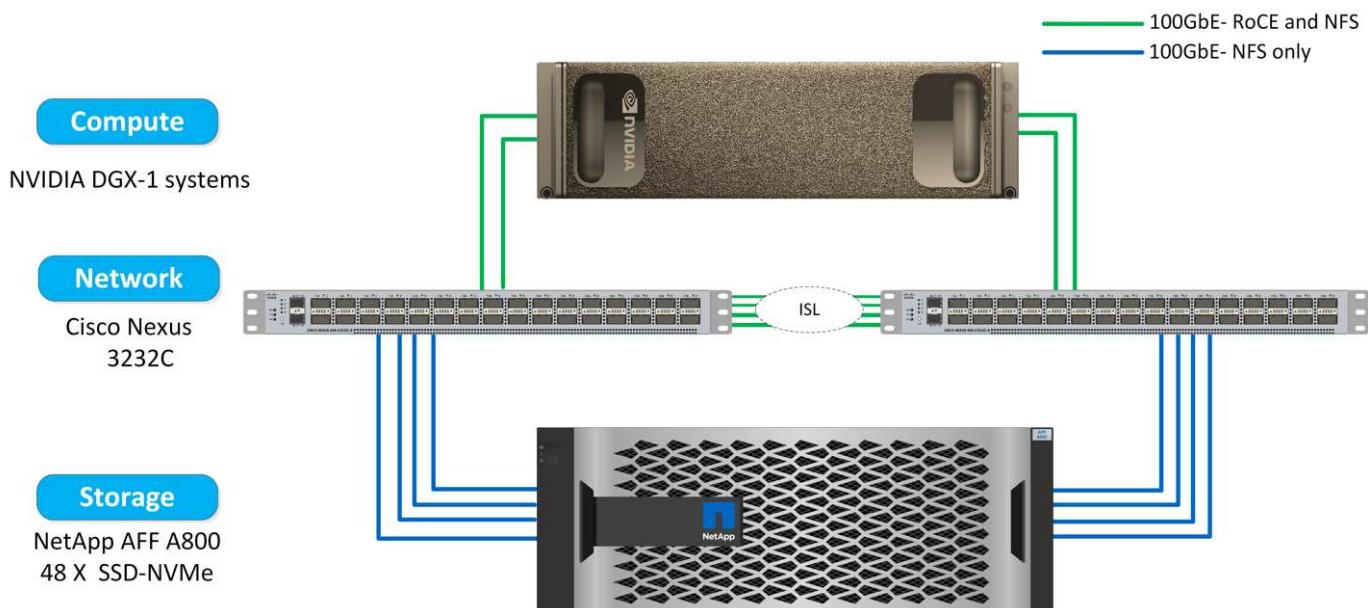
### NetApp Overview

NetApp is the data authority for the hybrid cloud. NetApp provides 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, NetApp empowers global organizations to unleash the full potential of their data to expand customer touch points, foster greater innovation, and optimize their operations.

### NetApp ONTAP AI

NetApp ONTAP AI, powered by NVIDIA DGX systems and NetApp cloud-connected all-flash storage, streamlines the flow of data reliably and speeds up analytics, training, and inference with your data fabric that spans from edge to core to cloud. It gives IT organizations an architecture that provides the following benefits:

- Eliminates design complexities
  - Allows independent scaling of compute and storage
  - Enables customers to start small and scale seamlessly
  - Offers a range of storage options for various performance and cost points
- NetApp ONTAP AI offers converged infrastructure stacks incorporating NVIDIA DGX-1, a petaflop-scale AI system, and NVIDIA Mellanox high-performance Ethernet switches to unify AI workloads, simplify deployment, and accelerate ROI. We leveraged ONTAP AI with one DGX-1 and NetApp AFF A800 storage system for this technical report. The following image shows the topology of ONTAP AI with the DGX-1 system used in this validation.



### NetApp AI Control Plane

The NetApp AI Control Plane enables you to unleash AI and ML with a solution that offers extreme scalability, streamlined deployment, and nonstop data availability. The AI Control Plane solution integrates Kubernetes and Kubeflow with a data fabric enabled by NetApp. Kubernetes, the industry-standard container orchestration platform for cloud-native deployments, enables workload scalability and portability. Kubeflow is an open-source machine-learning platform that simplifies management and deployment, enabling developers to do more data science in less time. A data fabric enabled by NetApp offers uncompromising data availability and portability to make sure that your data is accessible across the pipeline, from edge to core to cloud. This technical report uses the NetApp AI Control Plane in an MLRun pipeline. The following image shows Kubernetes cluster

management page where you can have different endpoints for each cluster. We connected NFS Persistent Volumes to the Kubernetes cluster, and the following images show an Persistent Volume connected to the cluster, where [NetApp Trident](#) offers persistent storage support and data management capabilities.

4 Kubernetes Clusters

kubernetes

Cluster Endpoint: https://3.20.111.39:6443 Cluster Version: v1.15.5 Trident Version: 19.07.1 Working Environments: 0

kubernetes

Cluster Endpoint: https://172.31.14.31:6443 Cluster Version: v1.15.5 Trident Version: 19.07.1 Working Environments: 1

## Persistent Volumes for Kubernetes

Connected with Kubernetes Cluster

Cloud Volumes ONTAP is connected to 1 Kubernetes cluster. View Cluster ⓘ

You can connect another Kubernetes cluster to this Cloud Volumes ONTAP system. If the Kubernetes cluster is in a different network than Cloud Volumes ONTAP, specify a custom export policy to provide access to clients.

Kubernetes Cluster

Select Kubernetes Cluster: kubernetes

Custom Export Policy (Optional)

Custom Export Policy: 172.31.0.0/16

Set as default storage class

NFS  iSCSI

Connect Cancel

## Volumes

4 Volumes | 300 GB Allocated | 1.43 GB Total Used



## Iguazio Overview

The Iguazio Data Science Platform is a fully integrated and secure data-science platform as a service (PaaS) that simplifies development, accelerates performance, facilitates collaboration, and addresses operational challenges. This platform incorporates the following components, and the Iguazio Data Science Platform is presented in the following image:

- A data-science workbench that includes Jupyter Notebooks, integrated analytics engines, and Python packages
- Model management with experiments tracking and automated pipeline capabilities
- Managed data and ML services over a scalable Kubernetes cluster
- Nuclio, a real-time serverless functions framework
- An extremely fast and secure data layer that supports SQL, NoSQL, time-series databases, files (simple objects), and streaming
- Integration with third-party data sources such as NetApp, Amazon S3, HDFS, SQL databases, and streaming or messaging protocols
- Real-time dashboards based on Grafana



[Next: Software and Hardware Requirements](#)

## Software and Hardware Requirements

### Network Configuration

The following is the network configuration requirement for setting up in the cloud:

- The Iguazio cluster and NetApp Cloud Volumes must be in the same virtual private cloud.
- The cloud manager must have access to port 6443 on the Iguazio app nodes.
- We used Amazon Web Services in this technical report. However, users have the option of deploying the solution in any Cloud provider. For on-premises testing in ONTAP AI with NVIDIA DGX-1, we used the Iguazio hosted DNS service for convenience.

Clients must be able to access dynamically created DNS domains. Customers can use their own DNS if desired.

### Hardware Requirements

You can install Iguazio on-premises in your own cluster. We have verified the solution in NetApp ONTAP AI with an NVIDIA DGX-1 system. The following table lists the hardware used to test this solution.

Hardware	Quantity
DGX-1 systems	1
NetApp AFF A800 system	1 high-availability (HA) pair, includes 2 controllers and 48 NVMe SSDs (3.8TB or above)
Cisco Nexus 3232C network switches	2

The following table lists the software components required for on-premise testing:

Software	Version or Other Information
NetApp ONTAP data management software	9.7
Cisco NX-OS switch firmware	7.0(3)I6(1)
NVIDIA DGX OS	4.4 - Ubuntu 18.04 LTS
Docker container platform	19.03.5
Container version	20.01-tf1-py2
Machine learning framework	TensorFlow 1.15.0
Iguazio	Version 2.8+
ESX Server	6.5

This solution was fully tested with Iguazio version 2.5 and NetApp Cloud Volumes ONTAP for AWS. The Iguazio cluster and NetApp software are both running on AWS.

Software	Version or Type
Iguazio	Version 2.8+
App node	M5.4xlarge
Data node	I3.4xlarge

[Next: Network Device Failure Prediction Use Case Summary](#)

## Network Device Failure Prediction Use Case Summary

This use case is based on an Iguazio customer in the telecommunications space in Asia. With 100K enterprise customers and 125k network outage events per year, there was a critical need to predict and take proactive action to prevent network failures from affecting customers. This solution provided them with the following benefits:

- Predictive analytics for network failures
- Integration with a ticketing system
- Taking proactive action to prevent network failuresAs a result of this implementation of Iguazio, 60% of failures were proactively prevented.

[Next: Setup Overview](#)

## Setup Overview

### Iguazio Installation

Iguazio can be installed on-premises or on a cloud provider. Provisioning can be done as a service and managed by Iguazio or by the customer. In both cases, Iguazio provides a deployment application (Provazio) to deploy and manage clusters.

For on-premises installation, please refer to [NVA-1121](#) for compute, network, and storage setup. On-premises deployment of Iguazio is provided by Iguazio without additional cost to the customer. See [this page](#) for DNS and SMTP server configurations. The Provazio installation page is shown as follows.

Installation Scenario General Clusters Cloud

- Bare metal / virtual machines  
Installs the system on bare-metal or virtual-machine instances, pre-provisioned with prerequ...

- AWS  
Creates applicable compute/networking resources in AWS and installs the system on the in...

- Azure  
Creates applicable compute/networking resources in Azure and installs the system on the i...

- AWS (pre-provisioned)  
Installs the system on Amazon Web Services instances, manually provisioned beforehand

- Azure (pre-provisioned)  
Installs the system on Microsoft Azure instances, manually provisioned beforehand

- Advanced  
Show advanced options in the next steps

[BACK](#)[NEXT](#)

## Next: Configuring Kubernetes Cluster

### Configuring Kubernetes Cluster

This section is divided into two parts for cloud and on-premises deployment respectively.

#### Cloud Deployment Kubernetes Configuration

Through NetApp Cloud Manager, you can define the connection to the Iguazio Kubernetes cluster. Trident requires access to multiple resources in the cluster to make the volume available.

1. To enable access, obtain the Kubernetes config file from one the Iguazio nodes. The file is located under `/home/Iguazio/.kube/config`. Download this file to your desktop.
2. Go to Discover Cluster to configure.

3. Upload the Kubernetes config file. See the following image.

## Upload Kubernetes Configuration File

Upload the Kubernetes configuration file (kubeconfig) so Cloud Manager can install Trident on the Kubernetes cluster.

Connecting Cloud Volumes ONTAP with a Kubernetes cluster enables users to request and manage persistent volumes using native Kubernetes interfaces and constructs. Users can take advantage of ONTAP's advanced data management features without having to know anything about it. Storage provisioning is enabled by using NetApp Trident.

Learn more about [Trident for Kubernetes](#).

[Upload File](#)

4. Deploy Trident and associate a volume with the cluster. See the following image on defining and assigning a Persistent Volume to the Iguazio cluster. This process creates a Persistent Volume (PV) in Iguazio's Kubernetes cluster. Before you can use it, you must define a Persistent Volume Claim (PVC).

## Persistent Volumes for Kubernetes

### Connected with Kubernetes Cluster

Cloud Volumes ONTAP is connected to 1 Kubernetes cluster. View Cluster [\(1\)](#)

You can connect another Kubernetes cluster to this Cloud Volumes ONTAP system. If the Kubernetes cluster is in a different network than Cloud Volumes ONTAP, specify a custom export policy to provide access to clients.

Kubernetes Cluster	Custom Export Policy (Optional) <a href="#">(1)</a>
Select Kubernetes Cluster	Custom Export Policy
<input type="text" value="kubernetes"/>	<input type="text" value="172.31.0.0/16"/>
<input checked="" type="checkbox"/> Set as default storage class	
<input checked="" type="radio"/> NFS <input type="radio"/> iSCSI	
<a href="#">Connect</a> <a href="#">Cancel</a>	

### On-Premises Deployment Kubernetes Configuration

For on-premises installation of NetApp Trident, see [TR-4798](#) for details. After configuring your Kubernetes cluster and installing NetApp Trident, you can connect Trident to the Iguazio cluster to enable NetApp data management capabilities, such as taking Snapshot copies of your data and model.

[Next: Define Persistent Volume Claim](#)

#### Define Persistent Volume Claim

1. Save the following YAML to a file to create a PVC of type Basic.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 100Gi
  storageClassName: netapp-file
```

## 2. Apply the YAML file to your Iguazio Kubernetes cluster.

```
Kubectl -n default-tenant apply -f <your yaml file>
```

### Attach NetApp Volume to the Jupyter Notebook

Iguazio offers several managed services to provide data scientists with a full end-to-end stack for development and deployment of AI/ML applications. You can read more about these components at the [Iguazio Overview of Application Services and Tools](#).

One of the managed services is Jupyter Notebook. Each developer gets its own deployment of a notebook container with the resources they need for development. To give them access to the NetApp Cloud Volume, you can assign the volume to their container and resource allocation, running user, and environment variable settings for Persistent Volume Claims is presented in the following image.

For an on-premises configuration, you can refer to [TR-4798](#) on the Trident setup to enable NetApp ONTAP data management capabilities, such as taking Snapshot copies of your data or model for versioning control. Add the following line in your Trident back- end config file to make Snapshot directories visible:

```
{  
  ...  
  "defaults": {  
    "snapshotDir": "true"  
  }  
}
```

You must create a Trident back- end config file in JSON format, and then run the following [Trident command](#) to reference it:

```
tridentctl create backend -f <backend-file>
```

The screenshot shows the Iguazio UI for configuring a pod. Under the 'Resources' section, there are fields for 'Memory' and 'CPU'. Each has 'Request' and 'Limit' fields with dropdown menus for units (GB, milliCPU). Below these are 'Inactivity window' and 'Running User' fields. The 'Inactivity window' has a slider set to 10m. The 'Running User' field contains 'admin'.

The screenshot shows the Iguazio UI for configuring a pod. Under the 'Environment Variables' section, there is a button to 'Create a new environment variable'. Under 'Persistent Volume Claims (PVCs)', there is a table with one row: 'Name' is 'basic' and 'Mount Path' is '/netapp'. There is also a 'Add PVC' button.

[Next: Deploying the Application](#)

## Deploying the Application

The following sections describe how to install and deploy the application.

Next: [Get Code from GitHub](#).

### Get Code from GitHub

Now that the NetApp Cloud Volume or NetApp Trident volume is available to the Iguazio cluster and the developer environment, you can start reviewing the application.

Users have their own workspace (directory). On every notebook, the path to the user directory is `/User`. The Iguazio platform manages the directory. If you follow the instructions above, the NetApp Cloud volume is available in the `/netapp` directory.

Get the code from GitHub using a Jupyter terminal.



At the Jupyter terminal prompt, clone the project.

```
cd /User  
git clone .
```

You should now see the `netops-` `netapp` folder on the file tree in Jupyter workspace.

Next: [Configure Working Environment](#)

### Configure Working Environment

Copy the Notebook `set_env-Example.ipynb` as `set_env.ipynb`. Open and edit `set_env.ipynb`. This notebook sets variables for credentials, file locations, and

execution drivers.

If you follow the instructions above, the following steps are the only changes to make:

1. Obtain this value from the Iguazio services dashboard: docker\_registry

Example: docker-registry.default-tenant.app.clusterq.iguaziodev.com:80

2. Change admin to your Iguazio username:

```
IGZ_CONTAINER_PATH = '/users/admin'
```

The following are the ONTAP system connection details. Include the volume name that was generated when Trident was installed. The following setting is for an on-premises ONTAP cluster:

```
ontapClusterMgmtHostname = '0.0.0.0'  
ontapClusterAdminUsername = 'USER'  
ontapClusterAdminPassword = 'PASSWORD'  
sourceVolumeName = 'SOURCE VOLUME'
```

The following setting is for Cloud Volumes ONTAP:

```
MANAGER=ontapClusterMgmtHostname  
svm='svm'  
email='email'  
password=ontapClusterAdminPassword  
weid="weid"  
volume=sourceVolumeName
```

## Create Base Docker Images

Everything you need to build an ML pipeline is included in the Iguazio platform. The developer can define the specifications of the Docker images required to run the pipeline and execute the image creation from Jupyter Notebook. Open the notebook `create- images.ipynb` and Run All Cells.

This notebook creates two images that we use in the pipeline.

- iguazio/netapp. Used to handle ML tasks.

## Create image for training pipeline

```
[4]: fn.build_config(image=docker_registry+'/iguazio/netapp', commands=['pip install '\  
    'v3io_frames fsspec>=0.3.3 PyYAML==5.1.2 pyarrow==0.15.1 pandas==0.25.3 matplotlib seaborn yellowb  
fn.deploy()
```

- netapp/pipeline. Contains utilities to handle NetApp Snapshot copies.

## Create image for Ontap utilities

```
[@]: fn.build_config(imagedocker_registry + '/netapp/pipeline:latest', commands=['apt -y update', 'pip install vlio_framess netapp_ontap']
fn.deploy()
```

## Review Individual Jupyter Notebooks

The following table lists the libraries and frameworks we used to build this task. All these components have been fully integrated with Iguazio's role- based access and security controls.

Libraries/Framework	Description
MLRun	An managed by Iguazio to enable the assembly, execution, and monitoring of an ML/AI pipeline.
Nuclio	A serverless functions framework integrated with Iguazio. Also available as an open-source project managed by Iguazio.
Kubeflow	A Kubernetes-based framework to deploy the pipeline. This is also an open-source project to which Iguazio contributes. It is integrated with Iguazio for added security and integration with the rest of the infrastructure.
Docker	A Docker registry run as a service in the Iguazio platform. You can also change this to connect to your registry.
NetApp Cloud Volumes	Cloud Volumes running on AWS give us access to large amounts of data and the ability to take Snapshot copies to version the datasets used for training.
Trident	Trident is an open-source project managed by NetApp. It facilitates the integration with storage and compute resources in Kubernetes.

We used several notebooks to construct the ML pipeline. Each notebook can be tested individually before being brought together in the pipeline. We cover each notebook individually following the deployment flow of this demonstration application.

The desired result is a pipeline that trains a model based on a Snapshot copy of the data and deploys the model for inference. A block diagram of a completed MLRun pipeline is shown in the following image.



## Deploy Data Generation Function

This section describes how we used Nuclio serverless functions to generate network device data. The use case is adapted from an Iguazio client that deployed the pipeline and used Iguazio services to monitor and predict network device failures.

We simulated data coming from network devices. Executing the Jupyter notebook `data-generator.ipynb` creates a serverless function that runs every 10 minutes and generates a Parquet file with new data. To deploy the function, run all the cells in this notebook. See the [Nuclio website](#) to review any unfamiliar components in this notebook.

A cell with the following comment is ignored when generating the function. Every cell in the notebook is assumed to be part of the function. Import the Nuclio module to enable `%nuclio` magic.

```
# nuclio: ignore
import nuclio
```

In the spec for the function, we defined the environment in which the function executes, how it is triggered, and the resources it consumes.

```
spec = nuclio.ConfigSpec(config={"spec.triggers.inference.kind": "cron",
"spec.triggers.inference.attributes.interval" : "10m",
"spec.readinessTimeoutSeconds" : 60,
"spec.minReplicas" : 1},.....
```

The `init_context` function is invoked by the Nuclio framework upon initialization of the function.

```
def init_context(context):
    ...
```

Any code not in a function is invoked when the function initializes. When you invoke it, a handler function is executed. You can change the name of the handler and specify it in the function spec.

```
def handler(context, event):
    ...
```

You can test the function from the notebook prior to deployment.

```
%time
# nuclio: ignore
init_context(context)
event = nuclio.Event(body='')
output = handler(context, event)
output
```

The function can be deployed from the notebook or it can be deployed from a CI/CD pipeline (adapting this code).

```
addr = nuclio.deploy_file(name='generator', project='netops', spec=spec,
tag='v1.1')
```

## Pipeline Notebooks

These notebooks are not meant to be executed individually for this setup. This is just a review of each notebook. We invoked them as part of the pipeline. To execute them individually, review the MLRun documentation to execute them as Kubernetes jobs.

### **snap\_cv.ipynb**

This notebook handles the Cloud Volume Snapshot copies at the beginning of the pipeline. It passes the name of the volume to the pipeline context. This notebook invokes a shell script to handle the Snapshot copy. While running in the pipeline, the execution context contains variables to help locate all files needed for execution.

While writing this code, the developer does not have to worry about the file location in the container that executes it. As described later, this application is deployed with all its dependencies, and it is the definition of the pipeline parameters that provides the execution context.

```
command = os.path.join(context.get_param('APP_DIR'), "snap_cv.sh")
```

The created Snapshot copy location is placed in the MLRun context to be consumed by steps in the pipeline.

```
context.log_result('snapVolumeDetails', snap_path)
```

The next three notebooks are run in parallel.

### **data-prep.ipynb**

Raw metrics must be turned into features to enable model training. This notebook reads the raw metrics from the Snapshot directory and writes the features for model training to the NetApp volume.

When running in the context of the pipeline, the input DATA\_DIR contains the Snapshot copy location.

```
metrics_table = os.path.join(str(mlruncontext.get_input('DATA_DIR',
os.getenv('DATA_DIR','/netpp'))),
                           mlruncontext.get_param('metrics_table',
os.getenv('metrics_table','netops_metrics_parquet')))
```

### **describe.ipynb**

To visualize the incoming metrics, we deploy a pipeline step that provides plots and graphs that are available through the Kubeflow and MLRun UIs. Each execution has its own version of this visualization tool.

```
ax.set_title("features correlation")
plt.savefig(os.path.join(base_path, "plots/corr.png"))
context.log_artifact(PlotArtifact("correlation", body=plt.gcf()),
local_path="plots/corr.html")
```

### **deploy-feature-function.ipynb**

We continuously monitor the metrics looking for anomalies. This notebook creates a serverless function that generates the features need to run prediction on incoming metrics. This notebook invokes the creation of the function. The function code is in the notebook data-prep.ipynb. Notice that we use the same notebook as a step in the pipeline for this purpose.

### **training.ipynb**

After we create the features, we trigger the model training. The output of this step is the model to be used for inferencing. We also collect statistics to keep track of each execution (experiment).

For example, the following command enters the accuracy score into the context for that experiment. This value is visible in Kubeflow and MLRun.

```
context.log_result('accuracy', score)
```

## deploy-inference-function.ipynb

The last step in the pipeline is to deploy the model as a serverless function for continuous inferencing. This notebook invokes the creation of the serverless function defined in `nuclio-inference-function.ipynb`.

## Review and Build Pipeline

The combination of running all the notebooks in a pipeline enables the continuous run of experiments to reassess the accuracy of the model against new metrics. First, open the `pipeline.ipynb` notebook. We take you through details that show how NetApp and Iguazio simplify the deployment of this ML pipeline.

We use MLRun to provide context and handle resource allocation to each step of the pipeline. The MLRun API service runs in the Iguazio platform and is the point of interaction with Kubernetes resources. Each developer cannot directly request resources; the API handles the requests and enables access controls.

```
# MLRun API connection definition
mlconf.dbpath = 'http://mlrun-api:8080'
```

The pipeline can work with NetApp Cloud Volumes and on-premises volumes. We built this demonstration to use Cloud Volumes, but you can see in the code the option to run on-premises.

```

# Initialize the NetApp snap function once for all functions in a notebook
if [ NETAPP_CLOUD_VOLUME ]:
    snapfn =
code_to_function('snap',project='NetApp',kind='job',filename="snap_cv.ipynb").apply(mount_v3io())
    snap_params = {
        "metrics_table" : metrics_table,
        "NETAPP_MOUNT_PATH" : NETAPP_MOUNT_PATH,
        'MANAGER' : MANAGER,
        'svm' : svm,
        'email': email,
        'password': password ,
        'weid': weid,
        'volume': volume,
        "APP_DIR" : APP_DIR
    }
else:
    snapfn =
code_to_function('snap',project='NetApp',kind='job',filename="snapshot.ipynb").apply(mount_v3io())
...
snapfn.spec.image = docker_registry + '/netapp/pipeline:latest'
snapfn.spec.volume_mounts =
[snapfn.spec.volume_mounts[0],netapp_volume_mounts]
    snapfn.spec.volumes = [ snapfn.spec.volumes[0],netapp_volumes]

```

The first action needed to turn a Jupyter notebook into a Kubeflow step is to turn the code into a function. A function has all the specifications required to run that notebook. As you scroll down the notebook, you can see that we define a function for every step in the pipeline.

Part of the Notebook	Description
<code_to_function> (part of the MLRun module)	Name of the function: Project name. used to organize all project artifacts. This is visible in the MLRun UI. Kind. In this case, a Kubernetes job. This could be Dask, mpi, sparkk8s, and more. See the MLRun documentation for more details. File. The name of the notebook. This can also be a location in Git (HTTP).
image	The name of the Docker image we are using for this step. We created this earlier with the create-image.ipynb notebook.
volume_mounts & volumes	Details to mount the NetApp Cloud Volume at run time.

We also define parameters for the steps.

```

params={    "FEATURES_TABLE":FEATURES_TABLE,
            "SAVE_TO" : SAVE_TO,
            "metrics_table" : metrics_table,
            'FROM_TSDB': 0,
            'PREDICTIONS_TABLE': PREDICTIONS_TABLE,
            'TRAIN_ON_LAST': '1d',
            'TRAIN_SIZE':0.7,
            'NUMBER_OF_SHARDS' : 4,
            'MODEL_FILENAME' : 'netops.v3.model.pickle',
            'APP_DIR' : APP_DIR,
            'FUNCTION_NAME' : 'netops-inference',
            'PROJECT_NAME' : 'netops',
            'NETAPP_SIM' : NETAPP_SIM,
            'NETAPP_MOUNT_PATH': NETAPP_MOUNT_PATH,
            'NETAPP_PVC CLAIM' : NETAPP_PVC CLAIM,
            'IGZ_CONTAINER_PATH' : IGZ_CONTAINER_PATH,
            'IGZ_MOUNT_PATH' : IGZ_MOUNT_PATH
        }

```

After you have the function definition for all steps, you can construct the pipeline. We use the `kfp` module to make this definition. The difference between using MLRun and building on your own is the simplification and shortening of the coding.

The functions we defined are turned into step components using the `as_step` function of MLRun.

## Snapshot Step Definition

Initiate a Snapshot function, output, and mount v3io as source:

```

snap = snapfn.as_step(NewTask(handler='handler',params=snap_params),
name='NetApp_Cloud_Volume_Snapshot',outputs=['snapVolumeDetails','training
_parquet_file']).apply(mount_v3io())

```

Parameters	Details
NewTask	NewTask is the definition of the function run.
(MLRun module)	Handler. Name of the Python function to invoke. We used the name <code>handler</code> in the notebook, but it is not required. params. The parameters we passed to the execution. Inside our code, we use <code>context.get_param('PARAMETER')</code> to get the values.

Parameters	Details
as_step	Name. Name of the Kubeflow pipeline step. outputs. These are the values that the step adds to the dictionary on completion. Take a look at the snap_cv.ipynb notebook. mount_v3io(). This configures the step to mount /User for the user executing the pipeline.

```
prep = data_prep.as_step(name='data-prep',
handler='handler',params=params,
                     inputs = {'DATA_DIR':
snap.outputs['snapVolumeDetails']} ,
out_path=artifacts_path).apply(mount_v3io()).after(snap)
```

Parameters	Details
inputs	You can pass to a step the outputs of a previous step. In this case, snap.outputs['snapVolumeDetails'] is the name of the Snapshot copy we created on the snap step.
out_path	A location to place artifacts generating using the MLRun module log_artifacts.

You can run `pipeline.ipynb` from top to bottom. You can then go to the Pipelines tab from the Iguazio dashboard to monitor progress as seen in the Iguazio dashboard Pipelines tab.



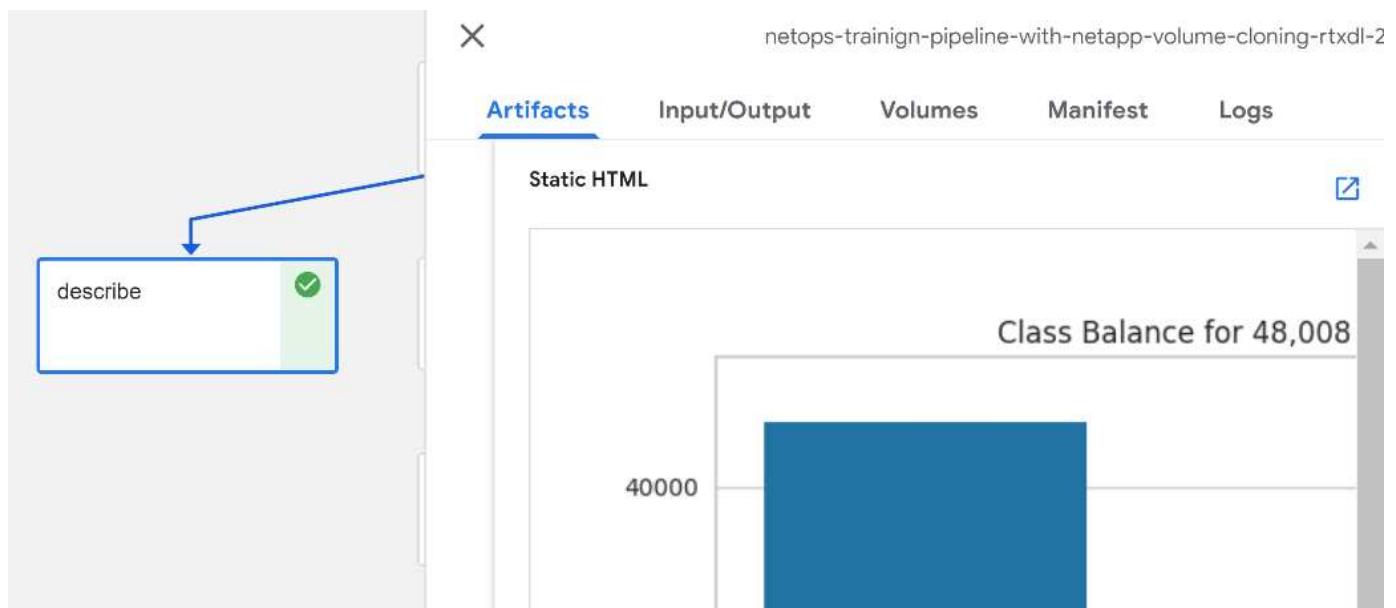
Because we logged the accuracy of training step in every run, we have a record of accuracy for each experiment, as seen in the record of training accuracy.

<input type="checkbox"/>	Run name	Status	Duration	Pipeline Version	Recurring ...	Start time	accuracy
<input type="checkbox"/>	xgb_pipeline 2020-03-24 18-51-08...	✓	0:08:43	[View pipeline]	-	3/24/2020, 2:51:09 PM	0.985
<input type="checkbox"/>	xgb_pipeline 2020-03-19 13-31-08...	✓	0:08:14	[View pipeline]	-	3/19/2020, 9:31:19 AM	0.980
<input type="checkbox"/>	xgb_pipeline 2020-03-18 12-56-08...	✓	0:08:11	[View pipeline]	-	3/18/2020, 8:56:08 AM	0.990
<input type="checkbox"/>	xgb_pipeline 2020-03-17 19-49-08...	✓	0:08:03	[View pipeline]	-	3/17/2020, 3:49:31 PM	0.985
<input type="checkbox"/>	xgb_pipeline 2020-03-17 18-34-08...	✓	0:05:54	[View pipeline]	-	3/17/2020, 2:34:56 PM	0.980
<input type="checkbox"/>	xgb_pipeline 2020-03-17 17-34-08...	✓	0:04:48	[View pipeline]	-	3/17/2020, 1:34:16 PM	0.982
<input type="checkbox"/>	xgb_pipeline 2020-03-17 17-01-08...	✓	0:05:25	[View pipeline]	-	3/17/2020, 1:01:58 PM	0.987
<input type="checkbox"/>	xgb_pipeline 2020-03-16 16-47-08...	✓	0:06:08	[View pipeline]	-	3/16/2020, 12:47:19 ...	0.983
<input type="checkbox"/>	xgb_pipeline 2020-03-16 13-57-08...	✓	0:05:18	[View pipeline]	-	3/16/2020, 9:57:03 AM	0.980

If you select the Snapshot step, you can see the name of the Snapshot copy that was used to run this experiment.



The described step has visual artifacts to explore the metrics we used. You can expand to view the full plot as seen in the following image.



The MLRun API database also tracks inputs, outputs, and artifacts for each run organized by project. An example of inputs, outputs, and artifacts for each run can be seen in the following image.

The screenshot shows the MLRun UI interface. At the top, there's a dark header with the MLRun UI logo. Below it, a navigation bar has a 'Projects' tab selected, indicated by a grey background. Three project cards are displayed: 'NetApp', 'default', and 'describe'. Each card has a small icon at the top left, followed by the project name. Below each name are two tabs: 'Jobs' and 'Artifacts'. The 'Jobs' tab is highlighted with a blue background.

For each job, we store additional details.

The screenshot shows a detailed view of a job named 'describe'. On the left, a sidebar lists other jobs: 'deploy-model', 'xgb\_train', 'data-prep', 'describe', 'deploy-features-function', and 'NetApp\_Cloud\_Volume\_Sna'. The main area shows the 'describe' job details. It includes the job name, start time (24 Mar, 14:52:45), and an 'Info' tab. The 'Info' tab contains fields for 'UID' (66ef22187efb4ad89e8da8433c2a460e) and 'Start time' (24 Mar, 14:52:45). Below the 'Info' tab is a 'Parameters' section with 'Completed'. Underneath is a 'Results' section with three buttons: 'class\_label...', 'key: summary', and 'label\_colu...'. The 'key: summary' button is currently selected.

There is more information about MLRun than we can cover in this document. AI artifacts, including the definition of the steps and functions, can be saved to the API database, versioned, and invoked individually or as a full project. Projects can also be saved and pushed to Git for later use. We encourage you to learn more at the [MLRun GitHub site](#).

[Next: Deploy Grafana Dashboard](#)

### Deploy Grafana Dashboard

After everything is deployed, we run inferences on new data. The models predict failure on network device equipment. The results of the prediction are stored in an Iguazio TimeSeries table. You can visualize the results with Grafana in the platform integrated with Iguazio's security and data access policy.

You can deploy the dashboard by importing the provided JSON file into the Grafana interfaces in the cluster.

1. To verify that the Grafana service is running, look under Services.

Services							
Name	Type	Running User	Version	CPU (cores)	Memory	File System	Avg. Latency
docker-registry	Type: Docker Registry	root	2.7.1	96μ		1.67 GB	
framesd	Type: V3ID Frame	root	0.6.10	369μ		795.19 MB	
grafana	Type: Grafana	root	6.6.0	1m		38.39 MB	
jupyter	Type: Jupyter Note	admin	1.0.2	81m		3.27 GB	
log-forwarder	Type: Log Forwarder	root	6.7.2	0		0 bytes	

2. If it is not present, deploy an instance from the Services section:
  - a. Click New Service.
  - b. Select Grafana from the list.
  - c. Accept the defaults.
  - d. Click Next Step.
  - e. Enter your user ID.
  - f. Click Save Service.
  - g. Click Apply Changes at the top.
3. To deploy the dashboard, download the file `NetopsPredictions-Dashboard.json` through the Jupyter interface.



4. Open Grafana from the Services section and import the dashboard.



5. Click Upload \*.json File and select the file that you downloaded earlier (NetopsPredictions-Dashboard.json). The dashboard displays after the upload is completed.



## Deploy Cleanup Function

When you generate a lot of data, it is important to keep things clean and organized. To do so, deploy the cleanup function with the `cleanup.ipynb` notebook.

## Benefits

NetApp and Iguazio speed up and simplify the deployment of AI and ML applications by building in essential frameworks, such as Kubeflow, Apache Spark, and TensorFlow, along with orchestration tools like Docker and Kubernetes. By unifying the end-to-end data pipeline, NetApp and Iguazio reduce the latency and complexity inherent in many advanced computing workloads, effectively bridging the gap between development and operations. Data scientists can run queries on large datasets and securely share data and algorithmic models with authorized users during the training phase. After the containerized models are ready for production, you can easily move them from development environments to operational environments.

[Next: Conclusion](#)

## Conclusion

When building your own AI/ML pipelines, configuring the integration, management, security, and accessibility of the components in an architecture is a challenging task. Giving developers access and control of their environment presents another set of challenges.

The combination of NetApp and Iguazio brings these technologies together as managed services to accelerate technology adoption and improve the time to market for new AI/ML applications.

[Next: Where to Find Additional Information](#)

# Use Cases

## Responsible AI and confidential inferencing - NetApp AI with Protopia Image Transformation

### TR-4928: Responsible AI and confidential inferencing - NetApp AI with Protopia Image Transformation

Sathish Thyagarajan, Michael Oglesby, NetApp  
Byung Hoon Ahn, Jennifer Cwagenberg, Protopia

Visual interpretations have become an integral part of communication with the emergence of image capturing and image processing. Artificial intelligence (AI) in digital image processing brings novel business opportunities, such as in the medical field for cancer and other disease identification, in geospatial visual analytics for studying environmental hazards, in pattern recognition, in video processing for fighting crime, and so on. However, this opportunity also comes with extraordinary responsibilities.

The more decisions organizations put into the hands of AI, the more they accept risks related to data privacy and security and legal, ethical, and regulatory issues. Responsible AI enables a practice that allows companies and government organizations to build trust and governance that is crucial for AI at scale in large enterprises. This document describes an AI inferencing solution validated by NetApp under three different scenarios by using NetApp data management technologies with Protopia data obfuscation software to privatize sensitive data and reduce risks and ethical concerns.

Millions of images are generated every day with various digital devices by both consumers and business entities. The consequent massive explosion of data and computational workload makes businesses turn to cloud computing platforms for scale and efficiency. Meanwhile, privacy concerns over the sensitive information contained in image data arise with transfer to a public cloud. The lack of security and privacy assurances become the main barrier to deployment of image-processing AI systems.

Additionally, there is the [right to erasure](#) by the GDPR, the right of an individual to request that an organization erase all their personal data. There is also the [Privacy Act](#), which establishes a code of fair information practices. Digital images such as photographs can constitute personal data under the GDPR, which governs how data must be collected, processed, and erased. Failure to do so is a failure to comply with GDPR, which might lead to hefty fines for breaching compliances that can be seriously damaging to organizations. Privacy principles are among the backbone of implementing responsible AI that ensure fairness in the machine learning (ML) and deep learning (DL) model predictions and lowers risks associated with violating privacy or regulatory compliance.

This document describes a validated design solution under three different scenarios with and without image obfuscation relevant to preserving privacy and deploying a responsible AI solution:

- **Scenario 1.** On-demand inferencing within Jupyter notebook.
- **Scenario 2.** Batch inferencing on Kubernetes.
- **Scenario 3.** NVIDIA Triton inference server.

For this solution, we use the Face Detection Data Set and Benchmark (FDDB), a dataset of face regions designed for studying the problem of unconstrained face detection, combined with the PyTorch machine learning framework for implementation of FaceBoxes. This dataset contains the annotations for 5171 faces in a set of 2845 images of various resolutions. Furthermore, this technical report presents some of the solution areas and relevant use cases gathered from NetApp customers and field engineers in situations where this solution is applicable.

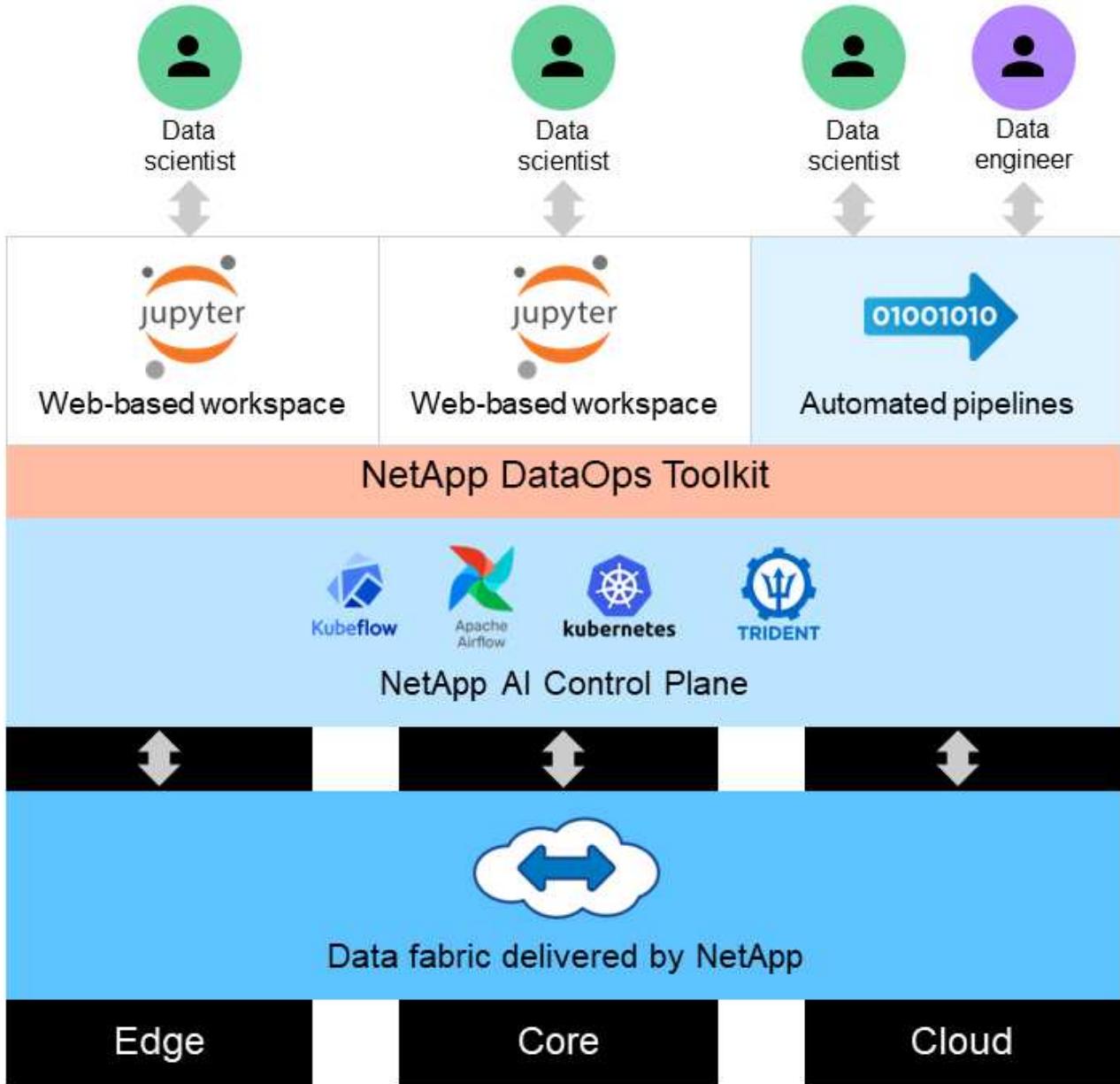
## **Target audience**

This technical report is intended for the following audiences:

- Business leaders and enterprise architects who want to design and deploy responsible AI and address data protection and privacy issues concerning facial image processing in public spaces.
- Data scientists, data engineers, AI/ machine learning (ML) researchers, and developers of AI/ML systems who aim to protect and preserve privacy.
- Enterprise architects who design data obfuscation solutions for AI/ML models and applications that comply with regulatory standards such as GDPR, CCPA, or the Privacy Act of the Department of Defense (DoD) and government organizations.
- Data scientists and AI engineers looking for efficient ways to deploy deep learning (DL) and AI/ML/DL inferencing models that protect sensitive information.
- Edge device managers and edge server administrators responsible for deployment and management of edge inferencing models.

## **Solution architecture**

This solution is designed to handle real-time and batch inferencing AI workloads on large datasets by using the processing power of GPUs alongside traditional CPUs. This validation demonstrates the privacy-preserving inference for ML and optimal data management required for organizations seeking responsible AI deployments. This solution provides an architecture suited for a single or multi-node Kubernetes platform for edge and cloud computing interconnected with NetApp ONTAP AI at the core on-premises, NetApp DataOps Toolkit, and Protopia obfuscation software using Jupyter Lab and CLI interfaces. The following figure shows the logical architecture overview of data fabric powered by NetApp with DataOps Toolkit and Protopia.



Protopia obfuscation software runs seamlessly on top of the NetApp DataOps Toolkit and transforms the data before leaving the storage server.

[Next: Solution areas.](#)

## Solution areas

[Previous: Overview.](#)

Digital image processing comes with a lot of advantages, allowing many organizations to make the most of data associated with visual representations. This NetApp and Protopia solution provides a unique AI inferencing design to protect and privatize AI/ML data across the ML/DL life cycle. It enables customers to retain ownership of sensitive data, use public- or hybrid-cloud deployment models for scale and efficiency by alleviating concerns related to privacy, and deploy AI inferencing at the edge.

## **Environmental intelligence**

There are many ways industries can take advantage of geospatial analytics in the areas of environmental hazards. Governments and the department of public works can derive actionable insights on public health and weather conditions to better advise the public during a pandemic or a natural disaster such as wildfires. For example, you can identify a COVID- positive patient in public spaces, such as airports or hospitals, without compromising the privacy of the affected individual and alert the respective authorities and the public in the vicinity for necessary safety measures.

## **Edge device wearables**

In the military and on battlefields, you can use AI inferencing on the edge as wearable devices to track soldier health, monitor driver behavior, and alert authorities on the safety and associated risks of approaching military vehicles while preserving and protecting the privacy of soldiers. The future of the military is going high-tech with the Internet of Battlefield Things (IoBT) and the Internet of Military Things (IoMT) for wearable combat gear that help soldiers identify enemies and perform better in battle by using rapid edge computing. Protecting and preserving visual data collected from edge devices such as drones and wearable gears is crucial to keep hackers and the enemy at bay.

## **Noncombatant evacuation operations**

Noncombatant evacuation operations (NEOs) are conducted by the DoD to assist in evacuating US citizens and nationals, DoD civilian personnel, and designated persons (host nation (HN) and third-country nationals (TCNs)) whose lives are in danger to an appropriate safe haven. The administrative controls in place use largely manual evacuee screening processes. However, the accuracy, security, and speed of evacuee identification, evacuee tracking, and threat screening could potentially be improved by using highly automated AI/ML tools combined with AI/ML video obfuscation technologies.

## **Cloud migration of AI/ML analytics**

Enterprise customers have traditionally trained and deployed AI/ML models on-premises. For economies of scale and efficiency reasons, these customers are expanding to move AI/ML functions into public, hybrid, or multi-cloud cloud deployments. However, they are bound by what data can be exposed to other infrastructures. NetApp solutions address a full range of cybersecurity threats required for [data protection](#) and security assessment and, when combined with Protopia data transformation, minimize the risks associated with migrating image processing AI/ML workloads to the cloud.

For additional use cases for edge computing and AI inferencing across other industries, see [TR-4886 AI Inferencing at the Edge](#) and the NetApp AI blog, [Intelligence versus privacy](#).

[Next: Technology overview](#).

**Technology overview**

[Previous: Solution areas](#).

## **Protopia**

Protopia AI offers a unobtrusive, software-only solution for confidential inference in the market today. The Protopia solution delivers unparalleled protection for inference services by minimizing exposure of sensitive information. AI is only fed the information in the data record that is truly essential to perform the task at hand and nothing more. Most inference tasks do not use all the information that exists in every data record. Regardless of whether your AI is consuming images, voice, video, or even structured tabular data, Protopia delivers only what the inference service needs. The patented core technology uses mathematically curated noise to stochastically transform the data and garble the information that is not needed by a given ML service.

This solution does not mask the data; rather, it changes the data representation by using curated random noise.

The Protopia solution formulates the problem of changing the representation as a gradient-based perturbation maximization method that still retains the pertinent information in the input feature space with respect to the functionality of the model. This discovery process is run as a fine-tuning pass at the end of training the ML model. After the pass automatically generates a set of probability distributions, a low-overhead data transformation applies noise samples from these distributions to the data, obfuscating it before passing it to the model for inferencing.

### **NetApp ONTAP AI**

The NetApp ONTAP AI reference architecture, powered by DGX A100 systems and NetApp cloud connected storage systems, was developed and verified by NetApp and NVIDIA. It gives IT organizations an architecture that provides the following benefits:

- Eliminates design complexities
- Allows independent scaling of compute and storage
- Enables customers to start small and scale seamlessly
- Offers a range of storage options for various performance and cost points

ONTAP AI tightly integrates DGX A100 systems and NetApp AFF A800 storage systems with state-of-the-art networking. ONTAP AI simplifies AI deployments by eliminating design complexity and guesswork. Customers can start small and grow nondisruptively while intelligently managing data from the edge to the core to the cloud and back.

The following figure shows several variations in the ONTAP AI family of solutions with DGX A100 systems. AFF A800 system performance is verified with up to eight DGX A100 systems. By adding storage controller pairs to the ONTAP cluster, the architecture can scale to multiple racks to support many DGX A100 systems and petabytes of storage capacity with linear performance. This approach offers the flexibility to alter compute-to-storage ratios independently based on the size of the DL models that are used and the required performance metrics.



For additional information about ONTAP AI, see [NVA-1153: NetApp ONTAP AI with NVIDIA DGX A100 Systems and Mellanox Spectrum Ethernet Switches](#).

#### NetApp ONTAP

ONTAP 9.11, the latest generation of storage management software from NetApp, enables businesses to modernize infrastructure and transition to a cloud-ready data center. Leveraging industry-leading data management capabilities, ONTAP enables the management and protection of data with a single set of tools, regardless of where that data resides. You can also move data freely to wherever it is needed: the edge, the core, or the cloud. ONTAP 9.11 includes numerous features that simplify data management, accelerate, and protect critical data, and enable next generation infrastructure capabilities across hybrid cloud architectures.

#### NetApp DataOps Toolkit

NetApp DataOps Toolkit is a Python library that makes it simple for developers, data scientists, DevOps engineers, and data engineers to perform various data management tasks, such as near-instantaneous provisioning of a new data volume or JupyterLab workspace, near-instantaneous cloning of a data volume or JupyterLab workspace, and near-instantaneous taking snapshots of a data volume or JupyterLab workspace for traceability or baselining. This Python library can function as either a command-line utility or a library of functions that you can import into any Python program or Jupyter notebook.

## NVIDIA Triton Inference Server

NVIDIA Triton Inference Server is an open-source inference serving software that helps standardize model deployment and execution to deliver fast and scalable AI in production. Triton Inference Server streamlines AI inferencing by enabling teams to deploy, run, and scale trained AI models from any framework on any GPU- or CPU-based infrastructure. Triton Inference Server supports all major frameworks, such as TensorFlow, NVIDIA TensorRT, PyTorch, MXNet, OpenVINO, and so on. Triton integrates with Kubernetes for orchestration and scaling that you can use in all major public cloud AI and Kubernetes platforms. It's also integrated with many MLOps software solutions.

## PyTorch

[PyTorch](#) is an open-source ML framework. It is an optimized tensor library for deep learning that uses GPUs and CPUs. The PyTorch package contains data structures for multidimensional tensors that provide many utilities for efficient serializing of tensors among other useful utilities. It also has a CUDA counterpart that enables you to run your tensor computations on an NVIDIA GPU with compute capability. In this validation, we use the OpenCV-Python (cv2) library to validate our model while taking advantage of Python's most intuitive computer vision concepts.

## Simplify data management

Data management is crucial to enterprise IT operations and data scientists so that appropriate resources are used for AI applications and training AI/ML datasets. The following additional information about NetApp technologies is out of scope for this validation but might be relevant depending on your deployment.

ONTAP data management software includes the following features to streamline and simplify operations and reduce your total cost of operation:

- Inline data compaction and expanded deduplication. Data compaction reduces wasted space inside storage blocks, and deduplication significantly increases effective capacity. This applies to data stored locally and data tiered to the cloud.
- Minimum, maximum, and adaptive quality of service (AQoS). Granular quality of service (QoS) controls help maintain performance levels for critical applications in highly shared environments.
- NetApp FabricPool. Provides automatic tiering of cold data to public and private cloud storage options, including Amazon Web Services (AWS), Azure, and NetApp StorageGRID storage solution. For more information about FabricPool, see [TR-4598: FabricPool best practices](#).

## Accelerate and protect data

ONTAP delivers superior levels of performance and data protection and extends these capabilities in the following ways:

- Performance and lower latency. ONTAP offers the highest possible throughput at the lowest possible latency.
- Data protection. ONTAP provides built-in data protection capabilities with common management across all platforms.
- NetApp Volume Encryption (NVE). ONTAP offers native volume-level encryption with both onboard and External Key Management support.
- Multitenancy and multifactor authentication. ONTAP enables sharing of infrastructure resources with the highest levels of security.

## Future-proof infrastructure

ONTAP helps meet demanding and constantly changing business needs with the following features:

- Seamless scaling and nondisruptive operations. ONTAP supports the nondisruptive addition of capacity to existing controllers and to scale-out clusters. Customers can upgrade to the latest technologies, such as NVMe and 32Gb FC, without costly data migrations or outages.
- Cloud connection. ONTAP is the most cloud-connected storage management software, with options for software-defined storage (ONTAP Select) and cloud-native instances (NetApp Cloud Volumes Service) in all public clouds.
- Integration with emerging applications. ONTAP offers enterprise-grade data services for next generation platforms and applications, such as autonomous vehicles, smart cities, and Industry 4.0, by using the same infrastructure that supports existing enterprise apps.

### NetApp Astra Control

The NetApp Astra product family offers storage and application-aware data management services for Kubernetes applications on-premises and in the public cloud, powered by NetApp storage and data management technologies. It enables you to easily back up Kubernetes applications, migrate data to a different cluster, and instantly create working application clones. If you need to manage Kubernetes applications running in a public cloud, see the documentation for [Astra Control Service](#). Astra Control Service is a NetApp-managed service that provides application-aware data management of Kubernetes clusters in Google Kubernetes Engine (GKE) and Azure Kubernetes Service (AKS).

### NetApp Astra Trident

Astra [Trident](#) from NetApp is an open-source dynamic storage orchestrator for Docker and Kubernetes that simplifies the creation, management, and consumption of persistent storage. Trident, a Kubernetes-native application, runs directly within a Kubernetes cluster. Trident enables customers to seamlessly deploy DL container images onto NetApp storage and provides an enterprise-grade experience for AI container deployments. Kubernetes users (ML developers, data scientists, and so on) can create, manage, and automate orchestration and cloning to take advantage of advanced data management capabilities powered by NetApp technology.

### NetApp Cloud Sync

[Cloud Sync](#) is a NetApp service for rapid and secure data synchronization. Whether you need to transfer files between on-premises NFS or SMB file shares, NetApp StorageGRID, NetApp ONTAP S3, NetApp Cloud Volumes Service, Azure NetApp Files, Amazon Simple Storage Service (Amazon S3), Amazon Elastic File System (Amazon EFS), Azure Blob, Google Cloud Storage, or IBM Cloud Object Storage, Cloud Sync moves the files where you need them quickly and securely. After your data is transferred, it is fully available for use on both source and target. Cloud Sync continuously synchronizes the data based on your predefined schedule, moving only the deltas, so that time and money spent on data replication is minimized. Cloud Sync is a software-as-a-service (SaaS) tool that is extremely simple to set up and use. Data transfers that are triggered by Cloud Sync are carried out by data brokers. You can deploy Cloud Sync data brokers in AWS, Azure, Google Cloud Platform, or on-premises.

### NetApp Cloud Data Sense

Driven by powerful AI algorithms, [NetApp Cloud Data Sense](#) provides automated controls and data governance across your entire data estate. You can easily pinpoint cost-savings, identify compliance and privacy concerns, and find optimization opportunities. The Cloud Data Sense dashboard gives you the insight to identify duplicate data to eliminate redundancy, map personal, nonpersonal, and sensitive data and turn on alerts for sensitive data and anomalies.

[Next: Test and validation plan.](#)

## Test and validation plan

[Previous: Technology overview.](#)

For this solution design, the following three scenarios were validated:

- An inferencing task, with and without Protopia obfuscation, within a JupyterLab workspace that was orchestrated by using the NetApp DataOps Toolkit for Kubernetes.
- A batch inferencing job, with and without Protopia obfuscation, on Kubernetes with a data volume that was orchestrated by using NetApp DataOps Toolkit for Kubernetes.
- An inferencing task using an NVIDIA Triton Inference Server instance that was orchestrated by using the NetApp DataOps Toolkit for Kubernetes. We applied Protopia obfuscation to the image before invoking the Triton inference API to simulate the common requirement that any data that is transmitted over the network must be obfuscated. This workflow is applicable to use cases where data is collected within a trusted zone but must be passed outside of that trusted zone for inferencing. Without Protopia obfuscation, it is not possible to implement this type of workflow without sensitive data leaving the trusted zone.

[Next: Test configuration.](#)

## Test configuration

[Previous: Test and validation plan.](#)

The following table outlines the solution design validation environment.

Component	Version
Kubernetes	1.21.6
NetApp Astra Trident CSI Driver	22.01.0
NetApp DataOps Toolkit for Kubernetes	2.3.0
NVIDIA Triton Inference Server	21.11-py3

[Next: Test procedure.](#)

## Test procedure

[Previous: Test configuration.](#)

This section describes the tasks needed to complete the validation.

### Prerequisites

To execute the tasks outlined in this section, you must have access to a Linux or macOS host with the following tools installed and configured:

- Kubectl (configured for access to an existing Kubernetes cluster)
  - Installation and configuration instructions can be found [here](#).
- NetApp DataOps Toolkit for Kubernetes

- Installation instructions can be found [here](#).

### Scenario 1 – On-demand inferencing in JupyterLab

1. Create a Kubernetes namespace for AI/ML inferencing workloads.

```
$ kubectl create namespace inference  
namespace/inference created
```

2. Use the NetApp DataOps Toolkit to provision a persistent volume for storing the data on which you will perform the inferencing.

```
$ netapp_dataops_k8s_cli.py create volume --namespace=inference --pvc  
--name=inference-data --size=50Gi  
Creating PersistentVolumeClaim (PVC) 'inference-data' in namespace  
'inference'.  
PersistentVolumeClaim (PVC) 'inference-data' created. Waiting for  
Kubernetes to bind volume to PVC.  
Volume successfully created and bound to PersistentVolumeClaim (PVC)  
'inference-data' in namespace 'inference'.
```

3. Use the NetApp DataOps Toolkit to create a new JupyterLab workspace. Mount the persistent volume that was created in the previous step by using the `--mount- pvc` option. Allocate NVIDIA GPUs to the workspace as necessary by using the `-- nvidia-gpu` option.

In the following example, the persistent volume `inference-data` is mounted to the JupyterLab workspace container at `/home/jovyan/data`. When using official Project Jupyter container images, `/home/jovyan` is presented as the top-level directory within the JupyterLab web interface.

```
$ netapp_dataops_k8s_cli.py create jupyterlab --namespace=inference  
--workspace-name=live-inference --size=50Gi --nvidia-gpu=2 --mount  
-pvc=inference-data:/home/jovyan/data  
Set workspace password (this password will be required in order to  
access the workspace):  
Re-enter password:  
Creating persistent volume for workspace...  
Creating PersistentVolumeClaim (PVC) 'ntap-dsutil-jupyterlab-live-  
inference' in namespace 'inference'.  
PersistentVolumeClaim (PVC) 'ntap-dsutil-jupyterlab-live-inference'  
created. Waiting for Kubernetes to bind volume to PVC.  
Volume successfully created and bound to PersistentVolumeClaim (PVC)  
'ntap-dsutil-jupyterlab-live-inference' in namespace 'inference'.  
Creating Service 'ntap-dsutil-jupyterlab-live-inference' in namespace  
'inference'.  
Service successfully created.  
Attaching Additional PVC: 'inference-data' at mount_path:  
'/home/jovyan/data'.  
Creating Deployment 'ntap-dsutil-jupyterlab-live-inference' in namespace  
'inference'.  
Deployment 'ntap-dsutil-jupyterlab-live-inference' created.  
Waiting for Deployment 'ntap-dsutil-jupyterlab-live-inference' to reach  
Ready state.  
Deployment successfully created.  
Workspace successfully created.  
To access workspace, navigate to http://192.168.0.152:32721
```

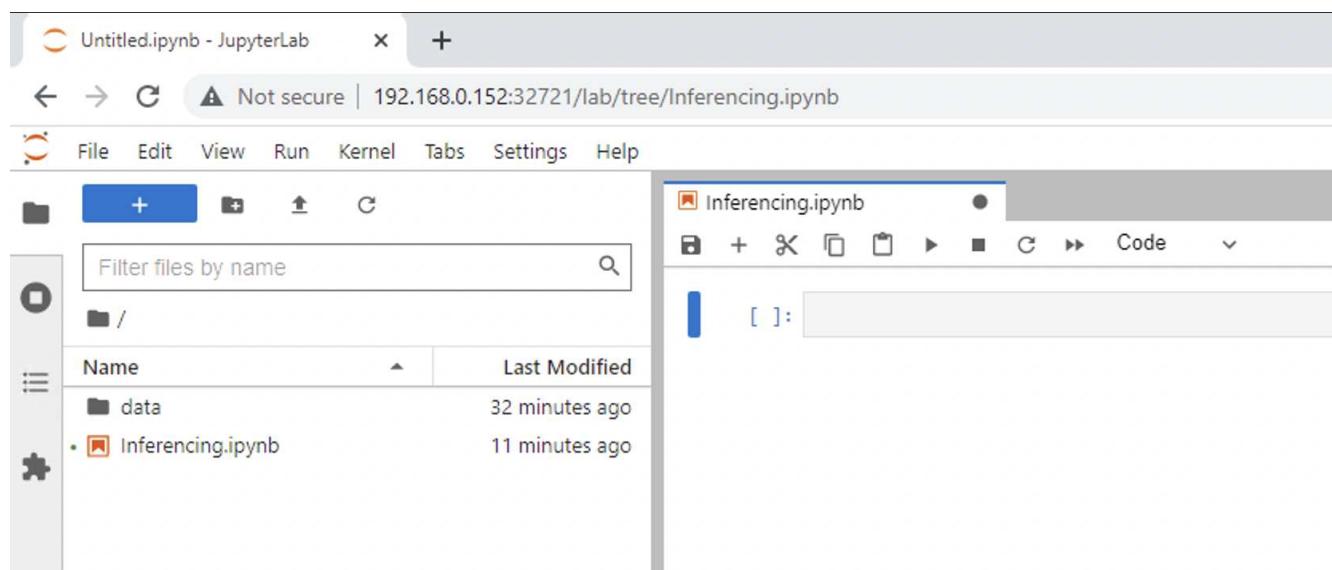
4. Access the JupyterLab workspace by using the URL specified in the output of the `create jupyterlab` command. The data directory represents the persistent volume that was mounted to the workspace.



5. Open the `data` directory and upload the files on which the inferencing is to be performed. When files are uploaded to the `data` directory, they are automatically stored on the persistent volume that was mounted to the workspace. To upload files, click the Upload Files icon, as shown in the following image.



6. Return to the top-level directory and create a new notebook.



7. Add inferencing code to the notebook. The following example shows inferencing code for an image detection use case.

Launcher X image-demo-pytorch.ipynb X

Code Python 3 (ipykernel) ⚡

### STEP 3-1: Clean (Without obfuscation) detection

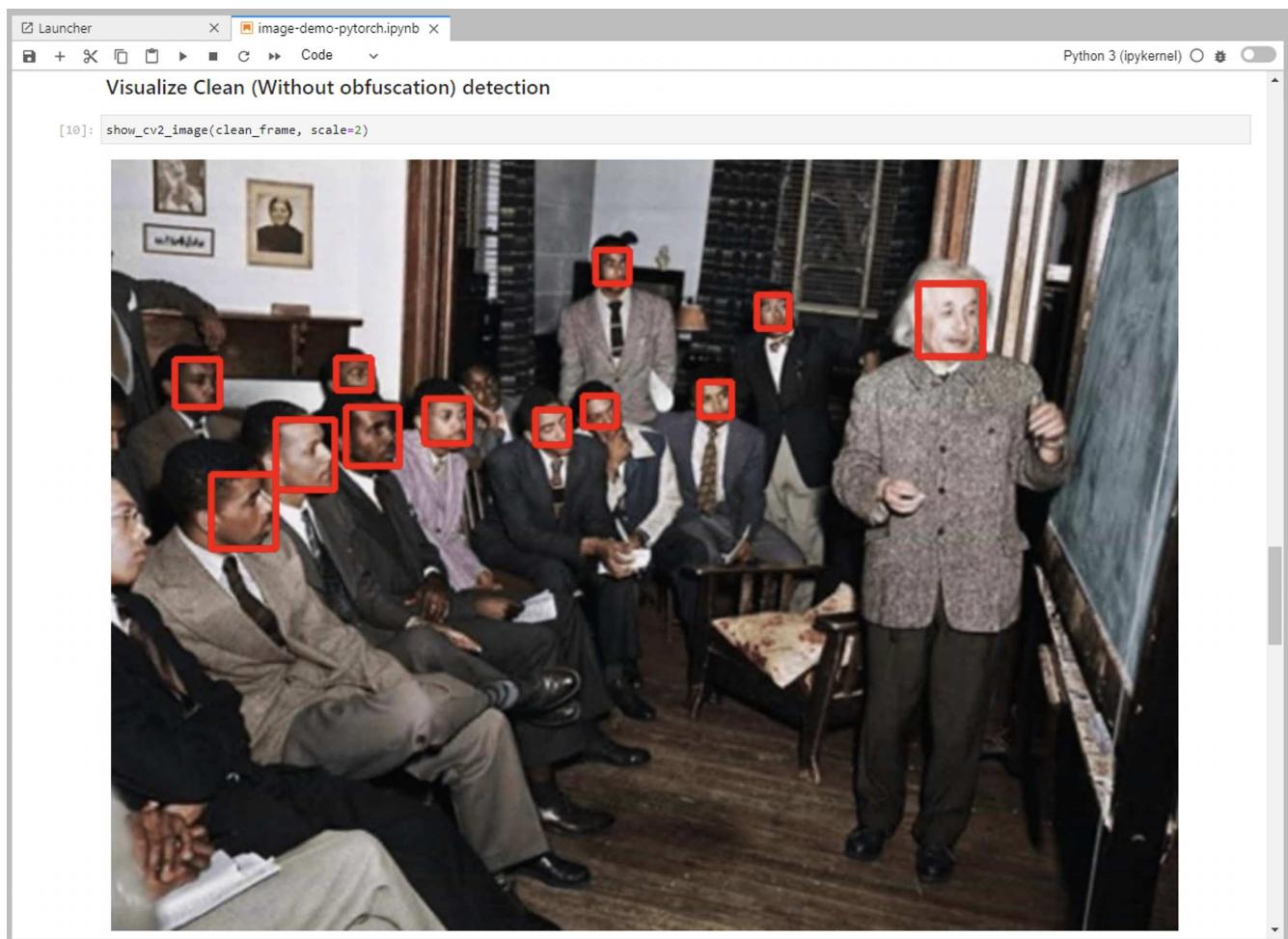
```
[9]: # get current frame
frame = input_image

# preprocess input
preprocessed_input = preprocess_input(frame)
preprocessed_input = torch.Tensor(preprocessed_input).to(device)

# run forward pass
clean_activation = clean_model.forward_head(preprocessed_input) # runs the first few layers
loc, pred = clean_model.forward_tail(clean_activation) # runs rest of the layers

# postprocess output
clean_pred = (loc.detach().cpu().numpy(), pred.detach().cpu().numpy())
clean_outputs = postprocess_outputs(
    clean_pred, [[input_image_width, input_image_height]], priors, THRESHOLD
)

# draw rectangles
clean_frame = copy.deepcopy(frame) # needs to be deep copy
for (x1, y1, x2, y2, s) in clean_outputs[0]:
    x1, y1 = int(x1), int(y1)
    x2, y2 = int(x2), int(y2)
    cv2.rectangle(clean_frame, (x1, y1), (x2, y2), (0, 0, 255), 4)
```



8. Add Protopia obfuscation to your inferencing code. Protopia works directly with customers to provide use-case specific documentation and is outside of the scope of this technical report. The following example shows inferencing code for an image detection use case with Protopia obfuscation added.

## STEP 3-2: Protopia AI (With obfuscation) detection

```
[11]: # get current frame
frame = input_image

# preprocess input
preprocessed_input = preprocess_input(frame)
preprocessed_input = torch.Tensor(preprocessed_input).to(device)

# run forward pass
not_noisy_activation = noisy_model.forward_head(preprocessed_input) # runs the first few layers
#####
# SINGLE ADDITIONAL LINE FOR PRIVATE INFERENCE #
#####
noisy_activation = noisy_model.forward_noise(not_noisy_activation)
#####
loc, pred = noisy_model.forward_tail(noisy_activation) # runs rest of the layers

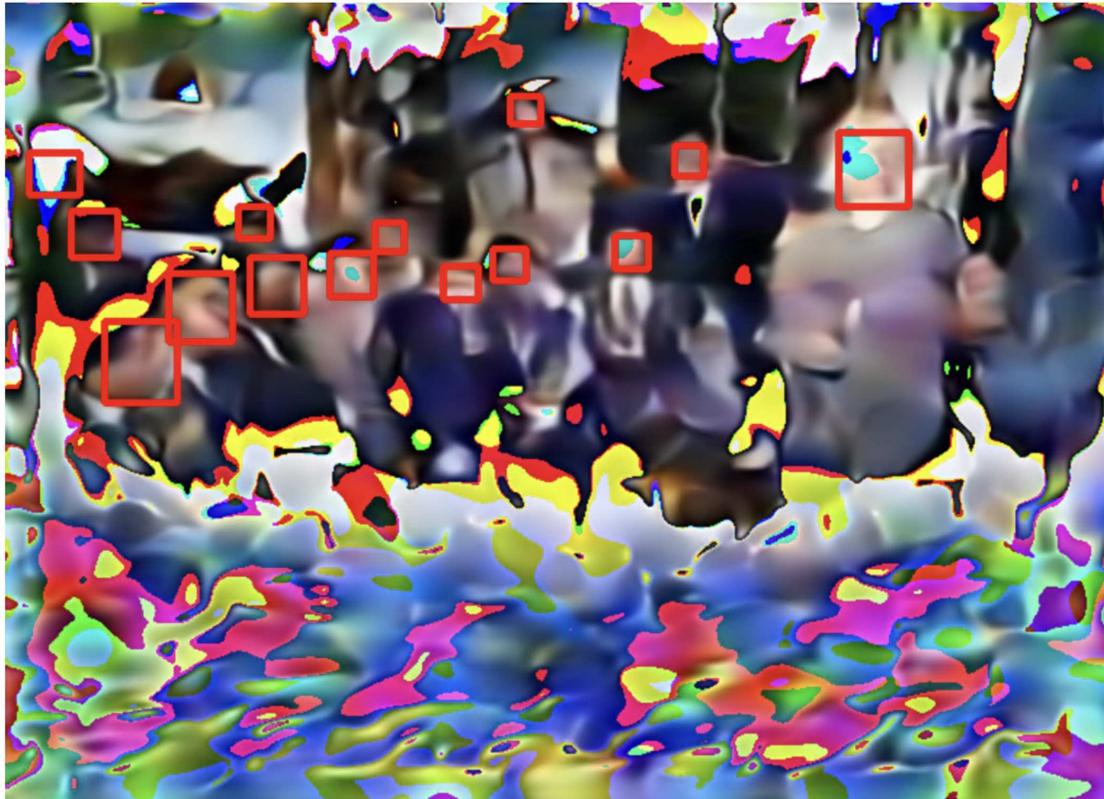
# postprocess output
noisy_pred = (loc.detach().cpu().numpy(), pred.detach().cpu().numpy())
noisy_outputs = postprocess_outputs(
    noisy_pred, [[input_image_width, input_image_height]], priors, THRESHOLD * 0.5
)

# get reconstruction of the noisy activation
noisy_reconstruction = decoder_function(noisy_activation)
noisy_reconstruction = noisy_reconstruction.detach().cpu().numpy()[0]
noisy_reconstruction = unprocess_output(
    noisy_reconstruction, (input_image_width, input_image_height), True
).astype(np.uint8)

# draw rectangles
for (x1, y1, x2, y2, s) in noisy_outputs[0]:
    x1, y1 = int(x1), int(y1)
    x2, y2 = int(x2), int(y2)
    cv2.rectangle(noisy_reconstruction, (x1, y1), (x2, y2), (0, 0, 255), 4)
```

## Visualize Protopia AI (With obfuscation) detection

```
[12]: show_cv2_image(noisy_reconstruction, scale=2)
```



## Scenario 2 – Batch inferencing on Kubernetes

1. Create a Kubernetes namespace for AI/ML inferencing workloads.

```
$ kubectl create namespace inference  
namespace/inference created
```

2. Use the NetApp DataOps Toolkit to provision a persistent volume for storing the data on which you will perform the inferencing.

```
$ netapp_dataops_k8s_cli.py create volume --namespace=inference --pvc  
-name=inference-data --size=50Gi  
Creating PersistentVolumeClaim (PVC) 'inference-data' in namespace  
'inference'.  
PersistentVolumeClaim (PVC) 'inference-data' created. Waiting for  
Kubernetes to bind volume to PVC.  
Volume successfully created and bound to PersistentVolumeClaim (PVC)  
'inference-data' in namespace 'inference'.
```

3. Populate the new persistent volume with the data on which you will perform the inferencing.

There are several methods for loading data onto a PVC. If your data is currently stored in an S3-compatible object storage platform, such as NetApp StorageGRID or Amazon S3, then you can use [NetApp DataOps Toolkit S3 Data Mover capabilities](#). Another simple method is to create a JupyterLab workspace and then upload files through the JupyterLab web interface, as outlined in Steps 3 to 5 in the section “[Scenario 1 – On-demand inferencing in JupyterLab](#).”

4. Create a Kubernetes job for your batch inferencing task. The following example shows a batch inferencing job for an image detection use case. This job performs inferencing on each image in a set of images and writes inferencing accuracy metrics to stdout.

```
$ vi inference-job-raw.yaml
apiVersion: batch/v1
kind: Job
metadata:
  name: netapp-inference-raw
  namespace: inference
spec:
  backoffLimit: 5
  template:
    spec:
      volumes:
        - name: data
          persistentVolumeClaim:
            claimName: inference-data
        - name: dshm
          emptyDir:
            medium: Memory
      containers:
        - name: inference
          image: netapp-protopia-inference:latest
          imagePullPolicy: IfNotPresent
          command: ["python3", "run-accuracy-measurement.py", "--dataset",
                    "/data/netapp-face-detection/FDDB"]
          resources:
            limits:
              nvidia.com/gpu: 2
      volumeMounts:
        - mountPath: /data
          name: data
        - mountPath: /dev/shm
          name: dshm
      restartPolicy: Never
$ kubectl create -f inference-job-raw.yaml
job.batch/netapp-inference-raw created
```

5. Confirm that the inferencing job completed successfully.

```
$ kubectl -n inference logs netapp-inference-raw-255sp
100%|██████████| 89/89 [00:52<00:00, 1.68it/s]
Reading Predictions : 100%|██████████| 10/10 [00:01<00:00, 6.23it/s]
Predicting ... : 100%|██████████| 10/10 [00:16<00:00, 1.64s/it]
===== Results =====
FDDB-fold-1 Val AP: 0.9491256561145955
FDDB-fold-2 Val AP: 0.9205024466101926
FDDB-fold-3 Val AP: 0.9253013871078468
FDDB-fold-4 Val AP: 0.9399781485863011
FDDB-fold-5 Val AP: 0.9504280149478732
FDDB-fold-6 Val AP: 0.9416473519339292
FDDB-fold-7 Val AP: 0.9241631566241117
FDDB-fold-8 Val AP: 0.9072663297546659
FDDB-fold-9 Val AP: 0.9339648715035469
FDDB-fold-10 Val AP: 0.9447707905560152
FDDB Dataset Average AP: 0.9337148153739079
=====
mAP: 0.9337148153739079
```

6. Add Protopia obfuscation to your inferencing job. You can find use case-specific instructions for adding Protopia obfuscation directly from Protopia, which is outside of the scope of this technical report. The following example shows a batch inferencing job for a face detection use case with Protopia obfuscation added by using an ALPHA value of 0.8. This job applies Protopia obfuscation before performing inferencing for each image in a set of images and then writes inferencing accuracy metrics to stdout.

We repeated this step for ALPHA values 0.05, 0.1, 0.2, 0.4, 0.6, 0.8, 0.9, and 0.95. You can see the results in [“Inferencing accuracy comparison.”](#)

```

$ vi inference-job-protopia-0.8.yaml
apiVersion: batch/v1
kind: Job
metadata:
  name: netapp-inference-protopia-0.8
  namespace: inference
spec:
  backoffLimit: 5
  template:
    spec:
      volumes:
        - name: data
          persistentVolumeClaim:
            claimName: inference-data
        - name: dshm
          emptyDir:
            medium: Memory
      containers:
        - name: inference
          image: netapp-protopia-inference:latest
          imagePullPolicy: IfNotPresent
          env:
            - name: ALPHA
              value: "0.8"
          command: ["python3", "run-accuracy-measurement.py", "--dataset",
                    "/data/netapp-face-detection/FDDB", "--alpha", "$(ALPHA)", "--noisy"]
          resources:
            limits:
              nvidia.com/gpu: 2
      volumeMounts:
        - mountPath: /data
          name: data
        - mountPath: /dev/shm
          name: dshm
      restartPolicy: Never
$ kubectl create -f inference-job-protopia-0.8.yaml
job.batch/netapp-inference-protopia-0.8 created

```

7. Confirm that the inferencing job completed successfully.

```
$ kubectl -n inference logs netapp-inference-protopia-0.8-b4dkz
100%|██████████| 89/89 [01:05<00:00, 1.37it/s]
Reading Predictions : 100%|██████████| 10/10 [00:02<00:00, 3.67it/s]
Predicting ... : 100%|██████████| 10/10 [00:22<00:00, 2.24s/it]
===== Results =====
FDDB-fold-1 Val AP: 0.8953066115834589
FDDB-fold-2 Val AP: 0.8819580264029936
FDDB-fold-3 Val AP: 0.8781107458462862
FDDB-fold-4 Val AP: 0.9085731346308461
FDDB-fold-5 Val AP: 0.9166445508275378
FDDB-fold-6 Val AP: 0.9101178994188819
FDDB-fold-7 Val AP: 0.8383443678423771
FDDB-fold-8 Val AP: 0.8476311547659464
FDDB-fold-9 Val AP: 0.8739624502111121
FDDB-fold-10 Val AP: 0.8905468076424851
FDDB Dataset Average AP: 0.8841195749171925
=====
mAP: 0.8841195749171925
```

### Scenario 3 – NVIDIA Triton Inference Server

1. Create a Kubernetes namespace for AI/ML inferencing workloads.

```
$ kubectl create namespace inference
namespace/inference created
```

2. Use the NetApp DataOps Toolkit to provision a persistent volume to use as a model repository for the NVIDIA Triton Inference Server.

```
$ netapp_dataops_k8s_cli.py create volume --namespace=inference --pvc
--name=triton-model-repo --size=100Gi
Creating PersistentVolumeClaim (PVC) 'triton-model-repo' in namespace
'inference'.
PersistentVolumeClaim (PVC) 'triton-model-repo' created. Waiting for
Kubernetes to bind volume to PVC.
Volume successfully created and bound to PersistentVolumeClaim (PVC)
'triton-model-repo' in namespace 'inference'.
```

3. Store your model on the new persistent volume in a [format](#) that is recognized by the NVIDIA Triton Inference Server.

There are several methods for loading data onto a PVC. A simple method is to create a JupyterLab workspace and then upload files through the JupyterLab web interface, as outlined in steps 3 to 5 in “[Scenario 1 – On-demand inferencing in JupyterLab](#).”

4. Use NetApp DataOps Toolkit to deploy a new NVIDIA Triton Inference Server instance.

```
$ netapp_dataops_k8s_cli.py create triton-server --namespace=inference  
--server-name=netapp-inference --model-repo-pvc-name=triton-model-repo  
Creating Service 'ntap-dsutil-triton-netapp-inference' in namespace  
'inference'.  
Service successfully created.  
Creating Deployment 'ntap-dsutil-triton-netapp-inference' in namespace  
'inference'.  
Deployment 'ntap-dsutil-triton-netapp-inference' created.  
Waiting for Deployment 'ntap-dsutil-triton-netapp-inference' to reach  
Ready state.  
Deployment successfully created.  
Server successfully created.  
Server endpoints:  
http: 192.168.0.152: 31208  
grpc: 192.168.0.152: 32736  
metrics: 192.168.0.152: 30009/metrics
```

5. Use a Triton client SDK to perform an inferencing task. The following Python code excerpt uses the Triton Python client SDK to perform an inferencing task for an face detection use case. This example calls the Triton API and passes in an image for inferencing. The Triton Inference Server then receives the request, invokes the model, and returns the inferencing output as part of the API results.

```
# get current frame
frame = input_image
# preprocess input
preprocessed_input = preprocess_input(frame)
preprocessed_input = torch.Tensor(preprocessed_input).to(device)
# run forward pass
clean_activation = clean_model_head(preprocessed_input) # runs the
first few layers
#####
#####
#####
#           pass clean image to Triton Inference Server API for
inferencing          #
#####
#####
#####
triton_client =
httpclient.InferenceServerClient(url="192.168.0.152:31208",
verbose=False)
model_name = "face_detection_base"
inputs = []
outputs = []
inputs.append(httpclient.InferInput("INPUT_0", [1, 128, 32, 32],
```

```

    "FP32"))
inputs[0].set_data_from_numpy(clean_activation.detach().cpu().numpy(),
binary_data=False)
outputs.append(httpclient.InferRequestedOutput("OUTPUT__0",
binary_data=False))
outputs.append(httpclient.InferRequestedOutput("OUTPUT__1",
binary_data=False))
results = triton_client.infer(
    model_name,
    inputs,
    outputs=outputs,
    #query_params=query_params,
    headers=None,
    request_compression_algorithm=None,
    response_compression_algorithm=None)
#print(results.get_response())
statistics =
triton_client.get_inference_statistics(model_name=model_name,
headers=None)
print(statistics)
if len(statistics["model_stats"]) != 1:
    print("FAILED: Inference Statistics")
    sys.exit(1)

loc_numpy = results.as_numpy("OUTPUT__0")
pred_numpy = results.as_numpy("OUTPUT__1")
#####
#####
# postprocess output
clean_pred = (loc_numpy, pred_numpy)
clean_outputs = postprocess_outputs(
    clean_pred, [[input_image_width, input_image_height]], priors,
THRESHOLD
)
# draw rectangles
clean_frame = copy.deepcopy(frame) # needs to be deep copy
for (x1, y1, x2, y2, s) in clean_outputs[0]:
    x1, y1 = int(x1), int(y1)
    x2, y2 = int(x2), int(y2)
    cv2.rectangle(clean_frame, (x1, y1), (x2, y2), (0, 0, 255), 4)

```

6. Add Protopia obfuscation to your inferencing code. You can find use case-specific instructions for adding Protopia obfuscation directly from Protopia; however, this process is outside the scope of this technical report. The following example shows the same Python code that is shown in the preceding step 5, but with Protopia obfuscation added.

Note that the Protopia obfuscation is applied to the image before it is passed to the Triton API. Thus, the

non-obfuscated image never leaves the local machine. Only the obfuscated image is passed across the network. This workflow is applicable to use cases in which data is collected within a trusted zone but then needs to be passed outside of that trusted zone for inferencing. Without Protopia obfuscation, it is not possible to implement this type of workflow without sensitive data ever leaving the trusted zone.

```
# get current frame
frame = input_image
# preprocess input
preprocessed_input = preprocess_input(frame)
preprocessed_input = torch.Tensor(preprocessed_input).to(device)
# run forward pass
not_noisy_activation = noisy_model_head(preprocessed_input) # runs the
first few layers
#####
#       obfuscate image locally prior to inferencing #
#       SINGLE ADITIONAL LINE FOR PRIVATE INFERENCE #
#####
noisy_activation = noisy_model_noise(not_noisy_activation)
#####
#       pass obfuscated image to Triton Inference Server API for
inferencing      #
#####
triton_client =
httpclient.InferenceServerClient(url="192.168.0.152:31208",
verbose=False)
model_name = "face_detection_noisy"
inputs = []
outputs = []
inputs.append(httpclient.InferInput("INPUT_0", [1, 128, 32, 32],
"FP32"))
inputs[0].set_data_from_numpy(noisy_activation.detach().cpu().numpy(),
binary_data=False)
outputs.append(httpclient.InferRequestedOutput("OUTPUT_0",
binary_data=False))
outputs.append(httpclient.InferRequestedOutput("OUTPUT_1",
binary_data=False))
results = triton_client.infer(
    model_name,
    inputs,
    outputs=outputs,
    #query_params=query_params,
    headers=None,
    request_compression_algorithm=None,
```

```

        response_compression_algorithm=None)
#print(results.get_response())
statistics =
    triton_client.get_inference_statistics(model_name=model_name,
headers=None)
print(statistics)
if len(statistics["model_stats"]) != 1:
    print("FAILED: Inference Statistics")
    sys.exit(1)

loc_numpy = results.as_numpy("OUTPUT__0")
pred_numpy = results.as_numpy("OUTPUT__1")
#####
#####

# postprocess output
noisy_pred = (loc_numpy, pred_numpy)
noisy_outputs = postprocess_outputs(
    noisy_pred, [[input_image_width, input_image_height]], priors,
THRESHOLD * 0.5
)
# get reconstruction of the noisy activation
noisy_reconstruction = decoder_function(noisy_activation)
noisy_reconstruction = noisy_reconstruction.detach().cpu().numpy()[0]
noisy_reconstruction = unpreprocess_output(
    noisy_reconstruction, (input_image_width, input_image_height), True
).astype(np.uint8)
# draw rectangles
for (x1, y1, x2, y2, s) in noisy_outputs[0]:
    x1, y1 = int(x1), int(y1)
    x2, y2 = int(x2), int(y2)
    cv2.rectangle(noisy_reconstruction, (x1, y1), (x2, y2), (0, 0, 255),
4)

```

[Next: Inferencing accuracy comparison.](#)

## Inferencing accuracy comparison

[Previous: Test procedure.](#)

For this validation, we performed inferencing for an image detection use case by using a set of raw images. We then performed the same inferencing task on the same set of images with Protopia obfuscation added before inferencing. We repeated the task using different values of ALPHA for the Protopia obfuscation component. In the context of Protopia obfuscation, the ALPHA value represents the amount of obfuscation that is applied, with a higher ALPHA value representing a higher level of obfuscation. We then compared inferencing accuracy across these different runs.

The following two tables provide details about our use case and outline the results.

Protopia works directly with customers to determine the appropriate ALPHA value for a specific use case.

Component	Details
Model	FaceBoxes (PyTorch) -
Dataset	FDDB dataset

Protopia obfuscation	ALPHA	Accuracy
No	N/A	0.9337148153739079
Yes	0.05	0.9028766627325002
Yes	0.1	0.9024301009661478
Yes	0.2	0.9081836283186224
Yes	0.4	0.9073066107482036
Yes	0.6	0.8847816568680239
Yes	0.8	0.8841195749171925
Yes	0.9	0.8455427675252052
Yes	0.95	0.8455427675252052

[Next: Obfuscation speed.](#)

## Obfuscation speed

[Previous: Inferencing accuracy comparison.](#)

For this validation, we applied Protopia obfuscation to a 1920 x 1080 pixel image five times and measured the amount of time that it took for the obfuscation step to complete each time. We used PyTorch running on a single NVIDIA V100 GPU to apply the obfuscation, and we cleared the GPU cache between runs. The obfuscation step took 5.47ms, 5.27ms, 4.54ms, 5.24ms, and 4.84ms respectively to complete across the five runs. The average speed was 5.072ms.

[Next: Conclusion.](#)

## Conclusion

[Previous: Obfuscation speed.](#)

Data exists in three states: at rest, in transit, and in compute. An important part of any AI inferencing service should be the protection of data from threats during the entire process. Protecting data during inferencing is critical because the process can expose private information about both external customers and the business providing the inferencing service. Protopia AI is a nonobtrusive software-only solution for confidential AI inferencing in today's market. With Protopia, AI is fed only the transformed information in the data records that is essential to carrying out the AI/ML task at hand and nothing more. This stochastic transformation is not a form of masking and is based on mathematically changing the representation of the data by using curated noise.

NetApp storage systems with ONTAP capabilities deliver the same or better performance as local SSD storage and, combined with the NetApp DataOps Toolkit, offer the following benefits to data scientists, data engineers, AI/ML developers, and business or enterprise IT decision makers:

- Effortless sharing of data between AI systems, analytics, and other critical business systems. This data sharing reduces infrastructure overhead, improves performance, and streamlines data management across the enterprise.
- Independently scalable compute and storage to minimize costs and improve resource usage.
- Streamlined development and deployment workflows using integrated Snapshot copies and clones for instantaneous and space-efficient user workspaces, integrated version control, and automated deployment.
- Enterprise-grade data protection and data governance for disaster recovery, business continuity, and regulatory requirements.
- Simplified invocation of data management operations; rapidly take Snapshot copies of data scientist workspaces for backup and traceability from the NetApp DataOps Toolkit in Jupyter notebooks.

The NetApp and Protopia solution provides a flexible, scale-out architecture that is ideal for enterprise-grade AI inference deployments. It enables data protection and provides privacy for sensitive information where confidential AI inferencing requirements can be met with responsible AI practices in both on-premises and hybrid cloud deployments.

[Next: Where to find additional information, acknowledgements, and version history.](#)

## **Where to find additional information, acknowledgements, and version history**

[Previous: Conclusion.](#)

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

- NetApp ONTAP data management software — ONTAP information library  
<http://mysupport.netapp.com/documentation/productlibrary/index.html?productID=62286>
- NetApp Persistent Storage for Containers—NetApp Trident  
<https://netapp.io/persistent-storage-provisioner-for-kubernetes/>
- NetApp DataOps Toolkit  
<https://github.com/NetApp/netapp-dataops-toolkit>
- NetApp Persistent Storage for Containers—NetApp Astra Trident  
<https://netapp.io/persistent-storage-provisioner-for-kubernetes/>
- Protopia AI—Confidential Inference  
<https://protopia.ai/blog/protopia-ai-takes-on-the-missing-link-in-ai-privacy-confidential-inference/>
- NetApp Cloud Sync  
[https://docs.netapp.com/us-en/occm/concept\\_cloud\\_sync.html#how-cloud-sync-works](https://docs.netapp.com/us-en/occm/concept_cloud_sync.html#how-cloud-sync-works)
- NVIDIA Triton Inference Server  
<https://developer.nvidia.com/nvidia-triton-inference-server>

- NVIDIA Triton Inference Server Documentation  
<https://docs.nvidia.com/deeplearning/triton-inference-server/index.html>
- FaceBoxes in PyTorch  
<https://github.com/zisianw/FaceBoxes.PyTorch>

## Acknowledgments

- Mark Cates, Principal Product Manager, NetApp
- Sufian Ahmad, Technical Marketing Engineer, NetApp
- Hadi Esmaeilzadeh, Chief Technology Officer and Professor, Protopia AI

## Version history

Version	Date	Document Version History
Version 1.0	May 2022	Initial release.

## Sentiment analysis with NetApp AI

### TR-4910: Sentiment Analysis from Customer Communications with NetApp AI

Rick Huang, Sathish Thyagarajan, and David Arnette, NetApp  
 Diego Sosa-Coba, SFL Scientific

This technical report provides design guidance for customers to perform sentiment analysis in an enterprise-level global support center by using NetApp data management technologies with an NVIDIA software framework using transfer learning and conversational AI. This solution is applicable to any industry wanting to gain customer insights from recorded speech or text files representing chat logs, emails, and other text or audio communications. We implemented an end-to-end pipeline to demonstrate automatic speech recognition, real-time sentiment analysis, and deep-learning natural-language-processing model-retraining capabilities on a GPU-accelerated compute cluster with NetApp cloud-connected all flash storage. Massive, state-of-the-art language models can be trained and optimized to perform inference rapidly with the global support center to create an exceptional customer experience and objective, long-term employee performance evaluations.

Sentiment analysis is a field of study within Natural Language Processing (NLP) by which positive, negative, or neutral sentiments are extracted from text. Conversational AI systems have risen to a near global level of integration as more and more people come to interact with them. Sentiment analysis has a variety of use cases, from determining support center employee performance in conversations with callers and providing appropriate automated chatbot responses to predicting a firm's stock price based on the interactions between firm representatives and the audience at quarterly earnings calls. Furthermore, sentiment analysis can be used to determine the customer's view on the products, services, or support provided by the brand.

This end-to-end solution uses NLP models to perform high level sentiment analysis that enables support-center analytical frameworks. Audio recordings are processed into written text, and sentiment is extracted from each sentence in the conversation. Results, aggregated into a dashboard, can be crafted to analyze conversation sentiments, both historically and in real-time. This solution can be generalized to other solutions with similar data modalities and output needs. With the appropriate data, other use cases can be accomplished. For example, company earnings calls can be analyzed for sentiment using the same end-to-end pipeline. Other forms of NLP analyses, such as topic modeling and named entity recognition (NER), are also possible due to the flexible nature of the pipeline.

These AI implementations were made possible by NVIDIA RIVA, the NVIDIA TAO Toolkit, and the NetApp DataOps Toolkit working together. NVIDIA's tools are used to rapidly deploy highly performant AI solutions using prebuilt models and pipelines. The NetApp DataOps Toolkit simplifies various data management tasks to speed up development.

#### **Customer value**

Businesses see value from an employee-assessment and customer-reaction tool for text, audio, and video conversation for sentiment analysis. Managers benefit from the information presented in the dashboard, allowing for an assessment of the employees and customer satisfaction based on both sides of the conversation.

Additionally, the NetApp DataOps Toolkit manages the versioning and allocation of data within the customer's infrastructure. This leads to frequent updates of the analytics presented within the dashboard without creating unwieldy data storage costs.

[Next: Use cases.](#)

#### **Use cases**

[Previous: Support center analytics.](#)

Due to the number of calls that these support centers process, assessment of call performance could take significant time if performed manually. Traditional methods, like bag-of-words counting and other methods, can achieve some automation, but these methods do not capture more nuanced aspects and semantic context of dynamic language. AI modeling techniques can be used to perform some of these more nuanced analyses in an automated manner. Furthermore, with the current state of the art, pretrained modeling tools published by NVIDIA, AWS, Google, and others, an end-to-end pipeline with complex models can be now stood up and customized with relative ease.

An end-to-end pipeline for support center sentiment analysis ingests audio files in real time as employees converse with callers. Then, these audio files are processed for use in the speech-to-text component which converts them into a text format. Each sentence in the conversation receives a label indicating the sentiment (positive, negative, or neutral).

Sentiment analysis can provide an essential aspect of the conversations for assessment of call performance. These sentiments add an additional level of depth to the interactions between employees and callers. The AI-assisted sentiment dashboard provides managers with a real-time tracking of sentiment within a conversation, along with a retrospective analysis of the employee's past calls.

There are prebuilt tools that can be combined in powerful ways to quickly create an end-to-end AI pipeline to solve this problem. In this case, the NVIDIA RIVA library can be used to perform the two in-series tasks: audio transcription and sentiment analysis. The first is a supervised learning signal processing algorithm and the second is a supervised learning NLP classification algorithm. These out-of-the-box algorithms can be fine-tuned for any relevant use case with business-relevant data using the NVIDIA TAO Toolkit. This leads to more accurate and powerful solutions being built for only a fraction of the cost and resources. Customers can incorporate the [NVIDIA Maxine](#) framework for GPU-accelerated video conferencing applications in their support center design.

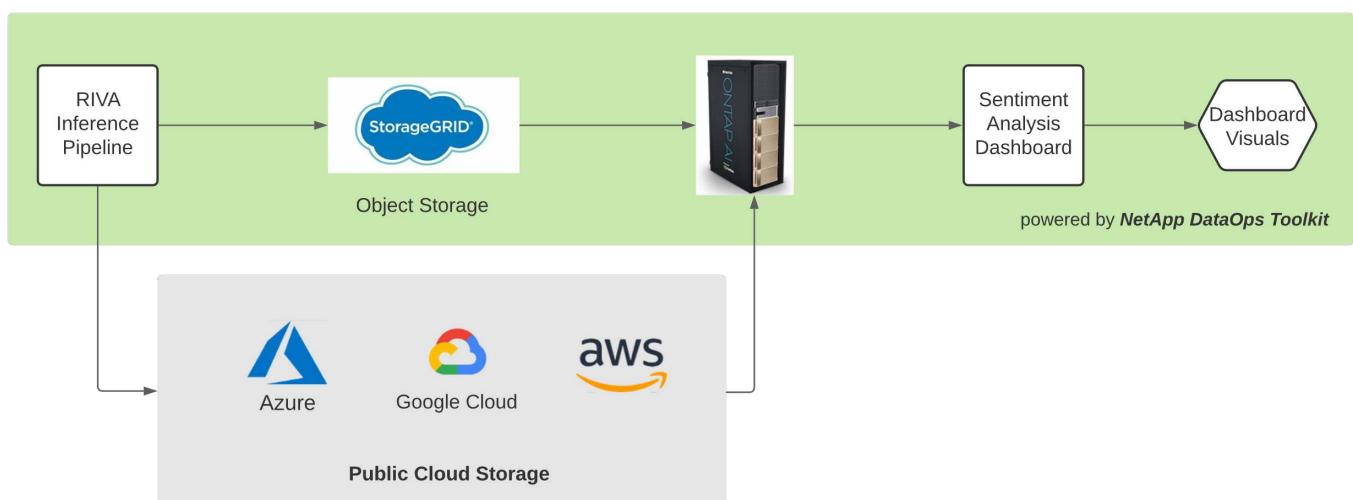
The following use cases are at the core of this solution. Both use cases use the TAO Toolkit for model fine-tuning and RIVA for model deployment.

- Speech-to-text
- Sentiment analysis

To analyze support center interactions between employees and customers, each customer conversation in the form of audio calls can be run through the pipeline to extract sentence-level sentiments. Those sentiments can then be verified by a human to justify the sentiments or adjust them as needed. The labeled data is then passed onto the fine-tuning step to improve sentiment predictions. If labeled sentiment data already exists, then model fine-tuning can be expedited. In either case, the pipeline is generalizable to other solutions that require the ingestion of audio and the classification of sentences.



AI sentiment outputs are either uploaded to an external cloud database or to a company- managed storage system. The sentiment outputs are transferred from this larger database into local storage for use within the dashboard that displays the sentiment analysis for managers. The dashboard's primary functionality is to interface with the customer service employee in real time. Managers can assess and provide feedback on employees during their calls with live updates of the sentiment of each sentence, as well as an historic review of the employee's past performance or customer reactions.



The [NetApp DataOps Toolkit](#) can continue to manage data storage systems even after the RIVA inference pipeline generates sentiment labels. Those AI results can be uploaded to a data storage system managed by the NetApp DataOps Toolkit. The data storage systems must be capable of managing hundreds of inserts and selects every minute. The local device storage system queries the larger data storage in real-time for extraction. The larger data storage instance can also be queried for historical data to further enhance the dashboard experience. The NetApp DataOps Toolkit facilitates both these uses by rapidly cloning data and distributing it across all the dashboards that use it.

## Target Audience

The target audience for the solution includes the following groups:

- Employee managers
- Data engineers/data scientists
- IT administrators (on-premises, cloud, or hybrid)

Tracking sentiments throughout conversations is a valuable tool for assessing employee performance. Using the AI-dashboard, managers can see how employees and callers change their feelings in real time, allowing for live assessments and guidance sessions. Moreover, businesses can gain valuable customer insights from customers engaged in vocal conversations, text chatbots, and video conferencing. Such customer analytics uses the capabilities of multimodal processing at scale with modern, state-of-the-art AI models and workflows.

On the data side, a large number of audio files are processed daily by the support center. The NetApp DataOps Toolkit facilitates this data handling task for both the periodic fine-tuning of models and sentiment analysis dashboards.

IT administrators also benefit from the NetApp DataOps Toolkit as it allows them to move data quickly between deployment and production environments. The NVIDIA environments and servers must also be managed and distributed to allow for real time inference.

[Next: Architecture.](#)

## Architecture

[Previous: Use cases.](#)

The architecture of this support center solution revolves around NVIDIA's prebuilt tools and the NetApp DataOps Toolkit. NVIDIA's tools are used to rapidly deploy high-performance AI-solutions using prebuilt models and pipelines. The NetApp DataOps Toolkit simplifies various data management tasks to speed up development.

## Solution technology

[NVIDIA RIVA](#) is a GPU-accelerated SDK for building multimodal conversational AI applications that deliver real-time performance on GPUs. The NVIDIA Train, Adapt, and Optimize (TAO) Toolkit provides a faster, easier way to accelerate training and quickly create highly accurate and performant, domain-specific AI models.

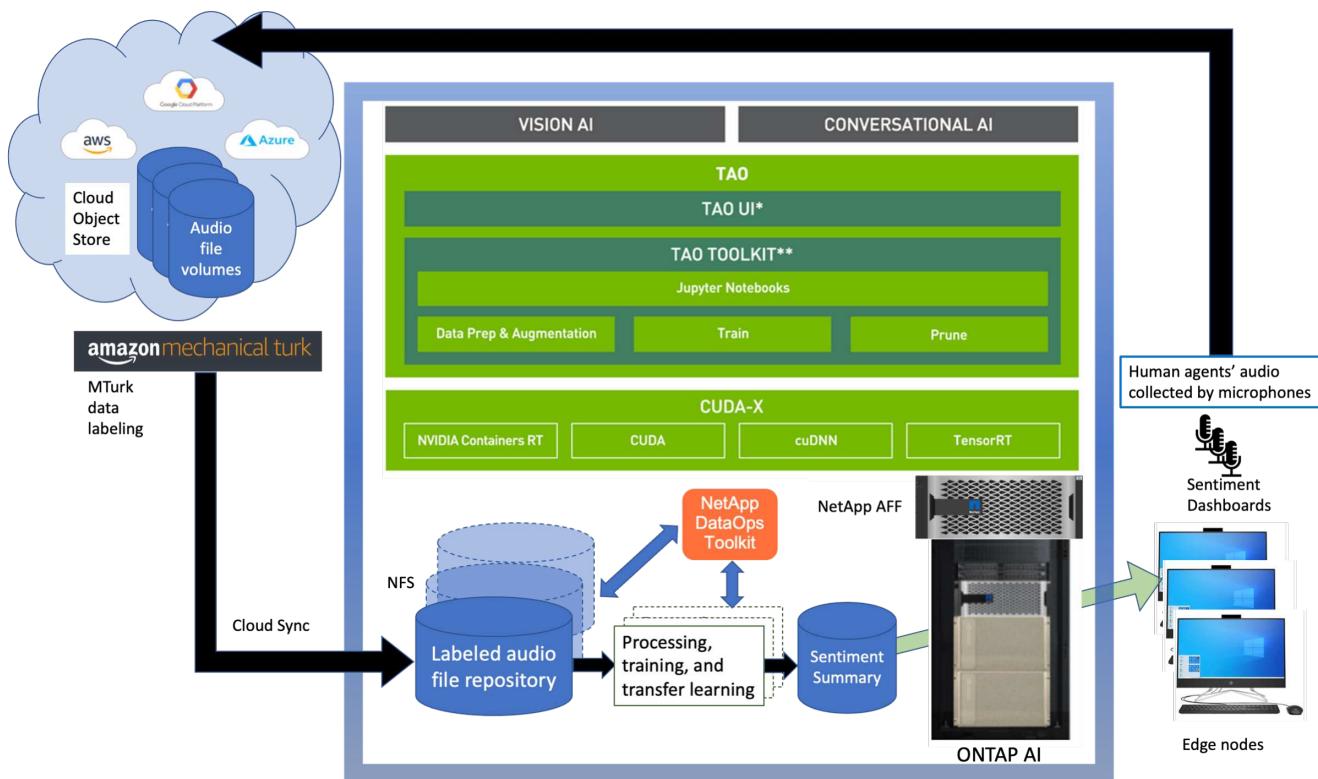
The NetApp DataOps Toolkit is a Python library that makes it simple for developers, data scientists, DevOps engineers, and data engineers to perform various data management tasks. This includes near-instantaneous provisioning of a new data volume or JupyterLab workspace, near-instantaneous cloning of a data volume or JupyterLab workspace, and near-instantaneous snapshotting of a data volume or JupyterLab workspace for traceability and baselining.

## Architectural Diagram

The following diagram shows the solution architecture. There are three main environment categories: the cloud, the core, and the edge. Each of the categories can be geographically dispersed. For example, the cloud contains object stores with audio files in buckets in different regions, whereas the core might contain datacenters linked via a high-speed network or NetApp Cloud Sync. The edge nodes denote the individual human agent's daily working platforms, where interactive dashboard tools and microphones are available to visualize sentiment and collect audio data from conversations with customers.

In GPU-accelerated datacenters, businesses can use the NVIDIA RIVA framework to build conversational AI applications, to which the Tao Toolkit connects for model finetuning and retraining using transfer L-learning techniques. These compute applications and workflows are powered by the NetApp DataOps Toolkit, enabling the best data management capabilities ONTAP has to offer. The toolkit allows corporate data teams to rapidly prototype their models with associated structured and unstructured data via snapshots and clones for traceability, versioning, A/B testing, thus providing security, governance, and regulatory compliance. See the section "["Storage Design"](#)" for more details.

This solution demonstrates the audio file processing, NLP model training, transfer learning, and data management detail steps. The resulting end-to-end pipeline generates a sentiment summary that displays in real-time on human support agents' dashboards.



## Hardware requirements

The following table lists the hardware components that are required to implement the solution. The hardware components that are used in any particular implementation of the solution might vary based on customer requirements.

Response latency tests	Time (milliseconds)
Data processing	10

Response latency tests	Time (milliseconds)
Inferencing	10

These response-time tests were run on 50,000+ audio files across 560 conversations. Each audio file was ~100KB in size as an MP3 and ~1 MB when converted to WAV. The data processing step converts MP3s into WAV files. The inference steps convert the audio files into text and extract a sentiment from the text. These steps are all independent of one another and can be parallelized to speed up the process.

Taking into account the latency of transferring data between stores, managers should be able to see updates to the real time sentiment analysis within a second of the end of the sentence.

## NVIDIA RIVA hardware

Hardware	Requirements
OS	Linux x86_64
GPU memory (ASR)	Streaming models: ~5600 MB Non-streaming models: ~3100 MB
GPU memory (NLP)	~500MB per BERT model

## NVIDIA TAO Toolkit hardware

Hardware	Requirements
System RAM	32GB
GPU RAM	32GB
CPU	8 core
GPU	NVIDIA (A100, V100 and RTX 30x0)
SSD	100GB

## Flash storage system

### NetApp ONTAP 9

ONTAP 9.9, the latest generation of storage management software from NetApp, enables businesses to modernize infrastructure and transition to a cloud-ready data center. Leveraging industry-leading data management capabilities, ONTAP enables the management and protection of data with a single set of tools, regardless of where that data resides. You can also move data freely to wherever it is needed: the edge, the core, or the cloud. ONTAP 9.9 includes numerous features that simplify data management, accelerate, and protect critical data, and enable next generation infrastructure capabilities across hybrid cloud architectures.

### NetApp Cloud Sync

[Cloud Sync](#) is a NetApp service for rapid and secure data synchronization that allows you to transfer files between on-premises NFS or SMB file shares to any of the following targets:

- NetApp StorageGRID
- NetApp ONTAP S3

- NetApp Cloud Volumes Service
- Azure NetApp Files
- Amazon Simple Storage Service (Amazon S3)
- Amazon Elastic File System (Amazon EFS)
- Azure Blob
- Google Cloud Storage
- IBM Cloud Object Storage

Cloud Sync moves the files where you need them quickly and securely. After your data is transferred, it is fully available for use on both the source and the target. Cloud Sync continuously synchronizes the data, based on your predefined schedule, moving only the deltas, so that time and money spent on data replication is minimized. Cloud Sync is a software as a service (SaaS) tool that is simple to set up and use. Data transfers that are triggered by Cloud Sync are carried out by data brokers. You can deploy Cloud Sync data brokers in AWS, Azure, Google Cloud Platform, or on-premises.

## **NetApp StorageGRID**

The StorageGRID software-defined object storage suite supports a wide range of use cases across public, private, and hybrid multi-cloud environments seamlessly. With industry leading innovations, NetApp StorageGRID stores, secures, protect, and preserves unstructured data for multi-purpose use including automated lifecycle management for long periods of time. For more information, see the [NetApp StorageGRID](#) site.

## **Software requirements**

The following table lists the software components that are required to implement this solution. The software components that are used in any particular implementation of the solution might vary based on customer requirements.

<b>Host machine</b>	<b>Requirements</b>
RIVA (formerly JARVIS)	1.4.0
TAO Toolkit (formerly Transfer Learning Toolkit)	3.0
ONTAP	9.9.1
DGX OS	5.1
DOTK	2.0.0

## **NVIDIA RIVA Software**

<b>Software</b>	<b>Requirements</b>
Docker	>19.02 (with nvidia-docker installed) ≥19.03 if not using DGX
NVIDIA Driver	465.19.01+ 418.40+, 440.33+, 450.51+, 460.27+ for Data Center GPUs
Container OS	Ubuntu 20.04

Software	Requirements
CUDA	11.3.0
cuBLAS	11.5.1.101
cuDNN	8.2.0.41
NCCL	2.9.6
TensorRT	7.2.3.4
Triton Inference Server	2.9.0

## NVIDIA TAO Toolkit software

Software	Requirements
Ubuntu 18.04 LTS	18.04
python	>=3.6.9
docker-ce	>19.03.5
docker-API	1.40
nvidia-container-toolkit	>1.3.0-1
nvidia-container-runtime	3.4.0-1
nvidia-docker2	2.5.0-1
nvidia-driver	>455
python-pip	>21.06
nvidia-pyindex	Latest version

## Use case details

This solution applies to the following use cases:

- Speech-to-text
- Sentiment analysis



The speech-to-text use case begins by ingesting audio files for the support centers. This audio is then processed to fit the structure required by RIVA. If the audio files have not already been split into their units of analysis, then this must be done before passing the audio to RIVA. After the audio file is processed, it is passed to the RIVA server as an API call. The server employs one of the many models it is hosting and returns a response. This speech-to-text (part of Automatic Speech Recognition) returns a text representation of the audio. From there, the pipeline switches over to the sentiment analysis portion.

For sentiment analysis, the text output from the Automatic Speech Recognition serves as the input to the Text Classification. Text Classification is the NVIDIA component for classifying text to any number of categories. The sentiment categories range from positive to negative for the support center conversations. The performance of the models can be assessed using a holdout set to determine the success of the fine-tuning step.



A similar pipeline is used for both the speech-to-text and sentiment analysis within the TAO Toolkit. The major difference is the use of labels which are required for the fine-tuning of the models. The TAO Toolkit pipeline begins with the processing of the data files. Then the pretrained models (coming from the [NVIDIA NGC Catalog](#)) are fine-tuned using the support center data. The fine-tuned models are evaluated based on their corresponding performance metrics and, if they are more performant than the pretrained models, are deployed to the RIVA server.

[Next: Design considerations.](#)

## Design considerations

[Previous: Architecture.](#)

### Network and compute design

Depending on the restrictions on data security, all data must remain within the customer's infrastructure or a secure environment.



## Storage design

The NetApp DataOps Toolkit serves as the primary service for managing storage systems. The DataOps Toolkit is a Python library that makes it simple for developers, data scientists, DevOps engineers, and data engineers to perform various data management tasks, such as near-instantaneous provisioning of a new data volume or JupyterLab workspace, near-instantaneous cloning of a data volume or JupyterLab workspace, and near-instantaneous snapshotting of a data volume or JupyterLab workspace for traceability or baselining. This Python library can function as either a command line utility or a library of functions that can be imported into any Python program or Jupyter Notebook.

## RIVA best practices

NVIDIA provides several general [best data practices](#) for using RIVA:

- **Use lossless audio formats if possible.** The use of lossy codecs such as MP3 can reduce quality.
- **Augment training data.** Adding background noise to audio training data can initially decrease accuracy and yet increase robustness.
- **Limit vocabulary size if using scraped text.** Many online sources contain typos or ancillary pronouns and uncommon words. Removing these can improve the language model.
- **Use a minimum sampling rate of 16kHz if possible.** However, try not to resample, because doing so decreases audio quality.

In addition to these best practices, customers must prioritize gathering a representative sample dataset with accurate labels for each step of the pipeline. In other words, the sample dataset should proportionally reflect specified characteristics exemplified in a target dataset. Similarly, the dataset annotators have a responsibility to balance accuracy and the speed of labeling so that the quality and quantity of the data are both maximized. For example, this support center solution requires audio files, labeled text, and sentiment labels. The sequential nature of this solution means that errors from the beginning of the pipeline are propagated all the way through to the end. If the audio files are of poor quality, the text transcriptions and sentiment labels will be as well.

This error propagation similarly applies to the models trained on this data. If the sentiment predictions are 100% accurate but the speech-to-text model performs poorly, then the final pipeline is limited by the initial audio- to- text transcriptions. It is essential that developers consider each model's performance individually and as a component of a larger pipeline. In this particular case, the end goal is to develop a pipeline that can accurately predict the sentiment. Therefore, the overall metric on which to assess the pipeline is the accuracy of the sentiments, which the speech-to-text transcription directly affects.



The NetApp DataOps Toolkit complements the data quality-checking pipeline through the use of its near-instantaneous data cloning technology. Each labeled file must be assessed and compared to the existing labeled files. Distributing these quality checks across various data storage systems ensures that these checks are executed quickly and efficiently.

[Next: Deploying support-center sentiment analysis.](#)

## Deploying support center sentiment analysis

[Previous: Design considerations.](#)

Deploying the solution involves the following components:

1. NetApp DataOps Toolkit
2. NGC Configuration
3. NVIDIA RIVA Server
4. NVIDIA TAO Toolkit
5. Export TAO models to RIVA

To perform deployment, complete the following steps:

### NetApp DataOps Toolkit: Support center sentiment analysis

To use the [NetApp DataOps Toolkit](#), complete the following steps:

1. Pip install the toolkit.

```
python3 -m pip install netapp-dataops-traditional
```

2. Configure the data management

```
netapp_dataops_cli.py config
```

#### NGC configuration: Support center sentiment analysis

To set up [NVIDIA NGC](#), complete the following steps:

1. Download the NGC.

```
wget -O ngccli_linux.zip  
https://ngc.nvidia.com/downloads/ngccli_linux.zip && unzip -o  
ngccli_linux.zip && chmod u+x ngc
```

2. Add your current directory to path.

```
echo "export PATH=\"$PATH:$PWD\" >> ~/.bash_profile && source  
~/.bash_profile
```

3. You must configure NGC CLI for your use so that you can run the commands. Enter the following command, including your API key when prompted.

```
ngc config set
```

For operating systems that are not Linux-based, visit [here](#).

#### NVIDIA RIVA server: Support center sentiment analysis

To set up [NVIDIA RIVA](#), complete the following steps:

1. Download the RIVA files from NGC.

```
ngc registry resource download-version  
nvidia/riva/riva_quickstart:1.4.0-beta
```

2. Initialize the RIVA setup (`riva_init.sh`).
3. Start the RIVA server (`riva_start.sh`).
4. Start the RIVA client (`riva_start_client.sh`).
5. Within the RIVA client, install the audio processing library ([FFMPEG](#))

```
apt-get install ffmpeg
```

6. Start the [Jupyter](#) server.
7. Run the RIVA Inference Pipeline Notebook.

#### NVIDIA TAO Toolkit: Support center sentiment analysis

To set up NVIDIA TAO Toolkit, complete the following steps:

1. Prepare and activate a [virtual environment](#) for TAO Toolkit.
2. Install the [required packages](#).
3. Manually pull the image used during training and fine-tuning.

```
docker pull nvcr.io/nvidia/tao/tao-toolkit-pyt:v3.21.08-py3
```

4. Start the [Jupyter](#) server.
5. Run the TAO Fine-Tuning Notebook.

#### Export TAO models to RIVA: Support center sentiment analysis

To use [TAO Toolkit models in RIVA](#), complete the following steps:

1. Save models within the TAO Fine-Tuning Notebook.
2. Copy TAO trained models to the RIVA model directory.
3. Start the RIVA server (`riva_start.sh`).

#### Deployment roadblocks

Here are a few things to keep in mind as you develop your own solution:

- The NetApp DataOps Toolkit is installed first to ensure that the data storage system runs optimally.
- NVIDIA NGC must be installed before anything else because it authenticates the downloading of images and models.
- RIVA must be installed before the TAO Toolkit. The RIVA installation configures the docker daemon to pull images as needed.
- DGX and docker must have internet access to download the models.

[Next: Validation results.](#)

#### Validation results

[Previous: Deploying support-center sentiment analysis.](#)

As mentioned in the previous section, errors are propagated throughout the pipeline whenever there are two or more machine learning models running in sequence. For this solution, the sentiment of the sentence is the most important factor in measuring the firm's stock risk level. The speech-to-text model, although essential to the pipeline, serves as the preprocessing unit before the sentiments can be predicted. What really matters is the difference in sentiment between the ground truth sentences and the predicted sentences. This serves as a proxy for the word error rate (WER). The speech-to-text accuracy is important, but the WER is not directly used in the final pipeline metric.

```
PIPELINE_SENTIMENT_METRIC = MEAN(DIFF(GT_sentiment, ASR_sentiment))
```

These sentiment metrics can be calculated for the F1 Score, Recall, and Precision of each sentence. The results can be then aggregated and displayed within a confusion matrix, along with the confidence intervals for each metric.

The benefit of using transfer learning is an increase in model performance for a fraction of data requirements, training time, and cost. The fine-tuned models should also be compared to their baseline versions to ensure the transfer learning enhances the performance instead of impairing it. In other words, the fine-tuned model should perform better on the support center data than the pretrained model.

## Pipeline assessment

Test case	Details
Test number	Pipeline sentiment metric
Test prerequisites	Fine-tuned models for speech-to-text and sentiment analysis models
Expected outcome	The sentiment metric of the fine-tuned model performs better than the original pretrained model.

## Pipeline sentiment metric

1. Calculate the sentiment metric for the baseline model.
2. Calculate the sentiment metric for the fine-tuned model.
3. Calculate the difference between those metrics.
4. Average the differences across all sentences.

Next: [Videos and demos](#).

## Videos and demos

Previous: [Validation results](#).

There are two notebooks that contain the sentiment analysis pipeline: "[Support-Center-Model-Transfer-Learning-and-Fine-Tuning.ipynb](#)" and "[Support-Center-Sentiment-Analysis-Pipeline.ipynb](#)". Together, these notebooks demonstrate how to develop a pipeline to ingest support center data and extract sentiments from each sentence using state-of-the-art deep learning models fine-tuned on the user's data.

### Support Center - Sentiment Analysis Pipeline.ipynb

This notebook contains the inference RIVA pipeline for ingesting audio, converting it to text, and extracting sentiments for use in an external dashboard. Dataset are automatically downloaded and processed if this has not already been done. The first section in the notebook is the Speech-to-Text which handles the conversion of audio files to text. This is followed by the Sentiment Analysis section which extracts sentiments for each text sentence and displays those results in a format similar to the proposed dashboard.



This notebook must be run before the model training and fine-tuning because the MP3 dataset must be downloaded and converted into the correct format.

# Call Center - Sentiment Analysis Pipeline

This notebook demonstrates how to build a pipeline for sentiment analysis of call center conversations. The goal of this pipeline is to develop sentiment analysis for use within an external dashboard.

This tutorial will guide you through the use of [NVIDIA's RIVA](#) for automatic speech recognition and text classification. This tutorial uses NetApp cloud storage for data storage and a pre-trained RIVA model.

## Channels

These are the channels on which RIVA is hosting models.

- speech: 51051
- voice: 61051

These channels **must** be aligned with `riva_speech_api_port` and `riva_vision_api_port` within `config.sh`

```
In [4]: speech_channel = "localhost:51051"
voice_channel = "localhost:61051"
```

## Speech-To-Text

Automatic Speech Recognition (ASR) takes as input an audio stream or audio buffer and returns one or more text transcripts, along with additional optional metadata. ASR represents a full speech recognition pipeline that is GPU accelerated with optimized performance and accuracy. ASR supports synchronous and streaming recognition modes.

For more information on NVIDIA RIVA's Automatic Speech Recognition, visit [here](#).

## Constants

Use these constants to affect different aspects of this pipeline:

- `DATA_DIR` : base folder where data is stored
- `DATASET_NAME` : name of the call center dataset
- `COMPANY_DATE` : folder name identifying the particular call center conversation

## Support Center - Model Training and Fine-Tuning.ipynb

The TAO Toolkit virtual environment must be set up before executing the notebook (see the TAO Toolkit section in the Commands Overview for installation instructions).

This notebook relies on the TAO Toolkit to fine-tune deep learning models on the customers data. As with the previous notebook, this one is separated into two sections for the Speech-to-Text and Sentiment Analysis components. Each section goes through data processing, model training and fine-tuning, evaluation of results, and model export. Finally, there is an end section for deploying both your fine-tuned models for use in RIVA.

# Call Center - Model Transfer Learning and Fine-Tuning

TAO Toolkit is a python based AI toolkit for taking purpose-built pre-trained AI models and customizing them with your own data. Transfer learning extracts learned features from an existing neural network to a new one. Transfer learning is often used when creating a large training dataset is not feasible in order to enhance the base performance of state-of-the-art models.

For this call center solution, the speech-to-text and sentiment analysis models are fine-tuned on call center data to augment the model performance on business specific terminology.

For more information on the TAO Toolkit, please visit [here](#).



## Installing necessary dependencies

For ease of use, please install TAO Toolkit inside a python virtual environment. We recommend performing this step first and then launching the notebook from the virtual environment. Please refer to the README for these instructions.

[Next: Conclusion.](#)

## Conclusion

[Previous: Videos and demos.](#)

As customer experience has become increasingly regarded as a key competitive battleground, an AI-augmented global support center becomes a critical component that companies in almost every industry cannot afford to neglect. The solution proposed in this technical report has been demonstrated to support the delivery of such exceptional customer experiences, and the challenge now is to ensure businesses are taking actions to modernize their AI infrastructure and workflows.

The best implementations of AI in customer service are not to replace human agents. Rather, AI can empower them to create exceptional customer experiences via real-time sentiment analysis, dispute escalation, and multimodal affective computing to detect verbal, non-verbal, and facial cues with which comprehensive AI

models can make recommendations at scale and supplement what an individual human agent might be lacking. AI can also provide a better match between a particular customer with currently available agents. Using AI, businesses can extract valuable customer sentiment regarding their thoughts and impressions of the provider's products, services, and brand image.

The solution can also be used to construct time-series data for support agents to serve as an objective performance evaluation metric. Conventional customer satisfaction surveys often lack sufficient responses. By collecting long-term employee and customer sentiment, employers can make informed decisions regarding support agents' performance.

The combination of NetApp, SFL Scientific, open-source orchestration frameworks, and NVIDIA brings the latest technologies together as managed services with great flexibility to accelerate technology adoption and improve the time to market for new AI/ML applications. These advanced services are delivered on-premises that can be easily ported for cloud-native environment as well as hybrid deployment architectures.

Next: [Where to find additional information](#).

## Where to find additional information

Previous: [Conclusion](#).

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

- 3D interactive demos

[www.netapp.com/ai](http://www.netapp.com/ai)

- Connect directly with a NetApp AI specialist

<https://www.netapp.com/artificial-intelligence/>

- NVIDIA Base Command Platform with NetApp solution brief

<https://www.netapp.com/pdf.html?item=/media/32792-DS-4145-NVIDIA-Base-Command-Platform-with-NetApp.pdf>

- NetApp for AI 10 Good Reasons infographic

<https://www.netapp.com/us/media/netapp-ai-10-good-reasons.pdf>

- AI in Healthcare: Deep learning to identify COVID-19 lesions in lung CT scans white paper

<https://www.netapp.com/pdf.html?item=/media/31240-WP-7342.pdf>

- AI in Healthcare: Monitoring face mask usage in healthcare settings white paper

<https://www.netapp.com/pdf.html?item=/media/37490-NA-611-Monitoring-face-mask-usage-in-healthcare-settings.pdf>

- AI in Healthcare: Diagnostic Imaging Technical Report

<https://www.netapp.com/pdf.html?item=/media/7395-tr4811.pdf>

- AI for Retail: NetApp Conversational AI using NVIDIA RIVA

[https://docs.netapp.com/us-en/netapp-solutions/ai/cainvidia\\_executive\\_summary.html](https://docs.netapp.com/us-en/netapp-solutions/ai/cainvidia_executive_summary.html)

- NetApp ONTAP AI solution brief

<https://www.netapp.com/pdf.html?item=/media/6736-sb-3939.pdf>

- NetApp DataOps Toolkit solution brief

<https://www.netapp.com/pdf.html?item=/media/21480-SB-4111-1220-NA-Data-Science-Toolkit.pdf>

- NetApp AI Control Plane solution brief

<https://www.netapp.com/pdf.html?item=/media/6737-sb-4055.pdf>

- Transforming Industry with Data Drive AI eBook

<https://www.netapp.com/us/media/na-337.pdf>

- NetApp EF-Series AI solution brief

<https://www.netapp.com/pdf.html?item=/media/26708-SB-4136-NetApp-AI-E-Series.pdf>

- NetApp AI and Lenovo ThinkSystem for AI Inferencing solution brief

<https://www.netapp.com/pdf.html?item=/media/25316-SB-4129.pdf>

- NetApp AI and Lenovo ThinkSystem for enterprise AI and ML solution brief

<https://www.netapp.com/pdf.html?item=/media/25317-SB-4128.pdf>

- NetApp and NVIDIA – Redefining What is Possible with AI video

<https://www.youtube.com/watch?v=38xw65SteUc>

## Distributed training in Azure - Click-Through Rate Prediction

### TR-4904: Distributed training in Azure - Click-Through Rate Prediction

Rick Huang, Verron Martina, Muneer Ahmad, NetApp

The work of a data scientist should be focused on the training and tuning of machine learning (ML) and artificial intelligence (AI) models. However, according to research by Google, data scientists spend approximately 80% of their time figuring out how to make their models work with enterprise applications and run at scale.

To manage end-to-end AI/ML projects, a wider understanding of enterprise components is needed. Although DevOps have taken over the definition, integration, and deployment, these types of components, ML operations target a similar flow that includes AI/ML projects. To get an idea of what an end-to-end AI/ML pipeline touches in the enterprise, see the following list of required components:

- Storage
- Networking
- Databases
- File systems

- Containers
- Continuous integration and continuous deployment (CI/CD) pipeline
- Integrated development environment (IDE)
- Security
- Data access policies
- Hardware
- Cloud
- Virtualization
- Data science toolsets and libraries

### Target audience

The world of data science touches multiple disciplines in IT and business:

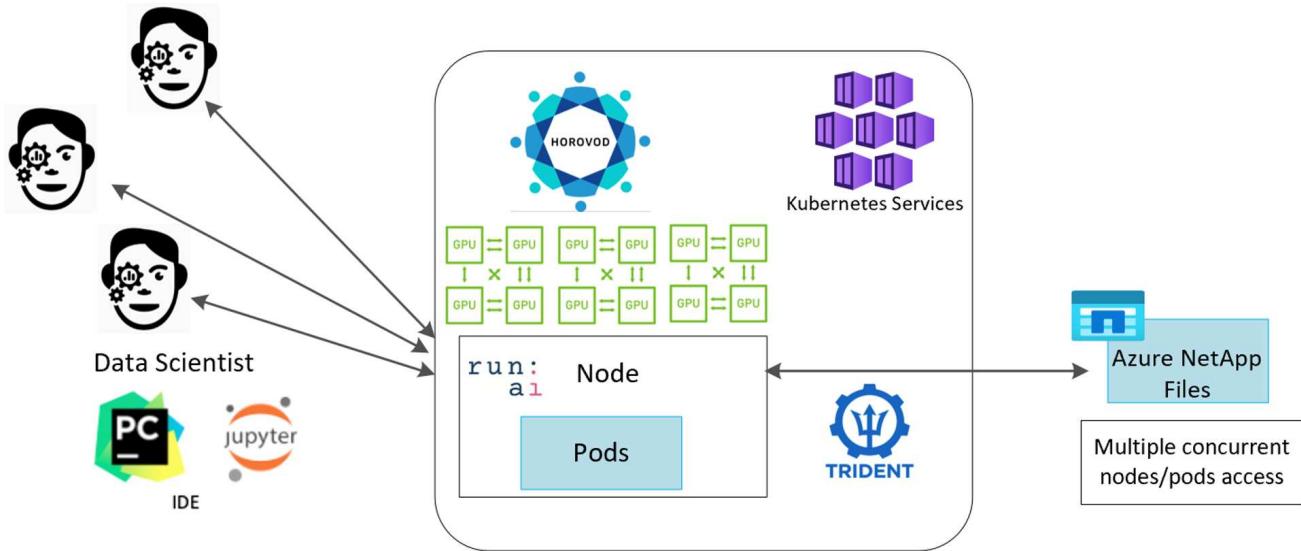
- The data scientist needs the flexibility to use their tools and libraries of choice.
- The data engineer needs to know how the data flows and where it resides.
- A DevOps engineer needs the tools to integrate new AI/ML applications into their CI/CD pipelines.
- Cloud administrators and architects need to be able to set up and manage Azure resources.
- Business users want to have access to AI/ML applications.

In this technical report, we describe how Azure NetApp Files, RAPIDS AI, Dask, and Azure help each of these roles bring value to business.

### Solution overview

This solution follows the lifecycle of an AI/ML application. We start with the work of data scientists to define the different steps needed to prepare data and train models. By leveraging RAPIDS on Dask, we perform distributed training across the Azure Kubernetes Service (AKS) cluster to drastically reduce the training time when compared to the conventional Python scikit-learn approach. To complete the full cycle, we integrate the pipeline with Azure NetApp Files.

Azure NetApp Files provides various performance tiers. Customers can start with a Standard tier and scale out and scale up to a high-performance tier nondisruptively without moving any data. This capability enables data scientists to train models at scale without any performance issues, avoiding any data silos across the cluster, as shown in figure below.



[Next: Technology overview.](#)

## Technology overview

[Previous: Introduction.](#)

### Microsoft and NetApp

Since May 2019, Microsoft has delivered an Azure native, first-party portal service for enterprise NFS and SMB file services based on NetApp ONTAP technology. This development is driven by a strategic partnership between Microsoft and NetApp and further extends the reach of world-class ONTAP data services to Azure.

### Azure NetApp Files

The Azure NetApp Files service is an enterprise-class, high-performance, metered file storage service. Azure NetApp Files supports any workload type and is highly available by default. You can select service and performance levels and set up Snapshot copies through the service. Azure NetApp Files is an Azure first-party service for migrating and running the most demanding enterprise-file workloads in the cloud, including databases, SAP, and high-performance computing applications with no code changes.

This reference architecture gives IT organizations the following advantages:

- Eliminates design complexities
- Enables independent scaling of compute and storage
- Enables customers to start small and scale seamlessly
- Offers a range of storage tiers for various performance and cost points

### Dask and NVIDIA RAPIDS overview

Dask is an open-source, parallel computing tool that scales Python libraries on multiple machines and provides faster processing of large amounts of data. It provides an API similar to single-threaded conventional Python libraries, such as Pandas, Numpy, and scikit-learn. As a result, native Python users are not forced to change much in their existing code to use resources across the cluster.

NVIDIA RAPIDS is a suite of open-source libraries that makes it possible to run end-to-end ML and data

analytics workflows entirely on GPUs. Together with Dask, it enables you to easily scale from GPU workstation (scale up) to multinode, multi-GPU clusters (scale out).

For deploying Dask on a cluster, you could use Kubernetes for resource orchestration. You could also scale up or scale down the worker nodes as per the process requirement, which in-turn can help to optimize the cluster resource consumption, as shown in the following figure.



[Next: Software requirements.](#)

## Software requirements

[Previous: Technology overview.](#)

The following table lists the software requirements needed for this solution.

Software	Version
Azure Kubernetes Service	1.18.14
RAPIDS and Dask container image	Repository: "rapidsai/rapidsai" Tag: 0.17-cuda11.0-runtime-ubuntu18.04
NetApp Trident	20.01.1
Helm	3.0.0

[Next: Cloud resource requirements.](#)

## Cloud resource requirements

[Previous: Software requirements.](#)

## Configure Azure NetApp Files

Configure Azure NetApp Files as described in [QuickStart: Set up Azure NetApp Files and create an NFS volume](#).

You can proceed past the section “Create NFS volume for Azure NetApp Files” because you are going to create volumes through Trident. Before continuing, complete the following steps:

1. Register for Azure NetApp Files and NetApp Resource Provider (through the Azure Shell) ([link](#)).
2. Create an account in Azure NetApp Files ([link](#)).
3. Set up a capacity pool (a minimum 4TB Standard or Premium, depending on your need) ([link](#)). The following table lists the network configuration requirements for setting up in the cloud. The Dask cluster and Azure NetApp Files must be in the same Azure Virtual Network (VNet) or a peered VNet.

Resources	Type/version
Azure Kubernetes Service	1.18.14
Agent node	3x Standard_DS2_v2
GPU node	3x Standard_NC6s_v3
Azure NetApp Files	Standard capacity pool
Capacity in TB	4

Next: [Click-through rate prediction use case summary](#).

## Click-through rate prediction use case summary

Previous: [Cloud resource requirements](#).

This use case is based on the publicly available [Terabyte Click Logs](#) dataset from [Criteo AI Lab](#). With the recent advances in ML platforms and applications, a lot of attention is now on learning at scale. The click-through rate (CTR) is defined as the average number of click-throughs per hundred online ad impressions (expressed as a percentage). It is widely adopted as a key metric in various industry verticals and use cases, including digital marketing, retail, e-commerce, and service providers. Examples of using CTR as an important metric for potential customer traffic include the following:

- **Digital marketing:** In [Google Analytics](#), CTR can be used to gauge how well an advertiser or merchant’s keywords, ads, and free listings are performing. A high CTR is a good indication that users find your ads and listings helpful and relevant. CTR also contributes to your keyword’s expected CTR, which is a component of [Ad Rank](#).
- **E-commerce:** In addition to leveraging [Google Analytics](#), there are at least some visitor statistics in an e-commerce backend. Although these statistics might not seem useful at first glance, they are typically easy to read and might be more accurate than other information. First-party datasets composed of such statistics are proprietary and are therefore the most relevant to e-commerce sellers, buyers, and platforms. These datasets can be used for setting benchmarks, comparing results to last year and yesterday by constructing a time-series for further analysis.
- **Retail:** Brick-and-mortar retailers can correlate the number of visitors and the number of customers to the CTR. The number of customers can be seen from their point-of-sale history. The CTR from retailers’ websites or ad traffic might result in the aforementioned sales. Loyalty programs are another use case, because customers redirected from online ads or other websites might join to earn rewards. Retailers can acquire customers via loyalty programs and record behaviors from sales histories to build a recommendation system that not only predicts consumer buying behaviors in different categories but also

personalizes coupons and decreases churn.

- **Service providers:** Telecommunication companies and internet service providers have an abundance of first-party user telemetry data for insightful AI, ML, and analytics use cases. For example, a telecom can leverage its mobile subscribers' web browsing top level domain history logs daily to fine-tune existing models to produce up-to-date audience segmentation, predict customer behavior, and collaborate with advertisers to place real-time ads for better online experience. In such data-driven marketing workflow, CTR is an important metric to reflect conversions.

In the context of digital marketing, [Criteo Terabyte Click Logs](#) are now the dataset of reference in assessing the scalability of ML platforms and algorithms. By predicting the click-through rate, an advertiser can select the visitors who are most likely to respond to the ads, analyze their browsing history, and show the most relevant ads based on the interests of the user.

The solution provided in this technical report highlights the following benefits:

- Azure NetApp Files advantages in distributed or large-scale training
- RAPIDS CUDA-enabled data processing (cuDF, cuPy, and so on) and ML algorithms (cuML)
- The Dask parallel computing framework for distributed training

An end-to-end workflow built on RAPIDS AI and Azure NetApp Files demonstrates the drastic improvement in random forest model training time by two orders of magnitude. This improvement is significant comparing to the conventional Pandas approach when dealing with real-world click logs with 45GB of structured tabular data (on average) each day. This is equivalent to a DataFrame containing roughly twenty billion rows. We will demonstrate cluster environment setup, framework and library installation, data loading and processing, conventional versus distributed training, visualization and monitoring, and compare critical end-to-end runtime results in this technical report.

[Next: Install and set up the aks cluster.](#)

## Setup

### Install and set up the AKS cluster

[Previous: Click-through rate prediction use case summary.](#)

To install and set up the AKS cluster, see the webpage [Create an AKS Cluster](#) and then complete the following steps:

1. When selecting the type of node (system [CPU] or worker [GPU] nodes), select the following:
  - a. Primary system nodes should be Standard DS2v2 (agentpool default three nodes).
  - b. Then add the worker node Standard\_NC6s\_v3 pool (three nodes minimum) for the user group (for GPU nodes) named gppool.

Add node pool				
Name	Mode	OS type	Node count	Node size
agentpool	System	Linux	3	Standard_DS2_v2
gppool	User	Linux	3	Standard_NC6s_v3

2. Deployment takes 5 to 10 minutes. After it is complete, click Connect to Cluster.
3. To connect to the newly created AKS cluster, install the following from your local environment (laptop/pc):
  - a. The Kubernetes command-line tool using the [instructions provided for your specific OS](#)
  - b. The Azure CLI as described in the document, [Install the Azure CLI](#)
4. To access the AKS cluster from the terminal, enter `az login` and enter the credentials.
5. Run the following two commands:

```
az account set --subscription xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
aks get-credentials --resource-group resourcegroup --name aksclustername
```

6. Enter Azure CLI: `kubectl get nodes`.
7. If all six nodes are up and running, as shown in the following example, your AKS cluster is ready and connected to your local environment

```
verronmartina@verron-mac-0 ~ % kubectl get nodes
NAME                               STATUS   ROLES   AGE     VERSION
aks-agentpool-34613062-vmss00000   Ready    agent   22m    v1.18.14
aks-agentpool-34613062-vmss00001   Ready    agent   22m    v1.18.14
aks-agentpool-34613062-vmss00002   Ready    agent   22m    v1.18.14
aks-gpupool-34613062-vmss00000   Ready    agent   20m    v1.18.14
aks-gpupool-34613062-vmss00001   Ready    agent   20m    v1.18.14
aks-gpupool-34613062-vmss00002   Ready    agent   20m    v1.18.14
verronmartina@verron-mac-0 ~ %
```

[Next: Create a delegated subnet for Azure NetApp Files.](#)

[Create a delegated subnet for Azure NetApp Files](#)

[Previous: Install and set up the AKS cluster.](#)

To create a delegated subnet for Azure NetApp Files, complete the following steps:

1. Navigate to Virtual Networks within the Azure portal. Find your newly created virtual network. It should have a prefix such as `aks-vnet`.
2. Click the name of the VNet.



Dashboard >

## Virtual networks

X

seanlucealive (Default Directory)



Manage view



Refresh



Export to CSV



Open query



Assign tags



Feedback

Filter by name...

Subscription == AzureSub01

Resource group == all

Location == all

+ Add filter

Showing 1 to 5 of 5 records.

No grouping

List view

Name ↑↓

Resource group ↑↓

Location ↑↓

Subscription ↑↓

aks-vnet-22885919

MC\_sluce.rg\_TridentDemo\_eastus2

East US 2

AzureSub01

...

3. Click Subnets and click +Subnet from the top toolbar.

The screenshot shows the 'aks-vnet-22885919 | Subnets' page. The top navigation bar includes 'Microsoft Azure', a search bar, and user profile icons. The left sidebar lists options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Address space, Connected devices, and Subnets (which is highlighted with a red box). The main content area shows a table of subnets. The first column is 'Name ↑↓' with 'aks-subnet' listed. The second column is 'IPv4 ↑↓' with '10.240.0.0/16 (65530 av... -)'. The third column is 'IPv6 (many availab... ↑↓' with '-'. The fourth column is 'Delegated to ↑↓' with '-'. The fifth column is 'Security group ↑↓' with 'aks-agentpool-2288591... \*\*\*'. A red box highlights the '+ Subnet' button in the toolbar at the top of the subnet list.

4. Provide the subnet with a name such as ANF.sn and, under the Subnet Delegation heading, select Microsoft.Netapp/volumes. Do not change anything else. Click OK.

## Add subnet

X

Name \*

ANF.sn



Subnet address range \* ⓘ

10.0.0.0/24

10.0.0.0 - 10.0.0.255 (251 + 5 Azure reserved addresses)

Add IPv6 address space ⓘ

NAT gateway ⓘ

None



Network security group

None



Route table

None



### SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

0 selected



### SUBNET DELEGATION

Delegate subnet to a service ⓘ

Microsoft.Netapp/volumes



OK

Cancel

Azure NetApp Files volumes are allocated to the application cluster and are consumed as persistent volume claims (PVCs) in Kubernetes. In turn, this process provides you the flexibility to map them to different services, such as Jupyter notebooks, serverless functions, and so on.

Users of services can consume storage from the platform in many ways. As this technical report discusses NFSs, the main benefits of Azure NetApp Files are:

- Providing users with the ability to use Snapshot copies.
- Enabling users to store large quantities of data on Azure NetApp Files volumes.
- Using the performance benefits of Azure NetApp Files volumes when running their models on large sets of files.

Next: Peer AKS vnet and Azure NetApp Files vnet.

## Peer AKS VNet and Azure NetApp Files VNet

Previous: [Create a delegated subnet for Azure NetApp Files.](#)

To peer the AKS VNet to the Azure NetApp Files VNet, complete the following steps:

1. Enter Virtual Networks in the search field.
2. Select `vnet aks-vnet-name`. Click it and enter Peerings in the search field.
3. Click +Add.
4. Enter the following descriptors:
  - a. The peering link name is `aks-vnet-name_to_anf`.
  - b. subscriptionID and Azure NetApp Files VNet as the VNet peering partner.
  - c. Leave all the nonasterisk sections with the default values.
5. Click Add.

For more information, see [Create, change, or delete a virtual network peering](#).

Next: [Install Trident](#).

## Install Trident

Previous: [Peer AKS VNet and Azure NetApp Files VNet](#).

To install Trident using Helm, complete the following steps:

1. Install Helm (for installation instructions, visit the [source](#)).
2. Download and extract the Trident 20.01.1 installer.

```
$ wget  
$ tar -xf trident-installer-21.01.1.tar.gz
```

3. Change the directory to `trident-installer`.

```
$ cd trident-installer
```

4. Copy `tridentctl` to a directory in your system \$PATH.

```
$ sudo cp ./tridentctl /usr/local/bin
```

5. Install Trident on the Kubernetes (K8s) cluster with Helm ([source](#)):

- a. Change the directory to the `helm` directory.

```
$ cd helm
```

b. Install Trident.

```
$ helm install trident trident-operator-21.01.1.tgz --namespace  
trident --create-namespace
```

c. Check the status of Trident pods.

```
$ kubectl -n trident get pods
```

If all the pods are up and running, then Trident is installed and you can move forward.

6. Set up the Azure NetApp Files backend and storage class for AKS.

a. Create an Azure Service Principle.

The service principal is how Trident communicates with Azure to manipulate your Azure NetApp Files resources.

```
$ az ad sp create-for-rbac --name ""
```

The output should look like the following example:

```
{  
  "appId": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",  
  "displayName": "netapptrident",  
  "name": "",  
  "password": "xxxxxxxxxxxxxxxx.xxxxxxxxxxxxxx",  
  "tenant": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"  
}
```

7. Create a Trident backend json file, example name anf-backend.json.

8. Using your preferred text editor, complete the following fields inside the anf-backend.json file:

```
{
    "version": 1,
    "storageDriverName": "azure-netapp-files",
    "subscriptionID": "fakec765-4774-fake-ae98-a721add4fake",
    "tenantID": "fakef836-edc1-fake-bff9-b2d865eefake",
    "clientID": "fake0f63-bf8e-fake-8076-8de91e57fake",
    "clientSecret": "SECRET",
    "location": "westeurope",
    "serviceLevel": "Standard",
    "virtualNetwork": "anf-vnet",
    "subnet": "default",
    "nfsMountOptions": "vers=3,proto=tcp",
    "limitVolumeSize": "500Gi",
    "defaults": {
        "exportRule": "0.0.0.0/0",
        "size": "200Gi"
    }
}
```

9. Substitute the following fields:

- **subscriptionID**. Your Azure subscription ID.
- **tenantID**. Your Azure Tenant ID from the output of `az ad sp` in the previous step.
- **clientID**. Your appID from the output of `az ad sp` in the previous step.
- **clientSecret**. Your password from the output of `az ad sp` in the previous step.

10. Instruct Trident to create the Azure NetApp Files backend in the `trident` namespace using `anf-backend.json` as the configuration file:

```
$tridentctl create backend -f anf-backend.json -n trident
```

NAME	STORAGE DRIVER	UUID	STATE	VOLUMES
azurenappfiles_86181	azure-netapp-files	2ca85462-59ac-4946-be05-c03f5575a2ad	online	0

11. Create a storage class. Kubernetes users provision volumes by using PVCs that specify a storage class by name. Instruct K8s to create a storage class `azurenappfiles` that references the Trident backend created in the previous step.

12. Create a YAML (`anf-storage-class.yaml`) file for storage class and copy.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: azurenetaappfiles
  provisioner: netapp.io/trident
  parameters:
    backendType: "azure-netapp-files"
$kubectl create -f anf-storage-class.yaml
```

13. Verify that the storage class was created.

```
kubectl get sc azurenetaappfiles
```

NAME	PROVISIONER	RECLAIMPOLICY	VOLUMEBINDINGMODE	ALLOWVOLUMEEXPANSION	AGE
azurenetaappfiles	csi.trident.netapp.io	Delete	Immediate	false	98s

Next: Set up Dask with RAPIDS deployment on AKS using Helm.

#### **Set up Dask with RAPIDS deployment on AKS using Helm**

[Previous: Install Trident.](#)

To set up Dask with RAPIDS deployment on AKS using Helm, complete the following steps:

1. Create a namespace for installing Dask with RAPIDS.

```
kubectl create namespace rapids-dask
```

2. Create a PVC to store the click-through rate dataset:

- a. Save the following YAML content to a file to create a PVC.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-criteo-data
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Gi
  storageClassName: azurenetaappfiles
```

- b. Apply the YAML file to your Kubernetes cluster.

```
kubectl -n rapids-dask apply -f <your yaml file>
```

3. Clone the `rapidsai` git repository (<https://github.com/rapidsai/helm-chart>).

```
git clone https://github.com/rapidsai/helm-chart helm-chart
```

4. Modify `values.yaml` and include the PVC created earlier for workers and Jupyter workspace.

- a. Go to the `rapidsai` directory of the repository.

```
cd helm-chart/rapidsai
```

- b. Update the `values.yaml` file and mount the volume using PVC.

```
dask:  
...  
worker:  
  name: worker  
...  
  mounts:  
    volumes:  
      - name: data  
        persistentVolumeClaim:  
          claimName: pvc-criteo-data  
    volumeMounts:  
      - name: data  
        mountPath: /data  
...  
jupyter:  
  name: jupyter  
...  
  mounts:  
    volumes:  
      - name: data  
        persistentVolumeClaim:  
          claimName: pvc-criteo-data  
    volumeMounts:  
      - name: data  
        mountPath: /data  
...
```

5. Go to the repository's home directory and deploy Dask with three worker nodes on AKS using Helm.

```
cd ..  
helm dep update rapidsai  
helm install rapids-dask --namespace rapids-dask rapidsai
```

[Next: Azure NetApp Files performance tiers.](#)

#### Azure NetApp Files performance tiers

[Previous: Set up Dask with RAPIDS deployment on AKS using Helm.](#)

You can change the service level of an existing volume by moving the volume to another capacity pool that uses the service level you want for the volume. This solution enables customers to start with a small dataset and small number of GPUs in Standard Tier and scale out or scale up to Premium Tier as the amount of data and GPUs increase. The Premium Tier offers four times the throughput per terabyte as the Standard Tier, and scale up is performed without having to move any data to change the service level of a volume.

#### Dynamically change the service level of a volume

To dynamically change the service level of a volume, complete the following steps:

1. On the Volumes page, right-click the volume whose service level you want to change. Select Change Pool.

Name	Path	Service Level	Capacity Pool	Actions
NFSv3	10.28.254.4:/norootfor...	Standard	pool0	...
NFSv4.1	NAS-735a.docs.lab:/for...	Premium	pool0	Resize 
NFSv4.1	NAS-735a.docs.lab:/krt...	Premium	pool0	Edit 
NFSv3	10.28.254.4:/moveme0...	Premium	pool0	Change pool 
NFSv3	10.28.254.4:/placeholder...	Premium	pool0	Delete 

2. In the Change Pool window, select the capacity pool to which you want to move the volume.



3. Click OK.

## Automate performance tier change

The following options are available to automate performance tier changes:

- Dynamic Service Level change is still in Public Preview at this time and not enabled by default. To enable this feature on the Azure Subscription, see this documentation about how to [Dynamically change the service level of a volume](#).
- Azure CLI volume pool change commands are provided in [volume pool change documentation](#) and in the following example:

```
az netappfiles volume pool-change -g mygroup --account-name myaccname  
--pool-name mypoolname --name myvolname --new-pool-resource-id  
mynewresourceid
```

- PowerShell: The [Set-AzNetAppFilesVolumePool cmdlet](#) changes the pool of an Azure NetApp Files volume and is shown in the following example:

```

Set-AzNetAppFilesVolumePool
-ResourceGroupName "MyRG"
-AccountName "MyAnfAccount"
-PoolName "MyAnfPool"
-Name "MyAnfVolume"
-NewPoolResourceId 7d6e4069-6c78-6c61-7bf6-c60968e45fbf

```

[Next: Libraries for data processing and model training.](#)

## Click through rate prediction data processing and model training

### Libraries for data processing and model training

[Previous: Azure NetApp Files performance tiers.](#)

The following table lists the libraries and frameworks that were used to build this task. All these components have been fully integrated with Azure's role-based access and security controls.

Libraries/framework	Description
Dask cuML	For ML to work on GPU, the <a href="#">cuML library</a> provides access to the RAPIDS cuML package with Dask. RAPIDS cuML implements popular ML algorithms, including clustering, dimensionality reduction, and regression approaches, with high-performance GPU-based implementations, offering speed-ups of up to 100x over CPU-based approaches.
Dask cuDF	cuDF includes various other functions supporting GPU-accelerated extract, transform, load (ETL), such as data subsetting, transformations, one-hot encoding, and more. The RAPIDS team maintains a <a href="#">dask-cudf library</a> that includes helper methods to use Dask and cuDF.
Scikit Learn	Scikit-learn provides dozens of built-in machine learning algorithms and models, called estimators. Each <a href="#">estimator</a> can be fitted to some data using its <a href="#">fit</a> method.

We used two notebooks to construct the ML pipelines for comparison; one is the conventional Pandas scikit-learn approach, and the other is distributed training with RAPIDS and Dask. Each notebook can be tested individually to see the performance in terms of time and scale. We cover each notebook individually to demonstrate the benefits of distributed training using RAPIDS and Dask.

[Next: Load Criteo Click Logs day 15 in Pandas and train a scikit-learn random forest model.](#)

### Load Criteo Click Logs day 15 in Pandas and train a scikit-learn random forest model

[Previous: Libraries for data processing and model training.](#)

This section describes how we used Pandas and Dask DataFrames to load Click Logs data from the Criteo

Terabyte dataset. The use case is relevant in digital advertising for ad exchanges to build users' profiles by predicting whether ads will be clicked or if the exchange isn't using an accurate model in an automated pipeline.

We loaded day 15 data from the Click Logs dataset, totaling 45GB. Running the following cell in Jupyter notebook CTR-PandasRF-collated.ipynb creates a Pandas DataFrame that contains the first 50 million rows and generates a scikit-learn random forest model.

```
%%time
import pandas as pd
import numpy as np
header = ['col'+str(i) for i in range (1,41)] #note that according to
criteo, the first column in the dataset is Click Through (CT). Consist of
40 columns
first_row_taken = 50_000_000 # use this in pd.read_csv() if your compute
resource is limited.
# total number of rows in day15 is 20B
# take 50M rows
"""
Read data & display the following metrics:
1. Total number of rows per day
2. df loading time in the cluster
3. Train a random forest model
"""
df = pd.read_csv(file, nrows=first_row_taken, delimiter='\t',
names=header)
# take numerical columns
df_sliced = df.iloc[:, 0:14]
# split data into training and Y
Y = df_sliced.pop('col1') # first column is binary (click or not)
# change df_sliced data types & fillna
df_sliced = df_sliced.astype(np.float32).fillna(0)
from sklearn.ensemble import RandomForestClassifier
# Random Forest building parameters
# n_streams = 8 # optimization
max_depth = 10
n_bins = 16
n_trees = 10
rf_model = RandomForestClassifier(max_depth=max_depth,
n_estimators=n_trees)
rf_model.fit(df_sliced, Y)
```

To perform prediction by using a trained random forest model, run the following paragraph in this notebook. We took the last one million rows from day 15 as the test set to avoid any duplication. The cell also calculates accuracy of prediction, defined as the percentage of occurrences the model accurately predicts whether a user clicks an ad or not. To review any unfamiliar components in this notebook, see the [official scikit-learn documentation](#).

```

# testing data, last 1M rows in day15
test_file = '/data/day_15_test'
with open(test_file) as g:
    print(g.readline())

# DataFrame processing for test data
test_df = pd.read_csv(test_file, delimiter='\t', names=header)
test_df_sliced = test_df.iloc[:, 0:14]
test_Y = test_df_sliced.pop('col1')
test_df_sliced = test_df_sliced.astype(np.float32).fillna(0)
# prediction & calculating error
pred_df = rf_model.predict(test_df_sliced)
from sklearn import metrics
# Model Accuracy
print("Accuracy:",metrics.accuracy_score(test_Y, pred_df))

```

[Next: Load Day 15 in Dask and train a Dask cuML random forest model.](#)

[Load Day 15 in Dask and train a Dask cuML random forest model](#)

[Previous: Load Criteo Click Logs day 15 in Pandas and train a scikit-learn random forest model.](#)

In a manner similar to the previous section, load Criteo Click Logs day 15 in Pandas and train a scikit-learn random forest model. In this example, we performed DataFrame loading with Dask cuDF and trained a random forest model in Dask cuML. We compared the differences in training time and scale in the section [“Training time comparison.”](#)

### criteo\_dask\_RF.ipynb

This notebook imports numpy, cuml, and the necessary dask libraries, as shown in the following example:

```

import cuml
from dask.distributed import Client, progress, wait
import dask_cudf
import numpy as np
import cudf
from cuml.dask.ensemble import RandomForestClassifier as cumlDaskRF
from cuml.dask.common import utils as dask_utils

```

Initiate Dask Client().

```
client = Client()
```

If your cluster is configured correctly, you can see the status of worker nodes.

```
client
workers = client.has_what().keys()
n_workers = len(workers)
n_streams = 8 # Performance optimization
```

In our AKS cluster, the following status is displayed:

Client	Cluster
<b>Scheduler:</b> tcp://rapidsai-scheduler:8786	<b>Workers:</b> 3
<b>Dashboard:</b> <a href="#">/proxy/rapidsai-scheduler:8787/status</a>	<b>Cores:</b> 3
	<b>Memory:</b> 354.55 GB

Note that Dask employs the lazy execution paradigm: rather than executing the processing code instantly, Dask builds a Directed Acyclic Graph (DAG) of execution instead. DAG contains a set of tasks and their interactions that each worker needs to run. This layout means the tasks do not run until the user tells Dask to execute them in one way or another. With Dask you have three main options:

- **Call compute() on a DataFrame.** This call processes all the partitions and then returns results to the scheduler for final aggregation and conversion to cuDF DataFrame. This option should be used sparingly and only on heavily reduced results unless your scheduler node runs out of memory.
- **Call persist() on a DataFrame.** This call executes the graph, but, instead of returning the results to the scheduler node, it maintains them across the cluster in memory so the user can reuse these intermediate results down the pipeline without the need for rerunning the same processing.
- **Call head() on a DataFrame.** Just like with cuDF, this call returns 10 records back to the scheduler node. This option can be used to quickly check if your DataFrame contains the desired output format, or if the records themselves make sense, depending on your processing and calculation.

Therefore, unless the user calls either of these actions, the workers sit idle waiting for the scheduler to initiate the processing. This lazy execution paradigm is common in modern parallel and distributed computing frameworks such as Apache Spark.

The following paragraph trains a random forest model by using Dask cuML for distributed GPU-accelerated computing and calculates model prediction accuracy.

```

Adsf
# Random Forest building parameters
n_streams = 8 # optimization
max_depth = 10
n_bins = 16
n_trees = 10
cuml_model = cumlDaskRF(max_depth=max_depth, n_estimators=n_trees,
n_bins=n_bins, n_streams=n_streams, verbose=True, client=client)
cuml_model.fit(gdf_sliced_small, Y)
# Model prediction
pred_df = cuml_model.predict(gdf_test)
# calculate accuracy
cu_score = cuml.metrics.accuracy_score( test_y, pred_df )

```

[Next: Monitor Dask using native Task Streams dashboard.](#)

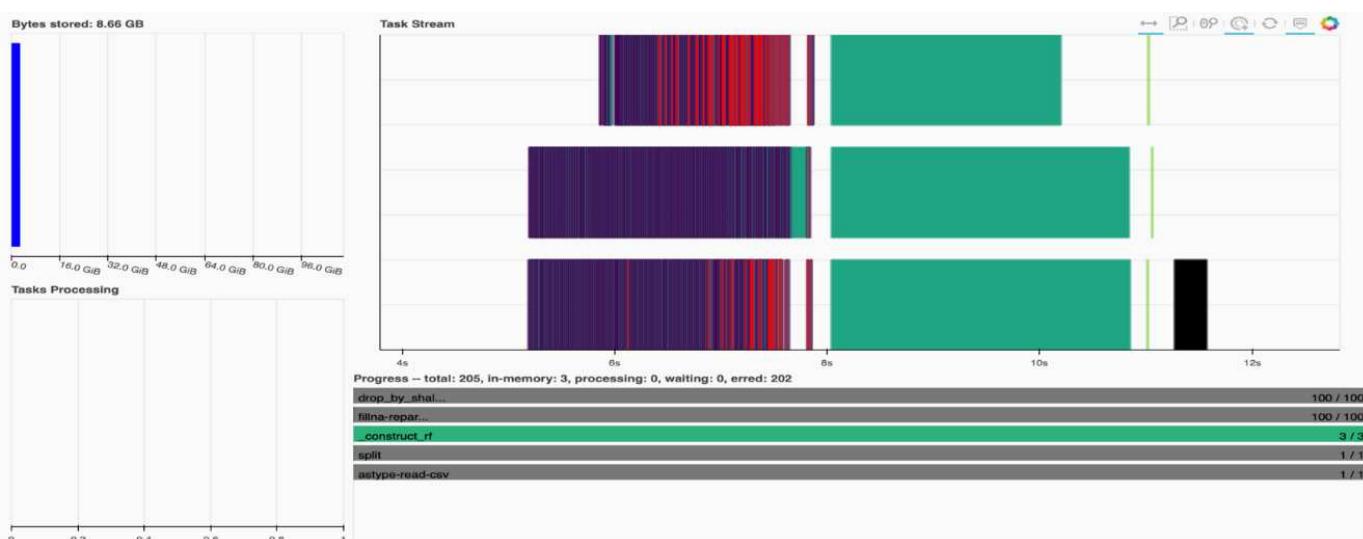
#### Monitor Dask using native Task Streams dashboard

[Previous: Load Day 15 in Dask and train a Dask cuML random forest model.](#)

The [Dask distributed scheduler](#) provides live feedback in two forms:

- An interactive dashboard containing many plots and tables with live information
- A progress bar suitable for interactive use in consoles or notebooks

In our case, the following figure shows how you can monitor the task progress, including Bytes Stored, the Task Stream with a detailed breakdown of the number of streams, and Progress by task names with associated functions executed. In our case, because we have three worker nodes, there are three main chunks of stream and the color codes denote different tasks within each stream.



You have the option to analyze individual tasks and examine the execution time in milliseconds or identify any obstacles or hindrances. For example, the following figure shows the Task Streams for the random forest model fitting stage. There are considerably more functions being executed, including unique chunk for DataFrame processing, `_construct_rf` for fitting the random forest, and so on. Most of the time was spent on

DataFrame operations due to the large size (45GB) of one day of data from the Criteo Click Logs.



[Next: Training time comparison.](#)

### Training time comparison

[Previous: Monitor Dask using native Task Streams dashboard.](#)

This section compares the model training time using conventional Pandas compared to Dask. For Pandas, we loaded a smaller amount of data due to the nature of slower processing time to avoid memory overflow. Therefore, we interpolated the results to offer a fair comparison.

The following table shows the raw training time comparison when there is significantly less data used for the Pandas random forest model (50 million rows out of 20 billion per day15 of the dataset). This sample is only using less than 0.25% of all available data. Whereas for Dask-cuML we trained the random forest model on all 20 billion available rows. The two approaches yielded comparable training time.

Approach	Training time
Scikit-learn: Using only 50M rows in day15 as the training data	47 minutes and 21 seconds
RAPIDS-Dask: Using all 20B rows in day15 as the training data	1 hour, 12 minutes, and 11 seconds

If we interpolate the training time results linearly, as shown in the following table, there is a significant advantage to using distributed training with Dask. It would take the conventional Pandas scikit-learn approach 13 days to process and train 45GB of data for a single day of click logs, whereas the RAPIDS-Dask approach processes the same amount of data 262.39 times faster.

Approach	Training time
Scikit-learn: Using all 20B rows in day15 as the training data	13 days, 3 hours, 40 minutes, and 11 seconds
RAPIDS-Dask: Using all 20B rows in day15 as the training data	1 hour, 12 minutes, and 11 seconds

In the previous table, you can see that by using RAPIDS with Dask to distribute the data processing and model training across multiple GPU instances, the run time is significantly shorter compared to conventional Pandas DataFrame processing with scikit-learn model training. This framework enables scaling up and out in the cloud as well as on-premises in a multinode, multi-GPU cluster.

[Next: Monitor Dask and RAPIDS with Prometheus and Grafana.](#)

#### **Monitor Dask and RAPIDS with Prometheus and Grafana**

[Previous: Training time comparison.](#)

After everything is deployed, run inferences on new data. The models predict whether a user clicks an ad based on browsing activities. The results of the prediction are stored in a Dask cuDF. You can monitor the results with Prometheus and visualize in Grafana dashboards.

For more information, see this [RAPIDS AI Medium post](#).

[Next: Dataset and Model Versioning using NetApp DataOps Toolkit.](#)

#### **Dataset and model versioning using NetApp DataOps Toolkit**

[Previous: Monitor Dask and RAPIDS with Prometheus and Grafana.](#)

The NetApp DataOps Toolkit for Kubernetes abstracts storage resources and Kubernetes workloads up to the data-science workspace level. These capabilities are packaged in a simple, easy-to-use interface that is designed for data scientists and data engineers. Using the familiar form of a Python program, the Toolkit enables data scientists and engineers to provision and destroy JupyterLab workspaces in just seconds. These workspaces can contain terabytes, or even petabytes, of storage capacity, enabling data scientists to store all their training datasets directly in their project workspaces. Gone are the days of separately managing workspaces and data volumes.

For more information, visit the Toolkit's [GitHub repository](#).

[Next: Conclusion.](#)

#### **Jupyter notebooks for reference**

[Previous: Dataset and Model Versioning using NetApp DataOps Toolkit.](#)

There are two Jupyter notebooks associated with this technical report:

- **CTR-PandasRF-collated.ipynb.** This notebook loads Day 15 from the Criteo Terabyte Click Logs dataset, processes and formats data into a Pandas DataFrame, trains a Scikit-learn random forest model, performs prediction, and calculates accuracy.
- **criteo\_dask\_RF.ipynb.** This notebook loads Day 15 from the Criteo Terabyte Click Logs dataset, processes and formats data into a Dask cuDF, trains a Dask cuML random forest model, performs prediction, and calculates accuracy. By leveraging multiple worker nodes with GPUs, this distributed data and model processing and training approach is highly efficient. The more data you process, the greater the time savings versus a conventional ML approach. You can deploy this notebook in the cloud, on-premises, or in a hybrid environment where your Kubernetes cluster contains compute and storage in different locations, as long as your networking setup enables the free movement of data and model distribution.

[Next: Conclusion.](#)

## Conclusion

Previous: [Dataset and Model Versioning using NetApp DataOps Toolkit.](#)

Azure NetApp Files, RAPIDS, and Dask speed up and simplify the deployment of large-scale ML processing and training by integrating with orchestration tools such as Docker and Kubernetes. By unifying the end-to-end data pipeline, this solution reduces the latency and complexity inherent in many advanced computing workloads, effectively bridging the gap between development and operations. Data scientists can run queries on large datasets and securely share data and algorithmic models with other users during the training phase.

When building your own AI/ML pipelines, configuring the integration, management, security, and accessibility of the components in an architecture is a challenging task. Giving developers access and control of their environment presents another set of challenges.

By building an end-to-end distributed training model and data pipeline in the cloud, we demonstrated two orders of magnitude improvement in total workflow completion time versus a conventional, open-source approach that did not leverage GPU-accelerated data processing and compute frameworks.

The combination of NetApp, Microsoft, opens-source orchestration frameworks, and NVIDIA brings the latest technologies together as managed services with great flexibility to accelerate technology adoption and improve the time to market for new AI/ML applications. These advanced services are delivered in a cloud-native environment that can be easily ported for on-premises as well as hybrid deployment architectures.

Next: [Where to find additional information.](#)

## Where to find additional information

Previous: [Conclusion.](#)

To learn more about the information that is described in this document, see the following resources:

- Azure NetApp Files:

- Solutions architecture page for Azure NetApp Files

<https://docs.microsoft.com/azure/azure-netapp-files/azure-netapp-files-solution-architectures>

- Trident persistent storage for containers:

- Azure NetApp Files and Trident

<https://netapptrident.readthedocs.io/en/stablev20.07/kubernetes/operations/tasks/backends/anf.html>

- Dask and RAPIDS:

- Dask

<https://docs.dask.org/en/latest/>

- Install Dask

<https://docs.dask.org/en/latest/install.html>

- Dask API

<https://docs.dask.org/en/latest/api.html>

- Dask Machine Learning  
<https://examples.dask.org/machine-learning.html>
- Dask Distributed Diagnostics  
<https://docs.dask.org/en/latest/diagnostics-distributed.html>
- ML framework and tools:
  - TensorFlow: An Open-Source Machine Learning Framework for Everyone  
<https://www.tensorflow.org/>
  - Docker  
<https://docs.docker.com>
  - Kubernetes  
<https://kubernetes.io/docs/home/>
  - Kubeflow  
<http://www.kubeflow.org/>
  - Jupyter Notebook Server  
<http://www.jupyter.org/>

Next: Version history.

## Version history

Previous: Where to find additional information.

Version	Date	Document version history
Version 1.0	August 2021	Initial release.

## TR-4896: Distributed training in Azure: Lane detection - Solution design

Muneer Ahmad and Verron Martina, NetApp  
 Ronen Dar, RUN:AI

Since May 2019, Microsoft delivers an Azure native, first-party portal service for enterprise NFS and SMB file services based on NetApp ONTAP technology. This development is driven by a strategic partnership between Microsoft and NetApp and further extends the reach of world-class ONTAP data services to Azure.

NetApp, a leading cloud data services provider, has teamed up with RUN: AI, a company virtualizing AI infrastructure, to allow faster AI experimentation with full GPU utilization. The partnership enables teams to speed up AI by running many experiments in parallel, with fast access to data, and leveraging limitless compute resources. RUN: AI enables full GPU utilization by automating resource allocation, and the proven architecture of Azure NetApp Files enables every experiment to run at maximum speed by eliminating data pipeline obstructions.

NetApp and RUN: AI have joined forces to offer customers a future-proof platform for their AI journey in Azure. From analytics and high-performance computing (HPC) to autonomous decisions (where customers can optimize their IT investments by only paying for what they need, when they need it), the alliance between NetApp and RUN: AI offers a single unified experience in the Azure Cloud.

## Solution overview

In this architecture, the focus is on the most computationally intensive part of the AI or machine learning (ML) distributed training process of lane detection. Lane detection is one of the most important tasks in autonomous driving, which helps to guide vehicles by localization of the lane markings. Static components like lane markings guide the vehicle to drive on the highway interactively and safely.

Convolutional Neural Network (CNN)-based approaches have pushed scene understanding and segmentation to a new level. Although it doesn't perform well for objects with long structures and regions that could be occluded (for example, poles, shade on the lane, and so on). Spatial Convolutional Neural Network (SCNN) generalizes the CNN to a rich spatial level. It allows information propagation between neurons in the same layer, which makes it best suited for structured objects such as lanes, poles, or truck with occlusions. This compatibility is because the spatial information can be reinforced, and it preserves smoothness and continuity.

Thousands of scene images need to be injected in the system to allow the model learn and distinguish the various components in the dataset. These images include weather, daytime or nighttime, multilane highway roads, and other traffic conditions.

For training, there is a need for good quality and quantity of data. Single GPU or multiple GPUs can take days to weeks to complete the training. Data-distributed training can speed up the process by using multiple and multinode GPUs. Horovod is one such framework that grants distributed training but reading data across clusters of GPUs could act as a hindrance. Azure NetApp Files provides ultrafast, high throughput and sustained low latency to provide scale-out/scale-up capabilities so that GPUs are leveraged to the best of their computational capacity. Our experiments verified that all the GPUs across the cluster are used more than 96% on average for training the lane detection using SCNN.

## Target audience

Data science incorporates multiple disciplines in IT and business, therefore multiple personas are part of our targeted audience:

- Data scientists need the flexibility to use the tools and libraries of their choice.
- Data engineers need to know how the data flows and where it resides.
- Autonomous driving use-case experts.
- Cloud administrators and architects to set up and manage cloud (Azure) resources.
- A DevOps engineer needs the tools to integrate new AI/ML applications into their continuous integration and continuous deployment (CI/CD) pipelines.
- Business users want to have access to AI/ML applications.

In this document, we describe how Azure NetApp Files, RUN: AI, and Microsoft Azure help each of these roles bring value to business.

## Solution technology

This section covers the technology requirements for the lane detection use case by implementing a distributed training solution at scale that fully runs in the Azure cloud. The figure below provides an overview of the solution architecture.

The elements used in this solution are:

- Azure Kubernetes Service (AKS)
- Azure Compute SKUs with NVIDIA GPUs
- Azure NetApp Files
- RUN: AI
- NetApp Trident

Links to all the elements mentioned here are listed in the [Additional information](#) section.



#### Cloud resources and services requirements

The following table lists the hardware components that are required to implement the solution. The cloud components that are used in any implementation of the solution might vary based on customer requirements.

Cloud	Quantity
AKS	Minimum of three system nodes and three GPU worker nodes
Virtual machine (VM) SKU system nodes	Three Standard_DS2_v2
VM SKU GPU worker nodes	Three Standard_NC6s_v3
Azure NetApp Files	4TB standard tier

#### Software requirements

The following table lists the software components that are required to implement the solution. The software components that are used in any implementation of the solution might vary based on customer requirements.

Software	Version or other information
AKS - Kubernetes version	1.18.14
RUN:AI CLI	v2.2.25
RUN:AI Orchestration Kubernetes Operator version	1.0.109

Software	Version or other information
Horovod	0.21.2
NetApp Trident	20.01.1
Helm	3.0.0

## Lane detection – Distributed training with RUN:AI

This section provides details on setting up the platform for performing lane detection distributed training at scale using the RUN: AI orchestrator. We discuss installation of all the solution elements and running the distributed training job on the said platform. ML versioning is completed by using NetApp SnapshotTM linked with RUN: AI experiments for achieving data and model reproducibility. ML versioning plays a crucial role in tracking models, sharing work between team members, reproducibility of results, rolling new model versions to production, and data provenance. NetApp ML version control (Snapshot) can capture point-in-time versions of the data, trained models, and logs associated with each experiment. It has rich API support making it easy to integrate with the RUN: AI platform; you just have to trigger an event based on the training state. You also have to capture the state of the whole experiment without changing anything in the code or the containers running on top of Kubernetes (K8s).

Finally, this technical report wraps up with performance evaluation on multiple GPU-enabled nodes across AKS.

### Distributed training for lane detection use case using the TuSimple dataset

In this technical report, distributed training is performed on the TuSimple dataset for lane detection. Horovod is used in the training code for conducting data distributed training on multiple GPU nodes simultaneously in the Kubernetes cluster through AKS. Code is packaged as container images for TuSimple data download and processing. Processed data is stored on persistent volumes allocated by NetApp Trident plug-in. For the training, one more container image is created, and it uses the data stored on persistent volumes created during downloading the data.

To submit the data and training job, use RUN: AI for orchestrating the resource allocation and management. RUN: AI allows you to perform Message Passing Interface (MPI) operations which are needed for Horovod. This layout allows multiple GPU nodes to communicate with each other for updating the training weights after every training mini batch. It also enables monitoring of training through the UI and CLI, making it easy to monitor the progress of experiments.

NetApp Snapshot is integrated within the training code and captures the state of data and the trained model for every experiment. This capability enables you to track the version of data and code used, and the associated trained model generated.

### AKS setup and installation

For setup and installation of the AKS cluster go to [Create an AKS Cluster](#). Then, follow these series of steps:

1. When selecting the type of nodes (whether it be system (CPU) or worker (GPU) nodes), select the following:
  - a. Add primary system node named `agentpool` at the `Standard_DS2_v2` size. Use the default three nodes.
  - b. Add worker node `gpupool` with the `Standard_NC6s_v3` pool size. Use three nodes minimum for GPU nodes.

<input type="button"/> Add node pool	<input type="button"/> Delete			
Name	Mode	OS type	Node count	Node size
<input type="checkbox"/> agentpool	System	Linux	3	Standard_DS2_v2
<input type="checkbox"/> gpupool	User	Linux	3	Standard_NC6s_v



Deployment takes 5–10 minutes.

- After deployment is complete, click Connect to Cluster. To connect to the newly created AKS cluster, install the Kubernetes command-line tool from your local environment (laptop/PC). Visit [Install Tools](#) to install it as per your OS.
- [Install Azure CLI on your local environment](#).
- To access the AKS cluster from the terminal, first enter `az login` and put in the credentials.
- Run the following two commands:

```
az account set --subscription xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
aks get-credentials --resource-group resourcegroup --name aksclustername
```

- Enter this command in the Azure CLI:

```
kubectl get nodes
```



If all six nodes are up and running as seen here, your AKS cluster is ready and connected to your local environment.

```
verronmartina@verron-mac-0 ~ % kubectl get nodes
NAME                           STATUS  ROLES   AGE    VERSION
aks-agentpool-34613062-vmss00000  Ready   agent   22m   v1.18.14
aks-agentpool-34613062-vmss00001  Ready   agent   22m   v1.18.14
aks-agentpool-34613062-vmss00002  Ready   agent   22m   v1.18.14
aks-gpupool-34613062-vmss00000  Ready   agent   20m   v1.18.14
aks-gpupool-34613062-vmss00001  Ready   agent   20m   v1.18.14
aks-gpupool-34613062-vmss00002  Ready   agent   20m   v1.18.14
verronmartina@verron-mac-0 ~ %
```

#### Create a delegated subnet for Azure NetApp Files

To create a delegated subnet for Azure NetApp Files, follow this series of steps:

- Navigate to Virtual networks within the Azure portal. Find your newly created virtual network. It should have a prefix such as aks-vnet, as seen here. Click the name of the virtual network.

Microsoft Azure

Search resources, services, and docs (G+/)

Dashboard > Virtual networks

Virtual networks (Default Directory)

Add Manage view Refresh Export to CSV Open query Assign tags Feedback

Filter by name... Subscription == AzureSub01 Resource group == all Location == all Add filter

Showing 1 to 5 of 5 records.

Name	Resource group	Location	Subscription
aks-vnet-22885919	MC_sluce.rg_TridentDemo_eastus2	East US 2	AzureSub01

No grouping List view

2. Click Subnets and select +Subnet from the top toolbar.

Microsoft Azure

Search resources, services, and docs (G+/)

Dashboard > Virtual networks > aks-vnet-22885919

aks-vnet-22885919 | Subnets

Virtual network

Search (Ctrl+I) + Subnet Gateway subnet Refresh Manage users Delete

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Address space Connected devices Subnets

Search subnets

Name	IPv4	IPv6 (many availab...)	Delegated to	Security group
aks-subnet	10.240.0.0/16 (65530 av...)	-	-	aks-agentpool-2288591...

3. Provide the subnet with a name such as ANF.sn and under the Subnet Delegation heading, select Microsoft.NetApp/volumes. Do not change anything else. Click OK.

## Add subnet

X

Name \*

ANF.sn



Subnet address range \* ⓘ

10.0.0.0/24

10.0.0.0 - 10.0.0.255 (251 + 5 Azure reserved addresses)

Add IPv6 address space ⓘ

NAT gateway ⓘ

None



Network security group

None



Route table

None



### SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

0 selected



### SUBNET DELEGATION

Delegate subnet to a service ⓘ

Microsoft.Netapp/volumes



OK

Cancel

Azure NetApp Files volumes are allocated to the application cluster and are consumed as persistent volume claims (PVCs) in Kubernetes. In turn, this allocation provides us the flexibility to map volumes to different services, be it Jupyter notebooks, serverless functions, and so on

Users of services can consume storage from the platform in many ways. The main benefits of Azure NetApp Files are:

- Provides users with the ability to use snapshots.
- Enables users to store large quantities of data on Azure NetApp Files volumes.
- Procure the performance benefits of Azure NetApp Files volumes when running their models on large sets of files.

## Azure NetApp Files setup

To complete the setup of Azure NetApp Files, you must first configure it as described in [Quickstart: Set up Azure NetApp Files and create an NFS volume](#).

However, you may omit the steps to create an NFS volume for Azure NetApp Files as you will create volumes through Trident. Before continuing, be sure that you have:

1. [Registered for Azure NetApp Files and NetApp Resource Provider \(through the Azure Cloud Shell\)](#).
2. [Created an account in Azure NetApp Files](#).
3. [Set up a capacity pool \(minimum 4TiB Standard or Premium depending on your needs\)](#).

## Peering of AKS virtual network and Azure NetApp Files virtual network

Next, peer the AKS virtual network (VNet) with the Azure NetApp Files VNet by following these steps:

1. In the search box at the top of the Azure portal, type virtual networks.
2. Click VNet aks- vnet-name, then enter Peerings in the search field.
3. Click +Add and enter the information provided in the table below:

Field	Value or description
Peering link name	aks-vnet-name_to_anf
SubscriptionID	Subscription of the Azure NetApp Files VNet to which you're peering
VNet peering partner	Azure NetApp Files VNet



Leave all the nonasterisk sections on default

4. Click ADD or OK to add the peering to the virtual network.

For more information, visit [Create, change, or delete a virtual network peering](#).

## Trident

Trident is an open-source project that NetApp maintains for application container persistent storage. Trident has been implemented as an external provisioner controller that runs as a pod itself, monitoring volumes and completely automating the provisioning process.

NetApp Trident enables smooth integration with K8s by creating and attaching persistent volumes for storing training datasets and trained models. This capability makes it easier for data scientists and data engineers to use K8s without the hassle of manually storing and managing datasets. Trident also eliminates the need for data scientists to learn managing new data platforms as it integrates the data management-related tasks through the logical API integration.

## Install Trident

To install Trident software, complete the following steps:

1. [First install helm](#).
2. Download and extract the Trident 21.01.1 installer.

```
wget  
https://github.com/NetApp/trident/releases/download/v21.01.1/trident-  
installer-21.01.1.tar.gz  
tar -xf trident-installer-21.01.1.tar.gz
```

3. Change the directory to `trident-installer`.

```
cd trident-installer
```

4. Copy `tridentctl` to a directory in your system \$PATH.

```
cp ./tridentctl /usr/local/bin
```

5. Install Trident on K8s cluster with Helm:

- a. Change directory to helm directory.

```
cd helm
```

- b. Install Trident.

```
helm install trident trident-operator-21.01.1.tgz --namespace trident  
--create-namespace
```

- c. Check the status of Trident pods the usual K8s way:

```
kubectl -n trident get pods
```

- d. If all the pods are up and running, Trident is installed and you are good to move forward.

#### **Set up Azure NetApp Files back-end and storage class**

To set up Azure NetApp Files back-end and storage class, complete the following steps:

1. Switch back to the home directory.

```
cd ~
```

2. Clone the [project repository](#) lane-detection-SCNN-horovod.

3. Go to the `trident-config` directory.

```
cd ./lane-detection-SCNN-horovod/trident-config
```

4. Create an Azure Service Principle (the service principle is how Trident communicates with Azure to access your Azure NetApp Files resources).

```
az ad sp create-for-rbac --name
```

The output should look like the following example:

```
{  
    "appId": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",  
    "displayName": "netapprtrident",  
    "name": "http://netapprtrident",  
    "password": "xxxxxxxxxxxxxx.xxxxxxxxxxxxxx",  
    "tenant": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"  
}
```

5. Create the Trident backend json file.
6. Using your preferred text editor, complete the following fields from the table below inside the anf-backend.json file.

Field	Value
subscriptionID	Your Azure Subscription ID
tenantID	Your Azure Tenant ID (from the output of az ad sp in the previous step)
clientID	Your appID (from the output of az ad sp in the previous step)
clientSecret	Your password (from the output of az ad sp in the previous step)

The file should look like the following example:

```
{
    "version": 1,
    "storageDriverName": "azure-netapp-files",
    "subscriptionID": "fakec765-4774-fake-ae98-a721add4fake",
    "tenantID": "fakef836-edc1-fake-bff9-b2d865eefake",
    "clientID": "fake0f63-bf8e-fake-8076-8de91e57fake",
    "clientSecret": "SECRET",
    "location": "westeurope",
    "serviceLevel": "Standard",
    "virtualNetwork": "anf-vnet",
    "subnet": "default",
    "nfsMountOptions": "vers=3,proto=tcp",
    "limitVolumeSize": "500Gi",
    "defaults": {
        "exportRule": "0.0.0.0/0",
        "size": "200Gi"
    }
}
```

7. Instruct Trident to create the Azure NetApp Files back- end in the trident namespace, using anf-backend.json as the configuration file as follows:

```
tridentctl create backend -f anf-backend.json -n trident
```

8. Create the storage class:

- a. K8 users provision volumes by using PVCs that specify a storage class by name. Instruct K8s to create a storage class azurenetaffiles that will reference the Azure NetApp Files back end created in the previous step using the following:

```
kubectl create -f anf-storage-class.yaml
```

- b. Check that storage class is created by using the following command:

```
kubectl get sc azurenetaffiles
```

The output should look like the following example:

NAME	PROVISIONER	RECLAIMPOLICY	VOLUMEBINDINGMODE	ALLOWVOLUMEEXPANSION	AGE
azurenetaffiles	csi.trident.netapp.io	Delete	Immediate	false	98s

#### Deploy and set up volume snapshot components on AKS

If your cluster does not come pre-installed with the correct volume snapshot components, you may manually install these components by running the following steps:



AKS 1.18.14 does not have pre-installed Snapshot Controller.

1. Install Snapshot Beta CRDs by using the following commands:

```
kubectl create -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-3.0/client/config/crd/snapshot.storage.k8s.io_volumesnapshotclasses.yaml  
kubectl create -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-3.0/client/config/crd/snapshot.storage.k8s.io_volumesnapshotcontents.yaml  
kubectl create -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-3.0/client/config/crd/snapshot.storage.k8s.io_volumesnapshots.yaml
```

2. Install Snapshot Controller by using the following documents from GitHub:

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-3.0/deploy/kubernetes/snapshot-controller/rbac-snapshot-controller.yaml  
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-3.0/deploy/kubernetes/snapshot-controller/setup-snapshot-controller.yaml
```

3. Set up K8s volumesnapshotclass: Before creating a volume snapshot, a **volume snapshot class** must be set up. Create a volume snapshot class for Azure NetApp Files, and use it to achieve ML versioning by using NetApp Snapshot technology. Create `volumesnapshotclass netapp-csi-snapclass` and set it to default `volumesnapshotclass` as such:

```
kubectl create -f netapp-volume-snapshot-class.yaml
```

The output should look like the following example:

```
volumesnapshotclass.snapshot.storage.k8s.io/netapp-csi-snapclass created
```

4. Check that the volume Snapshot copy class was created by using the following command:

```
kubectl get volumesnapshotclass
```

The output should look like the following example:

NAME	DRIVER	DELETIONPOLICY	AGE
netapp-csi-snapclass	csi.trident.netapp.io	Delete	63s

## RUN:AI installation

To install RUN:AI, complete the following steps:

1. [Install RUN:AI cluster on AKS](#).
2. Go to app.runai.ai, click create New Project, and name it lane-detection. It will create a namespace on a K8s cluster starting with runai- followed by the project name. In this case, the namespace created would be runai-lane-detection.

The screenshot shows the 'New Project' creation interface. On the left, there's a sidebar with tabs: 'Basics' (selected), 'Node Affinity', and 'Time Limit'. The main area is titled 'Basics' and contains the following fields:

- Project Name**: A text input field containing 'lane-detection'.
- Assigned GPUs**: A dropdown menu showing the number '3'.
- Over-quota for project**: A checkbox labeled 'Allow over-quota' which is checked.

At the bottom right are two buttons: a blue 'Save' button and a white 'Cancel' button.

3. [Install RUN:AI CLI](#).
4. On your terminal, set lane-detection as a default RUN: AI project by using the following command:

```
`runai config project lane-detection`
```

The output should look like the following example:

```
Project lane-detection has been set as default project
```

5. Create ClusterRole and ClusterRoleBinding for the project namespace (for example, lane-detection) so the default service account belonging to runai-lane-detection namespace has permission to perform volumesnapshot operations during job execution:
  - a. List namespaces to check that runai-lane-detection exists by using this command:

```
kubectl get namespaces
```

The output should appear like the following example:

NAME	STATUS	AGE
default	Active	130m
kube-node-lease	Active	130m
kube-public	Active	130m
kube-system	Active	130m
runai	Active	4m44s
runai-lane-detection	Active	13s
trident	Active	102m

6. Create ClusterRole netappssnapshot and ClusterRoleBinding netappssnapshot using the following commands:

```
`kubectl create -f runai-project-snap-role.yaml`  
`kubectl create -f runai-project-snap-role-binding.yaml`
```

#### Download and process the TuSimple dataset as RUN:AI job

The process to download and process the TuSimple dataset as a RUN: AI job is optional. It involves the following steps:

1. Build and push the docker image, or omit this step if you want to use an existing docker image (for example, muneer7589/download-tusimple:1.0)
  - a. Switch to the home directory:

```
cd ~
```

- b. Go to the data directory of the project lane-detection-SCNN-horovod:

```
cd ./lane-detection-SCNN-horovod/data
```

- c. Modify build\_image.sh shell script and change docker repository to yours. For example, replace muneer7589 with your docker repository name. You could also change the docker image name and

TAG (such as download-tusimple and 1.0):

```
#!/bin/bash
#
# A simple script to build the Docker image.
#
# $ build_image.sh
set -ex

IMAGE=muneer7589/download-tusimple
TAG=1.0

# Build image
echo "Building image: "$IMAGE
docker build . -f Dockerfile \
--tag "${IMAGE}:${TAG}"
echo "Finished building image: "$IMAGE

# Push image
echo "Pushing image: "$IMAGE
docker push "${IMAGE}:${TAG}"
echo "Finished pushing image: "$IMAGE
```

- d. Run the script to build the docker image and push it to the docker repository using these commands:

```
chmod +x build_image.sh
./build_image.sh
```

2. Submit the RUN: AI job to download, extract, pre-process, and store the TuSimple lane detection dataset in a pvc, which is dynamically created by NetApp Trident:

- a. Use the following commands to submit the RUN: AI job:

```
runai submit
--name download-tusimple-data
--pvc azurenetaffiles:100Gi:/mnt
--image muneer7589/download-tusimple:1.0
```

- b. Enter the information from the table below to submit the RUN:AI job:

Field	Value or description
-name	Name of the job
-pvc	PVC of the format [StorageClassName]:Size:ContainerMountPath  In the above job submission, you are creating an PVC based on-demand using Trident with storage class azurenetaffiles. Persistent volume capacity here is 100Gi and it's mounted at path /mnt.
-image	Docker image to use when creating the container for this job

The output should look like the following example:

```
The job 'download-tusimple-data' has been submitted successfully
You can run `runai describe job download-tusimple-data -p lane-detection` to check the job status
```

- c. List the submitted RUN:AI jobs.

```
runai list jobs
```

```
Showing jobs for project lane-detection
NAME          STATUS      AGE     NODE           IMAGE          TYPE    PROJECT      USER      GPUs Allocated (Requested)
PODs Running (Pending)  SERVICE URL(S)
download-tusimple-data  ContainerCreating  1m   aks-agentpool-34613062-vmss00000a  muneer7589/download-tusimple:1.0  Train  lane-detection  veronamartina  0 (0)
1 (@)
```

- d. Check the submitted job logs.

```
runai logs download-tusimple-data -t 10
```

```
751150K ..... 6% 16.2M 20m37s
751200K ..... 6% 11.1M 20m37s
751250K ..... 6% 12.5M 20m36s
751300K ..... 6% 11.3M 20m36s
751350K ..... 6% 15.2M 20m36s
751400K ..... 6% 10.5M 20m36s
751450K ..... 6% 15.2M 20m36s
751500K ..... 6% 14.1M 20m36s
751550K ..... 6% 24.3M 20m36s
751600K ..... 6% 26.3M 20m36s
```

- e. List the pvc created. Use this pvc command for training in the next step.

```
kubectl get pvc | grep download-tusimple-data
```

The output should look like the following example:

```
pvc-download-tusimple-data-0    Bound    pvc-bb03b74d-2c17-40c4-a445-79f3de8d16d5    100Gi    RWO    azurenetsappfiles    4m47s
```

- f. Check the job in RUN: AI UI (or app.run.ai).

The screenshot shows a table of jobs in the RUN: AI UI. The columns are: Job Name, Status, User, Project, Total Run Time, Creation Time, Type, GPU Utilization, Used CPU, and a small icon. There are eight rows:

Job Name	Status	User	Project	Total Run Time	Creation Time	Type	GPU Utilization	Used CPU
download-tusimple-data	Running	vernonma...	lane-detection	00:07:11	03/03/21, 2:51PM	Train	-	0.00
build1	Deleted	root	lane-detection	00:01:56	03/01/21, 10:18...	Interactive	-	-
download-tusimple-data	Deleted	root	lane-detection	-	03/01/21, 9:58AM	Train	-	-
download-tusimple-data	Deleted	root	lane-detection	-	03/01/21, 10:03...	Train	-	-
download-tusimple-data	Deleted	root	lane-detection	00:02:55	03/01/21, 10:24...	Train	-	-
download-tusimple-data	Deleted	root	lane-detection	-	03/01/21, 10:30...	Train	-	-
download-tusimple-data	Deleted	root	lane-detection	00:13:17	03/01/21, 11:41...	Train	-	-
download-tusimple-data-1	Deleted	vernonma...	lane-detection	-	02/26/21, 5:30PM	Train	-	-

### Perform distributed lane detection training using Horovod

Performing distributed lane detection training using Horovod is an optional process. However, here are the steps involved:

1. Build and push the docker image, or skip this step if you want to use the existing docker image (for example, muneer7589/dist-lane-detection:3.1) :

- a. Switch to home directory.

```
cd ~
```

- b. Go to the project directory lane-detection-SCNN-horovod.

```
cd ./lane-detection-SCNN-horovod
```

- c. Modify the build\_image.sh shell script and change docker repository to yours (for example, replace muneer7589 with your docker repository name). You could also change the docker image name and TAG (dist-lane-detection and 3.1, for example).

```

#!/bin/bash
#
# A simple script to build the distributed Docker image.
#
# $ build_image.sh
set -ex

IMAGE=muneer7589/dist-lane-detection
TAG=3.0

# Build image
echo "Building image: "$IMAGE
docker build . -f Dockerfile \
--tag "${IMAGE}:${TAG}"
echo "Finished building image: "$IMAGE

# Push image
echo "Pushing image: "$IMAGE
docker push "${IMAGE}:${TAG}"
echo "Finished pushing image: "$IMAGE

```

- d. Run the script to build the docker image and push to the docker repository.

```

chmod +x build_image.sh
./build_image.sh

```

2. Submit the RUN: AI job for carrying out distributed training (MPI):

- Using submit of RUN: AI for automatically creating PVC in the previous step (for downloading data) only allows you to have RWO access, which does not allow multiple pods or nodes to access the same PVC for distributed training. Update the access mode to ReadWriteMany and use the Kubernetes patch to do so.
- First, get the volume name of the PVC by running the following command:

```
kubectl get pvc | grep download-tusimple-data
```

```

root@ai-w-gpu-2:/mnt/ai_data/anf_runai/lane-detection-SCNN-horovod# kubectl get pvc | grep download-tusimple-data
pvc-download-tusimple-data-0 Bound pvc-bb03b74d-2c17-40c4-a445-79f3de8d16d5 100Gi RWX azurenetaffiles 2d4h

```

- Patch the volume and update access mode to ReadWriteMany (replace volume name with yours in the following command):

```

kubectl patch pv pvc-bb03b74d-2c17-40c4-a445-79f3de8d16d5 -p
'{"spec":{"accessModes":["ReadWriteMany"]}}'

```

- d. Submit the RUN: AI MPI job for executing the distributed training` job using information from the table below:

```
runai submit-mpi
--name dist-lane-detection-training
--large-shm
--processes=3
--gpu 1
--pvc pvc-download-tusimple-data-0:/mnt
--image muneer7589/dist-lane-detection:3.1
-e USE_WORKERS="true"
-e NUM_WORKERS=4
-e BATCH_SIZE=33
-e USE_VAL="false"
-e VAL_BATCH_SIZE=99
-e ENABLE_SNAPSHOT="true"
-e PVC_NAME="pvc-download-tusimple-data-0"
```

Field	Value or description
name	Name of the distributed training job
large shm	Mount a large /dev/shm device  It is a shared file system mounted on RAM and provides large enough shared memory for multiple CPU workers to process and load batches into CPU RAM.
processes	Number of distributed training processes
gpu	Number of GPUs/processes to allocate for the job  In this job, there are three GPU worker processes (--processes=3), each allocated with a single GPU (--gpu 1)
pvc	Use existing persistent volume (pvc-download-tusimple-data-0) created by previous job (download-tusimple-data) and it is mounted at path /mnt
image	Docker image to use when creating the container for this job
Define environment variables to be set in the container	
USE_WORKERS	Setting the argument to true turns on multi-process data loading
NUM_WORKERS	Number of data loader worker processes
BATCH_SIZE	Training batch size

Field	Value or description
USE_VAL	Setting the argument to true allows validation
VAL_BATCH_SIZE	Validation batch size
ENABLE_SNAPSHOT	Setting the argument to true enables taking data and trained model snapshots for ML versioning purposes
PVC_NAME	Name of the pvc to take a snapshot of. In the above job submission, you are taking a snapshot of pvc-download-tusimple-data-0, consisting of dataset and trained models

The output should look like the following example:

```
The job 'dist-lane-detection-training' has been submitted successfully
You can run `runai describe job dist-lane-detection-training -p lane-detection` to check the job status.
```

- e. List the submitted job.

```
runai list jobs
```

NAME	STATUS	AGE	NODE	IMAGE	TYPE	PROJECT	USER	GPUs Allocated (Requested)	PODs
download-tusimple-data	Succeeded	1d		muneeer7589/download-tusimple:1.0	Train	lane-detection	vernonmartina	- (0)	0 (0)
dist-lane-detection-training	Init:0/1	2m	<multiple>	muneeer7589/dist-lane-detection:3.1	Train	lane-detection	root	3 (3)	4 (0)

- f. Submitted job logs:

```
runai logs dist-lane-detection-training
```

```
root@ai-w-gpu-2:~/runai# runai logs dist-lane-detection-training
Running with 3 workers
2021-03-04 17:29:23.158449: I tensorflow/stream_executor/platform/default/dso_loader.cc:48] Successfully opened dynamic library libcudart.so.10.1
+ POD_NAME=dist-lane-detection-training-worker-0
+ [ d = - ]
+ shift
+ /opt/kube/kubectl cp /opt/kube/hosts dist-lane-detection-training-worker-0:/etc/hosts_of_nodes
+ POD_NAME=dist-lane-detection-training-worker-2
+ [ d = - ]
+ shift
+ /opt/kube/kubectl cp /opt/kube/hosts dist-lane-detection-training-worker-2:/etc/hosts_of_nodes
+ POD_NAME=dist-lane-detection-training-worker-1
```

- g. Check training job in RUN: AI GUI (or app.runai.ai): RUN: AI Dashboard, as seen in the figures below. The first figure details three GPUs allocated for the distributed training job spread across three nodes on AKS, and the second RUN:AI jobs:



- h. After the training is finished, check the NetApp Snapshot copy that was created and linked with RUN: AI job.

```
runai logs dist-lane-detection-training --tail 1
```

```
[1,0]<stdout>:Snapshot snap-pvc-download-tusimple-data-0-dist-lane-detection-training-launcher-2021-03-05-16-23-42 created in namespace runai-lane-detection
```

```
kubectl get volumesnapshots | grep download-tusimple-data-0
```

## Restore data from the NetApp Snapshot copy

To restore data from the NetApp Snapshot copy, complete the following steps:

1. Switch to home directory.

```
cd ~
```

2. Go to the project directory lane-detection-SCNN-horovod.

```
cd ./lane-detection-SCNN-horovod
```

3. Modify `restore-snapshot-pvc.yaml` and update `dataSource` name field to the Snapshot copy from which you want to restore data. You could also change PVC name where the data will be restored to, in this example its `restored-tusimple`.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: restored-tusimple
spec:
  storageClassName: azurenetappfiles
  dataSource:
    name: snap-pvc-download-tusimple-data-0-dist-lane-detection-training-launcher-2021-03-05-16-23-42
    kind: VolumeSnapshot
    apiGroup: snapshot.storage.k8s.io
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 100Gi
```

4. Create a new PVC by using `restore-snapshot-pvc.yaml`.

```
kubectl create -f restore-snapshot-pvc.yaml
```

The output should look like the following example:

```
persistentvolumeclaim/restored-tusimple created
```

5. If you want to use the just restored data for training, job submission remains the same as before; only replace the `PVC_NAME` with the restored `PVC_NAME` when submitting the training job, as seen in the following commands:

```
runai submit-mpi
--name dist-lane-detection-training
--large-shm
--processes=3
--gpu 1
--pvc restored-tusimple:/mnt
--image muneer7589/dist-lane-detection:3.1
-e USE_WORKERS="true"
-e NUM_WORKERS=4
-e BATCH_SIZE=33
-e USE_VAL="false"
-e VAL_BATCH_SIZE=99
-e ENABLE_SNAPSHOT="true"
-e PVC_NAME="restored-tusimple"
```

## Performance evaluation

To show the linear scalability of the solution, performance tests have been done for two scenarios: one GPU and three GPUs. GPU allocation, GPU and memory utilization, different single- and three- node metrics have been captured during the training on the TuSimple lane detection dataset. Data is increased five- fold just for the sake of analyzing resource utilization during the training processes.

The solution enables customers to start with a small dataset and a few GPUs. When the amount of data and the demand of GPUs increase, customers can dynamically scale out the terabytes in the Standard Tier and quickly scale up to the Premium Tier to get four times the throughput per terabyte without moving any data. This process is further explained in the section, [Azure NetApp Files service levels](#).

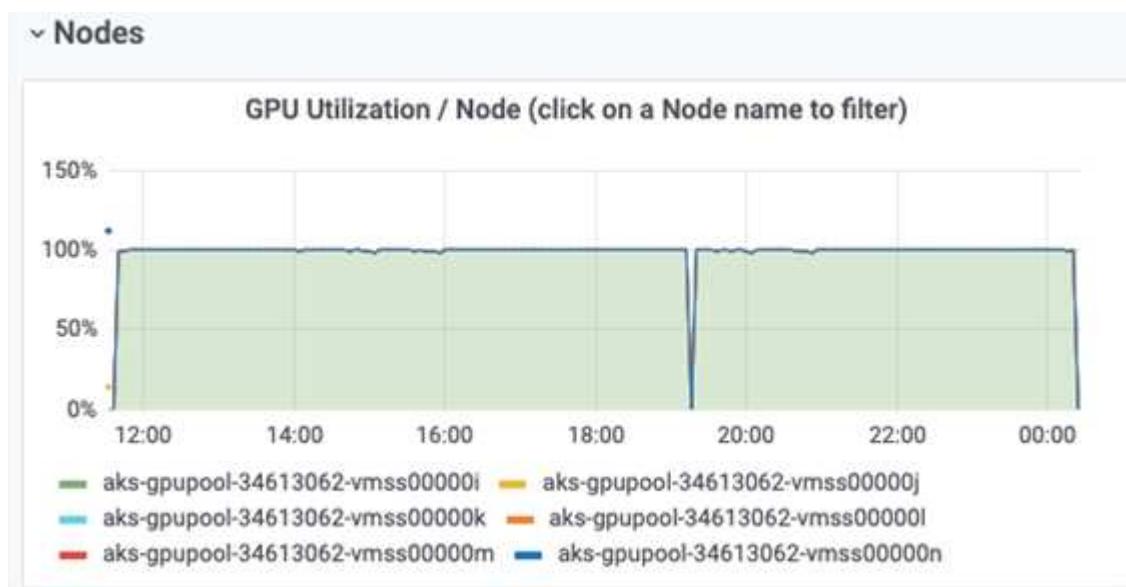
Processing time on one GPU was 12 hours and 45 minutes. Processing time on three GPUs across three nodes was approximately 4 hours and 30 minutes.

The figures shown throughout the remainder of this document illustrate examples of performance and scalability based on individual business needs.

The figure below illustrates 1 GPU allocation and memory utilization.



The figure below illustrates single node GPU utilization.



The figure below illustrates single node memory size (16GB).



The figure below illustrates single node GPU count (1).



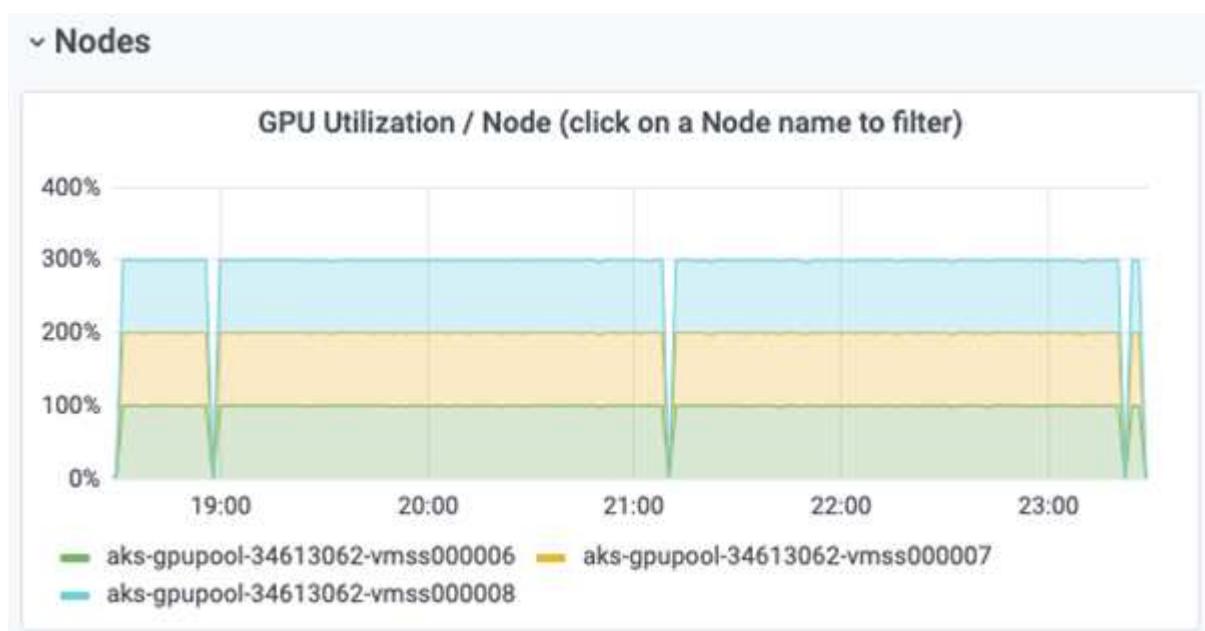
The figure below illustrates single node GPU allocation (%).



The figure below illustrates three GPUs across three nodes – GPUs allocation and memory.



The figure below illustrates three GPUs across three nodes utilization (%).



The figure below illustrates three GPUs across three nodes memory utilization (%).



#### Azure NetApp Files service levels

You can change the service level of an existing volume by moving the volume to another capacity pool that uses the [service level](#) you want for the volume. This existing service-level change for the volume does not require that you migrate data. It also does not affect access to the volume.

#### Dynamically change the service level of a volume

To change the service level of a volume, use the following steps:

1. On the Volumes page, right-click the volume whose service level you want to change. Select Change Pool.

NFSv3	Path	Service Level	pool0	...
NFSv4.1	10.28.254.4:/norootfor...	Standard		
NFSv4.1	NAS-735a.docs.lab:/for...	Premium		
NFSv3	NAS-735a.docs.lab:/krt...	Premium		
NFSv3	10.28.254.4:/moveme0	Premium		
NFSv3	10.28.254.4:/placeholder	Premium		

2. In the Change Pool window, select the capacity pool you want to move the volume to. Then, click OK.



## Automate service level change

Dynamic Service Level change is currently still in Public Preview, but it is not enabled by default. To enable this feature on the Azure subscription, follow these steps provided in the document “[Dynamically change the service level of a volume](#).”

- You can also use the following commands for Azure: CLI. For more information about changing the pool size of Azure NetApp Files, visit [az netappfiles volume: Manage Azure NetApp Files \(ANF\) volume resources](#).

```
az netappfiles volume pool-change -g mygroup  
--account-name myaccname  
-pool-name mypoolname  
--name myvolname  
--new-pool-resource-id mynewresourceid
```

- The `set- aznetappfilesvolumepool` cmdlet shown here can change the pool of an Azure NetApp Files volume. More information about changing volume pool size and Azure PowerShell can be found by visiting [Change pool for an Azure NetApp Files volume](#).

```
Set-AzNetAppFilesVolumePool  
-ResourceGroupName "MyRG"  
-AccountName "MyAnfAccount"  
-PoolName "MyAnfPool"  
-Name "MyAnfVolume"  
-NewPoolResourceId 7d6e4069-6c78-6c61-7bf6-c60968e45fbf
```

## Conclusion

NetApp and RUN: AI have partnered in the creation of this technical report to demonstrate the unique capabilities of the Azure NetApp Files together with the RUN: AI platform for simplifying orchestration of AI workloads. This technical report provides a reference architecture for streamlining the process of both data pipelines and workload orchestration for distributed lane detection training.

In conclusion, with regard to distributed training at scale (especially in a public cloud environment), the resource orchestration and storage component is a critical part of the solution. Making sure that data managing never hinders multiple GPU processing, therefore results in the optimal utilization of GPU cycles. Thus, making the system as cost effective as possible for large- scale distributed training purposes.

Data fabric delivered by NetApp overcomes the challenge by enabling data scientists and data engineers to connect together on-premises and in the cloud to have synchronous data, without performing any manual intervention. In other words, data fabric smooths the process of managing AI workflow spread across multiple locations. It also facilitates on demand-based data availability by bringing data close to compute and performing analysis, training, and validation wherever and whenever needed. This capability not only enables data integration but also protection and security of the entire data pipeline.

## Additional information

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

- Dataset: TuSimple

[https://github.com/TuSimple/tusimple-benchmark/tree/master/doc/lane\\_detection](https://github.com/TuSimple/tusimple-benchmark/tree/master/doc/lane_detection)

- Deep Learning Network Architecture: Spatial Convolutional Neural Network

<https://arxiv.org/abs/1712.06080>

- Distributed deep learning training framework: Horovod

<https://horovod.ai/>

- RUN: AI container orchestration solution: RUN: AI product introduction

<https://docs.run.ai/home/components/>

- RUN: AI installation documentation

<https://docs.run.ai/Administrator/Cluster-Setup/cluster-install/#step-3-install-runai>  
<https://docs.run.ai/Administrator/Researcher-Setup/cli-install/#runai-cli-installation>

- Submitting jobs in RUN: AI CLI

<https://docs.run.ai/Researcher/cli-reference/runai-submit/>

<https://docs.run.ai/Researcher/cli-reference/runai-submit-mpi/>

- Azure Cloud resources: Azure NetApp Files

<https://docs.microsoft.com/azure/azure-netapp-files/>

- Azure Kubernetes Service

<https://azure.microsoft.com/services/kubernetes-service/-features>

- Azure VM SKUs

<https://azure.microsoft.com/services/virtual-machines/>

- Azure VM with GPU SKUs

<https://docs.microsoft.com/azure/virtual-machines/sizes-gpu>

- NetApp Trident

<https://github.com/NetApp/trident/releases>

- Data Fabric powered by NetApp

<https://www.netapp.com/data-fabric/what-is-data-fabric/>

- NetApp Product Documentation

<https://www.netapp.com/support-and-training/documentation/>

## TR-4841: Hybrid Cloud AI Operating System with Data Caching

Rick Huang, David Arnette, NetApp

Yochay Ettun, cnvrg.io

The explosive growth of data and the exponential growth of ML and AI have converged to create a zettabyte economy with unique development and implementation challenges.

Although it is a widely known that ML models are data-hungry and require high-performance data storage proximal to compute resources, in practice, it is not so straight forward to implement this model, especially with hybrid cloud and elastic compute instances. Massive quantities of data are usually stored in low-cost data lakes, where high-performance AI compute resources such as GPUs cannot efficiently access it. This problem is aggravated in a hybrid-cloud infrastructure where some workloads operate in the cloud and some are located on-premises or in a different HPC environment entirely.

In this document, we present a novel solution that allows IT professionals and data engineers to create a truly hybrid cloud AI platform with a topology-aware data hub that enables data scientists to instantly and automatically create a cache of their datasets in proximity to their compute resources, wherever they are located. As a result, not only can high-performance model training be accomplished, but additional benefits are created, including the collaboration of multiple AI practitioners, who have immediate access to dataset caches, versions, and lineages within a dataset version hub.

[Next: Use Case Overview and Problem Statement](#)

## Use Case Overview and Problem Statement

Datasets and dataset versions are typically located in a data lake, such as NetApp StorageGrid object-based storage, which offers reduced cost and other operational advantages. Data scientists pull these datasets and engineer them in multiple steps to prepare them for training with a specific model, often creating multiple versions along the way. As the next step, the data scientist must pick optimized compute resources (GPUs, high-end CPU instances, an on-premises cluster, and so on) to run the model. The following figure depicts the lack of dataset proximity in an ML compute environment.



However, multiple training experiments must run in parallel in different compute environments, each of which require a download of the dataset from the data lake, which is an expensive and time-consuming process. Proximity of the dataset to the compute environment (especially for a hybrid cloud) is not guaranteed. In addition, other team members that run their own experiments with the same dataset must go through the same arduous process. Beyond the obvious slow data access, challenges include difficulties tracking dataset versions, dataset sharing, collaboration, and reproducibility.

## Customer Requirements

Customer requirements can vary in order to achieve high- performance ML runs while efficiently using resources; for example, customers might require the following:

- Fast access to datasets from each compute instance executing the training model without incurring expensive downloads and data access complexities
- The use any compute instance (GPU or CPU) in the cloud or on-premises without concern for the location

of the datasets

- Increased efficiency and productivity by running multiple training experiments in parallel with different compute resources on the same dataset without unnecessary delays and data latency
- Minimized compute instance costs
- Improved reproducibility with tools to keep records of the datasets, their lineage, versions, and other metadata details
- Enhanced sharing and collaboration so that any authorized member of the team can access the datasets and run experiments

To implement dataset caching with NetApp ONTAP data management software, customers must perform the following tasks:

- Configure and set the NFS storage that is closest to the compute resources.
- Determine which dataset and version to cache.
- Monitor the total memory committed to cached datasets and how much NFS storage is available for additional cache commits (for example, cache management).
- Age out of datasets in the cache if they have not been used in certain time. The default is one day; other configuration options are available.

[Next: Solution Overview](#)

## Solution Overview

This section reviews a conventional data science pipeline and its drawbacks. It also presents the architecture of the proposed dataset caching solution.

### Conventional Data Science Pipeline and Drawbacks

A typical sequence of ML model development and deployment involves iterative steps that include the following:

- Ingesting data
- Data preprocessing (creating multiple versions of the datasets)
- Running multiple experiments involving hyperparameter optimization, different models, and so on
- Deployment
- Monitoringcnvrg.io has developed a comprehensive platform to automate all tasks from research to deployment. A small sample of dashboard screenshots pertaining to the pipeline is shown in the following figure.



It is very common to have multiple datasets in play from public repositories and private data. In addition, each dataset is likely to have multiple versions resulting from dataset cleanup or feature engineering. A dashboard that provides a dataset hub and a version hub is needed to make sure collaboration and consistency tools are available to the team, as can be seen in the following figure.

The next step in the pipeline is training, which requires multiple parallel instances of training models, each associated with a dataset and a certain compute instance. The binding of a dataset to a certain experiment with a certain compute instance is a challenge because it is possible that some experiments are performed by GPU instances from Amazon Web Services (AWS), while other experiments are performed by DGX-1 or DGX-2 instances on-premises. Other experiments might be executed in CPU servers in GCP, while the dataset location is not in reasonable proximity to the compute resources performing the training. A reasonable proximity would have full 10GbE or more low-latency connectivity from the dataset storage to the compute instance.

It is a common practice for data scientists to download the dataset to the compute instance performing the training and execute the experiment. However, there are several potential problems with this approach:

- When the data scientist downloads the dataset to a compute instance, there are no guarantees that the integrated compute storage is high performance (an example of a high-performance system would be the ONTAP AFF A800 NVMe solution).
- When the downloaded dataset resides in one compute node, storage can become a bottleneck when distributed models are executed over multiple nodes (unlike with NetApp ONTAP high-performance distributed storage).
- The next iteration of the training experiment might be performed in a different compute instance due to queue conflicts or priorities, again creating significant network distance from the dataset to the compute location.
- Other team members executing training experiments on the same compute cluster cannot share this dataset; each performs the (expensive) download of the dataset from an arbitrary location.
- If other datasets or versions of the same dataset are needed for the subsequent training jobs, the data scientists must again perform the (expensive) download of the dataset to the compute instance performing the training. NetApp and cnvrg.io have created a new dataset caching solution that eliminates these

hurdles. The solution creates accelerated execution of the ML pipeline by caching hot datasets on the ONTAP high-performance storage system. With ONTAP NFS, the datasets are cached once (and only once) in a data fabric powered by NetApp (such as AFF A800), which is collocated with the compute. As the NetApp ONTAP NFS high-speed storage can serve multiple ML compute nodes, the performance of the training models is optimized, bringing cost savings, productivity, and operational efficiency to the organization.

## Solution Architecture

This solution from NetApp and cnvrg.io provides dataset caching, as shown in the following figure. Dataset caching allows data scientists to pick a desired dataset or dataset version and move it to the ONTAP NFS cache, which lies in proximity to the ML compute cluster. The data scientist can now run multiple experiments without incurring delays or downloads. In addition, all collaborating engineers can use the same dataset with the attached compute cluster (with the freedom to pick any node) without additional downloads from the data lake. The data scientists are offered a dashboard that tracks and monitors all datasets and versions and provides a view of which datasets were cached.

The cnvrg.io platform auto-detects aged datasets that have not been used for a certain time and evicts them from the cache, which maintains free NFS cache space for more frequently used datasets. It is important to note that dataset caching with ONTAP works in the cloud and on-premises, thus providing maximum flexibility.



[Next: Concepts and Components](#)

## Concepts and Components

This section covers concepts and components associated with data caching in an ML workflow.

## Machine Learning

ML is rapidly becoming essential to many businesses and organizations around the world. Therefore, IT and DevOps teams are now facing the challenge of standardizing ML workloads and provisioning cloud, on-premises, and hybrid compute resources that support the dynamic and intensive workflows that ML jobs and pipelines require.

### Container-Based Machine Learning and Kubernetes

Containers are isolated user-space instances that run on top of a shared host operating system kernel. The adoption of containers is rapidly increasing. Containers offer many of the same application sandboxing benefits that virtual machines (VMs) offer. However, because the hypervisor and guest operating system layers that VMs rely on have been eliminated, containers are far more lightweight.

Containers also allow the efficient packaging of application dependencies, run times, and so on directly with an application. The most commonly used container packaging format is the Docker container. An application that has been containerized in the Docker container format can be executed on any machine that can run Docker containers. This is true even if the application's dependencies are not present on the machine, because all dependencies are packaged in the container itself. For more information, visit the [Docker website](#).

Kubernetes, the popular container orchestrator, allows data scientists to launch flexible, container-based jobs and pipelines. It also enables infrastructure teams to manage and monitor ML workloads in a single managed and cloud-native environment. For more information, visit the [Kubernetes website](#).

### cnvrg.io

cnvrg.io is an AI operating system that transforms the way enterprises manage, scale, and accelerate AI and data science development from research to production. The code-first platform is built by data scientists for data scientists and offers flexibility to run on-premises or in the cloud. With model management, MLOps, and continual ML solutions, cnvrg.io brings top-of-the-line technology to data science teams so they can spend less time on DevOps and focus on the real magic—algorithms. Since using cnvrg.io, teams across industries have gotten more models to production resulting in increased business value.

### cnvrg.io Meta-Scheduler

cnvrg.io has a unique architecture that allows IT and engineers to attach different compute resources to the same control plane and have cnvrg.io manage ML jobs across all resources. This means that IT can attach multiple on-premises Kubernetes clusters, VM servers, and cloud accounts and run ML workloads on all resources, as shown in the following figure.



## **cnvrg.io Data Caching**

cnvrg.io allows data scientists to define hot and cold dataset versions with its data-caching technology. By default, datasets are stored in a centralized object storage database. Then, data scientists can cache a specific data version on the selected compute resource to save time on download and therefore increase ML development and productivity. Datasets that are cached and are not in use for a few days are automatically cleared from the selected NFS. Caching and clearing the cache can be performed with a single click; no coding, IT, or DevOps work is required.

## **cnvrg.io Flows and ML Pipelines**

cnvrg.io Flows is a tool for building production ML pipelines. Each component in a flow is a script/code running on a selected compute with a base docker image. This design enables data scientists and engineers to build a single pipeline that can run both on-premises and in the cloud. cnvrg.io makes sure data, parameters, and artifacts are moving between the different components. In addition, each flow is monitored and tracked for 100% reproducible data science.

## **cnvrg.io CORE**

cnvrg.io CORE is a free platform for the data science community to help data scientists focus more on data science and less on DevOps. CORE's flexible infrastructure gives data scientists the control to use any language, AI framework, or compute environment whether on-premises or in the cloud so they can do what they do best, build algorithms. cnvrg.io CORE can be easily installed with a single command on any Kubernetes cluster.

## **NetApp ONTAP AI**

ONTAP AI is a data center reference architecture for ML and deep learning (DL) workloads that uses NetApp AFF storage systems and NVIDIA DGX systems with Tesla V100 GPUs. ONTAP AI is based on the industry-standard NFS file protocol over 100Gb Ethernet, providing customers with a high-performance ML/DL infrastructure that uses standard data center technologies to reduce implementation and administration overhead. Using standardized network and protocols enables ONTAP AI to integrate into hybrid cloud environments while maintaining operational consistency and simplicity. As a prevalidated infrastructure solution, ONTAP AI reduces deployment time and risk and reduces administration overhead significantly, allowing customers to realize faster time to value.

## **NVIDIA DeepOps**

DeepOps is an open source project from NVIDIA that, by using Ansible, automates the deployment of GPU server clusters according to best practices. DeepOps is modular and can be used for various deployment tasks. For this document and the validation exercise that it describes, DeepOps is used to deploy a Kubernetes cluster that consists of GPU server worker nodes. For more information, visit the [DeepOps website](#).

## **NetApp Trident**

Trident is an open source storage orchestrator developed and maintained by NetApp that greatly simplifies the creation, management, and consumption of persistent storage for Kubernetes workloads. Trident itself is a Kubernetes-native application—it runs directly within a Kubernetes cluster. With Trident, Kubernetes users (developers, data scientists, Kubernetes administrators, and so on) can create, manage, and interact with persistent storage volumes in the standard Kubernetes format that they are already familiar with. At the same time, they can take advantage of NetApp advanced data management capabilities and a data fabric that is powered by NetApp technology. Trident abstracts away the complexities of persistent storage and makes it simple to consume. For more information, visit the [Trident website](#).

## **NetApp StorageGRID**

NetApp StorageGRID is a software-defined object storage platform designed to meet these needs by providing simple, cloud-like storage that users can access using the S3 protocol. StorageGRID is a scale-out system designed to support multiple nodes across internet-connected sites, regardless of distance. With the intelligent policy engine of StorageGRID, users can choose erasure-coding objects across sites for geo-resiliency or object replication between remote sites to minimize WAN access latency. StorageGrid provides an excellent private-cloud primary object storage data lake in this solution.

## **NetApp Cloud Volumes ONTAP**

NetApp Cloud Volumes ONTAP data management software delivers control, protection, and efficiency to user data with the flexibility of public cloud providers including AWS, Google Cloud Platform, and Microsoft Azure. Cloud Volumes ONTAP is cloud-native data management software built on the NetApp ONTAP storage software, providing users with a superior universal storage platform that addresses their cloud data needs. Having the same storage software in the cloud and on-premises provides users with the value of a data fabric without having to train IT staff in all-new methods to manage data.

For customers that are interested in hybrid cloud deployment models, Cloud Volumes ONTAP can provide the same capabilities and class-leading performance in most public clouds to provide a consistent and seamless user experience in any environment.

[Next: Hardware and Software Requirements](#)

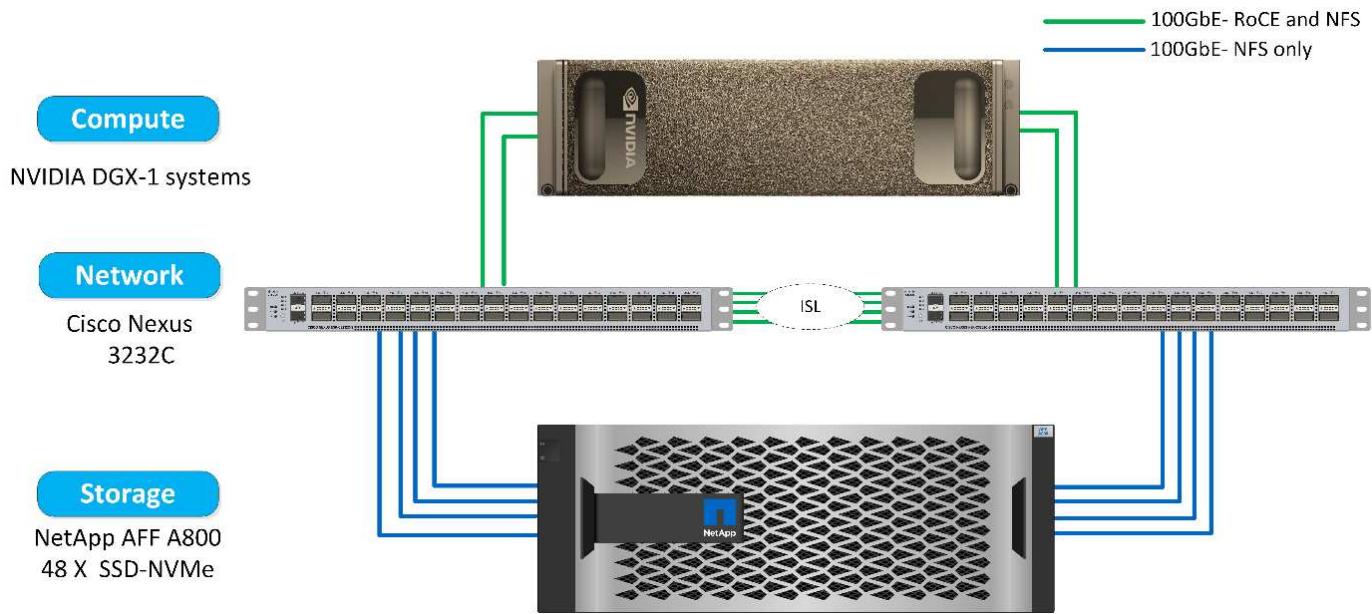
## **Hardware and Software Requirements**

This section covers the technology requirements for the ONTAP AI solution.

### **Hardware Requirements**

Although hardware requirements depend on specific customer workloads, ONTAP AI can be deployed at any scale for data engineering, model training, and production inferencing from a single GPU up to rack-scale configurations for large-scale ML/DL operations. For more information about ONTAP AI, see the [ONTAP AI website](#).

This solution was validated using a DGX-1 system for compute, a NetApp AFF A800 storage system, and Cisco Nexus 3232C for network connectivity. The AFF A800 used in this validation can support as many as 10 DGX-1 systems for most ML/DL workloads. The following figure shows the ONTAP AI topology used for model training in this validation.



To extend this solution to a public cloud, Cloud Volumes ONTAP can be deployed alongside cloud GPU compute resources and integrated into a hybrid cloud data fabric that enables customers to use whatever resources are appropriate for any given workload.

### Software Requirements

The following table shows the specific software versions used in this solution validation.

Component	Version
Ubuntu	18.04.4 LTS
NVIDIA DGX OS	4.4.0
NVIDIA DeepOps	20.02.1
Kubernetes	1.15
Helm	3.1.0
cnvrg.io	3.0.0
NetApp ONTAP	9.6P4

For this solution validation, Kubernetes was deployed as a single-node cluster on the DGX-1 system. For large-scale deployments, independent Kubernetes master nodes should be deployed to provide high availability of management services as well as reserve valuable DGX resources for ML and DL workloads.

[Next: Solution Deployment and Validation Details](#)

### Solution Deployment and Validation Details

The following sections discuss the details of solution deployment and validation.

[Next: ONTAP AI Deployment](#)

## ONTAP AI Deployment

Deployment of ONTAP AI requires the installation and configuration of networking, compute, and storage hardware. Specific instructions for deployment of the ONTAP AI infrastructure are beyond the scope of this document. For detailed deployment information, see [NVA-1121-DEPLOY: NetApp ONTAP AI, Powered by NVIDIA](#).

For this solution validation, a single volume was created and mounted to the DGX-1 system. That mount point was then mounted to the containers to make data accessible for training. For large-scale deployments, NetApp Trident automates the creation and mounting of volumes to eliminate administrative overhead and enable end-user management of resources.

[Next: Kubernetes Deployment](#)

## Kubernetes Deployment

To deploy and configure your Kubernetes cluster with NVIDIA DeepOps, perform the following tasks from a deployment jump host:

1. Download NVIDIA DeepOps by following the instructions on the [Getting Started page](#) on the NVIDIA DeepOps GitHub site.
2. Deploy Kubernetes in your cluster by following the instructions on the [Kubernetes Deployment Guide](#) on the NVIDIA DeepOps GitHub site.



For the DeepOps Kubernetes deployment to work, the same user must exist on all Kubernetes master and worker nodes.

If the deployment fails, change the value of `kubectl_localhost` to `false` in `deepops/config/group_vars/k8s-cluster.yml` and repeat step 2. The `Copy kubectl binary to ansible host` task, which executes only when the value of `kubectl_localhost` is `true`, relies on the `fetch Ansible module`, which has known memory usage issues. These memory usage issues can sometimes cause the task to fail. If the task fails because of a memory issue, then the remainder of the deployment operation does not complete successfully.

If the deployment completes successfully after you have changed the value of `kubectl_localhost` to `false`, then you must manually copy the `kubectl` binary from a Kubernetes master node to the deployment jump host. You can find the location of the `kubectl` binary on a specific master node by running the `which kubectl` command directly on that node.

[Next: Cnvrge.io Deployment](#)

## cnvrg.io Deployment

### Deploy cnvrg CORE Using Helm

Helm is the easiest way to quickly deploy cnvrg using any cluster, on-premises, Minikube, or on any cloud cluster (such as AKS, EKS, and GKE). This section describes how cnvrg was installed on an on-premises (DGX-1) instance with Kubernetes installed.

### Prerequisites

Before you can complete the installation, you must install and prepare the following dependencies on your

local machine:

- Kubectl
- Helm 3.x
- Kubernetes cluster 1.15+

## Deploy Using Helm

1. To download the most updated cnvrg helm charts, run the following command:

```
helm repo add cnvrg https://helm.cnvrg.io  
helm repo update
```

2. Before you deploy cnvrg, you need the external IP address of the cluster and the name of the node on which you will deploy cnvrg. To deploy cnvrg on an on-premises Kubernetes cluster, run the following command:

```
helm install cnvrg cnvrg/cnvrg --timeout 1500s --wait \ --set  
global.external_ip=<ip_of_cluster> \ --set global.node=<name_of_node>
```

3. Run the `helm install` command. All the services and systems automatically install on your cluster. The process can take up to 15 minutes.
4. The `helm install` command can take up to 10 minutes. When the deployment completes, go to the URL of your newly deployed cnvrg or add the new cluster as a resource inside your organization. The `helm` command informs you of the correct URL.

Thank you for installing cnvrg.io!  
Your installation of cnvrg.io is now available, and can be reached via:  
Talk to our team via email at

5. When the status of all the containers is running or complete, cnvrg has been successfully deployed. It should look similar to the following example output:

NAME	READY	STATUS	RESTARTS	AGE
cnvrg-app-69fbb9df98-6xrgf	1/1	Running	0	2m
cnvrg-sidekiq-b9d54d889-5x4fc	1/1	Running	0	2m
controller-65895b47d4-s96v6	1/1	Running	0	2m
init-app-vs-config-wv9c4	0/1	Completed	0	9m
init-gateway-vs-config-2zbpp	0/1	Completed	0	9m
init-minio-vs-config-cd2rg	0/1	Completed	0	9m
minio-0	1/1	Running	0	2m
postgres-0	1/1	Running	0	2m
redis-695c49c986-kcbt9	1/1	Running	0	2m
seeder-wh655	0/1	Completed	0	2m
speaker-5sghr	1/1	Running	0	2m

## Computer Vision Model Training with ResNet50 and the Chest X-ray Dataset

cnvrg.io AI OS was deployed on a Kubernetes setup on a NetApp ONTAP AI architecture powered by the NVIDIA DGX system. For validation, we used the NIH Chest X-ray dataset consisting of de-identified images of chest x-rays. The images were in the PNG format. The data was provided by the NIH Clinical Center and is available through the [NIH download site](#). We used a 250GB sample of the data with 627, 615 images across 15 classes.

The dataset was uploaded to the cnvrg platform and was cached on an NFS export from the NetApp AFF A800 storage system.

## Set up the Compute Resources

The cnvrg architecture and meta-scheduling capability allow engineers and IT professionals to attach different compute resources to a single platform. In our setup, we used the same cluster cnvrg that was deployed for running the deep-learning workloads. If you need to attach additional clusters, use the GUI, as shown in the following screenshot.



## Load Data

To upload data to the cnvrg platform, you can use the GUI or the cnvrg CLI. For large datasets, NetApp recommends using the CLI because it is a strong, scalable, and reliable tool that can handle a large number of files.

To upload data, complete the following steps:

1. Download the [cnvrg CLI](#).
2. navigate to the x-ray directory.
3. Initialize the dataset in the platform with the `cnvrg data init` command.
4. Upload all contents of the directory to the central data lake with the `cnvrg data sync` command. After the data is uploaded to the central object store (StorageGRID, S3, or others), you can browse with the GUI. The following figure shows a loaded chest X-ray fibrosis image PNG file. In addition, cnvrg versions the data so that any model you build can be reproduced down to the data version.



## Cach Data

To make training faster and avoid downloading 600k+ files for each model training and experiment, we used the data-caching feature after data was initially uploaded to the central data-lake object store.



After users click Cache, cnvrg downloads the data in its specific commit from the remote object store and caches it on the ONTAP NFS volume. After it completes, the data is available for instant training. In addition, if the data is not used for a few days (for model training or exploration, for example), cnvrg automatically clears the cache.

## Build an ML Pipeline with Cached Data

cnvrg flows allows you to easily build production ML pipelines. Flows are flexible, can work for any kind of ML use case, and can be created through the GUI or code. Each component in a flow can run on a different compute resource with a different Docker image, which makes it possible to build hybrid cloud and optimized ML pipelines.



## Building the Chest X-ray Flow: Setting Data

We added our dataset to a newly created flow. When adding the dataset, you can select the specific version (commit) and indicate whether you want the cached version. In this example, we selected the cached commit.



## Building the Chest X-ray Flow: Setting Training Model: ResNet50

In the pipeline, you can add any kind of custom code you want. In cnvrg, there is also the AI library, a reusable ML components collection. In the AI library, there are algorithms, scripts, data sources, and other solutions that can be used in any ML or deep learning flow. In this example, we selected the prebuilt ResNet50 module. We used default parameters such as batch\_size:128, epochs:10, and more. These parameters can be viewed in the AI Library docs. The following screenshot shows the new flow with the X-ray dataset connected to ResNet50.



## Define the Compute Resource for ResNet50

Each algorithm or component in cnvrg flows can run on a different compute instance, with a different Docker image. In our setup, we wanted to run the training algorithm on the NVIDIA DGX systems with the NetApp ONTAP AI architecture. In The following figure, we selected `gpu-real`, which is a compute template and specification for our on-premises cluster. We also created a queue of templates and selected multiple templates. In this way, if the `gpu-real` resource cannot be allocated (if, for example, other data scientists are using it), then you can enable automatic cloud-bursting by adding a cloud provider template. The following screenshot shows the use of `gpu-real` as a compute node for ResNet50.



## Tracking and Monitoring Results

After a flow is executed, cnvrg triggers the tracking and monitoring engine. Each run of a flow is automatically documented and updated in real time. Hyperparameters, metrics, resource usage (GPU utilization, and more), code version, artifacts, logs, and so on are automatically available in the Experiments section, as shown in the following two screenshots.

**X-ray train (ResNet50)**  
by yochz

**Status:** Success Duration: 33m 54s

**Input:** python3 resnet50.py --data /data/x-ray-sample-splitted --data\_test None --output\_model model.h5 --val\_size 0.2

**Start Time:** 22-Mar-2020, 3:55:37 PM    **End Time:** 22-Mar-2020, 4:29:22 PM    **Duration:** 33m 45s    **Compute:** gpu-real    **Image:** tensorflow:20.01-tf2-py3

**Start Commit:** e0854e73    **End Commit:** a980dd8e

**CPU**    **Memory**    **Block IO**    **GPU**    **GPU Memory**

**Classes list:** ["No Finding", "Hemato", "Fibrosis", "Pleural\_Thickening", "Mass", "Infiltration", "Effusion", "Cardiomegaly", "Atelectasis", "Edema", "Consolidation", "Touch Bar Shot 2020-03-12 at 7.53.13 PM.png", "Pneumonia", "Pneumothorax", "Nodule", "Emphysema"]

**Model:** resnet50    **GPU Found:** 1    **tensorflow local version:** 2.0.0

**GridSearch\_ID:** 2451r    **output\_layer\_activation:** softmax    **hidden\_layer\_activation:** relu    **pooling\_height:** 2  
**pooling\_width:** 2    **conv\_height:** 3    **conv\_width:** 3    **image\_height:** 224  
**image\_width:** 224    **optimizer:** adam    **dropout:** 0.3    **image\_color:** rgb  
**batch\_size:** 1024    **steps\_per\_epoch:** 10    **epoches:** 10    **val\_size:** 0.2  
**output\_model:** model.h5    **data\_test:** None

**loss**

Epoch	Experiment 50 Loss
0	2.35
1	1.85
2	1.75
3	1.70
4	1.68
5	1.67
6	1.66
7	1.65
8	1.64
9	1.63
10	1.62
11	1.61



Next: Conclusion

## Conclusion

NetApp and cnvrg.io have partnered to offer customers a complete data management solution for ML and DL software development. ONTAP AI provides high-performance compute and storage for any scale of operation, and cnvrg.io software streamlines data science workflows and improves resource utilization.

Next: [Acknowledgments](#)

## Acknowledgments

- Mike Oglesby, Technical Marketing Engineer, NetApp
- Santosh Rao, Senior Technical Director, NetApp

Next: [Where to Find Additional Information](#)

## Where to Find Additional Information

To learn more about the information that is described in this document, see the following resources:

- Cnvrg.io (<https://cnvrg.io>):
  - Cnvrg CORE (free ML platform)  
<https://cnvrg.io/platform/core>
  - Cnvrg docs  
<https://app.cnvrg.io/docs>
- NVIDIA DGX-1 servers:
  - NVIDIA DGX-1 servers  
<https://www.nvidia.com/en-us/data-center/dgx-1/>
  - NVIDIA Tesla V100 Tensor Core GPU  
<https://www.nvidia.com/en-us/data-center/tesla-v100/>
  - NVIDIA GPU Cloud (NGC)  
<https://www.nvidia.com/en-us/gpu-cloud/>
- NetApp AFF systems:
  - AFF datasheet  
<https://www.netapp.com/us/media/d-3582.pdf>
  - NetApp FlashAdvantage for AFF  
<https://www.netapp.com/us/media/ds-3733.pdf>
  - ONTAP 9.x documentation

<http://mysupport.netapp.com/documentation/productlibrary/index.html?productID=62286>

- NetApp FlexGroup technical report

<https://www.netapp.com/us/media/tr-4557.pdf>

- NetApp persistent storage for containers:

- NetApp Trident

<https://netapp.io/persistent-storage-provisioner-for-kubernetes/>

- NetApp Interoperability Matrix:

- NetApp Interoperability Matrix Tool

<http://support.netapp.com/matrix>

- ONTAP AI networking:

- Cisco Nexus 3232C Switches

<https://www.cisco.com/c/en/us/products/switches/nexus-3232c-switch/index.html>

- Mellanox Spectrum 2000 series switches

[http://www.mellanox.com/page/products\\_dyn?product\\_family=251&mtag=sn2000](http://www.mellanox.com/page/products_dyn?product_family=251&mtag=sn2000)

- ML framework and tools:

- DALI

<https://github.com/NVIDIA/DALI>

- TensorFlow: An Open-Source Machine Learning Framework for Everyone

<https://www.tensorflow.org/>

- Horovod: Uber's Open-Source Distributed Deep Learning Framework for TensorFlow

<https://eng.uber.com/horovod/>

- Enabling GPUs in the Container Runtime Ecosystem

<https://devblogs.nvidia.com/gpu-containers-runtime/>

- Docker

<https://docs.docker.com>

- Kubernetes

<https://kubernetes.io/docs/home/>

- NVIDIA DeepOps

<https://github.com/NVIDIA/deepops>

- Kubeflow  
<http://www.kubeflow.org/>
- Jupyter Notebook Server  
<http://www.jupyter.org/>
- Dataset and benchmarks:
  - NIH chest X-ray dataset  
<https://nihcc.app.box.com/v/ChestXray-NIHCC>
  - Xiaosong Wang, Yifan Peng, Le Lu, Zhiyong Lu, Mohammadadi Bagheri, Ronald Summers, ChestX-ray8: Hospital-scale Chest X-ray Database and Benchmarks on Weakly-Supervised Classification and Localization of Common Thorax Diseases, IEEE CVPR, pp. 3462-3471, 2017TR-4841-0620

## AI Inferencing at the Edge - NetApp with Lenovo ThinkSystem - Solution Design

### TR-4886: AI Inferencing at the Edge - NetApp with Lenovo ThinkSystem - Solution Design

Sathish Thyagarajan, NetApp  
 Miroslav Hodak, Lenovo

#### Summary

Several emerging application scenarios, such as advanced driver-assistance systems (ADAS), Industry 4.0, smart cities, and Internet of Things (IoT), require the processing of continuous data streams under a near-zero latency. This document describes a compute and storage architecture to deploy GPU-based artificial intelligence (AI) inferencing on NetApp storage controllers and Lenovo ThinkSystem servers in an edge environment that meets these requirements. This document also provides performance data for the industry standard MLPerf Inference benchmark, evaluating various inference tasks on edge servers equipped with NVIDIA T4 GPUs. We investigate the performance of offline, single stream, and multistream inference scenarios and show that the architecture with a cost-effective shared networked storage system is highly performant and provides a central point for data and model management for multiple edge servers.

#### Introduction

Companies are increasingly generating massive volumes of data at the network edge. To achieve maximum value from smart sensors and IoT data, organizations are looking for a real-time event streaming solution that enables edge computing. Computationally demanding jobs are therefore increasingly performed at the edge, outside of data centers. AI inference is one of the drivers of this trend. Edge servers provide sufficient computational power for these workloads, especially when using accelerators, but limited storage is often an issue, especially in multiserver environments. In this document we show how you can deploy a shared storage system in the edge environment and how it benefits AI inference workloads without imposing a performance penalty.

This document describes a reference architecture for AI inference at the edge. It combines multiple Lenovo ThinkSystem edge servers with a NetApp storage system to create a solution that is easy to deploy and manage. It is intended to be a baseline guide for practical deployments in various situations, such as the factory floor with multiple cameras and industrial sensors, point-of-sale (POS) systems in retail transactions, or Full Self-Driving (FSD) systems that identify visual anomalies in autonomous vehicles.

This document covers testing and validation of a compute and storage configuration consisting of Lenovo

ThinkSystem SE350 Edge Server and an entry-level NetApp AFF and EF-Series storage system. The reference architectures provide an efficient and cost-effective solution for AI deployments while also providing comprehensive data services, integrated data protection, seamless scalability, and cloud connected data storage with NetApp ONTAP and NetApp SANtricity data management software.

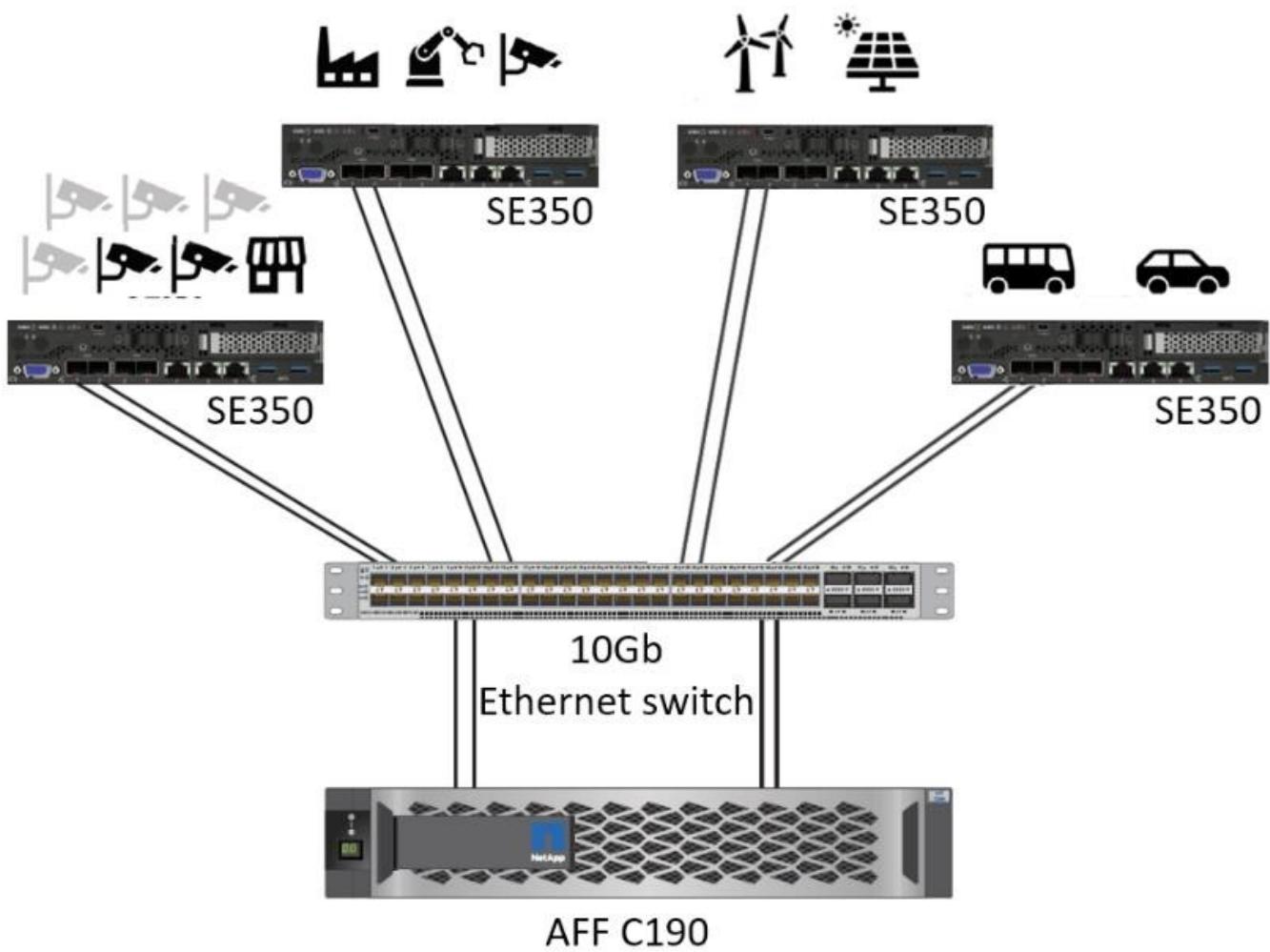
## Target audience

This document is intended for the following audiences:

- Business leaders and enterprise architects who want to productize AI at the edge.
- Data scientists, data engineers, AI/machine learning (ML) researchers, and developers of AI systems.
- Enterprise architects who design solutions for the development of AI/ML models and applications.
- Data scientists and AI engineers looking for efficient ways to deploy deep learning (DL) and ML models.
- Edge device managers and edge server administrators responsible for deployment and management of edge inferencing models.

## Solution architecture

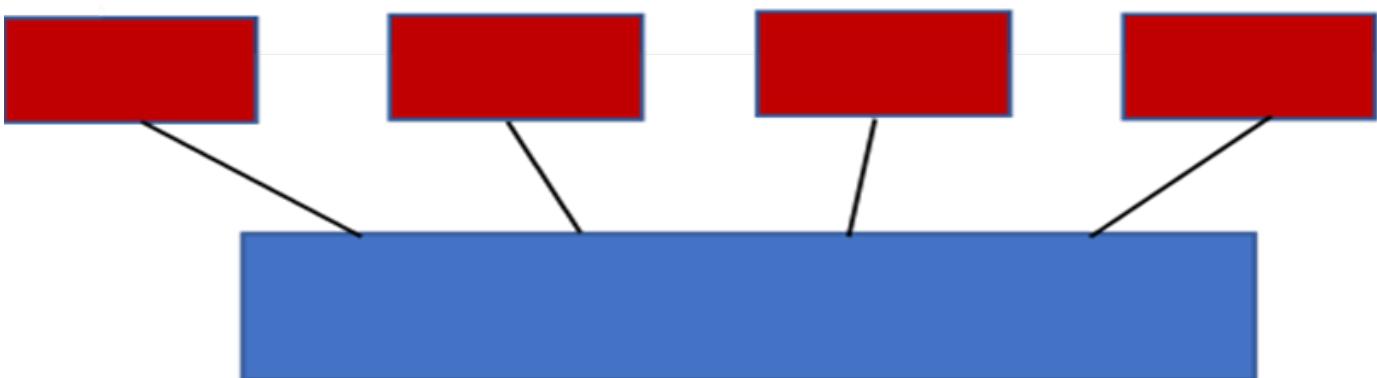
This Lenovo ThinkSystem server and NetApp ONTAP or NetApp SANtricity storage solution is designed to handle AI inferencing on large datasets using the processing power of GPUs alongside traditional CPUs. This validation demonstrates high performance and optimal data management with an architecture that uses either single or multiple Lenovo SR350 edge servers interconnected with a single NetApp AFF storage system, as shown in the following two figures.





The logical architecture overview in the following figure shows the roles of the compute and storage elements in this architecture. Specifically, it shows the following:

- Edge compute devices performing inference on the data it receives from cameras, sensors, and so on.
- A shared storage element that serves multiple purposes:
  - Provides a central location for inference models and other data needed to perform the inference. Compute servers access the storage directly and use inference models across the network without the need to copy them locally.
  - Updated models are pushed here.
  - Archives input data that edge servers receive for later analysis. For example, if the edge devices are connected to cameras, the storage element keeps the videos captured by the cameras.



red	blue
Lenovo compute system	NetApp AFF storage system
Edge devices performing inference on inputs from cameras, sensors, and so on.	Shared storage holding inference models and data from edge devices for later analysis.

This NetApp and Lenovo solution offers the following key benefits:

- GPU accelerated computing at the edge.
- Deployment of multiple edge servers backed and managed from a shared storage.
- Robust data protection to meet low recovery point objectives (RPOs) and recovery time objectives (RTOs) with no data loss.
- Optimized data management with NetApp Snapshot copies and clones to streamline development workflows.

## How to use this architecture

This document validates the design and performance of the proposed architecture. However, we have not tested certain software-level pieces, such as container, workload, or model management and data synchronization with cloud or data center on-premises, because they are specific to a deployment scenario. Here, multiple choices exist.

At the container management level, Kubernetes container management is a good choice and is well supported in either a fully upstream version (Canonical) or in a modified version suitable for enterprise deployments (Red Hat). The [NetApp AI Control Plane](#) which uses NetApp Trident and the newly added [NetApp DataOps Toolkit](#) provides built-in traceability, data management functions, interfaces, and tools for data scientists and data engineers to integrate with NetApp storage. Kubeflow, the ML toolkit for Kubernetes, provides additional AI capabilities along with a support for model versioning and KFServing on several platforms such as TensorFlow Serving or NVIDIA Triton Inference Server. Another option is NVIDIA EGX platform, which provides workload management along with access to a catalog of GPU-enabled AI inference containers. However, these options might require significant effort and expertise to put them into production and might require the assistance of a third-party independent software vendor (ISV) or consultant.

## Solution areas

The key benefit of AI inferencing and edge computing is the ability of devices to compute, process, and analyze data with a high level of quality without latency. There are far too many examples of edge computing use cases to describe in this document, but here are a few prominent ones:

### Automobiles: Autonomous vehicles

The classic edge computing illustration is in the advanced driver-assistance systems (ADAS) in autonomous vehicles (AV). The AI in driverless cars must rapidly process a lot of data from cameras and sensors to be a successful safe driver. Taking too long to interpret between an object and a human can mean life or death, therefore being able to process that data as close to the vehicle as possible is crucial. In this case, one or more edge compute servers handles the input from cameras, RADAR, LiDAR, and other sensors, while shared storage holds inference models and stores input data from sensors.

### Healthcare: Patient monitoring

One of the greatest impacts of AI and edge computing is its ability to enhance continuous monitoring of patients for chronic diseases both in at-home care and intensive care units (ICUs). Data from edge devices

that monitor insulin levels, respiration, neurological activity, cardiac rhythm, and gastrointestinal functions require instantaneous analysis of data that must be acted on immediately because there is limited time to act to save someone's life.

### **Retail: Cashier-less payment**

Edge computing can power AI and ML to help retailers reduce checkout time and increase foot traffic. Cashier-less systems support various components, such as the following:

- Authentication and access. Connecting the physical shopper to a validated account and permitting access to the retail space.
- Inventory monitoring. Using sensors, RFID tags, and computer vision systems to help confirm the selection or deselection of items by shoppers.

Here, each of the edge servers handle each checkout counter and the shared storage system serves as a central synchronization point.

### **Financial services: Human safety at kiosks and fraud prevention**

Banking organizations are using AI and edge computing to innovate and create personalized banking experiences. Interactive kiosks using real-time data analytics and AI inferencing now enable ATMs to not only help customers withdraw money, but proactively monitor kiosks through the images captured from cameras to identify risk to human safety or fraudulent behavior. In this scenario, edge compute servers and shared storage systems are connected to interactive kiosks and cameras to help banks collect and process data with AI inference models.

### **Manufacturing: Industry 4.0**

The fourth industrial revolution (Industry 4.0) has begun, along with emerging trends such as Smart Factory and 3D printing. To prepare for a data-led future, large-scale machine-to-machine (M2M) communication and IoT are integrated for increased automation without the need for human intervention. Manufacturing is already highly automated and adding AI features is a natural continuation of the long-term trend. AI enables automating operations that can be automated with the help of computer vision and other AI capabilities. You can automate quality control or tasks that rely on human vision or decision making to perform faster analyses of materials on assembly lines in factory floors to help manufacturing plants meet the required ISO standards of safety and quality management. Here, each compute edge server is connected to an array of sensors monitoring the manufacturing process and updated inference models are pushed to the shared storage, as needed.

### **Telecommunications: Rust detection, tower inspection, and network optimization**

The telecommunications industry uses computer vision and AI techniques to process images that automatically detect rust and identify cell towers that contain corrosion and, therefore, require further inspection. The use of drone images and AI models to identify distinct regions of a tower to analyze rust, surface cracks, and corrosion has increased in recent years. The demand continues to grow for AI technologies that enable telecommunication infrastructure and cell towers to be inspected efficiently, assessed regularly for degradation, and repaired promptly when required.

Additionally, another emerging use case in telecommunication is the use of AI and ML algorithms to predict data traffic patterns, detect 5G-capable devices, and automate and augment multiple-input and multiple-output (MIMO) energy management. MIMO hardware is used at radio towers to increase network capacity; however, this comes with additional energy costs. ML models for "MIMO sleep mode" deployed at cell sites can predict the efficient use of radios and help reduce energy consumption costs for mobile network operators (MNOs). AI inferencing and edge computing solutions help MNOs reduce the amount of data transmitted back-and-forth to

data centers, lower their TCO, optimize network operations, and improve overall performance for end users.

[Next: Technology overview.](#)

## Technology overview

[Previous: Introduction.](#)

### NetApp AFF systems

State-of-the-art NetApp AFF storage systems enable AI inference deployments at the edge to meet enterprise storage requirements with industry-leading performance, superior flexibility, cloud integration, and best-in class data management. Designed specifically for flash, NetApp AFF systems help accelerate, manage, and protect business-critical data.

- Entry-level NetApp AFF storage systems are based on FAS2750 hardware and SSD flash media
- Two controllers in HA configuration



NetApp entry-level AFF C190 storage systems support the following features:

- A maximum drive count of 24x 960GB SSDs
- Two possible configurations:
  - Ethernet (10GbE): 4x 10GBASE-T (RJ-45) ports
  - Unified (16Gb FC or 10GbE): 4x unified target adapter 2 (UTA2) ports
- A maximum of 50.5TB effective capacity



For NAS workloads, a single entry-level AFF C190 system supports throughput of 4.4GBps for sequential reads and 230K IOPS for small random reads at latencies of 1ms or less.

### NetApp AFF A220

NetApp also offers other entry-level storage systems that provide higher performance and scalability for larger-scale deployments. For NAS workloads, a single entry-level AFF A220 system supports:

- Throughput of 6.2GBps for sequential reads
- 375K IOPS for small random reads at latencies of 1ms or less
- Maximum drive count of 144x 960GB, 3.8TB, or 7.6TB SSDs
- AFF A220 scales to larger than 1PB of effective capacity

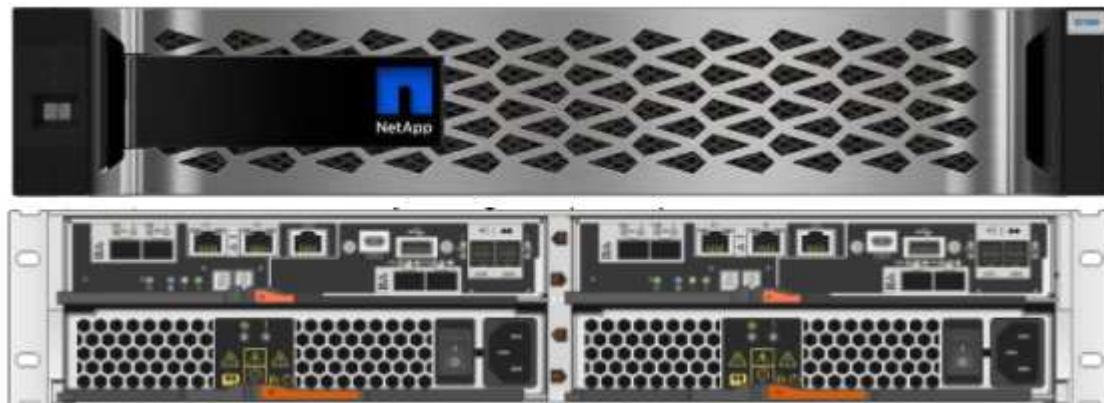
#### **NetApp AFF A250**

- Maximum effective capacity is 35PB with maximum scale out 2-24 nodes (12 HA pairs)
- Provides ≥ 45% performance increase over AFF A220
- 440k IOPS random reads @1ms
- Built on the latest NetApp ONTAP release: ONTAP 9.8
- Leverages two 25Gb Ethernet for HA and cluster interconnect

#### **NetApp E-Series EF Systems**

The EF-Series is a family of entry-level and mid-range all-flash SAN storage arrays that can accelerate access to your data and help you derive value from it faster with NetApp SANtricity software. These systems offer both SAS and NVMe flash storage and provide you with affordable to extreme IOPS, response times under 100 microseconds, and bandwidth up to 44GBps—making them ideal for mixed workloads and demanding applications such as AI inferencing and high-performance computing (HPC).

The following figure shows the NetApp EF280 storage system.



#### **NetApp EF280**

- 32Gb/16Gb FC, 25Gb/10Gb iSCSI, and 12Gb SAS support
- Maximum effective capacity is 96 drives totaling 1.5PB
- Throughput of 10GBps (sequential reads)
- 300K IOPs (random reads)
- The NetApp EF280 is the lowest cost all-flash array (AFA) in the NetApp portfolio

#### **NetApp EF300**

- 24x NVMe SSD drives for a total capacity of 367TB

- Expansion options totaling 240x NL-SAS HDDs, 96x SAS SSDs, or a combination
- 100Gb NVMe/IB, NVMe/RoCE, iSER/IB, and SRP/IB
- 32Gb NVME/FC, FCP
- 25Gb iSCSI
- 20GBps (sequential reads)
- 670K IOPs (random reads)



For more information, see the [NetApp EF-Series NetApp EF-Series all-flash arrays EF600, F300, EF570, and EF280 datasheet](#).

## NetApp ONTAP 9

ONTAP 9.8.1, the latest generation of storage management software from NetApp, enables businesses to modernize infrastructure and transition to a cloud-ready data center. Leveraging industry-leading data management capabilities, ONTAP enables the management and protection of data with a single set of tools, regardless of where that data resides. You can also move data freely to wherever it is needed: the edge, the core, or the cloud. ONTAP 9.8.1 includes numerous features that simplify data management, accelerate and protect critical data, and enable next generation infrastructure capabilities across hybrid cloud architectures.

### Simplify data management

Data management is crucial to enterprise IT operations so that appropriate resources are used for applications and datasets. ONTAP includes the following features to streamline and simplify operations and reduce the total cost of operation:

- **Inline data compaction and expanded deduplication.** Data compaction reduces wasted space inside storage blocks, and deduplication significantly increases effective capacity. This applies to data stored locally and data tiered to the cloud.
- **Minimum, maximum, and adaptive quality of service (AQoS).** Granular quality of service (QoS) controls help maintain performance levels for critical applications in highly shared environments.
- **NetApp FabricPool.** This feature provides automatic tiering of cold data to public and private cloud storage options, including Amazon Web Services (AWS), Azure, and NetApp StorageGRID storage solution. For more information about FabricPool, see [TR-4598](#).

### Accelerate and protect data

ONTAP 9 delivers superior levels of performance and data protection and extends these capabilities in the following ways:

- **Performance and lower latency.** ONTAP offers the highest possible throughput at the lowest possible latency.
- **Data protection.** ONTAP provides built-in data protection capabilities with common management across all platforms.
- **NetApp Volume Encryption (NVE).** ONTAP offers native volume-level encryption with both onboard and External Key Management support.
- **Multitenancy and multifactor authentication.** ONTAP enables sharing of infrastructure resources with the highest levels of security.

## Future-proof infrastructure

ONTAP 9 helps meet demanding and constantly changing business needs with the following features:

- **Seamless scaling and nondisruptive operations.** ONTAP supports the nondisruptive addition of capacity to existing controllers and to scale-out clusters. Customers can upgrade to the latest technologies, such as NVMe and 32Gb FC, without costly data migrations or outages.
- **Cloud connection.** ONTAP is the most cloud-connected storage management software, with options for software-defined storage (ONTAP Select) and cloud-native instances (NetApp Cloud Volumes Service) in all public clouds.
- **Integration with emerging applications.** ONTAP offers enterprise-grade data services for next generation platforms and applications, such as autonomous vehicles, smart cities, and Industry 4.0, by using the same infrastructure that supports existing enterprise apps.

## NetApp SANtricity

NetApp SANtricity is designed to deliver industry-leading performance, reliability, and simplicity to E-Series hybrid-flash and EF-Series all-flash arrays. Achieve maximum performance and utilization of your E-Series hybrid-flash and EF-Series all-flash arrays for heavy-workload applications, including data analytics, video surveillance, and backup and recovery. With SANtricity, configuration tweaking, maintenance, capacity expansion, and other tasks can be completed while the storage stays online. SANtricity also provides superior data protection, proactive monitoring, and certified security—all accessible through the easy-to-use, on-box System Manager interface. To learn more, see the [NetApp E-Series SANtricity Software datasheet](#).

## Performance optimized

Performance-optimized SANtricity software delivers data—with high IOPs, high throughput, and low latency—to all your data analytics, video surveillance, and backup apps. Accelerate performance for high-IOPS, low-latency applications and high-bandwidth, high-throughput applications.

## Maximize uptime

Complete all your management tasks while the storage stays online. Tweak configurations, perform maintenance, or expand capacity without disrupting I/O. Realize best-in-class reliability with automated features, online configuration, state-of-the-art Dynamic Disk Pools (DPP) technology, and more.

## Rest easy

SANtricity software delivers superior data protection, proactive monitoring, and certified security—all through the easy-to-use, on-box System Manager interface. Simplify storage-management chores. Gain the flexibility you need for advanced tuning of all E-Series storage systems. Manage your NetApp E-Series system—anytime, anywhere. Our on-box, web-based interface streamlines your management workflow.

## NetApp Trident

Trident from NetApp is an open-source dynamic storage orchestrator for Docker and Kubernetes that simplifies the creation, management, and consumption of persistent storage. Trident, a Kubernetes native application, runs directly within a Kubernetes cluster. Trident enables customers to seamlessly deploy DL container images onto NetApp storage and provides an enterprise-grade experience for AI container deployments. Kubernetes users (such as ML developers and data scientists) can create, manage, and automate orchestration and cloning to take advantage of NetApp advanced data management capabilities powered by NetApp technology.

## **NetApp Cloud Sync**

[Cloud Sync](#) is a NetApp service for rapid and secure data synchronization. Whether you need to transfer files between on-premises NFS or SMB file shares, NetApp StorageGRID, NetApp ONTAP S3, NetApp Cloud Volumes Service, Azure NetApp Files, Amazon Simple Storage Service (Amazon S3), Amazon Elastic File System (Amazon EFS), Azure Blob, Google Cloud Storage, or IBM Cloud Object Storage, Cloud Sync moves the files where you need them quickly and securely. After your data is transferred, it is fully available for use on both source and target. Cloud Sync continuously synchronizes the data, based on your predefined schedule, moving only the deltas, so time and money spent on data replication is minimized. Cloud Sync is a software as a service (SaaS) tool that is extremely simple to set up and use. Data transfers that are triggered by Cloud Sync are carried out by data brokers. You can deploy Cloud Sync data brokers in AWS, Azure, Google Cloud Platform, or on-premises.

## **Lenovo ThinkSystem servers**

Lenovo ThinkSystem servers feature innovative hardware, software, and services that solve customers' challenges today and deliver an evolutionary, fit-for-purpose, modular design approach to address tomorrow's challenges. These servers capitalize on best-in-class, industry-standard technologies coupled with differentiated Lenovo innovations to provide the greatest possible flexibility in x86 servers.

Key advantages of deploying Lenovo ThinkSystem servers include:

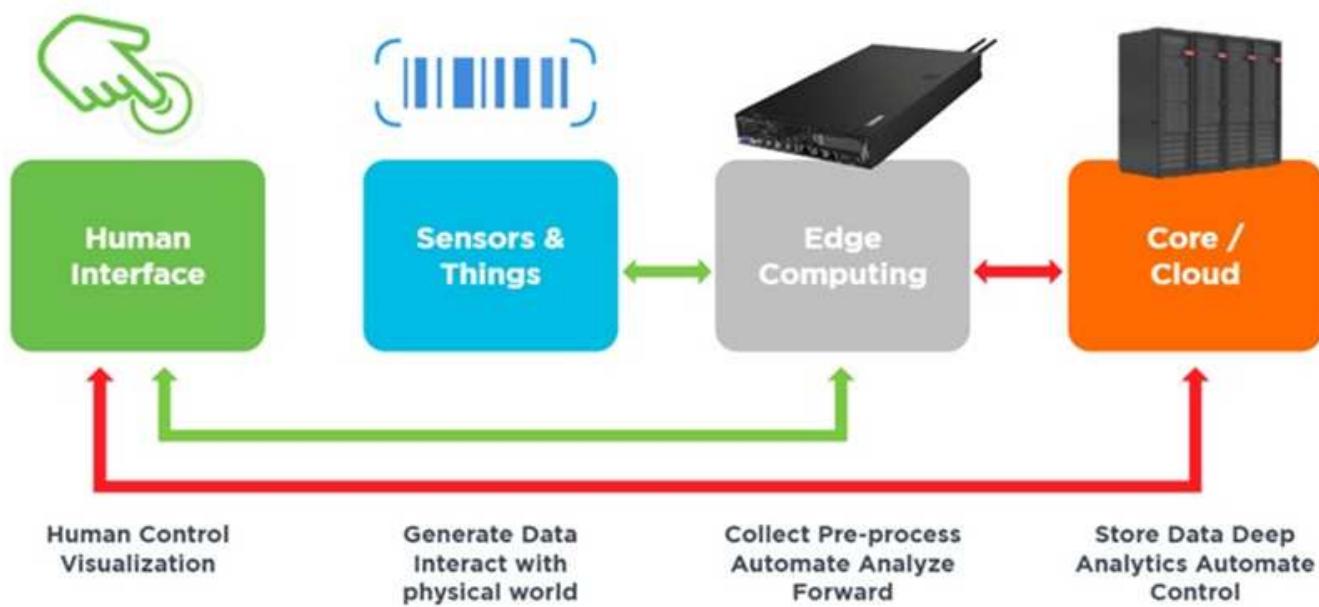
- Highly scalable, modular designs to grow with your business
- Industry-leading resilience to save hours of costly unscheduled downtime
- Fast flash technologies for lower latencies, quicker response times, and smarter data management in real time

In the AI area, Lenovo is taking a practical approach to helping enterprises understand and adopt the benefits of ML and AI for their workloads. Lenovo customers can explore and evaluate Lenovo AI offerings in Lenovo AI Innovation Centers to fully understand the value for their particular use case. To improve time to value, this customer-centric approach gives customers proof of concept for solution development platforms that are ready to use and optimized for AI.

## **Lenovo ThinkSystem SE350 Edge Server**

Edge computing allows data from IoT devices to be analyzed at the edge of the network before being sent to the data center or cloud. The Lenovo ThinkSystem SE350, as shown in the figure below, is designed for the unique requirements for deployment at the edge, with a focus on flexibility, connectivity, security, and remote manageability in a compact ruggedized and environmentally hardened form factor.

Featuring the Intel Xeon D processor with the flexibility to support acceleration for edge AI workloads, the SE350 is purpose-built for addressing the challenge of server deployments in a variety of environments outside the data center.



## MLPerf

MLPerf is the industry-leading benchmark suite for evaluating AI performance. It covers many areas of applied AI including image classification, object detection, medical imaging, and natural language processing (NLP). In this validation, we used Inference v0.7 workloads, which is the latest iteration of the MLPerf Inference at the completion of this validation. The [MLPerf Inference v0.7](#) suite includes four new benchmarks for data center and edge systems:

- **BERT.** Bi-directional Encoder Representation from Transformers (BERT) fine-tuned for question answering by using the SQuAD dataset.
- **DLRM.** Deep Learning Recommendation Model (DLRM) is a personalization and recommendation model that is trained to optimize click-through rates (CTR).
- **3D U-Net.** 3D U-Net architecture is trained on the Brain Tumor Segmentation (BraTS) dataset.
- **RNN-T.** Recurrent Neural Network Transducer (RNN-T) is an automatic speech recognition (ASR) model

that is trained on a subset of LibriSpeech. MLPerf Inference results and code are publicly available and released under Apache license. MLPerf Inference has an Edge division, which supports the following scenarios:

- **Single stream.** This scenario mimics systems where responsiveness is a critical factor, such as offline AI queries performed on smartphones. Individual queries are sent to the system and response times are recorded. 90th percentile latency of all the responses is reported as the result.
- **Multistream.** This benchmark is for systems that process input from multiple sensors. During the test, queries are sent at a fixed time interval. A QoS constraint (maximum allowed latency) is imposed. The test reports the number of streams that the system can process while meeting the QoS constraint.
- **Offline.** This is the simplest scenario covering batch processing applications and the metric is throughput in samples per second. All data is available to the system and the benchmark measures the time it takes to process all the samples.

Lenovo has published MLPerf Inference scores for SE350 with T4, the server used in this document. See the results at <https://mlperf.org/inference-results-0-7/> in the “Edge, Closed Division” section in entry #0.7-145.

[Next: Test plan.](#)

## Test plan

[Previous: Technology overview.](#)

This document follows MLPerf Inference v0.7 [code](#), MLPerf Inference v1.1 [code](#), and [rules](#). We ran MLPerf benchmarks designed for inference at the edge as defined in the follow table.

Area	Task	Model	Dataset	QSL size	Quality	Multistream latency constraint
Vision	Image classification	Resnet50v1.5	ImageNet (224x224)	1024	99% of FP32	50ms
Vision	Object detection (large)	SSD-ResNet34	COCO (1200x1200)	64	99% of FP32	66ms
Vision	Object detection (small)	SSD-MobileNetsv1	COCO (300x300)	256	99% of FP32	50ms
Vision	Medical image segmentation	3D UNET	BraTS 2019 (224x224x160 )	16	99% and 99.9% of FP32	n/a
Speech	Speech-to-text	RNNT	Librispeech dev-clean	2513	99% of FP32	n/a
Language	Language processing	BERT	SQuAD v1.1	10833	99% of FP32	n/a

The following table presents Edge benchmark scenarios.

Area	Task	Scenarios
Vision	Image classification	Single stream, offline, multistream

Area	Task	Scenarios
Vision	Object detection (large)	Single stream, offline, multistream
Vision	Object detection (small)	Single stream, offline, multistream
Vision	Medical image segmentation	Single stream, offline
Speech	Speech-to-text	Single stream, offline
Language	Language processing	Single stream, offline

We performed these benchmarks using the networked storage architecture developed in this validation and compared results to those from local runs on the edge servers previously submitted to MLPerf. The comparison is to determine how much impact the shared storage has on inference performance.

[Next: Test configuration.](#)

## Test configuration

[Previous: Test plan.](#)

The following figure shows the test configuration. We used the NetApp AFF C190 storage system and two Lenovo ThinkSystem SE350 servers (each with one NVIDIA T4 accelerator). These components are connected through a 10GbE network switch. The network storage holds validation/test datasets and pretrained models. The servers provide computational capability, and the storage is accessed over NFS protocol.

This section describes the tested configurations, the network infrastructure, the SE350 server, and the storage provisioning details. The following table lists the base components for the solution architecture.

Solution components	Details
Lenovo ThinkSystem servers	<ul style="list-style-type: none"> <li>2x SE350 servers each with one NVIDIA T4 GPU card</li> </ul>
	<ul style="list-style-type: none"> <li>Each server contains one Intel Xeon D-2123IT CPU with four physical cores running at 2.20GHz and 128GB RAM</li> </ul>
Entry-level NetApp AFF storage system (HA pair)	<ul style="list-style-type: none"> <li>NetApp ONTAP 9 software</li> <li>24x 960GB SSDs</li> <li>NFS protocol</li> <li>One interface group per controller, with four logical IP addresses for mount points</li> </ul>



The following table lists the storage configuration: AFF C190 with 2RU, 24 drive slots.

Controller	Aggregate	FlexGroup volume	Aggregatesize	Volumesize	Operating systemmount point
Controller1	Aggr1	/netapplenovo_AI_fg	8.42TiB	15TB	/netapp_lenovo_fg
Controller2	Aggr2		8.42TiB		

The /netappLenovo\_AI\_fg folder contains the datasets used for model validation.

The figure below shows the test configuration. We used the NetApp EF280 storage system and two Lenovo ThinkSystem SE350 servers (each with one NVIDIA T4 accelerator). These components are connected through a 10GbE network switch. The network storage holds validation/test datasets and pretrained models. The servers provide computational capability, and the storage is accessed over NFS protocol.

The following table lists the storage configuration for EF280.

Controller	Volume Group	Volume	Volumesize	DDPsize	Connection method
Controller1	DDP1	Volume 1	8.42TiB	16TB	SE350-1 to iSCSI LUN 0
Controller2		Volume 2	8.42TiB		SE350-2 to iSCSI LUN 1



[Next: Test procedure.](#)

## Test procedure

[Previous: Test configuration.](#)

We used the following test procedure in this validation.

## Operating system and AI inference setup

For AFF C190, we used Ubuntu 18.04 with NVIDIA drivers and docker with support for NVIDIA GPUs and used MLPerf [code](#) available as a part of the Lenovo submission to MLPerf Inference v0.7.

For EF280, we used Ubuntu 20.04 with NVIDIA drivers and docker with support for NVIDIA GPUs and MLPerf [code](#) available as a part of the Lenovo submission to MLPerf Inference v1.1.

To set up the AI inference, follow these steps:

1. Download datasets that require registration, the ImageNet 2012 Validation set, Criteo Terabyte dataset, and BraTS 2019 Training set, and then unzip the files.
2. Create a working directory with at least 1TB and define environmental variable `MLPERF_SCRATCH_PATH` referring to the directory.

You should share this directory on the shared storage for the network storage use case, or the local disk when testing with local data.

3. Run the `make prebuild` command, which builds and launches the docker container for the required inference tasks.



The following commands are all executed from within the running docker container:

- Download pretrained AI models for MLPerf Inference tasks: `make download_model`
- Download additional datasets that are freely downloadable: `make download_data`
- Preprocess the data: `make preprocess_data`
- Run: `make build`.
- Build inference engines optimized for the GPU in compute servers: `make generate_engines`
- To run Inference workloads, run the following (one command):

```
make run_harness RUN_ARGS="--benchmarks=<BENCHMARKS>
--scenarios=<SCENARIOS>"
```

## AI inference runs

Three types of runs were executed:

- Single server AI inference using local storage
- Single server AI inference using network storage
- Multi-server AI inference using network storage

[Next: Test results.](#)

## Test results

[Previous: Test procedure.](#)

### Test results for AFF

A multitude of tests were run to evaluate the performance of the proposed architecture. There are six different workloads (image classification, object detection [small], object detection [large], medical imaging, speech-to-text, and natural language processing [NLP]), which you can run in three different scenarios: offline, single stream, and multistream.



The last scenario is implemented only for image classification and object detection.

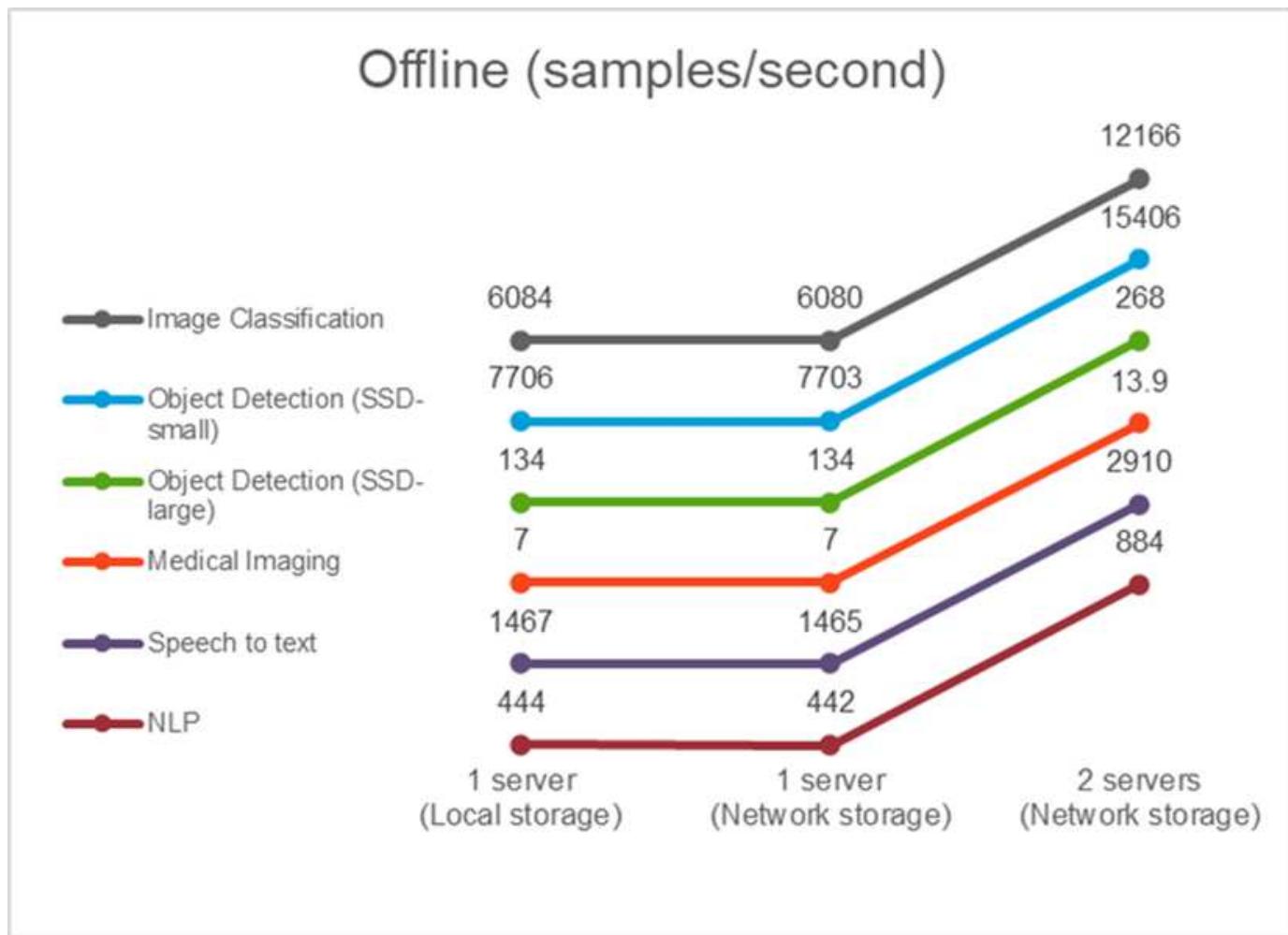
This gives 15 possible workloads, which were all tested under three different setups:

- Single server/local storage
- Single server/network storage
- Multi-server/network storage

The results are described in the following sections.

### AI inference in offline scenario for AFF

In this scenario, all the data was available to the server and the time it took to process all the samples was measured. We report bandwidths in samples per second as the results of the tests. When more than one compute server was used, we report total bandwidth summed over all the servers. The results for all three use cases are shown in the figure below. For the two-server case, we report combined bandwidth from both servers.



The results show that network storage does not negatively affect the performance—the change is minimal and for some tasks, none is found. When adding the second server, the total bandwidth either exactly doubles, or at worst, the change is less than 1%.

### AI inference in a single stream scenario for AFF

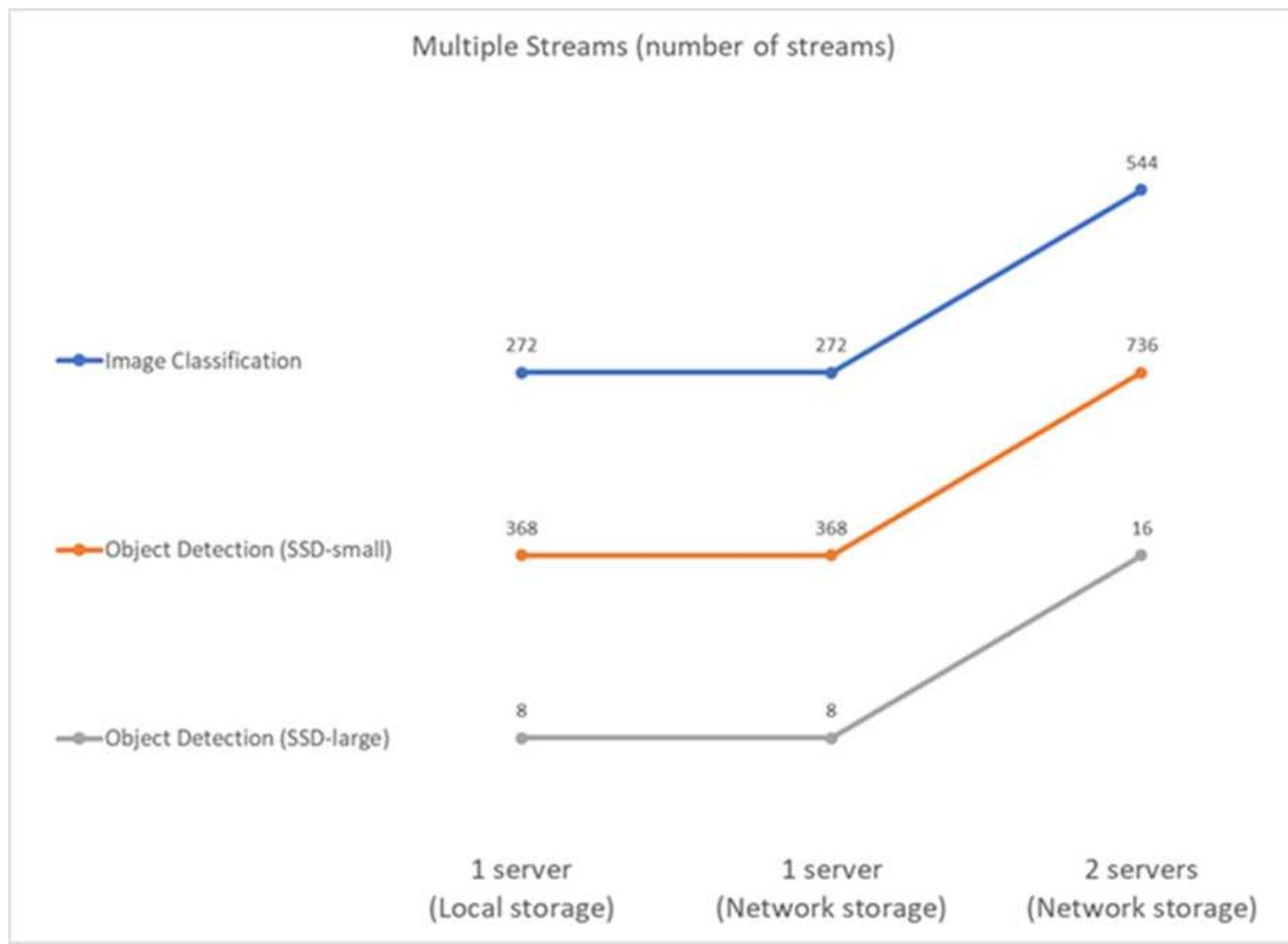
This benchmark measures latency. For the multiple computational server case, we report the average latency. The results for the suite of tasks are given in the figure below. For the two-server case, we report the average latency from both servers.



The results, again, show that the network storage is sufficient to handle the tasks. The difference between local and network storage in the one server case is minimal or none. Similarly, when two servers use the same storage, the latency on both servers stays the same or changes by a very small amount.

### AI inference in multistream scenario for AFF

In this case, the result is the number of streams that the system can handle while satisfying the QoS constraint. Thus, the result is always an integer. For more than one server, we report the total number of streams summed over all the servers. Not all workloads support this scenario, but we have executed those that do. The results of our tests are summarized in the figure below. For the two-server case, we report the combined number of streams from both servers.



The results show perfect performance of the setup—local and networking storage give the same results and adding the second server doubles the number of streams the proposed setup can handle.

#### Test results for EF

A multitude of tests were run to evaluate the performance of the proposed architecture. There are six different workloads (image classification, object detection [small], object detection [large], medical imaging, speech-to-text, and natural language processing [NLP]), which were run in two different scenarios: offline and single stream. The results are described in the following sections.

#### AI inference in offline scenario for EF

In this scenario, all the data was available to the server and the time it took to process all the samples was measured. We report bandwidths in samples per second as the results of the tests. For single node runs we report average from both servers, while for two server runs we report total bandwidth summed over all the servers. The results for use cases are shown in the figure below.



The results show that network storage does not negatively affect the performance—the change is minimal and for some tasks, none is found. When adding the second server, the total bandwidth either exactly doubles, or at worst, the change is less than 1%.

#### AI inference in a single stream scenario for EF

This benchmark measures latency. For all cases, we report average latency across all servers involved in the runs. The results for the suite of tasks are given.



The results show again that the network storage is sufficient to handle the tasks. The difference between the local and network storage in the one server case is minimal or none. Similarly, when two servers use the same storage, the latency on both servers stays the same or changes by a very small amount.

[Next: Architecture sizing options.](#)

## Architecture sizing options

[Previous: Test results.](#)

You can adjust the setup used for the validation to fit other use cases.

### Compute server

We used an Intel Xeon D-2123IT CPU, which is the lowest level of CPU supported in SE350, with four physical cores and 60W TDP. While the server does not support replacing CPUs, it can be ordered with a more powerful CPU. The top CPU supported is Intel Xeon D-2183IT with 16 cores, 100W running at 2.20GHz. This increases the CPU computational capability considerably. While CPU was not a bottleneck for running the inference workloads themselves, it helps with data processing and other tasks related to inference. At present, NVIDIA T4 is the only GPU available for edge use cases; therefore, currently, there is no ability to upgrade or downgrade the GPU.

### Shared storage

For testing and validation, the NetApp AFF C190 system, which has maximum storage capacity of 50.5TB, a throughput of 4.4GBps for sequential reads, and 230K IOPS for small random reads, was used for the purpose of this document and is proven to be well-suited for edge inference workloads.

However, if you require more storage capacity or faster networking speeds, you should use the NetApp AFF A220 or [NetApp AFF A250](#) storage systems. In addition, the NetApp EF280 system, which has a maximum capacity of 1.5PB, bandwidth 10Gbps was also used for the purpose of this solution validation. If you prefer more storage capacity with higher bandwidth, [NetApp EF300](#) can be used.

[Next: Conclusion.](#)

## Conclusion

[Previous: Architecture sizing options.](#)

AI-driven automation and edge computing is a leading approach to help business organizations achieve digital transformation and maximize operational efficiency and safety. With edge computing, data is processed much faster because it does not have to travel to and from a data center. Therefore, the cost associated with sending data back and forth to data centers or the cloud is diminished. Lower latency and increased speed can be beneficial when businesses must make decisions in near-real time using AI inferencing models deployed at the edge.

NetApp storage systems deliver the same or better performance as local SSD storage and offer the following benefits to data scientists, data engineers, AI/ML developers, and business or IT decision makers:

- Effortless sharing of data between AI systems, analytics, and other critical business systems. This data sharing reduces infrastructure overhead, improves performance, and streamlines data management across the enterprise.
- Independently scalable compute and storage to minimize costs and improve resource usage.
- Streamlined development and deployment workflows using integrated Snapshot copies and clones for instantaneous and space-efficient user workspaces, integrated version control, and automated deployment.
- Enterprise-grade data protection for disaster recovery and business continuity. The NetApp and Lenovo solution presented in this document is a flexible, scale-out architecture that is ideal for enterprise-grade AI inference deployments at the edge.

## Acknowledgments

- J.J. Falkanger, Sr. Manager, HPC & AI Solutions, Lenovo
- Dave Arnette, Technical Marketing Engineer, NetApp
- Joey Parnell, Tech Lead E-Series AI Solutions, NetApp
- Cody Harryman, QA Engineer, NetApp

## Where to find additional information

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

- NetApp AFF A-Series arrays product page  
<https://www.netapp.com/data-storage/aff-a-series/>
- NetApp ONTAP data management software—ONTAP 9 information library  
<http://mysupport.netapp.com/documentation/productlibrary/index.html?productID=62286>
- TR-4727: NetApp EF-Series Introduction

<https://www.netapp.com/pdf.html?item=/media/17179-tr4727pdf.pdf>

- NetApp E-Series SANtricity Software Datasheet

<https://www.netapp.com/pdf.html?item=/media/19775-ds-3171-66862.pdf>

- NetApp Persistent Storage for Containers—NetApp Trident

<https://netapp.io/persistent-storage-provisioner-for-kubernetes/>

- MLPerf

- <https://mlcommons.org/en/>
- <http://www.image-net.org/>
- <https://mlcommons.org/en/news/mlperf-inference-v11/>

- NetApp Cloud Sync

[https://docs.netapp.com/us-en/occm/concept\\_cloud\\_sync.html#how-cloud-sync-works](https://docs.netapp.com/us-en/occm/concept_cloud_sync.html#how-cloud-sync-works)

- TensorFlow benchmark

<https://github.com/tensorflow/benchmarks>

- Lenovo ThinkSystem SE350 Edge Server

<https://lenovopress.com/lp1168>

- Lenovo ThinkSystem DM5100F Unified Flash Storage Array

<https://lenovopress.com/lp1365-thinksystem-dm5100f-unified-flash-storage-array> [<https://lenovopress.com/lp1365-thinksystem-dm5100f-unified-flash-storage-array>]

## Version history

Version	Date	Document version history
Version 1.0	March 2021	Initial release
Version 2.0	October 2021	Updated with EF and MLPerf Inference v1.1

## WP-7328: NetApp Conversational AI Using NVIDIA Jarvis

Rick Huang, Sung-Han Lin, NetApp  
Davide Onofrio, NVIDIA

The NVIDIA DGX family of systems is made up of the world's first integrated artificial intelligence (AI)-based systems that are purpose-built for enterprise AI. NetApp AFF storage systems deliver extreme performance and industry-leading hybrid cloud data-management capabilities. NetApp and NVIDIA have partnered to create the NetApp ONTAP AI reference architecture, a turnkey solution for AI and machine learning (ML) workloads that provides enterprise-class performance, reliability, and support.

This white paper gives directional guidance to customers building conversational AI systems in support of different use cases in various industry verticals. It includes information about the deployment of the system

using NVIDIA Jarvis. The tests were performed using an NVIDIA DGX Station and a NetApp AFF A220 storage system.

The target audience for the solution includes the following groups:

- Enterprise architects who design solutions for the development of AI models and software for conversational AI use cases such as a virtual retail assistant
- Data scientists looking for efficient ways to achieve language modeling development goals
- Data engineers in charge of maintaining and processing text data such as customer questions and dialogue transcripts
- Executive and IT decision makers and business leaders interested in transforming the conversational AI experience and achieving the fastest time to market from AI initiatives

[Next: Solution Overview](#)

## Solution Overview

### NetApp ONTAP AI and Cloud Sync

The NetApp ONTAP AI architecture, powered by NVIDIA DGX systems and NetApp cloud-connected storage systems, was developed and verified by NetApp and NVIDIA. This reference architecture gives IT organizations the following advantages:

- Eliminates design complexities
  - Enables independent scaling of compute and storage
  - Enables customers to start small and scale seamlessly
  - Offers a range of storage options for various performance and cost points
- NetApp ONTAP AI tightly integrates DGX systems and NetApp AFF A220 storage systems with state-of-the-art networking. NetApp ONTAP AI and DGX systems simplify AI deployments by eliminating design complexity and guesswork. Customers can start small and grow their systems in an uninterrupted manner while intelligently managing data from the edge to the core to the cloud and back.

NetApp Cloud Sync enables you to move data easily over various protocols, whether it's between two NFS shares, two CIFS shares, or one file share and Amazon S3, Amazon Elastic File System (EFS), or Azure Blob storage. Active-active operation means that you can continue to work with both source and target at the same time, incrementally synchronizing data changes when required. By enabling you to move and incrementally synchronize data between any source and destination system, whether on-premises or cloud-based, Cloud Sync opens up a wide variety of new ways in which you can use data. Migrating data between on-premises systems, cloud on-boarding and cloud migration, or collaboration and data analytics all become easily achievable. The figure below shows available sources and destinations.

In conversational AI systems, developers can leverage Cloud Sync to archive conversation history from the cloud to data centers to enable offline training of natural language processing (NLP) models. By training models to recognize more intents, the conversational AI system will be better equipped to manage more complex questions from end-users.

### NVIDIA Jarvis Multimodal Framework



[NVIDIA Jarvis](#) is an end-to-end framework for building conversational AI services. It includes the following GPU-optimized services:

- Automatic speech recognition (ASR)
- Natural language understanding (NLU)
- Integration with domain-specific fulfillment services
- Text-to-speech (TTS)
- Computer vision (CV) Jarvis-based services use state-of-the-art deep learning models to address the complex and challenging task of real-time conversational AI. To enable real-time, natural interaction with an end user, the models need to complete computation in under 300 milliseconds. Natural interactions are challenging, requiring multimodal sensory integration. Model pipelines are also complex and require coordination across the above services.

Jarvis is a fully accelerated, application framework for building multimodal conversational AI services that use an end-to-end deep learning pipeline. The Jarvis framework includes pretrained conversational AI models, tools, and optimized end-to-end services for speech, vision, and NLU tasks. In addition to AI services, Jarvis enables you to fuse vision, audio, and other sensor inputs simultaneously to deliver capabilities such as multi-user, multi-context conversations in applications such as virtual assistants, multi-user diarization, and call center assistants.

### NVIDIA NeMo

[NVIDIA NeMo](#) is an open-source Python toolkit for building, training, and fine-tuning GPU-accelerated state-of-the-art conversational AI models using easy-to-use application programming interfaces (APIs). NeMo runs mixed precision compute using Tensor Cores in NVIDIA GPUs and can scale up to multiple GPUs easily to deliver the highest training performance possible. NeMo is used to build models for real-time ASR, NLP, and TTS applications such as video call transcriptions, intelligent video assistants, and automated call center support across different industry verticals, including healthcare, finance, retail, and telecommunications.

We used NeMo to train models that recognize complex intents from user questions in archived conversation history. This training extends the capabilities of the retail virtual assistant beyond what Jarvis supports as

delivered.

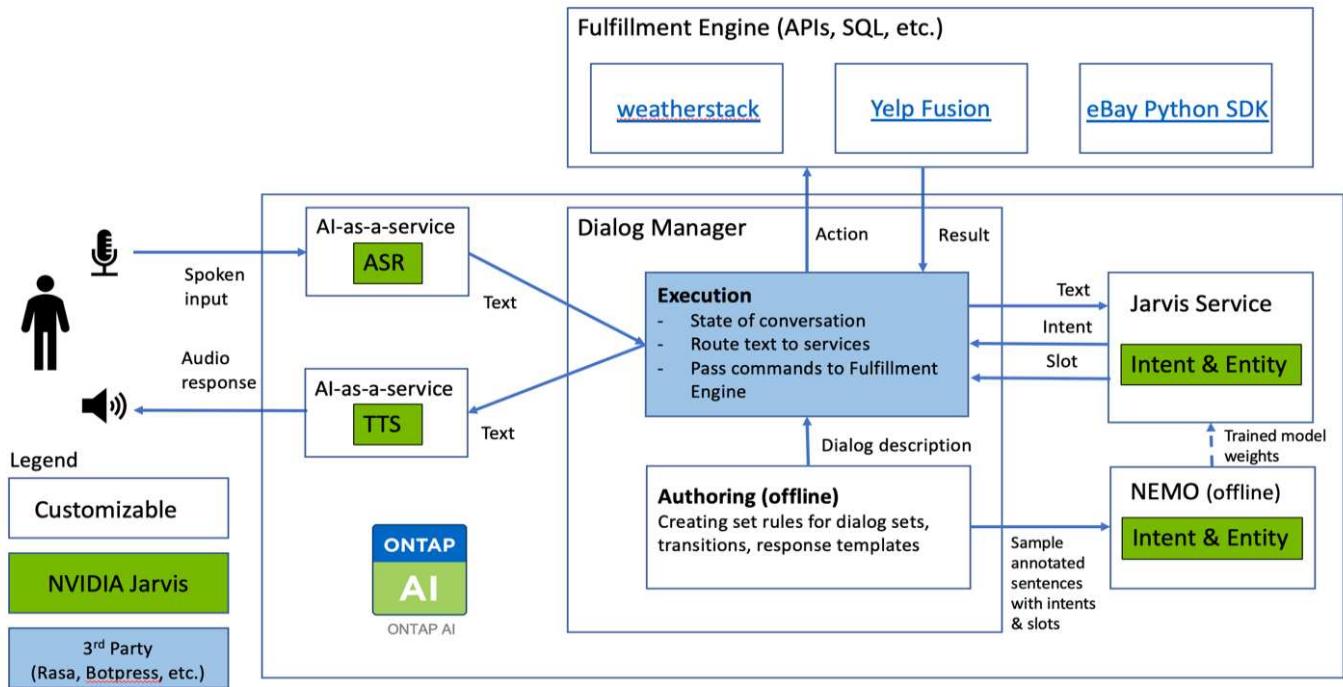
## Retail Use Case Summary

Using NVIDIA Jarvis, we built a virtual retail assistant that accepts speech or text input and answers questions regarding weather, points-of-interest, and inventory pricing. The conversational AI system is able to remember conversation flow, for example, ask a follow-up question if the user does not specify location for weather or points-of-interest. The system also recognizes complex entities such as “Thai food” or “laptop memory.” It understands natural language questions like “will it rain next week in Los Angeles?” A demonstration of the retail virtual assistant can be found in [Customize States and Flows for Retail Use Case](#).

Next: Solution Technology

## Solution Technology

The following figure illustrates the proposed conversational AI system architecture. You can interact with the system with either speech signal or text input. If spoken input is detected, Jarvis AI-as-service (AlaaS) performs ASR to produce text for Dialog Manager. Dialog Manager remembers states of conversation, routes text to corresponding services, and passes commands to Fulfillment Engine. Jarvis NLP Service takes in text, recognizes intents and entities, and outputs those intents and entity slots back to Dialog Manager, which then sends Action to Fulfillment Engine. Fulfillment Engine consists of third-party APIs or SQL databases that answer user queries. After receiving Result from Fulfillment Engine, Dialog Manager routes text to Jarvis TTS AlaaS to produce an audio response for the end-user. We can archive conversation history, annotate sentences with intents and slots for NeMo training such that NLP Service improves as more users interact with the system.



## Hardware Requirements

This solution was validated using one DGX Station and one AFF A220 storage system. Jarvis requires either a T4 or V100 GPU to perform deep neural network computations.

The following table lists the hardware components that are required to implement the solution as tested.

Hardware	Quantity
T4 or V100 GPU	1
NVIDIA DGX Station	1

## Software Requirements

The following table lists the software components that are required to implement the solution as tested.

Software	Version or Other Information
NetApp ONTAP data management software	9.6
Cisco NX-OS switch firmware	7.0(3)I6(1)
NVIDIA DGX OS	4.0.4 - Ubuntu 18.04 LTS
NVIDIA Jarvis Framework	EA v0.2
NVIDIA NeMo	nvcr.io/nvidia/nemo:v0.10
Docker container platform	18.06.1-ce [e68fc7a]

[Next: Build a Virtual Assistant Using Jarvis, Cloud Sync, and NeMo Overview](#)

## Overview

This section provides detail on the implementation of the virtual retail assistant.

[Next: Jarvis Deployment](#)

### Jarvis Deployment

You can sign up for [Jarvis Early Access program](#) to gain access to Jarvis containers on NVIDIA GPU Cloud (NGC). After receiving credentials from NVIDIA, you can deploy Jarvis using the following steps:

1. Sign-on to NGC.
2. Set your organization on NGC: ea-2-jarvis.
3. Locate Jarvis EA v0.2 assets: Jarvis containers are in Private Registry > Organization Containers.
4. Select Jarvis: navigate to Model Scripts and click Jarvis Quick Start
5. Verify that all assets are working properly.
6. Find the documentation to build your own applications: PDFs can be found in Model Scripts > Jarvis Documentation > File Browser.

[Next: Customize States and Flows for Retail Use Case](#)

### Customize States and Flows for Retail Use Case

You can customize States and Flows of Dialog Manager for your specific use cases. In our retail example, we have the following four yaml files to direct the conversation

according to different intents.

See the following list of file names and description of each file:

- `main_flow.yml`: Defines the main conversation flows and states and directs the flow to the other three yaml files when necessary.
- `retail_flow.yml`: Contains states related to retail or points-of-interest questions. The system either provides the information of the nearest store, or the price of a given item.
- `weather_flow.yml`: Contains states related to weather questions. If the location cannot be determined, the system asks a follow up question to clarify.
- `error_flow.yml`: Handles cases where user intents do not fall into the above three yaml files. After displaying an error message, the system re-routes back to accepting user questions. The following sections contain the detailed definitions for these yaml files.

### `main_flow.yml`

```
name: JarvisRetail
intent_transitions:
    jarvis_error: error
    price_check: retail_price_check
    inventory_check: retail_inventory_check
    store_location: retail_store_location
    weather.weather: weather
    weather.temperature: temperature
    weather.sunny: sunny
    weather.cloudy: cloudy
    weather.snow: snow
    weather.rainfall: rain
    weather.snow_yes_no: snowfall
    weather.rainfall_yes_no: rainfall
    weather.temperature_yes_no: tempyesno
    weather.humidity: humidity
    weather.humidity_yes_no: humidity
    navigation.startnavigationpoi: retail # Transitions should be context
and slot based. Redirecting for now.
    navigation.geteta: retail
    navigation.showdirection: retail
    navigation.showmappoi: idk_what_you_talkin_about
    nomatch.none: idk_what_you_talkin_about
states:
    init:
        type: message_text
        properties:
            text: "Hi, welcome to NARA retail and weather service. How can I
help you?"
        input_intent:
```

```

type: input_context
properties:
  nlp_type: jarvis
  entities:
    intent: dontcare
# This state is executed if the intent was not understood
dont_get_the_intent:
  type: message_text_random
  properties:
    responses:
      - "Sorry I didn't get that! Please come again."
      - "I beg your pardon! Say that again?"
      - "Are we talking about weather? What would you like to know?"
      - "Sorry I know only about the weather"
      - "You can ask me about the weather, the rainfall, the
temperature, I don't know much more"
  delay: 0
  transitions:
    next_state: input_intent
idk_what_you_talkin_about:
  type: message_text_random
  properties:
    responses:
      - "Sorry I didn't get that! Please come again."
      - "I beg your pardon! Say that again?"
      - "Are we talking about retail or weather? What would you like to
know?"
      - "Sorry I know only about retail and the weather"
      - "You can ask me about retail information or the weather, the
rainfall, the temperature. I don't know much more."
  delay: 0
  transitions:
    next_state: input_intent
error:
  type: change_context
  properties:
    update_keys:
      intent: 'error'
  transitions:
    flow: error_flow
retail_inventory_check:
  type: change_context
  properties:
    update_keys:
      intent: 'retail_inventory_check'
  transitions:

```

```
    flow: retail_flow
retail_price_check:
    type: change_context
properties:
    update_keys:
        intent: 'check_item_price'
transitions:
    flow: retail_flow
retail_store_location:
    type: change_context
properties:
    update_keys:
        intent: 'find_the_store'
transitions:
    flow: retail_flow
weather:
    type: change_context
properties:
    update_keys:
        intent: 'weather'
transitions:
    flow: weather_flow
temperature:
    type: change_context
properties:
    update_keys:
        intent: 'temperature'
transitions:
    flow: weather_flow
rainfall:
    type: change_context
properties:
    update_keys:
        intent: 'rainfall'
transitions:
    flow: weather_flow
sunny:
    type: change_context
properties:
    update_keys:
        intent: 'sunny'
transitions:
    flow: weather_flow
cloudy:
    type: change_context
properties:
```

```
    update_keys:
        intent: 'cloudy'
transitions:
    flow: weather_flow
snow:
    type: change_context
properties:
    update_keys:
        intent: 'snow'
transitions:
    flow: weather_flow
rain:
    type: change_context
properties:
    update_keys:
        intent: 'rain'
transitions:
    flow: weather_flow
snowfall:
    type: change_context
properties:
    update_keys:
        intent: 'snowfall'
transitions:
    flow: weather_flow
tempyesno:
    type: change_context
properties:
    update_keys:
        intent: 'tempyesno'
transitions:
    flow: weather_flow
humidity:
    type: change_context
properties:
    update_keys:
        intent: 'humidity'
transitions:
    flow: weather_flow
end_state:
    type: reset
transitions:
    next_state: init
```

## retail\_flow.yml

```
name: retail_flow
states:
  store_location:
    type: conditional_exists
    properties:
      key: '{{location}}'
    transitions:
      exists: retail_state
      notexists: ask_retail_location
  retail_state:
    type: Retail
    properties:
    transitions:
      next_state: output_retail
  output_retail:
    type: message_text
    properties:
      text: '{{retail_status}}'
    transitions:
      next_state: input_intent
  ask_retail_location:
    type: message_text
    properties:
      text: "For which location? I can find the closest store near you."
    transitions:
      next_state: input_retail_location
  input_retail_location:
    type: input_user
    properties:
      nlp_type: jarvis
      entities:
        slot: location
        require_match: true
    transitions:
      match: retail_state
      notmatch: check_retail_jarvis_error
  output_retail_acknowledge:
    type: message_text_random
    properties:
      responses:
        - 'ok in {{location}}'
        - 'the store in {{location}}'
        - 'I always wanted to shop in {{location}}'
    delay: 0
```

```

transitions:
  next_state: retail_state
output_retail_notlocation:
  type: message_text
  properties:
    text: "I did not understand the location. Can you please repeat?"
transitions:
  next_state: input_intent
check_rerail_jarvis_error:
  type: conditional_exists
  properties:
    key: '{{jarvis_error}}'
transitions:
  exists: show_retail_jarvis_api_error
  notexists: output_retail_notlocation
show_retail_jarvis_api_error:
  type: message_text
  properties:
    text: "I am having trouble understanding right now. Come again on
that?"
transitions:
  next_state: input_intent

```

## **weather\_flow.yml**

```

name: weather_flow
states:
  check_weather_location:
    type: conditional_exists
    properties:
      key: '{{location}}'
    transitions:
      exists: weather_state
      notexists: ask_weather_location
  weather_state:
    type: Weather
    properties:
    transitions:
      next_state: output_weather
  output_weather:
    type: message_text
    properties:
      text: '{{weather_status}}'
    transitions:
      next_state: input_intent

```

```

ask_weather_location:
    type: message_text
    properties:
        text: "For which location?"
transitions:
    next_state: input_weather_location
input_weather_location:
    type: input_user
    properties:
        nlp_type: jarvis
        entities:
            slot: location
            require_match: true
transitions:
    match: weather_state
    notmatch: check_jarvis_error
output_weather_acknowledge:
    type: message_text_random
    properties:
        responses:
            - 'ok in {{location}}'
            - 'the weather in {{location}}'
            - 'I always wanted to go in {{location}}'
    delay: 0
transitions:
    next_state: weather_state
output_weather_notlocation:
    type: message_text
    properties:
        text: "I did not understand the location, can you please repeat?"
transitions:
    next_state: input_intent
check_jarvis_error:
    type: conditional_exists
    properties:
        key: '{{jarvis_error}}'
transitions:
    exists: show_jarvis_api_error
    notexists: output_weather_notlocation
show_jarvis_api_error:
    type: message_text
    properties:
        text: "I am having troubled understanding right now. Come again on
that, else check jarvis services?"
transitions:
    next_state: input_intent

```

## error\_flow.yml

```
name: error_flow
states:
  error_state:
    type: message_text_random
    properties:
      responses:
        - "Sorry I didn't get that!"
        - "Are we talking about retail or weather? What would you like to know?"
        - "Sorry I know only about retail information or the weather"
        - "You can ask me about retail information or the weather, the rainfall, the temperature. I don't know much more"
        - "Let's talk about retail or the weather!"
    delay: 0
    transitions:
      next_state: input_intent
```

[Next: Connect to Third-Party APIs as Fulfillment Engine](#)

### Connect to Third-Party APIs as Fulfillment Engine

We connected the following third-party APIs as a Fulfillment Engine to answer questions:

- [WeatherStack API](#): returns weather, temperature, rainfall, and snow in a given location.
- [Yelp Fusion API](#): returns the nearest store information in a given location.
- [eBay Python SDK](#): returns the price of a given item.

[Next: NetApp Retail Assistant Demonstration](#)

### NetApp Retail Assistant Demonstration

We recorded a demonstration video of NetApp Retail Assistant (NARA). Click [this link](#) to open the following figure and play the video demonstration.

# NetApp NARA



Hi, welcome to NARA retail and weather service. How can I help you?

Write your message...

Submit

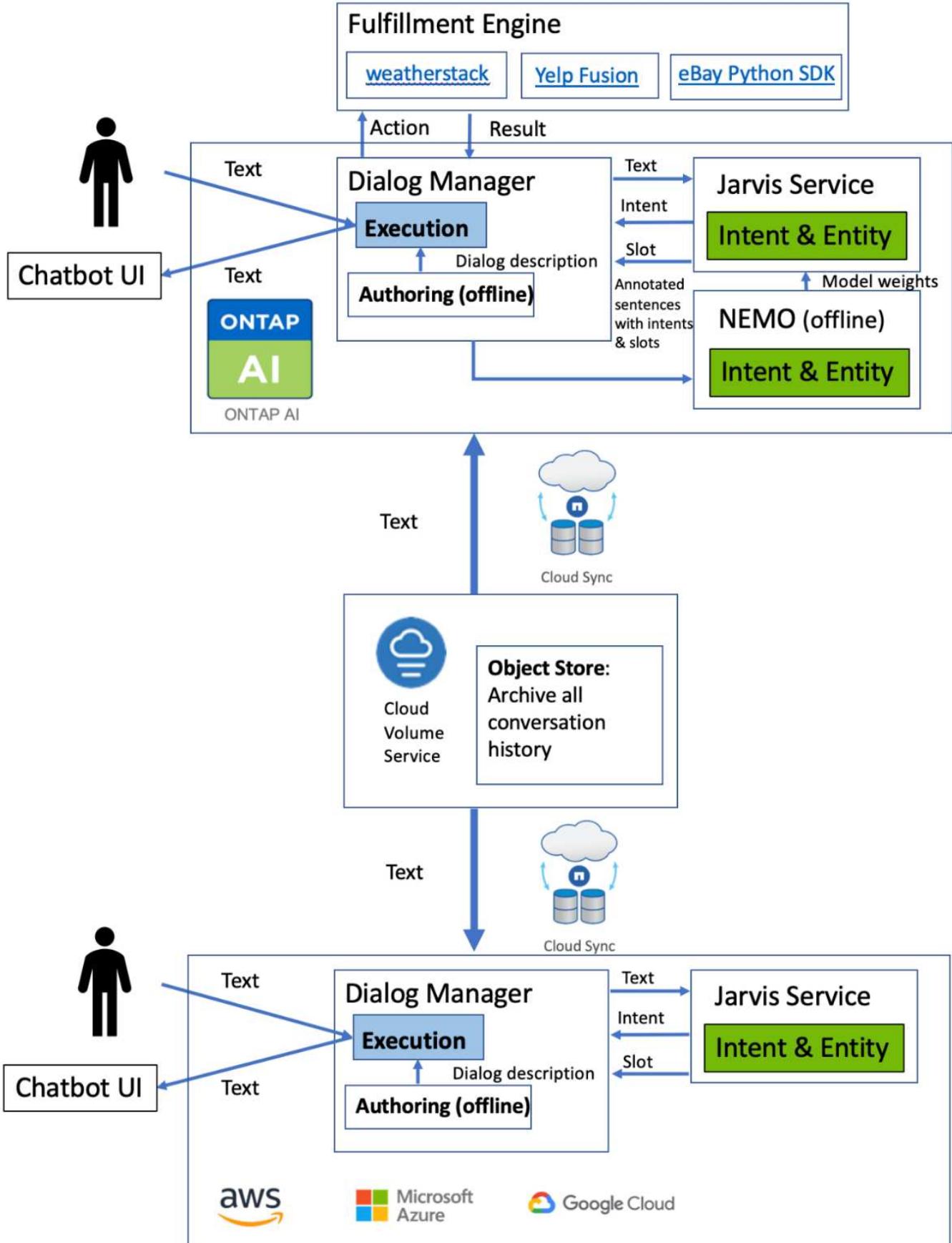
System replied. Waiting for user input.

Unmute System Speech

Next: Use NetApp Cloud Sync to Archive Conversation History

## Use NetApp Cloud Sync to Archive Conversation History

By dumping conversation history into a CSV file once a day, we can then leverage Cloud Sync to download the log files into local storage. The following figure shows the architecture of having Jarvis deployed on-premises and in public clouds, while using Cloud Sync to send conversation history for NeMo training. Details of NeMo training can be found in the section [Expand Intent Models Using NeMo Training](#).



Next: Expand Intent Models Using NeMo Training

## Expand Intent Models Using NeMo Training

NVIDIA NeMo is a toolkit built by NVIDIA for creating conversational AI applications. This toolkit includes collections of pre-trained modules for ASR, NLP, and TTS, enabling researchers and data scientists to easily compose complex neural network architectures and put more focus on designing their own applications.

As shown in the previous example, NARA can only handle a limited type of question. This is because the pre-trained NLP model only trains on these types of questions. If we want to enable NARA to handle a broader range of questions, we need to retrain it with our own datasets. Thus, here, we demonstrate how we can use NeMo to extend the NLP model to satisfy the requirements. We start by converting the log collected from NARA into the format for NeMo, and then train with the dataset to enhance the NLP model.

### Model

Our goal is to enable NARA to sort the items based on user preferences. For instance, we might ask NARA to suggest the highest-rated sushi restaurant or might want NARA to look up the jeans with the lowest price. To this end, we use the intent detection and slot filling model provided in NeMo as our training model. This model allows NARA to understand the intent of searching preference.

### Data Preparation

To train the model, we collect the dataset for this type of question, and convert it to the NeMo format. Here, we listed the files we use to train the model.

#### dict.intents.csv

This file lists all the intents we want the NeMo to understand. Here, we have two primary intents and one intent only used to categorize the questions that do not fit into any of the primary intents.

```
price_check  
find_the_store  
unknown
```

#### dict.slots.csv

This file lists all the slots we can label on our training questions.

```
B-store.type  
B-store.name  
B-store.status  
B-store.hour.start  
B-store.hour.end  
B-store.hour.day  
B-item.type  
B-item.name  
B-item.color  
B-item.size  
B-item.quantity  
B-location  
B-cost.high
```

```
B-cost.average  
B-cost.low  
B-time.period_of_time  
B-rating.high  
B-rating.average  
B-rating.low  
B-interrogative.location  
B-interrogative.manner  
B-interrogative.time  
B-interrogative.personal  
B-interrogative  
B-verb  
B-article  
I-store.type  
I-store.name  
I-store.status  
I-store.hour.start  
I-store.hour.end  
I-store.hour.day  
I-item.type  
I-item.name  
I-item.color  
I-item.size  
I-item.quantity  
I-location  
I-cost.high  
I-cost.average  
I-cost.low  
I-time.period_of_time  
I-rating.high  
I-rating.average  
I-rating.low  
I-interrogative.location  
I-interrogative.manner  
I-interrogative.time  
I-interrogative.personal  
I-interrogative  
I-verb  
I-article  
O
```

### train.tsv

This is the main training dataset. Each line starts with the question following the intent category listing in the file dict.intent.csv. The label is enumerated starting from zero.

## train\_slots.tsv

```
20 46 24 25 6 32 6  
52 52 24 6  
23 52 14 40 52 25 6 32 6  
...
```

## Train the Model

```
docker pull nvcr.io/nvidia/nemo:v0.10
```

We then use the following command to launch the container. In this command, we limit the container to use a single GPU (GPU ID = 1) since this is a lightweight training exercise. We also map our local workspace /workspace/nemo/ to the folder inside container /nemo.

```
NV_GPU='1' docker run --runtime=nvidia -it --shm-size=16g \  
--network=host --ulimit memlock=-1 --ulimit  
stack=67108864 \  
-v /workspace/nemo:/nemo\  
--rm nvcr.io/nvidia/nemo:v0.10
```

Inside the container, if we want to start from the original pre-trained BERT model, we can use the following command to start the training procedure. `data_dir` is the argument to set up the path of the training data. `work_dir` allows you to configure where you want to store the checkpoint files.

```
cd examples/nlp/intent_detection_slot_tagging/  
python joint_intent_slot_with_bert.py \  
--data_dir /nemo/training_data\  
--work_dir /nemo/log
```

If we have new training datasets and want to improve the previous model, we can use the following command to continue from the point we stopped. `checkpoint_dir` takes the path to the previous checkpoints folder.

```
cd examples/nlp/intent_detection_slot_tagging/  
python joint_intent_slot_infer.py \  
--data_dir /nemo/training_data \  
--checkpoint_dir /nemo/log/2020-05-04_18-34-20/checkpoints/ \  
--eval_file_prefix test
```

## Inference the Model

We need to validate the performance of the trained model after a certain number of epochs. The following command allows us to test the query one-by-one. For instance, in this command, we want to check if our

model can properly identify the intention of the query where can I get the best pasta.

```
cd examples/nlp/intent_detection_slot_tagging/
python joint_intent_slot_infer_b1.py \
--checkpoint_dir /nemo/log/2020-05-29_23-50-58/checkpoints/ \
--query "where can i get the best pasta" \
--data_dir /nemo/training_data/ \
--num_epochs=50
```

Then, the following is the output from the inference. In the output, we can see that our trained model can properly predict the intention find\_the\_store, and return the keywords we are interested in. With these keywords, we enable the NARA to search for what users want and do a more precise search.

```
[NeMo I 2020-05-30 00:06:54 actions:728] Evaluating batch 0 out of 1
[NeMo I 2020-05-30 00:06:55 inference_utils:34] Query: where can i get the
best pasta
[NeMo I 2020-05-30 00:06:55 inference_utils:36] Predicted intent: 1
find_the_store
[NeMo I 2020-05-30 00:06:55 inference_utils:50] where B-
interrogative.location
[NeMo I 2020-05-30 00:06:55 inference_utils:50] can O
[NeMo I 2020-05-30 00:06:55 inference_utils:50] i O
[NeMo I 2020-05-30 00:06:55 inference_utils:50] get B-verb
[NeMo I 2020-05-30 00:06:55 inference_utils:50] the B-article
[NeMo I 2020-05-30 00:06:55 inference_utils:50] best B-rating.high
[NeMo I 2020-05-30 00:06:55 inference_utils:50] pasta B-item.type
```

[Next: Conclusion](#)

## Conclusion

A true conversational AI system engages in human-like dialogue, understands context, and provides intelligent responses. Such AI models are often huge and highly complex. With NVIDIA GPUs and NetApp storage, massive, state-of-the-art language models can be trained and optimized to run inference rapidly. This is a major stride towards ending the trade-off between an AI model that is fast versus one that is large and complex. GPU-optimized language understanding models can be integrated into AI applications for industries such as healthcare, retail, and financial services, powering advanced digital voice assistants in smart speakers and customer service lines. These high-quality conversational AI systems allow businesses across verticals to provide previously unattainable personalized services when engaging with customers.

Jarvis enables the deployment of use cases such as virtual assistants, digital avatars, multimodal sensor fusion (CV fused with ASR/NLP/TTS), or any ASR/NLP/TTS/CV stand-alone use case, such as transcription. We built a virtual retail assistant that can answer questions regarding weather, points-of-interest, and inventory pricing. We also demonstrated how to improve the natural language understanding capabilities of the conversational AI system by archiving conversation history using Cloud Sync and training NeMo models on new data.

[Next: Acknowledgments](#)

## Acknowledgments

The authors gratefully acknowledge the contributions that were made to this white paper by our esteemed colleagues from NVIDIA: Davide Onofrio, Alex Qi, Sicong Ji, Marty Jain, and Robert Sohigian. The authors would also like to acknowledge the contributions of key NetApp team members: Santosh Rao, David Arnette, Michael Oglesby, Brent Davis, Andy Sayare, Erik Mulder, and Mike McNamara.

Our sincere appreciation and thanks go to all these individuals, who provided insight and expertise that greatly assisted in the creation of this paper.

## Next: Where to Find Additional Information

### Where to Find Additional Information

To learn more about the information that is described in this document, see the following resources:

- NVIDIA DGX Station, V100 GPU, GPU Cloud
  - NVIDIA DGX Station  
<https://www.nvidia.com/en-us/data-center/dgx-station/>
  - NVIDIA V100 Tensor Core GPU  
<https://www.nvidia.com/en-us/data-center/tesla-v100/>
  - NVIDIA NGC  
<https://www.nvidia.com/en-us/gpu-cloud/>
- NVIDIA Jarvis Multimodal Framework
  - NVIDIA Jarvis  
<https://developer.nvidia.com/nvidia-jarvis>
  - NVIDIA Jarvis Early Access  
<https://developer.nvidia.com/nvidia-jarvis-early-access>
- NVIDIA NeMo
  - NVIDIA NeMo  
<https://developer.nvidia.com/nvidia-nemo>
  - Developer Guide  
<https://nvidia.github.io/NeMo/>
- NetApp AFF systems
  - NetApp AFF A-Series Datasheet  
<https://www.netapp.com/us/media/ds-3582.pdf>
  - NetApp Flash Advantage for All Flash FAS  
<https://www.netapp.com/us/media/ds-3733.pdf>
  - ONTAP 9 Information Library  
<http://mysupport.netapp.com/documentation/productlibrary/index.html?productID=62286>
  - NetApp ONTAP FlexGroup Volumes technical report  
<https://www.netapp.com/us/media/tr-4557.pdf>
- NetApp ONTAP AI

- ONTAP AI with DGX-1 and Cisco Networking Design Guide  
<https://www.netapp.com/us/media/nva-1121-design.pdf>
- ONTAP AI with DGX-1 and Cisco Networking Deployment Guide  
<https://www.netapp.com/us/media/nva-1121-deploy.pdf>
- ONTAP AI with DGX-1 and Mellanox Networking Design Guide  
<http://www.netapp.com/us/media/nva-1138-design.pdf>
- ONTAP AI with DGX-2 Design Guide  
<https://www.netapp.com/us/media/nva-1135-design.pdf>

## TR-4858: NetApp Orchestration Solution with Run:AI

Rick Huang, David Arnette, Sung-Han Lin, NetApp  
Yaron Goldberg, Run:AI

NetApp AFF storage systems deliver extreme performance and industry-leading hybrid cloud data-management capabilities. NetApp and Run:AI have partnered to demonstrate the unique capabilities of the NetApp ONTAP AI solution for artificial intelligence (AI) and machine learning (ML) workloads that provides enterprise-class performance, reliability, and support. Run:AI orchestration of AI workloads adds a Kubernetes-based scheduling and resource utilization platform to help researchers manage and optimize GPU utilization. Together with the NVIDIA DGX systems, the combined solution from NetApp, NVIDIA, and Run:AI provide an infrastructure stack that is purpose-built for enterprise AI workloads. This technical report gives directional guidance to customers building conversational AI systems in support of various use cases and industry verticals. It includes information about the deployment of Run:AI and a NetApp AFF A800 storage system and serves as a reference architecture for the simplest way to achieve fast, successful deployment of AI initiatives.

The target audience for the solution includes the following groups:

- Enterprise architects who design solutions for the development of AI models and software for Kubernetes-based use cases such as containerized microservices
- Data scientists looking for efficient ways to achieve efficient model development goals in a cluster environment with multiple teams and projects
- Data engineers in charge of maintaining and running production models
- Executive and IT decision makers and business leaders who would like to create the optimal Kubernetes cluster resource utilization experience and achieve the fastest time to market from AI initiatives

[Next: Solution Overview](#)

### Solution Overview

#### NetApp ONTAP AI and AI Control Plane

The NetApp ONTAP AI architecture, developed and verified by NetApp and NVIDIA, is powered by NVIDIA DGX systems and NetApp cloud-connected storage systems. This reference architecture gives IT organizations the following advantages:

- Eliminates design complexities
- Enables independent scaling of compute and storage
- Enables customers to start small and scale seamlessly
- Offers a range of storage options for various performance and cost points

NetApp ONTAP AI tightly integrates DGX systems and NetApp AFF A800 storage systems with state-of-the-art networking. NetApp ONTAP AI and DGX systems simplify AI deployments by eliminating design complexity and guesswork. Customers can start small and grow their systems in an uninterrupted manner while intelligently managing data from the edge to the core to the cloud and back.

NetApp AI Control Plane is a full stack AI, ML, and deep learning (DL) data and experiment management solution for data scientists and data engineers. As organizations increase their use of AI, they face many challenges, including workload scalability and data availability. NetApp AI Control Plane addresses these challenges through functionalities, such as rapidly cloning a data namespace just as you would a Git repo, and defining and implementing AI training workflows that incorporate the near-instant creation of data and model baselines for traceability and versioning. With NetApp AI Control Plane, you can seamlessly replicate data across sites and regions and swiftly provision Jupyter Notebook workspaces with access to massive datasets.

### Run:AI Platform for AI Workload Orchestration

Run:AI has built the world's first orchestration and virtualization platform for AI infrastructure. By abstracting workloads from the underlying hardware, Run:AI creates a shared pool of GPU resources that can be dynamically provisioned, enabling efficient orchestration of AI workloads and optimized use of GPUs. Data scientists can seamlessly consume massive amounts of GPU power to improve and accelerate their research while IT teams retain centralized, cross-site control and real-time visibility over resource provisioning, queuing, and utilization. The Run:AI platform is built on top of Kubernetes, enabling simple integration with existing IT and data science workflows.

The Run:AI platform provides the following benefits:

- **Faster time to innovation.** By using Run:AI resource pooling, queueing, and prioritization mechanisms together with a NetApp storage system, researchers are removed from infrastructure management hassles and can focus exclusively on data science. Run:AI and NetApp customers increase productivity by running as many workloads as they need without compute or data pipeline bottlenecks.
- **Increased team productivity.** Run:AI fairness algorithms guarantee that all users and teams get their fair share of resources. Policies around priority projects can be preset, and the platform enables dynamic allocation of resources from one user or team to another, helping users to get timely access to coveted GPU resources.
- **Improved GPU utilization.** The Run:AI Scheduler enables users to easily make use of fractional GPUs, integer GPUs, and multiple nodes of GPUs for distributed training on Kubernetes. In this way, AI workloads run based on your needs, not capacity. Data science teams are able to run more AI experiments on the same infrastructure.

[Next: Solution Technology](#)

### Solution Technology

This solution was implemented with one NetApp AFF A800 system, two DGX-1 servers, and two Cisco Nexus 3232C 100GbE-switches. Each DGX-1 server is connected to the Nexus switches with four 100GbE connections that are used for inter-GPU communications by using remote direct memory access (RDMA) over Converged Ethernet (RoCE). Traditional IP communications for NFS storage access also occur on these links. Each storage controller is connected to the network switches by using four 100GbE-links. The following figure shows the ONTAP AI solution architecture used in this technical report for all testing scenarios.



#### Hardware Used in This Solution

This solution was validated using the ONTAP AI reference architecture two DGX-1 nodes and one AFF A800 storage system. See [NVA-1121](#) for more details about the infrastructure used in this validation.

The following table lists the hardware components that are required to implement the solution as tested.

Hardware	Quantity
DGX-1 systems	2
AFF A800	1
Nexus 3232C switches	2

#### Software Requirements

This solution was validated using a basic Kubernetes deployment with the Run:AI operator installed. Kubernetes was deployed using the [NVIDIA DeepOps](#) deployment engine, which deploys all required components for a production-ready environment. DeepOps automatically deployed [NetApp Trident](#) for persistent storage integration with the k8s environment, and default storage classes were created so containers leverage storage from the AFF A800 storage system. For more information on Trident with Kubernetes on ONTAP AI, see [TR-4798](#).

The following table lists the software components that are required to implement the solution as tested.

Software	Version or Other Information
NetApp ONTAP data management software	9.6p4
Cisco NX-OS switch firmware	7.0(3)I6(1)
NVIDIA DGX OS	4.0.4 - Ubuntu 18.04 LTS

Software	Version or Other Information
Kubernetes version	1.17
Trident version	20.04.0
Run:AI CLI	v2.1.13
Run:AI Orchestration Kubernetes Operator version	1.0.39
Docker container platform	18.06.1-ce [e68fc7a]

Additional software requirements for Run:AI can be found at [Run:AI GPU cluster prerequisites](#).

## Next: Optimal Cluster and GPU Utilization with Run AI

### Optimal Cluster and GPU Utilization with Run:AI

The following sections provide details on the Run:AI installation, test scenarios, and results performed in this validation.

We validated the operation and performance of this system by using industry standard benchmark tools, including TensorFlow benchmarks. The ImageNet dataset was used to train ResNet-50, which is a famous Convolutional Neural Network (CNN) DL model for image classification. ResNet-50 delivers an accurate training result with a faster processing time, which enabled us to drive a sufficient demand on the storage.

## Next: Run AI Installation.

### Run:AI Installation

To install Run:AI, complete the following steps:

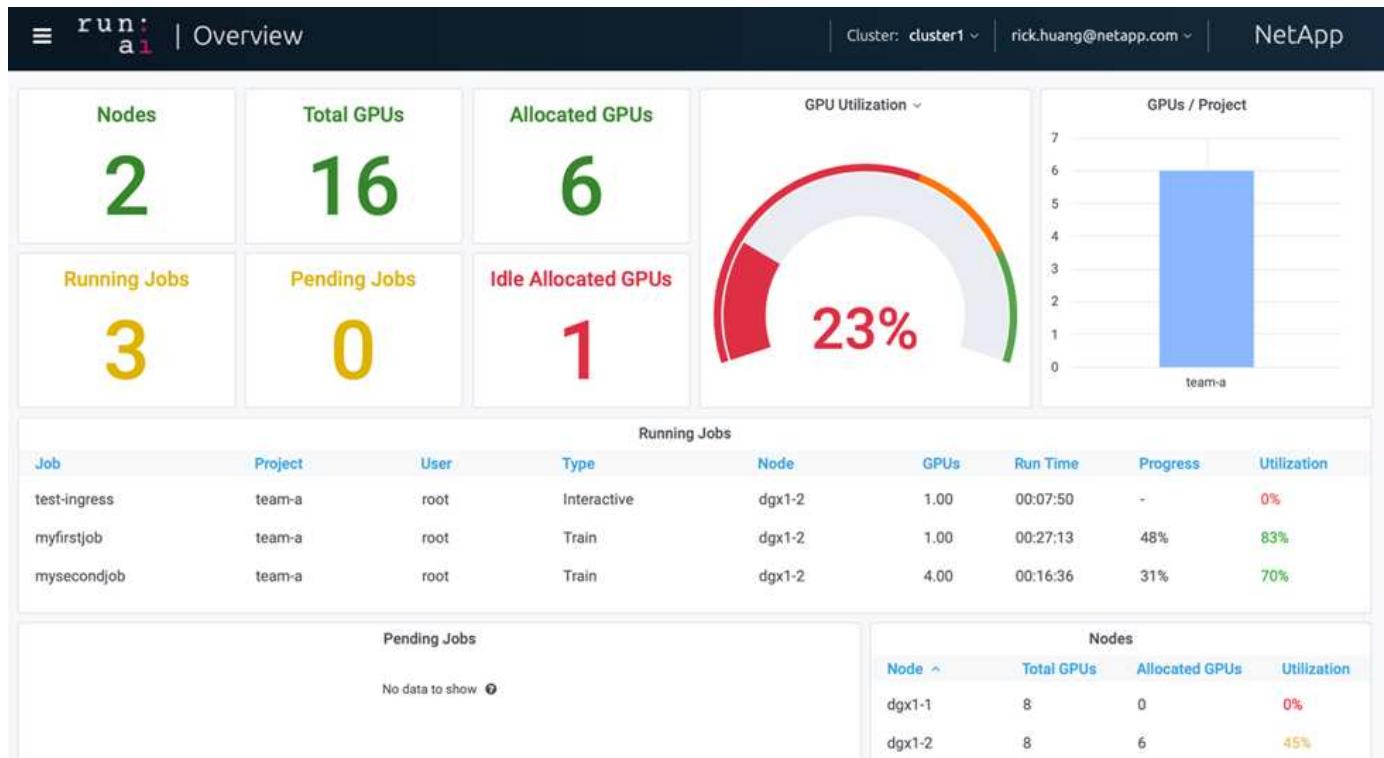
1. Install the Kubernetes cluster using DeepOps and configure the NetApp default storage class.
2. Prepare GPU nodes:
  - a. Verify that NVIDIA drivers are installed on GPU nodes.
  - b. Verify that `nvidia-docker` is installed and configured as the default docker runtime.
3. Install Run:AI:
  - a. Log into the [Run:AI Admin UI](#) to create the cluster.
  - b. Download the created `runai-operator-<clustername>.yaml` file.
  - c. Apply the operator configuration to the Kubernetes cluster.

```
kubectl apply -f runai-operator-<clustername>.yaml
```
4. Verify the installation:
  - a. Go to <https://app.run.ai/>.
  - b. Go to the Overview dashboard.
  - c. Verify that the number of GPUs on the top right reflects the expected number of GPUs and the GPU nodes are all in the list of servers. For more information about Run:AI deployment, see [installing Run:AI on an on-premise Kubernetes cluster](#) and [installing the Run:AI CLI](#).

Next: Run AI Dashboards and Views

## Run:AI Dashboards and Views

After installing Run:AI on your Kubernetes cluster and configuring the containers correctly, you see the following dashboards and views on <https://app.run.ai> in your browser, as shown in the following figure.



There are 16 total GPUs in the cluster provided by two DGX-1 nodes. You can see the number of nodes, the total available GPUs, the allocated GPUs that are assigned with workloads, the total number of running jobs, pending jobs, and idle allocated GPUs. On the right side, the bar diagram shows GPUs per Project, which summarizes how different teams are using the cluster resource. In the middle is the list of currently running jobs with job details, including job name, project, user, job type, the node each job is running on, the number of GPU(s) allocated for that job, the current run time of the job, job progress in percentage, and the GPU utilization for that job. Note that the cluster is under-utilized (GPU utilization at 23%) because there are only three running jobs submitted by a single team (team-a).

In the following section, we show how to create multiple teams in the Projects tab and allocate GPUs for each team to maximize cluster usage and manage resources when there are many users per cluster. The test scenarios mimic enterprise environments in which memory and GPU resources are shared among training, inferencing, and interactive workloads.

Next: Creating Projects for Data Science Teams and Allocating GPUs

## Creating Projects for Data Science Teams and Allocating GPUs

Researchers can submit workloads through the Run:AI CLI, Kubeflow, or similar processes. To streamline resource allocation and create prioritization, Run:AI introduces the concept of Projects. Projects are quota entities that associate a project name with GPU allocation and preferences. It is a simple and convenient way to manage multiple data science teams.

A researcher submitting a workload must associate a project with a workload request. The Run:AI scheduler compares the request against the current allocations and the project and determines whether the workload can

be allocated resources or whether it should remain in a pending state.

As a system administrator, you can set the following parameters in the Run:AI Projects tab:

- **Model projects.** Set a project per user, set a project per team of users, and set a project per a real organizational project.
- **Project quotas.** Each project is associated with a quota of GPUs that can be allocated for this project at the same time. This is a guaranteed quota in the sense that researchers using this project are guaranteed to get this number of GPUs no matter what the status in the cluster is. As a rule, the sum of the project allocation should be equal to the number of GPUs in the cluster. Beyond that, a user of this project can receive an over-quota. As long as GPUs are unused, a researcher using this project can get more GPUs. We demonstrate over-quota testing scenarios and fairness considerations in [Achieving High Cluster Utilization with Over-Quota GPU Allocation](#), [Basic Resource Allocation Fairness](#), and [Over-Quota Fairness](#).
- Create a new project, update an existing project, and delete an existing project.
- **Limit jobs to run on specific node groups.** You can assign specific projects to run only on specific nodes. This is useful when the project team needs specialized hardware, for example, with enough memory. Alternatively, a project team might be the owner of specific hardware that was acquired with a specialized budget, or when you might need to direct build or interactive workloads to work on weaker hardware and direct longer training or unattended workloads to faster nodes. For commands to group nodes and set affinity for a specific project, see the [Run:AI Documentation](#).
- **Limit the duration of interactive jobs.** Researchers frequently forget to close interactive jobs. This might lead to a waste of resources. Some organizations prefer to limit the duration of interactive jobs and close them automatically.

The following figure shows the Projects view with four teams created. Each team is assigned a different number of GPUs to account for different workloads, with the total number of GPUs equal to that of the total available GPUs in a cluster consisting of two DGX-1s.

Project Name	Assigned GPUs	Created	Training Node Affinity	Interactive Node Affinity
team-a	2	07/27/20, 9:28AM	none	none
team-b	4	07/28/20, 7:50AM	none	none
team-c	2	07/28/20, 7:50AM	none	none
team-d	8	07/28/20, 7:51AM	none	none

[Next: Submitting Jobs in Run AI CLI](#)

### Submitting Jobs in Run:AI CLI

This section provides the detail on basic Run:AI commands that you can use to run any Kubernetes job. It is divided into three parts according to workload type. AI/ML/DL workloads can be divided into two generic types:

- **Unattended training sessions.** With these types of workloads, the data scientist prepares a self-running workload and sends it for execution. During the execution, the customer can examine the results. This type of workload is often used in production or when model development is at a stage where no human intervention is required.

- **Interactive build sessions.** With these types of workloads, the data scientist opens an interactive session with Bash, Jupyter Notebook, remote PyCharm, or similar IDEs and accesses GPU resources directly. We include a third scenario for running interactive workloads with connected ports to reveal an internal port to the container user..

## Unattended Training Workloads

After setting up projects and allocating GPU(s), you can run any Kubernetes workload using the following command at the command line:

```
$ runai project set team-a runai submit hyper1 -i gcr.io/run-ai-demo/quickstart -g 1
```

This command starts an unattended training job for team-a with an allocation of a single GPU. The job is based on a sample docker image, gcr.io/run-ai-demo/quickstart. We named the job hyper1. You can then monitor the job's progress by running the following command:

```
$ runai list
```

The following figure shows the result of the `runai list` command. Typical statuses you might see include the following:

- ContainerCreating. The docker container is being downloaded from the cloud repository.
- Pending. The job is waiting to be scheduled.
- Running. The job is running.

```
You can run "runai get hyper1 -p team-a" to check the job status
~> runai list
Showing jobs for project team-a
NAME    STATUS   AGE     NODE          IMAGE                               TYPE      PROJECT  USER   GPUs
hyper1  Running  11s   gke-dev-yaron1-gpu-4-pool-154f511d-5nk5  gcr.io/run-ai-demo/quickstart  Train    team-a  yaron  1
```

To get an additional status on your job, run the following command:

```
$ runai get hyper1
```

To view the logs of the job, run the `runai logs <job-name>` command:

```
$ runai logs hyper1
```

In this example, you should see the log of a running DL session, including the current training epoch, ETA, loss function value, accuracy, and time elapsed for each step.

You can view the cluster status on the Run:AI UI at <https://app.run.ai/>. Under Dashboards > Overview, you can monitor GPU utilization.

To stop this workload, run the following command:

```
$ runai delte hyper1
```

This command stops the training workload. You can verify this action by running `runai list` again. For more detail, see [launching unattended training workloads](#).

## Interactive Build Workloads

After setting up projects and allocating GPU(s) you can run an interactive build workload using the following command at the command line:

```
$ runai submit build1 -i python -g 1 --interactive --command sleep --args infinity
```

The job is based on a sample docker image python. We named the job build1.



The `--interactive` flag means that the job does not have a start or end. It is the researcher's responsibility to close the job. The administrator can define a time limit for interactive jobs after which they are terminated by the system.

The `--g 1` flag allocates a single GPU to this job. The command and argument provided is `--command sleep --args infinity`. You must provide a command, or the container starts and then exits immediately.

The following commands work similarly to the commands described in [Unattended Training Workloads](#):

- `runai list`: Shows the name, status, age, node, image, project, user, and GPUs for jobs.
- `runai get build1`: Displays additional status on the job build1.
- `runai delete build1`: Stops the interactive workload build1. To get a bash shell to the container, the following command:

```
$ runai bash build1
```

This provides a direct shell into the computer. Data scientists can then develop or finetune their models within the container.

You can view the cluster status on the Run:AI UI at <https://app.run.ai>. For more detail, see [starting and using interactive build workloads](#).

## Interactive Workloads with Connected Ports

As an extension of interactive build workloads, you can reveal internal ports to the container user when starting a container with the Run:AI CLI. This is useful for cloud environments, working with Jupyter Notebooks, or connecting to other microservices. [Ingress](#) allows access to Kubernetes services from outside the Kubernetes cluster. You can configure access by creating a collection of rules that define which inbound connections reach which services.

For better management of external access to the services in a cluster, we suggest that cluster administrators install [Ingress](#) and configure LoadBalancer.

To use Ingress as a service type, run the following command to set the method type and the ports when submitting your workload:

```
$ runai submit test-ingress -i jupyter/base-notebook -g 1 \
--interactive --service-type=ingress --port 8888 \
--args="--NotebookApp.base_url=test-ingress" --command=start-notebook.sh
```

After the container starts successfully, execute `runai list` to see the SERVICE URL(S) with which to access the Jupyter Notebook. The URL is composed of the ingress endpoint, the job name, and the port. For example, see <https://10.255.174.13/test-ingress-8888>.

For more details, see [launching an interactive build workload with connected ports](#).

## Next: Achieving High Cluster Utilization

### Achieving High Cluster Utilization

In this section, we emulate a realistic scenario in which four data science teams each submit their own workloads to demonstrate the Run:AI orchestration solution that achieves high cluster utilization while maintaining prioritization and balancing GPU resources. We start by using the ResNet-50 benchmark described in the section [ResNet-50 with ImageNet Dataset Benchmark Summary](#):

```
$ runai submit netapp1 -i netapp/tensorflow-tf1-py3:20.01.0 --local-image
--large-shm -v /mnt:/mnt -v /tmp:/tmp --command python --args
"/netapp/scripts/run.py" --args "--
dataset_dir=/mnt/mount_0/dataset/imagenet/imagenet_original/" --args "--
num_mounts=2" --args "--dgx_version=dgx1" --args "--num_devices=1" -g 1
```

We ran the same ResNet-50 benchmark as in [NVA-1121](#). We used the flag `--local-image` for containers not residing in the public docker repository. We mounted the directories `/mnt` and `/tmp` on the host DGX-1 node to `/mnt` and `/tmp` to the container, respectively. The dataset is at NetApp AFFA800 with the `dataset_dir` argument pointing to the directory. Both `--num_devices=1` and `-g 1` mean that we allocate one GPU for this job. The former is an argument for the `run.py` script, while the latter is a flag for the `runai submit` command.

The following figure shows a system overview dashboard with 97% GPU utilization and all sixteen available GPUs allocated. You can easily see how many GPUs are allocated for each team in the GPUs/Project bar chart. The Running Jobs pane shows the current running job names, project, user, type, node, GPUs consumed, run time, progress, and utilization details. A list of workloads in queue with their wait time is shown in Pending Jobs. Finally, the Nodes box offers GPU numbers and utilization for individual DGX-1 nodes in the cluster.



Next: Fractional GPU Allocation for Less Demanding or Interactive Workloads

#### Fractional GPU Allocation for Less Demanding or Interactive Workloads

When researchers and developers are working on their models, whether in the development, hyperparameter tuning, or debugging stages, such workloads usually require fewer computational resources. It is therefore more efficient to provision fractional GPU and memory such that the same GPU can simultaneously be allocated to other workloads. Run:AI's orchestration solution provides a fractional GPU sharing system for containerized workloads on Kubernetes. The system supports workloads running CUDA programs and is especially suited for lightweight AI tasks such as inference and model building. The fractional GPU system transparently gives data science and AI engineering teams the ability to run multiple workloads simultaneously on a single GPU. This enables companies to run more workloads, such as computer vision, voice recognition, and natural language processing on the same hardware, thus lowering costs.

Run:AI's fractional GPU system effectively creates virtualized logical GPUs with their own memory and computing space that containers can use and access as if they were self-contained processors. This enables several workloads to run in containers side-by-side on the same GPU without interfering with each other. The solution is transparent, simple, and portable and it requires no changes to the containers themselves.

A typical usecase could see two to eight jobs running on the same GPU, meaning that you could do eight times the work with the same hardware.

For the job `frac05` belonging to project `team-d` in the following figure, we can see that the number of GPUs allocated was 0.50. This is further verified by the `nvidia-smi` command, which shows that the GPU memory available to the container was 16,255MB: half of the 32GB per V100 GPU in the DGX-1 node.

```

root@run-deploy:~# runai bash frac05 -p team-d
root@frac05-0:/workload# nvidia-smi
Tue Jul 28 15:17:03 2020
+-----+
| NVIDIA-SMI 450.51.05    Driver Version: 450.51.05    CUDA Version: 11.0    |
|-----+-----+-----+
| GPU  Name      Persistence-MI Bus-Id      Disp.A  Volatile Uncorr. ECC  |
| Fan  Temp  Perf  Pwr:Usage/Cap| Memory-Usage | GPU-Util  Compute M.  |
|                   |             |           |          MIG M.   |
|-----+-----+-----+-----+
|  0  Tesla V100-SXM2... On  00000000:07:00.0 Off    0          Default |
| N/A  57C   P0  240W / 300W | 15525MiB / 16255MiB | 100%       N/A |
|                   |             |           |          |
+-----+-----+-----+
+-----+
| Processes:
| GPU  GI  CI      PID  Type  Process name          GPU Memory  |
|       ID  ID
|-----+-----+-----+-----+-----+-----+
|  0  N/A N/A     156    C  python3            15525MiB  |
+-----+

```

[Next: Achieving High Cluster Utilization with Over-Quota GPU Allocation](#)

#### Achieving High Cluster Utilization with Over-Quota GPU Allocation

In this section and in the sections [Basic Resource Allocation Fairness](#), and [Over-Quota Fairness](#), we have devised advanced testing scenarios to demonstrate the Run:AI orchestration capabilities for complex workload management, automatic preemptive scheduling, and over-quota GPU provisioning. We did this to achieve high cluster-resource usage and optimize enterprise-level data science team productivity in an ONTAP AI environment.

For these three sections, set the following projects and quotas:

Project	Quota
team-a	4
team-b	2
team-c	2
team-d	8

In addition, we use the following containers for these three sections:

- Jupyter Notebook: `jupyter/base-notebook`
- Run:AI quickstart: `gcr.io/run-ai-demo/quickstart`

We set the following goals for this test scenario:

- Show the simplicity of resource provisioning and how resources are abstracted from users
- Show how users can easily provision fractions of a GPU and integer number of GPUs
- Show how the system eliminates compute bottlenecks by allowing teams or users to go over their resource quota if there are free GPUs in the cluster
- Show how data pipeline bottlenecks are eliminated by using the NetApp solution when running compute-intensive jobs, such as the NetApp container
- Show how multiple types of containers are running using the system
  - Jupyter Notebook
  - Run:AI container
- Show high utilization when the cluster is full

For details on the actual command sequence executed during the testing, see [Testing Details for Section 4.8](#).

When all 13 workloads are submitted, you can see a list of container names and GPUs allocated, as shown in the following figure. We have seven training and six interactive jobs, simulating four data science teams, each with their own models running or in development. For interactive jobs, individual developers are using Jupyter Notebooks to write or debug their code. Thus, it is suitable to provision GPU fractions without using too many cluster resources.

NAME	STATUS	AGE	NODE	IMAGE	TYPE	PROJECT	USER	GPUS	CREATED BY CLI	SERVICE URL(S)
b-4-gg	Running	2m	dgx1-2	gcr.io/run-ai-demo/quickstart	Train	team-b	root	2	true	
c-5-g	Running	2m	dgx1-2	gcr.io/run-ai-demo/quickstart	Train	team-c	root	1	true	
c-4-gg	Running	2m	dgx1-1	gcr.io/run-ai-demo/quickstart	Train	team-c	root	2	true	
b-3-g	Running	2m	dgx1-1	gcr.io/run-ai-demo/quickstart	Train	team-b	root	1	true	
c-3-g02	Running	2m	dgx1-1	gcr.io/run-ai-demo/quickstart	Interactive	team-c	root	0.2	true	
d-1-gggg	Running	2m	dgx1-2	gcr.io/run-ai-demo/quickstart	Train	team-d	root	4	true	
c-2-g03	Running	2m	dgx1-1	gcr.io/run-ai-demo/quickstart	Interactive	team-c	root	0.3	true	
c-1-g05	Running	2m	dgx1-1	gcr.io/run-ai-demo/quickstart	Interactive	team-c	root	0.5	true	
a-2-gg	Running	3m	dgx1-1	gcr.io/run-ai-demo/quickstart	Train	team-a	root	2	true	
b-2-g04	Running	3m	dgx1-2	gcr.io/run-ai-demo/quickstart	Interactive	team-b	root	0.4	true	
a-1-g	Running	3m	dgx1-1	gcr.io/run-ai-demo/quickstart	Train	team-a	root	1	true	
b-1-g06	Running	3m	dgx1-2	gcr.io/run-ai-demo/quickstart	Interactive	team-b	root	0.6	true	
a-1-1-jupyter	Running	3m	dgx1-1	jupyter/base-notebook	Interactive	team-a	root	1	true	<a href="http://10.61.218.134/a-1-1-jupyter">http://10.61.218.134/a-1-1-jupyter</a> , <a href="https://10.61.218.134/a-1-1-jupyter">https://10.61.218.134/a-1-1-jupyter</a>

The results of this testing scenario show the following:

- The cluster should be full: 16/16 GPUs are used.
- High cluster utilization.
- More experiments than GPUs due to fractional allocation.
- team-d is not using all their quota; therefore, team-b and team-c can use additional GPUs for their experiments, leading to faster time to innovation.

[Next: Basic Resource Allocation Fairness](#)

### Basic Resource Allocation Fairness

In this section, we show that, when team-d asks for more GPUs (they are under their quota), the system pauses the workloads of team-b and team-c and moves them into a pending state in a fair-share manner.

For details including job submissions, container images used, and command sequences executed, see the section [Testing Details for Section 4.9](#).

The following figure shows the resulting cluster utilization, GPUs allocated per team, and pending jobs due to automatic load balancing and preemptive scheduling. We can observe that when the total number of GPUs

requested by all team workloads exceeds the total available GPUs in the cluster, Run:AI's internal fairness algorithm pauses one job each for team-b and team-c because they have met their project quota. This provides overall high cluster utilization while data science teams still work under resource constraints set by an administrator.



The results of this testing scenario demonstrate the following:

- Automatic load balancing.** The system automatically balances the quota of the GPUs, such that each team is now using their quota. The workloads that were paused belong to teams that were over their quota.
- Fair share pause.** The system chooses to stop the workload of one team that was over their quota and then stop the workload of the other team. Run:AI has internal fairness algorithms.

Next: Over-Quota Fairness

### Over-Quota Fairness

In this section, we expand the scenario in which multiple teams submit workloads and exceed their quota. In this way, we demonstrate how Run:AI's fairness algorithm allocates cluster resources according to the ratio of preset quotas.

Goals for this test scenario:

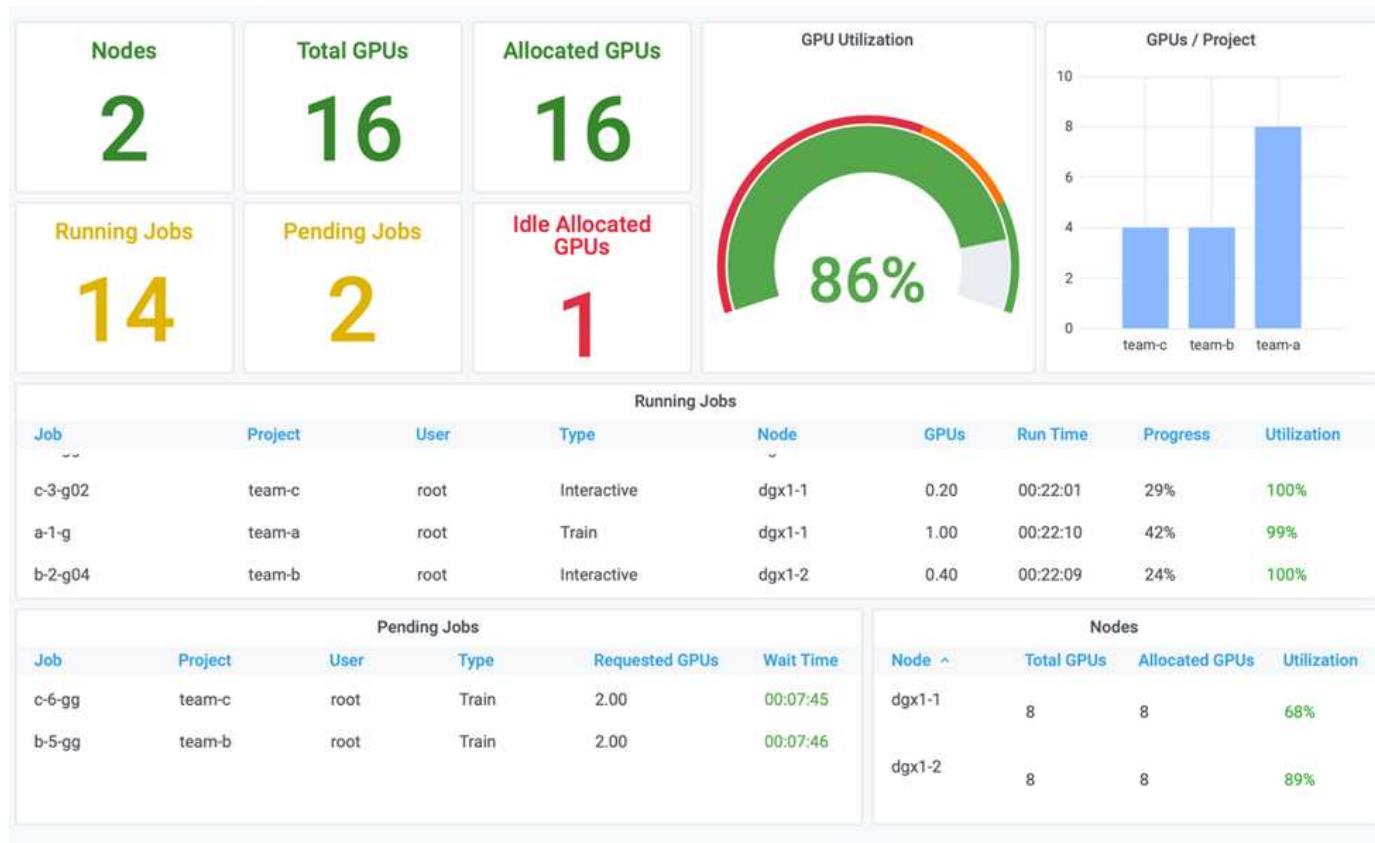
- Show queuing mechanism when multiple teams are requesting GPUs over their quota.
- Show how the system distributes a fair share of the cluster between multiple teams that are over their quota according to the ratio between their quotas, so that the team with the larger quota gets a larger share of the spare capacity.

At the end of [Basic Resource Allocation Fairness](#), there are two workloads queued: one for team-b and one

for team-c. In this section, we queue additional workloads.

For details including job submissions, container images used, and command sequences executed, see [Testing Details for section 4.10](#).

When all jobs are submitted according to the section [Testing Details for section 4.10](#), the system dashboard shows that team-a, team-b, and team-c all have more GPUs than their preset quota. team-a occupies four more GPUs than its preset soft quota (four), whereas team-b and team-c each occupy two more GPUs than their soft quota (two). The ratio of over-quota GPUs allocated is equal to that of their preset quota. This is because the system used the preset quota as a reference of priority and provisioned accordingly when multiple teams request more GPUs, exceeding their quota. Such automatic load balancing provides fairness and prioritization when enterprise data science teams are actively engaged in AI model development and production.



The results of this testing scenario show the following:

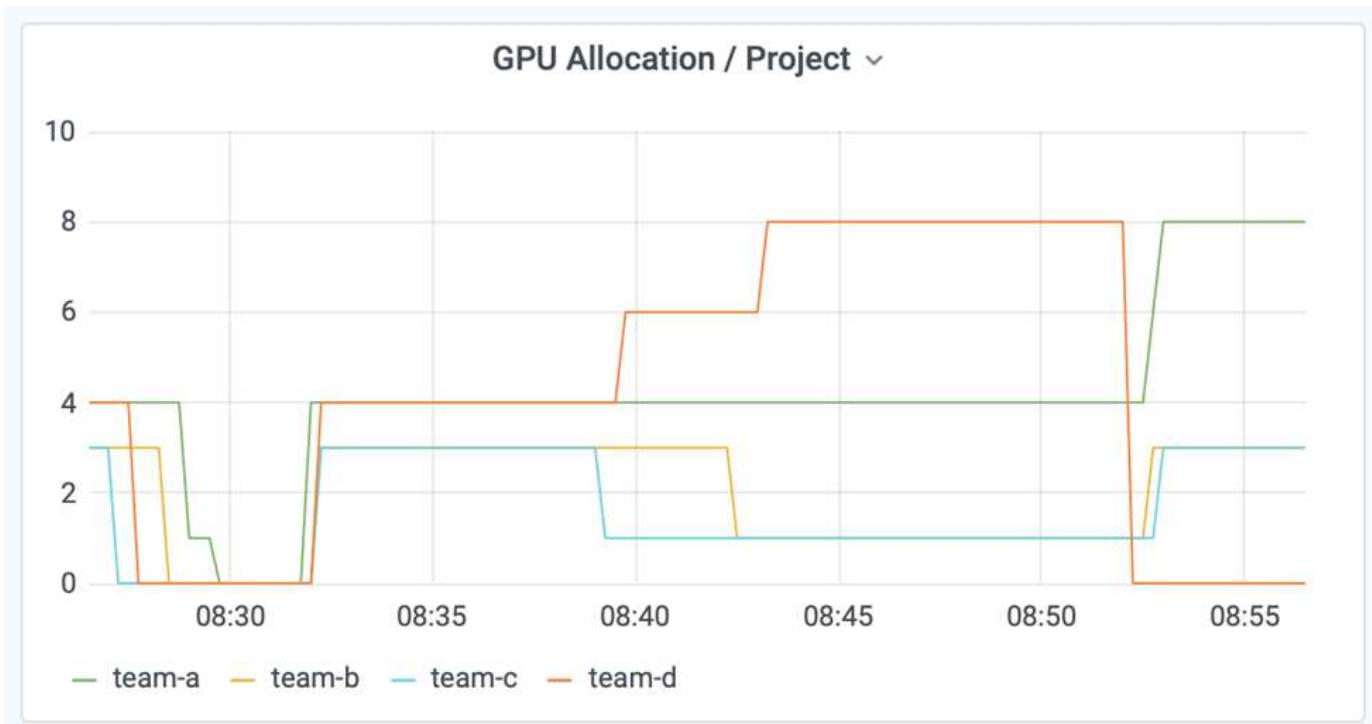
- The system starts to de-queue the workloads of other teams.
- The order of the dequeuing is decided according to fairness algorithms, such that team-b and team-c get the same amount of over-quota GPUs (since they have a similar quota), and team-a gets a double amount of GPUs since their quota is two times higher than the quota of team-b and team-c.
- All the allocation is done automatically.

Therefore, the system should stabilize on the following states:

Project	GPUs allocated	Comment
team-a	8/4	Four GPUs over the quota. Empty queue.

Project	GPUs allocated	Comment
team-b	4/2	Two GPUs over the quota. One workload queued.
team-c	4/2	Two GPUs over the quota. One workload queued.
team-d	0/8	Not using GPUs at all, no queued workloads.

The following figure shows the GPU allocation per project over time in the Run:AI Analytics dashboard for the sections [Achieving High Cluster Utilization with Over-Quota GPU Allocation](#), [Basic Resource Allocation Fairness](#), and [Over-Quota Fairness](#). Each line in the figure indicates the number of GPUs provisioned for a given data science team at any time. We can see that the system dynamically allocates GPUs according to workloads submitted. This allows teams to go over quota when there are available GPUs in the cluster, and then preempt jobs according to fairness, before finally reaching a stable state for all four teams.



Next: [Saving Data to a Trident-Provisioned PersistentVolume](#)

### Saving Data to a Trident-Provisioned PersistentVolume

NetApp Trident is a fully supported open source project designed to help you meet the sophisticated persistence demands of your containerized applications. You can read and write data to a Trident-provisioned Kubernetes PersistentVolume (PV) with the added benefit of data tiering, encryption, NetApp Snapshot technology, compliance, and high performance offered by NetApp ONTAP data management software.

### Reusing PVCs in an Existing Namespace

For larger AI projects, it might be more efficient for different containers to read and write data to the same Kubernetes PV. To reuse a Kubernetes Persistent Volume Claim (PVC), the user must have already created a PVC. See the [NetApp Trident documentation](#) for details on creating a PVC. Here is an example of reusing an existing PVC:

```
$ runai submit pvc-test -p team-a --pvc test:/tmp/pvc1mount -i gcr.io/run-ai-demo/quickstart -g 1
```

Run the following command to see the status of job pvc-test for project team-a:

```
$ runai get pvc-test -p team-a
```

You should see the PV /tmp/pvc1mount mounted to team-a job pvc-test. In this way, multiple containers can read from the same volume, which is useful when there are multiple competing models in development or in production. Data scientists can build an ensemble of models and then combine prediction results by majority voting or other techniques.

Use the following to access the container shell:

```
$ runai bash pvc-test -p team-a
```

You can then check the mounted volume and access your data within the container.

This capability of reusing PVCs works with NetApp FlexVol volumes and NetApp ONTAP FlexGroup volumes, enabling data engineers more flexible and robust data management options to leverage your data fabric powered by NetApp.

[Next: Conclusion](#)

## Conclusion

NetApp and Run:AI have partnered in this technical report to demonstrate the unique capabilities of the NetApp ONTAP AI solution together with the Run:AI Platform for simplifying orchestration of AI workloads. The preceding steps provide a reference architecture to streamline the process of data pipelines and workload orchestration for deep learning. Customers looking to implement these solutions are encouraged to reach out to NetApp and Run:AI for more information.

[Next: Testing Details for Section 4.8](#)

## Testing Details for Section 4.8

This section contains the testing details for the section [Achieving High Cluster Utilization with Over-Quota GPU Allocation](#).

Submit jobs in the following order:

Project	Image	# GPUs	Total	Comment
team-a	Jupyter	1	1/4	—
team-a	NetApp	1	2/4	—
team-a	Run:AI	2	4/4	Using all their quota
team-b	Run:AI	0.6	0.6/2	Fractional GPU

Project	Image	# GPUs	Total	Comment
team-b	Run:AI	0.4	1/2	Fractional GPU
team-b	NetApp	1	2/2	-
team-b	NetApp	2	4/2	Two over quota
team-c	Run:AI	0.5	0.5/2	Fractional GPU
team-c	Run:AI	0.3	0.8/2	Fractional GPU
team-c	Run:AI	0.2	1/2	Fractional GPU
team-c	NetApp	2	3/2	One over quota
team-c	NetApp	1	4/2	Two over quota
team-d	NetApp	4	4/8	Using half of their quota

Command structure:

```
$ runai submit <job-name> -p <project-name> -g <#GPUs> -i <image-name>
```

Actual command sequence used in testing:

```
$ runai submit a-1-1-jupyter -i jupyter/base-notebook -g 1 \
--interactive --service-type=ingress --port 8888 \
--args="--NotebookApp.base_url=team-a-test-ingress" --command=start
-notebook.sh -p team-a
$ runai submit a-1-g -i gcr.io/run-ai-demo/quickstart -g 1 -p team-a
$ runai submit a-2-gg -i gcr.io/run-ai-demo/quickstart -g 2 -p team-a
$ runai submit b-1-g06 -i gcr.io/run-ai-demo/quickstart -g 0.6
--interactive -p team-b
$ runai submit b-2-g04 -i gcr.io/run-ai-demo/quickstart -g 0.4
--interactive -p team-b
$ runai submit b-3-g -i gcr.io/run-ai-demo/quickstart -g 1 -p team-b
$ runai submit b-4-gg -i gcr.io/run-ai-demo/quickstart -g 2 -p team-b
$ runai submit c-1-g05 -i gcr.io/run-ai-demo/quickstart -g 0.5
--interactive -p team-c
$ runai submit c-2-g03 -i gcr.io/run-ai-demo/quickstart -g 0.3
--interactive -p team-c
$ runai submit c-3-g02 -i gcr.io/run-ai-demo/quickstart -g 0.2
--interactive -p team-c
$ runai submit c-4-gg -i gcr.io/run-ai-demo/quickstart -g 2 -p team-c
$ runai submit c-5-g -i gcr.io/run-ai-demo/quickstart -g 1 -p team-c
$ runai submit d-1-gggg -i gcr.io/run-ai-demo/quickstart -g 4 -p team-d
```

At this point, you should have the following states:

Project	GPUs Allocated	Workloads Queued
team-a	4/4 (soft quota/actual allocation)	None
team-b	4/2	None
team-c	4/2	None
team-d	4/8	None

See the section [Achieving High Cluster Utilization with Over-quota GPU Allocation](#) for discussions on the proceeding testing scenario.

[Next: Testing Details for Section 4.9](#)

### Testing Details for Section 4.9

This section contains testing details for the section [Basic Resource Allocation Fairness](#).

Submit jobs in the following order:

Project	# GPUs	Total	Comment
team-d	2	6/8	Team-b/c workload pauses and moves to pending.
team-d	2	8/8	Other team (b/c) workloads pause and move to pending.

See the following executed command sequence:

```
$ runai submit d-2-gg -i gcr.io/run-ai-demo/quickstart -g 2 -p team-d
$ runai submit d-3-gg -i gcr.io/run-ai-demo/quickstart -g 2 -p team-d
```

At this point, you should have the following states:

Project	GPUs Allocated	Workloads Queued
team-a	4/4	None
team-b	2/2	None
team-c	2/2	None
team-d	8/8	None

See the section [Basic Resource Allocation Fairness](#) for a discussion on the proceeding testing scenario.

[Next: Testing Details for Section 4.10](#)

### Testing Details for Section 4.10

This section contains testing details for the section [Over-Quota Fairness](#).

Submit jobs in the following order for team-a, team-b, and team-c:

Project	# GPUs	Total	Comment
team-a	2	4/4	1 workload queued
team-a	2	4/4	2 workloads queued
team-b	2	2/2	2 workloads queued
team-c	2	2/2	2 workloads queued

See the following executed command sequence:

```
$ runai submit a-3-gg -i gcr.io/run-ai-demo/quickstart -g 2 -p team-a$ runai submit a-4-gg -i gcr.io/run-ai-demo/quickstart -g 2 -p team-a$ runai submit b-5-gg -i gcr.io/run-ai-demo/quickstart -g 2 -p team-b$ runai submit c-6-gg -i gcr.io/run-ai-demo/quickstart -g 2 -p team-c
```

At this point, you should have the following states:

Project	GPUs Allocated	Workloads Queued
team-a	4/4	Two workloads asking for GPUs two each
team-b	2/2	Two workloads asking for two GPUs each
team-c	2/2	Two workloads asking for two GPUs each
team-d	8/8	None

Next, delete all the workloads for team-d:

```
$ runai delete -p team-d d-1-gggg d-2-gg d-3-gg
```

See the section [Over-Quota Fairness](#), for discussions on the proceeding testing scenario.

[Next: Where to Find Additional Information](#)

## Where to Find Additional Information

To learn more about the information that is described in this document, see the following resources:

- NVIDIA DGX Systems
  - NVIDIA DGX-1 System  
<https://www.nvidia.com/en-us/data-center/dgx-1/>
  - NVIDIA V100 Tensor Core GPU  
<https://www.nvidia.com/en-us/data-center/tesla-v100/>

- NVIDIA NGC  
<https://www.nvidia.com/en-us/gpu-cloud/>
- Run:AI container orchestration solution
  - Run:AI product introduction  
<https://docs.run.ai/home/components/>
  - Run:AI installation documentation  
<https://docs.run.ai/Administrator/Cluster-Setup/Installing-Run-AI-on-an-on-premise-Kubernetes-Cluster/>  
<https://docs.run.ai/Administrator/Researcher-Setup/Installing-the-Run-AI-Command-Line-Interface/>
  - Submitting jobs in Run:AI CLI  
<https://docs.run.ai/Researcher/Walkthroughs/Walkthrough-Launch-Unattended-Training-Workloads-/>  
<https://docs.run.ai/Researcher/Walkthroughs/Walkthrough-Start-and-Use-Interactive-Build-Workloads-/>
  - Allocating GPU fractions in Run:AI CLI  
<https://docs.run.ai/Researcher/Walkthroughs/Walkthrough-Using-GPU-Fractions/>
- NetApp AI Control Plane
  - Technical report  
<https://www.netapp.com/us/media/tr-4798.pdf>
  - Short-form demo  
[https://youtu.be/gfr\\_sO27Rvo](https://youtu.be/gfr_sO27Rvo)
  - GitHub repository  
[https://github.com/NetApp/kubeflow\\_jupyter\\_pipeline](https://github.com/NetApp/kubeflow_jupyter_pipeline)
- NetApp AFF systems
  - NetApp AFF A-Series Datasheet  
<https://www.netapp.com/us/media/ds-3582.pdf>
  - NetApp Flash Advantage for All Flash FAS  
<https://www.netapp.com/us/media/ds-3733.pdf>
  - ONTAP 9 Information Library  
<http://mysupport.netapp.com/documentation/productlibrary/index.html?productID=62286>
  - NetApp ONTAP FlexGroup Volumes technical report  
<https://www.netapp.com/us/media/tr-4557.pdf>
- NetApp ONTAP AI
  - ONTAP AI with DGX-1 and Cisco Networking Design Guide  
<https://www.netapp.com/us/media/nva-1121-design.pdf>
  - ONTAP AI with DGX-1 and Cisco Networking Deployment Guide  
<https://www.netapp.com/us/media/nva-1121-deploy.pdf>
  - ONTAP AI with DGX-1 and Mellanox Networking Design Guide  
<http://www.netapp.com/us/media/nva-1138-design.pdf>
  - ONTAP AI with DGX-2 Design Guide  
<https://www.netapp.com/us/media/nva-1135-design.pdf>

# NetApp Container Solutions

:x

## TR-4919: DevOps with NetApp Astra

Alan Cowles and Nikhil M Kulkarni, NetApp

### Use cases

The DevOps with NetApp Astra solution is architected to deliver exceptional value for customers with the following use cases:

- Easy to deploy and manage applications and development environments deployed on top of supported Kubernetes distributions.
- Discussion of real-world use cases for DevOps workflows and examples of the tools and methods that NetApp can provide to make adoption and use of these methods easier.
- Exploration of how application-consistent snapshot, backups, and clones can be used to enhance the DevOps experience.

### Business value

Enterprises are increasingly adopting DevOps practices to create new products, shorten release cycles, and rapidly add new features. Because of their innate agile nature, containers and microservices play a crucial role in supporting DevOps practices. However, practicing DevOps at a production scale in an enterprise environment presents its own challenges and imposes certain requirements on the underlying infrastructure, such as the following:

- High availability at all layers in the stack so that workflows are never interrupted.
- Ease of deployment and management procedures for the end user.
- API-driven and programmable infrastructure to keep up with microservices and developer agility.
- Ability to scale infrastructure independently and in an automated fashion, based on workload demands.
- Protecting applications alongside their backing persistent data sets for DevOps workflows accelerate time to market by not having to rely on redeployments or manual copying of data.

Recognizing these capabilities and challenges, this technical report outlines the process of improving and simplifying DevOps use cases for containerized applications using the wide portfolio of NetApp products.

### Technology overview

The DevOps with NetApp solution contains the following major components:

#### DevOps practices

DevOps practices focus on automated, repeatable, and easily manageable operations that enhance the development workflow by allowing the end user to control the environment in which they are developing their code. This solution provides several examples and use cases in which NetApp technology can be of the greatest benefit to such operations.

## Container orchestration

There are numerous container orchestration platforms in use today. Although most of these platforms are based on Kubernetes, each has pros and cons. So it is important to understand feature sets and integrations when selecting a container orchestration platform for DevOps workflows. With the NetApp Astra suite of products, we support the following platforms for full-fledged DevOps use cases:

- [Red Hat OpenShift 4.6.8+](#)
- [Rancher 2.5+](#)
- [Kubernetes 1.20+](#)
- [VMware Tanzu Kubernetes Grid 1.4+](#)
- [VMware Tanzu Kubernetes Grid Integrated Edition 1.12.2+](#)

## NetApp storage systems

NetApp has several storage systems perfect for enterprise data centers and hybrid cloud deployments. The NetApp portfolio includes NetApp ONTAP, NetApp Element, and NetApp e-Series storage systems, all of which can provide persistent storage for containerized applications.

For more information, visit the NetApp website [here](#).

## NetApp storage integrations

NetApp Astra Control Center offers a rich set of storage and application-aware data management services for stateful Kubernetes workloads deployed in an on-prem environment and powered by trusted NetApp data-protection technology.

For more information, visit the NetApp Astra website [here](#).

Astra Trident is an open-source and fully-supported storage orchestrator for containers and Kubernetes distributions like Red Hat OpenShift, VMware Tanzu, Anthos by Google Cloud etc..

For more information, visit the Astra Trident website [here](#).

[Next: DevOps Overview.](#)

## DevOps Overview

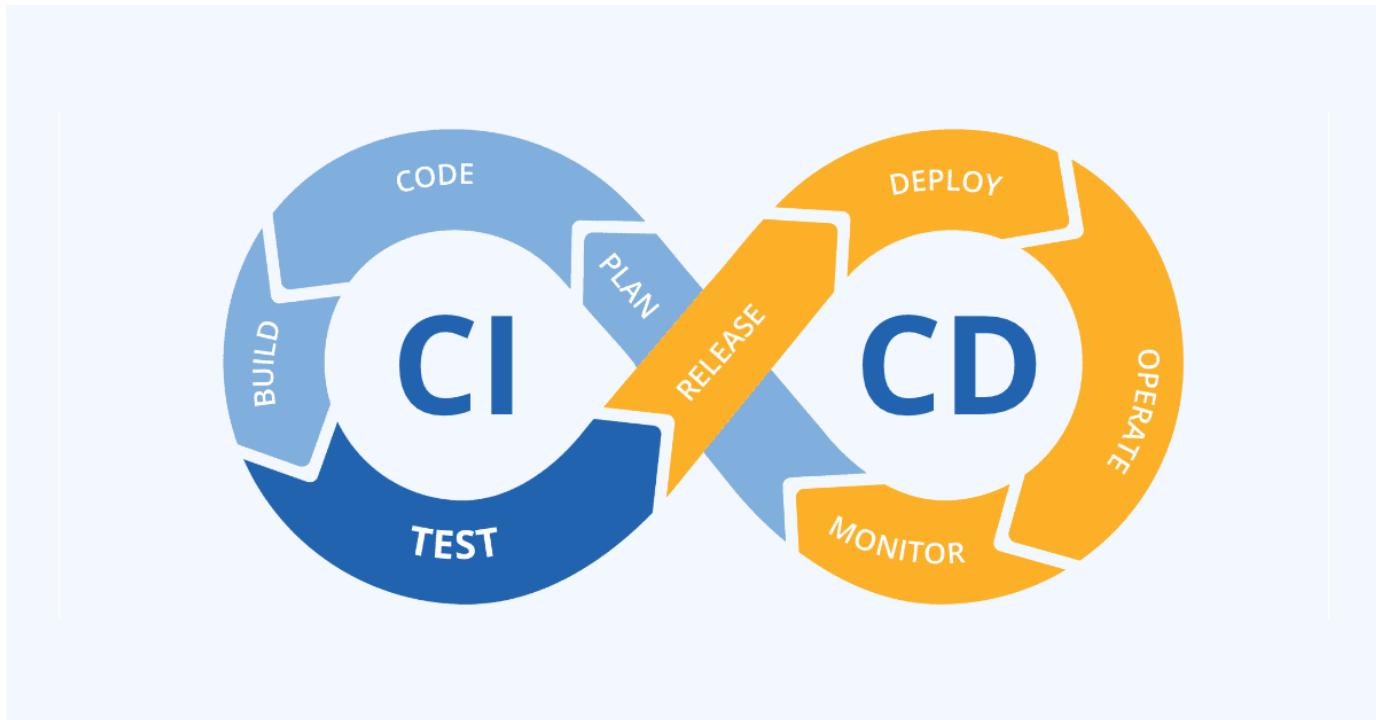
Over the past several years, organizations that build software have been embracing the concepts of DevOps. DevOps practices break down organizational barriers, bringing development and operations teams closer together. DevOps practices also empower the teams to accelerate delivery, increase availability, and make services and applications more stable, thus improving the team's productivity. In addition, adoption of an automation framework is also a key ingredient of success — from building, testing, and operating applications at scale or managing a fully automated infrastructure platform or stack. Below we discuss some primary use cases for DevOps where NetApp solutions can be implemented to help enhance the experiences that DevOps practitioners encounter during their daily practice.

## DevOps use cases

Although DevOps does not have a single, universally accepted definition, solutions for DevOps practitioners typically contain similar constructs or ideologies that enable easy implementation, repetition, and management at scale. The following sections describe potential use cases for DevOps workflows enabled by NetApp solutions.

## Continuous Integration, Continuous Delivery, and Continuous Deployment (CI/CD)

Continuous Integration, Continuous Delivery, and Continuous Deployment (CI/CD) is a coding philosophy that encourages developers to implement and transform their coding practices by establishing a method by which they can consistently update, test, and deploy their code in an automated fashion. The most popular method by which CI/CD is implemented in most DevOps workflows is that of the CI/CD pipeline, and there are several third-party software applications that can help achieve this.



See the following examples of popular applications that can help with CI/CD-type workflows:

[ArgoCD](#)

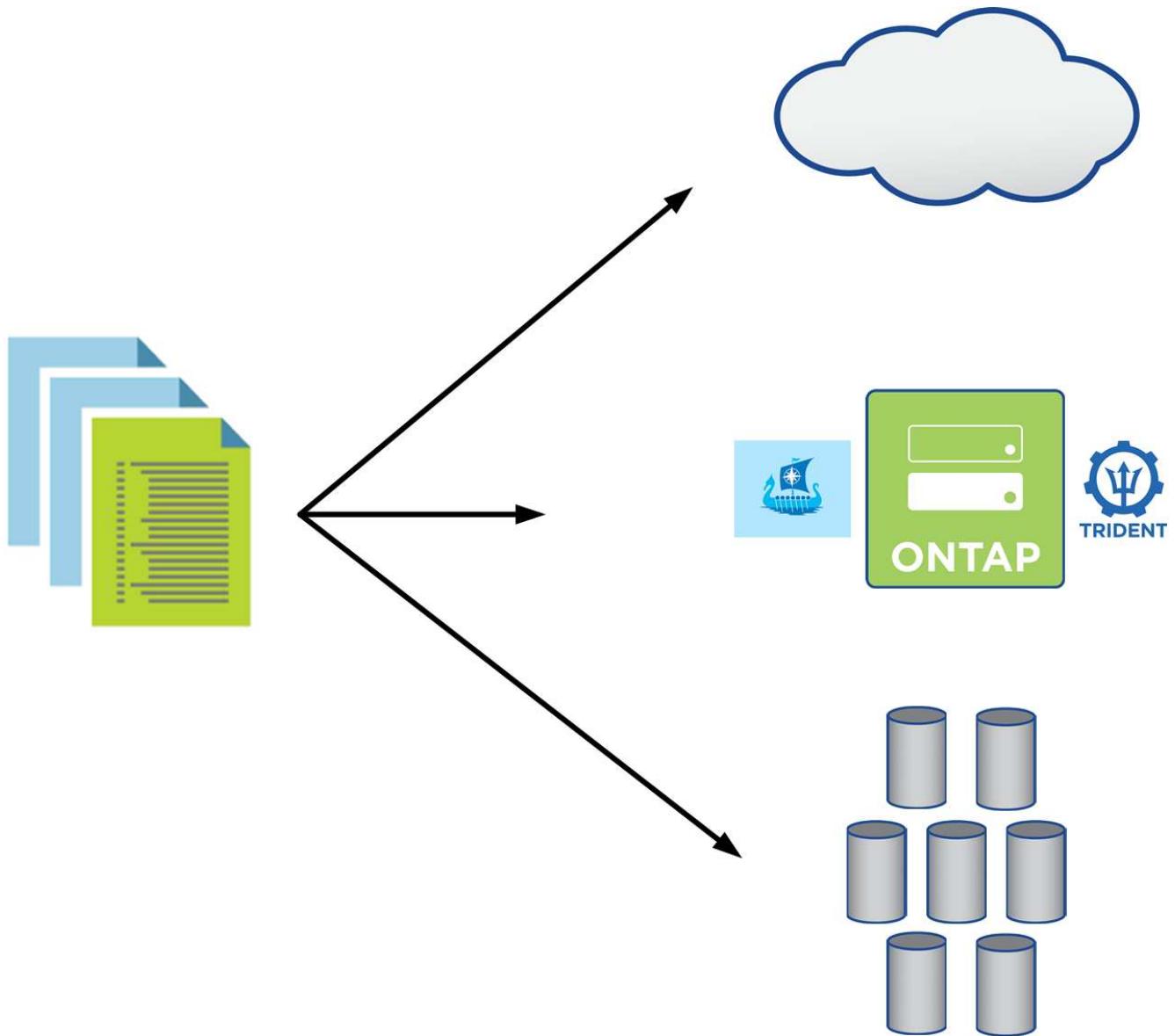
[Jenkins](#)

[Tekton](#)

Some of the use cases included later in this technical report have been demonstrated in Jenkins, but the primary CI/CD principles can be applied to whatever tool an organization has implemented in their own practices.

### Infrastructure as code

Infrastructure as code helps provision and manage IT resources through automated commands, APIs, and software development kits (SDK). This concept greatly enhance the DevOps experience by removing physical data center or resource limitations that could prevent developers from meeting their objectives.



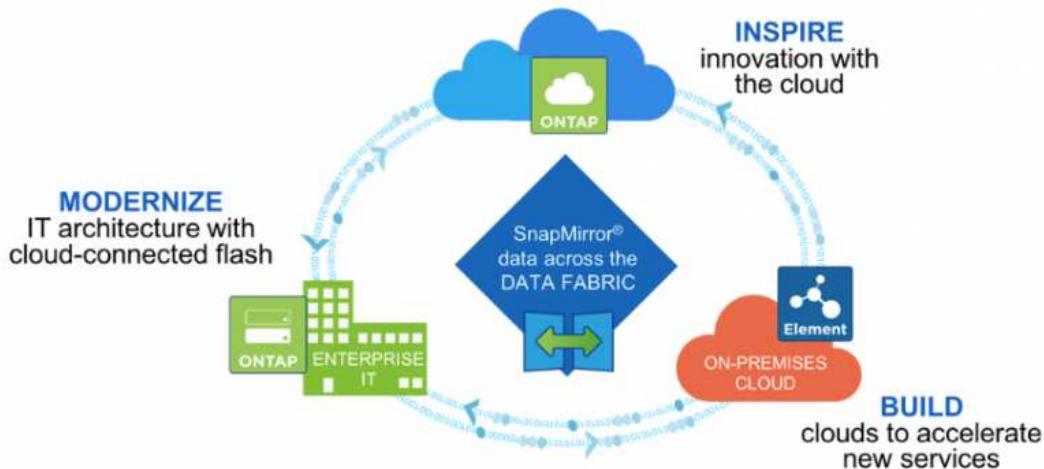
End users often use programming languages such as [Python](#) or automation tools such as [Ansible](#) or [Puppet](#) to create automated and repeatable infrastructure scaling actions that can be called by developers when needed.

Both NetApp ONTAP and Astra Control contain public facing APIs and ansible modules or software development toolkits that make automating operations very easy to adopt and integrate into DevOps processes.

[Next: NetApp Storage Systems Overview.](#)

## NetApp storage systems overview

NetApp has several storage platforms that are qualified with Astra Trident and Astra Control to provision, protect, and manage data for containerized applications.



- AFF and FAS systems run NetApp ONTAP and provide storage for both file-based (NFS) and block-based (iSCSI) use cases.
- Cloud Volumes ONTAP and ONTAP Select provide the same benefits in the cloud and virtual space respectively.
- NetApp Cloud Volumes Service (AWS/GCP) and Azure NetApp Files provide file-based storage in the cloud.



Each storage system in the NetApp portfolio can ease both data management and movement between on-premises sites and the cloud so that your data is where your applications are.

The following pages have additional information about the NetApp storage systems validated in the DevOps with NetApp solution:

- [NetApp ONTAP](#)

Next: [NetApp storage integrations overview](#).

## NetApp ONTAP

NetApp ONTAP is a powerful storage-software tool with capabilities such as an intuitive GUI, REST APIs with automation integration, AI-informed predictive analytics and corrective action, non-disruptive hardware upgrades, and cross-storage import.

For more information about the NetApp ONTAP storage system, visit the [NetApp ONTAP website](#).

ONTAP provides the following features:

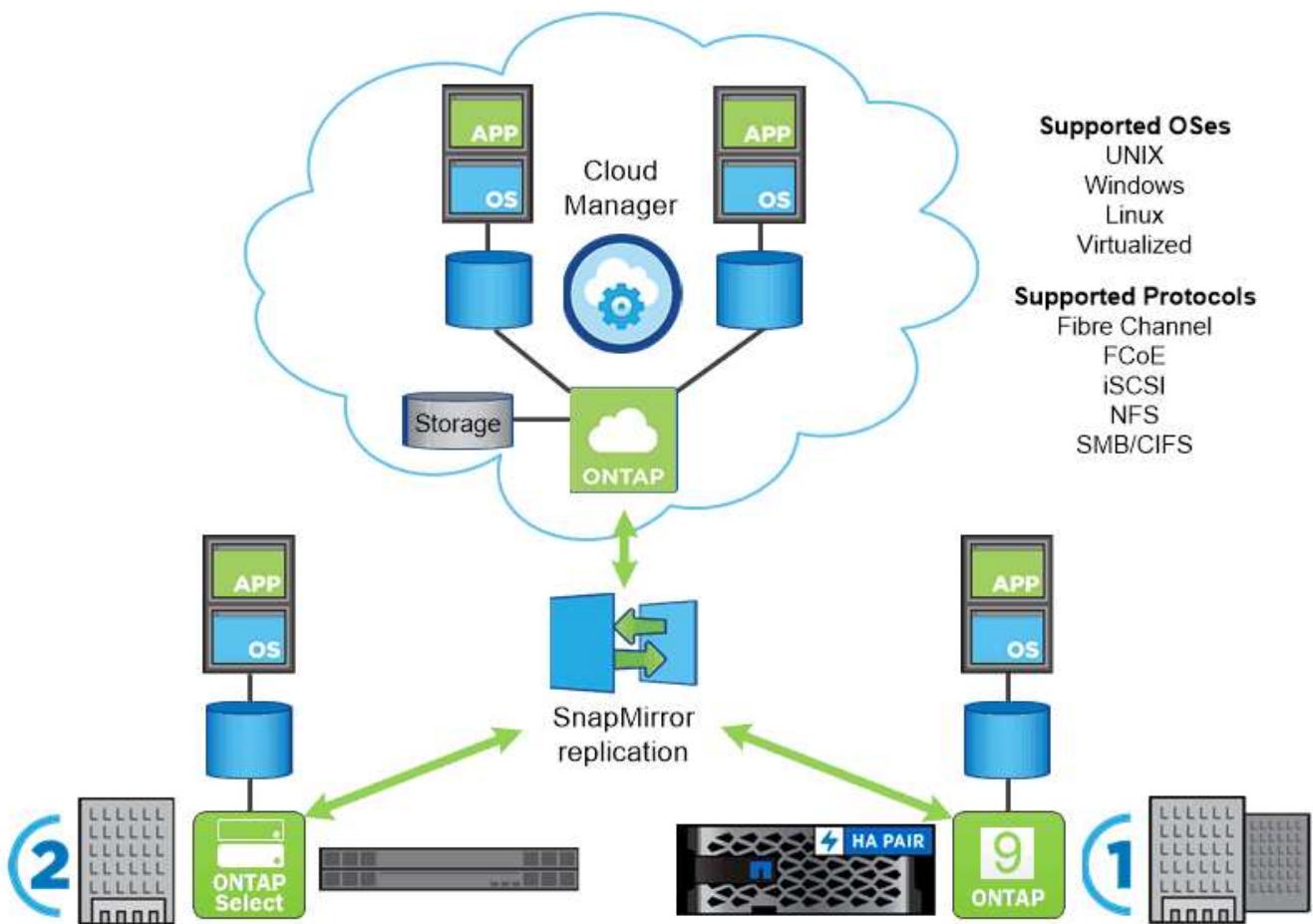
- A unified storage system with simultaneous data access and management of NFS, CIFS, iSCSI, FC, FCoE, and FC-NVMe protocols.
- Different deployment models include on-premises on all-flash, hybrid, and all-HDD hardware configurations; VM-based storage platforms on a supported hypervisor such as ONTAP Select; and in the cloud as Cloud Volumes ONTAP.

- Increased data storage efficiency on ONTAP systems with support for automatic data tiering, inline data compression, deduplication, and compaction.
- Workload-based, QoS-controlled storage.
- Seamless integration with a public cloud for tiering and protecting data. ONTAP also provides robust data protection capabilities that sets it apart in any environment:
  - **NetApp Snapshot copies.** A fast, point-in-time backup of data using a minimal amount of disk space with no additional performance overhead.
  - **NetApp SnapMirror.** Mirrors the Snapshot copies of data from one storage system to another. ONTAP supports mirroring data to other physical platforms and cloud-native services as well.
  - **NetApp SnapLock.** Efficiently administration of non-rewritable data by writing it to special volumes that cannot be overwritten or erased for a designated period.
  - **NetApp SnapVault.** Backs up data from multiple storage systems to a central Snapshot copy that serves as a backup to all designated systems.
  - **NetApp SyncMirror.** Provides real-time, RAID-level mirroring of data to two different plexes of disks that are connected physically to the same controller.
  - **NetApp SnapRestore.** Provides fast restoration of backed-up data on demand from Snapshot copies.
  - **NetApp FlexClone.** Provides instantaneous provisioning of a fully readable and writeable copy of a NetApp volume based on a Snapshot copy.

For more information about ONTAP, see the [ONTAP 9 Documentation Center](#).



NetApp ONTAP is available on-premises, virtualized, or in the cloud.



## NetApp platforms

### NetApp AFF/FAS

NetApp provides robust all-flash (AFF) and scale-out hybrid (FAS) storage platforms that are tailor-made with low-latency performance, integrated data protection, and multi-protocol support.

Both systems are powered by NetApp ONTAP data management software, the industry's most advanced data-management software for simplified, highly available, cloud-integrated storage management to deliver enterprise-class speed, efficiency, and security for your data fabric needs.

For more information about NETAPP AFF/FAS platforms, click [here](#).

### ONTAP Select

ONTAP Select is a software-defined deployment of NetApp ONTAP that can be deployed onto a hypervisor in your environment. It can be installed on VMware vSphere or on KVM, and it provides the full functionality and experience of a hardware-based ONTAP system.

For more information about ONTAP Select, click [here](#).

### Cloud Volumes ONTAP

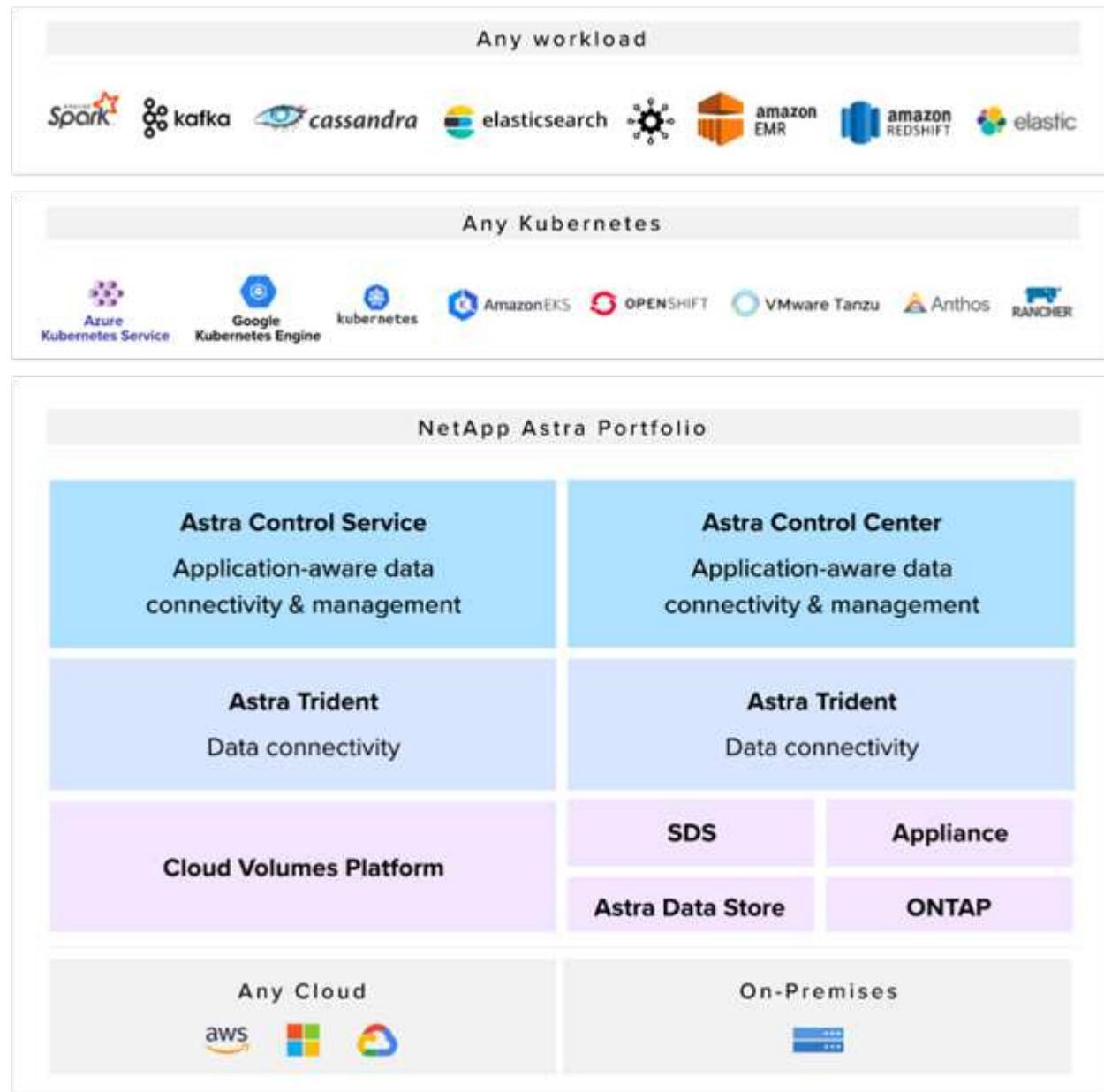
NetApp Cloud Volumes ONTAP is a cloud-deployed version of NetApp ONTAP available to be deployed in a number of public clouds, including: Amazon AWS, Microsoft Azure, and Google Cloud.

For more information about Cloud Volumes ONTAP, click [here](#).

Next: NetApp Storage Integrations Overview.

## NetApp Storage Integration Overview

NetApp provides a number of products to help you orchestrate, manage, protect, and migrate stateful containerized applications and their data.



NetApp Astra Control offers a rich set of storage and application-aware data management services for stateful Kubernetes workloads powered by NetApp data protection technology. The Astra Control Service is available to support stateful workloads in cloud-native Kubernetes deployments. The Astra Control Center is available to support stateful workloads in on-premises deployments of Enterprise Kubernetes platforms like Red Hat OpenShift, Rancher, VMware Tanzu etc. For more information visit the NetApp Astra Control website [here](#).

NetApp Astra Trident is an open-source and fully-supported storage orchestrator for containers and Kubernetes distributions like Red Hat OpenShift, Rancher, VMware Tanzu etc. For more information, visit the

Astra Trident website [here](#).

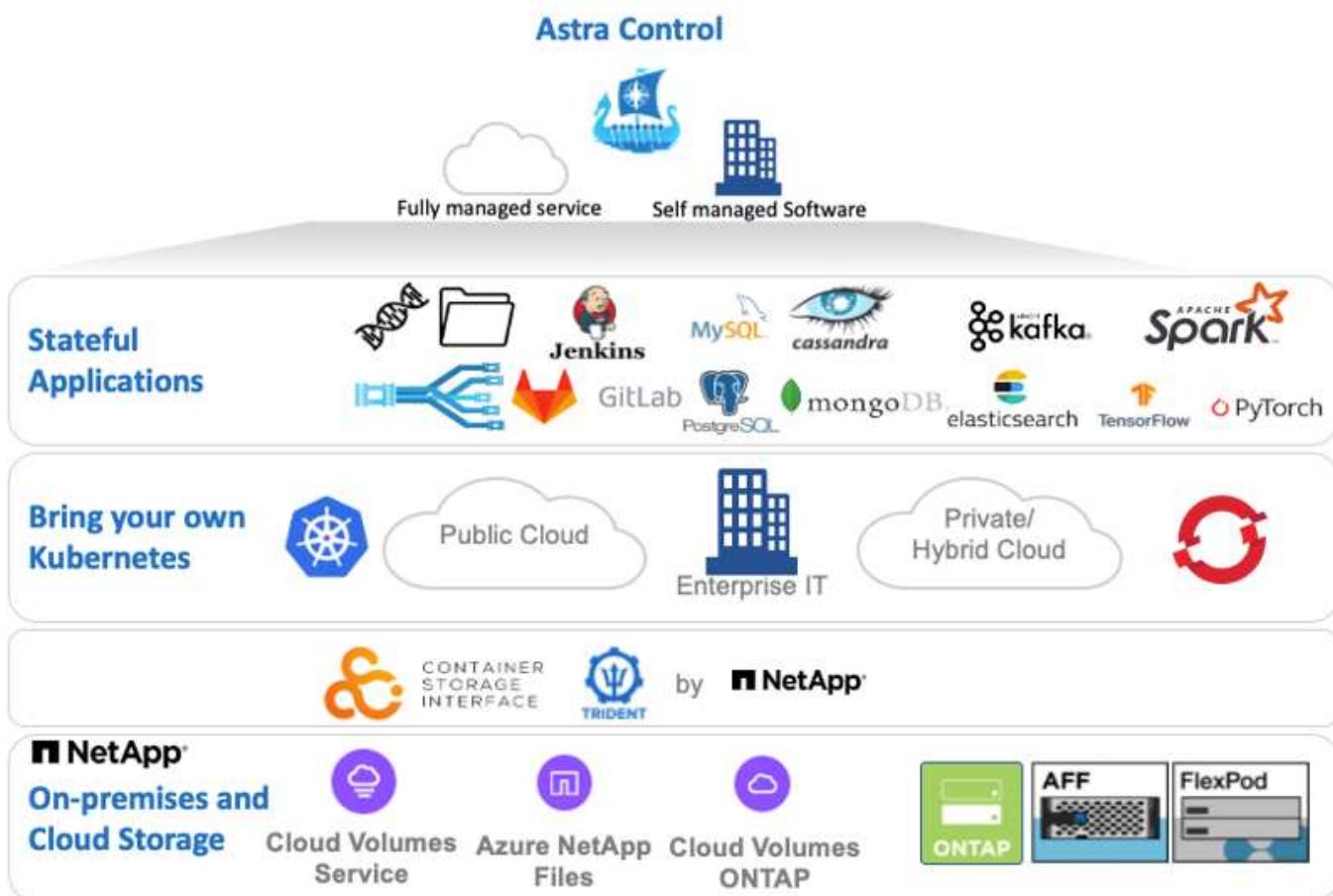
The following pages have additional information about the NetApp products that have been validated for application and persistent storage management in the DevOps with NetApp solution:

- [NetApp Astra Control Center](#)
- [NetApp Astra Trident](#)

Next: Use-case Validations: DevOps with NetApp Astra.

## NetApp Astra Control overview

NetApp Astra Control Center offers a rich set of storage and application-aware data management services for stateful Kubernetes workloads deployed in an on-premises environment and powered by NetApp data protection technology.



NetApp Astra Control Center can be installed on a Kubernetes cluster that has the Astra Trident storage orchestrator deployed and configured with storage classes and storage backends to NetApp ONTAP storage systems.

For more information on Astra Trident, see [this document here](#).

In a cloud-connected environment, Astra Control Center uses Cloud Insights to provide advanced monitoring and telemetry. In the absence of a Cloud Insights connection, limited monitoring and telemetry (seven days worth of metrics) is available and exported to Kubernetes native monitoring tools (Prometheus and Grafana) through open metrics endpoints.

Astra Control Center is fully integrated into the NetApp AutoSupport and Active IQ ecosystem to provide support for users, provide assistance with troubleshooting, and display usage statistics.

In addition to the paid version of Astra Control Center, a 90-day evaluation license is available. The evaluation version is supported through email and the community Slack channel. Customers have access to these resources, other knowledge-base articles, and documentation available from the in-product support dashboard.

To understand more about the Astra portfolio, visit the [Astra website](#).

For a detailed installation and operations guide on Astra Control Center, follow the documentation [here](#).

#### **Astra Control Center automation**

Astra Control Center has a fully functional REST API for programmatic access. Users can use any programming language or utility to interact with Astra Control REST API endpoints. To learn more about this API, see the documentation [here](#).

If you are looking for a ready-made software development toolkit for interacting with Astra Control REST APIs, NetApp provides a toolkit with Astra Control Python SDK, which you can download [here](#).

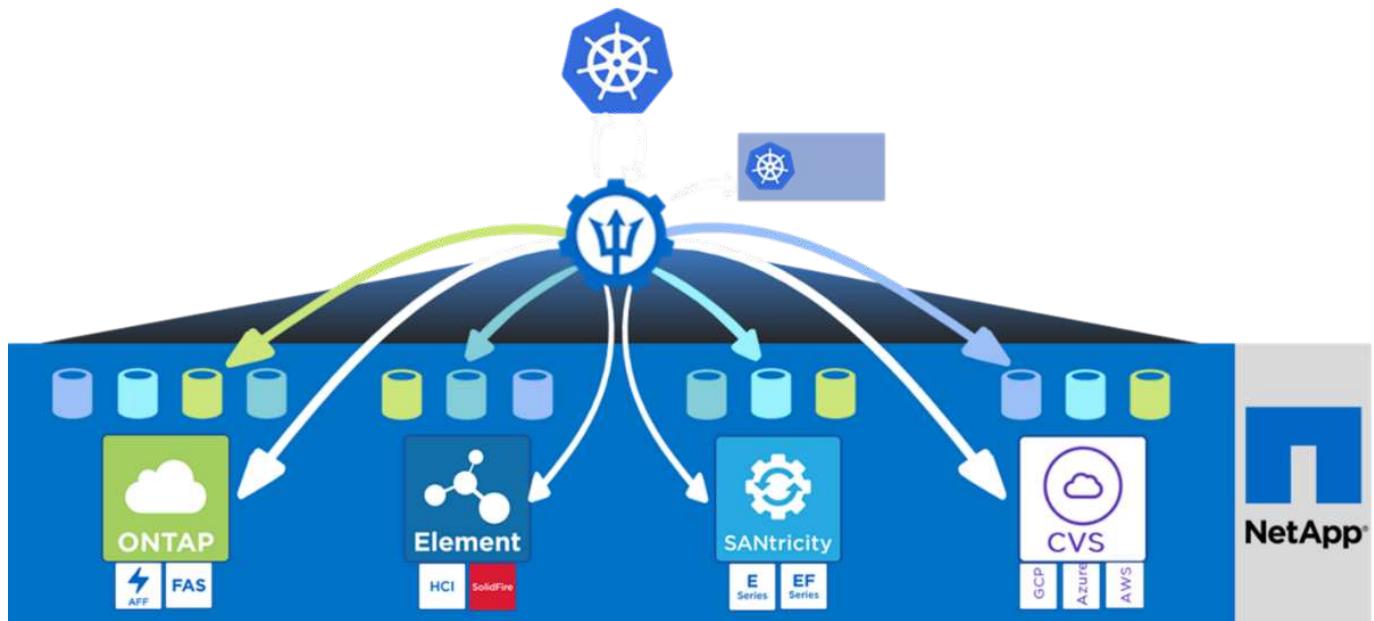
If programming is not appropriate for your situation and you would like to use a configuration management tool, you can clone and run the Ansible playbooks that NetApp publishes [here](#).

[Next: Use-case Validations: DevOps with NetApp Astra](#)

#### **Astra Trident Overview**

Astra Trident is an open-source and fully supported storage orchestrator for containers and Kubernetes distributions like Red Hat OpenShift, VMware Tanzu, Anthos by Google Cloud, Rancher etc. Trident works with the entire NetApp storage portfolio, including the NetApp ONTAP and Element storage systems, and it also supports NFS and iSCSI connections. Trident accelerates the DevOps workflow by allowing end users to provision and manage storage from their NetApp storage systems without requiring intervention from a storage administrator.

An administrator can configure a number of storage backends based on project needs and storage system models that enable advanced storage features, including compression, specific disk types, or QoS levels that guarantee a certain level of performance. After they are defined, these backends can be used by developers in their projects to create persistent volume claims (PVCs) and to attach persistent storage to their containers on demand.



Astra Trident has a rapid development cycle and, like Kubernetes, is released four times a year.

The latest version of Astra Trident is 22.01 released in January 2022. A support matrix for what version of Trident has been tested with which Kubernetes distribution can be found [here](#).

Starting with the 20.04 release, Trident setup is performed by the Trident operator. The operator makes large scale deployments easier and provides additional support, including self healing for pods that are deployed as a part of the Trident install.

With the 21.01 release, a Helm chart was made available to ease the installation of the Trident Operator.

Refer to the documentation [here](#) to install and use Astra Trident.

[Next: Use-case Validations: DevOps with NetApp Astra.](#)

## Use-case validation: DevOps with NetApp Astra

The following use cases have been validated for DevOps with NetApp Astra:

- Integrate Protection into CI/CD Pipelines with NetApp Astra Control
- Leverage Astra Control to facilitate Post-mortem Analysis and Restore the Application
- Accelerating Software Development with NetApp FlexClones

[Next: Videos and Demos - DevOps with NetApp Astra.](#)

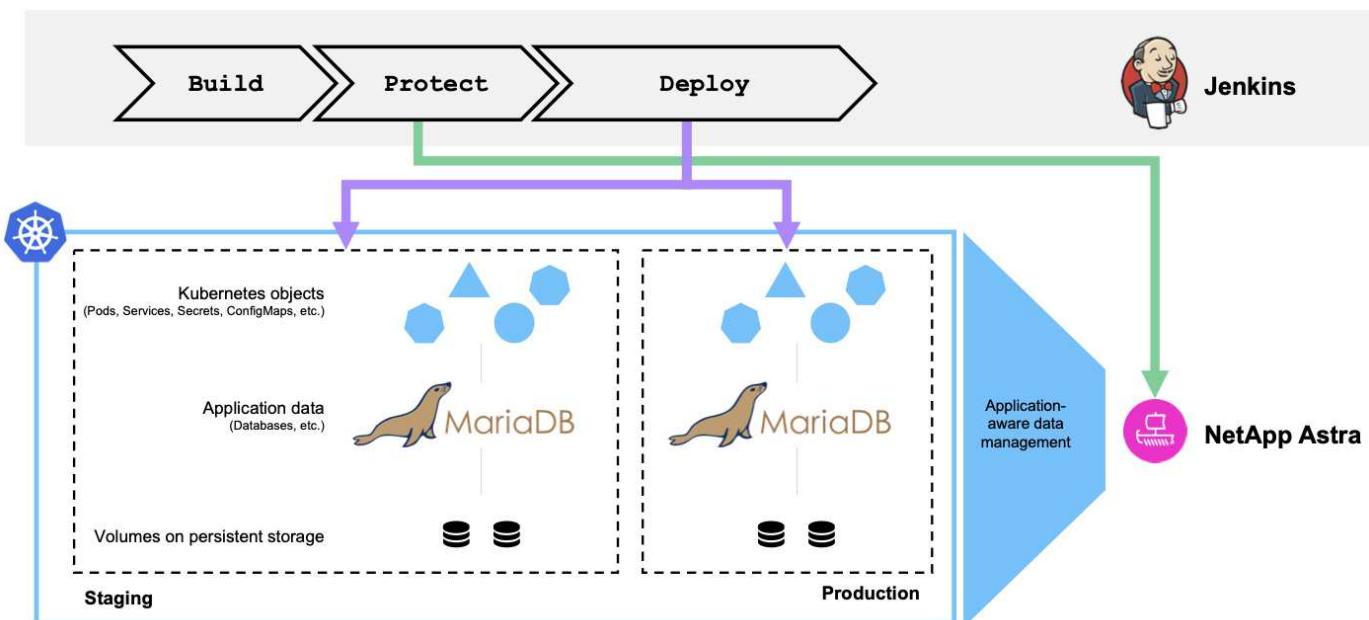
### Integrate Protection into CI/CD Pipelines with NetApp Astra Control

#### Overview

One of the most common uses of DevOps workflows is continuous integration and continuous deployment (CI/CD) pipelines that build, integrate, and run automated test suites on applications as developers commit new code. DevOps engineers and site-reliability engineers (SREs) typically have pipelines dedicated to the various workflows for new feature development, regression testing, bug fixes, quality engineering, and other functions in the development process.

As teams increase their level of automation, the pace of change for in-production applications can feel overwhelming. Therefore, some teams prefer to protect in-production applications or services. In addition to protecting the code and container images, they also want to protect the application state, configuration data (such as Kubernetes objects and resources associated with the application), and an application's persistent data.

In this use case, we take a closer look at a promotion-to-production pipeline that deploys a new version of an application: first into a staging environment and then into a production environment. This example applies equally to the major public clouds and also to an on-premises environment. Although we show the deployment of one version of the app, the pipeline can also be used with other strategies, such as blue/green or canary deployment. As part of the CI/CD pipeline, we're going to protect the application by creating a complete application backup. An application-aware backup of the in-production application and its data, state, and configuration can be useful for numerous DevOps workflows.



The application used for validating this use-case was [Magento](#), an e-commerce solution with a web-based front end; an Elasticsearch instance for search and analysis features; and a MariaDB database that tracks all the shopping inventory and transaction details. This containerized application was installed in a Red Hat OpenShift cluster. Every pod in the application used persistent volumes to store data. The persistent volumes were automatically created by NetApp Astra Trident, the Container Storage Interface-compliant storage orchestrator for Kubernetes that enables storage to be provisioned on NetApp storage systems. Further, to utilize the Astra Control Center's application protection capabilities, the application in question was managed by Astra Control, which was then used to trigger application backups that stored the state of the application along with the data held in persistent volumes. We used the [NetApp Astra Control Python SDK](#) to automate the process of triggering application backups, which was then introduced into a CI/CD pipeline. This pipeline was created and executed using a popular CI/CD tool called [[Jenkins](#)] to automate the flow to build, protect, and deploy the application.

Let us run through the prerequisites and procedure to introduce protection in a CI/CD pipeline.

#### Use-case validation prerequisites

The following tools or platforms were deployed and configured as prerequisites:

1. Red Hat OpenShift Container Platform
2. NetApp Astra Trident installed on OpenShift with a backend to NetApp ONTAP system configured

3. A default storageclass configured, pointing to a NetApp ONTAP backend
4. NetApp Astra Control Center installed on an OpenShift cluster
5. OpenShift cluster added as a managed cluster to Astra Control Center
6. Jenkins installed on an OpenShift cluster and configured with an agent node with a Docker engine installed on it

### Installing the application

Let's start with the initial installation of the application in the staging and production environments. For the purpose of this use case, this step is a prerequisite, so it is performed manually. The CI/CD pipeline is used for subsequent build and deploy workflows as a result of new version releases of the application.

The production environment in this use case is a namespace called `magento-prod`, and the corresponding staging environment is a namespace called `magento-staging` configured on the Red Hat OpenShift cluster. To install the application, complete the following steps:

1. Install the Magento application using bitnami helm chart on the production environment. We use RWX PVs for Magento and Mariadb pods.

```
[netapp-user@rhel7 na_astra_control_suite]$ helm install --version 14
magento bitnami/magento -n magento-prod --create-namespace --set
image.tag=2.4.1-debian-10-
r11,magentoHost=10.63.172.243,persistence.magento.accessMode=ReadWriteMa
ny,persistence.apache.accessMode=ReadWriteMany,mariadb.master.persistence.accessModes[0]=ReadWriteMany
```



Magento bitnami helm chart requires a LoadBalancer service to expose the Magento GUI service. We used [MetalLB](#) for providing an on-prem load balancer service in this example.

2. After a few minutes, verify that all pods and services are running.

```
[netapp-user@rhel7 na_astra_control_suite]$ oc get pods -n magento-prod
NAME                                         READY   STATUS
RESTARTS   AGE
magento-9d658fd96-qrxmt                     1/1    Running
0          49m
magento-elasticsearch-coordinating-only-69869cc5-768rm 1/1    Running
0          49m
magento-elasticsearch-data-0                  1/1    Running
0          49m
magento-elasticsearch-master-0                1/1    Running
0          49m
magento-mariadb-0                           1/1    Running
0          49m
```

3. Repeat the same procedure for the staging environment.

## Manage the Magento application in Astra Control Center

1. Navigate to Applications and select the Discovered applications tab.
2. Click the ellipsis against the Magento application in the production environment (`magento-prod`), and click Manage.
3. The Magento application is now managed by the Astra Control Center. All operations supported by Astra Control can be performed on the application. Note the version of the application as well.

The screenshot shows the Astra Control Center interface for managing the 'magento-prod' application. At the top, there's a header with the application name and a status indicator showing 'Available'. Below the header, there are two main sections: 'App status' and 'App protection status'. The 'App status' section indicates the application is 'Healthy'. The 'App protection status' section shows it is 'Partially Protected'. Further down, there are details about the application's images, protection schedule, group, and cluster. The images listed are docker.io/bitnami/elasticsearch:6.8.10-debian-10-r16, docker.io/bitnami/magento:2.4.1-debian-10-r11, and docker.io/bitnami/mariadb:10.3.23-debian-10-r38. The protection schedule is set to 'Disabled'. The application belongs to the 'magento-prod' group and is part of the 'ocp-vmw' cluster.

4. Repeat the steps for managing the Magento application in the staging environment (`magento-staging`).

## CI/CD pipeline with integrated protection

When we work with new versions of applications, we use a CI/CD pipeline to build the container image, take backups of both the staging and production environments, deploy the new version of the application to the staging environment, wait for approval to promotion to production, and then deploy the new version of the application to the production environment. To use a CI/CD pipeline, complete the following steps:

1. Log into Jenkins, and create the required credentials: one for Magento creds, one for Mariadb admin creds, and the third for Mariadb root creds.
2. Navigate to Manage Jenkins > Manage Credentials and click the appropriate domain.
3. Click Add Credentials, and set the kind to Username with password and scope set to Global. Enter the username, password, and an ID for the credentials and click OK.

The screenshot shows the Jenkins Manage Credentials screen. The user is adding a new global credential of type 'Username with password'. The 'Scope' is set to 'Global (Jenkins, nodes, items, all child items, etc)'. The 'Username' field contains 'admin', and the 'Password' field contains a masked value. The 'ID' field is set to 'magento-cred'. There is also a 'Description' field which is currently empty. At the bottom of the form is a blue 'OK' button.

4. Repeat the same procedure for the other two credentials.

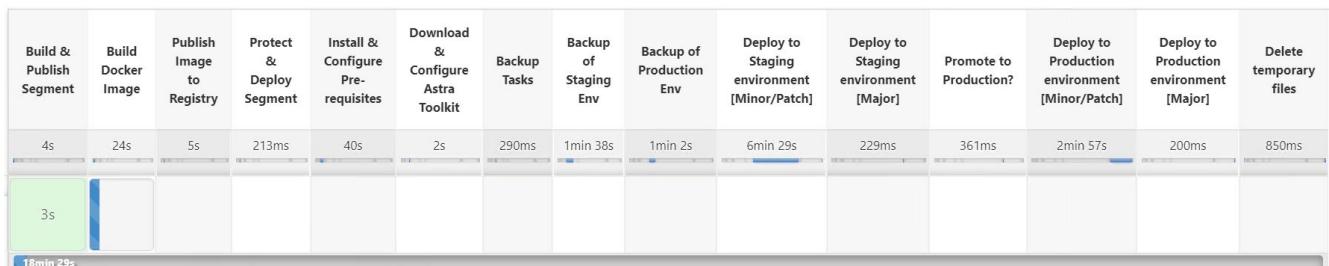
5. Go back to the Dashboard, create a pipeline by clicking New Item, and then click Pipeline.
6. Copy the pipeline from the Jenkinsfile [here](#).
7. Paste the pipeline into the Jenkins pipeline section and then click Save.
8. Fill the parameters of the Jenkins pipeline with the respective details including the helm chart version, the Magento application version to be upgraded to, the Astra toolkit version, the Astra Control Center FQDN, the API token, and its instance ID. Specify the docker registry, namespace, and Magento IP of both production and staging environments, and also specify the credential IDs of the credentials created.

```

MAGENTO_VERSION = '2.4.1-debian-10-r14'
CHART_VERSION = '14'
RELEASE_TYPE = 'MINOR'
ASTRA_TOOLKIT_VERSION = '2.0.2'
ASTRA_API_TOKEN = 'xxxxxxxxx'
ASTRA_INSTANCE_ID = 'xxx-xxx-xxx-xxx-xxx'
ASTRA_FQDN = 'netapp-astra-control-center.org.example.com'
DOCKER_REGISTRY = 'docker.io/netapp-solutions-cicd'
PROD_NAMESPACE = 'magento-prod'
PROD_MAGENTO_IP = 'x.x.x.x'
STAGING_NAMESPACE = 'magento-staging'
STAGING_MAGENTO_IP = 'x.x.x.x'
MAGENTO_CREDS = credentials('magento-cred')
MAGENTO_MARIADB_CREDS = credentials('magento-mariadb-cred')
MAGENTO_MARIADB_ROOT_CREDS = credentials('magento-mariadb-root-cred')

```

9. Click Build Now. The pipeline starts executing and progresses through the steps. The application image is first built and uploaded to the container registry.



10. The application backups are initiated via Astra Control.

App status: Healthy

Protection schedule: Disabled

Group: magento-prod

Cluster: ocp-vmw

Overview Data protection Storage Resources Activity

Actions Configure protection policy Search

Name	Ready	On-Schedule/On-Demand	Created	Actions
upgrade-prod-2-4-1-debian-10-r20	🕒	🕒 On-Demand	2021/10/29 14:43 UTC	Running

11. After the backup stages have completed successful, verify the backups from the Astra Control Center.

App status: Healthy

Protection schedule: Disabled

Group: magento-prod

Cluster: ocp-vmw

Overview Data protection Storage Resources Activity

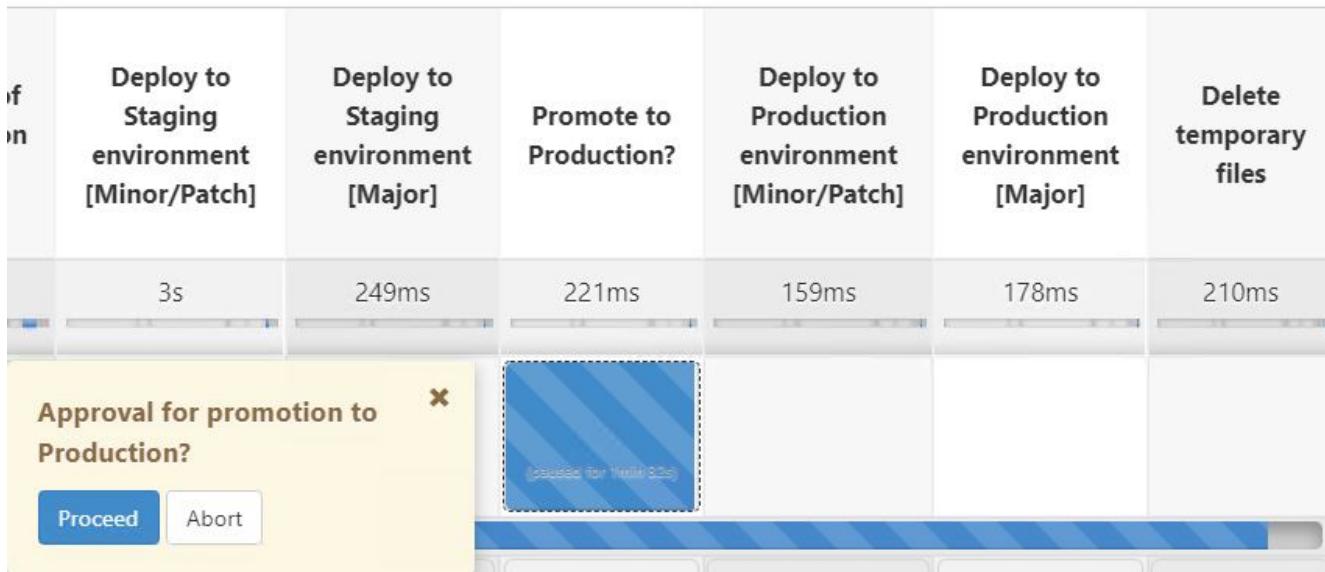
Actions Configure protection policy Search

Name	Ready	On-Schedule/On-Demand	Created	Actions
upgrade-prod-2-4-1-debian-10-r20	🕒	🕒 On-Demand	2021/10/29 14:43 UTC	Available

12. The new version of the application is then deployed to the staging environment.



13. After this step is completed, the program waits for the user to approve deployment to production. At this stage, assume that the QA team performs some manual testing and approves production. You can then click Approve to deploy the new version of the application to the production environment.



14. Verify that the production application is also upgraded to the desired version.

As part of the CI/CD pipeline, we demonstrated the ability to protect the application by creating a complete application-aware backup. Because the entire application has been backed up as part of the promotion-to-production pipeline, you can feel more confident about highly automated application deployments. This application-aware backup containing the data, state, and configuration of the application can be useful for numerous DevOps workflows. One important workflow would be to roll back to the previous version of the application in case of unforeseen issues.

Although we demonstrated a CI/CD workflow through with Jenkins tool, the concept can easily and efficiently be extrapolated to different tools and strategies. To see this use case in action, watch the video [here](#).

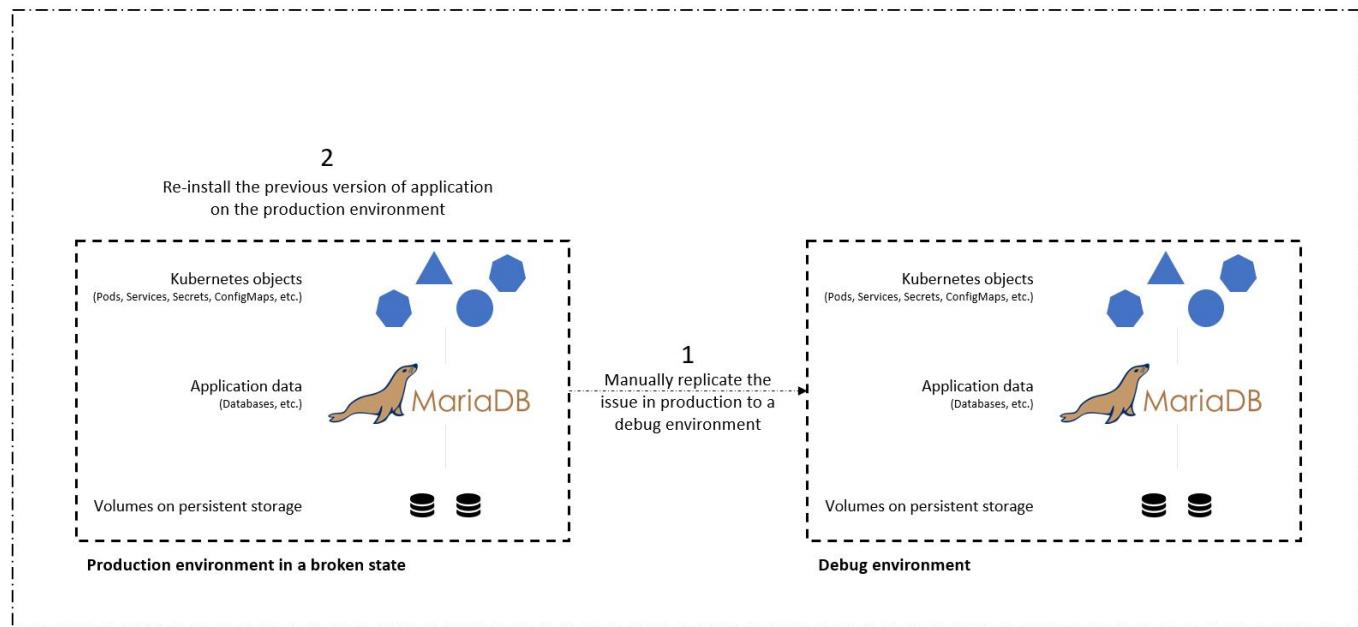
Next: [Videos and Demos - DevOps with NetApp Astra](#).

## Use Astra Control to facilitate post-mortem analysis and restore the application

### Overview

In the [first use case](#), we demonstrated how to use NetApp Astra Control Center to protect your applications in Kubernetes. That section describes how to integrate application backups via Astra Control directly into your development workflow by using the Python SDK in the NetApp Astra toolkit. This approach allows for the protection of development and production environments by automating on-demand backups during the continuous integration and continuous deployment (CI/CD) process. With this extra layer of application-consistent data protection added to the CI/CD pipeline and the production applications, the development processes is safe if something goes wrong in the process, which promotes good business-continuity practices.

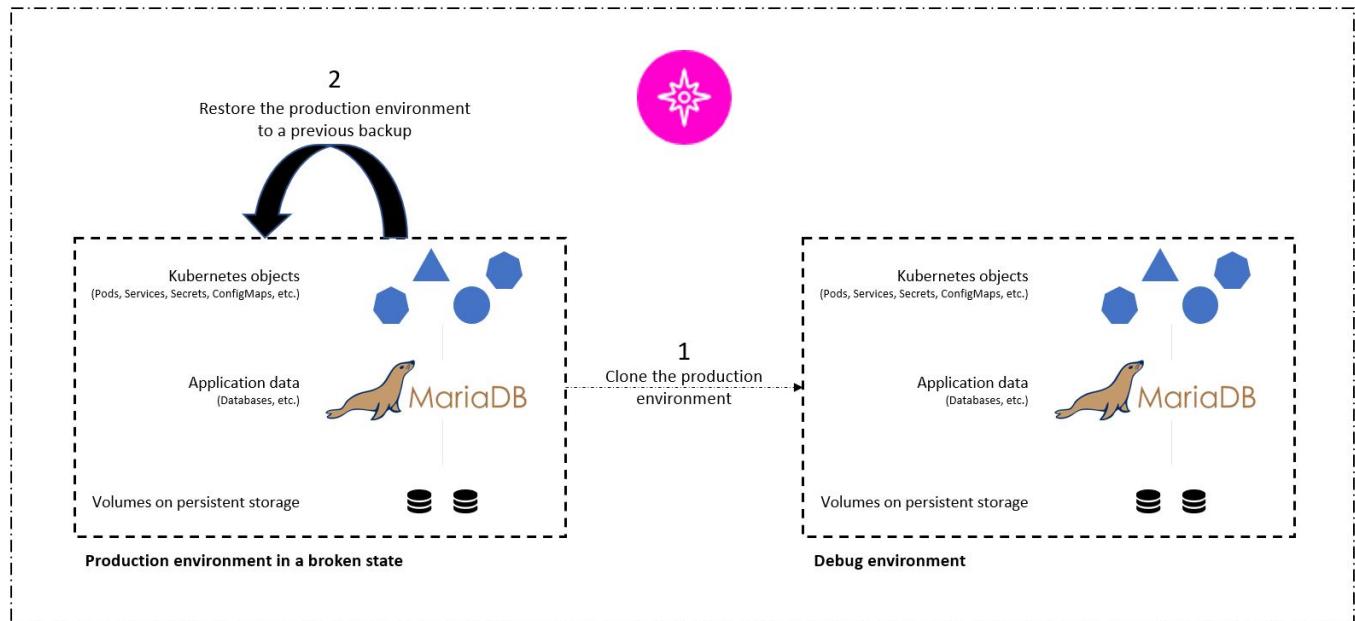
In a traditional workflow, after encountering a failure when the application is upgraded to a new version, the development team would attempt to troubleshoot the issue in real time based on bug reports being provided by customers. Alternatively, at the first sign of trouble, the team could attempt to redeploy the application to a parallel debugging environment to take that process offline. They could redeploy an older code base from a previous version into production, which would restore the application to working order.



Although this approach works, the team would have to make sure that the state of the broken production app matched that of the version seen in production when the issues occurred. They would also have to spend time promoting the known-good build into production by fetching code from their repository and redeploying the machine images to restore the application to a good running state. Also, in this scenario, we didn't consider whether the production database itself was corrupted by the faulty code. Ideally, there are separate backup processes in place for the database data, but must we assume that they're consistent with the state of the application as it was published? This is where the benefits of stateful and application-consistent backups, restores and clones with Astra Control really show their value.

First, we can use Astra Control to facilitate post-mortem analysis on the state of the application. We do this by cloning the buggy production version to a parallel testing environment in an application-consistent manner. Having this environment set aside in its bug-ridden state enable us to troubleshoot the problem in real time.

Furthermore, Astra Control supports the in-place restore capability that allows us to restore the production application to a last acceptable backup (that preceded the afflicted version of code). The restored version assumes the position of the previous, buggy production application, in an application-consistent and stateful manner, including the ingress IP previously assigned. As a result, customers accessing the front end would be unaware of the transition to the backup version.



### Use-case validation prerequisites

The following tools or platforms were deployed and configured as prerequisites:

- Red Hat OpenShift Container Platform.
- NetApp Astra Trident installed on OpenShift with a backend configured to a NetApp ONTAP system.
- A default storageclass configured, pointing to a NetApp ONTAP backend.
- NetApp Astra Control Center installed on an OpenShift cluster.
- OpenShift cluster added as a managed cluster to Astra Control Center.
- Jenkins installed on an OpenShift cluster.
- Magento application installed in the production environment. The production environment in this use case is a namespace called 'magento-prod' in a Red Hat OpenShift cluster.
- Production application managed by Astra Control Center.
- Known-good backup(s) of the production application captured with Astra Control.

### Clone and restore pipeline

Considering that the application has been upgraded to a new version, the application in the production environment (`magento-prod`) isn't behaving as intended after the upgrade. Let's assume that the data being returned by front-end queries doesn't match the request or that the database has in fact been corrupted. To clone and restore the pipeline, complete the following steps:



## This site can't be reached

10.63.172.243 took too long to respond.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)
- [Running Windows Network Diagnostics](#)

ERR\_CONNECTION\_TIMED\_OUT

[Reload](#)

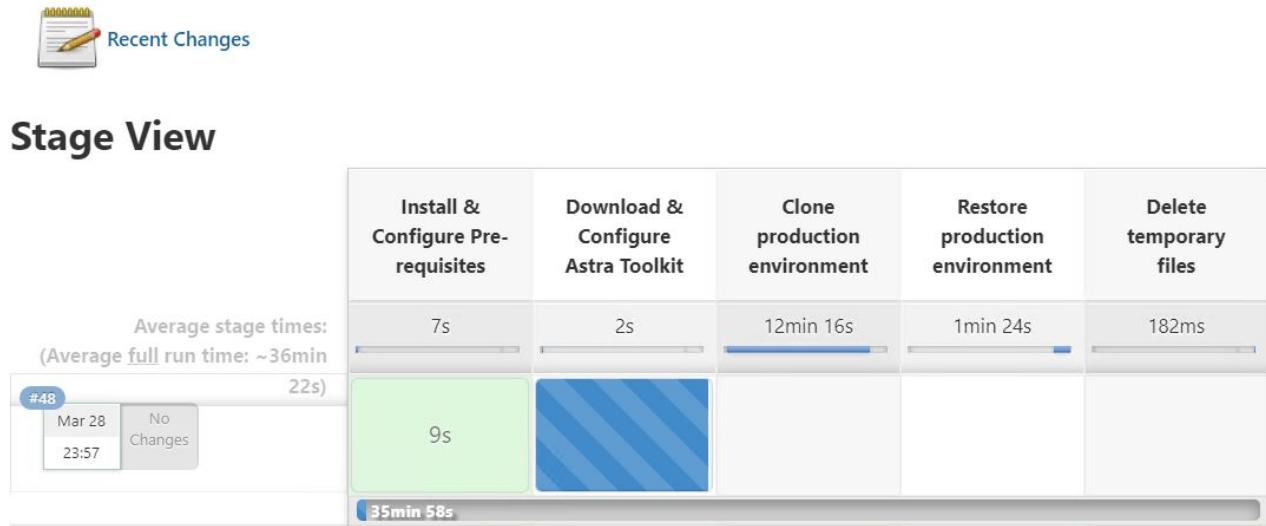
[Details](#)

1. Log into Jenkins and create a pipeline by clicking New Item and then Pipeline.
2. Copy the pipeline from the Jenkinsfile [here](#).
3. Paste the pipeline into the Jenkins pipeline section and then click Save.
4. Fill the parameters of the Jenkins pipeline with the respective details like the current Magento application version in production, the Astra Control Center FQDN, the API token, the instance ID and application name or namespace of production and debug environments, and the source and destination cluster names. For the purpose of this use case, the production environment is a namespace called 'magento-prod' and the debug environment is a namespace called 'magento-debug' configured on a Red Hat OpenShift cluster.

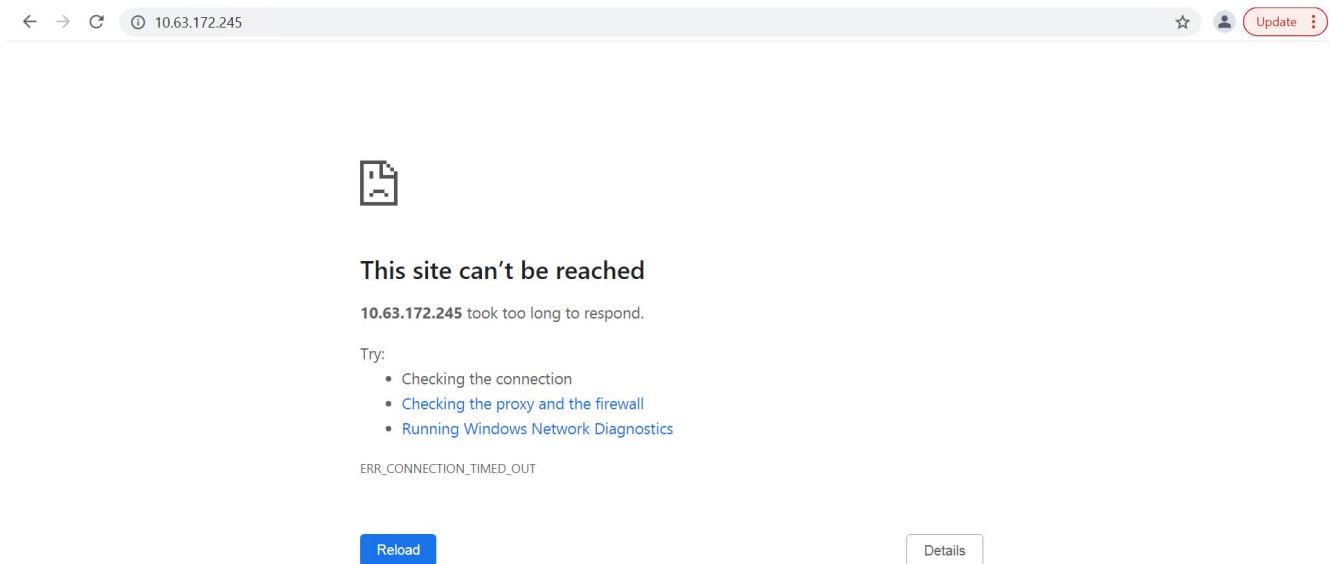
```
MAGENTO_VERSION = '2.4.1-debian-10-r14'  
ASTRA_TOOLKIT_VERSION = '2.0.2'  
ASTRA_API_TOKEN = 'xxxxxx'  
ASTRA_INSTANCE_ID = 'xxx-xxx-xxx-xxx-xxx'  
ASTRA_FQDN = 'netapp-astra-control-center.org.example.com'  
PROD_APP_NAME = 'magento-prod'  
DEBUG_APP_NAME = 'magento-debug'  
DEBUG_NAMESPACE = 'magento-debug'  
PROD_KUBERNETES_CLUSTER = 'ocp-vmw'  
DEBUG_KUBERNETES_CLUSTER = 'ocp-vmw'
```

5. Click Build Now. The pipeline starts executing and progresses through the steps. The application is first cloned in the current state to a debug environment, and the application is then restored to the known-working backup.

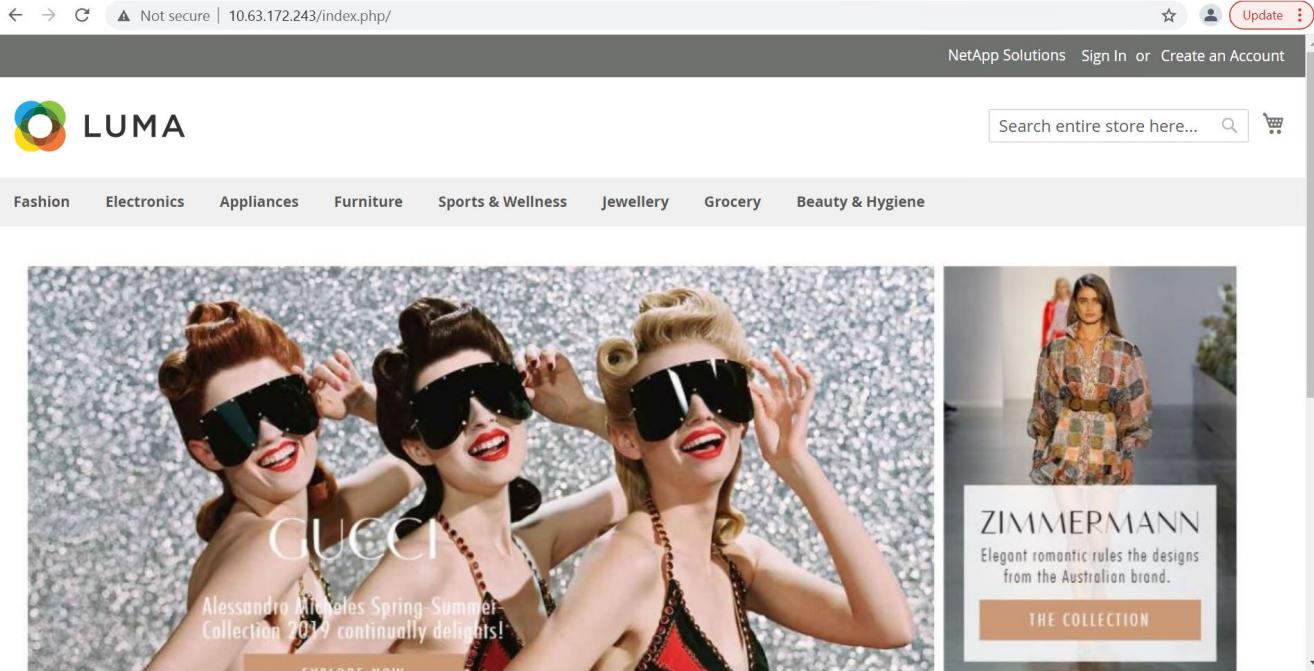
# Pipeline magento\_clone-for-triage\_restore-from-backup



6. Verify that the cloned application is the bug-containing version.



7. Verify that the production environment is restored to a working backup, and the application in production works as expected.



These two operations in tandem expedite the return to normal business operations. To see this use case in action, watch the video [here](#).

Next: Videos and Demos - DevOps with NetApp Astra.

## Accelerating software development with NetApp FlexClone technology

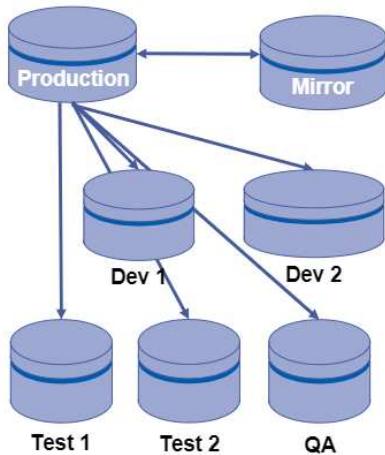
### Overview

Cloning a deployed application in a Kubernetes cluster is a very useful tool for developers that would like to expedite their workflows by sharing environments with partners or by testing new versions of code in a development environment without interfering with the version they are currently working on. The stateful and application-consistent cloning of a Kubernetes application is a major feature included with NetApp Astra Control, alongside the backup and restore of applications. As a bonus, if an application is cloned within the same Kubernetes cluster using the same storage backend, Astra Control defaults to using NetApp FlexClone technology for the duplication of persistent data volumes, speeding up the process significantly. By accelerating this process, the cloned environment is provisioned and available for use in a few moments, allowing developers to resume their work with just a brief pause when compared to redeploying their test or development environment. As an additional convenience, all of the functions available in NetApp Astra Control can be called with an API, which allows for easy integration into automation frameworks like Ansible. Therefore, environments can be staged even more rapidly because only minor changes are needed in a playbook or role to begin the cloning procedure.

### What is NetApp FlexClone technology?

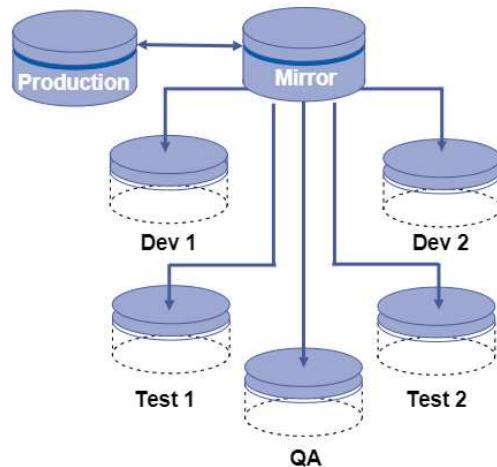
NetApp FlexClone technology is a writeable, point-in-time snapshot-based copy of a NetApp FlexVol. They are provisioned almost instantly, contain all of the data from the source volume, and consume no additional storage space until the data in the new volume begins to diverge from the source. They are often used in development or template-based environments when multiple copies of data are useful for staging purposes and storage systems have limited resources for provisioning these volumes. Compared to a traditional storage system in which data must be copied multiple times resulting in the consumption of significant storage space and time, NetApp FlexClone technology accelerates storage-dependant tasks.

## Traditional Data Copies



Traditional physical copies take additional time and consume additional storage space

## NetApp FlexClone Copies



NetApp FlexClone copies are near instantaneous and only consume space when written to

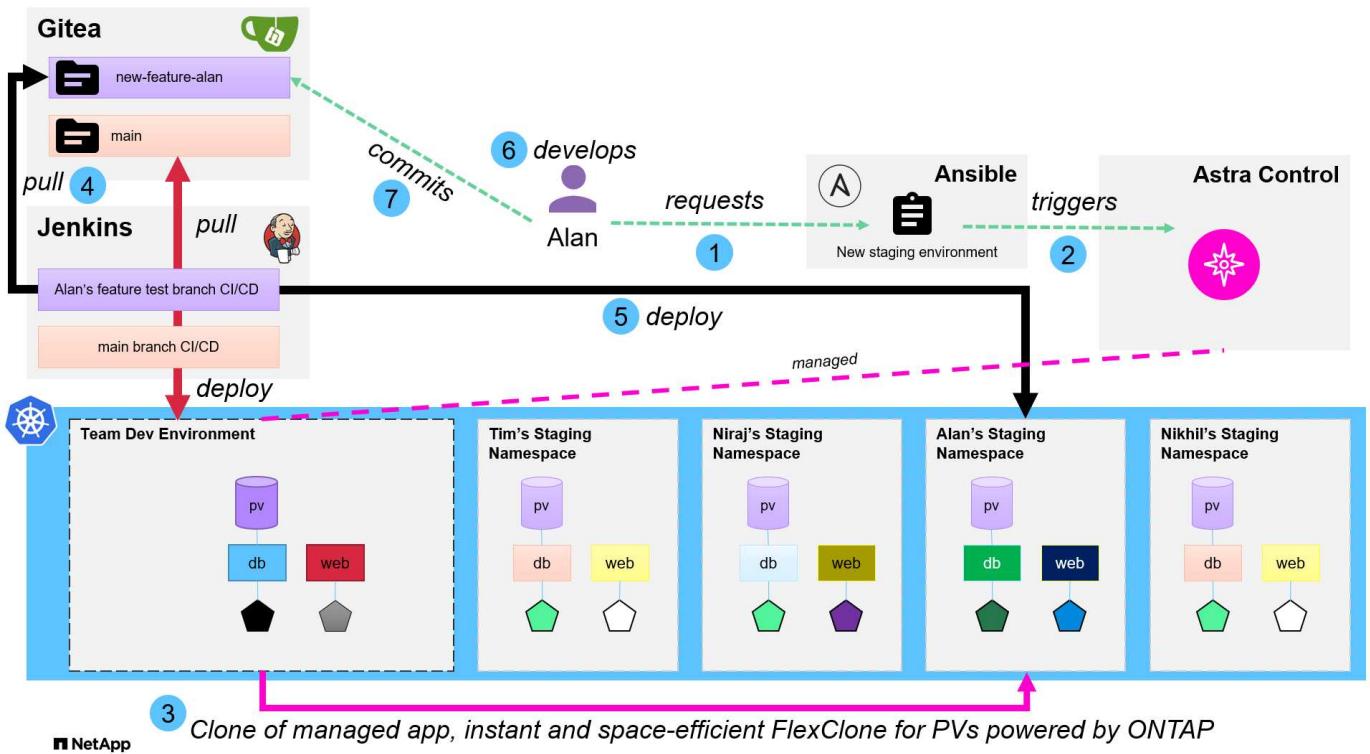
To find out more about NetApp FlexClone technology, visit the page on [NetApp Docs](#).

### Prerequisites

1. A supported Kubernetes Distribution, such as Red Hat OpenShift 4.6.8+, Rancher 2.5+, or Kubernetes 1.19+.
2. NetApp Astra Control Center 21.12+.
3. A NetApp ONTAP system with a storage backend configured through NetApp Astra Trident.
4. Ansible 2.9+.
5. Templates for the environments that you'd like to clone as managed applications in NetApp Astra Control.

### Use-case introduction

For this use case, we visualize something similar to the following workflow:



1. A user runs the ansible playbook to create a new staging environment.
2. Ansible uses the URI-API module to call out to Astra Control to execute the cloning operation.
3. Astra Control executes a cloning operation on a preprovisioned template environment, thus creating a new managed application.



This environment can be a single standalone application in development or an entire development environment like a Jenkins CI/CD pipeline.

4. The user then pulls a version of their code into the cloned dev environment from an online repository like Gitea.
5. The new version of the application is deployed and managed by NetApp Astra Control.



Both of these processes can be automated.

6. The user can develop new code in this cloned environment.
7. When the user is satisfied with their development efforts, they can push the code back to the hosted repository.

The use case presented here depends on the existence of golden templates for the particular environments or applications you would like to clone. In our environment we have created three such templates, one for a Wordpress deployment, one for a Magento deployment, and one for a Jenkins CI/CD environment with Gitea that we have titled DevTools.

The screenshot shows the HCG Solutions application management interface. On the left, there's a sidebar with various icons: a house, a circular arrow, a cube, a server, a person, and a document. The main area is titled "Applications". It has a toolbar with "Actions", "Define", a search bar, and a star icon. Below is a table with columns: Name, Ready, Protected, Cluster, Group, and Actions. There are three entries:

Name	Ready	Protected	Cluster	Group	Actions
<a href="#">devtools-template</a>	✓	ⓘ	ocp-vmware2	devtools-template	Available
<a href="#">magento-template</a>	✓	ⓘ	ocp-vmware2	magento-template	Available
<a href="#">wordpress-template</a>	✓	ⓘ	ocp-vmware2	wordpress-template	Available

Each of these environments is managed by NetApp Astra control, with persistent volumes currently stored on a NetApp ONTAP storage system with an NFS backend provided by NetApp Astra Trident.

#### Use-case validation

- Clone the ansible toolkit provided by the NetApp Solutions Engineering team, which includes the cloning role and the application update playbook.

```
[netapp-user@rhel7 ~]$ git clone https://github.com/NetApp-Automation/na_astra_control_suite.git
[netapp-user@rhel7 ~]$ cd na_astra_control_suite
```

- Edit `vars/clone_vars.yml` and fill in the global values that fit your Astra Control environment.

```
astra_control_fqdn: astra-control-center.example.com
astra_control_account_id: "xxxx-xxxx-xxxx-xxxx-xxxx"
astra_control_api_token: "xxxxxx"
```



The global environment values you need to fill out are available under the user profile icon in NetApp Astra Control under the API Access menu.

The screenshot shows the 'API access' page in the HCG Solutions section of NetApp Astra Control. At the top, there is a 'API documentation' link to <https://astra-control-center.cie.netapp.com>. To the right, the 'Account ID' is listed as fa9214eb-670d-41f1-bfcf-34cb3b69fda1. On the far right, there is a user profile icon with a red circle around it, indicating notifications. Below the header, the 'API tokens' section is visible. It includes a 'Generate API token' button and a table with columns for 'Token name' (checkbox), 'Created' (sort arrow), and 'Actions'. A large key icon is centered in the middle of the table area, accompanied by the text: 'You don't have any API token(s) right now. When you have created one, it will be listed here.' A blue 'Generate new API token' button is located at the bottom of the table section.

- With the global variables completed, you can choose the values for the specific application you wish to clone. To clone the devtools environment to a personal environment called alan-devtools, you would do the following:

```
clone_details:  
  - clone_name: alan-devtools  
    destination_namespace: alan-dev-namespace  
    source_cluster_name: ocp-vmware2  
    destination_cluster_name: ocp-vmware2  
    source_application_name: devtools-template
```



To take advantage of NetApp FlexClone technology in the cloning process, src-cluster and dest-cluster must be the same.

- You can now execute the playbook to clone the application.

```
[netapp-user@rhel7 na_astra_control_suite]$ ansible-playbook -K  
clone_app_playbook.yml]
```



The playbook as written must be run by the root user or someone that can escalate through the sudo process by passing the "-K" argument.

- When the playbook completes its run, the cloned application shows as available in the Astra Control Center console.

Name	Ready	Protected	Cluster	Group	Actions
alans-devtools	✓	⚠	ocp-vmware2	alans-dev-namespace	Available
devtools-template	✓	ⓘ	ocp-vmware2	devtools-template	Available
magento-template	✓	ⓘ	ocp-vmware2	magento-template	Available
wordpress-template	✓	ⓘ	ocp-vmware2	wordpress-template	Available

- A user can then log into the Kubernetes environment where the application was deployed, verify that the application is exposed with a new IP address, and start their development work.

For a demonstration of this use case and a example of upgrading an application, see [here](#).

Next: [Videos and Demos - DevOps with NetApp Astra](#).

## Videos and demos: DevOps with NetApp Astra

The following videos demonstrate some of the capabilities described in this document:

- [Video: Integrate Data Protection in CI/CD pipeline with Astra Control](#)
- [Video: Leverage NetApp Astra Control to Perform Post-mortem Analysis and Restore Your Application](#)

- Video: Accelerate Software Development with Astra Control and NetApp FlexClone Technology

Next: Additional Information: DevOps with NetApp Astra.

## Additional Information: DevOps with NetApp Astra

To learn more about the information described in this document, review the following websites:

- NetApp Documentation

<https://docs.netapp.com/>

- Astra Trident Documentation

<https://docs.netapp.com/us-en/trident/>

- NetApp Astra Control Center Documentation

<https://docs.netapp.com/us-en/astra-control-center/>

- Ansible Documentation

<https://docs.ansible.com/>

- Red Hat OpenShift Documentation

[https://access.redhat.com/documentation/en-us/openshift\\_container\\_platform/4.8/](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.8/)

- Rancher Documentation

<https://rancher.com/docs/>

- Kubernetes Documentation

<https://kubernetes.io/docs/home/>

## NVA-1160: Red Hat OpenShift with NetApp

Alan Cowles and Nikhil M Kulkarni, NetApp

This reference document provides deployment validation of the Red Hat OpenShift solution, deployed through Installer Provisioned Infrastructure (IPI) in several different data center environments as validated by NetApp. It also details storage integration with NetApp storage systems by making use of the Astra Trident storage orchestrator for the management of persistent storage. Lastly, a number of solution validations and real world use cases are explored and documented.

### Use cases

The Red Hat OpenShift with NetApp solution is architected to deliver exceptional value for customers with the following use cases:

- Easy to deploy and manage Red Hat OpenShift deployed using IPI (Installer Provisioned Infrastructure) on bare metal, Red Hat OpenStack Platform, Red Hat Virtualization, and VMware vSphere.

- Combined power of enterprise container and virtualized workloads with Red Hat OpenShift deployed virtually on OSP, RHV, or vSphere, or on bare metal with OpenShift Virtualization.
- Real world configuration and use cases highlighting the features of Red Hat OpenShift when used with NetApp storage and Astra Trident, the open source storage orchestrator for Kubernetes.

## **Business value**

Enterprises are increasingly adopting DevOps practices to create new products, shorten release cycles, and rapidly add new features. Because of their innate agile nature, containers and microservices play a crucial role in supporting DevOps practices. However, practicing DevOps at a production scale in an enterprise environment presents its own challenges and imposes certain requirements on the underlying infrastructure, such as the following:

- High availability at all layers in the stack
- Ease of deployment procedures
- Non-disruptive operations and upgrades
- API-driven and programmable infrastructure to keep up with microservices agility
- Multitenancy with performance guarantees
- Ability to run virtualized and containerized workloads simultaneously
- Ability to scale infrastructure independently based on workload demands

Red Hat OpenShift with NetApp acknowledges these challenges and presents a solution that helps address each concern by implementing the fully automated deployment of Red Hat OpenShift IPI in the customer's choice of data center environment.

## **Technology overview**

The Red Hat OpenShift with NetApp solution is comprised of the following major components:

### **Red Hat OpenShift Container Platform**

Red Hat OpenShift Container Platform is a fully supported enterprise Kubernetes platform. Red Hat makes several enhancements to open-source Kubernetes to deliver an application platform with all the components fully integrated to build, deploy, and manage containerized applications.

For more information visit the OpenShift website [here](#).

### **NetApp storage systems**

NetApp has several storage systems perfect for enterprise data centers and hybrid cloud deployments. The NetApp portfolio includes NetApp ONTAP, NetApp Element, and NetApp e-Series storage systems, all of which can provide persistent storage for containerized applications.

For more information visit the NetApp website [here](#).

### **NetApp storage integrations**

NetApp Astra Control Center offers a rich set of storage and application-aware data management services for stateful Kubernetes workloads, deployed in an on-prem environment and powered by trusted NetApp data protection technology.

For more information, visit the NetApp Astra website [here](#).

Astra Trident is an open-source and fully-supported storage orchestrator for containers and Kubernetes distributions, including Red Hat OpenShift.

For more information, visit the Astra Trident website [here](#).

## Advanced configuration options

This section is dedicated to customizations that real world users would likely need to perform when deploying this solution into production, such as creating a dedicated private image registry or deploying custom load balancer instances.

## Current support matrix for validated releases

Technology	Purpose	Software version
NetApp ONTAP	Storage	9.8, 9.9.1
NetApp Element	Storage	12.3
NetApp Astra Control Center	Application Aware Data Management	21.12.60
NetApp Astra Trident	Storage Orchestration	22.01.0
Red Hat OpenShift	Container orchestration	4.6 EUS, 4.7, 4.8
Red Hat OpenStack Platform	Private Cloud Infrastructure	16.1
Red Hat Virtualization	Data center virtualization	4.4
VMware vSphere	Data center virtualization	6.7U3

Next: [Red Hat OpenShift Overview](#).

## OpenShift Overview

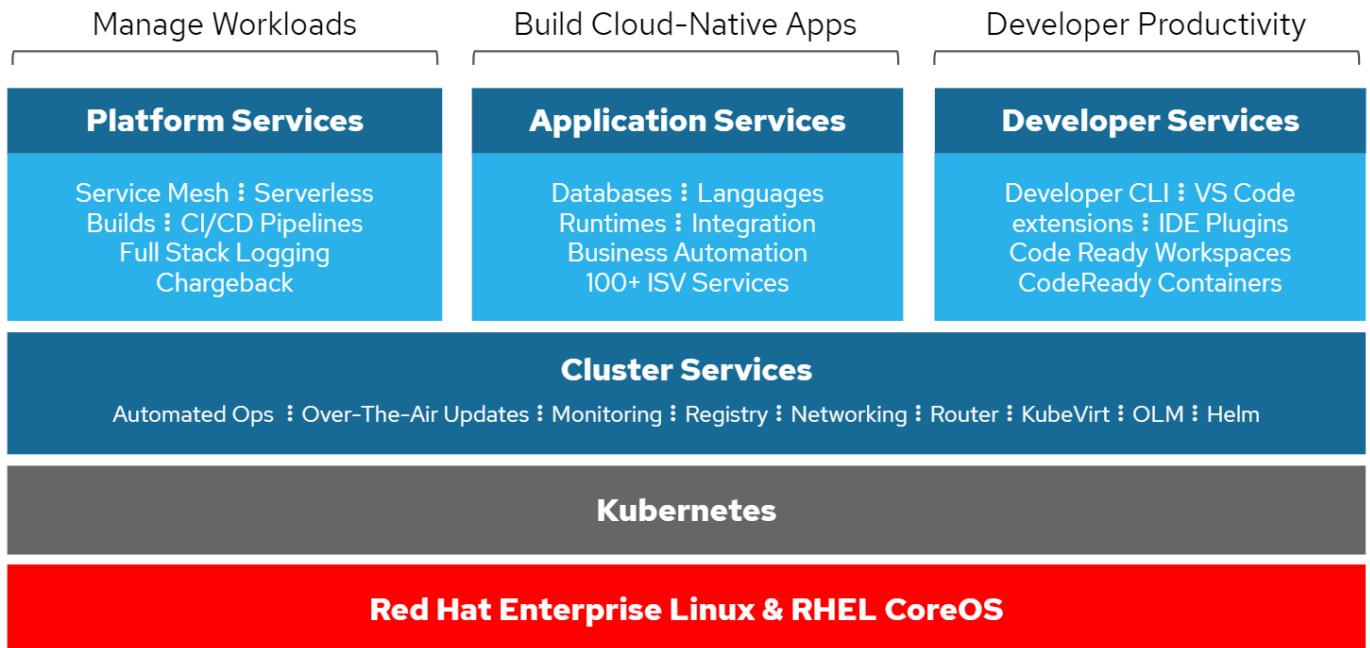
The Red Hat OpenShift Container Platform unites development and IT operations on a single platform to build, deploy, and manage applications consistently across on-premises and hybrid cloud infrastructures. Red Hat OpenShift is built on open-source innovation and industry standards, including Kubernetes and Red Hat Enterprise Linux CoreOS, the world's leading enterprise Linux distribution designed for container-based workloads. OpenShift is part of the Cloud Native Computing Foundation (CNCF) Certified Kubernetes program, providing portability and interoperability of container workloads.

### Red Hat OpenShift provides the following capabilities:

- **Self-service provisioning.** Developers can quickly and easily create applications on demand from the tools that they use most, while operations retain full control over the entire environment.
- **Persistent storage.** By providing support for persistent storage, OpenShift Container Platform allows you to run both stateful applications and cloud-native stateless applications.
- **Continuous integration and continuous development (CI/CD).** This source-code platform manages build and deployment images at scale.
- **Open-source standards.** These standards incorporate the Open Container Initiative (OCI) and Kubernetes for container orchestration, in addition to other open-source technologies. You are not

restricted to the technology or to the business roadmap of a specific vendor.

- **CI/CD pipelines.** OpenShift provides out-of-the-box support for CI/CD pipelines so that development teams can automate every step of the application delivery process and make sure it's executed on every change that is made to the code or configuration of the application.
- **Role-Based Access Control (RBAC).** This feature provides team and user tracking to help organize a large developer group.
- **Automated build and deploy.** OpenShift gives developers the option to build their containerized applications or have the platform build the containers from the application source code or even the binaries. The platform then automates deployment of these applications across the infrastructure based on the characteristic that was defined for the applications. For example, how quantity of resources that should be allocated and where on the infrastructure they should be deployed in order for them to be compliant with third-party licenses.
- **Consistent environments.** OpenShift makes sure that the environment provisioned for developers and across the lifecycle of the application is consistent from the operating system, to libraries, runtime version (for example, Java runtime), and even the application runtime in use (for example, tomcat) in order to remove the risks originated from inconsistent environments.
- **Configuration management.** Configuration and sensitive data management is built in to the platform to make sure that a consistent and environment agnostic application configuration is provided to the application no matter which technologies are used to build the application or which environment it is deployed.
- **Application logs and metrics.** Rapid feedback is an important aspect of application development. OpenShift integrated monitoring and log management provides immediate metrics back to developers in order for them to study how the application is behaving across changes and be able to fix issues as early as possible in the application lifecycle.
- **Security and container catalog.** OpenShift offers multitenancy and protects the user from harmful code execution by using established security with Security-Enhanced Linux (SELinux), CGroups, and Secure Computing Mode (seccomp) to isolate and protect containers. It also provides encryption through TLS certificates for the various subsystems and access to Red Hat certified containers ([access.redhat.com/containers](http://access.redhat.com/containers)) that are scanned and graded with a specific emphasis on security to provide certified, trusted, and secure application containers to end users.



Physical



Virtual



Private cloud



Public cloud



Managed cloud  
(Azure, AWS, IBM, Red Hat)

## Deployment methods for Red Hat OpenShift

Starting with Red Hat OpenShift 4, the deployment methods for OpenShift include manual deployments using User Provisioned Infrastructure (UPI) for highly customized deployments or fully automated deployments using Installer Provisioned Infrastructure (IPI).

The IPI installation method is the preferred method in most cases because it allows for the rapid deployment of OCP clusters for dev, test, and production environments.

### IPI installation of Red Hat OpenShift

The Installer Provisioned Infrastructure (IPI) deployment of OpenShift involves these high-level steps:

1. Visit the Red Hat OpenShift [website](#) and login with your SSO credentials.
2. Select the environment that you would like to deploy Red Hat OpenShift into.

## Install OpenShift Container Platform 4

3. On the next screen download the installer, the unique pull secret, and the CLI tools for management.

4. Follow the [installation instructions](#) provided by Red Hat to deploy to your environment of choice.

**NetApp validated OpenShift deployments**

NetApp has tested and validated the deployment of Red Hat OpenShift in its labs using the Installer Provisioned Infrastructure (IPI) deployment method in each of the following data center environments:

- [OpenShift on Bare Metal](#)
- [OpenShift on Red Hat OpenStack Platform](#)
- [OpenShift on Red Hat Virtualization](#)
- [OpenShift on VMware vSphere](#)

[Next: NetApp Storage Overview.](#)

## OpenShift on Bare Metal

OpenShift on Bare Metal provides an automated deployment of the OpenShift Container Platform on commodity servers.

OpenShift on Bare Metal is similar to virtual deployments of OpenShift, which provide ease of deployment, rapid provisioning, and scaling of OpenShift clusters, while supporting virtualized workloads for applications that are not ready to be containerized. By deploying on bare metal, you do not require the extra overhead necessary to manage the host hypervisor environment in addition to the OpenShift environment. By deploying directly on bare metal servers, you can also reduce the physical overhead limitations of having to share resources between the host and OpenShift environment.

**OpenShift on Bare Metal provides the following features:**

- **IPI or assisted installer deployment.** With an OpenShift cluster deployed by Installer Provisioned Infrastructure (IPI) on bare metal servers, customers can deploy a highly versatile, easily scalable OpenShift environment directly on commodity servers, without the need to manage a hypervisor layer.
- **Compact cluster design.** To minimize the hardware requirements, OpenShift on bare metal allows for users to deploy clusters of just 3 nodes, by enabling the OpenShift control plane nodes to also act as worker nodes and host containers.
- **OpenShift virtualization.** OpenShift can run virtual machines within containers by using OpenShift Virtualization. This container-native virtualization runs the KVM hypervisor inside of a container, and attaches persistent volumes for VM storage.
- **AI/ML-optimized infrastructure.** Deploy applications like Kubeflow for machine learning applications by incorporating GPU-based worker nodes to your OpenShift environment and leveraging OpenShift Advanced Scheduling.

### Network design

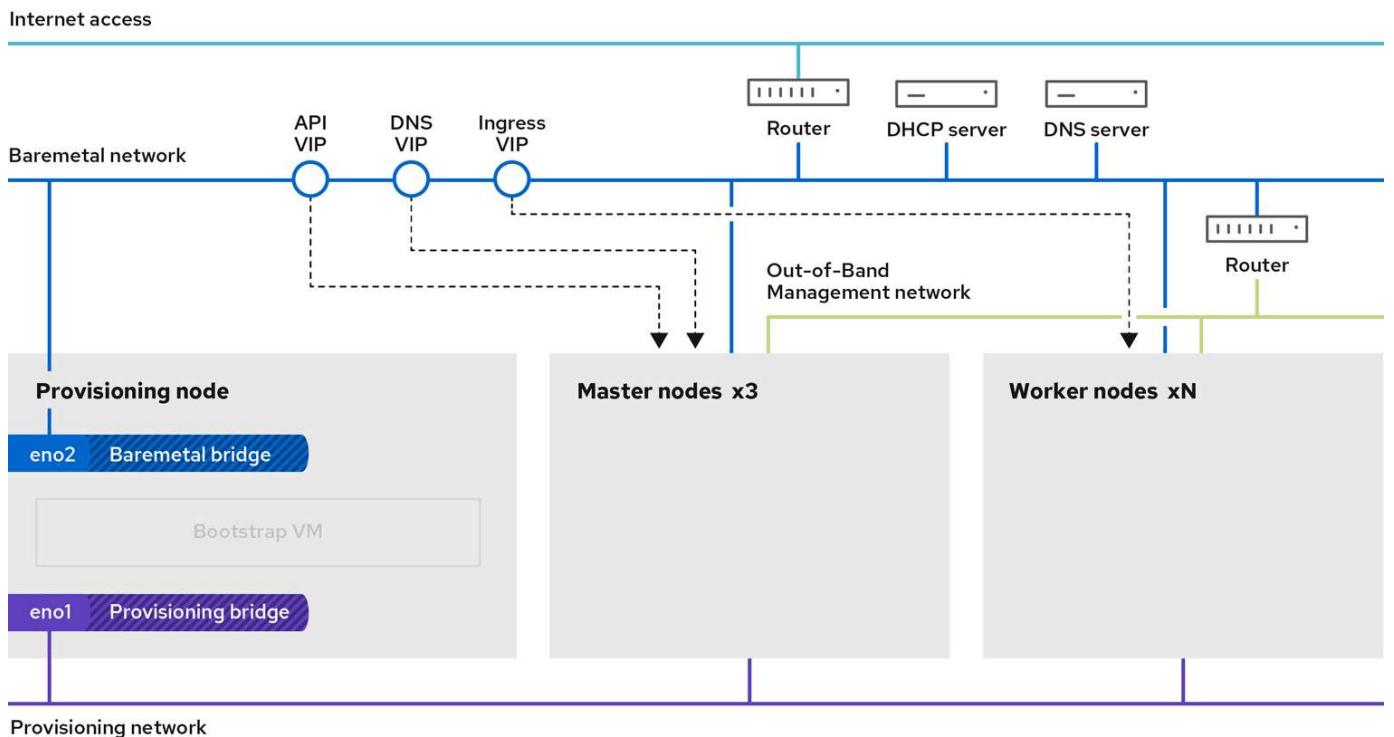
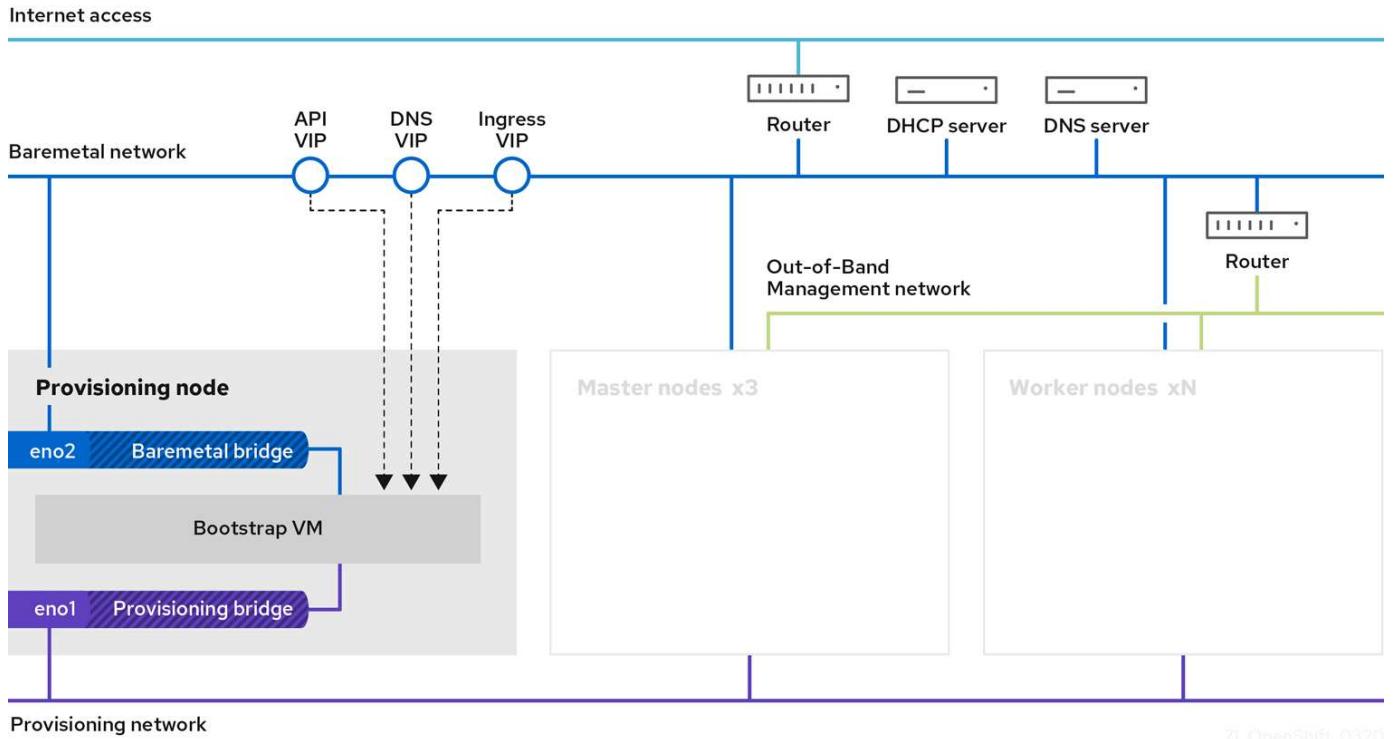
The Red Hat OpenShift on NetApp solution uses two data switches to provide primary data connectivity at 25Gbps. It also uses two management switches that provide connectivity at 1Gbps for in-band management for the storage nodes and out-of-band management for IPMI functionality.

For OpenShift bare-metal IPI deployment, you must create a provisioner node, a Red Hat Enterprise Linux 8 machine that must have network interfaces attached to separate networks.

- **Provisioning network.** This network is used to boot the bare-metal nodes and install the necessary images and packages to deploy the OpenShift cluster.
- **Bare-metal network.** This network is used for public-facing communication of the cluster after it is deployed.

For the setup of the provisioner node, the customer creates bridge interfaces that allow the traffic to route properly on the node itself and on the Bootstrap VM that is provisioned for deployment purposes. After the cluster is deployed, the API and ingress VIP addresses are migrated from the bootstrap node to the newly deployed cluster.

The following images depict the environment both during IPI deployment and after the deployment is complete.



## VLAN requirements

The Red Hat OpenShift with NetApp solution is designed to logically separate network traffic for different purposes by using virtual local area networks (VLANs).

VLANs	Purpose	VLAN ID
Out-of-band management network	Management for bare metal nodes and IPMI	16
Bare-metal network	Network for OpenShift services once cluster is available	181
Provisioning network	Network for PXE boot and installation of bare metal nodes via IPI	3485



Although each of these networks is virtually separated by VLANs, each physical port must be set up in Access Mode with the primary VLAN assigned, because there is no way to pass a VLAN tag during a PXE boot sequence.

## Network infrastructure support resources

The following infrastructure should be in place prior to the deployment of the OpenShift container platform:

- At least one DNS server that provides a full host-name resolution accessible from the in-band management network and the VM network.
- At least one NTP server that is accessible from the in-band management network and the VM network.
- (Optional) Outbound internet connectivity for both the in-band management network and the VM network.

[Next: NetApp storage overview.](#)

## OpenShift on Red Hat OpenStack Platform

The Red Hat OpenStack Platform delivers an integrated foundation to create, deploy, and scale a secure and reliable private OpenStack cloud.

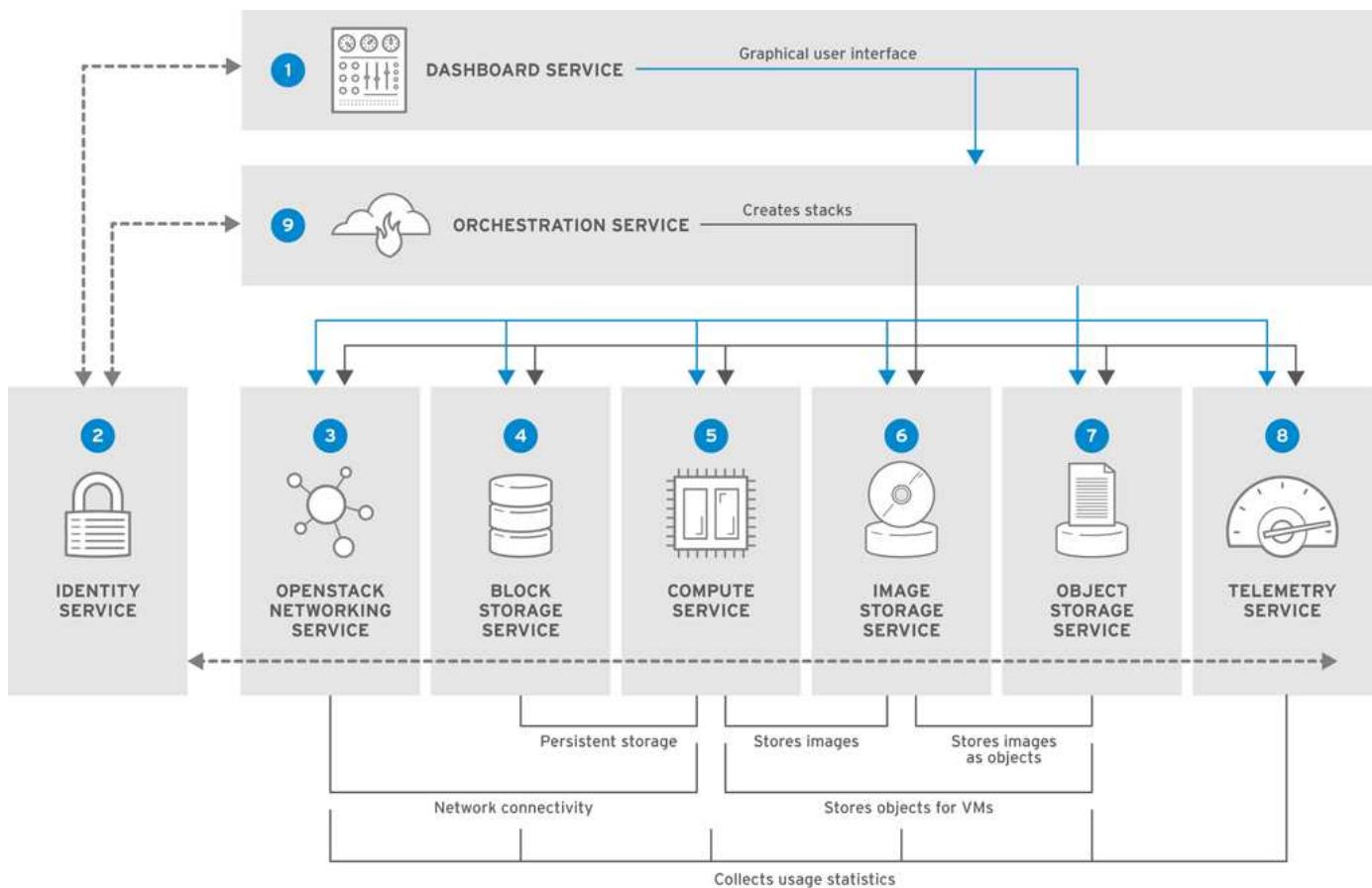
OSP is an infrastructure-as-a-service (IaaS) cloud implemented by a collection of control services that manage compute, storage, and networking resources. The environment is managed using a web-based interface that allows administrators and users to control, provision, and automate OpenStack resources. Additionally, the OpenStack infrastructure is facilitated through an extensive command line interface and API enabling full automation capabilities for administrators and end-users.

The OpenStack project is a rapidly developed community project that provides updated releases every six months. Initially Red Hat OpenStack Platform kept pace with this release cycle by publishing a new release along with every upstream release and providing long term support for every third release. Recently, with the OSP 16.0 release (based on OpenStack Train), Red Hat has chosen not to keep pace with release numbers but instead has backported new features into sub-releases. The most recent release is Red Hat OpenStack Platform 16.1, which includes backported advanced features from the Ussuri and Victoria releases upstream.

For more information about OSP see the [Red Hat OpenStack Platform website](#).

## OpenStack services

OpenStack Platform services are deployed as containers, which isolates services from one another and enables easy upgrades. The OpenStack Platform uses a set of containers built and managed with Kolla. The deployment of services is performed by pulling container images from the Red Hat Custom Portal. These service containers are managed using the Podman command and are deployed, configured, and maintained with Red Hat OpenStack Director.



Service	Project name	Description
Dashboard	Horizon	Web browser-based dashboard that you use to manage OpenStack services.
Identity	Keystone	Centralized service for authentication and authorization of OpenStack services and for managing users, projects, and roles.
OpenStack networking	Neutron	Provides connectivity between the interfaces of OpenStack services.
Block storage	Cinder	Manages persistent block storage volumes for virtual machines (VMs).
Compute	Nova	Manages and provisions VMs running on compute nodes.
Image	Glance	Registry service used to store resources such as VM images and volume snapshots.
Object storage	Swift	Allows users to storage and retrieve files and arbitrary data.

Telemetry	Ceilometer	Provides measurements of use of cloud resources.
Orchestration	Heat	Template-based orchestration engine that supports automatic creation of resource stacks.

#### Network design

The Red Hat OpenShift with NetApp solution uses two data switches to provide primary data connectivity at 25Gbps. It also uses two additional management switches that provide connectivity at 1Gbps for in-band management for the storage nodes and out-of-band management for IPMI functionality.

IPMI functionality is required by Red Hat OpenStack Director to deploy Red Hat OpenStack Platform using the Ironic bare-metal provision service.

#### VLAN requirements

Red Hat OpenShift with NetApp is designed to logically separate network traffic for different purposes by using virtual local area networks (VLANs). This configuration can be scaled to meet customer demands or to provide further isolation for specific network services. The following table lists the VLANs that are required to implement the solution while validating the solution at NetApp.

VLANs	Purpose	VLAN ID
Out-of-band management network	Network used for management of physical nodes and IPMI service for Ironic.	16
Storage infrastructure	Network used for controller nodes to map volumes directly to support infrastructure services like Swift.	201
Storage Cinder	Network used to map and attach block volumes directly to virtual instances deployed in the environment.	202
Internal API	Network used for communication between the OpenStack services using API communication, RPC messages, and database communication.	301
Tenant	Neutron provides each tenant with their own networks via tunneling through VXLAN. Network traffic is isolated within each tenant network. Each tenant network has an IP subnet associated with it, and network namespaces mean that multiple tenant networks can use the same address range without causing conflicts.	302

VLANs	Purpose	VLAN ID
Storage management	OpenStack Object Storage (Swift) uses this network to synchronize data objects between participating replica nodes. The proxy service acts as the intermediary interface between user requests and the underlying storage layer. The proxy receives incoming requests and locates the necessary replica to retrieve the requested data.	303
PXE	The OpenStack Director provides PXE boot as a part of the Ironic bare metal provisioning service to orchestrate the installation of the OSP Overcloud.	3484
External	Publicly available network which hosts the OpenStack Dashboard (Horizon) for graphical management and allows for public API calls to manage OpenStack services.	3485
In-band management network	Provides access for system administration functions such as SSH access, DNS traffic, and Network Time Protocol (NTP) traffic. This network also acts as a gateway for non-controller nodes.	3486

## Network infrastructure support resources

The following infrastructure should be in place prior to the deployment of the OpenShift Container Platform:

- At least one DNS server which provides a full host-name resolution.
- At least three NTP servers which can keep time synchronized for the servers in the solution.
- (Optional) Outbound internet connectivity for the OpenShift environment.

## Best practices for production deployments

This section lists several best practices that an organization should take into consideration before deploying this solution into production.

## Deploy OpenShift to an OSP private cloud with at least three compute nodes

The verified architecture described in this document presents the minimum hardware deployment suitable for HA operations by deploying three OSP controller nodes and two OSP compute nodes. This architecture ensures a fault tolerant configuration in which both compute nodes can launch virtual instances and deployed VMs can migrate between the two hypervisors.

Because Red Hat OpenShift initially deploys with three master nodes, a two-node configuration might cause at least two masters to occupy the same node, which can lead to a possible outage for OpenShift if that specific

node becomes unavailable. Therefore, it is a Red Hat best practice to deploy at least three OSP compute nodes so that the OpenShift masters can be distributed evenly and the solution receives an added degree of fault tolerance.

## Configure virtual machine/host affinity

Distributing the OpenShift masters across multiple hypervisor nodes can be achieved by enabling VM/host affinity.

Affinity is a way to define rules for a set of VMs and/or hosts that determine whether the VMs run together on the same host or hosts in the group or on different hosts. It is applied to VMs by creating affinity groups that consist of VMs and/or hosts with a set of identical parameters and conditions. Depending on whether the VMs in an affinity group run on the same host or hosts in the group or separately on different hosts, the parameters of the affinity group can define either positive affinity or negative affinity. In the Red Hat OpenStack Platform, host affinity and anti-affinity rules can be created and enforced by creating server groups and configuring filters so that instances deployed by Nova in a server group deploy on different compute nodes.

A server group has a default maximum of 10 virtual instances that it can manage placement for. This can be modified by updating the default quotas for Nova.



There is a specific hard affinity/anti-affinity limit for OSP server groups; if there are not enough resources to deploy on separate nodes or not enough resources to allow sharing of nodes, the VM fails to boot.

To configure affinity groups, see [How do I configure Affinity and Anti-Affinity for OpenStack instances?](#).

## Use a custom install file for OpenShift deployment

IPI makes the deployment of OpenShift clusters easy through the interactive wizard discussed earlier in this document. However, it is possible that you might need to change some default values as a part of a cluster deployment.

In these instances, you can run and task the wizard without immediately deploying a cluster; instead it creates a configuration file from which the cluster can be deployed later. This is very useful if you need to change any IPI defaults, or if you want to deploy multiple identical clusters in your environment for other uses such as multitenancy. For more information about creating a customized install configuration for OpenShift, see [Red Hat OpenShift Installing a Cluster on OpenStack with Customizations](#).

Next: [NetApp Storage Overview](#).

## OpenShift on Red Hat Virtualization

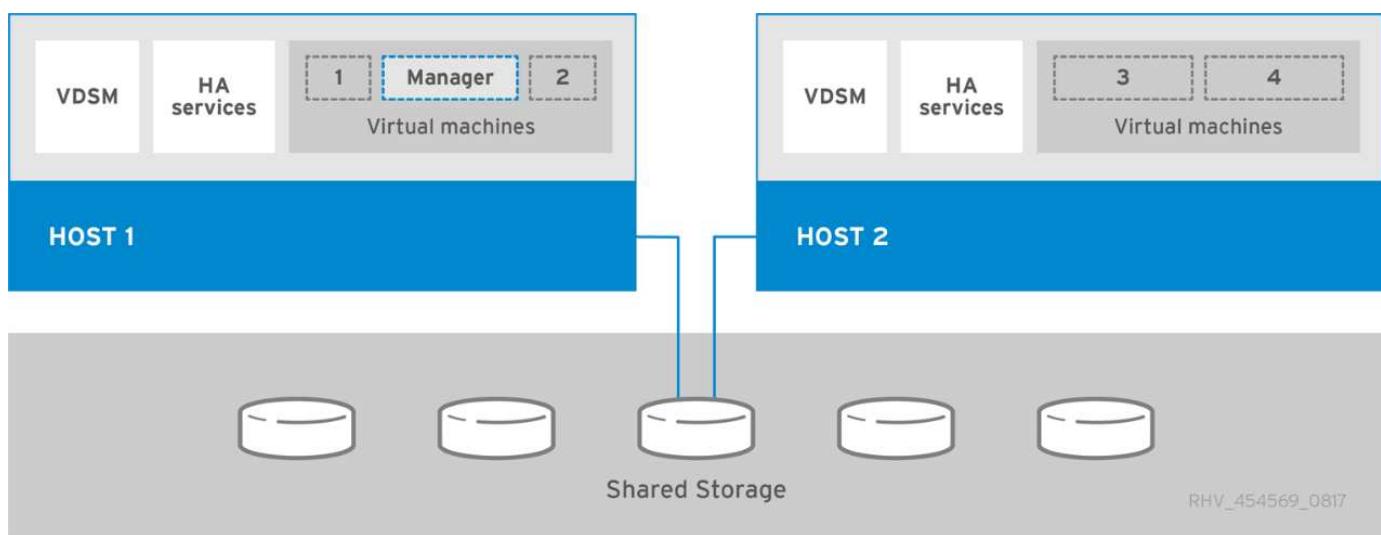
Red Hat Virtualization (RHV) is an enterprise virtual data center platform that runs on Red Hat Enterprise Linux (RHEL) and uses the KVM hypervisor.

For more information about RHV, see the [Red Hat Virtualization website](#).

RHV provides the following features:

- **Centralized management of VMs and hosts.** The RHV manager runs as a physical or virtual machine (VM) in the deployment and provides a web-based GUI for the management of the solution from a central interface.
- **Self-hosted engine.** To minimize hardware requirements, RHV allows RHV Manager (RHV-M) to be deployed as a VM on the same hosts that run guest VMs.

- **High availability.** To avoid disruption in event of host failures, RHV allows VMs to be configured for high availability. The highly available VMs are controlled at the cluster level using resiliency policies.
- **High scalability.** A single RHV cluster can have up to 200 hypervisor hosts enabling it to support requirements of massive VMs to host resource-greedy, enterprise-class workloads.
- **Enhanced security.** Inherited from RHV, Secure Virtualization (sVirt) and Security Enhanced Linux (SELinux) technologies are employed by RHV for the purposes of elevated security and hardening for the hosts and VMs. The key advantage from these features is logical isolation of a VM and its associated resources.



## Network design

The Red Hat OpenShift on NetApp solution uses two data switches to provide primary data connectivity at 25Gbps. It also uses two additional management switches that provide connectivity at 1Gbps for in-band management of the storage nodes and out-of-band management for IPMI functionality. OCP uses the virtual machine logical network on RHV for cluster management. This section describes the arrangement and purpose of each virtual network segment used in the solution and outlines the prerequisites for deploying the solution.

## VLAN requirements

Red Hat OpenShift on RHV is designed to logically separate network traffic for different purposes by using virtual local area networks (VLANs). This configuration can be scaled to meet customer demands or to provide further isolation for specific network services. The following table lists the VLANs that are required to implement the solution while validating the solution at NetApp.

VLANs	Purpose	VLAN ID
Out-of-band management network	Management for physical nodes and IPMI	16
VM Network	Virtual guest network access	1172
In-band management network	Management for RHV-H nodes, RHV-Manager, and ovirtmgmt network	3343
Storage network	Storage network for NetApp Element iSCSI	3344

VLANs	Purpose	VLAN ID
Migration network	Network for virtual guest migration	3345

## Network infrastructure support resources

The following infrastructure should be in place prior to the deployment of the OpenShift Container Platform:

- At least one DNS server providing full host-name resolution that is accessible from the in-band management network and the VM network.
- At least one NTP server that is accessible from the in-band management network and the VM network.
- (Optional) Outbound internet connectivity for both the in-band management network and the VM network.

## Best practices for production deployments

This section lists several best practices that an organization should take into consideration before deploying this solution into production.

## Deploy OpenShift to an RHV cluster of at least three nodes

The verified architecture described in this document presents the minimum hardware deployment suitable for HA operations by deploying two RHV-H hypervisor nodes and ensuring a fault tolerant configuration where both hosts can manage the hosted-engine and deployed VMs can migrate between the two hypervisors.

Because Red Hat OpenShift initially deploys with three master nodes, it is ensured in a two-node configuration that at least two masters will occupy the same node, which can lead to a possible outage for OpenShift if that specific node becomes unavailable. Therefore, it is a Red Hat best practice that at least three RHV-H hypervisor nodes be deployed as part of the solution so that the OpenShift masters can be distributed evenly and the solution receives an added degree of fault tolerance.

## Configure virtual machine/host affinity

You can distribute the OpenShift masters across multiple hypervisor nodes by enabling VM/host affinity.

Affinity is a way to define rules for a set of VMs and/or hosts that determine whether the VMs run together on the same host or hosts in the group or on different hosts. It is applied to VMs by creating affinity groups that consist of VMs and/or hosts with a set of identical parameters and conditions. Depending on whether the VMs in an affinity group run on the same host or hosts in the group or separately on different hosts, the parameters of the affinity group can define either positive affinity or negative affinity.

The conditions defined for the parameters can be either hard enforcement or soft enforcement. Hard enforcement ensures that the VMs in an affinity group always follows the positive or negative affinity strictly without any regards to external conditions. Soft enforcement ensures that a higher preference is set for the VMs in an affinity group to follow the positive or negative affinity whenever feasible. In the two or three hypervisor configuration described in this document, soft affinity is the recommended setting. In larger clusters, hard affinity can correctly distribute OpenShift nodes.

To configure affinity groups, see the [Red Hat 6.11. Affinity Groups documentation](#).

## Use a custom install file for OpenShift deployment

IPI makes the deployment of OpenShift clusters easy through the interactive wizard discussed earlier in this document. However, it is possible that there are some default values that might need to be changed as a part of cluster deployment.

In these instances, you can run and task the wizard without immediately deploying a cluster. Rather, a configuration file is created from which the cluster can be deployed later. This is very useful if you want to change any IPI defaults or if you want to deploy multiple identical clusters in your environment for other uses such as multitenancy. For more information about creating a customized install configuration for OpenShift, see [Red Hat OpenShift Installing a Cluster on RHV with Customizations](#).

Next: [NetApp storage overview](#).

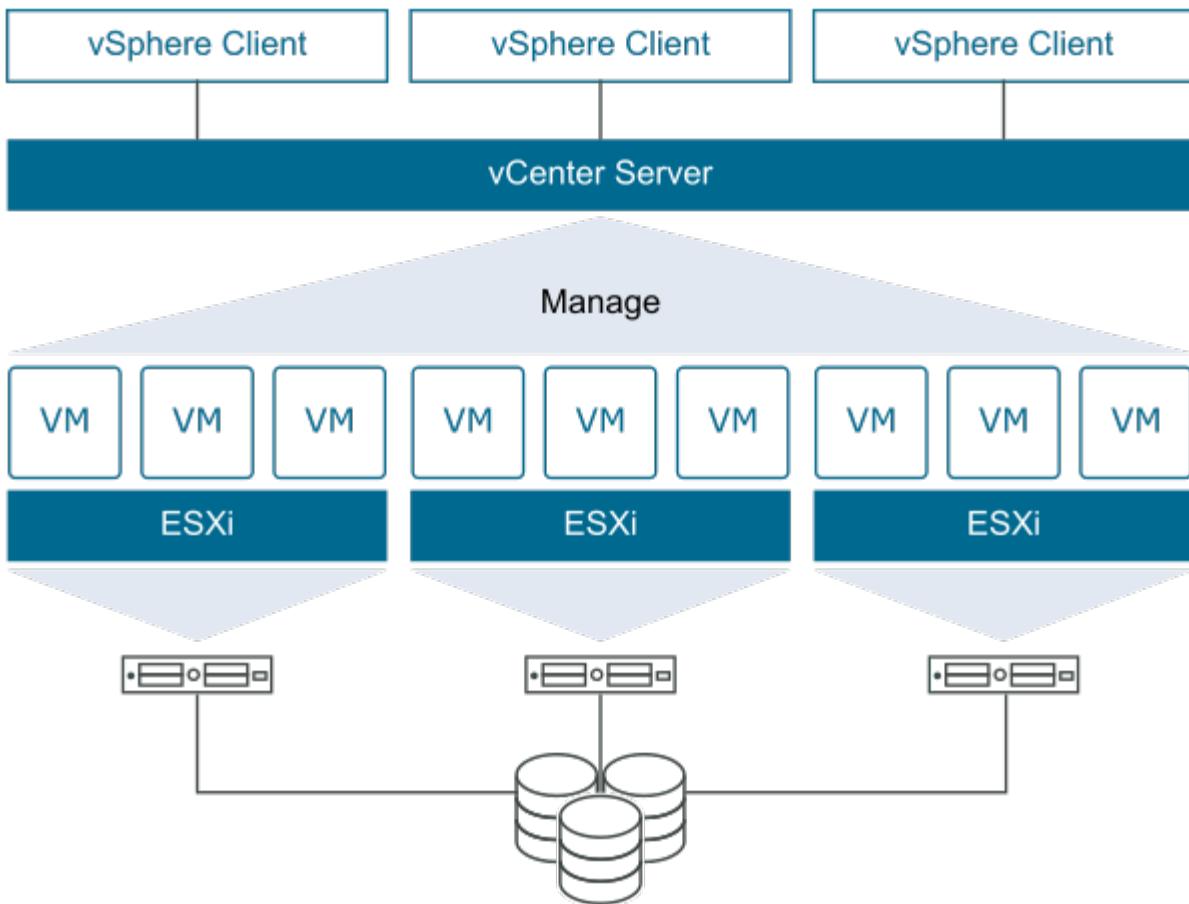
## OpenShift on VMware vSphere

VMware vSphere is a virtualization platform for centrally managing a large number of virtualized servers and networks running on the ESXi hypervisor.

For more information about VMware vSphere, see the [VMware vSphere website](#).

VMware vSphere provides the following features:

- **VMware vCenter Server.** VMware vCenter Server provides unified management of all hosts and VMs from a single console and aggregates performance monitoring of clusters, hosts, and VMs.
- **VMware vSphere vMotion.** VMware vCenter allows you to hot migrate VMs between nodes in the cluster upon request in a nondisruptive manner.
- **vSphere High Availability.** To avoid disruption in the event of host failures, VMware vSphere allows hosts to be clustered and configured for High Availability. VMs that are disrupted by host failure are rebooted shortly on other hosts in the cluster, restoring services.
- **Distributed Resource Scheduler (DRS).** A VMware vSphere cluster can be configured to load balance the resource needs of the VMs it is hosting. VMs with resource contentions can be hot migrated to other nodes in the cluster to make sure that enough resources are available.



## Network design

The Red Hat OpenShift on NetApp solution uses two data switches to provide primary data connectivity at 25Gbps. It also uses two additional management switches that provide connectivity at 1Gbps for in-band management for the storage nodes and out-of-band management for IPMI functionality. OCP uses the VM logical network on VMware vSphere for its cluster management. This section describes the arrangement and purpose of each virtual network segment used in the solution and outlines the prerequisites for deployment of the solution.

## VLAN requirements

Red Hat OpenShift on VMware vSphere is designed to logically separate network traffic for different purposes by using virtual local area networks (VLANs). This configuration can be scaled to meet customer demands or to provide further isolation for specific network services. The following table lists the VLANs that are required to implement the solution while validating the solution at NetApp.

VLANs	Purpose	VLAN ID
Out-of-band management network	Management for physical nodes and IPMI	16
VM Network	Virtual guest network access	181
Storage network	Storage network for ONTAP NFS	184
Storage network	Storage network for ONTAP iSCSI	185

VLANs	Purpose	VLAN ID
In-band management network	Management for ESXi Nodes, VCenter Server, ONTAP Select	3480
Storage network	Storage network for NetApp Element iSCSI	3481
Migration network	Network for virtual guest migration	3482

## Network infrastructure support resources

The following infrastructure should be in place prior to the deployment of the OpenShift Container Platform:

- At least one DNS server providing full host-name resolution that is accessible from the in-band management network and the VM network.
- At least one NTP server that is accessible from the in-band management network and the VM network.
- (Optional) Outbound internet connectivity for both the in-band management network and the VM network.

## Best practices for production deployments

This section lists several best practices that an organization should take into consideration before deploying this solution into production.

### Deploy OpenShift to an ESXi cluster of at least three nodes

The verified architecture described in this document presents the minimum hardware deployment suitable for HA operations by deploying two ESXi hypervisor nodes and ensuring a fault tolerant configuration by enabling VMware vSphere HA and VMware vMotion. This configuration allows deployed VMs to migrate between the two hypervisors and reboot should one host become unavailable.

Because Red Hat OpenShift initially deploys with three master nodes, at least two masters in a two-node configuration can occupy the same node under some circumstances, which can lead to a possible outage for OpenShift if that specific node becomes unavailable. Therefore, it is a Red Hat best practice that at least three ESXi hypervisor nodes must be deployed so that the OpenShift masters can be distributed evenly, which provides an added degree of fault tolerance.

### Configure virtual machine and host affinity

Ensuring the distribution of the OpenShift masters across multiple hypervisor nodes can be achieved by enabling VM and host affinity.

Affinity or anti-affinity is a way to define rules for a set of VMs and/or hosts that determine whether the VMs run together on the same host or hosts in the group or on different hosts. It is applied to VMs by creating affinity groups that consist of VMs and/or hosts with a set of identical parameters and conditions. Depending on whether the VMs in an affinity group run on the same host or hosts in the group or separately on different hosts, the parameters of the affinity group can define either positive affinity or negative affinity.

To configure affinity groups, see the [vSphere 6.7 Documentation: Using DRS Affinity Rules](#).

### Use a custom install file for OpenShift deployment

IPI makes the deployment of OpenShift clusters easy through the interactive wizard discussed earlier in this document. However, it is possible that you might need to change some default values as a part of a cluster

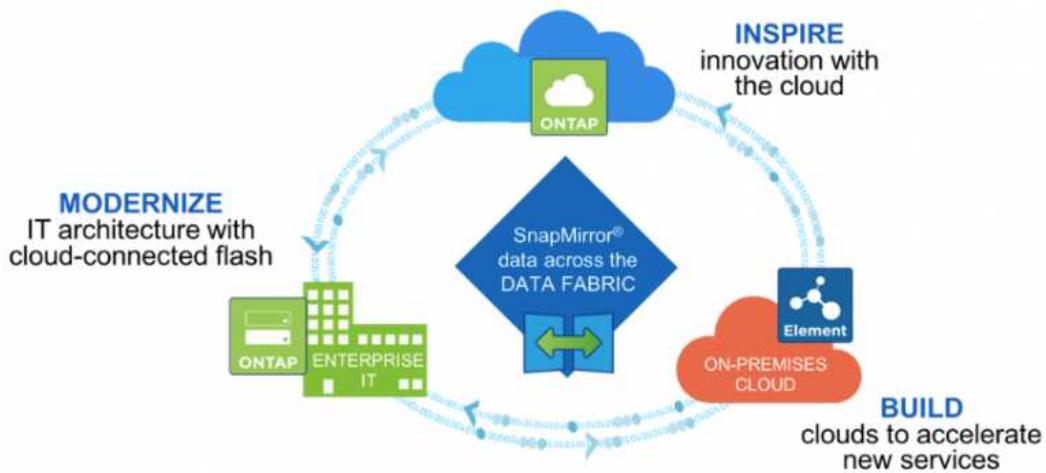
deployment.

In these instances, you can run and task the wizard without immediately deploying a cluster, but instead the wizard creates a configuration file from which the cluster can be deployed later. This is very useful if you need to change any IPI defaults, or if you want to deploy multiple identical clusters in your environment for other uses such as multitenancy. For more information about creating a customized install configuration for OpenShift, see [Red Hat OpenShift Installing a Cluster on vSphere with Customizations](#).

Next: [NetApp Storage Overview](#).

## NetApp Storage Overview

NetApp has several storage platforms that are qualified with our Astra Trident Storage Orchestrator to provision storage for applications deployed on Red Hat OpenShift.



- AFF and FAS systems run NetApp ONTAP and provide storage for both file-based (NFS) and block-based (iSCSI) use cases.
- Cloud Volumes ONTAP and ONTAP Select provide the same benefits in the cloud and virtual space respectively.
- NetApp Cloud Volumes Service (AWS/GCP) and Azure NetApp Files provide file-based storage in the cloud.
- NetApp Element storage systems provide for block-based (iSCSI) use cases in a highly scalable environment.

i Each storage system in the NetApp portfolio can ease both data management and movement between on-premises sites and the cloud, ensuring that your data is where your applications are.

The following pages have additional information about the NetApp storage systems validated in the Red Hat OpenShift with NetApp solution:

- [NetApp ONTAP](#)
- [NetApp Element](#)

Next: [NetApp Storage Integrations Overview](#)

## NetApp ONTAP

NetApp ONTAP is a powerful storage-software tool with capabilities such as an intuitive GUI, REST APIs with automation integration, AI-informed predictive analytics and corrective action, non-disruptive hardware upgrades, and cross-storage import.

For more information about the NetApp ONTAP storage system, visit the [NetApp ONTAP website](#).

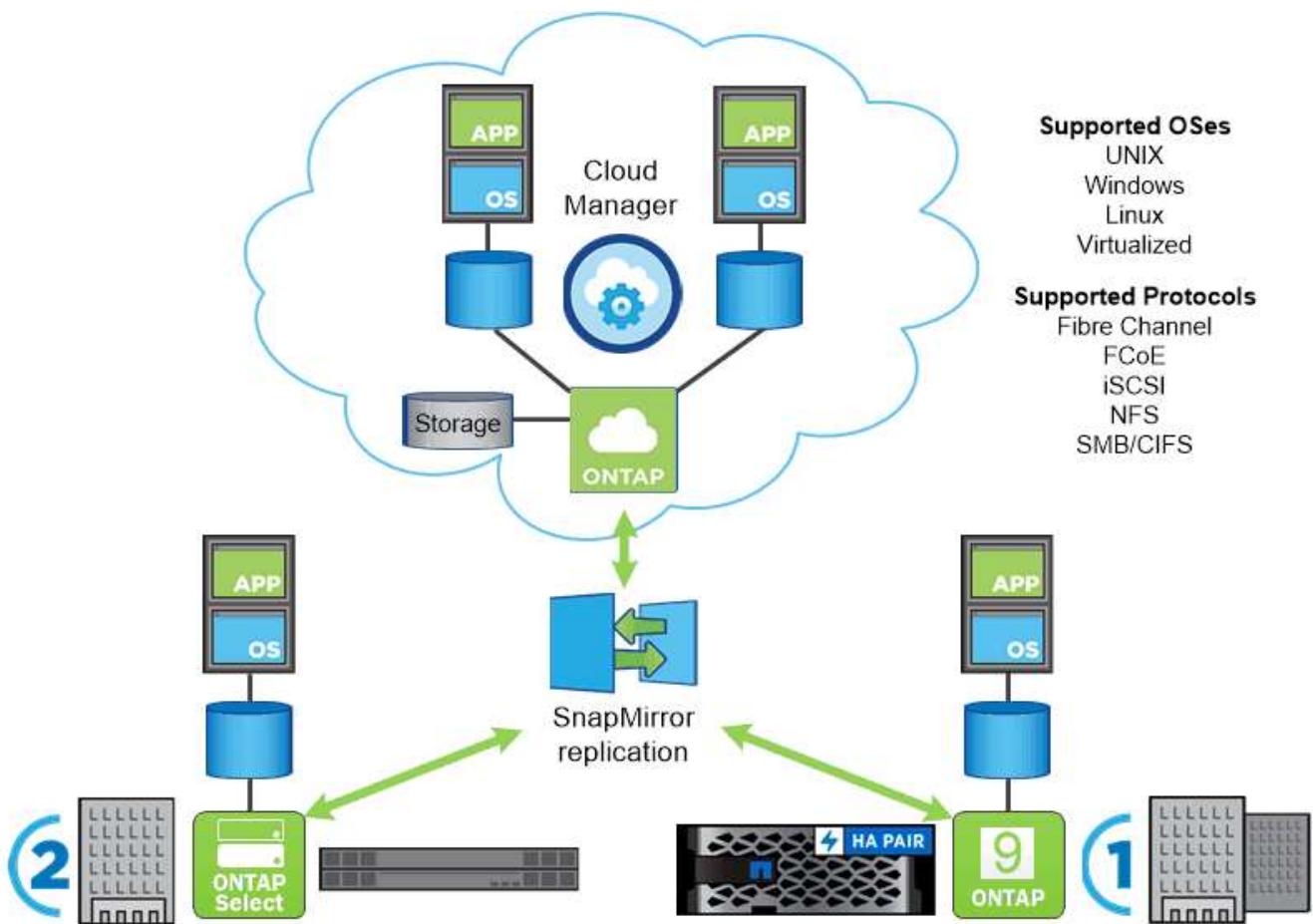
ONTAP provides the following features:

- A unified storage system with simultaneous data access and management of NFS, CIFS, iSCSI, FC, FCoE, and FC-NVMe protocols.
- Different deployment models include on-premises on all-flash, hybrid, and all-HDD hardware configurations; VM-based storage platforms on a supported hypervisor such as ONTAP Select; and in the cloud as Cloud Volumes ONTAP.
- Increased data storage efficiency on ONTAP systems with support for automatic data tiering, inline data compression, deduplication, and compaction.
- Workload-based, QoS-controlled storage.
- Seamless integration with a public cloud for tiering and protection of data. ONTAP also provides robust data protection capabilities that sets it apart in any environment:
  - **NetApp Snapshot copies.** A fast, point-in-time backup of data using a minimal amount of disk space with no additional performance overhead.
  - **NetApp SnapMirror.** Mirrors the Snapshot copies of data from one storage system to another. ONTAP supports mirroring data to other physical platforms and cloud-native services as well.
  - **NetApp SnapLock.** Efficiently administration of non-rewritable data by writing it to special volumes that cannot be overwritten or erased for a designated period.
  - **NetApp SnapVault.** Backs up data from multiple storage systems to a central Snapshot copy that serves as a backup to all designated systems.
  - **NetApp SyncMirror.** Provides real-time, RAID-level mirroring of data to two different plexes of disks that are connected physically to the same controller.
  - **NetApp SnapRestore.** Provides fast restoration of backed-up data on demand from Snapshot copies.
  - **NetApp FlexClone.** Provides instantaneous provisioning of a fully readable and writeable copy of a NetApp volume based on a Snapshot copy.

For more information about ONTAP, see the [ONTAP 9 Documentation Center](#).



NetApp ONTAP is available on-premises, virtualized, or in the cloud.



## NetApp platforms

### NetApp AFF/FAS

NetApp provides robust all-flash (AFF) and scale-out hybrid (FAS) storage platforms that are tailor-made with low-latency performance, integrated data protection, and multi-protocol support.

Both systems are powered by NetApp ONTAP data management software, the industry's most advanced data-management software for highly-available, cloud-integrated, simplified storage management to deliver enterprise-class speed, efficiency, and security your data fabric needs.

For more information about NETAPP AFF/FAS platforms, click [here](#).

### ONTAP Select

ONTAP Select is a software-defined deployment of NetApp ONTAP that can be deployed onto a hypervisor in your environment. It can be installed on VMware vSphere or on KVM and provides the full functionality and experience of a hardware-based ONTAP system.

For more information about ONTAP Select, click [here](#).

### Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP is a cloud-deployed version of NetApp ONTAP available to be deployed in a number of public clouds, including: Amazon AWS, Microsoft Azure, and Google Cloud.

For more information about Cloud Volumes ONTAP, click [here](#).

[Next: NetApp Storage Integrations Overview](#)

## NetApp Element: Red Hat OpenShift with NetApp

NetApp Element software provides modular, scalable performance, with each storage node delivering guaranteed capacity and throughput to the environment. NetApp Element systems can scale from 4 to 100 nodes in a single cluster and offer a number of advanced storage management features.



For more information about NetApp Element storage systems, visit the [NetApp Solidfire website](#).

### iSCSI login redirection and self-healing capabilities

NetApp Element software leverages the iSCSI storage protocol, a standard way to encapsulate SCSI commands on a traditional TCP/IP network. When SCSI standards change or when the performance of Ethernet networks improves, the iSCSI storage protocol benefits without the need for any changes.

Although all storage nodes have a management IP and a storage IP, NetApp Element software advertises a single storage virtual IP address (SVIP address) for all storage traffic in the cluster. As a part of the iSCSI login process, storage can respond that the target volume has been moved to a different address and therefore it cannot proceed with the negotiation process. The host then reissues the login request to the new address in a process that requires no host-side reconfiguration. This process is known as iSCSI login redirection.

iSCSI login redirection is a key part of the NetApp Element software cluster. When a host login request is received, the node decides which member of the cluster should handle the traffic based on the IOPS and the capacity requirements for the volume. Volumes are distributed across the NetApp Element software cluster and are redistributed if a single node is handling too much traffic for its volumes or if a new node is added. Multiple copies of a given volume are allocated across the array.

In this manner, if a node failure is followed by volume redistribution, there is no effect on host connectivity beyond a logout and login with redirection to the new location. With iSCSI login redirection, a NetApp Element software cluster is a self-healing, scale-out architecture that is capable of non-disruptive upgrades and operations.

### NetApp Element software cluster QoS

A NetApp Element software cluster allows QoS to be dynamically configured on a per-volume basis. You can use per-volume QoS settings to control storage performance based on SLAs that you define. The following three configurable parameters define the QoS:

- **Minimum IOPS.** The minimum number of sustained IOPS that the NetApp Element software cluster provides to a volume. The minimum IOPS configured for a volume is the guaranteed level of performance for a volume. Per-volume performance does not drop below this level.

- **Maximum IOPS.** The maximum number of sustained IOPS that the NetApp Element software cluster provides to a particular volume.
- **Burst IOPS.** The maximum number of IOPS allowed in a short burst scenario. The burst duration setting is configurable, with a default of 1 minute. If a volume has been running below the maximum IOPS level, burst credits are accumulated. When performance levels become very high and are pushed, short bursts of IOPS beyond the maximum IOPS are allowed on the volume.

## Multitenancy

Secure multitenancy is achieved with the following features:

- **Secure authentication.** The Challenge-Handshake Authentication Protocol (CHAP) is used for secure volume access. The Lightweight Directory Access Protocol (LDAP) is used for secure access to the cluster for management and reporting.
- **Volume access groups (VAGs).** Optionally, VAGs can be used in lieu of authentication, mapping any number of iSCSI initiator-specific iSCSI Qualified Names (IQNs) to one or more volumes. To access a volume in a VAG, the initiator's IQN must be in the allowed IQN list for the group of volumes.
- **Tenant virtual LANs (VLANs).** At the network level, end-to-end network security between iSCSI initiators and the NetApp Element software cluster is facilitated by using VLANs. For any VLAN that is created to isolate a workload or a tenant, NetApp Element Software creates a separate iSCSI target SVIP address that is accessible only through the specific VLAN.
- **VRF-enabled VLANs.** To further support security and scalability in the data center, NetApp Element software allows you to enable any tenant VLAN for VRF-like functionality. This feature adds these two key capabilities:
  - **L3 routing to a tenant SVIP address.** This feature allows you to situate iSCSI initiators on a separate network or VLAN from that of the NetApp Element software cluster.
  - **Overlapping or duplicate IP subnets.** This feature enables you to add a template to tenant environments, allowing each respective tenant VLAN to be assigned IP addresses from the same IP subnet. This capability can be useful for in-service provider environments where scale and preservation of IPspace are important.

## Enterprise storage efficiencies

The NetApp Element software cluster increases overall storage efficiency and performance. The following features are performed inline, are always on, and require no manual configuration by the user:

- **Deduplication.** The system only stores unique 4K blocks. Any duplicate 4K blocks are automatically associated to an already stored version of the data. Data is on block drives and is mirrored by using the NetApp Element software Helix data protection. This system significantly reduces capacity consumption and write operations within the system.
- **Compression.** Compression is performed inline before data is written to NVRAM. Data is compressed, stored in 4K blocks, and remains compressed in the system. This compression significantly reduces capacity consumption, write operations, and bandwidth consumption across the cluster.
- **Thin-provisioning.** This capability provides the right amount of storage at the time that you need it, eliminating capacity consumption that caused by overprovisioned volumes or underutilized volumes.
- **Helix.** The metadata for an individual volume is stored on a metadata drive and is replicated to a secondary metadata drive for redundancy.

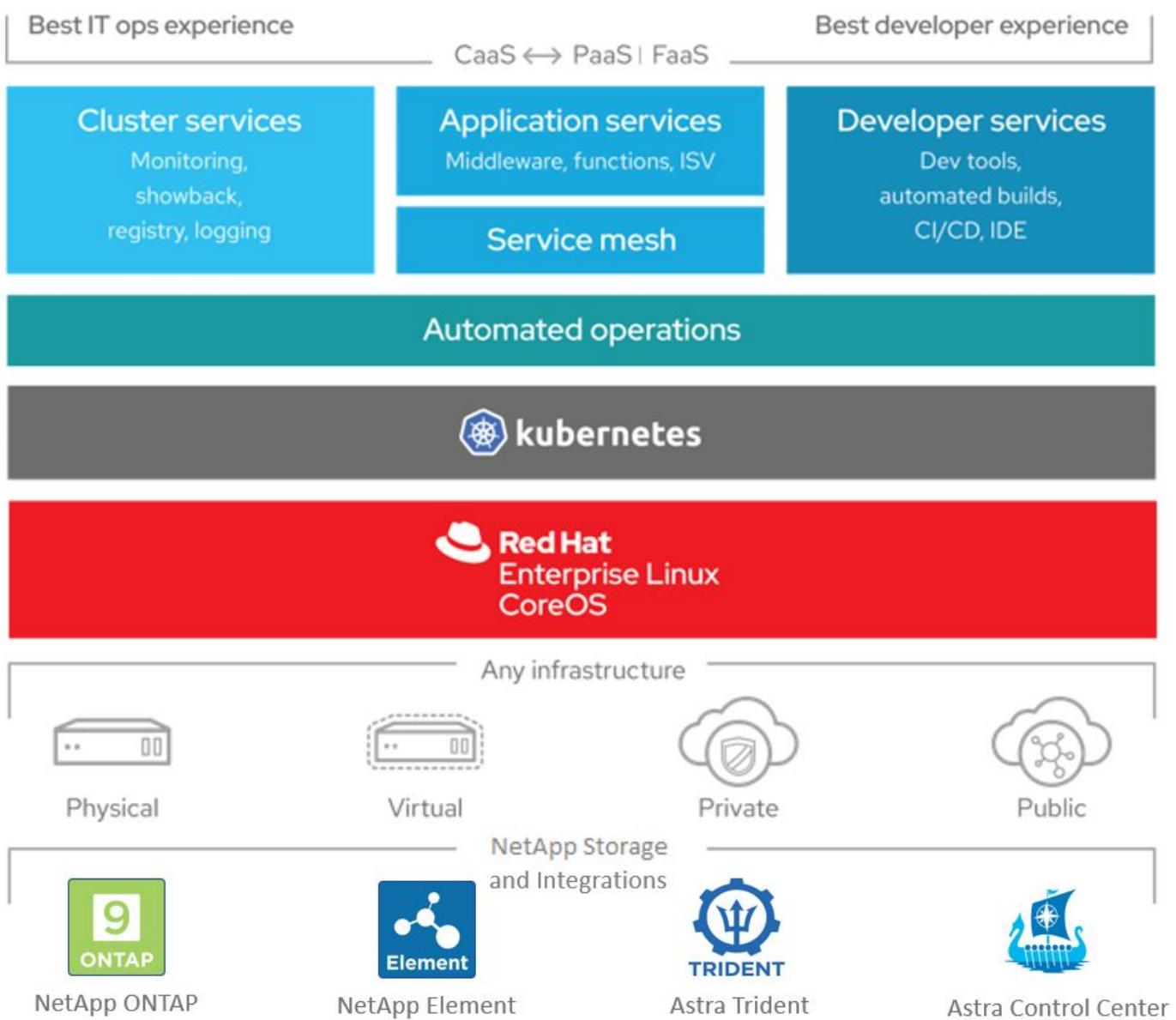


Element was designed for automation. All the storage features are available through APIs. These APIs are the only method that the UI uses to control the system.

Next: NetApp Storage Integrations Overview.

## NetApp Storage Integration Overview

NetApp provides a number of products to help you with orchestrating and managing persistent data in container based environments, such as Red Hat OpenShift.



NetApp Astra Control offers a rich set of storage and application-aware data management services for stateful Kubernetes workloads, powered by NetApp data protection technology. The Astra Control Service is available to support stateful workloads in cloud-native Kubernetes deployments. The Astra Control Center is available to support stateful workloads in on-premises deployments, like Red Hat OpenShift. For more information visit the NetApp Astra Control website [here](#).

NetApp Astra Trident is an open-source and fully-supported storage orchestrator for containers and Kubernetes distributions, including Red Hat OpenShift. For more information, visit the Astra Trident website [here](#).

The following pages have additional information about the NetApp products that have been validated for

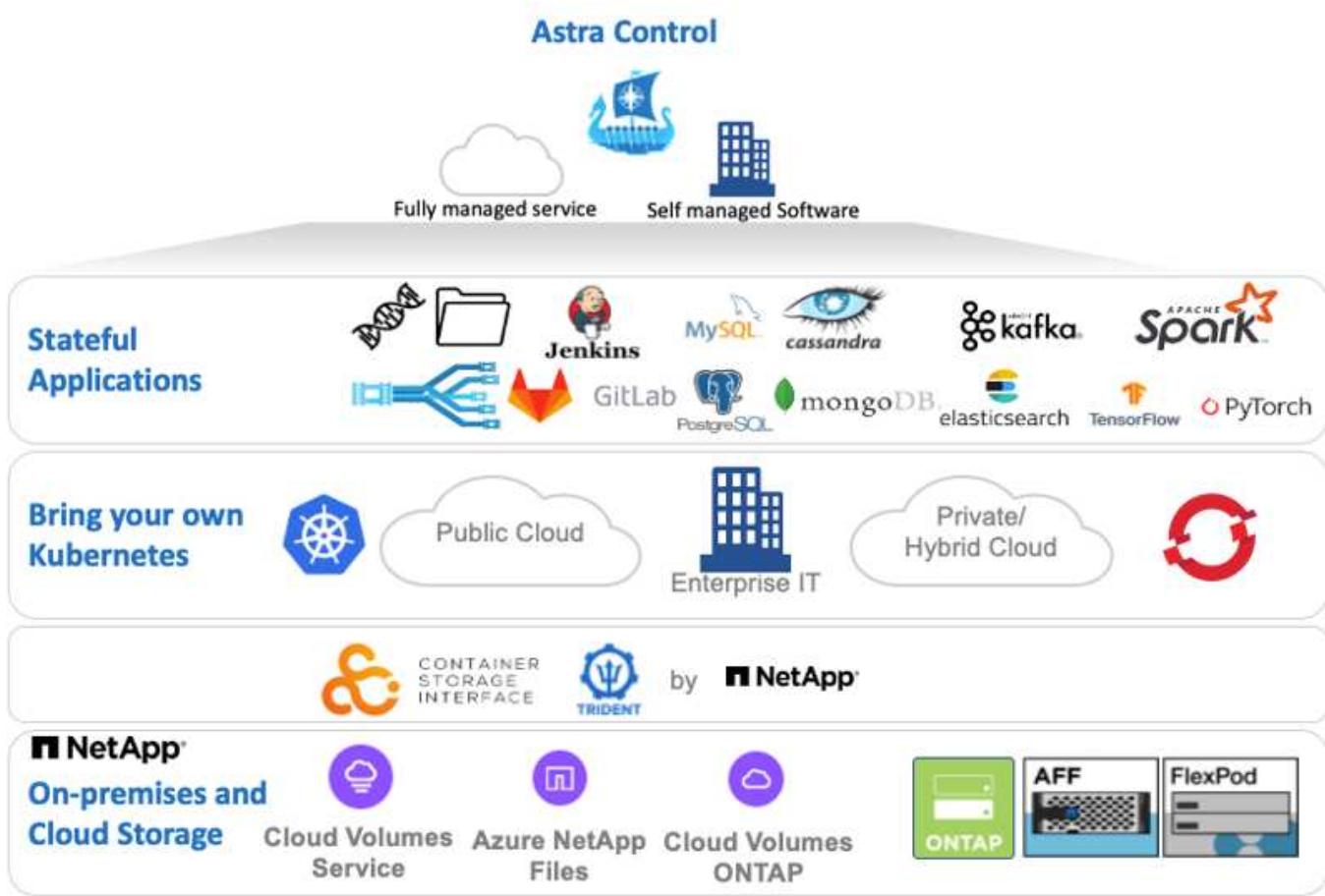
application and persistent storage management in the Red Hat OpenShift with NetApp solution:

- [NetApp Astra Control Center](#)
- [NetApp Astra Trident](#)

Next: [NetApp Astra Control Center Overview](#)

## NetApp Astra Control Center overview

NetApp Astra Control Center offers a rich set of storage and application-aware data management services for stateful Kubernetes workloads deployed in an on-premises environment and powered by NetApp data protection technology.



NetApp Astra Control Center can be installed on a Red Hat OpenShift cluster that has the Astra Trident storage orchestrator deployed and configured with storage classes and storage backends to NetApp ONTAP storage systems.

For the installation and configuration of Astra Trident to support Astra Control Center, see [this document here](#).

In a cloud-connected environment, Astra Control Center uses Cloud Insights to provide advanced monitoring and telemetry. In the absence of a Cloud Insights connection, limited monitoring and telemetry (7-days worth of metrics) is available and exported to Kubernetes native monitoring tools (Prometheus and Grafana) through open metrics endpoints.

Astra Control Center is fully integrated into the NetApp AutoSupport and Active IQ ecosystem to provide support for users, provide assistance with troubleshooting, and display usage statistics.

In addition to the paid version of Astra Control Center, a 90-day evaluation license is available. The evaluation version is supported through the email and community (Slack channel). Customers have access to these and other knowledge-base articles and the documentation available from the in-product support dashboard.

To get started with NetApp Astra Control Center, visit the [Astra website](#).

#### Astra Control Center installation prerequisites

1. One or more Red Hat OpenShift clusters. Versions 4.6 EUS and 4.7 are currently supported.
2. Astra Trident must already be installed and configured on each Red Hat OpenShift cluster.
3. One or more NetApp ONTAP storage systems running ONTAP 9.5 or greater.

 It's best practice for each OpenShift install at a site to have a dedicated SVM for persistent storage. Multi-site deployments require additional storage systems.
4. A Trident storage backend must be configured on each OpenShift cluster with an SVM backed by an ONTAP cluster.
5. A default StorageClass configured on each OpenShift cluster with Astra Trident as the storage provisioner.
6. A load balancer must be installed and configured on each OpenShift cluster for load balancing and exposing OpenShift Services.

 See the link [here](#) for information about load balancers that have been validated for this purpose.
7. A private image registry must be configured to host the NetApp Astra Control Center images.

 See the link [here](#) to install and configure an OpenShift private registry for this purpose.
8. You must have Cluster Admin access to the Red Hat OpenShift cluster.
9. You must have Admin access to NetApp ONTAP clusters.
10. An admin workstation with docker or podman, tridentctl, and oc or kubectl tools installed and added to your \$PATH.

 Docker installations must have docker version greater than 20.10 and Podman installations must have podman version greater than 3.0.

#### Install Astra Control Center

## Using OperatorHub

1. Log into the NetApp Support Site and download the latest version of NetApp Astra Control Center. To do so requires a license attached to your NetApp account. After you download the tarball, transfer it to the admin workstation.



To get started with a trial license for Astra Control, visit the [Astra registration site](#).

2. Unpack the tar ball and change the working directory to the resulting folder.

```
[netapp-user@rhel7 ~]$ tar -vxzf astra-control-center-  
21.12.60.tar.gz  
[netapp-user@rhel7 ~]$ cd astra-control-center-21.12.60
```

3. Before starting the installation, push the Astra Control Center images to an image registry. You can choose to do this with either Docker or Podman, instructions for both are provided in this step.

# Podman

- a. Export the registry FQDN with the organization/namespace/project name as a environment variable 'registry'.

```
[netapp-user@rhel7 ~]$ export REGISTRY=astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra
```

- b. Log into the registry.

```
[netapp-user@rhel7 ~]$ podman login -u ocp-user -p password  
--tls-verify=false astra-registry.apps.ocp-vmw.cie.netapp.com
```

If you are using kubeadm user to log into the private registry, then use token instead of password - podman login -u ocp-user -p token --tls-verify=false astra-registry.apps.ocp-vmw.cie.netapp.com.

Alternatively, you can create a service account, assign registry-editor and/or registry-viewer role (based on whether you require push/pull access) and log into the registry using service account's token.

- c. Create a shell script file and paste the following content in it.

```
[netapp-user@rhel7 ~]$ vi push-images-to-registry.sh

for astraImageFile in $(ls images/*.tar) ; do
    # Load to local cache. And store the name of the loaded
    image trimming the 'Loaded images: '
    astraImage=$(podman load --input ${astraImageFile} | sed
's/Loaded image(s): //')
    astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
    # Tag with local image repo.
    podman tag ${astraImage} ${REGISTRY}/${astraImage}
    # Push to the local repo.
    podman push ${REGISTRY}/${astraImage}
done
```

If you are using untrusted certificates for your registry, edit the shell script and use `--tls-verify=false` for the podman push command `podman push $REGISTRY/$(echo $astraImage | sed 's/[\\/]\\+\\//')` `--tls-verify=false`.

- d. Make the file executable.

```
[netapp-user@rhel7 ~]$ chmod +x push-images-to-registry.sh
```

- e. Execute the shell script.

```
[netapp-user@rhel7 ~]$ ./push-images-to-registry.sh
```

## Docker

- Export the registry FQDN with the organization/namespace/project name as a environment variable 'registry'.

```
[netapp-user@rhel7 ~]$ export REGISTRY=astra-  
registry.apps.ocp-vmw.cie.netapp.com/netapp-astra
```

- Log into the registry.

```
[netapp-user@rhel7 ~]$ docker login -u ocp-user -p password  
astra-registry.apps.ocp-vmw.cie.netapp.com
```



If you are using kubeadmin user to log into the private registry, then use token instead of password - docker login -u ocp-user -p token astra-registry.apps.ocp-vmw.cie.netapp.com.



Alternatively, you can create a service account, assign registry-editor and/or registry-viewer role (based on whether you require push/pull access) and log into the registry using service account's token.

- Create a shell script file and paste the following content in it.

```
[netapp-user@rhel7 ~]$ vi push-images-to-registry.sh  
  
for astraImageFile in $(ls images/*.tar) ; do  
    # Load to local cache. And store the name of the loaded  
    # image trimming the 'Loaded images: '  
    astraImage=$(docker load --input ${astraImageFile} | sed  
's/Loaded image: //')  
    astraImage=$(echo ${astraImage} | sed 's!localhost/!!')  
    # Tag with local image repo.  
    docker tag ${astraImage} ${REGISTRY}/${astraImage}  
    # Push to the local repo.  
    docker push ${REGISTRY}/${astraImage}  
done
```

- Make the file executable.

```
[netapp-user@rhel7 ~]$ chmod +x push-images-to-registry.sh
```

- Execute the shell script.

```
[netapp-user@rhel7 ~]$ ./push-images-to-registry.sh
```

- When using private image registries that are not publicly trusted, upload the image registry TLS certificates to the OpenShift nodes. To do so, create a configmap in the openshift-config namespace using the TLS certificates and patch it to the cluster image config to make the certificate trusted.

```
[netapp-user@rhel7 ~]$ oc create configmap default-ingress-ca -n openshift-config --from-file=astra-registry.apps.ocp -vmw.cie.netapp.com=tls.crt
```

```
[netapp-user@rhel7 ~]$ oc patch image.config.openshift.io/cluster --patch '{"spec":{"additionalTrustedCA":{"name":"default-ingress-ca"}}}' --type=merge
```



If you are using an OpenShift internal registry with default TLS certificates from the ingress operator with a route, you still need to follow the previous step to patch the certificates to the route hostname. To extract the certificates from ingress operator, you can use the command `oc extract secret/router-ca --keys=tls.crt -n openshift-ingress-operator`.

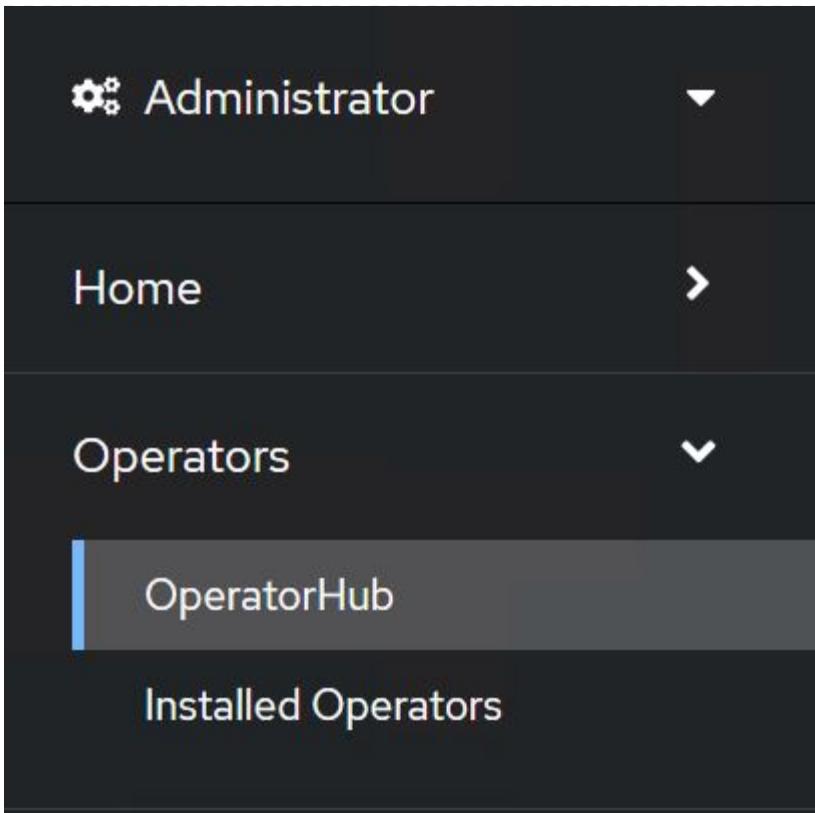
- Create a namespace `netapp-acc-operator` for Astra Control Center.

```
[netapp-user@rhel7 ~]$ oc create ns netapp-acc-operator  
namespace/netapp-acc-operator created
```

- Create a secret with credentials to log into the image registry in `netapp-acc-operator` namespace.

```
[netapp-user@rhel7 ~]$ oc create secret docker-registry astra-registry-cred --docker-server=astra-registry.apps.ocp -vmw.cie.netapp.com --docker-username=ocp-user --docker-password=password -n netapp-acc-operator  
secret/astra-registry-cred created
```

- Log into the Red Hat OpenShift GUI console with cluster-admin access.
- Select Administrator from the Perspective drop down.
- Navigate to Operators > OperatorHub and search for Astra.



10. Select netapp-acc-operator tile and click Install.

The screenshot shows a product card for "netapp-acc-operator".  
- \*\*Icon:\*\* A pink circle containing a white starburst symbol.  
- \*\*Name:\*\* netapp-acc-operator  
- \*\*Version:\*\* 21.12.63-1 provided by NetApp  
- \*\*Install Button:\*\* A blue button with the word "Install".  
- \*\*Latest version:\*\* 21.12.63-1  
- \*\*Description:\*\* Astra Control is an application-aware data management solution that manages, protects and moves data-rich Kubernetes workloads in both public clouds and on-premises.  
- \*\*Capability level:\*\*

- Basic Install
- Seamless Upgrades
- Full Lifecycle
- Deep Insights
- Auto Pilot

  
- \*\*How to deploy Astra Control:\*\* Refer to [Installation Procedure](#) to deploy Astra Control Center using the Operator.  
- \*\*Documentation:\*\* Refer to [Astra Control Center Documentation](#) to complete the setup and start managing applications.  
- \*\*Provider type:\*\* Certified  
- \*\*Provider:\*\* NetApp

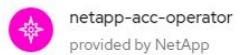
11. On the Install Operator screen, accept all default parameters and click Install.

## Install Operator

Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.

### Update channel \*

- alpha
- stable



netapp-acc-operator  
provided by NetApp

Provided APIs

### Installation mode \*

- All namespaces on the cluster (default)  
Operator will be available in all Namespaces.
- A specific namespace on the cluster  
This mode is not supported by this Operator



AstraControlCenter is the Schema for  
the astracontrolcenters API

### Installed Namespace \*

netapp-acc-operator (Operator recommended)

#### ⚠ Namespace already exists

Namespace **netapp-acc-operator** already exists and will be used. Other users can already have access to this namespace.

### Approval strategy \*

- Automatic
- Manual

**Install**

**Cancel**

12. Wait for the operator installation to complete.

**netapp-acc-operator**  
 21.12.63-1 provided by NetApp

---

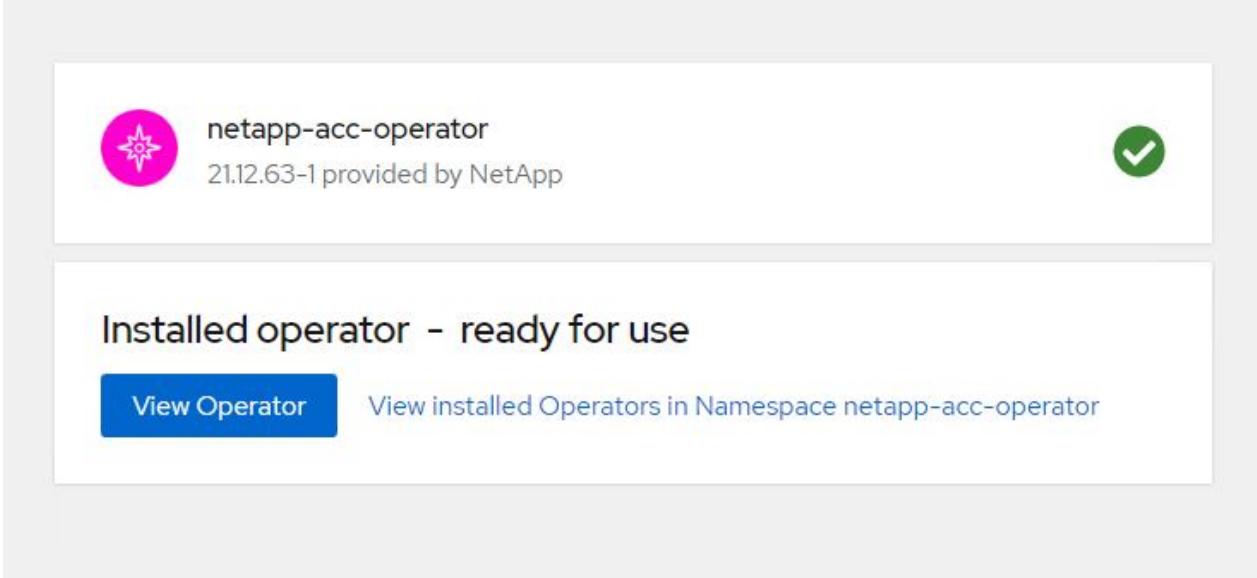
### Installing Operator

InstallWaiting: installing; waiting for deployment acc-operator-controller-manager to become ready: Waiting for rollout to finish: 0 of 1 updated replicas are available...

The Operator is being installed. This may take a few minutes.

[View installed Operators in Namespace netapp-acc-operator](#)

13. Once the operator installation succeeds, navigate to click on View Operator.



14. Then click on Create Instance in Astra Control Center tile in the operator.

A screenshot of the 'netapp-acc-operator' details page. The top navigation shows 'Installed Operators &gt; Operator details'. Below, the operator name 'netapp-acc-operator' and version '21.12.63-1 provided by NetApp' are displayed with a pink star icon. A horizontal menu bar includes 'Details' (which is underlined), 'YAML', 'Subscription', 'Events', and 'Astra Control Center'. The 'Details' tab is active. A section titled 'Provided APIs' contains a 'ACC Astra Control Center' button and a note: 'AstraControlCenter is the Schema for the astracontrolcenters API'. At the bottom is a 'Create instance' button with a plus sign icon.

15. Fill the Create AstraControlCenter form fields and click Create.

- Optionally edit the Astra Control Center instance name.
- Optionally enable or disable Auto Support. Retaining Auto Support functionality is recommended.
- Enter the FQDN for Astra Control Center.
- Enter the Astra Control Center version; the latest is displayed by default.
- Enter an account name for Astra Control Center and admin details like first name, last name and

email address.

- f. Enter the volume reclaim policy, default is Retain.
- g. In Image Registry, enter the FQDN for your registry along with the organization name as it was given while pushing the images to the registry (in this example, astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra)
- h. If you use a registry that requires authentication, enter the secret name in Image Registry section.
- i. Configure scaling options for Astra Control Center resource limits.
- j. Enter the storage class name if you want to place PVCs on a non-default storage class.
- k. Define CRD handling preferences.

Project: netapp-acc-operator ▾

**Name \***  
astra

**Labels**  
app=frontend

**Account Name \***  
HCG Solutions Engineering

Astra Control Center account name

**Astra Address \***  
astra-control-center.cie.netapp.com

AstraAddress defines how Astra will be found in the data center. This IP address and/or DNS A record must be created prior to provisioning Astra Control Center. Example - "astra.example.com" The A record and its IP address must be allocated prior to provisioning Astra Control Center

**Astra Version \***  
21.12.60

Version of AstraControlCenter to deploy. You are provided a Helm repository with a corresponding version. Example - 1.5.2, 1.4.2-patch

**Email \***  
solutions\_tme@netapp.com

EmailAddress will be notified by Astra as events warrant.

**Auto Support \*** ➤

AutoSupport indicates willingness to participate in NetApp's proactive support application, NetApp Active IQ. The default election is true and indicates support data will be sent to NetApp. An empty or blank election is the same as a default election. Air gapped installations should enter false.

**First Name**  
HCG

The first name of the SRE supporting Astra.

Last Name

The last name of the SRE supporting Astra.

**Image Registry**

The container image registry that is hosting the Astra application images, ACC Operator and ACC Helm Repository.

Name

The name of the image registry. For example "example.registry/astra". Do not prefix with protocol.

Secret

The name of the Kubernetes secret that will authenticate with the image registry.

Volume Reclaim Policy

Reclaim policy to be set for persistent volumes

Astra Resources Scaler

Default ▾

Scaling options for AstraControlCenter Resource limits.

Storage Class

The storage class to be used for PVCs. If not set, default storage class will be used.

Crd's

Options for how ACC should handle CRDs.

**Create** | **Cancel**

### Automated [Ansible]

1. For using the Ansible playbooks to deploy Astra Control Center, you will require a Ubuntu/RHEL machine with Ansible installed. Follow the procedure as described [here](#) for Ubuntu and in this [link](#) for RHEL.
2. Clone the GitHub repository that hosts the Ansible content.

```
git clone https://github.com/NetApp-Automation/na_astra_control_suite.git
```

3. Log into the NetApp Support Site and download the latest version of NetApp Astra Control Center. To do so requires a license attached to your NetApp account. After you download the tarball, transfer it to the workstation.



To get started with a trial license for Astra Control, visit the [Astra registration site](#).

4. Create or obtain a kubeconfig file with admin access to the OpenShift cluster on which Astra Control Center is to be installed.
5. Change the directory to the na\_astra\_control\_suite.

```
cd na_astra_control_suite
```

6. Edit the vars/vars.yml file and fill the variables with required information.

```
#Define whether or not to push the Astra Control Center images to  
your private registry [Allowed values: yes, no]  
push_images: yes  
  
#The directory hosting the Astra Control Center installer  
installer_directory: /home/admin/  
  
#Name of the Astra Control Center installer (Do not include the  
extension, just the name)  
astra_tar_ball_name: astra-control-center-21.12.60  
  
#The complete path to the kubeconfig file of the  
kubernetes/openshift cluster Astra Control Center needs to be  
installed to.  
hosting_ocp_kubeconfig_path: /home/admin/ocp-kubeconfig  
  
#Namespace in which Astra Control Center is to be installed  
astra_namespace: netapp-astra-cc  
  
#Astra Control Center Resources Scaler. Leave it blank if you want  
to accept the Default setting.  
astra_resources_scaler: Default  
  
#Storageclass to be used for Astra Control Center PVCs, it must be  
created before running the playbook [Leave it blank if you want the  
PVCs to use default storageclass]  
astra_trident_storageclass: basic  
  
#Reclaim Policy for Astra Control Center Persistent Volumes [Allowed  
values: Retain, Delete]  
storageclass_reclaim_policy: Retain  
  
#Private Registry Details  
astra_registry_name: "docker.io"  
  
#Whether the private registry requires credentials [Allowed values:  
yes, no]  
require_reg_creds: yes  
  
#If require_reg_creds is yes, then define the container image  
registry credentials
```

```

#Usually, the registry namespace and usernames are same for
individual users
astra_registry_namespace: "registry-user"
astra_registry_username: "registry-user"
astra_registry_password: "password"

#Kuberenets/OpenShift secret name for Astra Control Center
#This name will be assigned to the K8s secret created by the
playbook
astra_registry_secret_name: "astra-registry-credentials"

#Astra Control Center FQDN
acc_fqdn_address: astra-control-center-ui.cie.netapp.com

#Name of the Astra Control Center instance
acc_account_name: ACC Account Name

#Administrator details for Astra Control Center
admin_email_address: admin@example.com
admin_first_name: Admin
admin_last_name: Admin

```

- Run the playbook to deploy Astra Control Center. The playbook requires root privileges for certain configuration.

So if the user running the playbook is root or has passwordless sudo configured, then run the below command to run the playbook.

```
ansible-playbook playbook.yml
```

If the user has password-based sudo access configured, then run the below command to run the playbook and then enter the sudo password.

```
ansible-playbook playbook.yml -K
```

## Post Install Steps

- It might take several minutes for the installation to complete. Verify that all the pods and services in the netapp-astra-cc namespace are up and running.

```
[netapp-user@rhel7 ~]$ oc get all -n netapp-astra-cc
```

- Check the acc-operator-controller-manager logs to ensure that the installation is completed.

```
[netapp-user@rhel7 ~]$ oc logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f
```



The following message indicates the successful installation of Astra Control Center.

```
{"level":"info","ts":1624054318.029971,"logger":"controllers.AstraControlCenter","msg":"Successfully Reconciled AstraControlCenter in [seconds]s","AstraControlCenter":"netapp-astra-cc/astra","ae.Version":"[21.12.60]"}}
```

3. The username for logging into Astra Control Center is the email address of the administrator provided in the CRD file and the password is a string ACC- appended to the Astra Control Center UUID. Run the following command:

```
[netapp-user@rhel7 ~]$ oc get astracontrolcenters -n netapp-astra-cc  
NAME      UUID  
astra     345c55a5-bf2e-21f0-84b8-b6f2bce5e95f
```



In this example, the password is ACC-345c55a5-bf2e-21f0-84b8-b6f2bce5e95f.

4. Get the traefik service load balancer IP.

```
[netapp-user@rhel7 ~]$ oc get svc -n netapp-astra-cc | egrep 'EXTERNAL|traefik'  
  
NAME           TYPE        CLUSTER-IP  
EXTERNAL-IP    PORT(S)  
AGE  
traefik       LoadBalancer 172.30.99.142  
10.61.186.181 80:30343/TCP,443:30060/TCP  
16m
```

5. Add an entry in the DNS server pointing the FQDN provided in the Astra Control Center CRD file to the EXTERNAL-IP of the traefik service.

## New Host

X

Name (uses parent domain name if blank):

astra-control-center

Fully qualified domain name (FQDN):

astra-control-center.cie.netapp.com.

IP address:

10.61.186.181

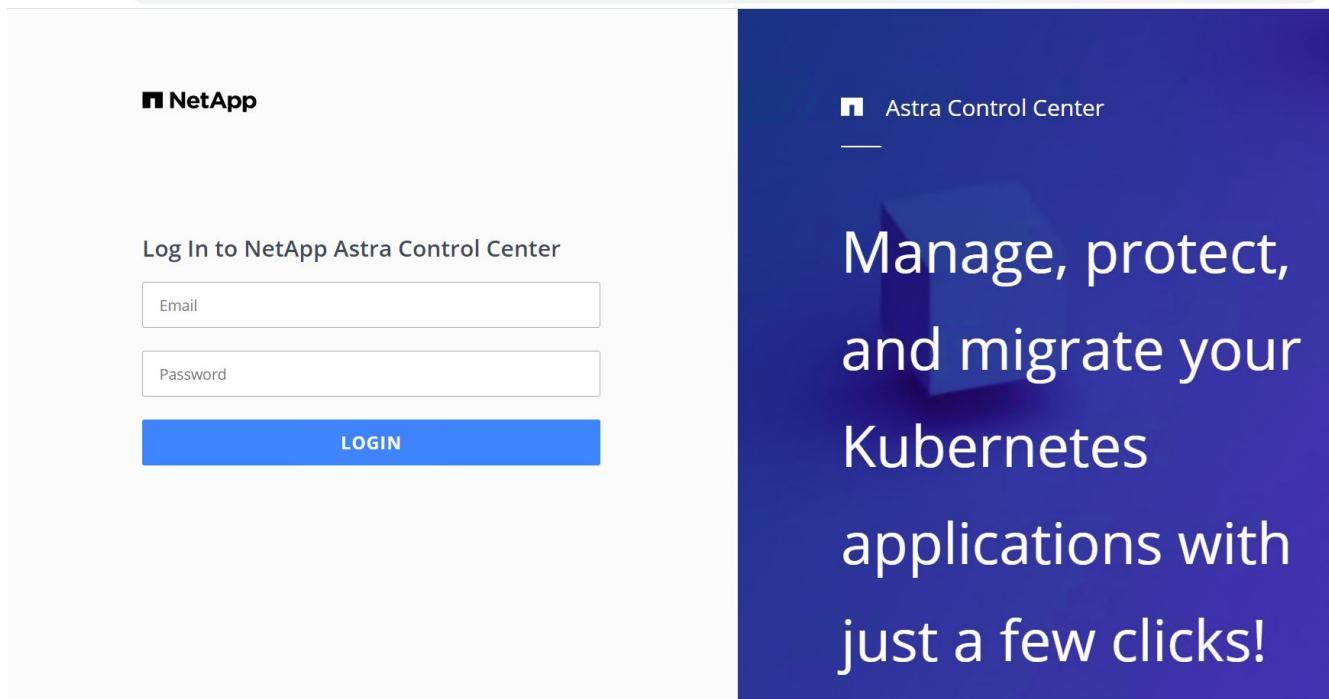
Create associated pointer (PTR) record

Allow any authenticated user to update DNS records with the same owner name

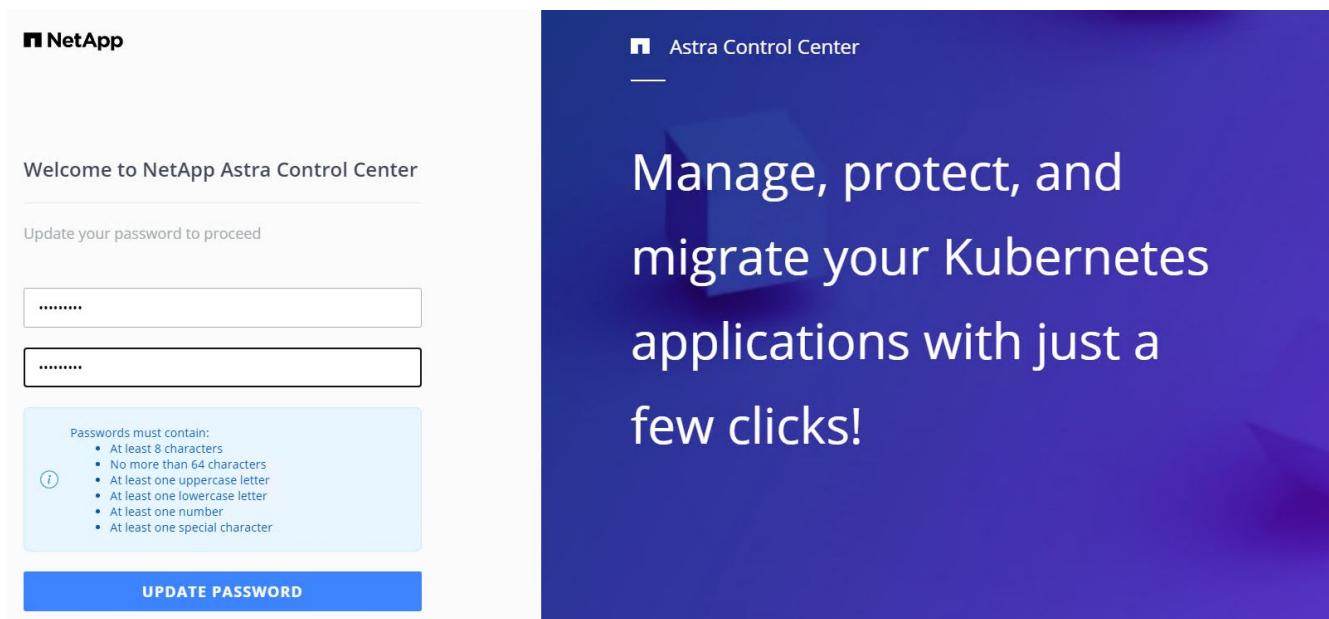
Add Host

Cancel

6. Log into the Astra Control Center GUI by browsing its FQDN.



- When you log into Astra Control Center GUI for the first time using the admin email address provided in CRD, you need to change the password.



- If you wish to add a user to Astra Control Center, navigate to Account > Users, click Add, enter the details of the user, and click Add.

**Add user**

**USER DETAILS**

First name Nikhil	Last name Kulkarni
Email address tme_nik@netapp.com	

**PASSWORD**

Temporary password *****	Confirm temporary password *****
-----------------------------	-------------------------------------

Passwords must contain:

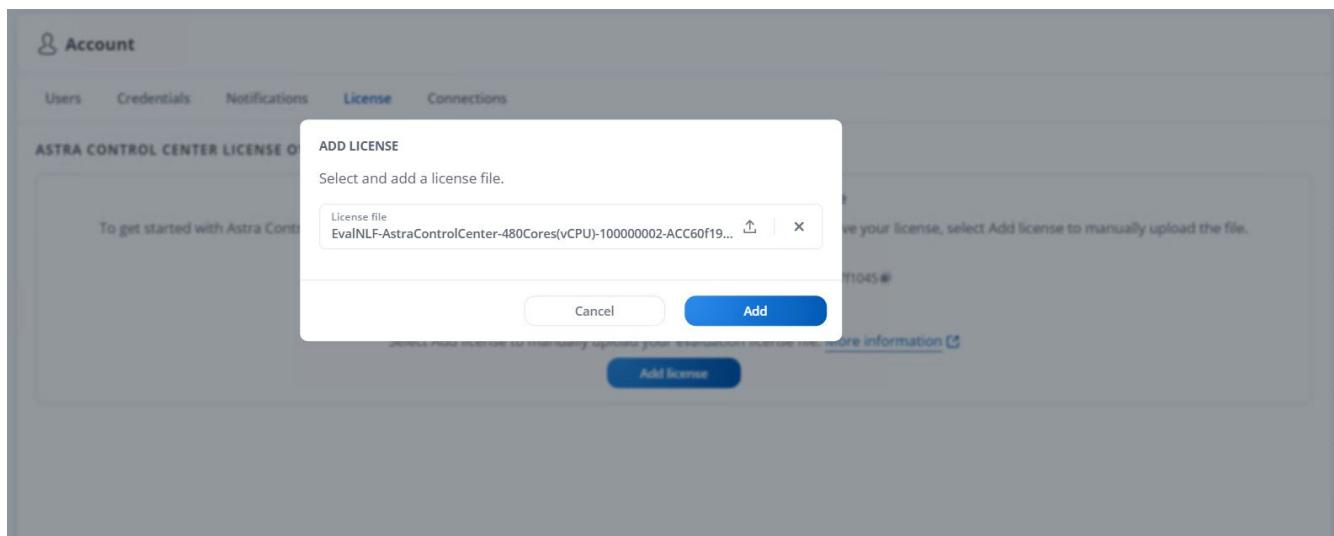
- At least 8 characters
- No more than 64 characters
- At least one lowercase letter
- At least one uppercase letter
- At least one number
- At least one special character

**USER ROLE**

Role Owner
---------------

Cancel
Add ✓

9. Astra Control Center requires a license for all of its functionalities to work. To add a license, navigate to Account > License, click Add License, and upload the license file.



If you encounter issues with the install or configuration of NetApp Astra Control Center, the knowledge base of known issues is available [here](#).

Next: Register your Red Hat OpenShift Clusters: Red Hat OpenShift with NetApp.

#### Register your Red Hat OpenShift Clusters with the Astra Control Center

To enable the Astra Control Center to manage your workloads, you must first register your Red Hat OpenShift cluster.

## Register Red Hat OpenShift clusters

1. The first step is to add the OpenShift clusters to the Astra Control Center and manage them. Go to Clusters and click Add a Cluster, upload the kubeconfig file for the OpenShift cluster, and click Select Storage.

The screenshot shows the 'Add cluster' wizard in progress, specifically Step 1/3: CREDENTIALS. On the left, there's a file upload interface with a button to 'Upload file' or 'Paste from clipboard'. A file named 'ocp-vmw kubeconfig.txt' is listed with options to upload or remove it. To the right of the file list is a field labeled 'Credential name' containing 'ocp-vmw'. On the far right, a sidebar titled 'ADDING A CLUSTER' contains instructions: 'Adding a cluster is needed for Astra Control to discover your Kubernetes applications.', 'Select a cloud provider and input credentials to get started.', and a link 'Read more in Clusters'. At the bottom of the main panel are 'Cancel' and 'Configure storage →' buttons.



The kubeconfig file can be generated to authenticate with a username and password or a token. Tokens expire after a limited amount of time and might leave the registered cluster unreachable. NetApp recommends using a kubeconfig file with a username and password to register your OpenShift clusters to Astra Control Center.

2. Astra Control Center detects the eligible storage classes. Now select the way that storageclass provisions volumes using Trident backed by an SVM on NetApp ONTAP and click Review. In the next pane, verify the details and click Add Cluster.

Set default	Storage class	Storage provisioner	Reclaim policy	Binding mode	Eligible
<input checked="" type="radio"/>	ocp-trident <small>Default</small>	csi.trident.netapp.io	Delete	Immediate	<span style="color: green;">✓</span>
<input type="radio"/>	ocp-trident-iscsi	csi.trident.netapp.io	Delete	Immediate	<span style="color: green;">✓</span>
<input type="radio"/>	project-1-sc	csi.trident.netapp.io	Delete	Immediate	<span style="color: orange;">⚠</span>
<input type="radio"/>	thin	kubernetes.io/vsphere-volume	Delete	Immediate	<span style="color: orange;">⚠</span>

[← Select credentials](#) [Review →](#)

3. Register both OpenShift clusters as described in step 1. When added, the clusters move to the Discovering status while Astra Control Center inspects them and installs the necessary agents. Cluster status changes to Running after they are successfully registered.

Name	Ready	Type	Version	Actions
ocp-vmw	<span style="color: green;">✓</span>	Red Hat OpenShift	v1.20.0+df9c838	<span style="color: green;">Running</span>
ocp-vmware2	<span style="color: green;">✓</span>	Red Hat OpenShift	v1.20.0+c8905da	<span style="color: green;">Running</span>



All Red Hat OpenShift clusters to be managed by Astra Control Center should have access to the image registry that was used for its installation as the agents installed on the managed clusters pull the images from that registry.

4. Import ONTAP clusters as storage resources to be managed as backends by Astra Control Center. When OpenShift clusters are added to Astra and a storageclass is configured, it automatically discovers and inspects the ONTAP cluster backing the storageclass but does not import it into the Astra Control Center to be managed.

- To import the ONTAP clusters, go to Backends, click the dropdown, and select Manage next to the ONTAP cluster to be managed. Enter the ONTAP cluster credentials, click Review Information, and then click Import Storage Backend.

- After the backends are added, the status changes to Available. These backends now have the information about the persistent volumes in the OpenShift cluster and the corresponding volumes on the ONTAP system.

Name	Status	Capacity	Type	Actions
K8s-OnTap	✓	0.11/1.07 TiB: 9.9%	ONTAP 9.8.0	<span>Available</span>
ONTAP-Select-02	✓	0.07/2.07 TiB: 3.3%	ONTAP 9.8.0	<span>Available</span>

7. For backup and restore across OpenShift clusters using Astra Control Center, you must provision an object storage bucket that supports the S3 protocol. Currently supported options are ONTAP S3, StorageGRID, and AWS S3. For the purpose of this installation, we are going to configure an AWS S3 bucket. Go to Buckets, click Add bucket, and select Generic S3. Enter the details about the S3 bucket and credentials to access it, click the checkbox "Make this bucket the default bucket for the cloud," and then click Add.

### Add bucket

**STORAGE BUCKET**

Enter the access details of your existing object store bucket to allow Astra Control to store your application backups.

Type <input checked="" type="checkbox"/> Generic S3	Existing bucket name ocp-vmware2-astra-cc
Description (optional)	S3 server name or IP address s3.us-east-1.amazonaws.com
<input checked="" type="checkbox"/> Make this bucket the default bucket for this cloud	

**SELECT CREDENTIALS**

Astra Control requires S3 access credentials with the roles necessary to facilitate Kubernetes application data management.

<input checked="" type="radio"/> Add	<input type="radio"/> Use existing
Access ID AMWSTCFKDSU6HWSZXABD	Secret key .....
Credential name AWS-S3	

**ADDING STORAGE BUCKETS**

Astra Control stores backups in your existing object store buckets. The first bucket added for a selected cloud will be designated as the default bucket for backup and clone operations.

Read more in [storage buckets](#).

Next: Choose the Applications To Protect.

#### Choose the applications to protect

After you have registered your Red Hat OpenShift clusters, you can discover the applications that are deployed and manage them via the Astra Control Center.

## Manage applications

- After the OpenShift clusters and ONTAP backends are registered with the Astra Control Center, the control center automatically starts discovering the applications in all the namespaces that are using the storageclass configured with the specified ONTAP backend.

The screenshot shows the Astra Control Center interface. On the left, there's a sidebar with navigation links: Dashboard, MANAGE YOUR APPS (highlighted in blue), Apps, Clusters, MANAGE YOUR STORAGE (Backend and Buckets), and MANAGE YOUR ACCOUNT (Account, Activity, Support). The main area is titled 'Apps' and shows a table of discovered applications. The columns are: Name, Ready, Cluster, Group, Discovered, and Actions. There are 29 entries listed. Some applications are marked as 'Managed' (indicated by a star icon) and others as 'Unmanaged'. One application, 'hive', is currently 'Discovering'. The status bar at the bottom right shows '1-25 of 29 entries'.

Name	Ready	Cluster	Group	Discovered	Actions
acc-operator-system	✓	ocp-vmware2	acc-operator-system	2021/07/29 11:11 UTC	Unmanaged
acc-operator-system	✓	ocp-vmw	acc-operator-system	2021/07/29 11:09 UTC	Unmanaged
default	✓	ocp-vmw	default	2021/07/29 11:09 UTC	Unmanaged
default	✓	ocp-vmware2	default	2021/07/29 11:11 UTC	Unmanaged
hive	✓	ocp-vmware2	hive	2021/07/29 11:11 UTC	Unmanaged
local-cluster	●	ocp-vmware2	local-cluster	2021/07/29 11:45 UTC	Discovering

2. Navigate to Apps > Discovered and click the dropdown menu next to the application you would like to manage using Astra. Then click Manage.

This screenshot is similar to the previous one, showing the Astra Control Center interface. The sidebar and main 'Apps' section are identical. However, in the 'Actions' column for the application 'wordpress-astra-fd2aa', a context menu is open with three options: 'Manage', 'Ignore', and 'Discovering'. The 'Manage' option is highlighted with a yellow background and a black outline. The status bar at the bottom right shows '1-25 of 29 entries'.

Name	Ready	Cluster	Group	Discovered	Actions
wordpress-astra-fd4f9	✓	ocp-vmw	wordpress-astra-fd4f9	2021/07/29 11:09 UTC	Unmanaged
wordpress-astra-fd2aa	●	ocp-vmware2	wordpress-astra-fd2aa	2021/07/29 11:11 UTC	Manage
wordpress-astra-5eeb9	●	ocp-vmware2	wordpress-astra-5eeb9	2021/07/29 11:11 UTC	Ignore
wordpress-astra-5ed9e	✓	ocp-vmw	wordpress-astra-5ed9e	2021/07/29 11:09 UTC	Discovering
wordpress-astra	✓	ocp-vmw	wordpress-astra	2021/07/29 11:09 UTC	Unmanaged
wordpress	●	ocp-vmw	wordpress	2021/07/29 11:09 UTC	Discovering

1. The application enters the Available state and can be viewed under the Managed tab in the Apps section.

The screenshot shows the 'Apps' section of the Astra Control Center. At the top, there are buttons for 'Actions', '+ Define', 'All Clusters' (with a dropdown), 'Search', 'Managed' (with a star icon), 'Discovered' (with a count of 175), and 'Ignored'. Below this is a table header with columns: Name, Ready, Protected, Cluster, Group, Discovered, and Actions. A single row is listed: 'wordpress-astra-ff4f9' (Ready, Protected, Cluster: ocp-vmw, Group: wordpress-astra-ff4f9, Discovered: 2021/07/29 11:09 UTC, Actions: Available). Below the table, it says '1-1 of 1 entries'.

[Next: Protect Your applications.](#)

### Protect your applications

After application workloads are managed by Astra Control Center, you can configure the protection settings for those workloads.

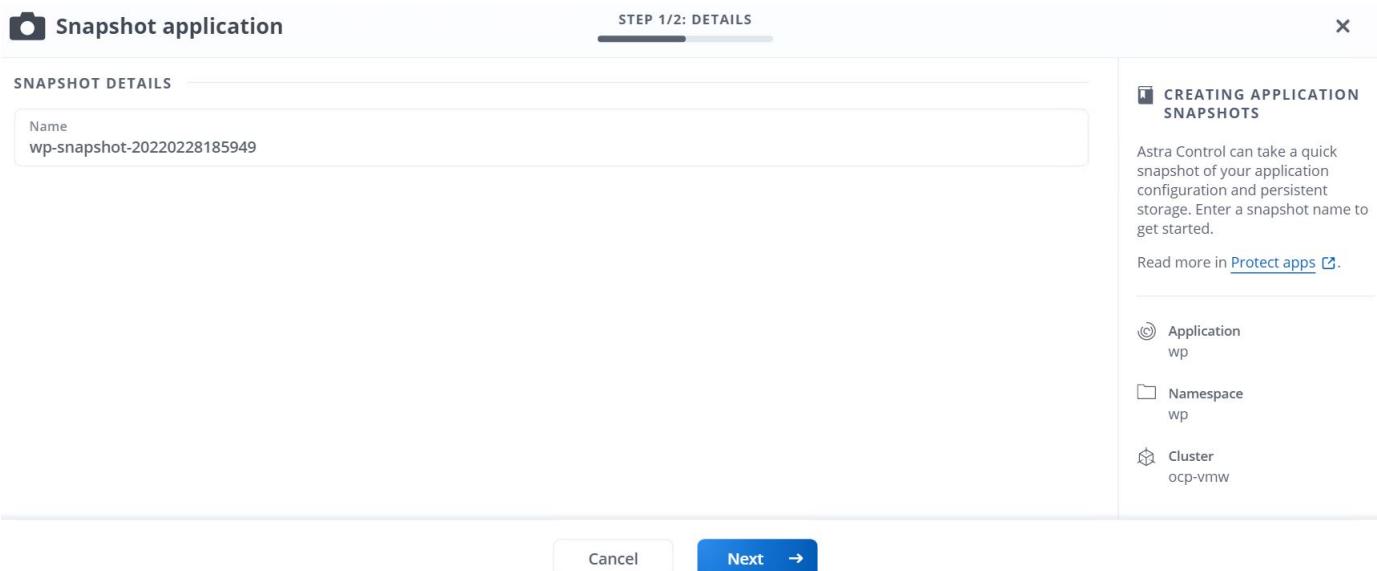
#### Creating an application snapshot

A snapshot of an application creates an ONTAP Snapshot copy that can be used to restore or clone the application to a specific point in time based on that Snapshot copy.

1. To take a snapshot of the application, navigate to the Apps > Managed tab and click the application you would like to make a Snapshot copy of. Click the dropdown menu next to the application name and click Snapshot.

The screenshot shows the application details for 'wp'. It has two main sections: 'APPLICATION STATUS' (Healthy) and 'APPLICATION PROTECTION STATUS' (Unprotected). Under 'Images', it lists 'docker.io/bitnami/mariadb:10.5.13-debian-10-r58' and 'docker.io/bitnami/wordpress:5.9.0-debian-10-r1'. Under 'Protection schedule', it shows 'Disabled'. The 'Group' is 'wp'. On the right, there's a dropdown menu with options: Running (selected), Snapshot, Backup, Clone, Restore, and Unmanage. The 'Cluster' dropdown shows 'ocp-vmw'.

2. Enter the snapshot details, click Next, and then click Snapshot. It takes about a minute to create the snapshot, and the status becomes Available after the snapshot is successfully created.



## Creating an application backup

A backup of an application captures the active state of the application and the configuration of its resources, converts them into files, and stores them in a remote object storage bucket.

For the backup and restore of managed applications in the Astra Control Center, you must configure superuser settings for the backing ONTAP systems as a prerequisite. To do so, enter the following commands.

```
ONTAP::> export-policy rule modify -vserver ocp-trident -policyname
default -ruleindex 1 -superuser sys
ONTAP::> export-policy rule modify -policyname default -ruleindex 1 -anon
65534 -vserver ocp-trident
```

- To create a backup of the managed application in the Astra Control Center, navigate to the Apps > Managed tab and click the application that you want to take a backup of. Click the dropdown menu next to the application name and click Backup.

Images	Protection schedule	Group	Cluster
docker.io/bitnami/mariadb:10.5.13-debian-10-r58 docker.io/bitnami/wordpress:5.9.0-debian-10-r1	Disabled	wp	ocp-vmw

- Enter the backup details, select the object storage bucket to hold the backup files, click Next, and, after reviewing the details, click Backup. Depending on the size of the application and data, the backup can take several minutes, and the status of the backup becomes Available after the backup is completed successfully.

**STEP 1/2: DETAILS**

**BACKUP DETAILS**

Name: wp-backup

Backup from an existing snapshot [?](#)

**BACKUP DESTINATION**

Bucket: na-ocp-astra/na-ocp-acc [Available](#)

**CREATING APPLICATION BACKUPS**

Astra Control can take a backup of your application configuration and persistent storage. Persistent storage backups are transferred to your object store. Enter a backup name to get started.

Read more in [Application backups](#).

**wp**

- Application: wp
- Namespace: wp
- Cluster: ocp-vmw

[Cancel](#) [Next →](#)

## Restoring an application

At the push of a button, you can restore an application to the originating namespace in the same cluster or to a remote cluster for application protection and disaster recovery purposes.

1. To restore an application, navigate to Apps > Managed tab and click the app in question. Click the dropdown menu next to the application name and click **Restore**.

**wp**

**APPLICATION STATUS**  
Healthy

**APPLICATION PROTECTION STATUS**  
Partially protected

**Images**  
docker.io/bitnami/mariadb:10.5.13-debian-10-r58  
docker.io/bitnami/wordpress:5.9.0-debian-10-r1

**Protection schedule**  
Disabled

**Group**  
wp

**Cluster**  
ocp-vmw

**Running** [▼](#)

- Snapshot
- Backup
- Clone
- Restore
- Unmanage

2. Enter the name of the restore namespace, select the cluster you want to restore it to, and choose if you want to restore it from an existing snapshot or from a backup of the application. Click **Next**.

**Restore application**

**STEP 1/2: DETAILS**

**RESTORE DETAILS**

Destination cluster	ocp-vmw	Destination namespace	wp
---------------------	---------	-----------------------	----

**RESTORE SOURCE**

Application backup			
	Ready	On-Schedule/On-Demand	Created ↑
<input checked="" type="radio"/> wp-backup	<span>✓</span>	<span>🕒</span> On-Demand	2022/02/28 18:54 UTC

**RESTORING APPLICATIONS**

Astra Control can restore your application configuration and persistent storage. Select a source snapshot or backup for the restored application.

- Application wp
- Namespace wp
- Cluster ocp-vmw

**Cancel** **Next →**

3. On the review pane, enter `restore` and click Restore after you have reviewed the details.

**Restore application**

**STEP 2/2: SUMMARY**

**REVIEW RESTORE INFORMATION**

**⚠️** All existing resources associated with this application will be deleted and replaced with the source backup "wp-backup" taken on 2022/02/28 18:54 UTC. Persistent volumes will be deleted and recreated. External resources with dependencies on this application may be impacted.

We recommend taking a snapshot or a backup of your application before proceeding.

<b>BACKUP</b> wp-backup	<b>RESTORE</b> wp
<b>ORIGINAL GROUP</b> wp	<b>DESTINATION GROUP</b> wp
<b>ORIGINAL CLUSTER</b> ocp-vmw	<b>DESTINATION CLUSTER</b> ocp-vmw
<b>RESOURCE LABELS</b> ClusterRole kubernetes.io/bootstrapping:rbac-defaults +1 ClusterRoleBinding	<b>RESOURCE LABELS</b> ClusterRole kubernetes.io/bootstrapping:rbac-defaults +1 ClusterRoleBinding

Are you sure you want to restore the application "wp"?

Type `restore` below to confirm.

Confirm to restore  
`restore`

**Back** **Restore ✓**

4. The new application goes to the Restoring state while Astra Control Center restores the application on the selected cluster. After all the resources of the application are installed and detected by Astra, the application goes to the Available state.

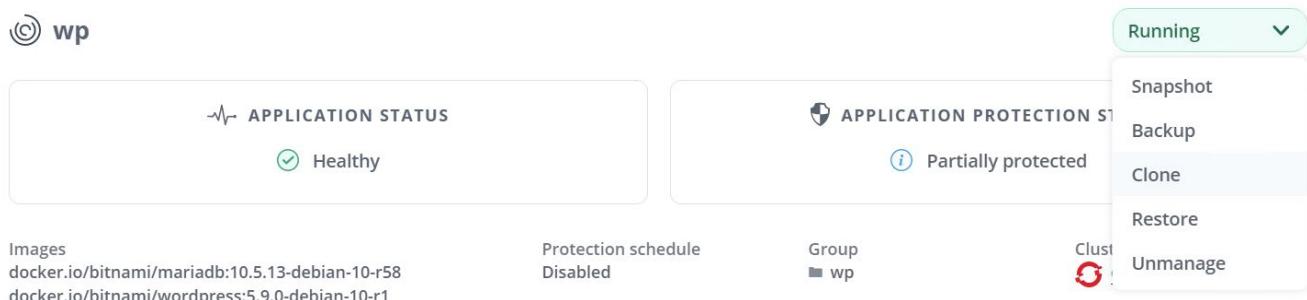
## Applications

Actions		+ Define	Actions	Search	Star	110	Reset
C   1-1 of 1 entries < >							
	Name	Ready	Protected	Cluster	Group	Discovered	Actions
<input type="checkbox"/>	wp			ocp-vmw	■ wp	2022/02/28 18:34 UTC	<span>Available</span>

### Cloning an application

You can clone an application to the originating cluster or to a remote cluster for dev/test or application protection and disaster recovery purposes. Cloning an application within the same cluster on the same storage backend uses NetApp FlexClone technology, which clones the PVCs instantly and saves storage space.

1. To clone an application, navigate to the Apps > Managed tab and click the app in question. Click the dropdown menu next to the application name and click Clone.



2. Enter the details of the new namespace, select the cluster you want to clone it to, and choose if you want to clone it from an existing snapshot or a backup or the current state of the application. Then click Next and click Clone on review pane once you have reviewed the details.

The screenshot shows the 'Clone application' wizard. The 'Clone DETAILS' section includes fields for 'Clone name' (wp-clone), 'Clone namespace' (wp-clone), 'Destination cluster' (ocp-vmw), and a checkbox for 'Clone from an existing snapshot or backup'. The right panel, titled 'CLONING APPLICATIONS', provides information about cloning and lists the source application ('wp'), its namespace ('wp'), and cluster ('ocp-vmw').

3. The new application goes to the Discovering state while Astra Control Center creates the application on the

selected cluster. After all the resources of the application are installed and detected by Astra, the application goes to the Available state.

## ⌚ Applications

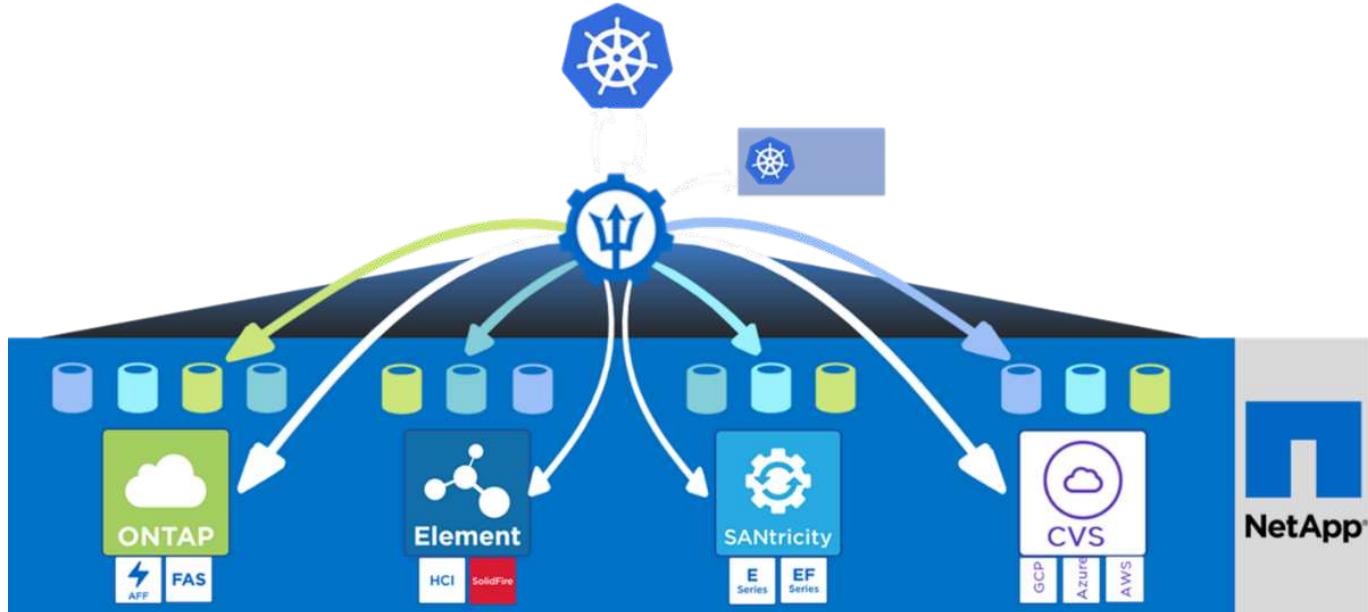
Applications						
	Name	Ready	Protected	Cluster	Group	Discovered
<input type="checkbox"/>	<a href="#">wp</a>			ocp-vmw	■ wp	2022/02/28 18:34 UTC
<input type="checkbox"/>	<a href="#">wp-clone</a>			ocp-vmw	■ wp-clone	2022/02/28 19:21 UTC

Next: Solution Validation/Use Cases.

## Astra Trident Overview

Astra Trident is an open-source and fully supported storage orchestrator for containers and Kubernetes distributions, including Red Hat OpenShift. Trident works with the entire NetApp storage portfolio, including the NetApp ONTAP and Element storage systems, and it also supports NFS and iSCSI connections. Trident accelerates the DevOps workflow by allowing end users to provision and manage storage from their NetApp storage systems without requiring intervention from a storage administrator.

An administrator can configure a number of storage backends based on project needs and storage system models that enable advanced storage features, including compression, specific disk types, or QoS levels that guarantee a certain level of performance. After they are defined, these backends can be used by developers in their projects to create persistent volume claims (PVCs) and to attach persistent storage to their containers on demand.



Astra Trident has a rapid development cycle, and just like Kubernetes, is released four times a year.

The latest version of Astra Trident is 22.01 released in January 2022. A support matrix for what version of Trident has been tested with which Kubernetes distribution can be found [here](#).

Starting with the 20.04 release, Trident setup is performed by the Trident operator. The operator makes large scale deployments easier and provides additional support including self healing for pods that are deployed as a part of the Trident install.

With the 21.01 release, a Helm chart was made available to ease the installation of the Trident Operator.

### Download Astra Trident

To install Trident on the deployed user cluster and provision a persistent volume, complete the following steps:

1. Download the installation archive to the admin workstation and extract the contents. The current version of Trident is 22.01, which can be downloaded [here](#).

```
[netapp-user@rhel7 ~]$ wget
https://github.com/NetApp/trident/releases/download/v22.01.0/trident-
installer-22.01.0.tar.gz
--2021-05-06 15:17:30--
https://github.com/NetApp/trident/releases/download/v22.01.0/trident-
installer-22.01.0.tar.gz
Resolving github.com (github.com) ... 140.82.114.3
Connecting to github.com (github.com)|140.82.114.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github-
releases.githubusercontent.com/77179634/a4fa9f00-a9f2-11eb-9053-
98e8e573d4ae?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIWNJYAX4CSVEH53A%2F20210506%2Fus-east-
1%2Fs3%2Faws4_request&X-Amz-Date=20210506T191643Z&X-Amz-Expires=300&X-
Amz-
Signature=8a49a2a1e08c147d1ddd8149ce45a5714f9853fee19bb1c507989b9543eb36
30&X-Amz-
SignedHeaders=host&actor_id=0&key_id=0&repo_id=77179634&response-
content-disposition=attachment%3B%20filename%3Dtrident-installer-
22.01.0.tar.gz&response-content-type=application%2Foctet-stream
[following]
--2021-05-06 15:17:30-- https://github-
releases.githubusercontent.com/77179634/a4fa9f00-a9f2-11eb-9053-
98e8e573d4ae?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIWNJYAX4CSVEH53A%2F20210506%2Fus-east-
1%2Fs3%2Faws4_request&X-Amz-Date=20210506T191643Z&X-Amz-Expires=300&X-
Amz-
Signature=8a49a2a1e08c147d1ddd8149ce45a5714f9853fee19bb1c507989b9543eb36
30&X-Amz-
SignedHeaders=host&actor_id=0&key_id=0&repo_id=77179634&response-
content-disposition=attachment%3B%20filename%3Dtrident-installer-
22.01.0.tar.gz&response-content-type=application%2Foctet-stream
```

```
Resolving github-releases.githubusercontent.com (github-releases.githubusercontent.com) ... 185.199.108.154, 185.199.109.154, 185.199.110.154, ...
Connecting to github-releases.githubusercontent.com (github-releases.githubusercontent.com)|185.199.108.154|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 38349341 (37M) [application/octet-stream]
Saving to: 'trident-installer-22.01.0.tar.gz'

100%[=====] 38,349,341 88.5MB/s
in 0.4s

2021-05-06 15:17:30 (88.5 MB/s) - 'trident-installer-22.01.0.tar.gz'
saved [38349341/38349341]
```

## 2. Extract the Trident install from the downloaded bundle.

```
[netapp-user@rhel7 ~]$ tar -xzf trident-installer-22.01.0.tar.gz
[netapp-user@rhel7 ~]$ cd trident-installer/
[netapp-user@rhel7 trident-installer]$
```

### Install the Trident Operator with Helm

1. First set the location of the user cluster's kubeconfig file as an environment variable so that you don't have to reference it, because Trident has no option to pass this file.

```
[netapp-user@rhel7 trident-installer]$ export KUBECONFIG=~/ocp-install/auth/kubeconfig
```

2. Run the Helm command to install the Trident operator from the tarball in the helm directory while creating the trident namespace in your user cluster.

```
[netapp-user@rhel7 trident-installer]$ helm install trident
helm/trident-operator-22.01.0.tgz --create-namespace --namespace trident
NAME: trident
LAST DEPLOYED: Fri May  7 12:54:25 2021
NAMESPACE: trident
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
Thank you for installing trident-operator, which will deploy and manage
NetApp's Trident CSI
storage provisioner for Kubernetes.
```

Your release is named 'trident' and is installed into the 'trident' namespace.

Please note that there must be only one instance of Trident (and trident-operator) in a Kubernetes cluster.

To configure Trident to manage storage resources, you will need a copy of tridentctl, which is available in pre-packaged Trident releases. You may find all Trident releases and source code online at <https://github.com/NetApp/trident>.

To learn more about the release, try:

```
$ helm status trident
$ helm get all trident
```

3. You can verify that Trident is successfully installed by checking the pods that are running in the namespace or by using the tridentctl binary to check the installed version.

```
[netapp-user@rhel7 trident-installer]$ oc get pods -n trident
NAME                      READY   STATUS    RESTARTS   AGE
trident-csi-5z451          1/2     Running   2          30s
trident-csi-696b685cf8-htdb2 6/6     Running   0          30s
trident-csi-b74p2          2/2     Running   0          30s
trident-csi-lrw4n          2/2     Running   0          30s
trident-operator-7c748d957-gr2gw 1/1     Running   0          36s

[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident version
+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 22.01.0        | 22.01.0       |
+-----+-----+
```

 In some cases, customer environments might require the customization of the Trident deployment. In these cases, it is also possible to manually install the Trident operator and update the included manifests to customize the deployment.

#### Manually install the Trident Operator

1. First, set the location of the user cluster's `kubeconfig` file as an environment variable so that you don't have to reference it, because Trident has no option to pass this file.

```
[netapp-user@rhel7 trident-installer]$ export KUBECONFIG=~/ocp-install/auth/kubeconfig
```

2. The `trident-installer` directory contains manifests for defining all the required resources. Using the appropriate manifests, create the `TridentOrchestrator` custom resource definition.

```
[netapp-user@rhel7 trident-installer]$ oc create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.yaml
customresourcedefinition.apiextensions.k8s.io/tridentorchestrators.tride
nt.netapp.io created
```

3. If one does not exist, create a Trident namespace in your cluster using the provided manifest.

```
[netapp-user@rhel7 trident-installer]$ oc apply -f deploy/namespace.yaml
namespace/trident created
```

4. Create the resources required for the Trident operator deployment, such as a `ServiceAccount` for the operator, a `ClusterRole` and `ClusterRoleBinding` to the `ServiceAccount`, a dedicated `PodSecurityPolicy`, or the operator itself.

```
[netapp-user@rhel7 trident-installer]$ oc create -f deploy/bundle.yaml
serviceaccount/trident-operator created
clusterrole.rbac.authorization.k8s.io/trident-operator created
clusterrolebinding.rbac.authorization.k8s.io/trident-operator created
deployment.apps/trident-operator created
podsecuritypolicy.policy/tridentoperatorpods created
```

5. You can check the status of the operator after it's deployed with the following commands:

```
[netapp-user@rhel7 trident-installer]$ oc get deployment -n trident
NAME           READY   UP-TO-DATE   AVAILABLE   AGE
trident-operator   1/1      1          1          23s
[netapp-user@rhel7 trident-installer]$ oc get pods -n trident
NAME                           READY   STATUS    RESTARTS   AGE
trident-operator-66f48895cc-lzczk   1/1     Running   0          41s
```

6. With the operator deployed, we can now use it to install Trident. This requires creating a TridentOrchestrator.

```
[netapp-user@rhel7 trident-installer]$ oc create -f
deploy/crds/tridentorchestrator_cr.yaml
tridentorchestrator.trident.netapp.io/trident created
[netapp-user@rhel7 trident-installer]$ oc describe torc trident
Name:          trident
Namespace:
Labels:        <none>
Annotations:   <none>
API Version:  trident.netapp.io/v1
Kind:          TridentOrchestrator
Metadata:
  Creation Timestamp:  2021-05-07T17:00:28Z
  Generation:        1
  Managed Fields:
    API Version:  trident.netapp.io/v1
    Fields Type:  FieldsV1
    fieldsV1:
      f:spec:
        ..
      f:debug:
      f:namespace:
  Manager:      kubectl-create
  Operation:    Update
  Time:         2021-05-07T17:00:28Z
  API Version:  trident.netapp.io/v1
```

```

Fields Type: FieldsV1
fieldsV1:
  f:status:
    .:
  f:currentInstallationParams:
    .:
    f:IPv6:
    f:autosupportHostname:
    f:autosupportImage:
    f:autosupportProxy:
    f:autosupportSerialNumber:
    f:debug:
    f:enableNodePrep:
    f:imagePullSecrets:
    f:imageRegistry:
    f:k8sTimeout:
    f:kubeletDir:
    f:logFormat:
    f:silenceAutosupport:
    f:tridentImage:
    f:message:
    f:namespace:
    f:status:
    f:version:
  Manager:          trident-operator
  Operation:        Update
  Time:            2021-05-07T17:00:28Z
  Resource Version: 931421
  Self Link:
  /apis/trident.netapp.io/v1/tridentorchestrators/trident
  UID:             8a26a7a6-dde8-4d55-9b66-a7126754d81f
Spec:
  Debug:           true
  Namespace:       trident
Status:
  Current Installation Params:
    IPv6:             false
    Autosupport Hostname:
    Autosupport Image: netapp/trident-autosupport:21.01
    Autosupport Proxy:
    Autosupport Serial Number:
    Debug:            true
    Enable Node Prep: false
    Image Pull Secrets:
    Image Registry:
    k8sTimeout:       30

```

```

Kubelet Dir:          /var/lib/kubelet
Log Format:           text
Silence Autosupport: false
Trident Image:        netapp/trident:22.01.0
Message:               Trident installed
Namespace:             trident
Status:                Installed
Version:               v22.01.0

Events:
Type    Reason     Age   From                  Message
----  -----  ----  -----
Normal  Installing  80s  trident-operator.netapp.io  Installing
Trident
Normal  Installed   68s  trident-operator.netapp.io  Trident
installed

```

7. You can verify that Trident is successfully installed by checking the pods that are running in the namespace or by using the `tridentctl` binary to check the installed version.

```

[netapp-user@rhel7 trident-installer]$ oc get pods -n trident
NAME                           READY   STATUS    RESTARTS   AGE
trident-csi-bb64c6cb4-lmd6h      6/6     Running   0          82s
trident-csi-gn59q                 2/2     Running   0          82s
trident-csi-m4szj                 2/2     Running   0          82s
trident-csi-sb9k9                 2/2     Running   0          82s
trident-operator-66f48895cc-lzczk  1/1     Running   0          2m39s

[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident version
+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 22.01.0          | 22.01.0          |
+-----+-----+

```

## Prepare worker nodes for storage

### NFS

Most Kubernetes distributions come with the packages and utilities to mount NFS backends installed by default, including Red Hat OpenShift.

However, for NFSv3, there is no mechanism to negotiate concurrency between the client and the server. Hence the maximum number of client-side sunrpc slot table entries must be manually synced with supported value on the server to ensure the best performance for the NFS connection without the server having to decrease the window size of the connection.

For ONTAP, the supported maximum number of sunrpc slot table entries is 128 i.e. ONTAP can serve 128

concurrent NFS requests at a time. However, by default, Red Hat CoreOS/Red Hat Enterprise Linux has maximum of 65,536 sunrpc slot table entries per connection. We need to set this value to 128 and this can be done using Machine Config Operator (MCO) in OpenShift.

To modify the maximum sunrpc slot table entries in OpenShift worker nodes, complete the following steps:

1. Log into the OCP web console and navigate to Compute > Machine Configs. Click Create Machine Config. Copy and paste the YAML file and click Create.

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  name: 98-worker-nfs-rpc-slot-tables
  labels:
    machineconfiguration.openshift.io/role: worker
spec:
  config:
    ignition:
      version: 3.2.0
    storage:
      files:
        - contents:
            source: data:text/plain;charset=utf-
8;base64,b3B0aW9ucyBzdW5ycGMgdGNwX21heF9zbG90X3RhYmx1X2VudHJpZXM9MTI4Cg==
=
          filesystem: root
          mode: 420
          path: /etc/modprobe.d/sunrpc.conf
```

2. After the MCO is created, the configuration needs to be applied on all worker nodes and rebooted one by one. The whole process takes approximately 20 to 30 minutes. Verify whether the machine config is applied by using `oc get mcp` and make sure that the machine config pool for workers is updated.

```
[netapp-user@rhel7 openshift-deploy]$ oc get mcp
NAME      CONFIG                      UPDATED     UPDATING
DEGRADED
master    rendered-master-a520ae930e1d135e0dee7168   True       False
False
worker    rendered-worker-de321b36eeba62df41feb7bc   True       False
False
```

## iSCSI

To prepare worker nodes to allow for the mapping of block storage volumes through the iSCSI protocol, you must install the necessary packages to support that functionality.

In Red Hat OpenShift, this is handled by applying an MCO (Machine Config Operator) to your cluster after it is deployed.

To configure the worker nodes to run iSCSI services, complete the following steps:

1. Log into the OCP web console and navigate to Compute > Machine Configs. Click Create Machine Config. Copy and paste the YAML file and click Create.

When not using multipathing:

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  labels:
    machineconfiguration.openshift.io/role: worker
  name: 99-worker-element-iscsi
spec:
  config:
    ignition:
      version: 3.2.0
    systemd:
      units:
        - name: iscsid.service
          enabled: true
          state: started
  osImageURL: ""
```

When using multipathing:

```

apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  name: 99-worker-ontap-iscsi
  labels:
    machineconfiguration.openshift.io/role: worker
spec:
  config:
    ignition:
      version: 3.2.0
    storage:
      files:
        - contents:
            source: data:text/plain;charset=utf-
8;base64,ZGVmYXVsdHMgewogICAgICAgIHZXJfZnJpZW5kbH1fbmFtZXgbm8KICAgICA
gICBmaW5kX211bHRpcGF0aHMgbm8KfQoKYmxhY2tsaXN0X2V4Y2VwdG1vbnMgewogICAgICA
gIHByb3BlcnR5ICIoU0NTSV9JREVOVF98SURfV1dOKSIKfQoKYmxhY2tsaXN0IHsKfQoK
      verification: {}
    filesystem: root
    mode: 400
    path: /etc/multipath.conf
  systemd:
    units:
      - name: iscsid.service
        enabled: true
        state: started
      - name: multipathd.service
        enabled: true
        state: started
  osImageURL: ""

```

- After the configuration is created, it takes approximately 20 to 30 minutes to apply the configuration to the worker nodes and reload them. Verify whether the machine config is applied by using `oc get mcp` and make sure that the machine config pool for workers is updated. You can also log into the worker nodes to confirm that the iscsid service is running (and the multipathd service is running if using multipathing).

```
[netapp-user@rhel7 openshift-deploy]$ oc get mcp
NAME      CONFIG                                     UPDATED     UPDATING
DEGRADED
master    rendered-master-a520ae930e1d135e0dee7168   True       False
False
worker    rendered-worker-de321b36eeba62df41feb7bc   True       False
False

[netapp-user@rhel7 openshift-deploy]$ ssh core@10.61.181.22 sudo
systemctl status iscsid
● iscsid.service - Open-iSCSI
   Loaded: loaded (/usr/lib/systemd/system/iscsid.service; enabled;
   vendor preset: disabled)
     Active: active (running) since Tue 2021-05-26 13:36:22 UTC; 3 min ago
       Docs: man:iscsid(8)
              man:iscsiadm(8)
   Main PID: 1242 (iscsid)
     Status: "Ready to process requests"
      Tasks: 1
     Memory: 4.9M
        CPU: 9ms
      CGroup: /system.slice/iscsid.service
              └─1242 /usr/sbin/iscsid -f

[netapp-user@rhel7 openshift-deploy]$ ssh core@10.61.181.22 sudo
systemctl status multipathd
● multipathd.service - Device-Mapper Multipath Device Controller
   Loaded: loaded (/usr/lib/systemd/system/multipathd.service; enabled;
   vendor preset: enabled)
     Active: active (running) since Tue 2021-05-26 13:36:22 UTC; 3 min ago
   Main PID: 918 (multipathd)
     Status: "up"
      Tasks: 7
     Memory: 13.7M
        CPU: 57ms
      CGroup: /system.slice/multipathd.service
              └─918 /sbin/multipathd -d -s
```



It is also possible to confirm that the MachineConfig has been successfully applied and services have been started as expected by running the `oc debug` command with the appropriate flags.

#### Create storage-system backends

After completing the Astra Trident Operator install, you must configure the backend for the specific NetApp

storage platform you are using. Follow the links below in order to continue the setup and configuration of Astra Trident.

- [NetApp ONTAP NFS](#)
- [NetApp ONTAP iSCSI](#)
- [NetApp Element iSCSI](#)

Next: [Solution Validation/Use Cases: Red Hat OpenShift with NetApp](#).

#### NetApp ONTAP NFS configuration

To enable Trident integration with the NetApp ONTAP storage system, you must create a backend that enables communication with the storage system.

1. There are sample backend files available in the downloaded installation archive in the `sample-input` folder hierarchy. For NetApp ONTAP systems serving NFS, copy the `backend-ontap-nas.json` file to your working directory and edit the file.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/backends-samples/ontap-nas/backend-ontap-nas.json ./
[netapp-user@rhel7 trident-installer]$ vi backend-ontap-nas.json
```

2. Edit the `backendName`, `managementLIF`, `dataLIF`, `svm`, `username`, and `password` values in this file.

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "ontap-nas+10.61.181.221",
  "managementLIF": "172.21.224.201",
  "dataLIF": "10.61.181.221",
  "svm": "trident_svm",
  "username": "cluster-admin",
  "password": "password"
}
```



It is a best practice to define the custom `backendName` value as a combination of the `storageDriverName` and the `dataLIF` that is serving NFS for easy identification.

3. With this backend file in place, run the following command to create your first backend.

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create
backend -f backend-ontap-nas.json
+-----+
+-----+-----+
|           NAME          | STORAGE DRIVER |             UUID
| STATE   | VOLUMES   |
+-----+-----+
+-----+-----+-----+
| ontap-nas+10.61.181.221 | ontap-nas      | be7a619d-c81d-445c-b80c-
5c87a73c5b1e | online |     0 |
+-----+-----+
+-----+-----+-----+
```

- With the backend created, you must next create a storage class. Just as with the backend, there is a sample storage class file that can be edited for the environment available in the sample-inputs folder. Copy it to the working directory and make necessary edits to reflect the backend created.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/storage-class-
samples/storage-class-csi.yaml.templ ./storage-class-basic.yaml
[netapp-user@rhel7 trident-installer]$ vi storage-class-basic.yaml
```

- The only edit that must be made to this file is to define the `backendType` value to the name of the storage driver from the newly created backend. Also note the `name`-field value, which must be referenced in a later step.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: basic-csi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
```



There is an optional field called `fsType` that is defined in this file. This line can be deleted in NFS backends.

- Run the `oc` command to create the storage class.

```
[netapp-user@rhel7 trident-installer]$ oc create -f storage-class-
basic.yaml
storageclass.storage.k8s.io/basic-csi created
```

7. With the storage class created, you must then create the first persistent volume claim (PVC). There is a sample `pvc-basic.yaml` file that can be used to perform this action located in `sample-input` as well.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/pvc-samples/pvc-basic.yaml ./
[netapp-user@rhel7 trident-installer]$ vi pvc-basic.yaml
```

8. The only edit that must be made to this file is ensuring that the `storageClassName` field matches the one just created. The PVC definition can be further customized as required by the workload to be provisioned.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

9. Create the PVC by issuing the `oc` command. Creation can take some time depending on the size of the backing volume being created, so you can watch the process as it completes.

```
[netapp-user@rhel7 trident-installer]$ oc create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ oc get pvc
NAME      STATUS      VOLUME                                     CAPACITY
ACCESS MODES     STORAGECLASS     AGE
basic     Bound      pvc-b4370d37-0fa4-4c17-bd86-94f96c94b42d   1Gi
          RWO        basic-csi       7s
```

[Next: Solution validation/use cases.](#)

#### NetApp ONTAP iSCSI configuration

To enable Trident integration with the NetApp ONTAP storage system, you must create a backend that enables communication with the storage system.

1. There are sample backend files available in the downloaded installation archive in the `sample-input` folder hierarchy. For NetApp ONTAP systems serving iSCSI, copy the `backend-ontap-san.json` file to your working directory and edit the file.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/backends-samples/ontap-san/backend-ontap-san.json ./
[netapp-user@rhel7 trident-installer]$ vi backend-ontap-san.json
```

2. Edit the managementLIF, dataLIF, svm, username, and password values in this file.

```
{  
    "version": 1,  
    "storageDriverName": "ontap-san",  
    "managementLIF": "172.21.224.201",  
    "dataLIF": "10.61.181.240",  
    "svm": "trident_svm",  
    "username": "admin",  
    "password": "password"  
}
```

3. With this backend file in place, run the following command to create your first backend.

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create backend -f backend-ontap-san.json  
+-----+-----+  
+-----+-----+-----+  
|       NAME           | STORAGE DRIVER |          UUID  
| STATE   | VOLUMES |  
+-----+-----+  
+-----+-----+-----+  
| ontapsan_10.61.181.241 | ontap-san      | 6788533c-7fea-4a35-b797-  
fb9bb3322b91 | online | 0 |  
+-----+-----+  
+-----+-----+-----+
```

4. With the backend created, you must next create a storage class. Just as with the backend, there is a sample storage class file that can be edited for the environment available in the sample-inputs folder. Copy it to the working directory and make necessary edits to reflect the backend created.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/storage-class-samples/storage-class-csi.yaml.templ ./storage-class-basic.yaml
[netapp-user@rhel7 trident-installer]$ vi storage-class-basic.yaml
```

5. The only edit that must be made to this file is to define the backendType value to the name of the storage driver from the newly created backend. Also note the name-field value, which must be referenced in a later step.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: basic-csi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
```



There is an optional field called `fsType` that is defined in this file. In iSCSI backends, this value can be set to a specific Linux filesystem type (XFS, ext4, etc) or can be deleted to allow OpenShift to decide what filesystem to use.

6. Run the `oc` command to create the storage class.

```
[netapp-user@rhel7 trident-installer]$ oc create -f storage-class-
basic.yaml
storageclass.storage.k8s.io/basic-csi created
```

7. With the storage class created, you must then create the first persistent volume claim (PVC). There is a sample `pvc-basic.yaml` file that can be used to perform this action located in `sample-inputs` as well.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/pvc-samples/pvc-
basic.yaml .
[netapp-user@rhel7 trident-installer]$ vi pvc-basic.yaml
```

8. The only edit that must be made to this file is ensuring that the `storageClassName` field matches the one just created. The PVC definition can be further customized as required by the workload to be provisioned.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

9. Create the PVC by issuing the `oc` command. Creation can take some time depending on the size of the backing volume being created, so you can watch the process as it completes.

```
[netapp-user@rhel7 trident-installer]$ oc create -f pvc-basic.yaml
persistentvolumeclaim/basic created
```

```
[netapp-user@rhel7 trident-installer]$ oc get pvc
NAME      STATUS    VOLUME                                     CAPACITY
ACCESS MODES   STORAGECLASS   AGE
basic     Bound     pvc-7ceac1ba-0189-43c7-8f98-094719f7956c   1Gi
RWO          basic-csi   3s
```

[Next: Solution validation/use cases.](#)

#### NetApp Element iSCSI configuration

To enable Trident integration with the NetApp Element storage system, you must create a backend that enables communication with the storage system using the iSCSI protocol.

1. There are sample backend files available in the downloaded installation archive in the `sample-input` folder hierarchy. For NetApp Element systems serving iSCSI, copy the `backend-solidfire.json` file to your working directory and edit the file.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/backends-
samples/solidfire/backend-solidfire.json ./
[netapp-user@rhel7 trident-installer]$ vi ./backend-solidfire.json
```

- a. Edit the user, password, and MVIP value on the `EndPoint` line.
- b. Edit the `SVIP` value.

```
{
  "version": 1,
  "storageDriverName": "solidfire-san",
  "Endpoint": "https://trident:password@172.21.224.150/json-
rpc/8.0",
  "SVIP": "10.61.180.200:3260",
  "TenantName": "trident",
  "Types": [{"Type": "Bronze", "Qos": {"minIOPS": 1000, "maxIOPS": 2000, "burstIOPS": 4000},
             {"Type": "Silver", "Qos": {"minIOPS": 4000, "maxIOPS": 6000, "burstIOPS": 8000}},
             {"Type": "Gold", "Qos": {"minIOPS": 6000, "maxIOPS": 8000, "burstIOPS": 10000}}]
}
```

2. With this back-end file in place, run the following command to create your first backend.

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create
backend -f backend-solidfire.json
+-----+
+-----+-----+
|           NAME          | STORAGE DRIVER |             UUID
| STATE   | VOLUMES   |
+-----+-----+
+-----+-----+
| solidfire_10.61.180.200 | solidfire-san | b90783ee-e0c9-49af-8d26-
3ea87ce2efdf | online |      0 |
+-----+-----+
+-----+-----+
```

- With the backend created, you must next create a storage class. Just as with the backend, there is a sample storage class file that can be edited for the environment available in the sample-inputs folder. Copy it to the working directory and make necessary edits to reflect the backend created.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/storage-class-
samples/storage-class-csi.yaml.templ ./storage-class-basic.yaml
[netapp-user@rhel7 trident-installer]$ vi storage-class-basic.yaml
```

- The only edit that must be made to this file is to define the `backendType` value to the name of the storage driver from the newly created backend. Also note the `name`-field value, which must be referenced in a later step.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: basic-csi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "solidfire-san"
```



There is an optional field called `fsType` that is defined in this file. In iSCSI backends, this value can be set to a specific Linux filesystem type (XFS, ext4, and so on), or it can be deleted to allow OpenShift to decide what filesystem to use.

- Run the `oc` command to create the storage class.

```
[netapp-user@rhel7 trident-installer]$ oc create -f storage-class-
basic.yaml
storageclass.storage.k8s.io/basic-csi created
```

6. With the storage class created, you must then create the first persistent volume claim (PVC). There is a sample `pvc-basic.yaml` file that can be used to perform this action located in `sample-input` as well.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/pvc-samples/pvc-basic.yaml ./
[netapp-user@rhel7 trident-installer]$ vi pvc-basic.yaml
```

7. The only edit that must be made to this file is ensuring that the `storageClassName` field matches the one just created. The PVC definition can be further customized as required by the workload to be provisioned.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

8. Create the PVC by issuing the `oc` command. Creation can take some time depending on the size of the backing volume being created, so you can watch the process as it completes.

```
[netapp-user@rhel7 trident-installer]$ oc create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ oc get pvc
NAME      STATUS      VOLUME                                     CAPACITY
ACCESS MODES     STORAGECLASS     AGE
basic     Bound      pvc-3445b5cc-df24-453d-a1e6-b484e874349d   1Gi
          RWO        basic-csi       5s
```

[Next: Solution validation/use cases.](#)

## Advanced Configuration Options For OpenShift

### Exploring load balancer options: Red Hat OpenShift with NetApp

In most cases, Red Hat OpenShift makes applications available to the outside world through routes. A service is exposed by giving it an externally reachable hostname. The defined route and the endpoints identified by its service can be consumed by an OpenShift router to provide this named connectivity to external clients.

However in some cases, applications require the deployment and configuration of customized load balancers

to expose the appropriate services. One example of this is NetApp Astra Control Center. To meet this need, we have evaluated a number of custom load balancer options. Their installation and configuration are described in this section.

The following pages have additional information about load balancer options validated in the Red Hat OpenShift with NetApp solution:

- [MetalLB](#)
- [F5 BIG-IP](#)

[Next: Solution validation/use cases: Red Hat OpenShift with NetApp.](#)

### Installing MetalLB load balancers: Red Hat OpenShift with NetApp

This page lists the installation and configuration instructions for the MetalLB load balancer.

MetalLB is a self-hosted network load balancer installed on your OpenShift cluster that allows the creation of OpenShift services of type load balancer in clusters that do not run on a cloud provider. The two main features of MetalLB that work together to support LoadBalancer services are address allocation and external announcement.

#### MetalLB configuration options

Based on how MetalLB announces the IP address assigned to LoadBalancer services outside of the OpenShift cluster, it operates in two modes:

- **Layer 2 mode.** In this mode, one node in the OpenShift cluster takes ownership of the service and responds to ARP requests for that IP to make it reachable outside of the OpenShift cluster. Because only the node advertises the IP, it has a bandwidth bottleneck and slow failover limitations. For more information, see the documentation [here](#).
- **BGP mode.** In this mode, all nodes in the OpenShift cluster establish BGP peering sessions with a router and advertise the routes to forward traffic to the service IPs. The prerequisite for this is to integrate MetalLB with a router in that network. Owing to the hashing mechanism in BGP, it has certain limitation when IP-to-Node mapping for a service changes. For more information, refer to the documentation [here](#).



For the purpose of this document, we are configuring MetalLB in layer-2 mode.

### Installing The MetalLB Load Balancer

1. Download the MetalLB resources.

```
[netapp-user@rhel7 ~]$ wget https://raw.githubusercontent.com/metallb/metallb/v0.10.2/manifests/namespace.yaml  
[netapp-user@rhel7 ~]$ wget https://raw.githubusercontent.com/metallb/metallb/v0.10.2/manifests/metallb.yaml
```

2. Edit file `metallb.yaml` and remove `spec.template.spec.securityContext` from controller Deployment and the speaker DaemonSet.

**Lines to be deleted:**

```
securityContext:  
  runAsNonRoot: true  
  runAsUser: 65534
```

3. Create the metallb-system namespace.

```
[netapp-user@rhel7 ~]$ oc create -f namespace.yaml  
namespace/metallb-system created
```

4. Create the MetalLB CR.

```
[netapp-user@rhel7 ~]$ oc create -f metallb.yaml  
podsecuritypolicy.policy/controller created  
podsecuritypolicy.policy/speaker created  
serviceaccount/controller created  
serviceaccount/speaker created  
clusterrole.rbac.authorization.k8s.io/metallb-system:controller created  
clusterrole.rbac.authorization.k8s.io/metallb-system:speaker created  
role.rbac.authorization.k8s.io/config-watcher created  
role.rbac.authorization.k8s.io/pod-lister created  
role.rbac.authorization.k8s.io/controller created  
clusterrolebinding.rbac.authorization.k8s.io/metallb-system:controller  
created  
clusterrolebinding.rbac.authorization.k8s.io/metallb-system:speaker  
created  
rolebinding.rbac.authorization.k8s.io/config-watcher created  
rolebinding.rbac.authorization.k8s.io/pod-lister created  
rolebinding.rbac.authorization.k8s.io/controller created  
daemonset.apps/speaker created  
deployment.apps/controller created
```

5. Before configuring the MetalLB speaker, grant the speaker DaemonSet elevated privileges so that it can perform the networking configuration required to make the load balancers work.

```
[netapp-user@rhel7 ~]$ oc adm policy add-scc-to-user privileged -n  
metallb-system -z speaker  
clusterrole.rbac.authorization.k8s.io/system:openshift:scc:privileged  
added: "speaker"
```

6. Configure MetalLB by creating a ConfigMap in the metallb-system namespace.

```
[netapp-user@rhel7 ~]$ vim metallb-config.yaml
```

```
apiVersion: v1
kind: ConfigMap
metadata:
  namespace: metallb-system
  name: config
data:
  config: |
    address-pools:
    - name: default
      protocol: layer2
      addresses:
      - 10.63.17.10-10.63.17.200
```

```
[netapp-user@rhel7 ~]$ oc create -f metallb-config.yaml
configmap/config created
```

7. Now when loadbalancer services are created, MetallB assigns an externalIP to the services and advertises the IP address by responding to ARP requests.



If you wish to configure MetallB in BGP mode, skip step 6 above and follow the procedure in the MetallB documentation [here](#).

Next: [Solution validation/use cases: Red Hat OpenShift with NetApp](#).

#### Installing F5 BIG-IP Load Balancers

F5 BIG-IP is an Application Delivery Controller (ADC) that offers a broad set of advanced production-grade traffic management and security services like L4-L7 load balancing, SSL/TLS offload, DNS, firewall and many more. These services drastically increase the availability, security and performance of your applications.

F5 BIG-IP can be deployed and consumed in various ways, on dedicated hardware, in the cloud, or as a virtual appliance on-premises. Refer to the documentation [here](#) to explore and deploy F5 BIG-IP as per requirement.

For efficient integration of F5 BIG-IP services with Red Hat OpenShift, F5 offers the BIG-IP Container Ingress Service (CIS). CIS is installed as a controller pod that watches OpenShift API for certain Custom Resource Definitions (CRDs) and manages the F5 BIG-IP system configuration. F5 BIG-IP CIS can be configured to control service types LoadBalancers and Routes in OpenShift.

Further, for automatic IP address allocation to service the type LoadBalancer, you can utilize the F5 IPAM controller. The F5 IPAM controller is installed as a controller pod that watches OpenShift API for LoadBalancer services with an ipamLabel annotation to allocate the IP address from a preconfigured pool.

This page lists the installation and configuration instructions for F5 BIG-IP CIS and IPAM controller. As a prerequisite, you must have an F5 BIG-IP system deployed and licensed. It must also be licensed for SDN services, which are included by default with the BIG-IP VE base license.



F5 BIG-IP can be deployed in standalone or cluster mode. For the purpose of this validation, F5 BIG-IP was deployed in standalone mode, but, for production purposes, it is preferred to have a cluster of BIG-IPs to avoid a single point of failure.



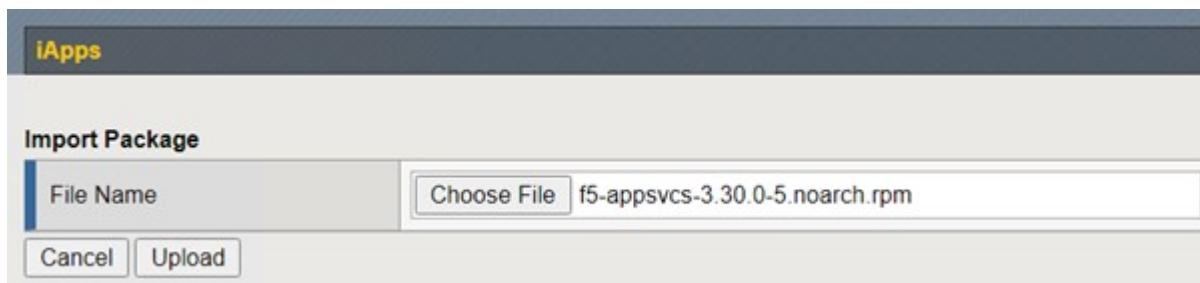
An F5 BIG-IP system can be deployed on dedicated hardware, in the cloud, or as a virtual appliance on-premises with versions greater than 12.x for it to be integrated with F5 CIS. For the purpose of this document, the F5 BIG-IP system was validated as a virtual appliance, for example using the BIG-IP VE edition.

## Validated releases

Technology	Software version
Red Hat OpenShift	4.6 EUS, 4.7
F5 BIG-IP VE edition	16.1.0
F5 Container Ingress Service	2.5.1
F5 IPAM Controller	0.1.4
F5 AS3	3.30.0

## Installation

1. Install the F5 Application Services 3 extension to allow BIG-IP systems to accept configurations in JSON instead of imperative commands. Go to [F5 AS3 GitHub repository](#), and download the latest RPM file.
2. Log into F5 BIG-IP system, navigate to iApps > Package Management LX and click Import.
3. Click Choose File and select the downloaded AS3 RPM file, click OK, and then click Upload.



4. Confirm that the AS3 extension is installed successfully.



5. Next configure the resources required for communication between OpenShift and BIG-IP systems. First create a tunnel between OpenShift and the BIG-IP server by creating a VXLAN tunnel interface on the BIG-IP system for OpenShift SDN. Navigate to Network > Tunnels > Profiles, click Create, and set the Parent Profile to vxlan and the Flooding Type to Multicast. Enter a name for the profile and click Finished.

Network > Tunnels > Profiles : VXLAN > New VXLAN Profile...

<b>General Properties</b>	
Name	vxlan-multipoint
Parent Profile	vxlan
Description	
<b>Settings</b>	
Port	4789
Flooding Type	Multicast <input checked="" type="checkbox"/>
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

6. Navigate to Network > Tunnels > Tunnel List, click Create, and enter the name and local IP address for the tunnel. Select the tunnel profile that was created in the previous step and click Finished.

Network > Tunnels : Tunnel List > New Tunnel...

<b>Configuration</b>	
Name	openshift_vxlan
Description	
Key	0
Profile	vxlan-multipoint
Local Address	10.63.172.239
Secondary Address	Any
Remote Address	Any
Mode	Bidirectional
MTU	0
Use PMTU	<input checked="" type="checkbox"/> Enabled
TOS	Preserve
Auto-Last Hop	Default
Traffic Group	None
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

7. Log into the Red Hat OpenShift cluster with cluster-admin privileges.
8. Create a hostsubnet on OpenShift for the F5 BIG-IP server, which extends the subnet from the OpenShift cluster to the F5 BIG-IP server. Download the host subnet YAML definition.

```
wget https://github.com/F5Networks/k8s-bigip-ctlr/blob/master/docs/config_examples/openshift/f5-kctlr-openshift-hostsubnet.yaml
```

9. Edit the host subnet file and add the BIG-IP VTEP (VXLAN tunnel) IP for the OpenShift SDN.

```
apiVersion: v1
kind: HostSubnet
metadata:
  name: f5-server
  annotations:
    pod.network.openshift.io/fixed-vnid-host: "0"
    pod.network.openshift.io/assign-subnet: "true"
  # provide a name for the node that will serve as BIG-IP's entry into the
  # cluster
  host: f5-server
  # The hostIP address will be the BIG-IP interface address routable to
  # the
  # OpenShift Origin nodes.
  # This address is the BIG-IP VTEP in the SDN's VXLAN.
  hostIP: 10.63.172.239
```



Change the hostIP and other details as applicable to your environment.

10. Create the HostSubnet resource.

```
[admin@rhel-7 ~]$ oc create -f f5-kctlr-openshift-hostsubnet.yaml
hostsubnet.network.openshift.io/f5-server created
```

11. Get the cluster IP subnet range for the host subnet created for the F5 BIG-IP server.

```
[admin@rhel-7 ~]$ oc get hostsubnet
```

NAME	HOST	HOST IP
SUBNET	EGRESS CIDRS	EGRESS IPS
f5-server		f5-server
10.131.0.0/23		10.63.172.239
ocp-vmw-nszws-master-0		ocp-vmw-nszws-master-0
10.128.0.0/23		10.63.172.44
ocp-vmw-nszws-master-1		ocp-vmw-nszws-master-1
10.130.0.0/23		10.63.172.47
ocp-vmw-nszws-master-2		ocp-vmw-nszws-master-2
10.129.0.0/23		10.63.172.48
ocp-vmw-nszws-worker-r8fh4		ocp-vmw-nszws-worker-r8fh4
10.130.2.0/23		10.63.172.7
ocp-vmw-nszws-worker-tvr46		ocp-vmw-nszws-worker-tvr46
10.129.2.0/23		10.63.172.11
ocp-vmw-nszws-worker-wdxhg		ocp-vmw-nszws-worker-wdxhg
10.128.2.0/23		10.63.172.24
ocp-vmw-nszws-worker-wg8r4		ocp-vmw-nszws-worker-wg8r4
10.131.2.0/23		10.63.172.15
ocp-vmw-nszws-worker-wtgef		ocp-vmw-nszws-worker-wtgef
10.128.4.0/23		10.63.172.17

12. Create a self IP on OpenShift VXLAN with an IP in OpenShift's host subnet range corresponding to the F5 BIG-IP server. Log into the F5 BIG-IP system, navigate to Network > Self IPs and click Create. Enter an IP from the cluster IP subnet created for F5 BIG-IP host subnet, select the VXLAN tunnel, and enter the other details. Then click Finished.

Network » Self IPs » New Self IP...

**Configuration**

Name	10.131.0.60
IP Address	10.131.0.60
Netmask	255.252.0.0
VLAN / Tunnel	openshift_vxla
Port Lockdown	Allow All
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)
Service Policy	None

Cancel Repeat Finished

13. Create a partition in the F5 BIG-IP system to be configured and used with CIS. Navigate to System > Users > Partition List, click Create, and enter the details. Then click Finished.

System » Users : Partition List » New Partition...

Properties	
Partition Name	ocp-vmw
Partition Default Route Domain	0 ▾
Description	<input type="checkbox"/> Extend Text Area <input type="checkbox"/> Wrap Text
Redundant Device Configuration	
Device Group	<input checked="" type="checkbox"/> Inherit device group from root folder None ▾
Traffic Group	<input checked="" type="checkbox"/> Inherit traffic group from root folder traffic-group-1 (floating) ▾
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	



F5 recommends that no manual configuration be done on the partition that is managed by CIS.

14. Install the F5 BIG-IP CIS using the operator from OperatorHub. Log into the Red Hat OpenShift cluster with cluster-admin privileges and create a secret with F5 BIG-IP system login credentials, which is a prerequisite for the operator.

```
[admin@rhel-7 ~]$ oc create secret generic bigip-login -n kube-system  
--from-literal=username=admin --from-literal=password=admin  
  
secret/bigip-login created
```

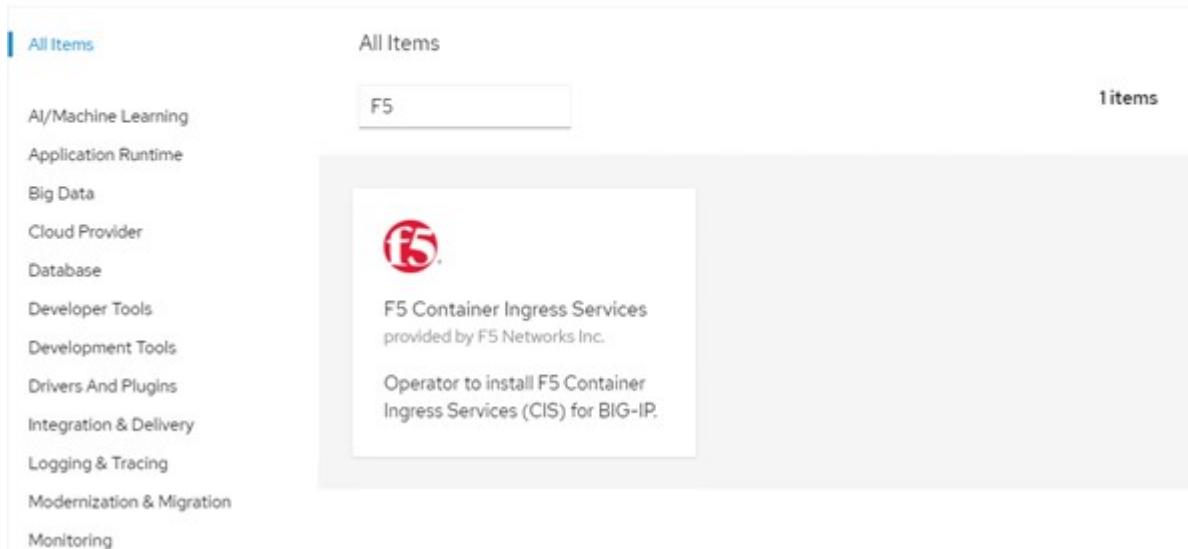
## 15. Install the F5 CIS CRDs.

```
[admin@rhel-7 ~]$ oc apply -f  
https://raw.githubusercontent.com/F5Networks/k8s-bigip-  
ctlr/master/docs/config_examples/crd/Install/customresourcedefinitions.y  
ml  
  
customresourcedefinition.apiextensions.k8s.io/virtualservers.cis.f5.com  
created  
customresourcedefinition.apiextensions.k8s.io/tlsprofiles.cis.f5.com  
created  
customresourcedefinition.apiextensions.k8s.io/transportservers.cis.f5.co  
m created  
customresourcedefinition.apiextensions.k8s.io/externaldnss.cis.f5.com  
created  
customresourcedefinition.apiextensions.k8s.io/ingresslinks.cis.f5.com  
created
```

## 16. Navigate to Operators > OperatorHub, search for the keyword F5, and click the F5 Container Ingress Service tile.

### OperatorHub

Discover Operators from the Kubernetes community and Red Hat partners, curated by Red Hat. You can purchase commercial software through [Red Hat Marketplace](#). You can install Operators on your clusters to provide optional add-ons and shared services to your developers. After installation, the Operator capabilities will appear in the [Developer Catalog](#) providing a self-service experience.



The screenshot shows the OperatorHub interface. On the left, there is a sidebar with a list of categories: All Items, AI/Machine Learning, Application Runtime, Big Data, Cloud Provider, Database, Developer Tools, Development Tools, Drivers And Plugins, Integration & Delivery, Logging & Tracing, Modernization & Migration, and Monitoring. The main area has a search bar with the text 'F5'. Below the search bar, there is a card for the 'F5 Container Ingress Services' operator. The card features the F5 logo, the text 'F5 Container Ingress Services provided by F5 Networks Inc.', and a description: 'Operator to install F5 Container Ingress Services (CIS) for BIG-IP.' To the right of the card, it says '1 items'.

17. Read the operator information and click Install.

The screenshot shows the F5 Container Ingress Services Operator page. At the top left is the F5 logo. To its right is the title "F5 Container Ingress Services" and below it "1.8.0 provided by F5 Networks Inc.". On the far right is a close button (an "X"). Below the title is a blue "Install" button. The main content area has a header "Latest version" with "1.8.0". It includes sections for "Capability level" (with "Basic Install" checked), "Provider type" (Certified), "Provider" (F5 Networks Inc.), "Repository" (https://github.com/F5Networks/k8s-bigip-ctlr), and "Container Image" (registry.connect.redhat.com/f5networks/k8s-bigip-ctlr). A section titled "Introduction" explains the operator's function: "This Operator installs F5 Container Ingress Services (CIS) for BIG-IP in your Cluster. This enables to configure and deploy CIS using Helm Charts." Another section, "F5 Container Ingress Services for BIG-IP", describes how CIS integrates with container orchestration environments to manage L4/L7 services. A "Documentation" section links to F5 documentation and OpenShift routes. A "Prerequisites" section instructs users to create BIG-IP login credentials using the command: 

```
oc create secret generic <SECRET-NAME> -n kube-system --from-literal=username=<USERNAME> --from-literal=password=<PASSWORD>
```

18. On the Install operator screen, leave all default parameters, and click Install.

## Install Operator

Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.

Update channel \*

beta

F5 Container Ingress Services  
provided by F5 Networks Inc.

Provided APIs

**F5ContainerIngressServices**

This CRD provides kind `F5ContainerIngressServices` to configure and deploy F5 Container Ingress Services.

Installation mode \*

All namespaces on the cluster (default)  
Operator will be available in all Namespaces.

A specific namespace on the cluster  
Operator will be available in a single Namespace only.

Installed Namespace \*

PR openshift-operators

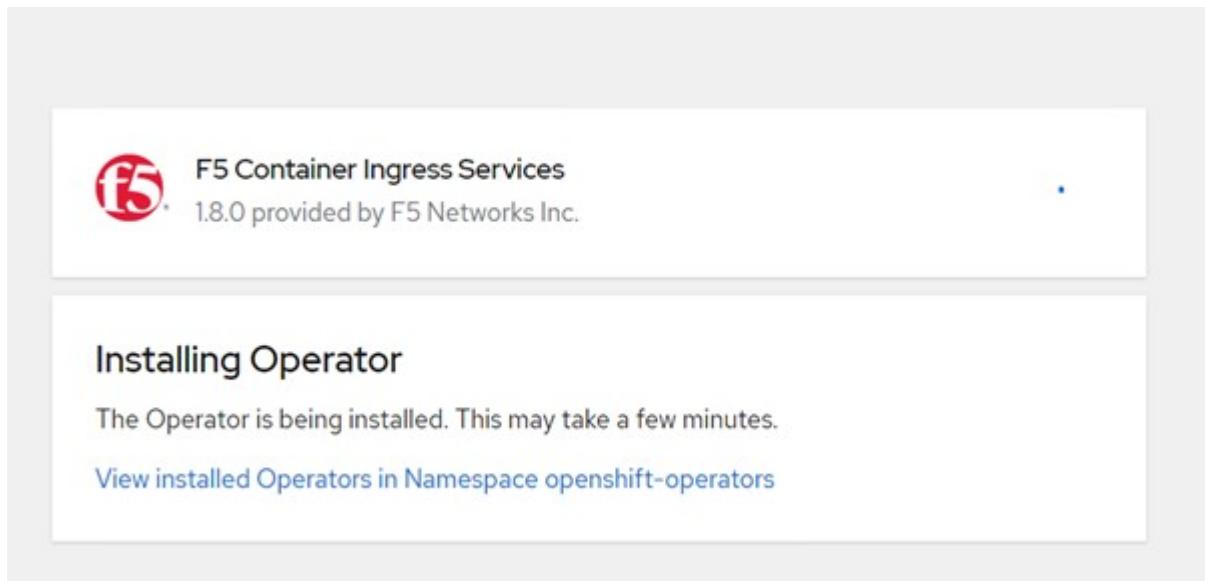
Approval strategy \*

Automatic

Manual

**Install** **Cancel**

19. It takes a while to install the operator.



20. After the operator is installed, the Installation Successful message is displayed.
21. Navigate to Operators > Installed Operators, click F5 Container Ingress Service, and then click Create Instance under the F5BigIpCtlr tile.



## F5 Container Ingress Services

1.8.0 provided by F5 Networks Inc.

[Details](#)[YAML](#)[Subscription](#)[Events](#)[F5BigIpCtlr](#)

## Provided APIs

**FBIC F5BigIpCtlr**

This CRD provides kind `F5BigIpCtlr` to configure and deploy F5 BIG-IP Controller.

 [Create instance](#)

22. Click YAML View and paste the following content after updating the necessary parameters.



Update the parameters `bigip_partition`, `openshift\_sdn\_name`, `bigip_url` and `bigip_login_secret` below to reflect the values for your setup before copying the content.

```

apiVersion: cis.f5.com/v1
kind: F5BigIpCtlr
metadata:
  name: f5-server
  namespace: openshift-operators
spec:
  args:
    log_as3_response: true
    agent: as3
    log_level: DEBUG
    bigip_partition: ocp-vmw
    openshift_sdn_name: /Common/openshift_vxlan
    bigip_url: 10.61.181.19
    insecure: true
    pool-member-type: cluster
    custom_resource_mode: true
    as3_validation: true
    ipam: true
    manage_configmaps: true
    bigip_login_secret: bigip-login
  image:
    pullPolicy: Always
    repo: f5networks/cntr-ingress-svcs
    user: registry.connect.redhat.com
  namespace: kube-system
  rbac:
    create: true
  resources: {}
  serviceAccount:
    create: true
  version: latest

```

23. After pasting this content, click Create. This installs the CIS pods in the kube-system namespace.

Pods								<a href="#">Create Pod</a>
Name	Status	Ready	Restarts	Owner	Memory	CPU		
f5-server-f5-bigip-ctlr-5d7578667d-qxdgj	Running	1/1	0	RS f5-server-f5-bigip-ctlr-5d7578667d	61.1 MiB	0.003 cores		



Red Hat OpenShift, by default, provides a way to expose the services via Routes for L7 load balancing. An inbuilt OpenShift router is responsible for advertising and handling traffic for these routes. However, you can also configure the F5 CIS to support the Routes through an external F5 BIG-IP system, which can run either as an auxiliary router or a replacement to the self-hosted OpenShift router. CIS creates a virtual server in the BIG-IP system that acts as a router for the OpenShift routes, and BIG-IP handles the advertisement and traffic routing. Refer to the documentation here for information on parameters to enable this feature. Note that these parameters are defined for OpenShift Deployment resource in the apps/v1 API. Therefore, when using these with the F5BigIpCtlr resource cis.f5.com/v1 API, replace the hyphens (-) with underscores (\_) for the parameter names.

24. The arguments that are passed to the creation of CIS resources include `ipam: true` and `custom_resource_mode: true`. These parameters are required for enabling CIS integration with an IPAM controller. Verify that the CIS has enabled IPAM integration by creating the F5 IPAM resource.

```
[admin@rhel-7 ~]$ oc get f5ipam -n kube-system  
  
NAMESPACE      NAME          AGE  
kube-system    ipam.10.61.181.19.ocp-vmw   43s
```

25. Create the service account, role and rolebinding required for the F5 IPAM controller. Create a YAML file and paste the following content.

```
[admin@rhel-7 ~]$ vi f5-ipam-rbac.yaml

kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: ipam-ctlr-clusterrole
rules:
  - apiGroups: ["fic.f5.com"]
    resources: ["ipams","ipams/status"]
    verbs: ["get", "list", "watch", "update", "patch"]
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: ipam-ctlr-clusterrole-binding
  namespace: kube-system
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: ipam-ctlr-clusterrole
subjects:
  - apiGroup: ""
    kind: ServiceAccount
    name: ipam-ctlr
    namespace: kube-system
---
apiVersion: v1
kind: ServiceAccount
metadata:
  name: ipam-ctlr
  namespace: kube-system
```

## 26. Create the resources.

```
[admin@rhel-7 ~]$ oc create -f f5-ipam-rbac.yaml

clusterrole.rbac.authorization.k8s.io/ipam-ctlr-clusterrole created
clusterrolebinding.rbac.authorization.k8s.io/ipam-ctlr-clusterrole-
binding created
serviceaccount/ipam-ctlr created
```

## 27. Create a YAML file and paste the F5 IPAM deployment definition provided below.



Update the ip-range parameter in spec.template.spec.containers[0].args below to reflect the ipamLabels and IP address ranges corresponding to your setup.



ipamLabels [range1 and range2 in below example] are required to be annotated for the services of type LoadBalancer for the IPAM controller to detect and assign an IP address from the defined range.

```
[admin@rhel-7 ~]$ vi f5-ipam-deployment.yaml

apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    name: f5-ipam-controller
    name: f5-ipam-controller
    namespace: kube-system
spec:
  replicas: 1
  selector:
    matchLabels:
      app: f5-ipam-controller
  template:
    metadata:
      creationTimestamp: null
      labels:
        app: f5-ipam-controller
    spec:
      containers:
        - args:
            - --orchestration=openshift
            - --ip-range='{"range1":"10.63.172.242-10.63.172.249",
"range2":"10.63.170.111-10.63.170.129"}'
            - --log-level=DEBUG
          command:
            - /app/bin/f5-ipam-controller
          image: registry.connect.redhat.com/f5networks/f5-ipam-
controller:latest
          imagePullPolicy: IfNotPresent
          name: f5-ipam-controller
        dnsPolicy: ClusterFirst
        restartPolicy: Always
        schedulerName: default-scheduler
        securityContext: {}
        serviceAccount: ipam-ctlr
        serviceAccountName: ipam-ctlr
```

28. Create the F5 IPAM controller deployment.

```
[admin@rhel-7 ~]$ oc create -f f5-ipam-deployment.yaml  
deployment/f5-ipam-controller created
```

29. Verify the F5 IPAM controller pods are running.

```
[admin@rhel-7 ~]$ oc get pods -n kube-system  
  
NAME                                READY   STATUS    RESTARTS  
AGE  
f5-ipam-controller-5986cff5bd-2bvn6   1/1     Running   0  
30s  
f5-server-f5-bigip-ctlr-5d7578667d-qxdgj   1/1     Running   0  
14m
```

30. Create the F5 IPAM schema.

```
[admin@rhel-7 ~]$ oc create -f  
https://raw.githubusercontent.com/F5Networks/f5-ipam-  
controller/main/docs/_static/schemas/ipam_schema.yaml  
  
customresourcedefinition.apiextensions.k8s.io/ipams.fic.f5.com
```

## Verification

1. Create a service of type LoadBalancer

```
[admin@rhel-7 ~]$ vi example_svc.yaml

apiVersion: v1
kind: Service
metadata:
  annotations:
    cis.f5.com/ipamLabel: range1
  labels:
    app: f5-demo-test
  name: f5-demo-test
  namespace: default
spec:
  ports:
  - name: f5-demo-test
    port: 80
    protocol: TCP
    targetPort: 80
  selector:
    app: f5-demo-test
  sessionAffinity: None
  type: LoadBalancer
```

```
[admin@rhel-7 ~]$ oc create -f example_svc.yaml

service/f5-demo-test created
```

## 2. Check if the IPAM controller assigns an external IP to it.

```
[admin@rhel-7 ~]$ oc get svc

NAME           TYPE      CLUSTER-IP      EXTERNAL-IP
PORT (S)       AGE
f5-demo-test   LoadBalancer 172.30.210.108  10.63.172.242
80:32605/TCP  27s
```

## 3. Create a deployment and use the LoadBalancer service that was created.

```
[admin@rhel-7 ~]$ vi example_deployment.yaml
```

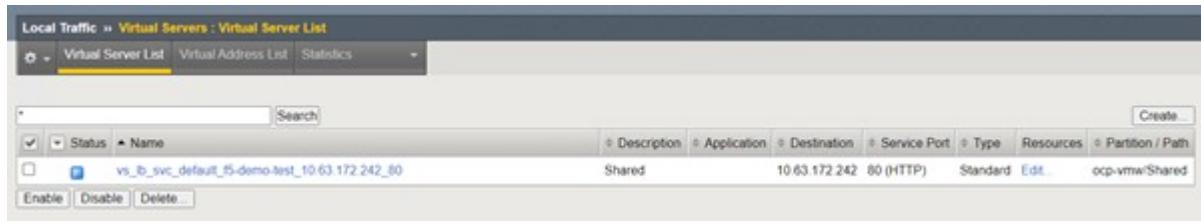
```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    app: f5-demo-test
    name: f5-demo-test
spec:
  replicas: 2
  selector:
    matchLabels:
      app: f5-demo-test
  template:
    metadata:
      labels:
        app: f5-demo-test
    spec:
      containers:
        - env:
            - name: service_name
              value: f5-demo-test
          image: nginx
          imagePullPolicy: Always
          name: f5-demo-test
          ports:
            - containerPort: 80
              protocol: TCP
```

```
[admin@rhel-7 ~]$ oc create -f example_deployment.yaml
deployment/f5-demo-test created
```

#### 4. Check if the pods are running.

```
[admin@rhel-7 ~]$ oc get pods
NAME                      READY   STATUS    RESTARTS   AGE
f5-demo-test-57c46f6f98-47wwp 1/1     Running   0          27s
f5-demo-test-57c46f6f98-cl2m8 1/1     Running   0          27s
```

#### 5. Check if the corresponding virtual server is created in the BIG-IP system for the service of type LoadBalancer in OpenShift. Navigate to Local Traffic > Virtual Servers > Virtual Server List.



Next: Solution Validation/Use Cases: Red Hat OpenShift with NetApp.

## Creating Private Image Registries

For most deployments of Red Hat OpenShift, using a public registry like [Quay.io](#) or [DockerHub](#) meets most customer's needs. However there are times when a customer may want to host their own private or customized images.

This procedure documents creating a private image registry which is backed by a persistent volume provided by Astra Trident and NetApp ONTAP.



Astra Control Center requires a registry to host the images the Astra containers require. The following section describes the steps to setup a private registry on Red Hat OpenShift cluster and pushing the images required to support the installation of Astra Control Center.

### Creating A private image registry

1. Remove the default annotation from the current default storage class and annotate the Trident-backed storage class as default for the OpenShift cluster.

```
[netapp-user@rhel7 ~]$ oc patch storageclass thin -p '{"metadata": {"annotations": {"storageclass.kubernetes.io/is-default-class": "false"}}}'
storageclass.storage.k8s.io/thin patched

[netapp-user@rhel7 ~]$ oc patch storageclass ocp-trident -p '{"metadata": {"annotations": {"storageclass.kubernetes.io/is-default-class": "true"}}}'
storageclass.storage.k8s.io/ocp-trident patched
```

2. Edit the imageregistry operator by entering the following storage parameters in the `spec` section.

```
[netapp-user@rhel7 ~]$ oc edit
configs.imageregistry.operator.openshift.io

storage:
  pvc:
    claim:
```

3. Enter the following parameters in the `spec` section for creating a OpenShift route with a custom hostname.

Save and exit.

```
routes:  
  - hostname: astra-registry.apps.ocp-vmw.cie.netapp.com  
    name: netapp-astra-route
```



The above route config is used when you want a custom hostname for your route. If you want OpenShift to create a route with a default hostname, you can add the following parameters to the spec section: `defaultRoute: true`.

## Custom TLS certificates

When you are using a custom hostname for the route, by default, it uses the default TLS configuration of the OpenShift Ingress operator. However, you can add a custom TLS configuration to the route. To do so, complete the following steps.

- Create a secret with the route's TLS certificates and key.

```
[netapp-user@rhel7 ~]$ oc create secret tls astra-route-tls -n openshift-image-registry -cert/home/admin/netapp-astra/tls.crt --key=/home/admin/netapp-astra/tls.key
```

- Edit the imageregistry operator and add the following parameters to the spec section.

```
[netapp-user@rhel7 ~]$ oc edit  
configs.imageregistry.operator.openshift.io  
  
routes:  
  - hostname: astra-registry.apps.ocp-vmw.cie.netapp.com  
    name: netapp-astra-route  
    secretName: astra-route-tls
```

- Edit the imageregistry operator again and change the management state of the operator to the Managed state. Save and exit.

```
oc edit configs.imageregistry/cluster  
  
managementState: Managed
```

- If all the prerequisites are satisfied, PVCs, pods, and services are created for the private image registry. In a few minutes, the registry should be up.

```
[netapp-user@rhel7 ~]$ oc get all -n openshift-image-registry
```

NAME	READY	STATUS
RESTARTS	AGE	
pod/cluster-image-registry-operator-74f6d954b6-rb7zr	1/1	Running
3 90d		
pod/image-pruner-1627257600-f5cpj	0/1	Completed
0 2d9h		
pod/image-pruner-1627344000-swqzx9	0/1	Completed
0 33h		
pod/image-pruner-1627430400-rv5nt	0/1	Completed
0 9h		
pod/image-registry-6758b547f-6pnj8	1/1	Running
0 76m		
pod/node-ca-bwb5r	1/1	Running
0 90d		
pod/node-ca-f8w54	1/1	Running
0 90d		
pod/node-ca-gjx7h	1/1	Running
0 90d		
pod/node-ca-lcx4k	1/1	Running
0 33d		
pod/node-ca-v7zmx	1/1	Running
0 7d21h		
pod/node-ca-xpppp	1/1	Running
0 89d		

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP
IP	PORT(S)	AGE	
service/image-registry	ClusterIP	172.30.196.167	<none>
5000/TCP	15h		
service/image-registry-operator	ClusterIP	None	<none>
60000/TCP	90d		

NAME	DESIRED	CURRENT	READY	UP-TO-DATE
AVAILABLE	NODE SELECTOR	AGE		
daemonset.apps/node-ca	6	6	6	6
kubernetes.io/os=linux	90d			

NAME	READY	UP-TO-DATE
AVAILABLE	AGE	
deployment.apps/cluster-image-registry-operator	1/1	1
90d		1
deployment.apps/image-registry	1/1	1
15h		1

NAME	CURRENT	READY	AGE	DESIRED
replicaset.apps/cluster-image-registry-operator-74f6d954b6	1	90d		1 1
replicaset.apps/image-registry-6758b547f	1	76m		1 1
replicaset.apps/image-registry-78bfb7f59	0	15h		0 0
replicaset.apps/image-registry-7fcc8d6cc8	0	80m		0 0
replicaset.apps/image-registry-864f88f5b	0	15h		0 0
replicaset.apps/image-registry-cb47ffffb	0	10h		0 0
NAME	COMPLETIONS	DURATION	AGE	
job.batch/image-pruner-1627257600	1/1	10s	2d9h	
job.batch/image-pruner-1627344000	1/1	6s	33h	
job.batch/image-pruner-1627430400	1/1	5s	9h	
NAME	SCHEDULE	SUSPEND	ACTIVE	LAST
SCHEDULE	AGE			
cronjob.batch/image-pruner	0 0 * * *	False	0	9h
90d				
NAME	HOST/PORT			
PATH	SERVICES	PORT	TERMINATION	WILDCARD
route.route.openshift.io/public-routes	astra-registry.apps.ocp-			
vmw.cie.netapp.com	image-registry	<all>	reencrypt	None

6. If you are using the default TLS certificates for the ingress operator OpenShift registry route, you can fetch the TLS certificates using the following command.

```
[netapp-user@rhel7 ~]$ oc extract secret/router-ca --keys=tls.crt -n openshift-ingress-operator
```

7. To allow OpenShift nodes to access and pull the images from the registry, add the certificates to the docker client on the OpenShift nodes. Create a configmap in the `openshift-config` namespace using the TLS certificates and patch it to the cluster image config to make the certificate trusted.

```
[netapp-user@rhel7 ~]$ oc create configmap astra-ca -n openshift-config  
--from-file=astra-registry.apps.ocp-vmw.cie.netapp.com=tls.crt  
  
[netapp-user@rhel7 ~]$ oc patch image.config.openshift.io/cluster  
--patch '{"spec":{"additionalTrustedCA":{"name":"astra-ca"}}}'  
--type=merge
```

8. The OpenShift internal registry is controlled by authentication. All the OpenShift users can access the OpenShift registry, but the operations that the logged in user can perform depends on the user permissions.
  - a. To allow a user or a group of users to pull images from the registry, the user(s) must have the registry-viewer role assigned.

```
[netapp-user@rhel7 ~]$ oc policy add-role-to-user registry-viewer  
ocp-user
```

```
[netapp-user@rhel7 ~]$ oc policy add-role-to-group registry-viewer  
ocp-user-group
```

- b. To allow a user or group of users to write or push images, the user(s) must have the registry-editor role assigned.

```
[netapp-user@rhel7 ~]$ oc policy add-role-to-user registry-editor  
ocp-user
```

```
[netapp-user@rhel7 ~]$ oc policy add-role-to-group registry-editor  
ocp-user-group
```

9. For OpenShift nodes to access the registry and push or pull the images, you need to configure a pull secret.

```
[netapp-user@rhel7 ~]$ oc create secret docker-registry astra-registry-  
credentials --docker-server=astra-registry.apps.ocp-vmw.cie.netapp.com  
--docker-username=ocp-user --docker-password=password
```

10. This pull secret can then be patched to serviceaccounts or be referenced in the corresponding pod definition.

- a. To patch it to service accounts, run the following command.

```
[netapp-user@rhel7 ~]$ oc secrets link <service_account_name> astra-  
registry-credentials --for=pull
```

- b. To reference the pull secret in the pod definition, add the following parameter to the spec section.

```
imagePullSecrets:  
  - name: astra-registry-credentials
```

11. To push or pull an image from workstations apart from OpenShift node, complete the following steps.

- a. Add the TLS certificates to the docker client.

```
[netapp-user@rhel7 ~]$ sudo mkdir /etc/docker/certs.d/astra-  
registry.apps.ocp-vmw.cie.netapp.com  
  
[netapp-user@rhel7 ~]$ sudo cp /path/to/tls.crt  
/etc/docker/certs.d/astra-registry.apps.ocp-vmw.cie.netapp.com
```

- b. Log into OpenShift using the oc login command.

```
[netapp-user@rhel7 ~]$ oc login --token=sha256~D49SpB_lesSrJYwrM0LIO  
-VRcjWHu0a27vKa0 --server=https://api.ocp-vmw.cie.netapp.com:6443
```

- c. Log into the registry using OpenShift user credentials with the podman/docker command.

#### podman

```
[netapp-user@rhel7 ~]$ podman login astra-registry.apps.ocp-  
vmw.cie.netapp.com -u kubeadmin -p $(oc whoami -t) --tls  
-verify=false
```

+

NOTE: If you are using kubeadmin user to log into the private registry, then use token instead of password.

#### docker

```
[netapp-user@rhel7 ~]$ docker login astra-registry.apps.ocp-  
vmw.cie.netapp.com -u kubeadmin -p $(oc whoami -t)
```

+

NOTE: If you are using kubeadmin user to log into the private registry, then use token instead of password.

- d. Push or pull the images.

### **podman**

```
[netapp-user@rhel7 ~]$ podman push astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest  
[netapp-user@rhel7 ~]$ podman pull astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest
```

### **docker**

```
[netapp-user@rhel7 ~]$ docker push astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest  
[netapp-user@rhel7 ~]$ docker pull astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest
```

Next: [Solution Validation/Use Cases: Red Hat OpenShift with NetApp](#).

## **Solution Validation and Use Cases: Red Hat OpenShift with NetApp**

The examples provided on this page are solution validations and use cases for Red Hat OpenShift with NetApp.

- [Deploy a Jenkins CI/CD Pipeline with Persistent Storage](#)
- [Configure Multitenancy on Red Hat OpenShift with NetApp](#)
- [Red Hat OpenShift Virtualization with NetApp ONTAP](#)
- [Advanced Cluster Management for Kubernetes on Red Hat OpenShift with NetApp](#)

Next: [Videos and Demos](#).

## **Deploy a Jenkins CI/CD Pipeline with Persistent Storage: Red Hat OpenShift with NetApp**

This section provides the steps to deploy a continuous integration/continuous delivery or deployment (CI/CD) pipeline with Jenkins to validate solution operation.

### **Create the resources required for Jenkins deployment**

To create the resources required for deploying the Jenkins application, complete the following steps:

1. Create a new project named Jenkins.

# Create Project

Name \*

Display Name

Description

Cancel

Create

2. In this example, we deployed Jenkins with persistent storage. To support the Jenkins build, create the PVC. Navigate to Storage > Persistent Volume Claims and click Create Persistent Volume Claim. Select the storage class that was created, make sure that the Persistent Volume Claim Name is jenkins, select the appropriate size and access mode, and then click Create.

## Create Persistent Volume Claim

[Edit YAML](#)**Storage Class** SC basic

Storage class for the new claim.

**Persistent Volume Claim Name \*** jenkins

A unique name for the storage claim within the project.

**Access Mode \***

- Single User (RWO)
- Shared Access (RWX)
- Read Only (ROX)

Permissions to the mounted drive.

**Size \*** 100

GiB ▾

Desired storage capacity.

- 
- Use label selectors to request storage

Use label selectors to define how storage is created.

[Create](#)[Cancel](#)

### Deploy Jenkins with Persistent Storage

To deploy Jenkins with persistent storage, complete the following steps:

1. In the upper left corner, change the role from Administrator to Developer. Click +Add and select From Catalog. In the Filter by Keyword bar, search for jenkins. Select Jenkins Service with Persistent Storage.

## Developer Catalog

Add shared apps, services, or source-to-image builders to your project from the Developer Catalog. Cluster admins can install additional apps which will show up here automatically.

- [All Items](#)
- [Languages](#)
- [Databases](#)
- [Middleware](#)
- [CI/CD](#)
- [Other](#)

Type

- Operator Backed (0)
- Helm Charts (0)
- Builder Image (0)
- Template (4)
- Service Class (0)

All Items

Group By: None ▾

Jenkins
Template

provided by Red Hat, Inc.

Jenkins service, with persistent storage. NOTE: You must have persistent volumes available in...

Jenkins
Template

provided by Red Hat, Inc.

Jenkins service, with persistent storage. NOTE: You must have persistent volumes available in...

Jenkins (Ephemeral)
Template

provided by Red Hat, Inc.

Jenkins service, without persistent storage. WARNING: Any data stored will be lost upon...

Jenkins (Ephemeral)
Template

provided by Red Hat, Inc.

Jenkins service, without persistent storage. WARNING:

2. Click Instantiate Template.

### Jenkins

Provided by Red Hat, Inc.

[Instantiate Template](#)

Provider	Description
Red Hat, Inc.	Jenkins service, with persistent storage.
Support	NOTE: You must have persistent volumes available in your cluster to use this template.
<a href="#">Get support ↗</a>	
Created At	<a href="#">Documentation</a>
⌚ May 26, 3:58 am	<a href="https://docs.okd.io/latest/using_images/other_images/jenkins.html">https://docs.okd.io/latest/using_images/other_images/jenkins.html ↗</a>

3. By default, the details for the Jenkins application are populated. Based on your requirements, modify the parameters and click Create. This process creates all the required resources for supporting Jenkins on

## OpenShift.

### Instantiate Template

Namespace \*

Jenkins Service Name

The name of the OpenShift Service exposed for the Jenkins container.

Jenkins JNLP Service Name

The name of the service used for master/slave communication.

Enable OAuth in Jenkins

Whether to enable OAuth OpenShift integration. If false, the static account 'admin' will be initialized with the password 'password'.

Memory Limit

Maximum amount of memory the container can use.

Volume Capacity \*

Volume space available for data, e.g. 512Mi, 2Gi.

Jenkins ImageStream Namespace

The OpenShift Namespace where the Jenkins ImageStream resides.

Disable memory intensive administrative monitors

Whether to perform memory intensive, possibly slow, synchronization with the Jenkins Update Center on start. If true, the Jenkins core update monitor and site warnings monitor are disabled.

Jenkins ImageStreamTag

Name of the ImageStreamTag to be used for the Jenkins image.

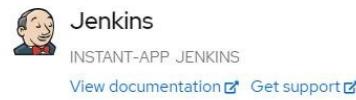
Fatal Error Log File

When a fatal error occurs, an error log is created with information and the state obtained at the time of the fatal error.

Allows use of Jenkins Update Center repository with invalid SSL certificate

Whether to allow use of a Jenkins Update Center that uses invalid certificate (self-signed, unknown CA). If any value other than 'false', certificate check is bypassed. By default, certificate check is enforced.

Create Cancel



Jenkins service, with persistent storage.

NOTE: You must have persistent volumes available in your cluster to use this template.

The following resources will be created:

- DeploymentConfig
- PersistentVolumeClaim
- RoleBinding
- Route
- Service
- ServiceAccount

4. The Jenkins pods take approximately 10 to 12 minutes to enter the Ready state.

## Pods

[Create Pod](#)


<span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px;">1</span>	Running	<span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px;">0</span>	Pending	<span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px;">0</span>	Terminating	<span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px;">0</span>	CrashLoopBackOff	<span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px;">1</span>	Completed	<span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px;">0</span>	Failed	<span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px;">0</span>	Unknown
---	---------	---	---------	---	-------------	---	------------------	---	-----------	---	--------	---	---------

[Select all filters](#)

1 of 2 Items

Name	Namespace	Status	Ready	Owner	Memory	CPU
jenkins-1-c77n9	jenkins	Running	1/1	jenkins-1	-	0.004 cores

5. After the pods are instantiated, navigate to Networking > Routes. To open the Jenkins webpage, click the URL provided for the jenkins route.

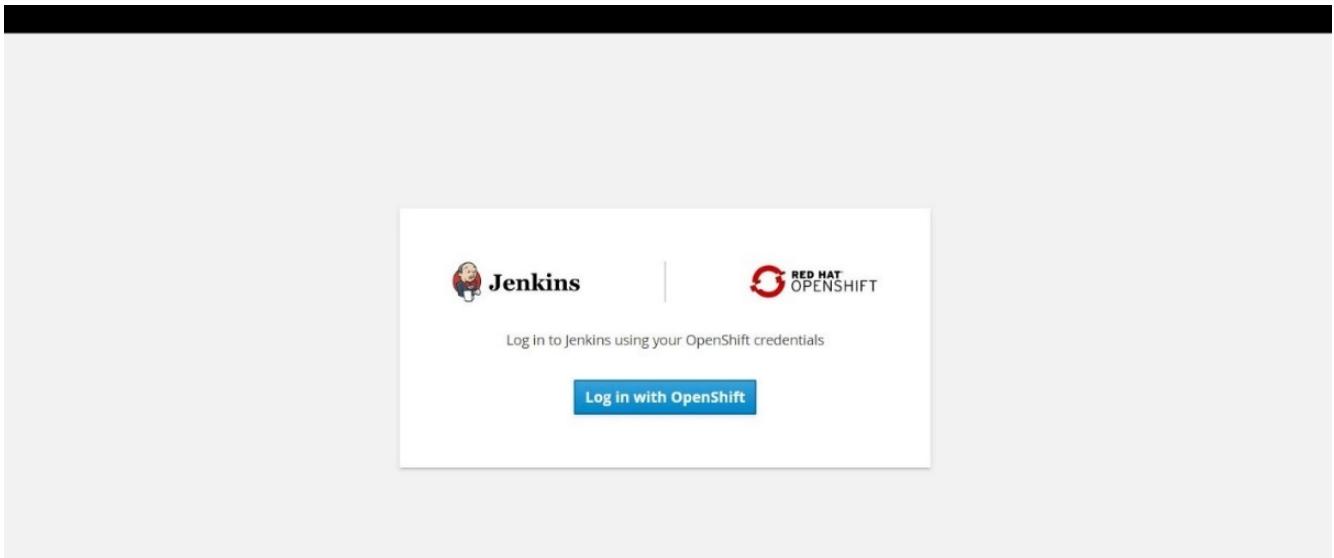
## Routes

[Create Route](#)


<span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px;">1</span>	Accepted	<span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px;">0</span>	Rejected	<span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px;">0</span>	Pending	<a href="#">Select all filters</a>	<span style="float: right;">1 Item</span>
---	----------	---	----------	---	---------	------------------------------------	---

Name	Namespace	Status	Location	Service
jenkins	jenkins	Accepted	<a href="https://jenkins-jenkins.apps.rhv-ocp-cluster.cie.netapp.com">https://jenkins-jenkins.apps.rhv-ocp-cluster.cie.netapp.com</a>	jenkins

6. Because OpenShift OAuth was used while creating the Jenkins app, click Log in with OpenShift.



7. Authorize the Jenkins service account to access the OpenShift users.

## Authorize Access

Service account jenkins in project jenkins is requesting permission to access your account (kube:admin)

### Requested permissions

#### user:info

Read-only access to your user information (including username, identities, and group membership)

#### user:check-access

Read-only access to view your privileges (for example, "can I create builds?")

You will be redirected to <https://jenkins-jenkins.apps.rhv-ocp-cluster.cie.netapp.com/securityRealm/finishLogin>

[Allow selected permissions](#) [Deny](#)

8. The Jenkins welcome page is displayed. Because we are using a Maven build, complete the Maven installation first. Navigate to Manage Jenkins > Global Tool Configuration, and then, in the Maven subhead, click Add Maven. Enter the name of your choice and make sure that the Install Automatically option is selected. Click Save.

Maven

Maven installations

Add Maven

Maven

Name: M3

Install automatically

Install from Apache

Version: 3.6.3

Add Installer

Delete Maven

9. You can now create a pipeline to demonstrate the CI/CD workflow. On the home page, click Create New Jobs or New Item from the left-hand menu.

The screenshot shows the Jenkins home page. At the top, there's a navigation bar with the Jenkins logo, a search bar, and user information (kube:admin | log out). Below the bar, a sidebar on the left lists links: New Item, People, Build History, Manage Jenkins, My Views, Open Blue Ocean, Lockable Resources, Credentials, and New View. The main content area features a "Welcome to Jenkins!" message with a sub-instruction: "Please [create new jobs](#) to get started." Below this, there are two sections: "Build Queue" (No builds in the queue) and "Build Executor Status" (1 Idle, 2 Idle).

10. On the Create Item page, enter the name of your choice, select Pipeline, and click Ok.

The screenshot shows the "Enter an item name" dialog. The input field contains "sample-demo". Below the input field, a note says "» Required field". A list of project types is shown with icons: Freestyle project (a box icon), Pipeline (a gear icon), Multi-configuration project (a wrench icon), Bitbucket Team/Project (a cloud icon), Folder (a folder icon), and GitHub Organization (a GitHub icon). At the bottom, there's an "OK" button and a note: "Creates a set of Pipeline projects according to detected branches in one SCM repository".

11. Select the Pipeline tab. From the Try Sample Pipeline drop-down menu, select Github + Maven. The code is automatically populated. Click Save.

General Build Triggers Advanced Project Options **Pipeline**

[Advanced...](#)

## Pipeline

Definition Pipeline script

Script

```

1  node {
2      def mvnHome
3      stage('Preparation') { // for display purposes
4          // Get some code from a GitHub repository
5          git 'https://github.com/jglick/simple-maven-project-with-tests.git'
6          // Get the Maven tool.
7          // ** NOTE: This 'M3' Maven tool must be configured
8          // ** in the global configuration.
9          mvnHome = tool 'M3'
10     }
11    stage('Build') {
12        // Run the maven build
13        withEnv(["MVN_HOME=$mvnHome"]) {
14            if (isUnix()) {
15                sh '$MVN_HOME/bin/mvn' -Dmaven.test.failure.ignore clean package'
16            } else {
17                bat("%MVN_HOME%\bin\mvn" -Dmaven.test.failure.ignore clean package)
18            }
19        }
20    }
21  }

```

GitHub + Maven

Use Groovy Sandbox

[Pipeline Syntax](#)

**Save** **Apply**

12. Click Build Now to trigger the development through the preparation, build, and testing phase. It can take several minutes to complete the whole build process and display the results of the build.

 Jenkins

Jenkins > sample-demo >

[Back to Dashboard](#)

[Status](#)

[Changes](#)

[Build Now](#)

[Delete Pipeline](#)

[Configure](#)

[Full Stage View](#)

[Open Blue Ocean](#)

[Rename](#)

[Pipeline Syntax](#)

**Pipeline sample-demo**

Last Successful Artifacts  
 [simple-maven-project-with-tests-1.0-SNAPSHOT.jar](#) 1.71 KB [view](#)

Recent Changes  


**Stage View**

Average stage times:  
(Average full run time: ~7s)

Preparation	Build	Results
2s	4s	69ms
2s	4s	69ms

 [Latest Test Result \(no failures\)](#)

#### Permalinks

- [Last build \(#1\), 1 min 23 sec ago](#)
- [Last stable build \(#1\), 1 min 23 sec ago](#)
- [Last successful build \(#1\), 1 min 23 sec ago](#)
- [Last completed build \(#1\), 1 min 23 sec ago](#)

13. Whenever there are any code changes, the pipeline can be rebuilt to patch the new version of software enabling continuous integration and continuous delivery. Click Recent Changes to track the changes from the previous version.

Next: Videos and Demos.

## Configure Multi-tenancy on Red Hat OpenShift with NetApp ONTAP

### Configuring multitenancy on Red Hat OpenShift with NetApp

Many organizations that run multiple applications or workloads on containers tend to deploy one Red Hat OpenShift cluster per application or workload. This allows them to implement strict isolation for the application or workload, optimize performance, and reduce security vulnerabilities. However, deploying a separate Red Hat OpenShift cluster for each application poses its own set of problems. It increases operational overhead having to monitor and manage each cluster on its own, increases cost owing to dedicated resources for different applications, and hinders efficient scalability.

To overcome these problems, one can consider running all the applications or workloads in a single Red Hat OpenShift cluster. But in such an architecture, resource isolation and application security vulnerabilities are one of the major challenges. Any security vulnerability in one workload could naturally spill over into another workload, thus increasing the impact zone. In addition, any abrupt uncontrolled resource utilization by one application can affect the performance of another application, because there is no resource allocation policy by default.

Therefore, organizations look out for solutions that pick up the best in both worlds, for example, by allowing them to run all their workloads in a single cluster and yet offering the benefits of a dedicated cluster for each workload.

One such effective solution is to configure multitenancy on Red Hat OpenShift. Multitenancy is an architecture that allows multiple tenants to coexist on the same cluster with proper isolation of resources, security, and so on. In this context, a tenant can be viewed as a subset of the cluster resources that are configured to be used by a particular group of users for an exclusive purpose. Configuring multitenancy on a Red Hat OpenShift cluster provides the following advantages:

- A reduction in CapEx and OpEx by allowing cluster resources to be shared
- Lower operational and management overhead
- Securing the workloads from cross-contamination of security breaches
- Protection of workloads from unexpected performance degradation due to resource contention

For a fully realized multitenant OpenShift cluster, quotas and restrictions must be configured for cluster resources belonging to different resource buckets: compute, storage, networking, security, and so on. Although we cover certain aspects of all the resource buckets in this solution, we focus on best practices for isolating and securing the data served or consumed by multiple workloads on the same Red Hat OpenShift cluster by configuring multitenancy on storage resources that are dynamically allocated by Astra Trident backed by NetApp ONTAP.

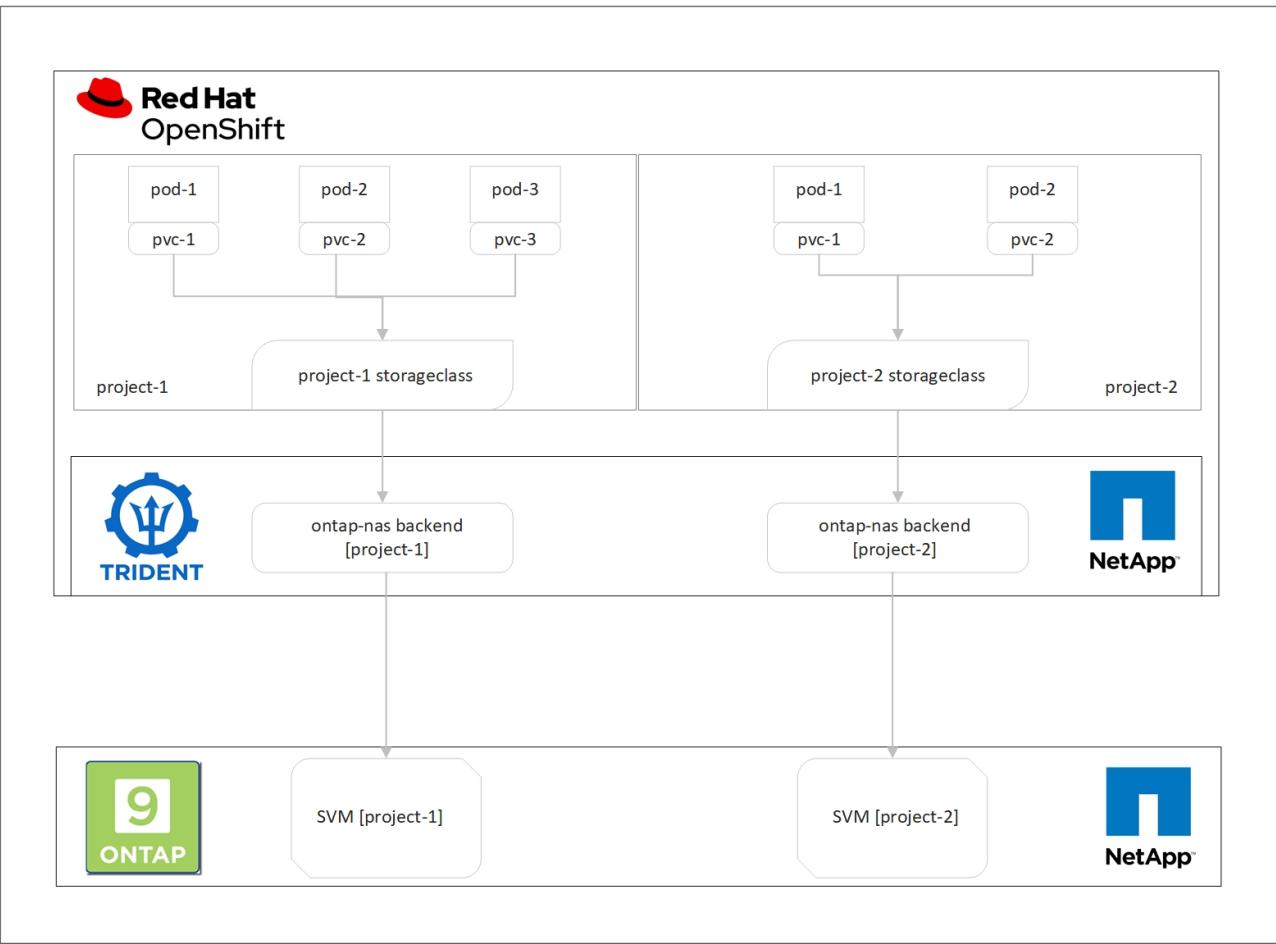
[Next: Architecture.](#)

## Architecture

Although Red Hat OpenShift and Astra Trident backed by NetApp ONTAP do not provide isolation between workloads by default, they offer a wide range of features that can be used to configure multitenancy. To better understand designing a multitenant solution on a Red Hat OpenShift cluster with Astra Trident backed by NetApp ONTAP, let us consider an example with a set of requirements and outline the configuration around it.

Let us assume that an organization runs two of its workloads on a Red Hat OpenShift cluster as part of two projects that two different teams are working on. The data for these workloads reside on PVCs that are dynamically provisioned by Astra Trident on a NetApp ONTAP NAS backend. The organization has a requirement to design a multitenant solution for these two workloads and isolate the resources used for these projects to make sure that security and performance is maintained, primarily focused on the data that serves those applications.

The following figure depicts the multitenant solution on a Red Hat OpenShift cluster with Astra Trident backed by NetApp ONTAP.



## Technology requirements

1. NetApp ONTAP storage cluster
2. Red Hat OpenShift cluster
3. Astra Trident

## Red Hat OpenShift – Cluster resources

From the Red Hat OpenShift cluster point of view, the top-level resource to start with is the project. An OpenShift project can be viewed as a cluster resource that divides the whole OpenShift cluster into multiple virtual clusters. Therefore, isolation at project level provides a base for configuring multitenancy.

Next up is to configure RBAC in the cluster. The best practice is to have all the developers working on a single project or workload configured into a single user group in the Identity Provider (IdP). Red Hat OpenShift allows IdP integration and user group synchronization thus allowing the users and groups from the IdP to be imported into the cluster. This helps the cluster administrators to segregate access of the cluster resources dedicated to a project to a user group or groups working on that project, thereby restricting unauthorized access to any cluster resources. To learn more about IdP integration with Red Hat OpenShift, see the documentation [here](#).

## NetApp ONTAP

It is important to isolate the shared storage serving as a persistent storage provider for a Red Hat OpenShift cluster to make sure that the volumes created on the storage for each project appear to the hosts as if they are

created on separate storage. To do this, create as many SVMs (storage virtual machines) on NetApp ONTAP as there are projects or workloads, and dedicate each SVM to a workload.

## Astra Trident

After you have different SVMs for different projects created on NetApp ONTAP, you must map each SVM to a different Trident backend. The backend configuration on Trident drives the allocation of persistent storage to OpenShift cluster resources, and it requires the details of the SVM to be mapped to. This should be the protocol driver for the backend at the minimum. Optionally, it allows you to define how the volumes are provisioned on the storage and to set limits for the size of volumes or usage of aggregates and so on. Details concerning the definition of the Trident backends can be found [here](#).

## Red Hat OpenShift – storage resources

After configuring the Trident backends, the next step is to configure StorageClasses. Configure as many storage classes as there are backends, providing each storage class access to spin up volumes only on one backend. We can map the StorageClass to a particular Trident backend by using the storagePools parameter while defining the storage class. The details to define a storage class can be found [here](#). Thus, there is a one-to-one mapping from StorageClass to Trident backend which points back to one SVM. This ensures that all storage claims via the StorageClass assigned to that project are served by the SVM dedicated to that project only.

Because storage classes are not namespaced resources, how do we ensure that storage claims to storage class of one project by pods in another namespace or project gets rejected? The answer is to use ResourceQuotas. ResourceQuotas are objects that control the total usage of resources per project. It can limit the number as well as the total amount of resources that can be consumed by objects in the project. Almost all the resources of a project can be limited using ResourceQuotas and using this efficiently can help organizations cut cost and outages due to overprovisioning or overconsumption of resources. Refer to the documentation [here](#) for more information.

For this use case, we need to limit the pods in a particular project from claiming storage from storage classes that are not dedicated to their project. To do that, we need to limit the persistent volume claims for other storage classes by setting `<storage-class-name>.storageclass.storage.k8s.io/persistentvolumeclaims` to 0. In addition, a cluster administrator must ensure that the developers in a project should not have access to modify the ResourceQuotas.

[Next: Configuration.](#)

## Configuration

For any multitenant solution, no user can have access to more cluster resources than is required. So, the entire set of resources that are to be configured as part of the multitenancy configuration is divided between cluster-admin, storage-admin, and developers working on each project.

The following table outlines the different tasks to be performed by different users:

Role	Tasks
<b>Cluster-admin</b>	Create projects for different applications or workloads
	Create ClusterRoles and RoleBindings for storage-admin
	Create Roles and RoleBindings for developers assigning access to specific projects
	[Optional] Configure projects to schedule pods on specific nodes
<b>Storage-admin</b>	Create SVMs on NetApp ONTAP
	Create Trident backends
	Create StorageClasses
	Create storage ResourceQuotas
<b>Developers</b>	Validate access to create or patch PVCs or pods in assigned project
	Validate access to create or patch PVCs or pods in another project
	Validate access to view or edit Projects, ResourceQuotas, and StorageClasses

[Next: Prerequisites.](#)

## Configuration

### Prerequisites

- NetApp ONTAP cluster
- Red Hat OpenShift cluster
- Trident installed on the cluster
- Admin workstation with tridentctl and oc tools installed and added to \$PATH
- Admin access to ONTAP
- Cluster-admin access to OpenShift cluster
- Cluster is integrated with Identity Provider
- Identity provider is configured to efficiently distinguish between users in different teams

[Next: Cluster Administrator Tasks.](#)

### Configuration: cluster-admin tasks

The following tasks are performed by the Red Hat OpenShift cluster-admin:

1. Log into Red Hat OpenShift cluster as the cluster-admin.
2. Create two projects corresponding to different projects.

```
oc create namespace project-1
oc create namespace project-2
```

### 3. Create the developer role for project-1.

```
cat << EOF | oc create -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: project-1
  name: developer-project-1
rules:
- verbs:
  - '*'
  apiGroups:
  - apps
  - batch
  - autoscaling
  - extensions
  - networking.k8s.io
  - policy
  - apps.openshift.io
  - build.openshift.io
  - image.openshift.io
  - ingress.operator.openshift.io
  - route.openshift.io
  - snapshot.storage.k8s.io
  - template.openshift.io
resources:
  - '*'
- verbs:
  - '*'
  apiGroups:
  - ''
resources:
  - bindings
  - configmaps
  - endpoints
  - events
  - persistentvolumeclaims
  - pods
  - pods/log
  - pods/attach
  - podtemplates
  - replicationcontrollers
```

```

- services
- limitranges
- namespaces
- componentstatuses
- nodes
- verbs:
  - '*'
apiGroups:
- trident.netapp.io
resources:
- tridentsnapshots
EOF

```



The role definition provided in this section is just an example. Developer roles must be defined based on end-user requirements.

4. Similarly, create developer roles for project-2.
5. All OpenShift and NetApp storage resources are usually managed by a storage admin. Access for storage administrators is controlled by the trident operator role that is created when Trident is installed. In addition to this, the storage admin also requires access to ResourceQuotas to control how storage is consumed.
6. Create a role for managing ResourceQuotas in all projects in the cluster to attach it to storage admin.

```

cat << EOF | oc create -f -
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: resource-quotas-role
rules:
- verbs:
  - '*'
apiGroups:
- ''
resources:
- resourcequotas
- verbs:
  - '*'
apiGroups:
- quota.openshift.io
resources:
- '*'
EOF

```

7. Make sure that the cluster is integrated with the organization's identity provider and that user groups are synchronized with cluster groups. The following example shows that the identity provider has been integrated with the cluster and synchronized with the user groups.

```
$ oc get groups
NAME                      USERS
ocp-netapp-storage-admins ocp-netapp-storage-admin
ocp-project-1              ocp-project-1-user
ocp-project-2              ocp-project-2-user
```

#### 8. Configure ClusterRoleBindings for storage admins.

```
cat << EOF | oc create -f -
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: netapp-storage-admin-trident-operator
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: ocp-netapp-storage-admins
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: trident-operator
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: netapp-storage-admin-resource-quotas-cr
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: ocp-netapp-storage-admins
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: resource-quotas-role
EOF
```



For storage admins, two roles must be bound: trident-operator and resource-quotas.

#### 9. Create RoleBindings for developers binding the developer-project-1 role to the corresponding group (ocp-project-1) in project-1.

```

cat << EOF | oc create -f -
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: project-1-developer
  namespace: project-1
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-project-1
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: developer-project-1
EOF

```

10. Similarly, create RoleBindings for developers binding the developer roles to the corresponding user group in project-2.

[Next: Storage Administrator Tasks.](#)

### Configuration: Storage-admin tasks

The following resources must be configured by a storage administrator:

1. Log into the NetApp ONTAP cluster as admin.
2. Navigate to Storage > Storage VMs and click Add. Create two SVMs, one for project-1 and the other for project-2, by providing the required details. Also create a vsadmin account to manage the SVM and its resources.

## Add Storage VM

X

STORAGE VM NAME

project-1-svm

### Access Protocol

SMB/CIFS, NFS

iSCSI

Enable SMB/CIFS

Enable NFS

Allow NFS client access

Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

RULES

Rule Index	Clients	Access Protocols	Read-Only R...	Read/Wr...
	10.61.181.0/24	Any	Any	Any

[+ Add](#)

DEFAULT LANGUAGE [?](#)

c.utf\_8



NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

K8s-Ontap-01

IP ADDRESS

SUBNET MASK

GATEWAY

BROADCAST DOMAIN

10.61.181.224

24

Add optional  
gateway

Default-4



3. Log into the Red Hat OpenShift cluster as the storage administrator.

4. Create the backend for project-1 and map it to the SVM dedicated to the project. NetApp recommends using the SVM's vsadmin account to connect the backend to SVM instead of using the ONTAP cluster administrator.

```

cat << EOF | tridentctl -n trident create backend -f
{
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "nfs_project_1",
    "managementLIF": "172.21.224.210",
    "dataLIF": "10.61.181.224",
    "svm": "project-1-svm",
    "username": "vsadmin",
    "password": "NetApp123"
}
EOF

```



We are using the ontap-nas driver for this example. Use the appropriate driver when creating the backend based on the use case.



We assume that Trident is installed in the trident project.

5. Similarly create the Trident backend for project-2 and map it to the SVM dedicated to project-2.
6. Next, create the storage classes. Create the storage class for project-1 and configure it to use the storage pools from backend dedicated to project-1 by setting the storagePools parameter.

```

cat << EOF | oc create -f -
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: project-1-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: ontap-nas
  storagePools: "nfs_project_1:.*"
EOF

```

7. Likewise, create a storage class for project-2 and configure it to use the storage pools from backend dedicated to project-2.
8. Create a ResourceQuota to restrict resources in project-1 requesting storage from storageclasses dedicated to other projects.

```
cat << EOF | oc create -f -
kind: ResourceQuota
apiVersion: v1
metadata:
  name: project-1-sc-rq
  namespace: project-1
spec:
  hard:
    project-2-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
EOF
```

9. Similarly, create a ResourceQuota to restrict resources in project-2 requesting storage from storageclasses dedicated to other projects.

[Next: Validation.](#)

## Validation

To validate the multitenant architecture that was configured in the previous steps, complete the following steps:

### Validate access to create PVCs or pods in assigned project

1. Log in as ocp-project-1-user, developer in project-1.
2. Check access to create a new project.

```
oc create ns sub-project-1
```

3. Create a PVC in project-1 using the storageclass that is assigned to project-1.

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-1
  namespace: project-1
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-1-sc
EOF
```

4. Check the PV associated with the PVC.

```
oc get pv
```

5. Validate that the PV and its volume is created in an SVM dedicated to project-1 on NetApp ONTAP.

```
volume show -vserver project-1-svm
```

6. Create a pod in project-1 and mount the PVC created in previous step.

```

cat << EOF | oc create -f -
kind: Pod
apiVersion: v1
metadata:
  name: test-pvc-pod
  namespace: project-1
spec:
  volumes:
    - name: test-pvc-project-1
      persistentVolumeClaim:
        claimName: test-pvc-project-1
  containers:
    - name: test-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
  volumeMounts:
    - mountPath: "/usr/share/nginx/html"
      name: test-pvc-project-1
EOF

```

7. Check if the pod is running and whether it mounted the volume.

```
oc describe pods test-pvc-pod -n project-1
```

**Validate access to create PVCs or pods in another project or use resources dedicated to another project**

1. Log in as ocp-project-1-user, developer in project-1.
2. Create a PVC in project-1 using the storageclass that is assigned to project-2.

```

cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-1-sc-2
  namespace: project-1
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-2-sc
EOF

```

### 3. Create a PVC in project-2.

```

cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-2-sc-1
  namespace: project-2
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-1-sc
EOF

```

### 4. Make sure that PVCs **test-pvc-project-1-sc-2** and **test-pvc-project-2-sc-1** were not created.

```

oc get pvc -n project-1
oc get pvc -n project-2

```

### 5. Create a pod in project-2.

```
cat << EOF | oc create -f -
kind: Pod
apiVersion: v1
metadata:
  name: test-pvc-pod
  namespace: project-1
spec:
  containers:
    - name: test-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
EOF
```

### Validate access to view and edit Projects, ResourceQuotas, and StorageClasses

1. Log in as ocp-project-1-user, developer in project-1.
2. Check access to create new projects.

```
oc create ns sub-project-1
```

3. Validate access to view projects.

```
oc get ns
```

4. Check if the user can view or edit ResourceQuotas in project-1.

```
oc get resourcequotas -n project-1
oc edit resourcequotas project-1-sc-rq -n project-1
```

5. Validate that the user has access to view the storageclasses.

```
oc get sc
```

6. Check access to describe the storageclasses.
7. Validate the user's access to edit the storageclasses.

```
oc edit sc project-1-sc
```

[Next: Scaling.](#)

## Scaling: Adding more projects

In a multitenant configuration, adding new projects with storage resources requires additional configuration to make sure that multitenancy is not violated. For adding more projects in a multitenant cluster, complete the following steps:

1. Log into the NetApp ONTAP cluster as a storage admin.
2. Navigate to Storage → Storage VMs and click Add. Create a new SVM dedicated to project-3. Also create a vsadmin account to manage the SVM and its resources.

## Add Storage VM

X

STORAGE VM NAME

project-3-svm

### Access Protocol

SMB/CIFS, NFS

iSCSI

Enable SMB/CIFS

Enable NFS

Allow NFS client access

Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

RULES

Rule Index	Clients	Access Protocols	Read-Only R...	Read/Wr...
	10.61.181.0/24	Any	Any	Any

[+ Add](#)

DEFAULT LANGUAGE [?](#)

c.utf\_8



NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

K8s-Ontap-01

IP ADDRESS

10.61.181.228

SUBNET MASK

24

GATEWAY

Add optional gateway

BROADCAST DOMAIN

Default-4



3. Log into the Red Hat OpenShift cluster as cluster admin.

4. Create a new project.

```
oc create ns project-3
```

5. Make sure that the user group for project-3 is created on IdP and synchronized with the OpenShift cluster.

```
oc get groups
```

## 6. Create the developer role for project-3.

```
cat << EOF | oc create -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: project-3
  name: developer-project-3
rules:
- verbs:
  - '*'
  apiGroups:
  - apps
  - batch
  - autoscaling
  - extensions
  - networking.k8s.io
  - policy
  - apps.openshift.io
  - build.openshift.io
  - image.openshift.io
  - ingress.operator.openshift.io
  - route.openshift.io
  - snapshot.storage.k8s.io
  - template.openshift.io
resources:
  - '*'
- verbs:
  - '*'
  apiGroups:
  - ''
resources:
  - bindings
  - configmaps
  - endpoints
  - events
  - persistentvolumeclaims
  - pods
  - pods/log
  - pods/attach
  - podtemplates
  - replicationcontrollers
  - services
```

```

- limitranges
- namespaces
- componentstatuses
- nodes
- verbs:
  - '*'
apiGroups:
- trident.netapp.io
resources:
- tridentsnapshots
EOF

```



The role definition provided in this section is just an example. The developer role must be defined based on the end-user requirements.

7. Create RoleBinding for developers in project-3 binding the developer-project-3 role to the corresponding group (ocp-project-3) in project-3.

```

cat << EOF | oc create -f -
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: project-3-developer
  namespace: project-3
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: ocp-project-3
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: developer-project-3
EOF

```

8. Login to the Red Hat OpenShift cluster as storage admin
9. Create a Trident backend and map it to the SVM dedicated to project-3. NetApp recommends using the SVM's vsadmin account to connect the backend to the SVM instead of using the ONTAP cluster administrator.

```

cat << EOF | tridentctl -n trident create backend -f
{
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "nfs_project_3",
    "managementLIF": "172.21.224.210",
    "dataLIF": "10.61.181.228",
    "svm": "project-3-svm",
    "username": "vsadmin",
    "password": "NetApp!23"
}
EOF

```



We are using the ontap-nas driver for this example. Use the appropriate driver for creating the backend based on the use-case.



We assume that Trident is installed in the trident project.

10. Create the storage class for project-3 and configure it to use the storage pools from backend dedicated to project-3.

```

cat << EOF | oc create -f -
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: project-3-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: ontap-nas
  storagePools: "nfs_project_3:.*"
EOF

```

11. Create a ResourceQuota to restrict resources in project-3 requesting storage from storageclasses dedicated to other projects.

```

cat << EOF | oc create -f -
kind: ResourceQuota
apiVersion: v1
metadata:
  name: project-3-sc-rq
  namespace: project-3
spec:
  hard:
    project-1-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
    project-2-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
EOF

```

12. Patch the ResourceQuotas in other projects to restrict resources in those projects from accessing storage from the storageclass dedicated to project-3.

```

oc patch resourcequotas project-1-sc-rq -n project-1 --patch
'{"spec":{"hard":{"project-3-
sc.storageclass.storage.k8s.io/persistentvolumeclaims": 0}}}'
oc patch resourcequotas project-2-sc-rq -n project-2 --patch
'{"spec":{"hard":{"project-3-
sc.storageclass.storage.k8s.io/persistentvolumeclaims": 0}}}'

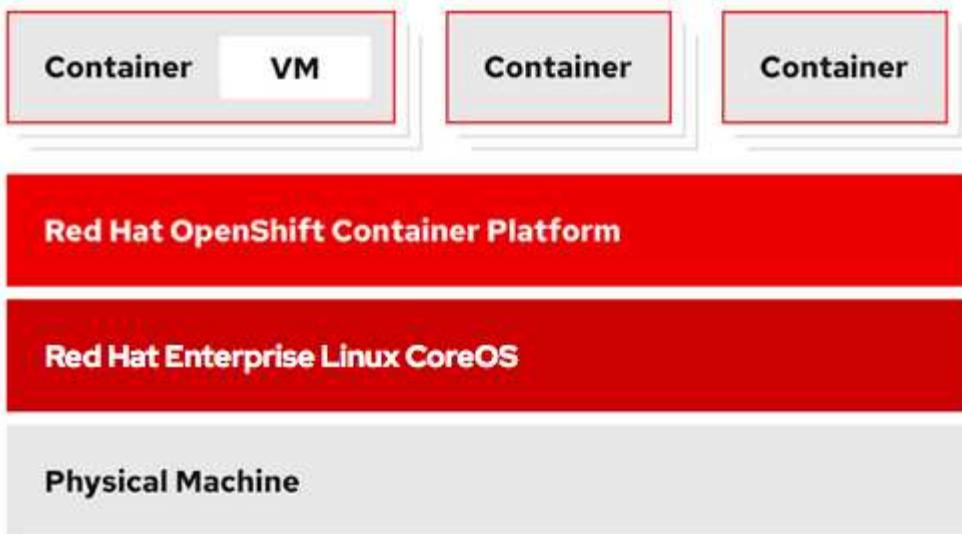
```

## Red Hat OpenShift Virtualization with NetApp ONTAP

### Red Hat OpenShift Virtualization with NetApp ONTAP

Depending on the specific use case, both containers and virtual machines (VMs) can serve as optimal platforms for different types of applications. Therefore, many organizations run some of their workloads on containers and some on VMs. Often, this leads organizations to face additional challenges by having to manage separate platforms: a hypervisor for VMs and a container orchestrator for applications.

To address this challenge, Red Hat introduced OpenShift Virtualization (formerly known as Container Native Virtualization) starting from OpenShift version 4.6. The OpenShift Virtualization feature enables you to run and manage virtual machines alongside containers on the same OpenShift Container Platform installation, providing hybrid management capability to automate deployment and management of VMs through operators. In addition to creating VMs in OpenShift, with OpenShift Virtualization, Red Hat also supports importing VMs from VMware vSphere, Red Hat Virtualization, and Red Hat OpenStack Platform deployments.



Certain features like live VM migration, VM disk cloning, VM snapshots and so on are also supported by OpenShift Virtualization with assistance from Astra Trident when backed by NetApp ONTAP. Examples of each of these workflows are discussed later in this document in their respective sections.

To learn more about Red Hat OpenShift Virtualization, see the documentation [here](#).

[Next: Deployment Prerequisites.](#)

## Deployment

### Deploy Red Hat OpenShift Virtualization with NetApp ONTAP

#### Prerequisites

- A Red Hat OpenShift cluster (later than version 4.6) installed on bare-metal infrastructure with RHCOS worker nodes
- The OpenShift cluster must be installed via installer provisioned infrastructure (IPI)
- Deploy Machine Health Checks to maintain HA for VMs
- A NetApp ONTAP cluster
- Astra Trident installed on the OpenShift cluster
- A Trident backend configured with an SVM on ONTAP cluster
- A StorageClass configured on the OpenShift cluster with Astra Trident as the provisioner
- Cluster-admin access to Red Hat OpenShift cluster
- Admin access to NetApp ONTAP cluster
- An admin workstation with tridentctl and oc tools installed and added to \$PATH

Because OpenShift Virtualization is managed by an operator installed on the OpenShift cluster, it imposes additional overhead on memory, CPU, and storage, which must be accounted for while planning the hardware requirements for the cluster. See the documentation [here](#) for more details.

Optionally, you can also specify a subset of the OpenShift cluster nodes to host the OpenShift Virtualization operators, controllers, and VMs by configuring node placement rules. To configure node placement rules for OpenShift Virtualization, follow the documentation [here](#).

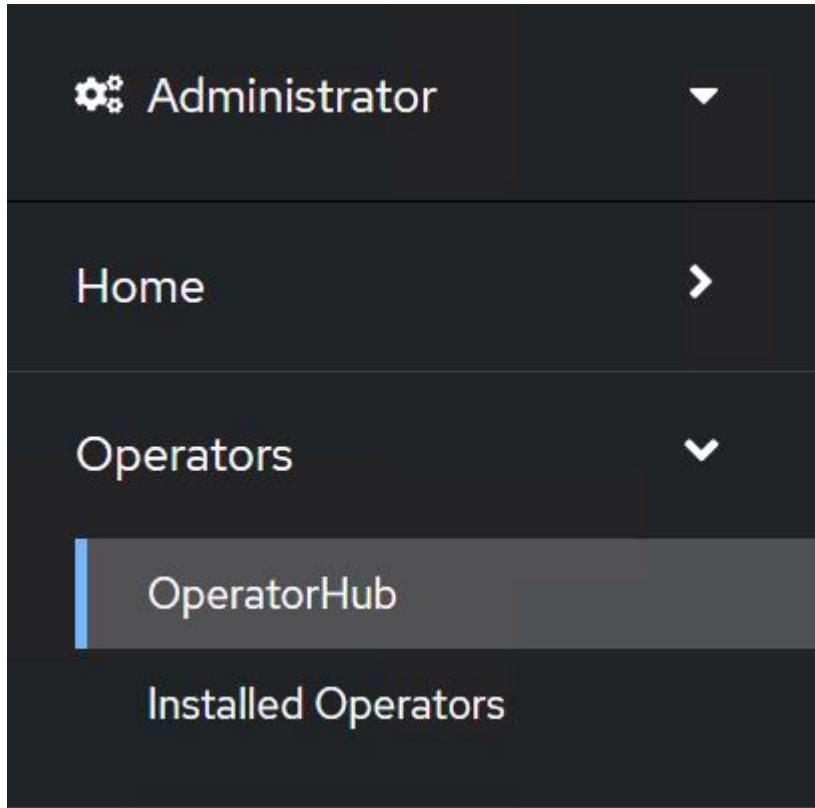
For the storage backing OpenShift Virtualization, NetApp recommends having a dedicated StorageClass that requests storage from a particular Trident backend, which in turn is backed by a dedicated SVM. This maintains a level of multitenancy with regard to the data being served for VM-based workloads on the OpenShift cluster.

Next: Deploy via operator.

#### Deploy Red Hat OpenShift Virtualization with NetApp ONTAP

To install OpenShift Virtualization, complete the following steps:

1. Log into the Red Hat OpenShift bare-metal cluster with cluster-admin access.
2. Select Administrator from the Perspective drop down.
3. Navigate to Operators > OperatorHub and search for OpenShift Virtualization.



4. Select the OpenShift Virtualization tile and click Install.



## OpenShift Virtualization

2.6.2 provided by Red Hat



Install

### Latest version

2.6.2

### Capability level

- Basic Install
- Seamless Upgrades
- Full Lifecycle
- Deep Insights
- Auto Pilot

### Provider type

Red Hat

### Provider

Red Hat

## Requirements

Your cluster must be installed on bare metal infrastructure with Red Hat Enterprise Linux CoreOS workers.

## Details

**OpenShift Virtualization** extends Red Hat OpenShift Container Platform, allowing you to host and manage virtualized workloads on the same platform as container-based workloads. From the OpenShift Container Platform web console, you can import a VMware virtual machine from vSphere, create new or clone existing VMs, perform live migrations between nodes, and more. You can use OpenShift Virtualization to manage both Linux and Windows VMs.

The technology behind OpenShift Virtualization is developed in the [KubeVirt](#) open source community. The KubeVirt project extends [Kubernetes](#) by adding additional virtualization resource types through [Custom Resource Definitions](#) (CRDs). Administrators can use Custom Resource Definitions to manage [VirtualMachine](#) resources alongside all other resources that Kubernetes provides.

- On the Install Operator screen, leave all default parameters and click **Install**.

### Update channel \*

- 2.1
- 2.2
- 2.3
- 2.4
- stable



OpenShift Virtualization  
provided by Red Hat

### Provided APIs

**OpenShift Virtualization Deployment** Required

Represents the deployment of OpenShift Virtualization

### Installation mode \*

- All namespaces on the cluster (default)  
This mode is not supported by this Operator
- A specific namespace on the cluster  
Operator will be available in a single Namespace only.

### Installed Namespace \*

- Operator recommended Namespace: **openshift-cnv**

#### Namespace creation

Namespace **openshift-cnv** does not exist and will be created.

- Select a Namespace

### Approval strategy \*

- Automatic
- Manual

Install

Cancel

6. Wait for the operator installation to complete.

The screenshot shows the OpenShift Virtualization operator page. At the top, there's a red circular icon with a white 'K8s' logo. To its right, the text 'OpenShift Virtualization' and '2.6.2 provided by Red Hat' is displayed. A progress bar is partially visible below this information.

## Installing Operator

The Operator is being installed. This may take a few minutes.

[View installed Operators in Namespace openshift-cnv](#)

7. After the operator has installed, click Create HyperConverged.

The screenshot shows the same OpenShift Virtualization operator page as before, but now with a large green circular icon containing a white checkmark to the right of the status text. The rest of the interface remains the same.

## Installed operator - operand required

The Operator has installed successfully. Create the required custom resource to be able to use this Operator.

**HC** HyperConverged ! Required

Creates and maintains an OpenShift Virtualization Deployment

[Create HyperConverged](#)

[View installed Operators in Namespace openshift-cnv](#)

8. On the Create HyperConverged screen, click Create, accepting all default parameters. This step starts the installation of OpenShift Virtualization.

**Name \***

**Labels**

**Infra** »

infra HyperConvergedConfig influences the pod configuration (currently only placement) for all the infra components needed on the virtualization enabled cluster but not necessarily directly on each node running VMs/VMIs.

**Workloads** »

workloads HyperConvergedConfig influences the pod configuration (currently only placement) of components which need to be running on a node where virtualization workloads should be able to run. Changes to Workloads HyperConvergedConfig can be applied only without existing workload.

**Bare Metal Platform**



true

BareMetalPlatform indicates whether the infrastructure is baremetal.

**Feature Gates** »

featureGates is a map of feature gate flags. Setting a flag to `true` will enable the feature. Setting `false` or removing the feature gate, disables the feature.

**Local Storage Class Name**

LocalStorageClassName the name of the local storage class.

**Create**

**Cancel**

- After all the pods move to the Running state in the openshift-cnv namespace and the OpenShift Virtualization operator is in the Succeeded state, the operator is ready to use. VMs can now be created on the OpenShift cluster.

Project: openshift-cnv ▾

**Installed Operators**

Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the [Understanding Operators documentation](#). Or create an Operator and ClusterServiceVersion using the [Operator SDK](#).

Name	Managed Namespaces	Status	Last updated	Provided APIs
 <a href="#">OpenShift Virtualization</a> 2.6.2 provided by Red Hat	 <a href="#">openshift-cnv</a>	<span style="color: green;">✓</span> Succeeded Up to date	May 18, 8:02 pm	<a href="#">OpenShift Virtualization Deployment</a> <a href="#">HostPathProvisioner deployment</a>

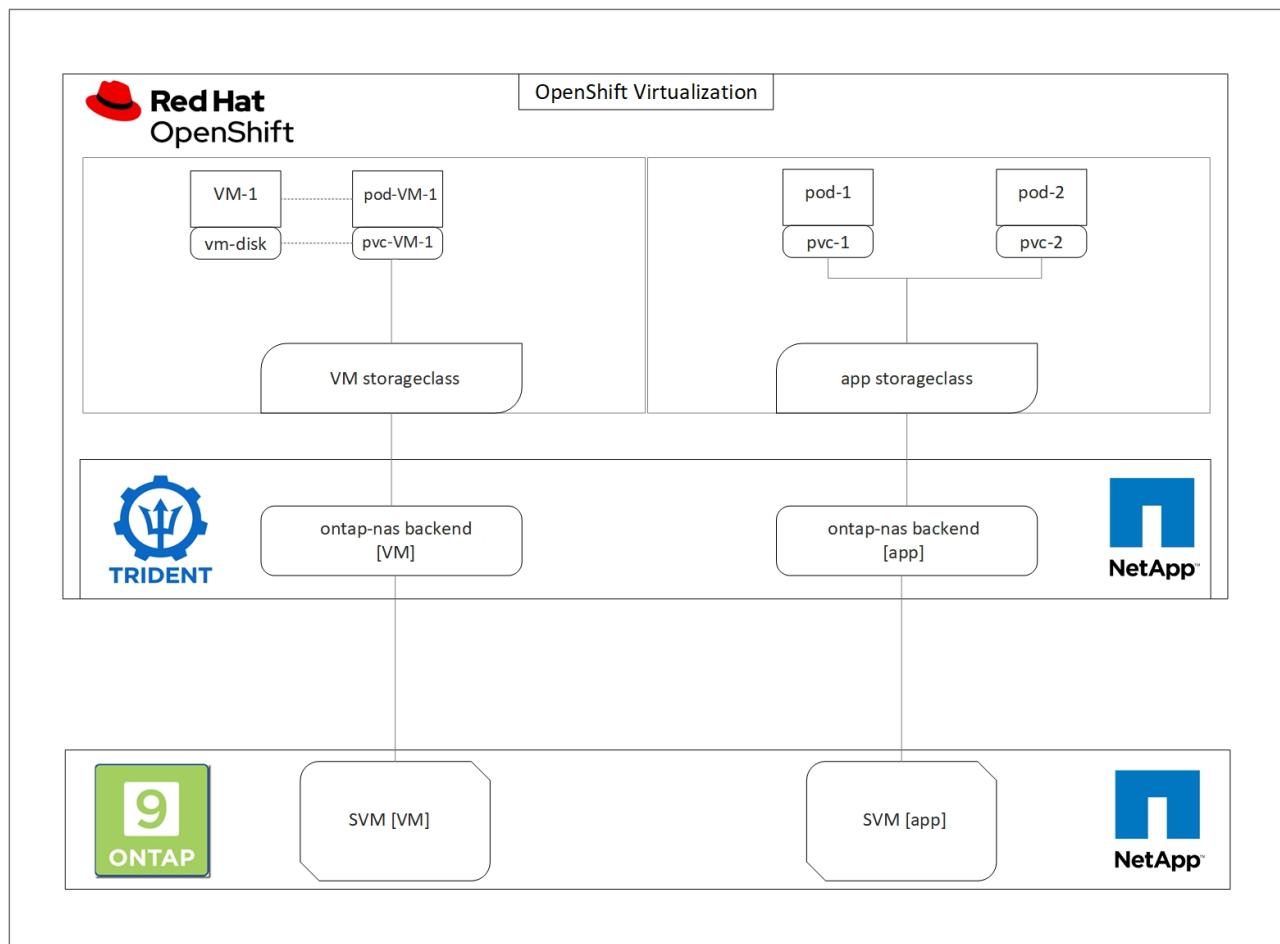
[Next: Workflows: Create VM.](#)

**Workflows**

**Workflows: Red Hat OpenShift Virtualization with NetApp ONTAP**

## Create VM

VMs are stateful deployments that require volumes to host the operating system and data. With CNV, because the VMs are run as pods, the VMs are backed by PVs hosted on NetApp ONTAP through Trident. These volumes are attached as disks and store the entire filesystem including the boot source of the VM.



To create a virtual machine on the OpenShift cluster, complete the following steps:

1. Navigate to Workloads > Virtualization > Virtual Machines and click Create > With Wizard.
2. Select the desired the operating system and click Next.
3. If the selected operating system has no boot source configured, you must configure it. For Boot Source, select whether you want to import the OS image from an URL or from a registry and provide the corresponding details. Expand Advanced and select the Trident-backed StorageClass. Then click Next.

## Boot source

This template does not have a boot source. Provide a custom boot source for this **CentOS 8.0+** VM virtual machine.

### Boot source type \*

Import via URL (creates PVC)

### Import URL \*

<https://access.cdn.redhat.com/content/origin/files/sha256/58/588167f828001e57688ec4b9b31c11a59d532489f527488ebc89ac5e952...>

Example: For RHEL, visit the [RHEL download page](#) (requires login) and copy the download link URL of the KVM guest image

Mount this as a CD-ROM boot source ?

### Persistent Volume Claim size \*

5 GiB ▾

Ensure your PVC size covers the requirements of the uncompressed image and any other space requirements. More storage can be added later.

### Advanced

### Storage class \*

basic (default)

### Access mode \*

Single User (RWO)

### Volume mode \*

Filesystem

4. If the selected operating system already has a boot source configured, the previous step can be skipped.
5. In the Review and Create pane, select the project you want to create the VM in and furnish the VM details. Make sure that the boot source is selected to be Clone and boot from CD-ROM with the appropriate PVC assigned for the selected OS.

1 Select template

2 Review and create

**Review and create**

You are creating a virtual machine from the Red Hat Enterprise Linux 8.0+ VM template.

**Project \***

PR default

**Virtual Machine Name \*** ⓘ

rhel8-light-bat

**Flavor \***

Small: 1 CPU | 2 GiB Memory

Storage	Workload profile ⓘ
40 GiB	server

**Boot source**

Clone and boot from CD-ROM

PVC rhel8

ⓘ A new disk has been added to support the CD-ROM boot source. Edit this disk by customizing the virtual machine.

▼ Disk details

rootdisk-install - Blank - 20GiB - virtio - default Storage class

Start this virtual machine after creation

**Create virtual machine**   **Customize virtual machine**   **Back**   **Cancel**

6. If you wish to customize the virtual machine, click Customize Virtual Machine and modify the required parameters.
7. Click Create Virtual Machine to create the virtual machine; this spins up a corresponding pod in the background.

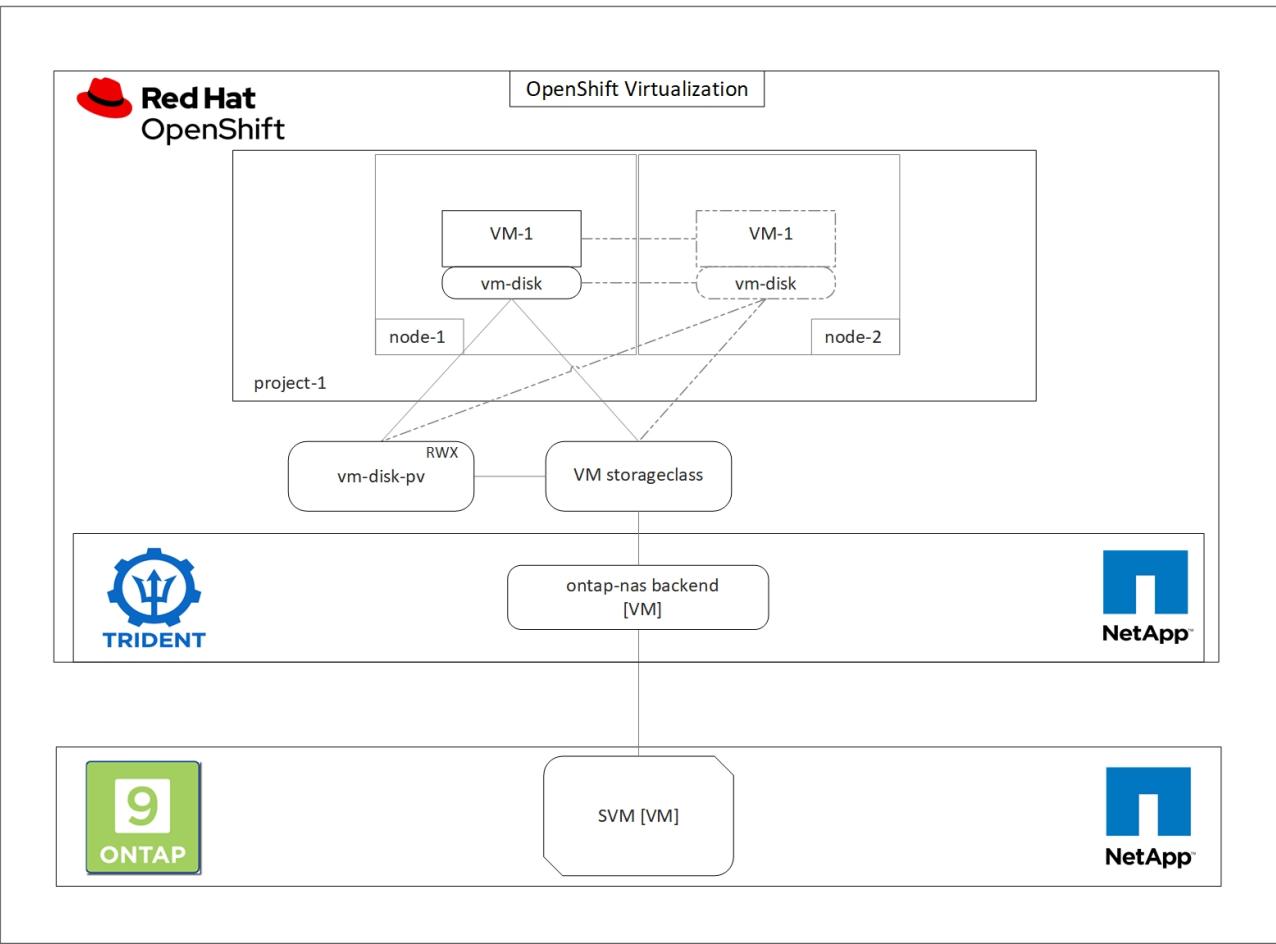
When a boot source is configured for a template or an operating system from an URL or from a registry, it creates a PVC in the openshift-virtualization-os-images project and downloads the KVM guest image to the PVC. You must make sure that template PVCs have enough provisioned space to accommodate the KVM guest image for the corresponding OS. These PVCs are then cloned and attached as rootdisks to virtual machines when they are created using the respective templates in any project.

[Next: Workflows: VM Live Migration.](#)

## Workflows: Red Hat OpenShift Virtualization with NetApp ONTAP

### VM Live Migration

Live Migration is a process of migrating a VM instance from one node to another in an OpenShift cluster with no downtime. For live migration to work in an OpenShift cluster, VMs must be bound to PVCs with shared ReadWriteMany access mode. Astra Trident backend configured with an SVM on a NetApp ONTAP cluster that is enabled for NFS protocol supports shared ReadWriteMany access for PVCs. Therefore, the VMs with PVCs that are requested from StorageClasses provisioned by Trident from NFS-enabled SVM can be migrated with no downtime.



To create a VM bound to PVCs with shared ReadWriteMany access:

1. Navigate to Workloads > Virtualization > Virtual Machines and click Create > With Wizard.
2. Select the desired the operating system and click Next. Let us assume the selected OS already had a boot source configured with it.
3. In the Review and Create pane, select the project you want to create the VM in and furnish the VM details. Make sure that the boot source is selected to be Clone and boot from CD-ROM with the appropriate PVC assigned for the selected OS.
4. Click Customize Virtual Machine and then click Storage.
5. Click the ellipsis next to rootdisk, and make sure that the storageclass provisioned using Trident is selected. Expand Advanced and select Shared Access (RWX) for Access Mode. Then click Save.

## Edit Disk

Type: Disk

Interface \*

virtio

Storage Class

basic (default)

▼ Advanced

Volume Mode

Filesystem

Volume Mode is set by Source PVC

Access Mode

Shared Access (RWX) - Not recommended for basic storage class

**ⓘ Access and Volume modes should follow storage feature matrix**

[Learn more ↗](#)

Cancel Save

6. Click Review and confirm and then click Create Virtual Machine.

To manually migrate a VM to another node in the OpenShift cluster, complete the following steps.

1. Navigate to Workloads > Virtualization > Virtual Machines.

2. For the VM you wish to migrate, click the ellipsis, and then click Migrate the Virtual Machine.

3. Click Migrate when the message pops up to confirm.



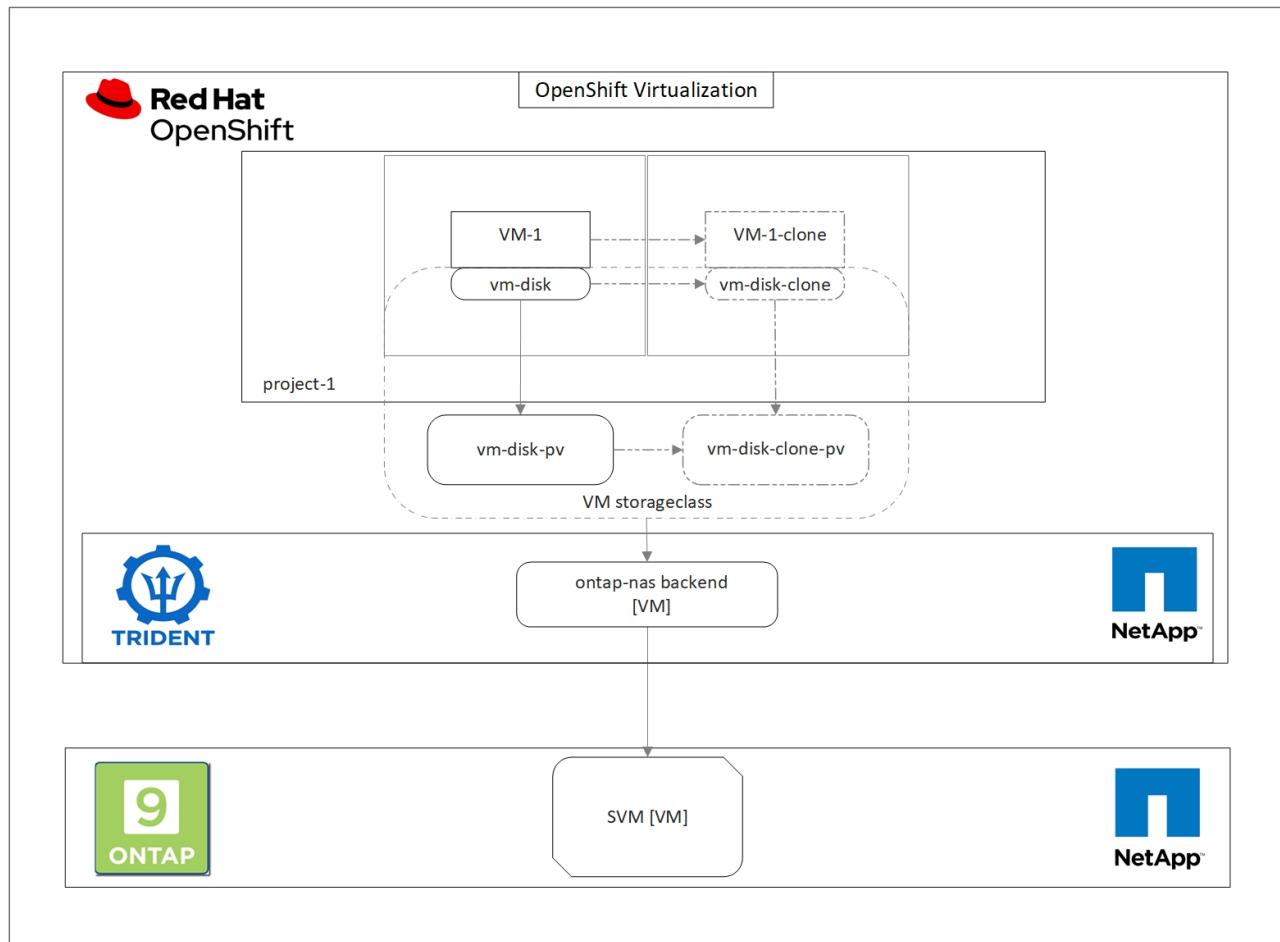
A VM instance in an OpenShift cluster automatically migrates to another node when the original node is placed into maintenance mode if the evictionStrategy is set to LiveMigrate.

[Next: Workflows: VM Cloning.](#)

## Workflows: Red Hat OpenShift Virtualization with NetApp ONTAP

### VM cloning

Cloning an existing VM in OpenShift is achieved with the support of Astra Trident's Volume CSI cloning feature. CSI volume cloning allows for creation of a new PVC using an existing PVC as the data source by duplicating its PV. After the new PVC is created, it functions as a separate entity and without any link to or dependency on the source PVC.



There are certain restrictions with CSI volume cloning to consider:

1. Source PVC and destination PVC must be in the same project.
2. Cloning is supported within the same storage class.
3. Cloning can be performed only when source and destination volumes use the same VolumeMode setting;

for example, a block volume can only be cloned to another block volume.

VMs in an OpenShift cluster can be cloned in two ways:

1. By shutting down the source VM
2. By keeping the source VM live

### **By Shutting down the source VM**

Cloning an existing VM by shutting down the VM is a native OpenShift feature that is implemented with support from Astra Trident. Complete the following steps to clone a VM.

1. Navigate to Workloads > Virtualization > Virtual Machines and click the ellipsis next to the virtual machine you wish to clone.
2. Click Clone Virtual Machine and provide the details for the new VM.

# Clone Virtual Machine

Name *	<input type="text" value="rhel8-short-frog-clone"/>											
Description	<input type="text"/>											
Namespace *	<input type="text" value="default"/>											
<input checked="" type="checkbox"/> Start virtual machine on clone												
Configuration	<table><tr><td>Operating System</td></tr><tr><td>Red Hat Enterprise Linux 8.0 or higher</td></tr><tr><td>Flavor</td></tr><tr><td>Small: 1 CPU   2 GiB Memory</td></tr><tr><td>Workload Profile</td></tr><tr><td>server</td></tr><tr><td>NICs</td></tr><tr><td>default - virtio</td></tr><tr><td>Disk</td></tr><tr><td>cloudinitdisk - cloud-init disk</td></tr><tr><td>rootdisk - 20Gi - basic</td></tr></table>	Operating System	Red Hat Enterprise Linux 8.0 or higher	Flavor	Small: 1 CPU   2 GiB Memory	Workload Profile	server	NICs	default - virtio	Disk	cloudinitdisk - cloud-init disk	rootdisk - 20Gi - basic
Operating System												
Red Hat Enterprise Linux 8.0 or higher												
Flavor												
Small: 1 CPU   2 GiB Memory												
Workload Profile												
server												
NICs												
default - virtio												
Disk												
cloudinitdisk - cloud-init disk												
rootdisk - 20Gi - basic												

**⚠ The VM rhel8-short-frog is still running. It will be powered off while cloning.**

[Cancel](#)

[Clone Virtual Machine](#)

3. Click Clone Virtual Machine; this shuts down the source VM and initiates the creation of the clone VM.
4. After this step is completed, you can access and verify the content of the cloned VM.

## By keeping the source VM live

An existing VM can also be cloned by cloning the existing PVC of the source VM and then creating a new VM using the cloned PVC. This method does not require you to shut down the source VM. Complete the following steps to clone a VM without shutting it down.

1. Navigate to Storage > PersistentVolumeClaims and click the ellipsis next to the PVC that is attached to the source VM.
2. Click Clone PVC and furnish the details for the new PVC.

## Clone

Name \*

rhel8-short-frog-rootdisk-28dvb-clone

Access Mode \*

Single User (RWO)  Shared Access (RWX)  Read Only (ROX)

Size \*

20

GiB



PVC details

Namespace	Requested capacity	Access mode
NS default	20 GiB	Shared Access (RWX)
Storage Class	Used capacity	Volume mode
SC basic	2.2 GiB	Filesystem

Cancel

Clone

3. Then click Clone. This creates a PVC for the new VM.
4. Navigate to Workloads > Virtualization > Virtual Machines and click Create > With YAML.
5. In the spec > template > spec > volumes section, attach the cloned PVC instead of the container disk. Provide all other details for the new VM according to your requirements.

```
- name: rootdisk
  persistentVolumeClaim:
    claimName: rhel8-short-frog-rootdisk-28dwb-clone
```

6. Click Create to create the new VM.
7. After the VM is created successfully, access and verify that the new VM is a clone of the source VM.

Next: [Workflows: Create VM from a Snapshot](#).

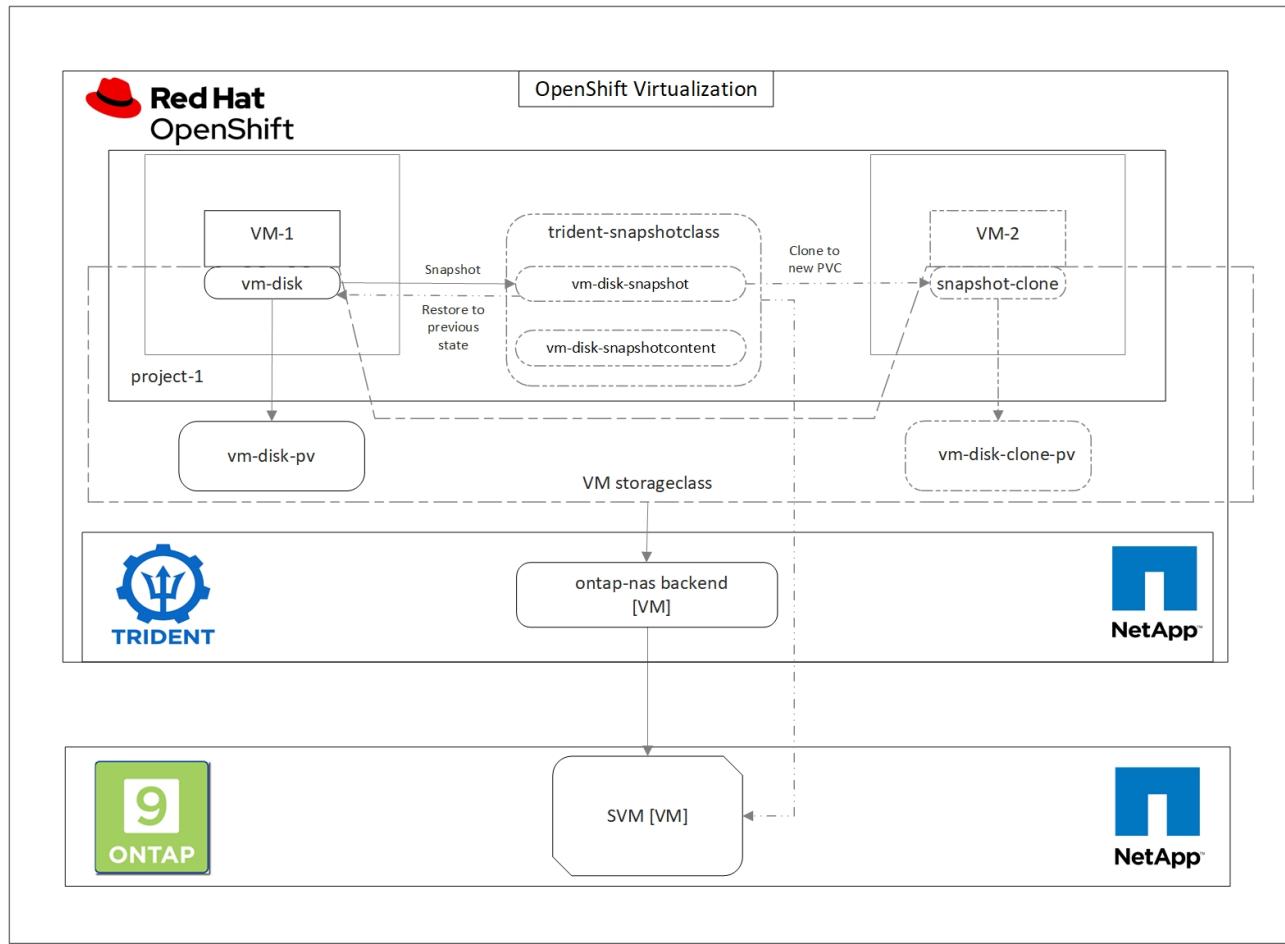
## Workflows: Red Hat OpenShift Virtualization with NetApp ONTAP

### Create VM from a Snapshot

With Astra Trident and Red Hat OpenShift, users can take a snapshot of a persistent volume on Storage Classes provisioned by it. With this feature, users can take a point-in-time copy of a volume and use it to create a new volume or restore the same volume back to a previous state. This enables or supports a variety of use-cases, from rollback to clones to data restore.

For Snapshot operations in OpenShift, the resources VolumeSnapshotClass, VolumeSnapshot, and VolumeSnapshotContent must be defined.

- A VolumeSnapshotContent is the actual snapshot taken from a volume in the cluster. It is cluster-wide resource analogous to PersistentVolume for storage.
- A VolumeSnapshot is a request for creating the snapshot of a volume. It is analogous to a PersistentVolumeClaim.
- VolumeSnapshotClass lets the administrator specify different attributes for a VolumeSnapshot. It allows you to have different attributes for different snapshots taken from the same volume.



To create Snapshot of a VM, complete the following steps:

1. Create a VolumeSnapshotClass that can then be used to create a VolumeSnapshot. Navigate to Storage > VolumeSnapshotClasses and click Create VolumeSnapshotClass.
2. Enter the name of the Snapshot Class, enter csi.trident.netapp.io for the driver, and click Create.

```

1  apiVersion: snapshot.storage.k8s.io/v1
2  kind: VolumeSnapshotClass
3  metadata:
4    name: trident-snapshot-class
5  driver: csi.trident.netapp.io
6  deletionPolicy: Delete
7

```

[Create](#)[Cancel](#) [Download](#)

3. Identify the PVC that is attached to the source VM and then create a Snapshot of that PVC. Navigate to Storage > VolumeSnapshots and click Create VolumeSnapshots.
4. Select the PVC that you want to create the Snapshot for, enter the name of the Snapshot or accept the default, and select the appropriate VolumeSnapshotClass. Then click Create.

## Create VolumeSnapshot

[Edit YAML](#)

**PersistentVolumeClaim \***

**PVC** rhel8-short-frog-rootdisk-28dvh

**Name \***

rhel8-short-frog-rootdisk-28dvh-snapshot

**Snapshot Class \***

**VSC** trident-snapshot-class

[Create](#)[Cancel](#)

5. This creates the snapshot of the PVC at that point in time.

## Create a new VM from the snapshot

1. First, restore the Snapshot into a new PVC. Navigate to Storage > VolumeSnapshots, click the ellipsis next to the Snapshot that you wish to restore, and click Restore as new PVC.
2. Enter the details of the new PVC and click Restore. This creates a new PVC.

## Restore as new PVC

When restore action for snapshot **rhel8-short-frog-rootdisk-28dvb-snapshot** is finished a new crash-consistent PVC copy will be created.

Name \*

rhel8-short-frog-rootdisk-28dvb-snapshot-restore

Storage Class \*

SC basic

Access Mode \*

Single User (RWO)  Shared Access (RWX)  Read Only (ROX)

Size \*

20

GiB



VolumeSnapshot details

Created at

May 21, 12:46 am

Namespace

default

Status

Ready

API version

snapshot.storage.k8s.io/v1

Size

20 GiB

3. Next, create a new VM from this PVC. Navigate to Workloads > Virtualization > Virtual Machines and click Create > With YAML.
4. In the spec > template > spec > volumes section, specify the new PVC created from Snapshot instead of

from the container disk. Provide all other details for the new VM according to your requirements.

```
- name: rootdisk
  persistentVolumeClaim:
    claimName: rhel8-short-frog-rootdisk-28dvb-snapshot-restore
```

5. Click Create to create the new VM.
6. After the VM is created successfully, access and verify that the new VM has the same state as that of the VM whose PVC was used to create the snapshot at the time when the snapshot was created.

## Advanced Cluster Management for Kubernetes on Red Hat OpenShift with NetApp

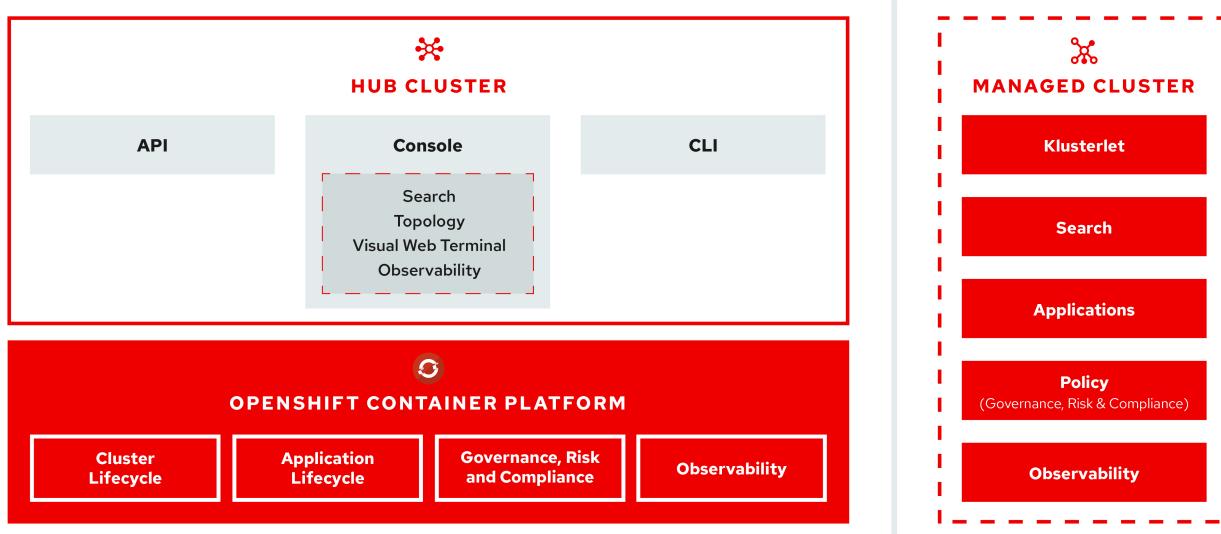
### Advanced Cluster Management for Kubernetes: Red Hat OpenShift with NetApp

As a containerized application transitions from development to production, many organizations require multiple Red Hat OpenShift clusters to support the testing and deployment of that application. In conjunction with this, organizations usually host multiple applications or workloads on OpenShift clusters. Therefore, each organization ends up managing a set of clusters, and OpenShift administrators must thus face the added challenge of managing and maintaining multiple clusters across a range of environments that span multiple on-premises data centers and public clouds. To address these challenges, Red Hat introduced Advanced Cluster Management for Kubernetes.

Red Hat Advanced Cluster Management for Kubernetes enables you to perform the following tasks:

1. Create, import, and manage multiple clusters across data centers and public clouds
2. Deploy and manage applications or workloads on multiple clusters from a single console
3. Monitor and analyze health and status of different cluster resources
4. Monitor and enforce security compliance across multiple clusters

Red Hat Advanced Cluster Management for Kubernetes is installed as an add-on to a Red Hat OpenShift cluster, and it uses this cluster as a central controller for all its operations. This cluster is known as hub cluster, and it exposes a management plane for the users to connect to Advanced Cluster Management. All the other OpenShift clusters that are either imported or created via the Advanced Cluster Management console are managed by the hub cluster and are called managed clusters. It installs an agent called Klusterlet on the managed clusters to connect them to the hub cluster and serve the requests for different activities related to cluster lifecycle management, application lifecycle management, observability, and security compliance.



For more information, see the documentation [here](#).

[Next: Deployment Prerequisites.](#)

## Deployment

### Deploy Advanced Cluster Management for Kubernetes

#### Prerequisites

1. A Red Hat OpenShift cluster (greater than version 4.5) for the hub cluster
2. Red Hat OpenShift clusters (greater than version 4.4.3) for managed clusters
3. Cluster-admin access to the Red Hat OpenShift cluster
4. A Red Hat subscription for Advanced Cluster Management for Kubernetes

Advanced Cluster Management is an add-on on for the OpenShift cluster, so there are certain requirements and restrictions on the hardware resources based on the features used across the hub and managed clusters. You need to take these issues into account when sizing the clusters. See the documentation [here](#) for more details.

Optionally, if the hub cluster has dedicated nodes for hosting infrastructure components and you would like to install Advanced Cluster Management resources only on those nodes, you need to add tolerations and selectors to those nodes accordingly. For more details, see the documentation [here](#).

[Next: Installation.](#)

### Deploy Advanced Cluster Management for Kubernetes

To install Advanced Cluster Management for Kubernetes on an OpenShift cluster, complete the following steps:

1. Choose an OpenShift cluster as the hub cluster and log into it with cluster-admin privileges.
2. Navigate to Operators > Operators Hub and search for Advanced Cluster Management for Kubernetes.

The screenshot shows the Red Hat OpenShift OperatorHub. The left sidebar is titled 'Administrator' and has sections for Home, Projects, Search, Explore, Events, Operators, OperatorHub (which is selected), and Installed Operators. The main area is titled 'Project: default' and shows 'All Items'. A search bar says 'Filter by keyword...'. There are 450 items. The 'Community' section displays three operators:

- 3scale API Management** provided by Red Hat
- Advanced Cluster Management for Kubernetes** provided by Red Hat
- Akka Cluster Operator** provided by Lightbend, Inc.

3. Select Advanced Cluster Management for Kubernetes and click Install.

### Advanced Cluster Management for Kubernetes

2.2.3 provided by Red Hat

**Install**

---

<b>Latest version</b>	2.2.3
<b>Capability level</b>	Red Hat Advanced Cluster Management for Kubernetes provides the multicluster hub, a central management console for managing multiple Kubernetes-based clusters across data centers, public clouds, and private clouds. You can use the hub to create Red Hat OpenShift Container Platform clusters on selected providers, or import existing Kubernetes-based clusters. After the clusters are managed, you can set compliance requirements to ensure that the clusters maintain the specified security requirements. You can also deploy business applications across your clusters.
<b>Provider type</b>	Red Hat Advanced Cluster Management for Kubernetes also provides the following operators:
<b>Provider</b>	<ul style="list-style-type: none"> <li>• Multicluster subscriptions: An operator that provides application management capabilities including subscribing to resources from a channel and deploying those resources on MCH-managed Kubernetes clusters based on placement rules.</li> <li>• Hive for Red Hat OpenShift: An operator that provides APIs for provisioning and performing initial configuration of OpenShift clusters. These operators are used by the multicluster hub to provide its provisioning and application-management capabilities.</li> </ul>
<b>Infrastructure features</b>	<b>How to Install</b>
Disconnected	Use of this Red Hat product requires a licensing and subscription agreement.

4. On the Install Operator screen, provide the necessary details (NetApp recommends retaining the default parameters) and click Install.

## Install Operator

Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.

### Update channel \*

- release-2.0
- release-2.1
- release-2.2

### Installation mode \*

- All namespaces on the cluster (default)  
This mode is not supported by this Operator
- A specific namespace on the cluster  
Operator will be available in a single Namespace only.

### Installed Namespace \*

- Operator recommended Namespace: **PR open-cluster-management**

 Namespace creation

Namespace **open-cluster-management** does not exist and will be created.

- Select a Namespace

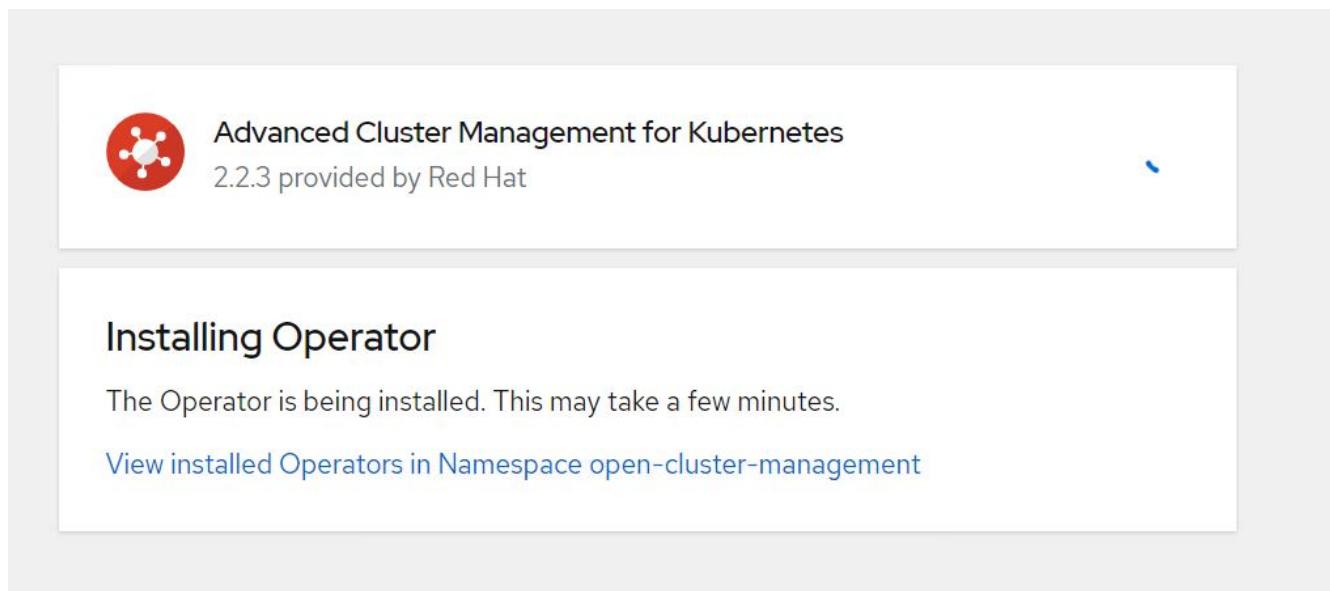
### Approval strategy \*

- Automatic
- Manual

**Install**

**Cancel**

5. Wait for the operator installation to complete.



The screenshot shows a status card for the "Advanced Cluster Management for Kubernetes" operator, version 2.2.3 provided by Red Hat. The card has a red circular icon with a white cluster symbol. The title is "Advanced Cluster Management for Kubernetes" and the version is "2.2.3 provided by Red Hat". Below the title, it says "Installing Operator". A message states "The Operator is being installed. This may take a few minutes." and provides a link "View installed Operators in Namespace open-cluster-management".

6. After the operator is installed, click Create MultiClusterHub.



## Advanced Cluster Management for Kubernetes

2.2.3 provided by Red Hat



### Installed operator - operand required

The Operator has installed successfully. Create the required custom resource to be able to use this Operator.

**MCH** MultiClusterHub ! Required

Advanced provisioning and management of OpenShift and Kubernetes clusters

[Create MultiClusterHub](#)

[View installed Operators in Namespace open-cluster-management](#)

- On the Create MultiClusterHub screen, click Create after furnishing the details. This initiates the installation of a multi-cluster hub.

Project: open-cluster-management ▾

Advanced Cluster Management for Kubernetes > Create MultiClusterHub

#### Create MultiClusterHub

Create by completing the form. Default values may be provided by the Operator authors.

Configure via:  Form view  YAML view

i Note: Some fields may not be represented in this form view. Please select "YAML view" for full control.

MultiClusterHub  
provided by Red Hat

MultiClusterHub defines the configuration for an instance of the MultiCluster Hub

Name \*

multicluscherhub

Labels

app=frontend

» Advanced configuration

[Create](#)

[Cancel](#)

- After all the pods move to the Running state in the open-cluster-management namespace and the operator moves to the Succeeded state, Advanced Cluster Management for Kubernetes is installed.

## Installed Operators

Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the [Understanding Operators documentation](#). Or create an Operator and ClusterServiceVersion using the [Operator SDK](#).

Name	Managed Namespaces	Status	Provided APIs
 Advanced Cluster Management for Kubernetes 2.2.3 provided by Red Hat	NS open-cluster-management	Succeeded Up to date	MultiClusterHub ClusterManager ClusterDeployment ClusterState <a href="#">View 25 more...</a>

9. It takes some time to complete the hub installation, and, after it is done, the MultiCluster hub moves to Running state.

Installed Operators > Operator details

 Advanced Cluster Management for Kubernetes  
2.2.3 provided by Red Hat

Actions ▾

Details YAML Subscription Events All instances **MultiClusterHub** ClusterManager ClusterDeployment ClusterSt...

**MultiClusterHubs**

Create MultiClusterHub

Name	Kind	Status	Labels
MCH multiclusterhub	MultiClusterHub	Phase: <span style="color: green;">✓</span> Running	No labels

10. It creates a route in the open-cluster-management namespace. Connect to the URL in the route to access the Advanced Cluster Management console.

Project: open-cluster-management ▾

**Routes**

Create Route

Filter ▾ Name mul

Name mul X Clear all filters

Name	Status	Location	Service
RT multicloud-console	<span style="color: green;">✓</span> Accepted	<a href="https://multicloud-console.apps.ocp-vmware2.cie.netapp.com">https://multicloud-console.apps.ocp-vmware2.cie.netapp.com</a>	S management-ingress

[Next: Features - Cluster Lifecycle Management.](#)

## Features

### Features: Advanced Cluster Management for Kubernetes on Red Hat OpenShift with NetApp

#### Cluster Lifecycle Management

To manage different OpenShift clusters, you can either create or import them into Advanced Cluster Management.

1. First navigate to Automate Infrastructures > Clusters.
2. To create a new OpenShift cluster, complete the following steps:
  - a. Create a provider connection: Navigate to Provider Connections and click Add a Connection, provide all the details corresponding to the selected provider type and click Add.

Select a provider and enter basic information

Provider \* ⓘ

aws Amazon Web Services

Connection name \* ⓘ

nik-hcl-aws

Namespace \* ⓘ

default

Configure your provider connection

Base DNS domain ⓘ

cie.netapp.com

AWS access key ID \* ⓘ

AKIATCFBZDOIASDSAH

AWS secret access key \* ⓘ

.....

Red Hat OpenShift pull secret \* ⓘ

```
FuS3pNbktVaHpINFc2MkZsbmtBVGN6TktmUlZXcHcxOW9teEZwQ0lYZld3cjJobGxJeDBQNOxIzeOyeGM5Q0ZwZk5RR2JUanIxNnNUM21Rb0FJb
UFjNC1BylpEWVZE0HltNxkTMDZPUVpoWFRHcGwtREIDQ2RSYlJRaTlxblDLT2oyQ3pVeUJfNllwcENSa2YyOUsyLWZGSFVfNA=","email":"Nikhil.k
ulkarni@netapp.com"}, "registry.redhat.io":
```

SSH private key \* ⓘ

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmuAAAAAeasdadssadm9uZQAAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACCLcwLgAvSIHAEp+DevIRNzaG2zkNreMIZ/UHyf0UWvAAAAAJh/wa6xf8Gu
```

SSH public key \* ⓘ

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIltzAuAC746agdh21cB4/4N6/VE3NobbOQ2t4zVn9QfJ/RRa8A root@nik-rhel8
```

- b. To create a new cluster, navigate to Clusters and click Add a Cluster > Create a Cluster. Provide the details for the cluster and the corresponding provider and click Create.

**Configuration**

Cluster name \* ⓘ  
rh-aws

**Distribution**

Select the type of Kubernetes distribution to use for your cluster.

Red Hat OpenShift

Select an infrastructure provider to host your Red Hat OpenShift cluster.

AWS Amazon Web Services

Google Cloud

Microsoft Azure

VMware vSphere

Bare Metal

Release image \* ⓘ  
quay.io/openshift-release-dev/ocp-release:4.7.12-x86\_64

Provider connection \* ⓘ  
nik-hcl-aws

Add a connection

- c. After the cluster is created, it appears in the cluster list with the status Ready.
3. To import an existing cluster, complete the following steps:
  - a. Navigate to Clusters and click Add a Cluster > Import an Existing Cluster.
  - b. Enter the name of the cluster and click Save Import and Generate Code. A command to add the existing cluster is displayed.
  - c. Click Copy Command and run the command on the cluster to be added to the hub cluster. This initiates the installation of the necessary agents on the cluster, and, after this process is complete, the cluster appears in the cluster list with status Ready.

Name \*

Additional labels

Once you click on "Save import and generate code", the information you entered will be used to generate the code and cannot be modified anymore. If you wish to change any information, you will have to delete and re-import this cluster.

Code generated successfully  Import saved

Run a command

1. Copy this command  
Click the button to have the command automatically copied to your clipboard.  
[Copy command](#)

2. Run this command with kubectl configured for your targeted cluster to start the import  
Log in to the existing cluster in your terminal and run the command.

[View cluster](#)

[Import another](#)

4. After you create and import multiple clusters, you can monitor and manage them from a single console.

[Next: Features - Application Lifecycle Management.](#)

## Features: Advanced Cluster Management for Kubernetes on Red Hat OpenShift with NetApp

### Application lifecycle management

To create an application and manage it across a set of clusters,

1. Navigate to Manage Applications from the sidebar and click Create Application. Provide the details of the application you would like to create and click Save.

## Create an application

 YAML: Off

Cancel

Save

Name\* ⓘ  
demo-app

Namespace\* ⓘ  
default X ▾

Repository location for resources

Repository types

Select the type of repository where resources that you want to deploy are located

Git

URL\* ⓘ  
<https://github.com/open-cluster-management/acm-hive-openshift-releases.git> X ▾

Branch ⓘ  
main X ▾

Path ⓘ  
clusterImageSets/fast/4.7 X ▾

2. After the application components are installed, the application appears in the list.

## Applications

⟳ Refresh every 15s ▾

Last update: 7:36:23 PM

Create application

Search						
Name	Namespace	Clusters	Resource	Time window	Created	⋮
demo-app	default	Local	Git <input checked="" type="checkbox"/>		8 days ago	⋮
1-1 of 1	◀◀	<	1	of 1	>	▶▶

3. The application can now be monitored and managed from the console.

Next: [Features - governance and risk](#).

## Features: Advanced Cluster Management for Kubernetes on Red Hat OpenShift with NetApp

### Governance and risk

This feature allows you to define the compliance policies for different clusters and make sure that the clusters adhere to it. You can configure the policies to either inform or remediate any deviations or violations of the rules.

1. Navigate to Governance and Risk from the sidebar.
2. To create compliance policies, click Create Policy, enter the details of the policy standards, and select the clusters that should adhere to this policy. If you want to automatically remediate the violations of this policy, select the checkbox Enforce if Supported and click Create.

# Create policy ⓘ



YAML: Off

**Name \***

policy-complianceoperator

**Namespace \*** ⓘ

default

**Specifications \*** ⓘ

1x ComplianceOperator

**Cluster selector** ⓘ

1x local-cluster: "true"

**Standards** ⓘ

1x NIST-CSF

**Categories** ⓘ

1x PR.IP Information Protection Processes and Procedures

**Controls** ⓘ

1x PR.IP-1 Baseline Configuration

 Enforce if supported ⓘ Disable policy ⓘ

3. After all the required policies are configured, any policy or cluster violations can be monitored and remediated from Advanced Cluster Management.

## Governance and risk ⓘ

Filter

Refresh every 10s

Last update: 12:54:01 PM

Create policy

Summary 1

Standards ▾

NIST-CSF



No violations found

Based on the industry standards, there are no cluster or policy violations.

Policies

Cluster violations

Find policies

Policy name	Namespace	Remediation	Cluster violations	Standards	Categories	Controls	Created	⋮
policy-complianceoperator	default	inform	0/1	NIST-CSF	PR.IP Information Protection Processes and Procedures	PR.IP-1 Baseline Configuration	32 minutes ago	⋮

1 - 1 of 1

« «

1

of 1

» »

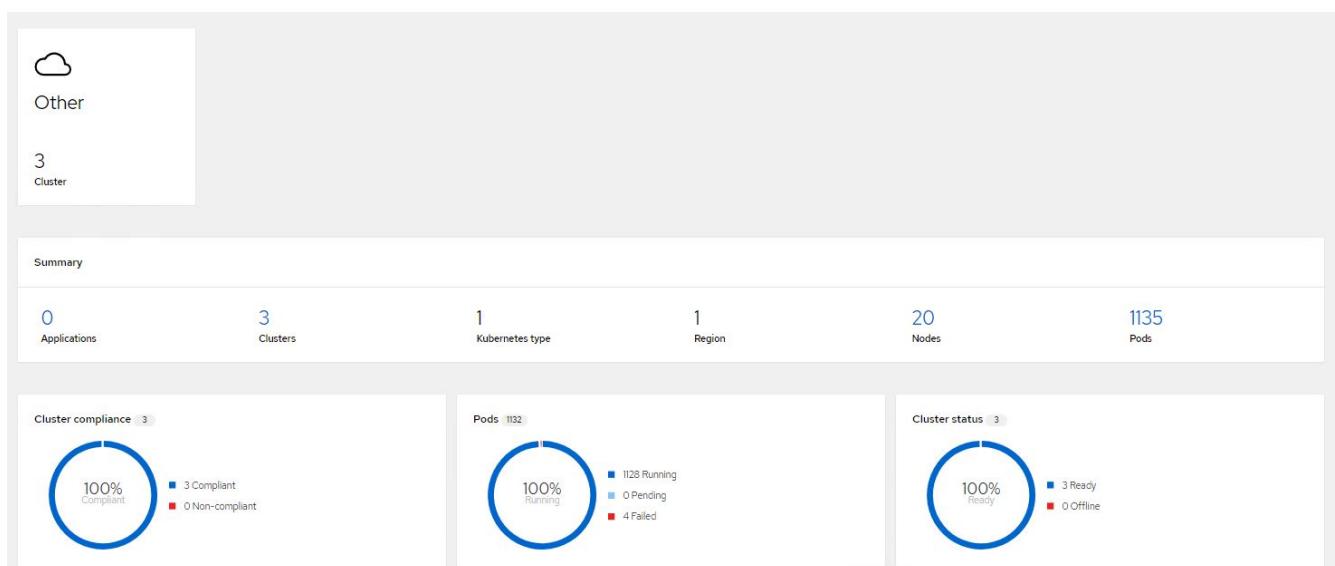
Next: Features - Observability.

## Features: Advanced Cluster Management for Kubernetes on Red Hat OpenShift with NetApp

### Observability

Advanced Cluster Management for Kubernetes provides a way to monitor the nodes, pods, and applications, and workloads across all the clusters.

1. Navigate to Observe Environments > Overview.

[Overview](#)
[+ Add provider connection](#)
[Refresh every 1m](#)  
Last update 12:35:03 AM


2. All pods and workloads across all clusters are monitored and sorted based on a variety of filters. Click Pods to view the corresponding data.

[Search](#)
[Saved searches ▾](#) | [Open new search tab](#)

3 Related cluster
673 Related secret
20 Related node
8 Related persistentvolumeclaim

8 Related persistentvolume
1 Related provisioning
2 Related searchcollector
3 Related iampolicycontroller

[Show all \(38\)](#)

▼ Pod (1135)

Name	14bbd46d68f3ddd50b9328cee6854a36807ef784dac2bded9cc20638fbpd582	⋮
Namespace	openshift-marketplace	
Cluster	local-cluster	
Status	Completed	
Restarts	0	
Host IP	10.61.186.27	
Pod IP	10.129.2.215	
Created	4 days ago	
Labels	controller-uid=dd259738-2cce-40e2-85d3-6ccf56904ba8	

3. All nodes across the clusters are monitored and analyzed based on a variety of data points. Click Nodes to get more insight into the corresponding details.

## Search

Saved searches ▾ | Open new search tab ↗

3 Related cluster	1k Related pod	12 Related service
-------------------	----------------	--------------------

Show all (3)

▼ Node (20)

Name	Cluster	Role	Architecture	OS image	CPU	Created	Labels
ocp-master-1-ocp-bare-metal.cie.netapp.com	ocp-bare-metal	master; worker	amd64	Red Hat Enterprise Linux CoreOS 47.83.202103292105-0 (Octpa)	48	a month ago	beta.kubernetes.io/arch=amd64 beta.kubernetes.io/os=linux kubernetes.io/arch=amd64 5 more
ocp-master-2-ocp-bare-metal.cie.netapp.com	ocp-bare-metal	master; worker	amd64	Red Hat Enterprise Linux CoreOS 47.83.202103292105-0 (Octpa)	48	a month ago	beta.kubernetes.io/arch=amd64 beta.kubernetes.io/os=linux kubernetes.io/arch=amd64 5 more
ocp-master-3-ocp-bare-metal.cie.netapp.com	ocp-bare-metal	master; worker	amd64	Red Hat Enterprise Linux CoreOS 47.83.202103292105-0 (Octpa)	48	a month ago	beta.kubernetes.io/arch=amd64 beta.kubernetes.io/os=linux kubernetes.io/arch=amd64 5 more

4. All clusters are monitored and organized based on different cluster resources and parameters. Click Clusters to view cluster details.

## Search

Saved searches ▾ | Open new search tab ↗

3k Related secret	787 Related pod	15 Related persistentvolumeclaim	17 Related node	1 Related application
15 Related persistentvolume	1 Related searchcollector	8 Related clusterclaim	3 Related resourcequota	5 Related identity

Show all (159)

▼ Cluster (2)

Name	Available	Hub accepted	Joined	Nodes	Kubernetes version	CPU	Memory	Console URL	Labels
local-cluster	True	True	True	8	v1.20.0+c8905da	84	418501Mi	Launch	cloud=VSphere clusterID=148632d9-69d5-4ae4-98ee-8df886463c3 installer.name=multiclusterhub 4 more
ocp-vmw	True	True	True	9	v1.20.0+df9c838	28	111981Mi	Launch	cloud=VSphere clusterID=9d76ac4e-4aae-4d45-a2e8-1b6b54282fe name=ocp-vmw 1 more

Next: Features - Create Resources.

## Features: Advanced Cluster Management for Kubernetes on Red Hat OpenShift with NetApp

### Create resources on multiple clusters

Advanced Cluster Management for Kubernetes allows users to create resources on one or more managed clusters simultaneously from the console. As an example, if you have OpenShift clusters at different sites backed with different NetApp ONTAP clusters and want to provision PVC's at both sites, you can click the (+) sign on the top bar. Then select the clusters on which you want to create the PVC, paste the resource YAML, and click Create.

## Create resource

Cancel

Create

Clusters | Select the clusters where the resource(s) will be deployed.

2 x local-cluster, ocp-vmw

Resource configuration | Enter the configuration manifest for the resource(s).

YAML

```
1 kind: PersistentVolumeClaim
2 apiVersion: v1
3 metadata:
4   name: demo-pvc
5 spec:
6   accessModes:
7     - ReadWriteOnce
8   resources:
9     requests:
10    storage: 1Gi
11  storageClassName: ocp-trident
```

## Videos and Demos: Red Hat OpenShift with NetApp

The following video demonstrate some of the capabilities documented in this document:

- Video: Accelerate Software Development with Astra Control and NetApp FlexClone Technology
- Video: Leverage NetApp Astra Control to Perform Post-mortem Analysis and Restore Your Application
- Video: Data Protection in CI/CD pipeline with Astra Control
- Video: Workload Migration using Astra Control Center - Red Hat OpenShift with NetApp
- Video: Workload Migration using Astra Trident and SnapMirror - Red Hat OpenShift with NetApp
- Video: Installing OpenShift Virtualization - Red Hat OpenShift with NetApp
- Video: Deploying a Virtual Machine with OpenShift Virtualization - Red Hat OpenShift with NetApp
- Video: NetApp HCI for Red Hat OpenShift on Red Hat Virtualization Deployment

Next: Additional Information: Red Hat OpenShift with NetApp.

## Additional Information: Red Hat OpenShift with NetApp

To learn more about the information described in this document, review the following websites:

- NetApp Documentation  
<https://docs.netapp.com/>
- Astra Trident Documentation  
<https://docs.netapp.com/us-en/trident/index.html>
- NetApp Astra Control Center Documentation

<https://docs.netapp.com/us-en/astra-control-center/>

- Red Hat OpenShift Documentation

[https://access.redhat.com/documentation/en-us/openshift\\_container\\_platform/4.7/](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.7/)

- Red Hat OpenStack Platform Documentation

[https://access.redhat.com/documentation/en-us/red\\_hat\\_openstack\\_platform/16.1/](https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/16.1/)

- Red Hat Virtualization Documentation

[https://access.redhat.com/documentation/en-us/red\\_hat\\_virtualization/4.4/](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.4/)

- VMware vSphere Documentation

<https://docs.vmware.com/>

## NVA-1165: Anthos with NetApp

Alan Cowles and Nikhil Kulkarni, NetApp

This reference document provides deployment validation of the Anthos with NetApp solution by NetApp and our engineering partners, when it is deployed in multiple data center environments.

It also details storage integration with NetApp storage systems by making use of the Astra Trident storage orchestrator for the management of persistent storage.

Lastly, a number of solution validations and real world use cases are explored and documented.

### Use cases

The Anthos with NetApp solution is architected to deliver exceptional value for customers with the following use cases:

- Easy to deploy and manage Anthos environment deployed using the provided 'bmctl' tool on bare metal or the 'gkectl' tool on VMware vSphere.
- Combined power of enterprise container and virtualized workloads with Anthos deployed virtually on vSphere or on bare metal with [kubevirt](#).
- Real-world configuration and use cases highlighting Anthos features when used with NetApp storage and Astra Trident, the open-source storage orchestrator for Kubernetes.

### Business value

Enterprises are increasingly adopting DevOps practices to create new products, shorten release cycles, and rapidly add new features. Because of their innate agile nature, containers and microservices play a crucial role in supporting DevOps practices. However, practicing DevOps at a production scale in an enterprise environment presents its own challenges and imposes certain requirements on the underlying infrastructure, such as the following:

- High availability at all layers in the stack
- Ease of deployment procedures

- Nondisruptive operations and upgrades
- API-driven and programmable infrastructure to keep up with microservices agility
- Multitenancy with performance guarantees
- Ability to run virtualized and containerized workloads simultaneously
- Ability to scale infrastructure independently based on workload demands

The Anthos with NetApp solution acknowledges these challenges and presents a solution that helps address each concern by implementing the fully automated deployment of Anthos On Prem in the customers data center environment of choice.

## **Technology overview**

The Anthos with NetApp solution is comprised of the following major components:

### **Anthos On Prem**

Anthos On Prem is a fully supported enterprise Kubernetes platform that can be deployed in the VMware vSphere hypervisor, or on a bare metal infrastructure of your choosing.

For more information about Anthos, see the Anthos website located [here](#).

### **NetApp storage systems**

NetApp has several storage systems perfect for enterprise data centers and hybrid cloud deployments. The NetApp portfolio includes NetApp ONTAP, NetApp Element, and NetApp e-Series storage systems, all of which can provide persistent storage for containerized applications.

For more information visit the NetApp website [here](#).

### **NetApp storage integrations**

Astra Trident is an open-source and fully-supported storage orchestrator for containers and Kubernetes distributions, including Anthos.

For more information, visit the Astra Trident website [here](#).

## **Advanced configuration options**

This section is dedicated to customizations that real world users would likely need to perform when deploying this solution into production, such as creating a dedicated private image registry or deploying custom load balancer instances.

## **Current support matrix for validated releases**

Technology	Purpose	Software version
NetApp ONTAP	Storage	9.8, 9.9.1
NetApp Element	Storage	12.3
NetApp Astra Trident	Storage Orchestration	22.01.0
Anthos Clusters on VMware	Container orchestration	1.10

Anthos on bare metal	Container Orchestration	1.10
VMware vSphere	Data center virtualization	6.7U3, 7.0U3

Next: [Anthos Overview: Anthos with NetApp](#).

## Anthos Overview

Anthos with NetApp is a verified, best-practice hybrid cloud architecture for the deployment of an on-premises Google Kubernetes Engine (GKE) environment in a reliable and dependable manner. This NetApp Verified Architecture reference document serves as both a design guide and a deployment validation of the Anthos with NetApp solution deployed to bare metal and virtual environments. The architecture described in this document has been validated by subject matter experts at NetApp and Google Cloud to provide the advantages of running Anthos within your enterprise data-center environment.

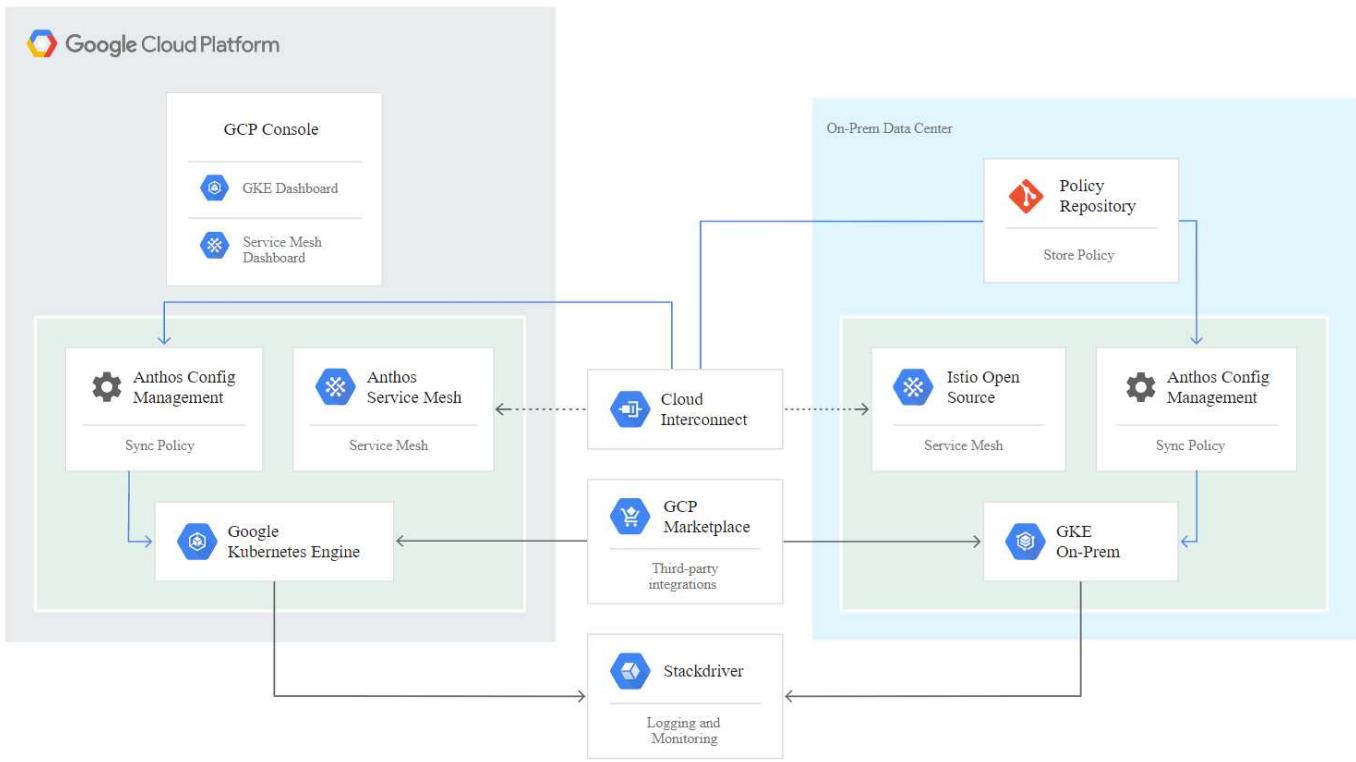
### Anthos

Anthos is a hybrid-cloud Kubernetes data center solution that enables organizations to construct and manage modern hybrid-cloud infrastructures while adopting agile workflows focused on application development. Anthos on VMware, a solution built on open-source technologies, runs on-premises in a VMware vSphere-based infrastructure, which can connect and interoperate with Anthos GKE in Google Cloud. Adopting containers, service mesh, and other transformational technologies enables organizations to experience consistent application development cycles and production-ready workloads in local and cloud-based environments. The following figure depicts the Anthos solution and how a deployment in an on-premises data center interconnects with infrastructure in the cloud.

For more information about Anthos, see the Anthos website located [here](#).

Anthos provides the following features:

- **Anthos configuration management.** Automates the policy and security of hybrid Kubernetes deployments.
- **Anthos Service Mesh.** Enhances application observability, security, and control with an Istio-powered service mesh.
- **Google Cloud Marketplace for Kubernetes Applications.** A catalog of curated container applications available for easy deployment.
- **Migrate for Anthos.** Automatic migration of physical services and VMs from on-premises to the cloud.
- **Stackdriver.** Management service offered by Google for logging and monitoring cloud instances.



## Deployment methods for Anthos

### Anthos clusters on VMware

Anthos clusters deployed to VMware vSphere environments are easy to deploy, maintain, and scale rapidly for most end-user Kubernetes workloads.

For more information about Anthos clusters on VMware, deployed with NetApp, please visit the page [here](#).

### Anthos on bare metal

Anthos clusters deployed on bare metal servers are hardware agnostic and allow you to select a compute platform optimized for your personalized use case.

For more information about Anthos on bare metal clusters deployed with NetApp, please visit the page [here](#).

Next: [NetApp Storage Overview: Anthos with NetApp](#).

### Anthos Clusters on VMware: Anthos with NetApp

Anthos clusters on VMware is an extension of Google Kubernetes Engine that is deployed in an end user's private data center. An organization can deploy the same applications designed to run in containers in Google Cloud in Kubernetes clusters on-premises.

Anthos clusters on VMware can be deployed into an existing VMware vSphere environment in your data center, which can save on capital expenses and enable more rapid deployment and scaling operations.

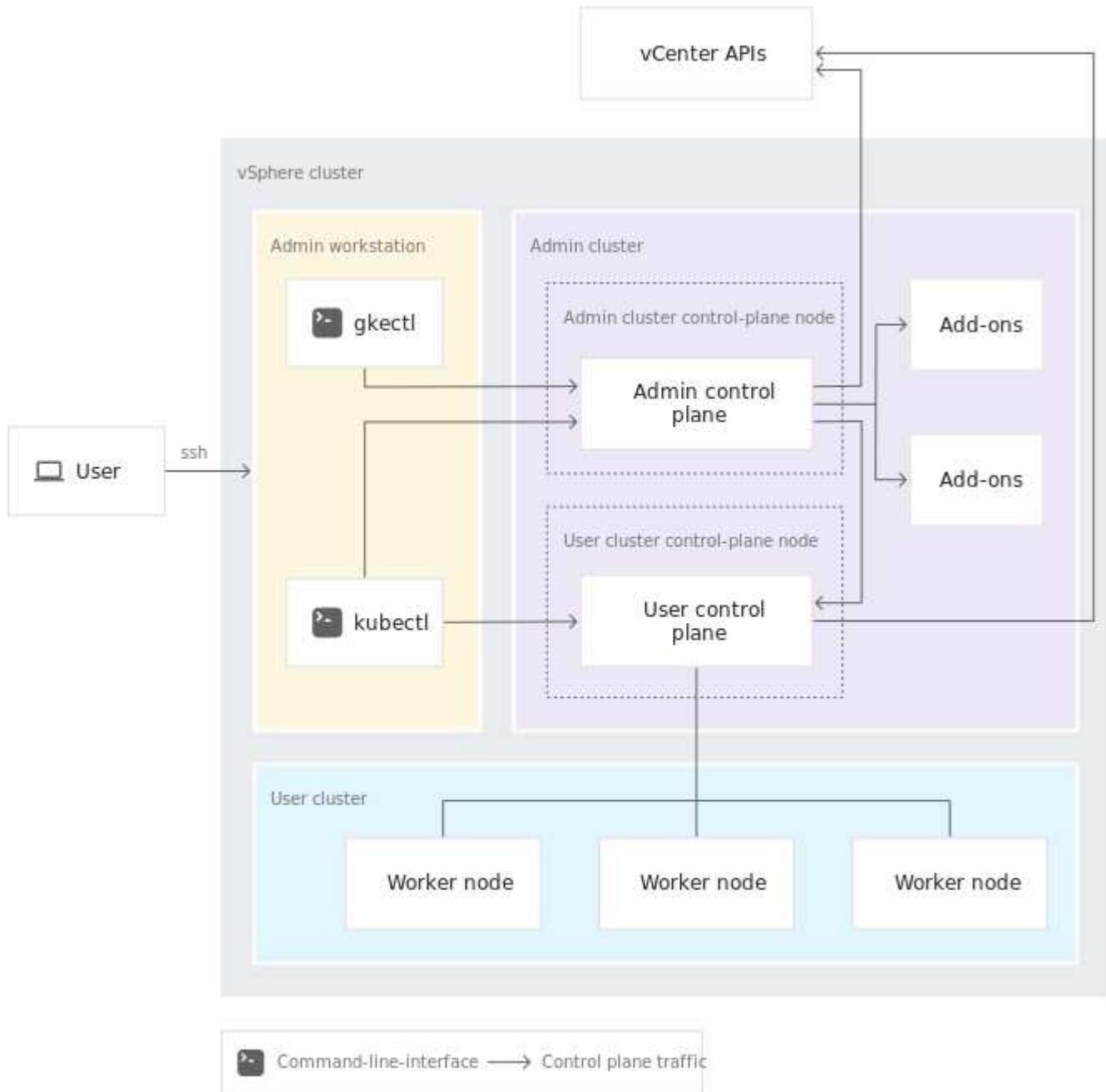
The deployment of Anthos clusters on VMware includes the following components:

- **Anthos Admin Workstation.** A deployment host from which gkectl and kubectl commands can be run to deploy and interact with Anthos deployments.
- **Admin Cluster.** The initial cluster deployed when setting up Anthos clusters on VMware. This cluster

manages all subordinate user cluster actions, including deployment, scaling, and upgrade.

- **User Cluster.** Each user cluster is deployed with its own load balancer instance or partition, allowing it to act as a standalone Kubernetes cluster for individual users or groups, helping to achieve full multitenancy.

The following graphic is a description of an Anthos clusters on VMware deployment.



## Benefits

Anthos clusters on VMware offers the following benefits:

- **Advanced multitenancy.** Each end user can be assigned their own user cluster, deployed with the virtual resources necessary for their own development environment.
- **Cost savings.** End users can realize significant cost savings by deploying multiple user clusters to the same physical environment, utilizing their own physical resources for their application deployments instead of provisioning resources in their Google Cloud environment or on large bare metal clusters.

- **Develop then publish.** On-premises deployments can be used while applications are in development, which allows for testing of applications in the privacy of a local data center before being made publicly available in the cloud.
- **Security requirements.** Customers with increased security concerns or sensitive data sets that cannot be stored in the public cloud are able to run their applications from the security of their own data centers, thereby meeting organizational requirements.

## VMware vSphere

VMware vSphere is a virtualization platform for centrally managing a large number of virtualized servers and networks running on the ESXi hypervisor.

For more information about VMware vSphere, see the [VMware vSphere website](#).

VMware vSphere provides the following features:

- **VMware vCenter Server.** VMware vCenter Server provides unified management of all hosts and VMs from a single console and aggregates performance monitoring of clusters, hosts, and VMs.
- **VMware vSphere vMotion.** VMware vCenter allows you to hot migrate VMs between nodes in the cluster upon request in a nondisruptive manner.
- **vSphere High Availability.** To avoid disruption in the event of host failures, VMware vSphere allows hosts to be clustered and configured for high availability. VMs that are disrupted by host failure are rebooted shortly on other hosts in the cluster, restoring services.
- **Distributed Resource Scheduler (DRS).** A VMware vSphere cluster can be configured to load balance the resource needs of the VMs it is hosting. VMs with resource contentions can be hot migrated to other nodes in the cluster to make sure that enough resources are available.

## Hardware requirements

### Compute

Google Cloud periodically requests updated validation of partner server platforms with new releases of Anthos through their Anthos Ready platform partner program. A listing of currently validated server platforms, and the versions of Anthos supported can be found [here](#).

The following table contains server platforms that have been tested by NetApp and NetApp partner engineers for the validation of Anthos clusters on VMware deployments. These include solutions such as the [NetApp FlexPod](#) with Cisco UCS servers and the [NetApp HCI](#) hybrid cloud infrastructure platform.

Manufacturer	Make	Model
Cisco	UCS	B200 M5
NetApp	HCI	C410

### Operating system

Anthos clusters on VMware can be deployed to both vSphere 6 and 7 environments as chosen by the customer to help match their current datacenter infrastructure.

The following table contains a list of Linux operating systems that have been used by NetApp and our partners to validate the solution.

<b>Operating System</b>	<b>Release</b>	<b>Anthos Versions</b>
VMware vSphere	6.7U3	1.10
VMware vSphere	7.0U3	1.10

## Additional hardware

To complete the deployment of Anthos with NetApp as a fully validated solution, additional data center components for networking and storage have been tested by NetApp and our partner engineers.

The following table includes information about these additional infrastructure components.

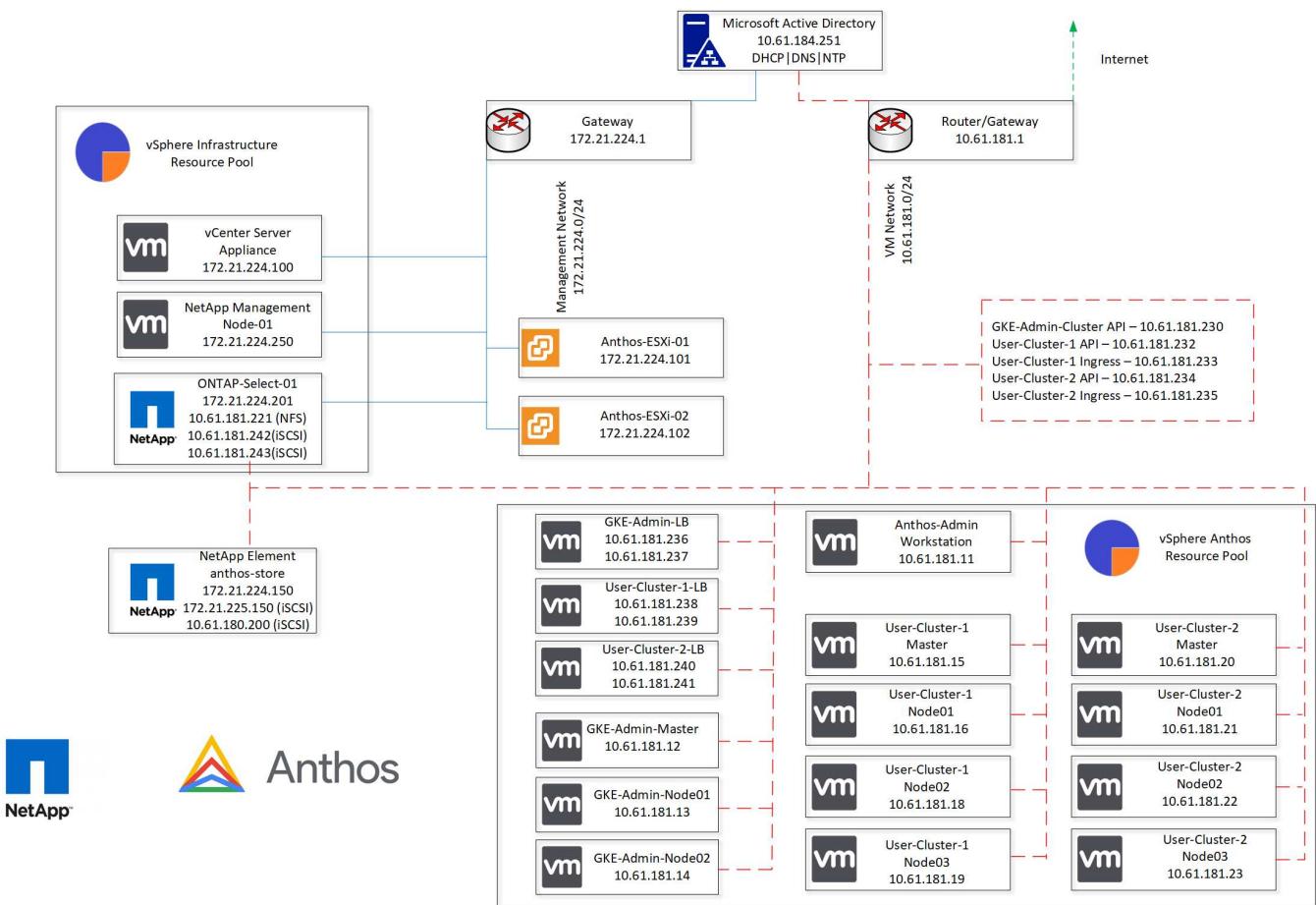
<b>Manufacturer</b>	<b>Hardware Name</b>	<b>Model</b>
Mellanox	SN	2010
NetApp	AFF	A250
NetApp	HCI	S410

## Additional software

The following table includes a list of software versions deployed in the validation environment.

<b>Manufacturer</b>	<b>Software Name</b>	<b>Version</b>
Cisco	UCS	4.1(3e)
NetApp	Element	12
NetApp	HCI	1.8
NetApp	ONTAP	9.9.1
NetApp	Astra Trident	22.01

During the Anthos Ready platform validation performed by NetApp, the lab environment was built based on the following diagram, which allowed us to test multiple deployed user clusters alongside multiple NetApp Storage systems and storage backends.



## Network infrastructure support resources

The following infrastructure should be in place prior to the deployment of Anthos:

- At least one DNS server providing full host-name resolution that is accessible from the in-band management network and the VM network.
- At least one NTP server that is accessible from the in-band management network and the VM network.
- A DHCP server available to provide network address leases on demand should clusters need to scale dynamically.
- (Optional) Outbound internet connectivity for both the in-band management network and the VM network.

## Best practices for production deployments

This section lists several best practices that an organization should take into consideration before deploying this solution into production.

## Deploy Anthos to an ESXi cluster of at least three nodes

Although it is possible to install Anthos in a vSphere cluster of less than three nodes for demonstration or evaluation purposes, this is not recommended for production workloads. While two nodes allow for basic HA and fault tolerance, an Anthos cluster configuration must be modified to disable default host affinity, and this deployment method is not supported by Google Cloud.

## Configure virtual machine and host affinity

Distributing Anthos cluster nodes across multiple hypervisor nodes can be achieved by enabling VM and host affinity.

Affinity or anti-affinity is a way to define rules for a set of VMs and/or hosts that determine whether the VMs run together on the same host or hosts in the group or on different hosts. It is applied to VMs by creating affinity groups that consist of VMs and/or hosts with a set of identical parameters and conditions. Depending on whether the VMs in an affinity group run on the same host or hosts in the group or separately on different hosts, the parameters of the affinity group can define either positive affinity or negative affinity.

To configure affinity groups, see the appropriate link below for your version of VMWare vSphere.

[vSphere 6.7 Documentation: Using DRS Affinity Rules.](#)

[vSphere 7.0 Documentation: Using DRS Affinity Rules.](#)

Next: [NetApp Storage Overview: Anthos with Netapp.](#)

## Anthos on bare metal: Anthos with NetApp

### Benefits

The hardware-agnostic capabilities of Anthos on bare metal allow you to select a compute platform optimized for your personalized use case and also provide many additional benefits.

Examples include:

- **Bring your own server.** You can use servers that match your existing infrastructure to reduce capital expenditure and management costs.
- **Bring your own Linux OS.** By choosing the Linux OS that you wish to deploy your Anthos on bare metal environment to, you can ensure that the Anthos environment fits neatly into your existing infrastructure and management schemes.
- **Improved performance and lowered cost.** Without the requirement of a hypervisor, Anthos on bare metal clusters call for direct access to server hardware resources, including performance-optimized hardware devices like GPUs.
- **Improved network performance and lowered latency.** Because the Anthos on bare metal server nodes are directly connected to your network without a virtualized abstraction layer, they can be optimized for low latency and performance.

### Hardware requirements

#### Compute

Google Cloud periodically requests updated validation of partner server platforms with new releases of Anthos through their Anthos Ready platform partner program. A listing of currently validated server platforms and the versions of Anthos supported can be found [here](#).

The following table contains server platforms that have been tested by NetApp and NetApp partner engineers for the validation of Anthos on bare metal deployments.

Manufacturer	Make	Model
Cisco	UCS	B200 M5

HPE	Proliant	DL360
-----	----------	-------

## Operating System

Anthos on bare metal nodes can be configured with several different Linux distributions as chosen by the customer to help match their current datacenter infrastructure.

The following table contains a list of Linux operating systems that have been used by NetApp and our partners to validate the solution.

Operating System	Release	Anthos Versions
CentOS	8.4	1.10
Red Hat Enterprise Linux	8.4	1.10
Ubuntu	18.04 LTS	1.10
Ubuntu	20.04 LTS	1.10

## Additional hardware

To complete the deployment of Anthos on bare metal as a fully validated solution, additional data center components for networking and storage have been tested by NetApp and our partner engineers.

The following table includes information about these additional infrastructure components.

Manufacturer	Hardware Name	Model
Cisco	Nexus	C9336C-FX2
NetApp	AFF	A250

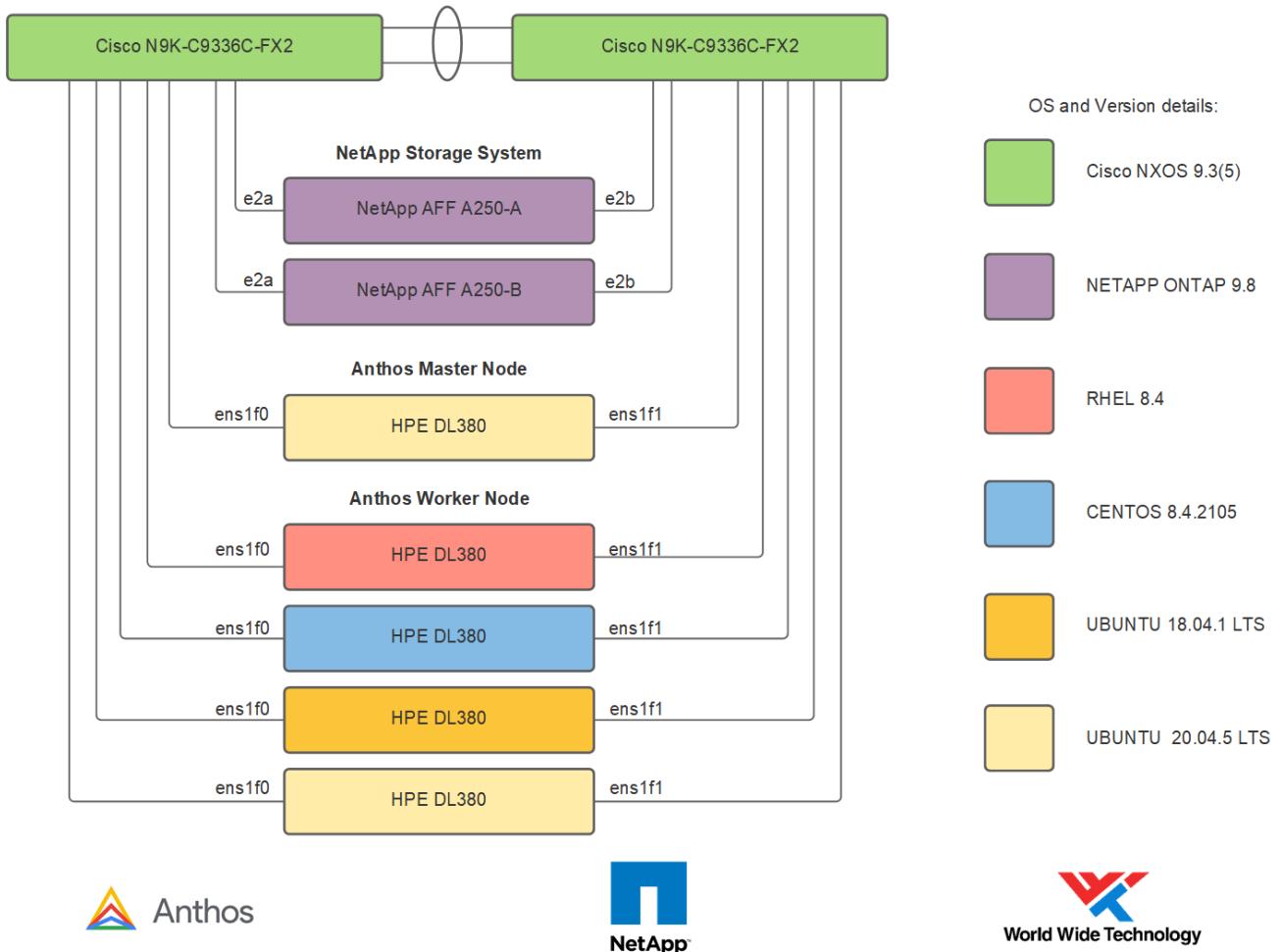
## Additional software

The following table includes a list of additional software versions deployed in the validation environment.

Manufacturer	Software name	Version
Cisco	NXOS	9.3(5)
NetApp	ONTAP	9.9.1
NetApp	Astra Trident	22.01

During the Anthos Ready platform validation performed by NetApp and our partner team at World Wide Technology (WWT), the lab environment was built based on the following diagram, which allowed us to test the functionality of each server type, operating system, the network devices, and storage systems deployed in the solution.

## Anthos BareMetal Physical Hardware Diagram



This multi-OS environment shows interoperability with supported OS versions for the Anthos on bare metal solution. We anticipate that customers will standardize on one or a subset of operating systems for their own deployment.

### Infrastructure support resources

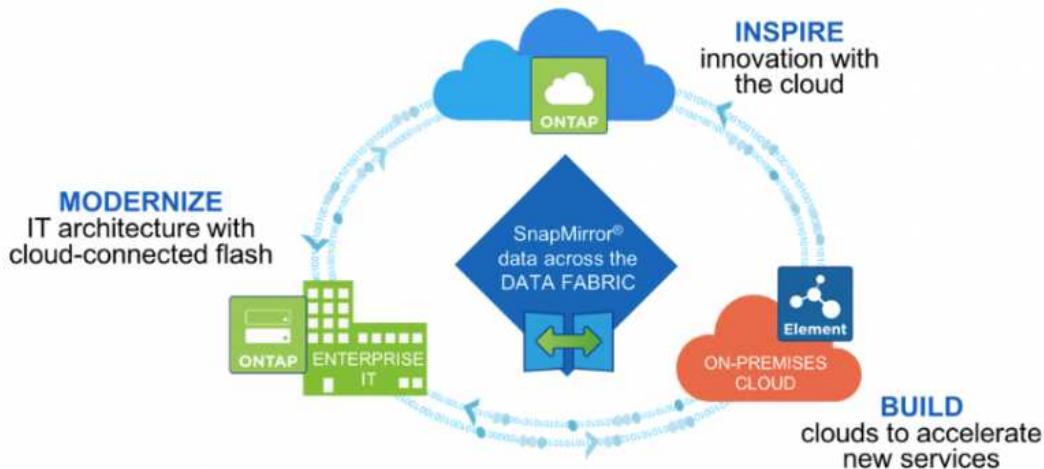
The following infrastructure should be in place prior to the deployment of Anthos on bare metal:

- At least one DNS server that provides a full host-name resolution accessible from the in-band management network and the VM network.
- At least one NTP server that is accessible from the in-band management network and the VM network.
- (Optional) Outbound internet connectivity for both the in-band management network and the VM network.

[Next: NetApp storage overview: Anthos with Netapp.](#)

### NetApp Storage Overview: Anthos with NetApp

NetApp has several storage platforms that are qualified with our Astra Trident Storage Orchestrator to provision storage for applications deployed on Anthos.



- AFF and FAS systems run NetApp ONTAP and provide storage for both file-based (NFS) and block-based (iSCSI) use cases.
- Cloud Volumes ONTAP and ONTAP Select provide the same benefits in the cloud and virtual space respectively.
- NetApp Cloud Volumes Service (AWS/GCP) and Azure NetApp Files provide file-based storage in the cloud.
- NetApp Element storage systems provide for block-based (iSCSI) use cases in a highly scalable environment.

**i** Each storage system in the NetApp portfolio can ease both data management and movement between on-premises sites and the cloud, ensuring that your data is where your applications are.

The following pages have additional information about the NetApp storage systems validated in the Anthos with NetApp solution:

- [NetApp ONTAP](#)
- [NetApp Element](#)

Next: [NetApp Storage Integrations Overview: Anthos with NetApp](#).

### NetApp ONTAP: Anthos with NetApp

NetApp ONTAP is a powerful storage-software tool with capabilities such as an intuitive GUI, REST APIs with automation integration, AI-informed predictive analytics and corrective action, nondisruptive hardware upgrades, and cross-storage import.

For more information about the NetApp ONTAP storage system, visit the [NetApp ONTAP website](#).

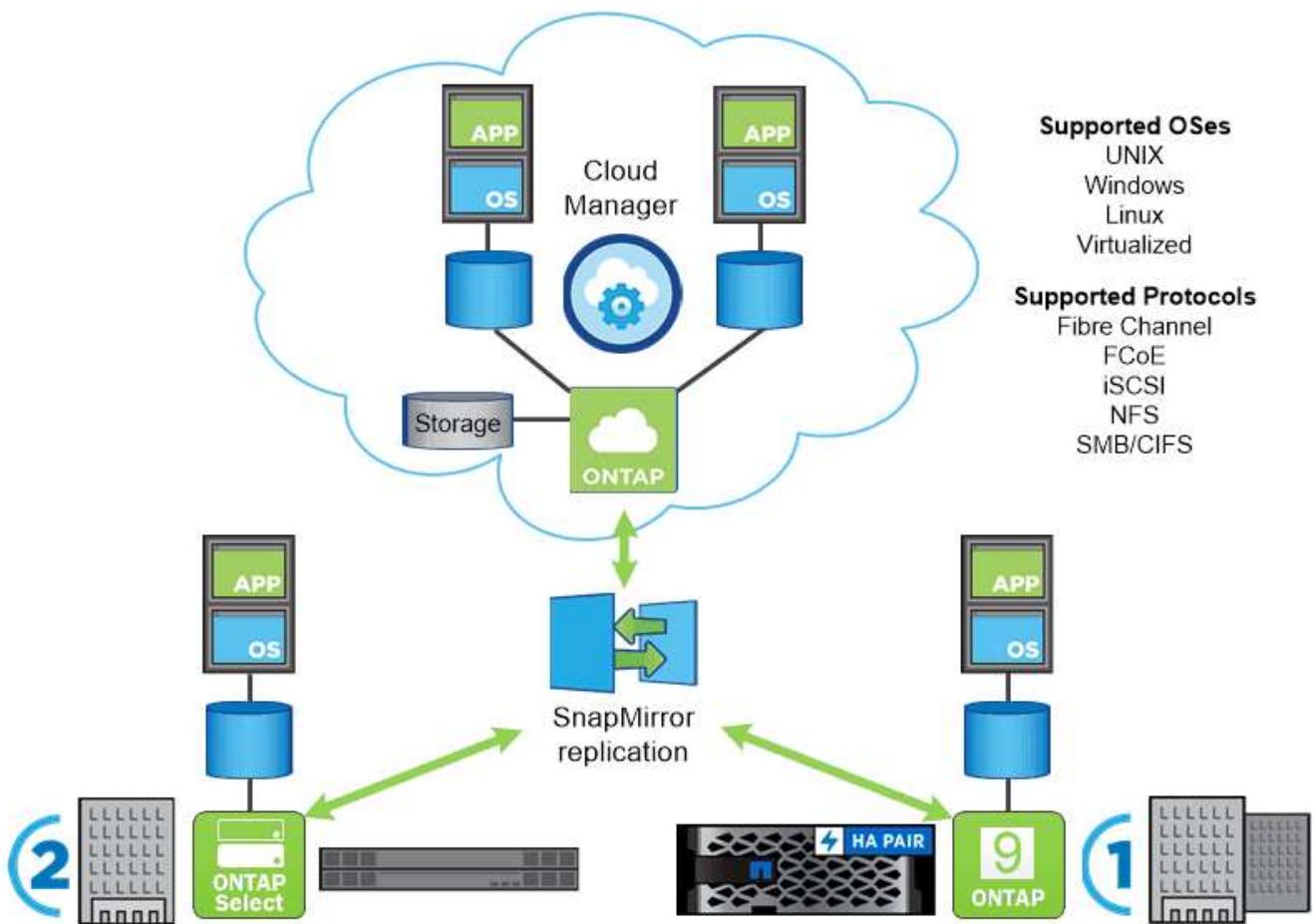
ONTAP provides the following features:

- A unified storage system with simultaneous data access and management of NFS, CIFS, iSCSI, FC, FCoE, and FC-NVMe protocols.
- Different deployment models include on-premises on all-flash, hybrid, and all-HDD hardware configurations; VM-based storage platforms on a supported hypervisor such as ONTAP Select; and in the cloud as Cloud Volumes ONTAP.
- Increased data storage efficiency on ONTAP systems with support for automatic data tiering, inline data compression, deduplication, and compaction.
- Workload-based, QoS-controlled storage.
- Seamless integration with a public cloud for tiering and protection of data. ONTAP also provides robust data protection capabilities that sets it apart in any environment:
  - **NetApp Snapshot copies.** A fast, point-in-time backup of data using a minimal amount of disk space with no additional performance overhead.
  - **NetApp SnapMirror.** Mirrors the Snapshot copies of data from one storage system to another. ONTAP supports mirroring data to other physical platforms and cloud-native services as well.
  - **NetApp SnapLock.** Efficiently administration of nonrewritable data by writing it to special volumes that cannot be overwritten or erased for a designated period.
  - **NetApp SnapVault.** Backs up data from multiple storage systems to a central Snapshot copy that serves as a backup to all designated systems.
  - **NetApp SyncMirror.** Provides real-time, RAID-level mirroring of data to two different plexes of disks that are connected physically to the same controller.
  - **NetApp SnapRestore.** Provides fast restoration of backed-up data on demand from Snapshot copies.
  - **NetApp FlexClone.** Provides instantaneous provisioning of a fully readable and writeable copy of a NetApp volume based on a Snapshot copy.

For more information about ONTAP, see the [ONTAP 9 Documentation Center](#).



NetApp ONTAP is available on-premises, virtualized, or in the cloud.



## NetApp platforms

### NetApp AFF/FAS

NetApp provides robust all-flash (AFF) and scale-out hybrid (FAS) storage platforms that are tailor-made with low-latency performance, integrated data protection, and multiprotocol support.

Both systems are powered by NetApp ONTAP data management software, the industry's most advanced data-management software for highly-available, cloud-integrated, simplified storage management to deliver the enterprise-class speed, efficiency, and security your data fabric needs.

For more information about NETAPP AFF and FAS platforms, click [here](#).

### ONTAP Select

ONTAP Select is a software-defined deployment of NetApp ONTAP that can be deployed onto a hypervisor in your environment. It can be installed on VMware vSphere or on KVM and provides the full functionality and experience of a hardware-based ONTAP system.

For more information about ONTAP Select, click [here](#).

### Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP is a cloud-deployed version of NetApp ONTAP available to be deployed in a number of public clouds, including: Amazon AWS, Microsoft Azure, and Google Cloud.

For more information about Cloud Volumes ONTAP, click [here](#).

Next: [NetApp Storage Integrations Overview: Anthos with NetApp](#).

## NetApp Element: Anthos with NetApp

NetApp Element software provides modular, scalable performance, with each storage node delivering guaranteed capacity and throughput to the environment. NetApp Element systems can scale from 4 to 100 nodes in a single cluster and offer a number of advanced storage management features.



For more information about NetApp Element storage systems, visit the [NetApp Solidfire website](#).

### iSCSI login redirection and self-healing capabilities

NetApp Element software leverages the iSCSI storage protocol, a standard way to encapsulate SCSI commands on a traditional TCP/IP network. When SCSI standards change or when the performance of Ethernet networks improves, the iSCSI storage protocol benefits without the need for any changes.

Although all storage nodes have a management IP and a storage IP, NetApp Element software advertises a single storage virtual IP address (SVIP address) for all storage traffic in the cluster. As a part of the iSCSI login process, storage can respond that the target volume has been moved to a different address and therefore it cannot proceed with the negotiation process. The host then reissues the login request to the new address in a process that requires no host-side reconfiguration. This process is known as iSCSI login redirection.

iSCSI login redirection is a key part of the NetApp Element software cluster. When a host login request is received, the node decides which member of the cluster should handle the traffic based on the IOPS and the capacity requirements for the volume. Volumes are distributed across the NetApp Element software cluster and are redistributed if a single node is handling too much traffic for its volumes or if a new node is added. Multiple copies of a given volume are allocated across the array.

In this manner, if a node failure is followed by volume redistribution, there is no effect on host connectivity beyond a logout and login with redirection to the new location. With iSCSI login redirection, a NetApp Element software cluster is a self-healing, scale-out architecture that is capable of nondisruptive upgrades and operations.

### NetApp Element software cluster QoS

A NetApp Element software cluster allows QoS to be dynamically configured on a per-volume basis. You can use per-volume QoS settings to control storage performance based on SLAs that you define. The following three configurable parameters define the QoS:

- **Minimum IOPS.** The minimum number of sustained IOPS that the NetApp Element software cluster provides to a volume. The minimum IOPS configured for a volume is the guaranteed level of performance for a volume. Per-volume performance does not drop below this level.

- **Maximum IOPS.** The maximum number of sustained IOPS that the NetApp Element software cluster provides to a particular volume.
- **Burst IOPS.** The maximum number of IOPS allowed in a short burst scenario. The burst duration setting is configurable, with a default of 1 minute. If a volume has been running below the maximum IOPS level, burst credits are accumulated. When performance levels become very high and are pushed, short bursts of IOPS beyond the maximum IOPS are allowed on the volume.

## Multitenancy

Secure multitenancy is achieved with the following features:

- **Secure authentication.** The Challenge-Handshake Authentication Protocol (CHAP) is used for secure volume access. The Lightweight Directory Access Protocol (LDAP) is used for secure access to the cluster for management and reporting.
- **Volume access groups (VAGs).** Optionally, VAGs can be used in lieu of authentication, mapping any number of iSCSI initiator-specific iSCSI Qualified Names (IQNs) to one or more volumes. To access a volume in a VAG, the initiator's IQN must be in the allowed IQN list for the group of volumes.
- **Tenant virtual LANs (VLANs).** At the network level, end-to-end network security between iSCSI initiators and the NetApp Element software cluster is facilitated by using VLANs. For any VLAN that is created to isolate a workload or a tenant, NetApp Element Software creates a separate iSCSI target SVIP address that is accessible only through the specific VLAN.
- **VRF-enabled VLANs.** To further support security and scalability in the data center, NetApp Element software allows you to enable any tenant VLAN for VRF-like functionality. This feature adds these two key capabilities:
  - **L3 routing to a tenant SVIP address.** This feature allows you to situate iSCSI initiators on a separate network or VLAN from that of the NetApp Element software cluster.
  - **Overlapping or duplicate IP subnets.** This feature enables you to add a template to tenant environments, allowing each respective tenant VLAN to be assigned IP addresses from the same IP subnet. This capability can be useful for in-service provider environments where scale and preservation of IPspace are important.

## Enterprise storage efficiencies

The NetApp Element software cluster increases overall storage efficiency and performance. The following features are performed inline, are always on, and require no manual configuration by the user:

- **Deduplication.** The system only stores unique 4K blocks. Any duplicate 4K blocks are automatically associated to an already stored version of the data. Data is on block drives and is mirrored by using the NetApp Element software Helix data protection. This system significantly reduces capacity consumption and write operations within the system.
- **Compression.** Compression is performed inline before data is written to NVRAM. Data is compressed, stored in 4K blocks, and remains compressed in the system. This compression significantly reduces capacity consumption, write operations, and bandwidth consumption across the cluster.
- **Thin-provisioning.** This capability provides the right amount of storage at the time that you need it, eliminating capacity consumption that caused by overprovisioned volumes or underutilized volumes.
- **Helix.** The metadata for an individual volume is stored on a metadata drive and is replicated to a secondary metadata drive for redundancy.



Element was designed for automation. All the storage features are available through APIs. These APIs are the only method that the UI uses to control the system.

Next: [NetApp Storage Integrations Overview: Anthos with NetApp](#).

## NetApp Storage Integration Overview

### Anthos Ready storage partner program.

Google Cloud periodically requests updated validation of partner storage integrations with new releases of Anthos through their Anthos Ready storage partner program. A listing of currently validated storage solutions, CSI drivers, available features, and the versions of Anthos supported can be found [here](#).

NetApp has maintained regular compliance with the requests to validate our Astra Trident CSI-compliant storage orchestrator, and our ONTAP and Element storage systems with versions of Anthos on a quarterly basis.

The following table contains the Anthos versions that have been tested by NetApp and NetApp partner engineers for the validation NetApp Astra Trident CSI drivers, and feature sets, as a part of the Anthos Ready storage partner program:

Deployment Type	Version	Storage System	Astra Trident Version	Protocol	Features
VMware	1.10	ONTAP	22.01	NAS	Multiwriter, Volume Expansion, SnapShots
VMware	1.10	ONTAP	22.01	SAN	Raw Block, Volume Expansion, SnapShots
VMware	1.10	Element	22.01	SAN	Raw Block, Volume Expansion, SnapShots
bare metal	1.10	ONTAP	22.01	NAS	Multiwriter, Volume Expansion, SnapShots
bare metal	1.10	ONTAP	22.01	SAN	Raw Block, Volume Expansion, SnapShots

### NetApp Storage Integrations

NetApp provides a number of products to help you with orchestrating and managing persistent data in container based environments, such as Anthos.

NetApp Astra Trident is an open-source and fully-supported storage orchestrator for containers and Kubernetes distributions, including Anthos. For more information, visit the Astra Trident website [here](#).

The following pages have additional information about the NetApp products that have been validated for application and persistent storage management in the Anthos with NetApp solution:

- [NetApp Astra Trident](#)

Next: Advanced Configuration Options: Anthos with NetApp.

## Astra Trident Overview

Astra Trident is an open-source and fully supported storage orchestrator for containers and Kubernetes distributions, including Anthos. Trident works with the entire NetApp storage portfolio, including the NetApp ONTAP and Element storage systems, and it also supports NFS and iSCSI connections. Trident accelerates the DevOps workflow by allowing end users to provision and manage storage from their NetApp storage systems without requiring intervention from a storage administrator.

An administrator can configure a number of storage backends based on project needs and storage system models that enable advanced storage features, including compression, specific disk types, or QoS levels that guarantee a certain level of performance. After they are defined, these backends can be used by developers in their projects to create persistent volume claims (PVCs) and to attach persistent storage to their containers on demand.

[Error: Missing Graphic Image]

Astra Trident has a rapid development cycle and, like Kubernetes, is released four times a year.

The latest version of Astra Trident, 22.01, was released in January 2022. A support matrix for what version of Trident has been tested with which Kubernetes distribution can be found [here](#).

Starting with the 20.04 release, Trident setup is performed by the Trident operator. The operator makes large scale deployments easier and provides additional support including self healing for pods that are deployed as a part of the Trident install.

With the 21.01 release, a Helm chart was made available to ease the installation of the Trident Operator.

## Download Astra Trident

To install Trident on the deployed user cluster and provision a persistent volume, complete the following steps:

1. Download the installation archive to the admin workstation and extract the contents. The current version of Trident is 22.01, which can be downloaded [here](#).

```
[ubuntu@gke-admin-ws-2021-07-15 ~]$ wget
https://github.com/NetApp/trident/releases/download/v22.01.0/trident-
installer-22.01.0.tar.gz
--2021-05-06 15:17:30--
https://github.com/NetApp/trident/releases/download/v22.01.0/trident-
installer-22.01.0.tar.gz
Resolving github.com (github.com)... 140.82.114.3
Connecting to github.com (github.com)|140.82.114.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github-
releases.githubusercontent.com/77179634/a4fa9f00-a9f2-11eb-9053-
98e8e573d4ae?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIWNJYAX4CSVEH53A%2F20210506%2Fus-east-
1%2Fs3%2Faws4_request&X-Amz-Date=20210506T191643Z&X-Amz-Expires=300&X-
```

```

Amz-
Signature=8a49a2a1e08c147d1ddd8149ce45a5714f9853fee19bb1c507989b9543eb36
30&X-Amz-
SignedHeaders=host&actor_id=0&key_id=0&repo_id=77179634&response-
content-disposition=attachment%3B%20filename%3Dtrident-installer-
22.01.0.tar.gz&response-content-type=application%2Foctet-stream
[following]
--2021-05-06 15:17:30-- https://github-
releases.githubusercontent.com/77179634/a4fa9f00-a9f2-11eb-9053-
98e8e573d4ae?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIWNJYAX4CSVEH53A%2F20210506%2Fus-east-
1%2Fs3%2Faws4_request&X-Amz-Date=20210506T191643Z&X-Amz-Expires=300&X-
Amz-
Signature=8a49a2a1e08c147d1ddd8149ce45a5714f9853fee19bb1c507989b9543eb36
30&X-Amz-
SignedHeaders=host&actor_id=0&key_id=0&repo_id=77179634&response-
content-disposition=attachment%3B%20filename%3Dtrident-installer-
22.01.0.tar.gz&response-content-type=application%2Foctet-stream
Resolving github-releases.githubusercontent.com (github-
releases.githubusercontent.com) ... 185.199.108.154, 185.199.109.154,
185.199.110.154, ...
Connecting to github-releases.githubusercontent.com (github-
releases.githubusercontent.com)|185.199.108.154|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 38349341 (37M) [application/octet-stream]
Saving to: 'trident-installer-22.01.0.tar.gz'

100%[=====>] 38,349,341 88.5MB/s
in 0.4s

2021-05-06 15:17:30 (88.5 MB/s) - 'trident-installer-22.01.0.tar.gz'
saved [38349341/38349341]

```

## 2. Extract the Trident install from the downloaded bundle.

```

[ubuntu@gke-admin-ws-2021-07-15 ~]$ tar -xzf trident-installer-
22.01.0.tar.gz
[ubuntu@gke-admin-ws-2021-07-15 ~]$ cd trident-installer/
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$

```

### Install the Trident Operator with Helm



Helm is not installed by default on the GKE-Admin workstation. You can easily install it using the apt tool available in Ubuntu.

1. First, set the location of the user cluster's kubeconfig file as an environment variable so that you don't have to reference it, because Trident has no option to pass this file.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ export  
KUBECONFIG=~/user-cluster-1/user-cluster-1-kubeconfig
```

2. Run the Helm command to install the Trident operator from the tarball in the helm directory while creating the trident namespace in your user cluster.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ helm install trident  
helm/trident-operator-22.01.0.tgz --create-namespace --namespace trident  
NAME: trident  
LAST DEPLOYED: Fri May 7 12:54:25 2021  
NAMESPACE: trident  
STATUS: deployed  
REVISION: 1  
TEST SUITE: None  
NOTES:  
Thank you for installing trident-operator, which will deploy and manage  
NetApp's Trident CSI  
storage provisioner for Kubernetes.  
  
Your release is named 'trident' and is installed into the 'trident'  
namespace.  
Please note that there must be only one instance of Trident (and  
trident-operator) in a Kubernetes cluster.  
  
To configure Trident to manage storage resources, you will need a copy  
of tridentctl, which is  
available in pre-packaged Trident releases. You may find all Trident  
releases and source code  
online at https://github.com/NetApp/trident.  
  
To learn more about the release, try:  
  
$ helm status trident  
$ helm get all trident
```

3. You can verify that Trident is successfully installed by checking the pods that are running in the namespace or by using the tridentctl binary to check the installed version.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ oc get pods -n trident
NAME                               READY   STATUS    RESTARTS   AGE
trident-csi-5z451                  1/2     Running   2          30s
trident-csi-696b685cf8-htdb2       6/6     Running   0          30s
trident-csi-b74p2                  2/2     Running   0          30s
trident-csi-lrw4n                  2/2     Running   0          30s
trident-operator-7c748d957-gr2gw   1/1     Running   0          36s

[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ ./tridentctl -n trident version
+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 22.01.0         | 22.01.0           |
+-----+-----+
```



In some cases, customer environments might require the customization of the Trident deployment. In these cases, it is also possible to manually install the Trident operator and update the included manifests to customize the deployment.

### Manually install the Trident Operator

1. First, set the location of the user cluster's kubeconfig file as an environment variable so that you don't have to reference it, because Trident has no option to pass this file.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ KUBECONFIG=~/user-cluster-1/user-cluster-1-kubeconfig
```

2. The `trident-installer` directory contains manifests for defining all the required resources. Using the appropriate manifests, create the `TridentOrchestrator` custom resource definition.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl create -f deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.yaml
customresourcedefinition.apiextensions.k8s.io/tridentorchestrators.tride
nt.netapp.io created
```

3. If one does not exist, create a Trident namespace in your cluster using the provided manifest.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl apply -f
deploy/namespace.yaml
namespace/trident created
```

4. Create the resources required for the Trident operator deployment, such as a ServiceAccount for the operator, a ClusterRole and ClusterRoleBinding to the ServiceAccount, a dedicated PodSecurityPolicy, or the operator itself.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl create -f deploy/bundle.yaml
serviceaccount/trident-operator created
clusterrole.rbac.authorization.k8s.io/trident-operator created
clusterrolebinding.rbac.authorization.k8s.io/trident-operator created
deployment.apps/trident-operator created
podsecuritypolicy.policy/tridentoperatorpods created
```

5. You can check the status of the operator after it's deployed with the following commands:

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl get deployment -n trident
NAME           READY   UP-TO-DATE   AVAILABLE   AGE
trident-operator   1/1      1          1          23s
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl get pods -n trident
NAME                           READY   STATUS    RESTARTS   AGE
trident-operator-66f48895cc-lzczk   1/1     Running   0          41s
```

6. With the operator deployed, we can now use it to install Trident. This requires creating a TridentOrchestrator.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl create -f deploy/crds/tridentorchestrator_cr.yaml
tridentorchestrator.trident.netapp.io/trident created
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl describe torc trident
Name:           trident
Namespace:
Labels:         <none>
Annotations:   <none>
API Version:  trident.netapp.io/v1
Kind:          TridentOrchestrator
Metadata:
  Creation Timestamp:  2021-05-07T17:00:28Z
  Generation:        1
  Managed Fields:
    API Version:  trident.netapp.io/v1
    Fields Type:   FieldsV1
    fieldsV1:
```

```

f:spec:
  .:
  f:debug:
  f:namespace:
    Manager:      kubectl-create
    Operation:   Update
    Time:        2021-05-07T17:00:28Z
    API Version: trident.netapp.io/v1
    Fields Type: FieldsV1
    fieldsV1:
      f:status:
        .:
        f:currentInstallationParams:
          .:
          f:IPv6:
            f:autosupportHostname:
            f:autosupportImage:
            f:autosupportProxy:
            f:autosupportSerialNumber:
            f:debug:
            f:enableNodePrep:
            f:imagePullSecrets:
            f:imageRegistry:
            f:k8sTimeout:
            f:kubeletDir:
            f:logFormat:
            f:silenceAutosupport:
            f:tridentImage:
            f:message:
            f:namespace:
            f:status:
            f:version:
    Manager:      trident-operator
    Operation:   Update
    Time:        2021-05-07T17:00:28Z
    Resource Version: 931421
    Self Link:
    /apis/trident.netapp.io/v1/tridentorchestrators/trident
    UID:          8a26a7a6-dde8-4d55-9b66-a7126754d81f
Spec:
  Debug:      true
  Namespace:  trident
Status:
  Current Installation Params:
    IPv6:           false
    Autosupport Hostname:

```

```

Autosupport Image:          netapp/trident-autosupport:21.01
Autosupport Proxy:
Autosupport Serial Number:
Debug:                      true
Enable Node Prep:           false
Image Pull Secrets:
Image Registry:
k8sTimeout:                 30
Kubelet Dir:                /var/lib/kubelet
Log Format:                 text
Silence Autosupport:        false
Trident Image:              netapp/trident:22.01.0
Message:                     Trident installed
Namespace:                  trident
Status:                      Installed
Version:                     v22.01.0

Events:
Type   Reason     Age    From            Message
----  -----     ----   ----
Normal  Installing  80s   trident-operator.netapp.io  Installing
Trident
Normal  Installed   68s   trident-operator.netapp.io  Trident
installed

```

7. You can verify that Trident is successfully installed by checking the pods that are running in the namespace or by using the `tridentctl` binary to check the installed version.

```

[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl get pods -n
trident
NAME                           READY   STATUS    RESTARTS   AGE
trident-csi-bb64c6cb4-lmd6h   6/6     Running   0          82s
trident-csi-gn59q             2/2     Running   0          82s
trident-csi-m4szj             2/2     Running   0          82s
trident-csi-sb9k9             2/2     Running   0          82s
trident-operator-66f48895cc-lzczk 1/1     Running   0          2m39s

[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ ./tridentctl -n
trident version
+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 22.01.0        | 22.01.0        |
+-----+-----+

```

## Create storage-system backends

After completing the Astra Trident Operator install, you must configure the backend for the specific NetApp storage platform you are using. Follow the links below in order to continue the setup and configuration of Astra Trident.

- [NetApp ONTAP NFS](#)
- [NetApp ONTAP iSCSI](#)
- [NetApp Element iSCSI](#)

Next: [Advanced Configuration Options: Anthos with NetApp](#).

### NetApp ONTAP NFS configuration: Anthos with NetApp

To enable Trident integration with the NetApp ONTAP storage system, you must create a backend that enables communication with the storage system.

1. There are sample backend files available in the downloaded installation archive in the `sample-input` folder hierarchy. For NetApp ONTAP systems serving NFS, copy the `backend-ontap-nas.json` file to your working directory and edit the file.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ cp sample-
input/backends-samples/ontap-nas/backend-ontap-nas.json ./
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ vi backend-ontap-
nas.json
```

2. Edit the `backendName`, `managementLIF`, `dataLIF`, `svm`, `username`, and `password` values in this file.

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "ontap-nas+10.61.181.221",
  "managementLIF": "172.21.224.201",
  "dataLIF": "10.61.181.221",
  "svm": "trident_svm",
  "username": "cluster-admin",
  "password": "password"
}
```



It is a best practice to define the custom `backendName` value as a combination of the `storageDriverName` and the `dataLIF` that is serving NFS for easy identification.

3. With this backend file in place, run the following command to create your first backend.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ ./tridentctl -n
trident create backend -f backend-ontap-nas.json
+-----+
+-----+-----+
|           NAME          | STORAGE DRIVER |             UUID
| STATE   | VOLUMES   |
+-----+-----+
+-----+-----+
| ontap-nas+10.61.181.221 | ontap-nas      | be7a619d-c81d-445c-b80c-
5c87a73c5b1e | online | 0 |
+-----+-----+
+-----+-----+
```

- With the backend created, you must next create a storage class. Just as with the backend, there is a sample storage class file that can be edited for the environment available in the sample-inputs folder. Copy it to the working directory and make necessary edits to reflect the backend created.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ cp sample-
input/storage-class-samples/storage-class-csi.yaml.template ./storage-
class-basic.yaml
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ vi storage-class-
basic.yaml
```

- The only edit that must be made to this file is to define the `backendType` value to the name of the storage driver from the newly created backend. Also note the `name-field` value, which must be referenced in a later step.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: basic-csi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
```



There is an optional field called `fsType` that is defined in this file. This line can be deleted in NFS backends.

- Run the `kubectl` command to create the storage class.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl create -f storage-class-basic.yaml
storageclass.storage.k8s.io/basic-csi created
```

- With the storage class created, you must then create the first persistent volume claim (PVC). There is a sample `pvc-basic.yaml` file that can be used to perform this action located in `sample-inputs` as well.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ cp sample-input/pvc-samples/pvc-basic.yaml .
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ vi pvc-basic.yaml
```

- The only edit that must be made to this file is ensuring that the `storageClassName` field matches the one just created. The PVC definition can be further customized as required by the workload to be provisioned.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

- Create the PVC by issuing the `kubectl` command. Creation can take some time depending on the size of the backing volume being created, so you can watch the process as it completes.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl get pvc
NAME      STATUS      VOLUME                                     CAPACITY
ACCESS MODES     STORAGECLASS     AGE
basic     Bound      pvc-b4370d37-0fa4-4c17-bd86-94f96c94b42d   1Gi
RWO          basic-csi        7s
```

[Next: Advanced Configuration Options: Anthos with NetApp.](#)

## NetApp ONTAP iSCSI configuration: Anthos with NetApp

To enable Trident integration with the NetApp ONTAP storage system, you must create a backend that enables communication with the storage system.

1. There are sample backend files available in the downloaded installation archive in the sample-input folder hierarchy. For NetApp ONTAP systems serving iSCSI, copy the `backend-ontap-san.json` file to your working directory and edit the file.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ cp sample-
input/backends-samples/ontap-san/backend-ontap-san.json ./
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ vi backend-ontap-
san.json
```

2. Edit the managementLIF, dataLIF, svm, username, and password values in this file.

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "managementLIF": "172.21.224.201",
  "dataLIF": "10.61.181.240",
  "svm": "trident_svm",
  "username": "admin",
  "password": "password"
}
```

3. With this backend file in place, run the following command to create your first backend.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ ./tridentctl -n
trident create backend -f backend-ontap-san.json
+-----+
+-----+-----+-----+
|       NAME          | STORAGE DRIVER |           UUID
| STATE   | VOLUMES   |
+-----+-----+
+-----+-----+-----+
| ontapsan_10.61.181.241 | ontap-san      | 6788533c-7fea-4a35-b797-
fb9bb3322b91 | online | 0 |
+-----+-----+
+-----+-----+-----+
```

4. With the backend created, you must next create a storage class. Just as with the backend, there is a sample storage class file that can be edited for the environment available in the sample-inputs folder. Copy it to the working directory and make necessary edits to reflect the backend created.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ cp sample-
input/storage-class-samples/storage-class-csi.yaml.tpl ./storage-
class-basic.yaml
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ vi storage-class-
basic.yaml
```

5. The only edit that must be made to this file is to define the `backendType` value to the name of the storage driver from the newly created backend. Also note the `name-field` value, which must be referenced in a later step.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: basic-csi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
```



There is an optional field called `fsType` that is defined in this file. In iSCSI backends, this value can be set to a specific Linux filesystem type (XFS, ext4, and so on) or can be deleted to allow OpenShift to decide what filesystem to use.

6. Run the `kubectl` command to create the storage class.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl create -f
storage-class-basic.yaml
storageclass.storage.k8s.io/basic-csi created
```

7. With the storage class created, you must then create the first persistent volume claim (PVC). There is a sample `pvc-basic.yaml` file that can be used to perform this action located in `sample-inputs` as well.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ cp sample-input/pvc-
samples/pvc-basic.yaml ./
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ vi pvc-basic.yaml
```

8. The only edit that must be made to this file is ensuring that the `storageClassName` field matches the one just created. The PVC definition can be further customized as required by the workload to be provisioned.

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi

```

9. Create the PVC by issuing the `kubectl` command. Creation can take some time depending on the size of the backing volume being created, so you can watch the process as it completes.

```

[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl create -f
pvc-basic.yaml
persistentvolumeclaim/basic created

[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl get pvc
NAME      STATUS      VOLUME                                     CAPACITY
ACCESS MODES     STORAGECLASS     AGE
basic     Bound      pvc-7ceac1ba-0189-43c7-8f98-094719f7956c   1Gi
RWO                  basic-csi      3s

```

[Next: Advanced Configuration Options: Anthos with NetApp.](#)

#### **NetApp Element iSCSI configuration: Anthos with NetApp**

To enable Trident integration with the NetApp Element storage system, you must create a backend that enables communication with the storage system using the iSCSI protocol.

1. There are sample backend files available in the downloaded installation archive in the `sample-input` folder hierarchy. For NetApp Element systems serving iSCSI, copy the `backend-solidfire.json` file to your working directory and edit the file.

```

[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ cp sample-
input/backends-samples/solidfire/backend-solidfire.json ./
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ vi ./backend-
solidfire.json

```

- a. Edit the user, password, and MVIP value on the `EndPoint` line.
- b. Edit the `SVIP` value.

```
{
  "version": 1,
  "storageDriverName": "solidfire-san",
  "Endpoint": "https://trident:password@172.21.224.150/json-
rpc/8.0",
  "SVIP": "10.61.180.200:3260",
  "TenantName": "trident",
  "Types": [{"Type": "Bronze", "Qos": {"minIOPS": 1000, "maxIOPS": 2000, "burstIOPS": 4000}}, {"Type": "Silver", "Qos": {"minIOPS": 4000, "maxIOPS": 6000, "burstIOPS": 8000}}, {"Type": "Gold", "Qos": {"minIOPS": 6000, "maxIOPS": 8000, "burstIOPS": 10000}}]
}
```

- With this back-end file in place, run the following command to create your first backend.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ ./tridentctl -n
trident create backend -f backend-solidfire.json
+-----+
+-----+-----+-----+
|       NAME          | STORAGE DRIVER |           UUID
| STATE   | VOLUMES | 
+-----+-----+
+-----+-----+-----+
| solidfire_10.61.180.200 | solidfire-san | b90783ee-e0c9-49af-8d26-
3ea87ce2efdf | online |      0 |
+-----+-----+
+-----+-----+-----+
```

- With the backend created, you must next create a storage class. Just as with the backend, there is a sample storage class file that can be edited for the environment available in the sample-inputs folder. Copy it to the working directory and make necessary edits to reflect the backend created.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ cp sample-
input/storage-class-samples/storage-class-csi.yaml.template ./storage-
class-basic.yaml
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ vi storage-class-
basic.yaml
```

- The only edit that must be made to this file is to define the `backendType` value to the name of the storage driver from the newly created backend. Also note the `name-field` value, which must be referenced in a later step.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: basic-csi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "solidfire-san"
```



There is an optional field called `fsType` that is defined in this file. In iSCSI backends, this value can be set to a specific Linux filesystem type (XFS, ext4, and so on), or it can be deleted to allow OpenShift to decide what filesystem to use.

5. Run the `kubectl` command to create the storage class.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl create -f
storage-class-basic.yaml
storageclass.storage.k8s.io/basic-csi created
```

6. With the storage class created, you must then create the first persistent volume claim (PVC). There is a sample `pvc-basic.yaml` file that can be used to perform this action located in `sample-inputs` as well.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ cp sample-input/pvc-
samples/pvc-basic.yaml ./
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ vi pvc-basic.yaml
```

7. The only edit that must be made to this file is ensuring that the `storageClassName` field matches the one just created. The PVC definition can be further customized as required by the workload to be provisioned.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

8. Create the PVC by issuing the `kubectl` command. Creation can take some time depending on the size of the backing volume being created, so you can watch the process as it completes.

```
[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[ubuntu@gke-admin-ws-2021-07-15 trident-installer]$ kubectl get pvc
NAME      STATUS    VOLUME                                     CAPACITY
ACCESS MODES   STORAGECLASS     AGE
basic      Bound    pvc-3445b5cc-df24-453d-a1e6-b484e874349d   1Gi
RWO                  basic-csi        5s
```

[Next: Advanced Configuration Options: Anthos with NetApp.](#)

## Advanced Configuration Options For Anthos

### Exploring load balancer options: Anthos with NetApp

An application deployed in Anthos is exposed to the world by a service, delivered by a load balancer deployed in the Anthos On Prem environment.

The following pages have additional information about load balancer options validated in the Anthos with NetApp solution:

- [F5 BIG-IP](#)
- [SeeSaw](#)

[Next: Solution validation/use cases: Anthos with NetApp.](#)

### Installing F5 BIG-IP load balancers: Anthos with NetApp

F5 BIG-IP is an Application Delivery Controller (ADC) that offers a broad set of advanced, production-grade traffic management and security services like L4-L7 load balancing, SSL/TLS offload, DNS, firewall, and many more. These services drastically increase the availability, security, and performance of your applications.

F5 BIG-IP can be deployed and consumed in various ways, including on dedicated hardware, in the cloud, or as a virtual appliance on-premises. Refer to the documentation here to explore and deploy F5 BIG-IP as per requirement.

F5 BIG-IP was the first of the bundled load balancer solutions available with Anthos On-Prem and was used in a number of the early Anthos Ready partner validations for the Anthos with NetApp solution.



F5 BIG-IP can be deployed in standalone or cluster mode. For the purpose of this validation, F5 BIG-IP was deployed in standalone mode, but, for production purposes, it is preferred to have a cluster of BIG-IPs to avoid a single point of failure.



An F5 BIG-IP system can be deployed on dedicated hardware, in the cloud, or as a virtual appliance on-premises with versions greater than 12.x for it to be integrated with F5 CIS. For the purpose of this document, the F5 BIG-IP system was validated as a virtual appliance, for example using the BIG-IP VE edition.

## Validated releases

This solution makes use of the virtual appliance deployed in VMware vSphere. Networking for the F5 Big-IP virtual appliance can be configured in a two-armed or three-armed configuration based on your network environment. The deployment in this document is based on the two-armed configuration. Additional details on configuring the virtual appliance for use with Anthos can be found [here](#).

The solutions engineering team at NetApp have validated the releases in the following table in our lab to work with deployments of Anthos On-Prem:

Make	Type	Version
F5	BIG-IP VE	15.0.1-0.0.11
F5	BIG-IP VE	16.1.0-0.0.19

## Installation

To install F5 BIG-IP, complete the following steps:

1. Download the virtual application Open Virtual Appliance (OVA) file from F5 [here](#).



To download the appliance, a user must register with F5. They provide a 30-day demo license for the Big-IP Virtual Edition Load Balancer. NetApp recommends a permanent 10Gbps license for the production deployment of an appliance.

2. Right-click the Infrastructure Resource Pool and select Deploy OVF Template. A wizard launches that allows you to select the OVA file that you just downloaded in Step 1. Click Next.

## Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template  
Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

<http://https://remoteserver-address/filetodeploy.ovf> | .ova

[Choose Files](#) BIGIP-15.0.1-0....ALL-vmware.ova

[CANCEL](#) [BACK](#) [NEXT](#)

3. Click Next to continue through each step and accept the default values for each screen presented until you reach the storage selection screen. Select the VM\_Datastore that was created earlier, and then click Next.
4. The next screen presented by the wizard allows you to customize the virtual networks for use in the environment. Select VM\_Network for the External field and select Management\_Network for the Management field. Internal and HA are used for advanced configurations for the F5 Big-IP appliance and are not configured. These parameters can be left alone, or they can be configured to connect to non-infrastructure, distributed port groups. Click Next.
5. Review the summary screen for the appliance, and, if all the information is correct, click Finish to start the deployment.
6. After the virtual appliance is deployed, right-click it and power it up. It should receive a DHCP address on the management network. The appliance is Linux-based, and it has VMware Tools deployed, so you can view the DHCP address it receives in the vSphere client.
7. Open a web browser and connect to the appliance at the IP address from the previous step. The default login is admin/admin, and, after the first login, the appliance immediately prompts you to change the admin password. It then returns you to a screen where you must log in with the new credentials.



8. The first screen prompts the user to complete the Setup Utility. Begin the utility by clicking Next.
9. The next screen prompts for activation of the license for the appliance. Click Activate to begin. When prompted on the next page, paste either the 30-day evaluation license key you received when you registered for the download or the permanent license you acquired when you purchased the appliance. Click Next.

**i** For the device to perform activation, the network defined on the management interface must be able to reach the internet.
10. On the next screen, the End User License Agreement (EULA) is presented. If the terms in the license are acceptable, click Accept.
11. The next screen counts the elapsed time as it verifies the configuration changes that have been made so far. Click Continue to resume with the initial configuration.
12. The Configuration Change window closes, and the Setup Utility displays the Resource Provisioning menu. This window lists the features that are currently licensed and the current resource allocations for the virtual appliance and each running service.
13. Clicking the Platform menu option on the left enables additional modification of the platform. Modifications include setting the management IP address configured with DHCP, setting the host name and the time zone the appliance is installed in, and securing the appliance from SSH accessibility.

14. Next click the Network menu, which enables you to configure standard networking features. Click Next to begin the Standard Network Configuration wizard.
15. The first page of the wizard configures redundancy; leave the defaults and click Next. The next page enables you to configure an internal interface on the load balancer. Interface 1.1 maps to the vmnic labeled Internal in the OVF deployment wizard.

[Big-IP Configuration] | *big-IP\_config\_8.png*



The spaces in this page for Self IP Address, Netmask, and Floating IP address can be filled with a non-routable IP for use as a placeholder. They can also be filled with an internal network that has been configured as a distributed port group for virtual guests if you are deploying the three-armed configuration. They must be completed to continue with the wizard.

16. The next page enables you to configure an external network that is used to map services to the pods deployed in Kubernetes. Select a static IP from the VM\_Network range, the appropriate subnet mask, and a floating IP from that same range. Interface 1.2 maps to the vmnic labeled External in the OVF deployment wizard.

[Big-IP Configuration] | *big-IP\_config\_9.png*

17. On the next page, you can configure an internal-HA network if you are deploying multiple virtual appliances in the environment. To proceed, you must fill the Self-IP Address and the Netmask fields, and you must select interface 1.3 as the VLAN Interface, which maps to the HA network defined by the OVF template wizard.
18. The next page enables you to configure the NTP servers. Then click Next to continue to the DNS setup. The DNS servers and domain search list should already be populated by the DHCP server. Click Next to accept the defaults and continue.
19. For the remainder of the wizard, click Next to continue through the advanced peering setup, the configuration of which is beyond the scope of this document. Then click Finish to exit the wizard.
20. Create individual partitions for the Anthos admin cluster and each user cluster deployed in the environment. Click System in the menu on the left, navigate to Users, and click Partition List.
21. The displayed screen only shows the current common partition. Click Create on the right to create the first additional partition, and name it GKE-Admin. Then click Repeat, and name the partition User-Cluster-1, and click the Repeat button again to name the next partition User-Cluster-2. Finally click Finished to complete the wizard. The Partition list screen returns with all the partitions now listed.

## Integration with Anthos

There is a section in each configuration file, respectively for the admin cluster, and each user cluster that you choose to deploy to configure the load balancer so that it will be managed by Anthos On Prem.

The following is a sample from the configuration of the partition for the GKE-Admin cluster, the values that need to be uncommented and modified are placed in bold text below:

```

# (Required) Load balancer configuration
loadBalancer:
  # (Required) The VIPs to use for load balancing
  vips:
    # Used to connect to the Kubernetes API
    controlPlaneVIP: "10.61.181.230"
    # # (Optional) Used for admin cluster addons (needed for multi cluster
features). Must
      # # be the same across clusters
      # # addonsVIP: ""
    # (Required) Which load balancer to use "F5BigIP" "Seesaw" or
"ManuallLB". Uncomment
      # the corresponding field below to provide the detailed spec
    kind: F5BigIP
    # # (Required when using "ManuallLB" kind) Specify pre-defined nodeports
    # manualLB:
      #   # NodePort for ingress service's http (only needed for user cluster)
      #   ingressHTTPNodePort: 0
      #   # NodePort for ingress service's https (only needed for user
cluster)
      #   ingressHTTPSNODEPort: 0
      #   # NodePort for control plane service
      #   controlPlaneNodePort: 30968
      #   # NodePort for addon service (only needed for admin cluster)
      #   addonsNodePort: 31405
    # # (Required when using "F5BigIP" kind) Specify the already-existing
partition and
    # # credentials
  f5BigIP:
    address: "172.21.224.21"
    credentials:
      username: "admin"
      password: "admin-password"
      partition: "GKE-Admin"
    #   # (Optional) Specify a pool name if using SNAT
    #   snatPoolName: ""
    # (Required when using "Seesaw" kind) Specify the Seesaw configs
    # seesaw:
      # (Required) The absolute or relative path to the yaml file to use for
IP allocation
      # for LB VMs. Must contain one or two IPs.
      # ipBlockFilePath: ""
      # (Required) The Virtual Router IDentifier of VRRP for the Seesaw
group. Must
        # be between 1-255 and unique in a VLAN.
        # vrid: 0

```

```

# (Required) The IP announced by the master of Seesaw group
# masterIP: ""

# (Required) The number CPUs per machine
# cpus: 4

# (Required) Memory size in MB per machine
# memoryMB: 8192

# (Optional) Network that the LB interface of Seesaw runs in (default:
cluster
  # network)
  # vCenter:
    # vSphere network name
    #   networkName: VM_Network
  # (Optional) Run two LB VMs to achieve high availability (default:
false)
  # enableHA: false

```

[Next: Solution Validation/Use Cases: Anthos with NetApp.](#)

#### Installing SeeSaw load balancers: Anthos with NetApp

This page lists the installation and configuration instructions for the SeeSaw managed load balancer.

Seesaw is the default managed network load balancer installed in an Anthos Clusters on VMware environment.

#### Installing The SeeSaw Load Balancer

The SeeSaw load balancer is fully integrated with Anthos Clusters on VMware and has automated deployment performed as part of the Admin and User cluster setups. There are blocks of text in the `cluster.yaml` configuration files that must be modified to provide load balancer info, and then there is an additional step prior to cluster deployment to deploy the load balancer using the built in 'gkectl' tool.

 SeeSaw load balancers can be deployed in HA or Non-HA mode. For the purpose of this validation, the SeeSaw load balancer was deployed in Non-HA mode, which is the default setting. For production purposes, NetApp recommends deploying SeeSaw in an HA configuration for fault tolerance and reliability.

#### Integration with Anthos

There is a section in each configuration file, respectively for the admin cluster, and each user cluster that you choose to deploy to configure the load balancer so that it is managed by Anthos On-Prem.

The following text is a sample from the configuration of the partition for the GKE-Admin cluster. The values that need to be uncommented and modified are placed in bold text below:

```

loadBalancer:
  # (Required) The VIPs to use for load balancing
  vips:
    # Used to connect to the Kubernetes API

```

```

controlPlaneVIP: "10.61.181.230"
# # (Optional) Used for admin cluster addons (needed for multi cluster
features). Must
# # be the same across clusters
# # addonsVIP: ""

# (Required) Which load balancer to use "F5BigIP" "Seesaw" or
"ManualLB". Uncomment
# the corresponding field below to provide the detailed spec
kind: Seesaw
# # (Required when using "ManualLB" kind) Specify pre-defined nodeports
# manualLB:
#     # NodePort for ingress service's http (only needed for user cluster)
#     ingressHTTPNodePort: 0
#     # NodePort for ingress service's https (only needed for user
cluster)
#     ingressHTTPSNodePort: 0
#     # NodePort for control plane service
#     controlPlaneNodePort: 30968
#     # NodePort for addon service (only needed for admin cluster)
#     addonsNodePort: 31405
# # (Required when using "F5BigIP" kind) Specify the already-existing
partition and
# # credentials
# f5BigIP:
#     address:
#     credentials:
#         username:
#         password:
#     partition:
#     # # (Optional) Specify a pool name if using SNAT
#     # snatPoolName: ""
# (Required when using "Seesaw" kind) Specify the Seesaw configs
seesaw:
# (Required) The absolute or relative path to the yaml file to use for
IP allocation
# for LB VMs. Must contain one or two IPs.
ipBlockFilePath: "admin-seesaw-block.yaml"
# (Required) The Virtual Router IDentifier of VRRP for the Seesaw
group. Must
# be between 1-255 and unique in a VLAN.
vrid: 100
# (Required) The IP announced by the master of Seesaw group
masterIP: "10.61.181.236"
# (Required) The number CPUs per machine
cpus: 1
# (Required) Memory size in MB per machine

```

```

memoryMB: 2048
#   (Optional) Network that the LB interface of Seesaw runs in (default:
cluster
#   network)
vCenter:
#   vSphere network name
networkName: VM_Network
#   (Optional) Run two LB VMs to achieve high availability (default:
false)
enableHA: false

```

The SeeSaw load balancer also has a separate static 'seesaw-block.yaml' file that must be provided for each cluster deployment. This file must be located in the same directory relative to the cluster.yaml deployment file, or the full path must be specified in the section above.

A sample of the admin-seesaw-block.yaml file looks like the following:

```

blocks:
- netmask: "255.255.255.0"
  gateway: "10.63.172.1"
  ips:
- ip: "10.63.172.152"
  hostname: "admin-seesaw-vm"

```



This file provides the gateway and netmask for the network that the load balancer provides to the underlying cluster, as well as the management IP and hostname for the virtual machine that is deployed to run the load balancer.

[Next: Solution validation/use cases: Anthos with NetApp.](#)

## Solution Validation and Use Cases: Anthos with NetApp

The examples provided on this page are solution validations and use cases for Anthos with NetApp.

[Next: Videos and Demos: Anthos with NetApp.](#)

## Videos and Demos: Anthos with NetApp

The following video demonstrate some of the capabilities documented in this document:

[Next: Additional Information: Anthos with NetApp.](#)

## Additional Information: Anthos with NetApp

To learn more about the information described in this document, review the following websites:

- NetApp Documentation

<https://docs.netapp.com/>

- NetApp Astra Trident Documentation

<https://docs.netapp.com/us-en/trident/index.html>

- NetApp Astra Control Center Documentation

<https://docs.netapp.com/us-en/astra-control-center/>

- Anthos Clusters on VMware Documentation

<https://cloud.google.com/anthos/clusters/docs/on-prem/1.10/overview>

- Anthos on bare metal Documentation

<https://cloud.google.com/anthos/clusters/docs/bare-metal/latest>

- VMware vSphere Documentation

<https://docs.vmware.com/>

## Archived Solutions

### WP-7337: Anthos on Bare Metal

Alan Cowles and Nikhil M Kulkarni, NetApp

NetApp and Google Cloud have had a strong relationship for several years now, with NetApp first introducing cloud data services for Google Cloud with Cloud Volumes ONTAP and the Cloud Volumes Service. This relationship was then expanded by validating the NetApp HCI platform for use with Google Cloud Anthos on-premises, a hypervisor-based hybrid multi-cloud Kubernetes solution deployed on VMware vSphere. NetApp then passed Anthos Ready qualification for NetApp Astra Trident, ONTAP, and the NFS protocol to provide dynamic persistent storage for containers.

Anthos can now be directly installed on bare-metal servers in a customer's environment, which adds an additional option for customers to extend Google Cloud into their local data centers without a hypervisor. Additionally, by leveraging the capabilities of NetApp ONTAP storage operating system and NetApp Astra Trident, you can extend your platform's capabilities by integrating persistent storage for containers.

This combination allows you to realize the full potential of your servers, storage, and networking combined with the support, service levels, monthly billing, and on-demand flexibility that Google Cloud provides. Because you are using your own hardware, network, and storage, you have direct control over application scale, security, and network latency, as well as having the benefit of managed and containerized applications with Anthos on bare metal.

[Next: Solution overview.](#)

#### Solution overview

##### NetApp ONTAP on NetApp AFF/FAS

NetApp AFF is a robust all-flash storage platform that provides low-latency performance, integrated data protection, multiprotocol support, and nondisruptive operations. Powered by NetApp ONTAP data management

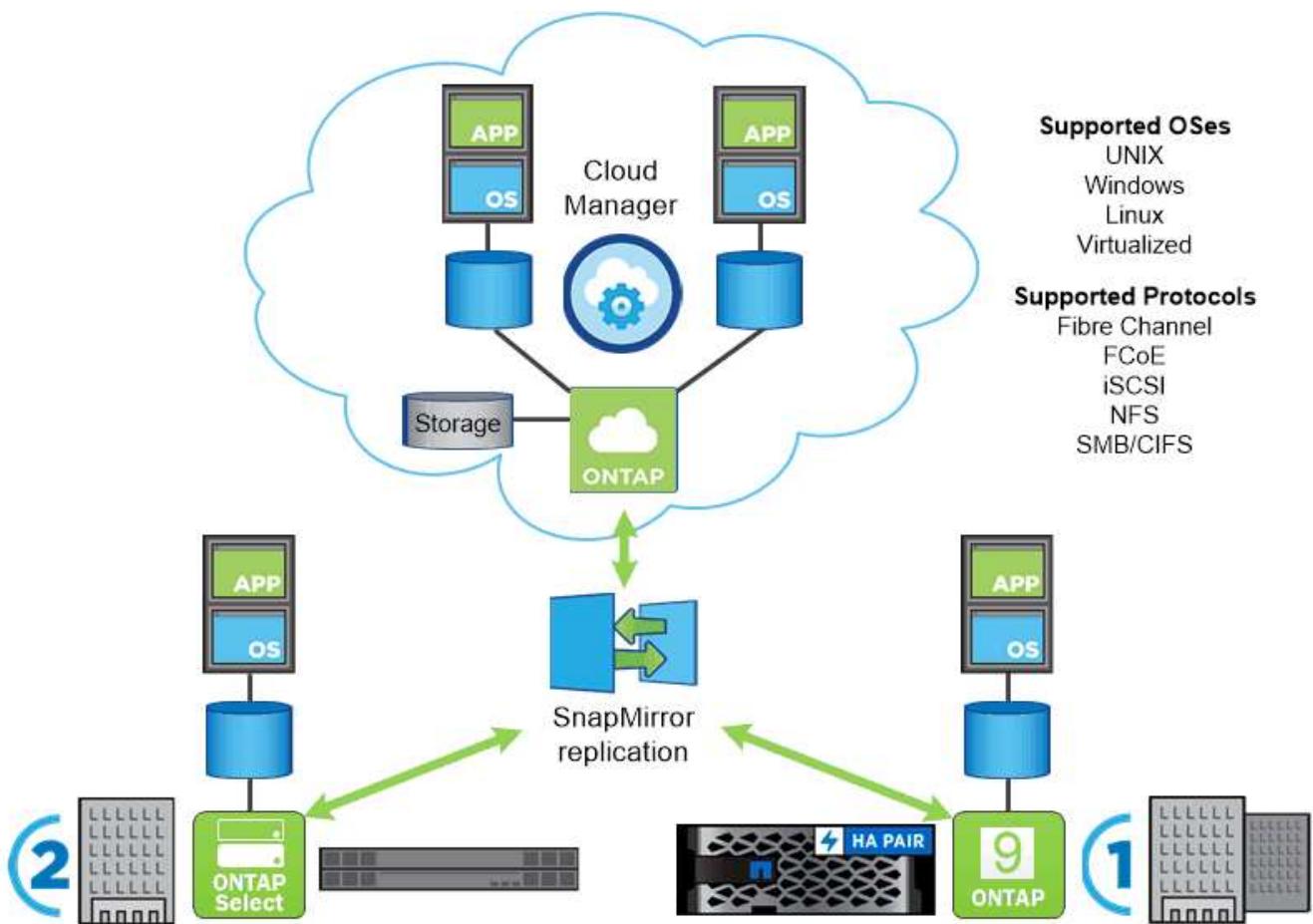
software, NetApp AFF ensures nondisruptive operations, from maintenance to upgrades to complete replacement of your storage system.

NetApp ONTAP is a powerful storage-software tool with capabilities such as an intuitive GUI, REST APIs with automation integration, AI-informed predictive analytics and corrective action, nondisruptive hardware upgrades, and cross-storage import.

ONTAP provides the following features:

- A unified storage system with simultaneous data access and management of NFS, CIFS, iSCSI, FC, FCoE, and FC-NVMe protocols.
- Different deployment models include on-premises on all-flash, hybrid, and all-HDD hardware configurations; VM-based storage platforms on a supported hypervisor such as ONTAP Select; and in the cloud as Cloud Volumes ONTAP.
- Increased data storage efficiency on ONTAP systems with support for automatic data tiering, inline data compression, deduplication, and compaction.
- Workload-based, QoS-controlled storage.
- Seamless integration with a public cloud for tiering and protection of data. ONTAP also provides robust data protection capabilities that sets it apart in any environment:
  - **NetApp Snapshot copies.** A fast, point-in-time backup of data using a minimal amount of disk space with no additional performance overhead.
  - **NetApp SnapMirror.** Mirrors the Snapshot copies of data from one storage system to another. ONTAP supports mirroring data to other physical platforms and cloud-native services as well.
  - **NetApp SnapLock.** Efficiently administration of non-rewritable data by writing it to special volumes that cannot be overwritten or erased for a designated period.
  - **NetApp SnapVault.** Backs up data from multiple storage systems to a central Snapshot copy that serves as a backup to all designated systems.
  - **NetApp SyncMirror.** Provides real-time, RAID-level mirroring of data to two different plexes of disks that are connected physically to the same controller.
  - **NetApp SnapRestore.** Provides fast restoration of backed-up data on demand from Snapshot copies.
  - **NetApp FlexClone.** Provides instantaneous provisioning of a fully readable and writeable copy of a NetApp volume based on a Snapshot copy. For more information about ONTAP, see the [ONTAP 9 Documentation Center](#).

NetApp ONTAP is available on-premises, virtualized, or in the cloud.



Across the NetApp data fabric, you can count on a common set of features and fast, efficient replication across platforms. You can use the same interface and the same data management tools.

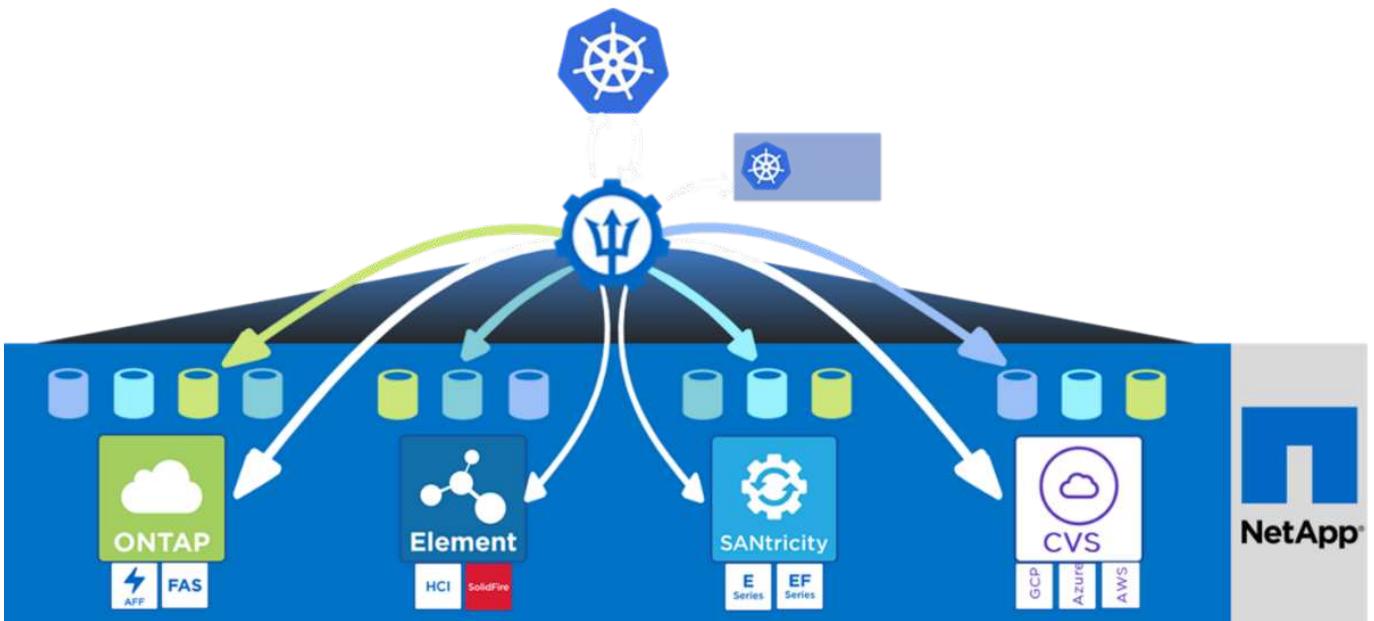
#### NetApp Astra Trident

NetApp Astra Trident is an open-source and fully supported storage orchestrator for containers and Kubernetes distributions, including Google Cloud Anthos. It works with the entire NetApp storage portfolio, including NetApp ONTAP software. Trident is fully CSI-compliant, and it accelerates the DevOps workflow by allowing you to provision and manage storage from your NetApp storage systems, without intervention from a storage administrator. Trident is deployed as an operator that communicates directly with the Kubernetes API endpoint to serve containers' storage requests in the form of persistent volume claims (PVCs) by creating and managing volumes on the NetApp storage system.

Persistent volumes (PVs) are provisioned based on storage classes defined in the Kubernetes environment. They use storage backends created by a storage administrator (which can be customized based on project needs) and storage system models to allow for any number of advanced storage features, such as compression, specific disk types, or QoS levels that guarantee performance.

For more information about NetApp Astra Trident, see the [Trident](#) page.

Trident orchestrates storage from each system and service in the NetApp portfolio.



### Google Cloud's Anthos

Google Cloud's Anthos is a cloud-based Kubernetes data center solution that enables organizations to construct and manage modern hybrid-cloud infrastructures while adopting agile workflows focused on application development. Anthos on bare metal extends the capability of Anthos to run on-premises directly on physical servers without a hypervisor layer and interoperate with Anthos GKE clusters in Google Cloud.

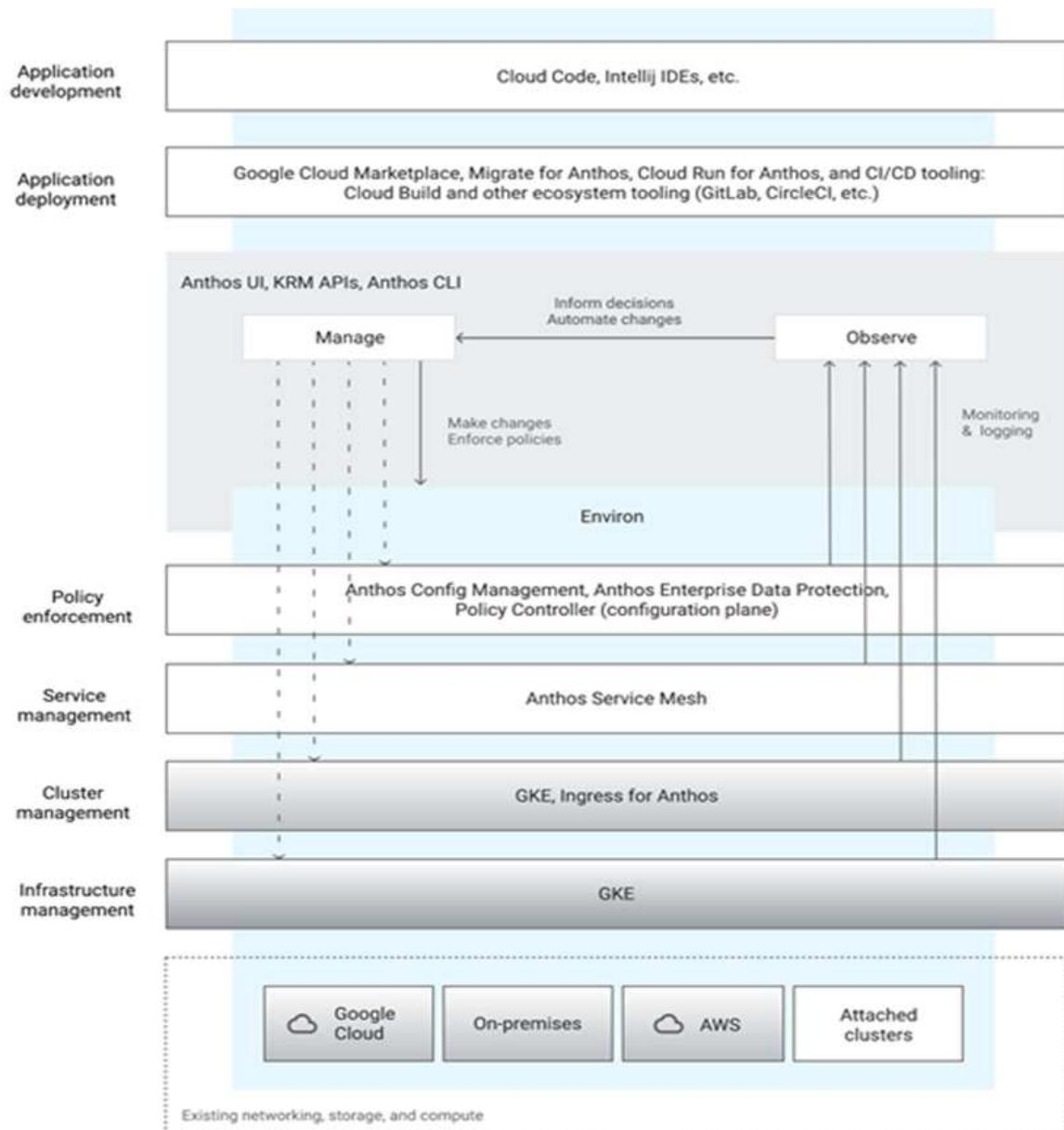
Adopting containers, service mesh, and other transformational technologies enables organizations to experience consistent application development cycles and production-ready workloads in local and cloud-based environments.

Anthos provides the following features:

- **Anthos configuration management.** Automates the policy and security of hybrid Kubernetes deployments.
- **Anthos Service Mesh.** Enhances application observability, security, and control with an Istio-powered service mesh.
- **Google Cloud Marketplace for Kubernetes applications.** A catalog of curated container applications available for easy deployment.
- **Migrate for Anthos.** Automatic migration of physical services and VMs from on-premises to the cloud. Figure 3 depicts the Anthos solution and how a deployment in an on-premises data center interconnects with infrastructure in the cloud.

For more information about Anthos, see the [Anthos website](#).

The following figure presents Google Cloud's Anthos architecture.



## Anthos on bare metal

Anthos on bare metal is an extension of GKE that is deployed in a customer's private data center. An organization can deploy the same applications designed to run in containers in Google Cloud in Anthos clusters on-premises. Anthos on bare metal runs directly on physical servers with the user's choice of underlying Linux operating system and provides customers with a full-fledged hybrid cloud environment with the capability to run at the core or edge of their data centers.

Anthos on bare metal offers the following benefits:

- **Hardware agnostic.** Customers can run Anthos on their choice of optimized hardware platform in their existing data centers.
- **Cost savings.** You can realize significant cost savings by using your own physical resources for application deployments instead of provisioning resources in the Google Cloud environment.
- **Develop then publish.** You can use on-premises deployments while applications are in development, which allows for the testing of applications in the privacy of your local data center before you make them publicly available in the cloud.

- **Better performance.** Intensive applications that demand low latency and the highest levels of performance can be run closer to the hardware.
- **Security requirements.** Customers with increased security concerns or sensitive data sets that cannot be stored in the public cloud are able to run their applications from the security of their own data centers, thereby meeting organizational requirements.
- **Management and operations.** Anthos on bare metal comes with a wide range of facilities that increase operational efficiency such as built-in networking, lifecycle management, diagnostics, health checks, logging, and monitoring.

[Next: Solution requirements.](#)

## Solution requirements

### Hardware requirements

#### Compute: bring your own server

The hardware-agnostic capabilities of Anthos on bare metal allow you to select a compute platform optimized for your use case. Therefore, you can match your existing infrastructure and reduce capital expenditure.

The following table lists the minimum number of compute hardware components that are required to implement this solution, although the hardware models used can vary based on customer requirements.

Usage	Hardware and model	Quantity
Admin nodes	Cisco UCS B200	3
Worker nodes	HP Proliant DL360	4

#### Storage: NetApp ONTAP

The following table lists the minimum number of storage-hardware components needed to implement the solution, although the hardware models used can vary based on customer requirements.

Hardware	Model	Quantity
NetApp AFF	NetApp AFF A300	2 (1 HA pair)

### Software requirements

The software versions identified in the following table were used by NetApp and our partners to validate the solution with NetApp, although the software components used can vary based on customer requirements.

Software	Purpose	Version
Ubuntu	OS on 3 Admins	20.04
	OS on Worker4	20.04
	OS on Worker3	18.04
CentOS	OS on Worker2	8.2
Red Hat Enterprise Linux	OS on Worker1	8.1
Anthos on bare metal	Container Orchestration	1.6.0

Software	Purpose	Version
NetApp ONTAP	Storage OS	9.7P8
NetApp Astra Trident	Container Storage Management	20.10



This multi-OS environment shows the interoperability with supported OS versions of the Anthos on bare metal solution. We anticipate that customers will standardize on one or a subset of operating systems for deployment.

For Anthos on bare metal hardware and software requirements, see the [Anthos on bare metal documentation page](#).

[Next: Deployment summary.](#)

## Deployment summary

For the initial validation of this solution, NetApp partnered with World Wide Technology (WWT) to establish an environment at WWT's Advanced Technology Center (ATC). Anthos was deployed on a bare metal infrastructure using the `bmctl` tool provided by Google Cloud. The following section details the deployment used for validation purposes.

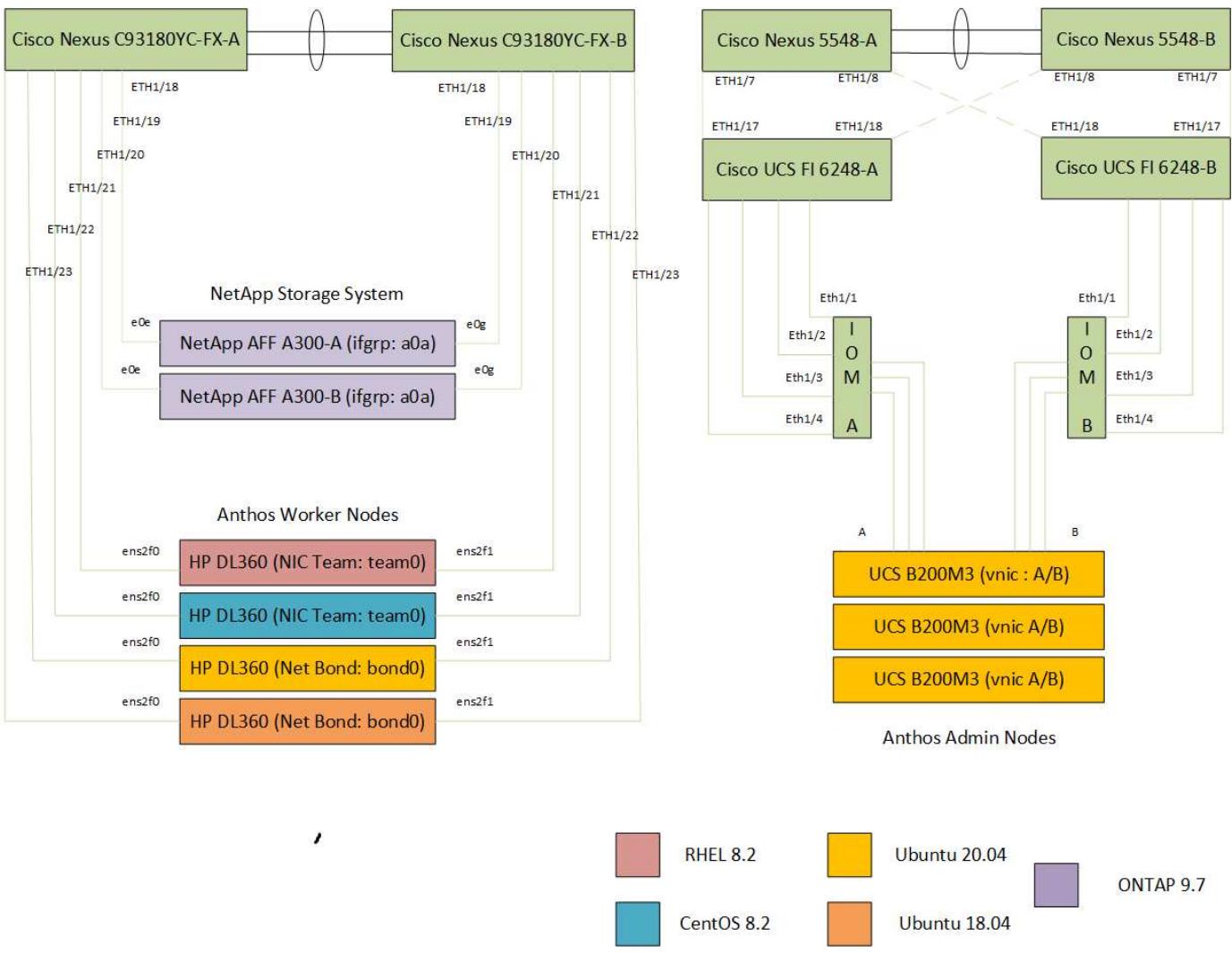
The Anthos on bare metal with NetApp solution was built as a highly available hybrid cluster with three Anthos control-plane nodes and four Anthos worker nodes.

The control-plane nodes used were Cisco UCS B200M3 blade servers hosted in a chassis and configured with a single virtual network interface card (vNIC) on each, which allowed for A/B failover at the Cisco UCS platform level for fault tolerance. The Cisco UCS chassis connected upstream to a pair of Cisco UCS 6248 fabric interconnects providing disparate paths for the separation of traffic along fabric A and fabric B. Those fabric interconnects connected upstream to a pair of Cisco Nexus 5548 data center switches that tied back to the core network at WWT.

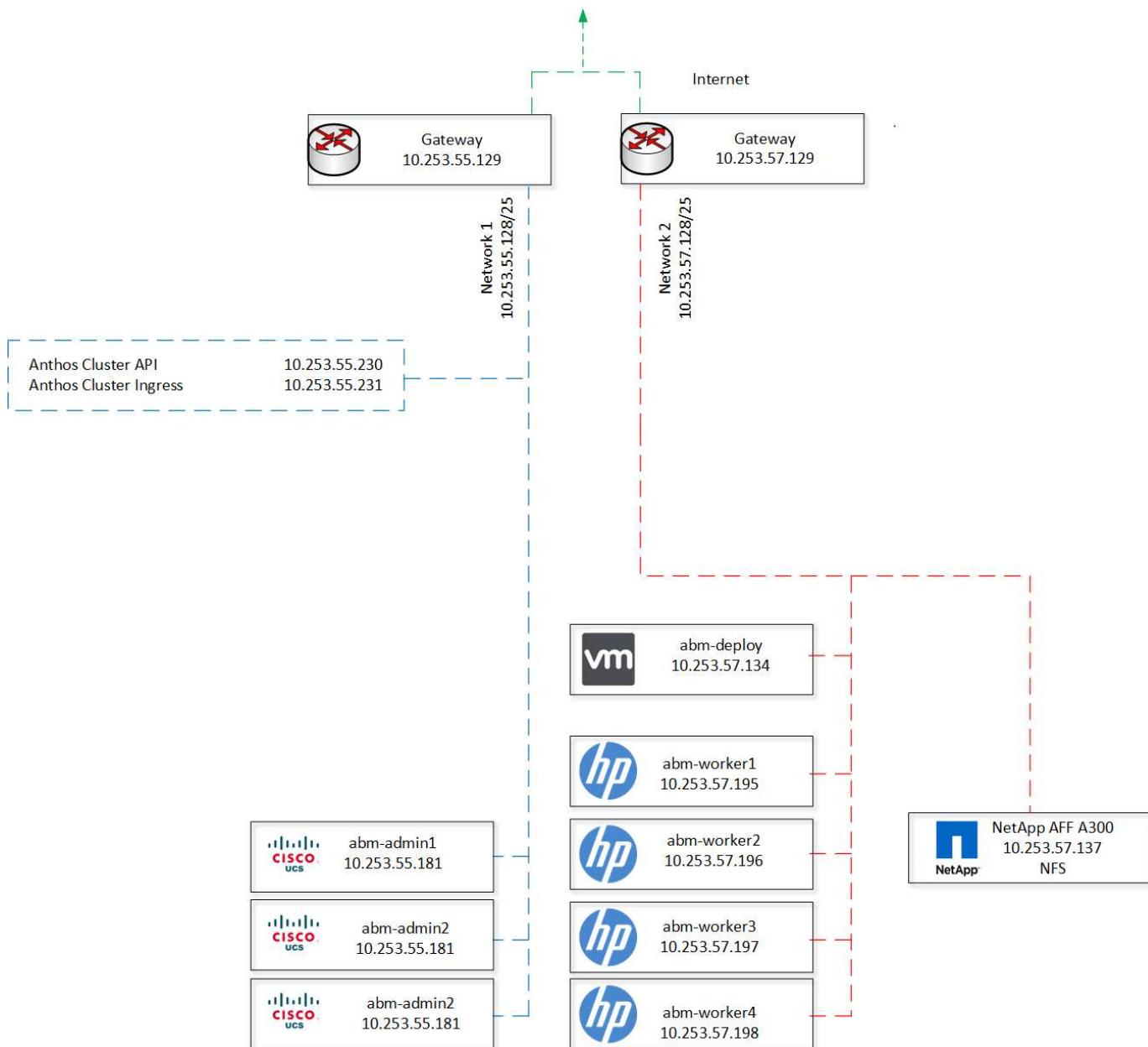
The worker nodes were HP Proliant DL360 nodes, each running one of the supported Linux distributions for Anthos on bare metal: Red Hat Enterprise Linux 8.2, CentOS 8.2, Ubuntu 20.04 LTS, or Ubuntu 18.04 LTS. The Red Hat Enterprise Linux 8 and CentOS 8 nodes were configured with NIC teams running in LACP mode and cabled to two Nexus 9k C93180YC-FX switches for fault tolerance. The Ubuntu servers were configured for network bonding in LACP mode and cabled to the same pair of Nexus 9k switches for fault tolerance.

The NetApp AFF A300 storage system running ONTAP 9.7 software was installed and connected physically to the same pair of Nexus 9k switches as the Anthos worker nodes. These network uplinks were aggregated into an interface group (a0a), and the appropriate data network VLAN was tagged to allow the worker nodes to interact with the storage system. A storage virtual machine (SVM) was created with data LIFs supporting the NFS protocol and dedicated to storage operations for Trident to provide persistent storage to the containers deployed in the Anthos on bare metal cluster. These persistent volumes were provided by NetApp Astra Trident 20.10, the latest release of the fully supported NetApp open-source storage orchestrator for Kubernetes.

The following figure depicts a physical cabling diagram of the solution to the top of rack data center switches.



The next figure presents a logical view of the solution as deployed and validated on the hardware in the lab at the NetApp partner WWT.



Next: Solution validation.

## Solution validation

The current deployment of this solution was put through two rigorous validation processes using tools provided by the Google Cloud team. These validations include a subset of the following tests:

- Partner validation of the Anthos-ready platform:
  - Confirm that all Anthos on bare metal platform services are installed and running.
  - Scale down the physical Anthos on bare metal cluster from four worker nodes to three and then back to four.
  - Create and delete a custom namespace.
  - Create a deployment of the Nginx web server, scaling that deployment by increasing the number of replicas.

- Create an ingress for the Nginx application and verify connectivity by curling the index.html.
- Successfully clean up all test suite activities and return the cluster to a pretest state.
- Partner validation of Anthos-ready storage:
  - Create a deployment with a persistent volume claim.
  - Use NetApp Astra Trident to provision and attach the requested persistent volume from NetApp ONTAP.
  - Validate the detach-and-reattach capability of persistent volumes.
  - Validate multi-attach, read-only access of persistent volumes from other pods on the node.
  - Validate the offline volume resize operation.
  - Verify that the persistent volume survives a cluster-scaling operation.

Next: Conclusion.

## Conclusion

Anthos on bare metal with NetApp provides a robust platform to run container-based workloads efficiently by allowing for the customization of deployed infrastructure. Customers can use the server infrastructure and supported operating system of their choice or even deploy the solution within their existing infrastructure. The power and flexibility of these environments increases greatly through the integration of NetApp ONTAP and NetApp Astra Trident, supporting stateful application workloads by efficiently provisioning and managing persistent storage for containers. By extending the potential of Google Cloud into their data center powered by NetApp, a customer can realize the benefits of a fully supported, highly available, easily scalable, and fully managed Kubernetes solution for development and production of their application workloads.

Next: Where to find additional information.

## Where to find additional information

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

- NetApp ONTAP Documentation Center

<https://docs.netapp.com/ontap-9/index.jsp>

- NetApp Astra Trident

<https://netapp-trident.readthedocs.io/en/stable-v20.10/>

- Google Cloud's Anthos

<https://cloud.google.com/anthos>

- Anthos on bare metal

<https://cloud.google.com/anthos/gke/docs/bare-metal>

# Data Migration and Data Protection

## Data Migration

### Best-Practice Guidelines for NetApp XCP

TR-4863: Best-Practice Guidelines for NetApp XCP - Data Mover, File Migration, and Analytics

Karthikeyan Nagalingam, NetApp

This document provides NetApp XCP best-practice guidelines and a test scenario-based solution. These best practices cover the migration workflow for on-premises as well as cloud, file-system analytics, troubleshooting, and performance tuning of XCP. The test-scenario section covers customer use cases and their requirements, the NetApp solution using XCP, and benefits to the customer.

[Next: NetApp XCP.](#)

### NetApp XCP

[Previous: Introduction.](#)

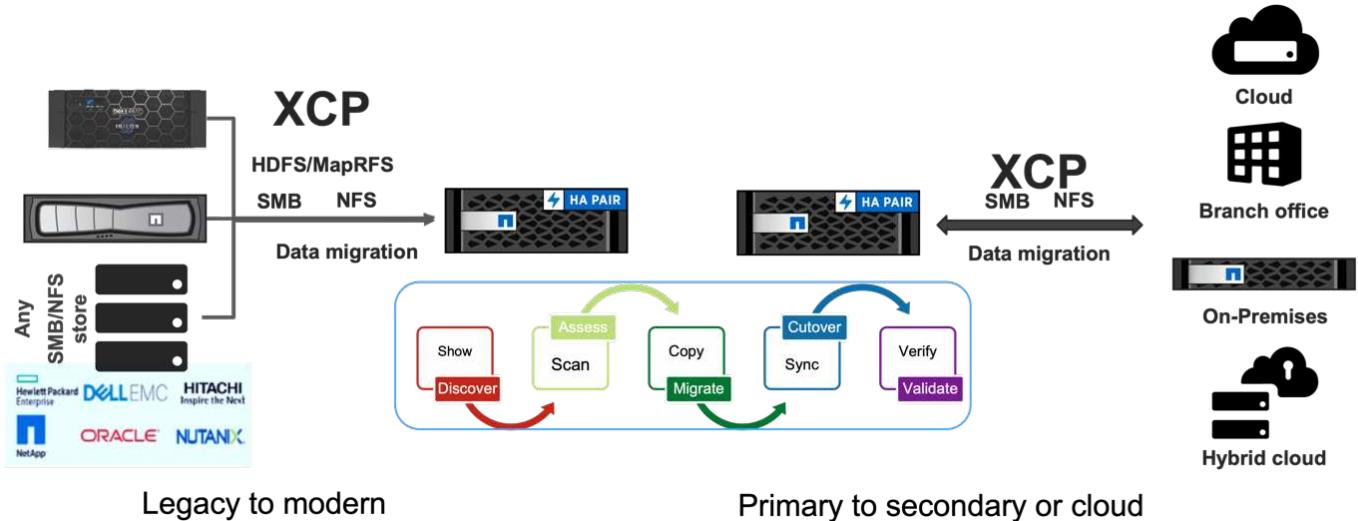
NetApp XCP transfers data by using multithreads and customizable features. It is designed for three major use cases: data move or migration, file-system analytics, and fast directory tree deletion.

#### Data move or migration

NetApp XCP transfers data from any NAS to NetApp NAS. This process consists of four major operations: scan, copy, sync, and verify. There are some additional features that help the data monitoring and transfer:

- **Scan.** Provides a high-level layout of NAS and MapR/HDFS data.
- **Copy.** Performs a baseline data transfer.
- **Sync.** Performs the incremental data transfer.
- **Verify.** Performs a thorough verification of the target.
- **Show (optional).** Discovers NAS shares.

The following figure illustrates XCP data migration and replication operations.



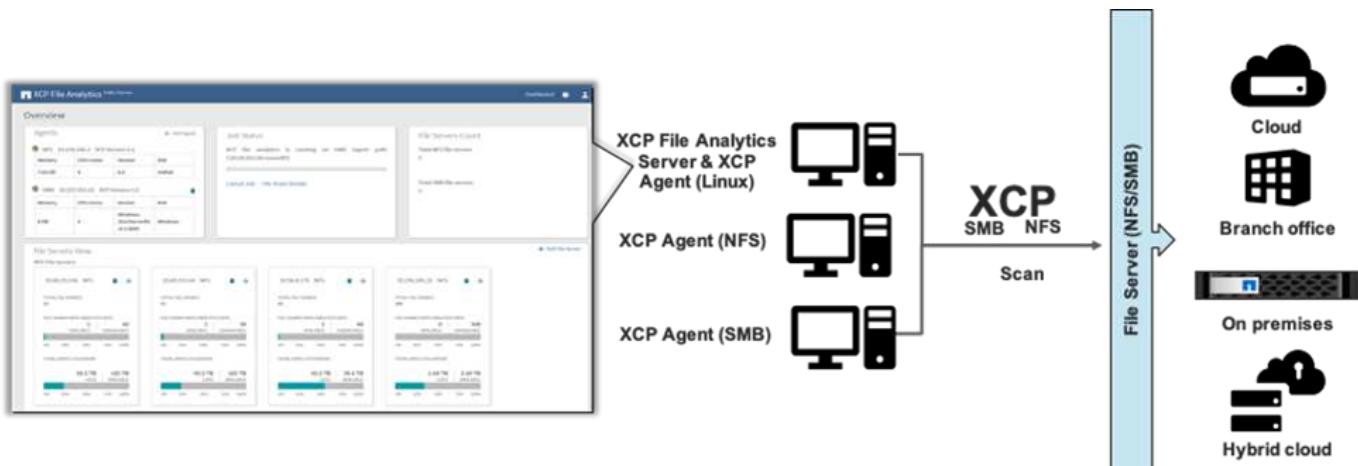
### File-system analytics

NetApp XCP natively enables you to identify, scrutinize, and analyze unstructured data to improve insights—a key requirement for enterprise customers who want to use those insights for better planning, to operationalize high-value digital assets, and for data governance through reporting and assessment.

Customers that deal with sensitive data can use NetApp XCP to answer typical operational questions, such as the following:

- Where is my data?
- How much data and what types of files do we have?
- What data is actively used and how much is dormant?

The following figure illustrates NetApp XCP file analytics communication from the GUI.



### Delete

It can be very challenging for storage teams and Electronic Design Automation (EDA) workloads to clean up large directories, whether it's stale data or test data that needs to be cleaned to recover storage space. XCP provides a fast delete functionality that can delete a complete directory tree. The NetApp XCP Delete function removes files and folders from a given NAS path. You can leverage the match filters to delete a specific set of files and folders. For a large number of files and folders, you can use the Force option, which does not require

a confirmation to delete.

### Live Source Migration support

Live Source Migration support included in XCP 1.7 allows migration from a data source that is in active use (read and write activity). XCP leaves out files that are being used during the migration job, such as copy and sync running, and skipped files information is captured in the XCP log.

This feature supports changes on the source but does not support changes on the destination. During migration, the destination should not be active. Live Source Migration support is only available for NFS migrations.



No special settings are required for Live Source Migrations.

### Prerequisites for XCP

Before you deploy NetApp XCP, the following prerequisites must be met:

1. Verify the NFS ports used by the NFS server by running the following command:

```
rpcinfo -p < NAS IP or on-prem nfs data LIF ip >
```

2. To access the location where you execute the XCP operations, such as on-premises or cloud instances (for example, Azure, AWS, or Google virtual machine [VM] instances), open the firewall ports for the NFS ports.
3. Verify that the NFS port is accessible from the XCP server by using the telnet command <on-prem nfs data LIF ip or NAS IP > 2049. The default port is 2049. If your environment has a different port, use that IP.
4. For NFS, verify that the shares are accessible from the XCP server by using the showmount -e < NAS IP > command.
5. Increase the number of inodes on the destination volume to more than the file count (number of files) on the source files.
6. Download the XCP license from the [NetApp XCP License Portal](#).
  - a. You must have a NetApp account in [mysupport.netapp.com](#) or you can register for free.
  - b. Download the license and have it ready.
7. Create one NFS share on-premises for each Azure NetApp volume or for the Cloud Volume Service (premium service level) in cloud for the XCP catalog.
8. Create an NAS volume and configure the share for the data destination.
9. For multiple XCP instances, you must have one or more servers or cloud instances to transfer the data from multiple source folders or files to the destination.
10. The maxdir size (default is 308MB) defines the maximum file count (approximately one million) in a single folder. Increase the maxdir size value to increase the file count. Increasing the value has an effect on additional CPU cycles.
11. In the cloud, NetApp recommends that you have ExpressRoute (Azure), Direct Connect (AWS), or Cloud Interconnect (GCP) between on-premises and cloud.

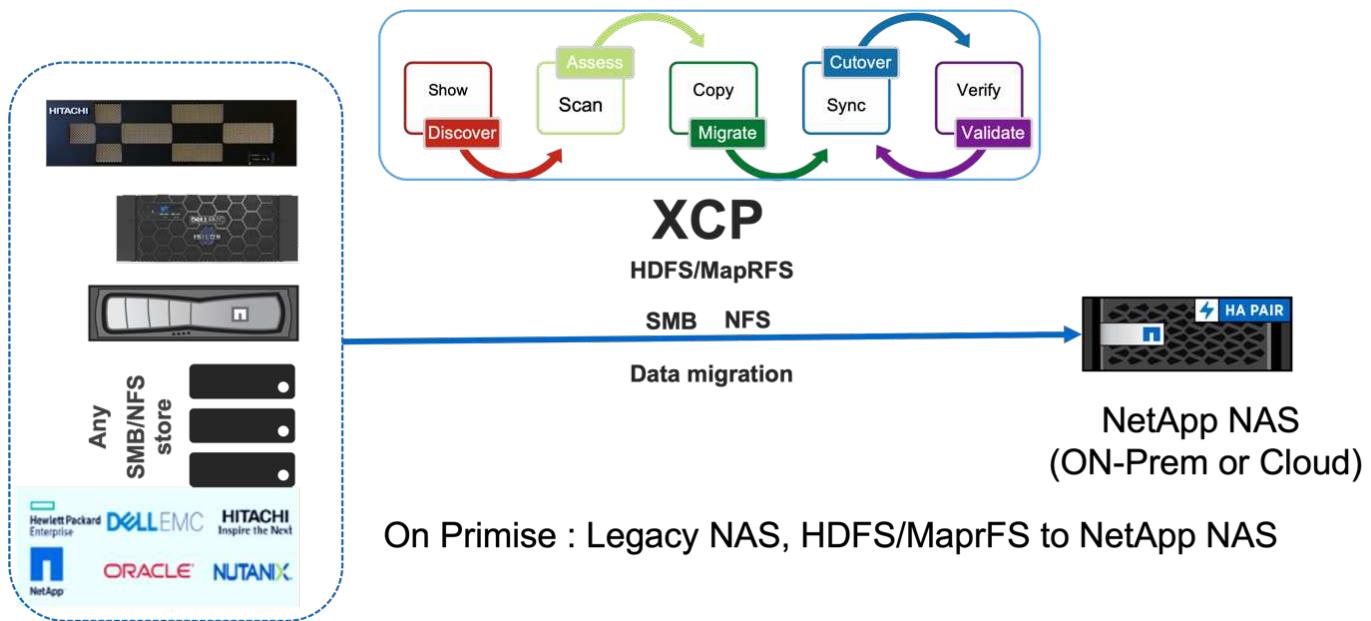
[Next: Migration workflow.](#)

## Migration workflow

Previous: [NetApp XCP](#).

Migration has different phases to follow for better planning and completion of the migration. To migrate data from third-party NAS storage or directly attached NAS exported storage using NetApp XCP, follow the migration guidelines provided in this section.

The following figure illustrates the migration workflow from any NAS to NetApp NAS.



### On-premises

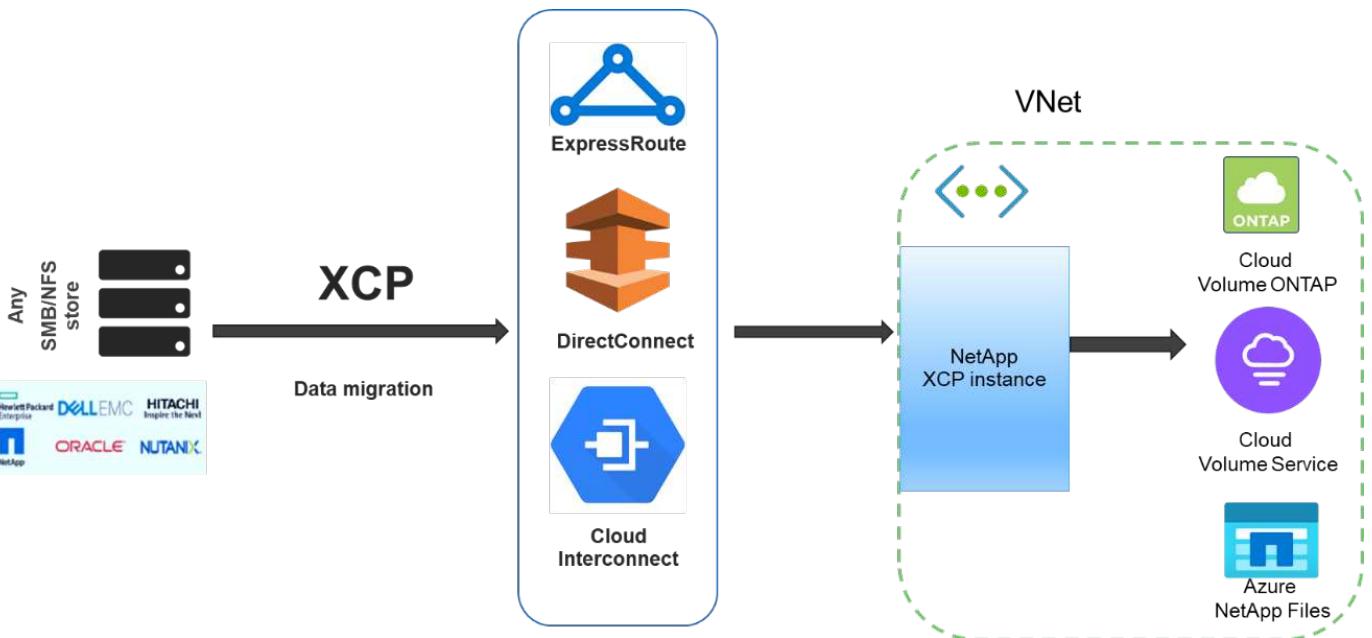
The migration workflow from any NAS to NetApp NAS includes the following steps:

1. Discover the NAS shares and data.
2. Scan the data and produce a report to find the layout of the data.
3. Create a baseline by running the XCP Copy command. For faster migrations, select more XCP instances and split the workload at the subfolder level to initiate parallel migration jobs.
4. For incremental updates, use XCP sync until the change rate is low for the cutover window.
5. Mark the source as read-only to perform a final sync by running the XCP sync command to complete the migration.
6. To verify that the data transferred correctly, compare the source and destination by running the `xcp verify` command.

### Cloud

For the cloud, you can follow a similar on-premises migration workflow if the connectivity between on-premises and the cloud is direct connect (AWS), ExpressRoute (Azure), or cloud interconnect (GCP).

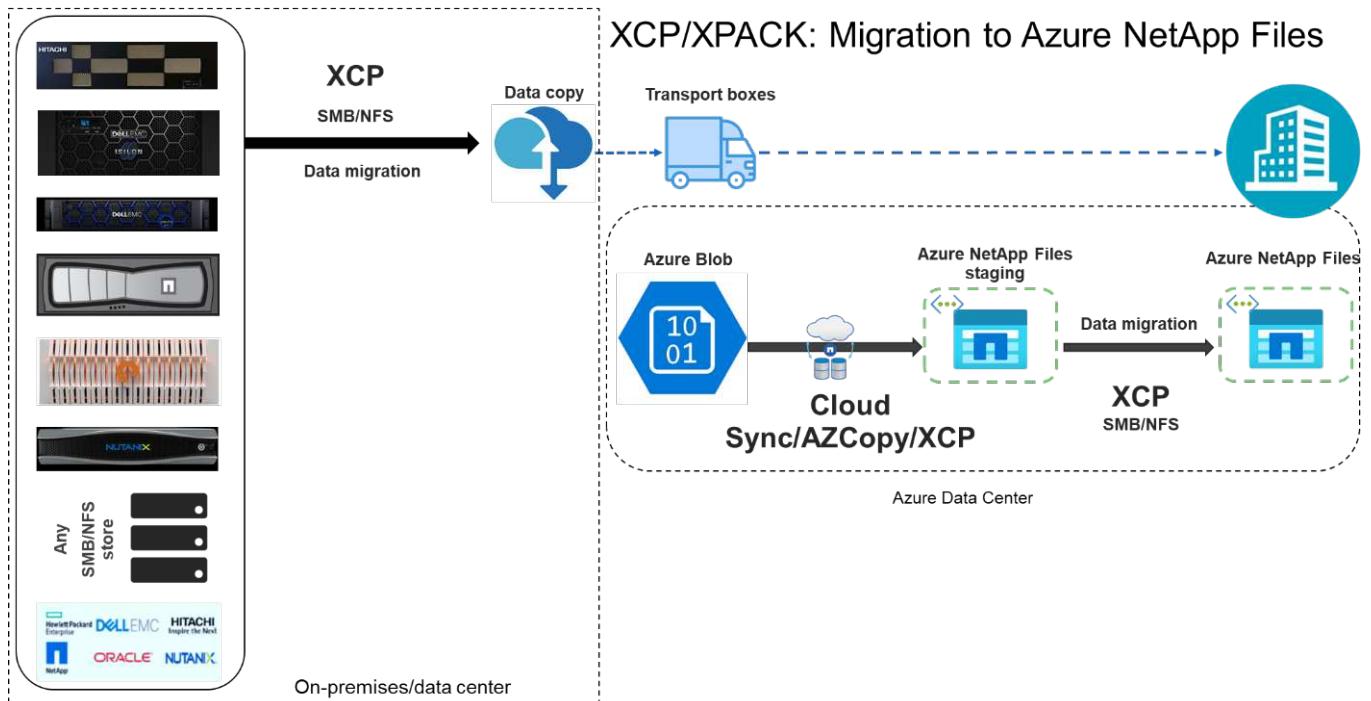
The following figure illustrates the migration workflow from on-premises to the cloud.



Data migration from any storage to cloud

If there is no direct internet connection between on-premises and the cloud, you must transfer the data from on-premises to the cloud through an offline data transport method such as truck. Each cloud service provider has a different method with different terminology to move data to their data center.

The following figure depicts the data mover solution for on-premises to Azure without ExpressRoute.



You can use a similar architecture with the respective components from the various cloud service providers.

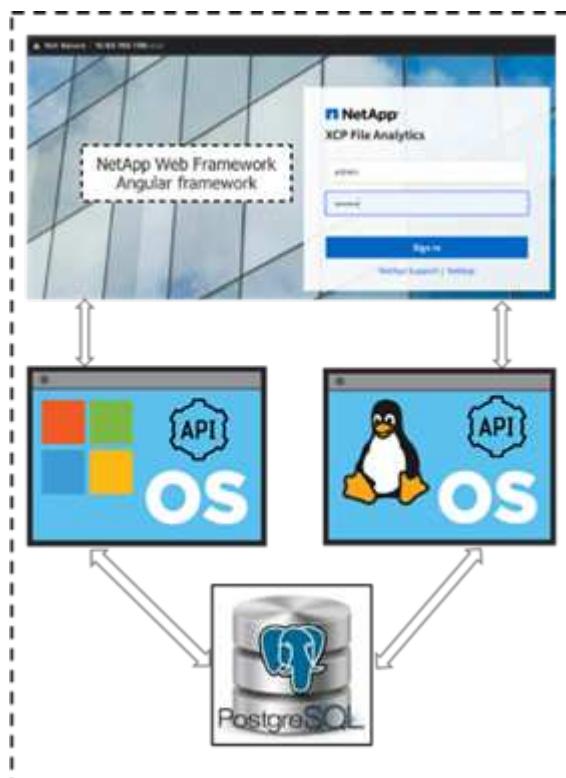
Next: File analytics.

## File analytics

Previous: [Migration workflow](#).

The NetApp XCP file analytics GUI helps to run file system scans by using XCP at the back end and visualizing statistics such as graphs and views for any NAS (NFS, SMB) file system. Starting in 1.6, XCP can be run as a service with the help of simple deployment steps by using the Configure and systemctl options. The XCP Configure option guides you to install and configure Postgres and a web server as well as collect credentials. The systemctl option runs XCP as a service for REST API communications from the GUI.

The following figure illustrates the XCP file analytics flow.



**i** For more information about the high-level architecture of XCP file analytics, GUI-based dashboard views such as stats view, and file distribution view details, see the blog post [NetApp XCP 1.6 Delivers Open File Analytics and Infrastructure Improvements](#).

There is a limited GUI in XCP 1.6 for customized graphs. To create the required graphs, you can use the CLI to run the `xcp scan` command with matching filters. See the following examples.

1. Generate a list of files modified beyond a year by using `xcp scan` and the `-match` filter with the space consumed.

```

[root@ch-vm-cent7-2 linux]# ./xcp scan -match "modified > 1*year" -l -q
192.168.89.110:/ifs/data_for_analysis > modified_morethan_year
XCP 1.6P1; (c) 2020 NetApp, Inc.; Licensed to Karthikeyan Nagalingam
[NetApp Inc] until Wed Sep 9 13:19:35 2020

xcp: WARNING: CPU count is only 1!

Filtered: 1 did not match

Xcp command : xcp scan -match modified > 1*year -l -q
192.168.89.110:/ifs/data_for_analysis
5,055 scanned, 5,054 matched, 0 error
Speed : 1.10 MiB in (510 KiB/s), 110 KiB out (49.5 KiB/s)
Total Time : 2s.
STATUS : PASSED
[root@ch-vm-cent7-2 linux]#
[root@ch-vm-cent7-2 linux]# cat modified_morethan_year
rwxr-xr-x --- 7056 503 0 512 7y99d
data_for_analysis/benchmarks/benchmarks/udf_TOBAGandTOTUPLE_7_benchmark.
out/6/_SUCCESS
rwxr-xr-x --- 7056 503 270 8.50KiB 7y99d
data_for_analysis/benchmarks/benchmarks/udf_TOBAGandTOTUPLE_7_benchmark.
out/6/part-r-00000
rw-r--r-- --- 7056 503 0 512 7y58d
data_for_analysis/benchmarks/benchmarks/udf_TOBAGandTOTUPLE_7_benchmark.
out/6/SUCCESS.crc
rw-r--r-- --- 7056 503 270 8.50KiB 7y99d
data_for_analysis/benchmarks/benchmarks/udf_TOBAGandTOTUPLE_7_benchmark.
out/6/out_original
rw-r--r-- --- 7056 503 270 8.50KiB 7y99d
data_for_analysis/benchmarks/benchmarks/udf_TOBAGandTOTUPLE_7_benchmark.
out/6/out_sorted
rwxr-xr-x --- 7056 503 0 512 7y99d
data_for_analysis/benchmarks/benchmarks/udf_TOBAGandTOTUPLE_7_benchmark.
out/2/_SUCCESS
rwxr-xr-x --- 7056 503 90 8.50KiB 7y99d
data_for_analysis/benchmarks/benchmarks/udf_TOBAGandTOTUPLE_7_benchmark.
out/2/part-r-00000
...
< console output removed due to page space size >
...

```

2. Find the space used by files that are more than one year old.

```
[root@ch-vm-cent7-2 linux]# ./xcp -du -match "modified > 1*year"
```

```

192.168.89.110:/ifs/data_for_analysis/
XCP 1.6.1; (c) 2020 NetApp, Inc.; Licensed to Karthikeyan Nagalingam
[NetApp Inc] until Wed Sep 9 13:19:35 2020
xcp: WARNING: CPU count is only 1!
52.5KiB
data_for_analysis/benchmarks/benchmarks/Macro_Scope_1_benchmark.out
28.5KiB
data_for_analysis/benchmarks/benchmarks/CollectedGroup_6_benchmark.out
28.5KiB data_for_analysis/benchmarks/benchmarks/Foreach_11_benchmark.out
153KiB
data_for_analysis/benchmarks/benchmarks/SecondarySort_9_benchmark.out
412KiB
data_for_analysis/benchmarks/benchmarks/CoGroupFlatten_6_benchmark.out
652KiB data_for_analysis/benchmarks/benchmarks/Iterator_1_benchmark.out
652KiB
data_for_analysis/benchmarks/benchmarks/LoaderDefaultDir_1_benchmark.out
652KiB data_for_analysis/benchmarks/benchmarks/Order_4_benchmark.out
28.5KiB
data_for_analysis/benchmarks/benchmarks/MapPartialAgg_4_benchmark.out/2
28.5KiB
data_for_analysis/benchmarks/benchmarks/CastScalar_11_benchmark.out/2
1.29MiB data_for_analysis/benchmarks/benchmarks/Order_18_benchmark.out
652KiB
data_for_analysis/benchmarks/benchmarks/FilterBoolean_5_benchmark.out
20.5KiB
data_for_analysis/benchmarks/benchmarks/Macro_DefinitionAndInline_5_benc
hmark.out/2
628KiB data_for_analysis/benchmarks/benchmarks/Types_29_benchmark.out
...
< console output removed due to page space size >
...
3.18MiB data_for_analysis/benchmarks/benchmarks/hadoop10
340KiB data_for_analysis/benchmarks/benchmarks/Split_5_benchmark.out
5.90GiB data_for_analysis/benchmarks/benchmarks
6.56GiB data_for_analysis/benchmarks
6.56GiB data_for_analysis

```

Filtered: 488 did not match

```

Xcp command : xcp -du -match modified > 1*year
192.168.89.110:/ifs/data_for_analysis/
Stats       : 5,055 scanned, 4,567 matched
Speed       : 1.10 MiB in (1.36 MiB/s), 110 KiB out (135 KiB/s)
Total Time  : 0s.
STATUS      : PASSED
[root@ch-vm-cent7-2 linux]#

```

3. Find the total size and graphical view of data that was modified more than one year ago.

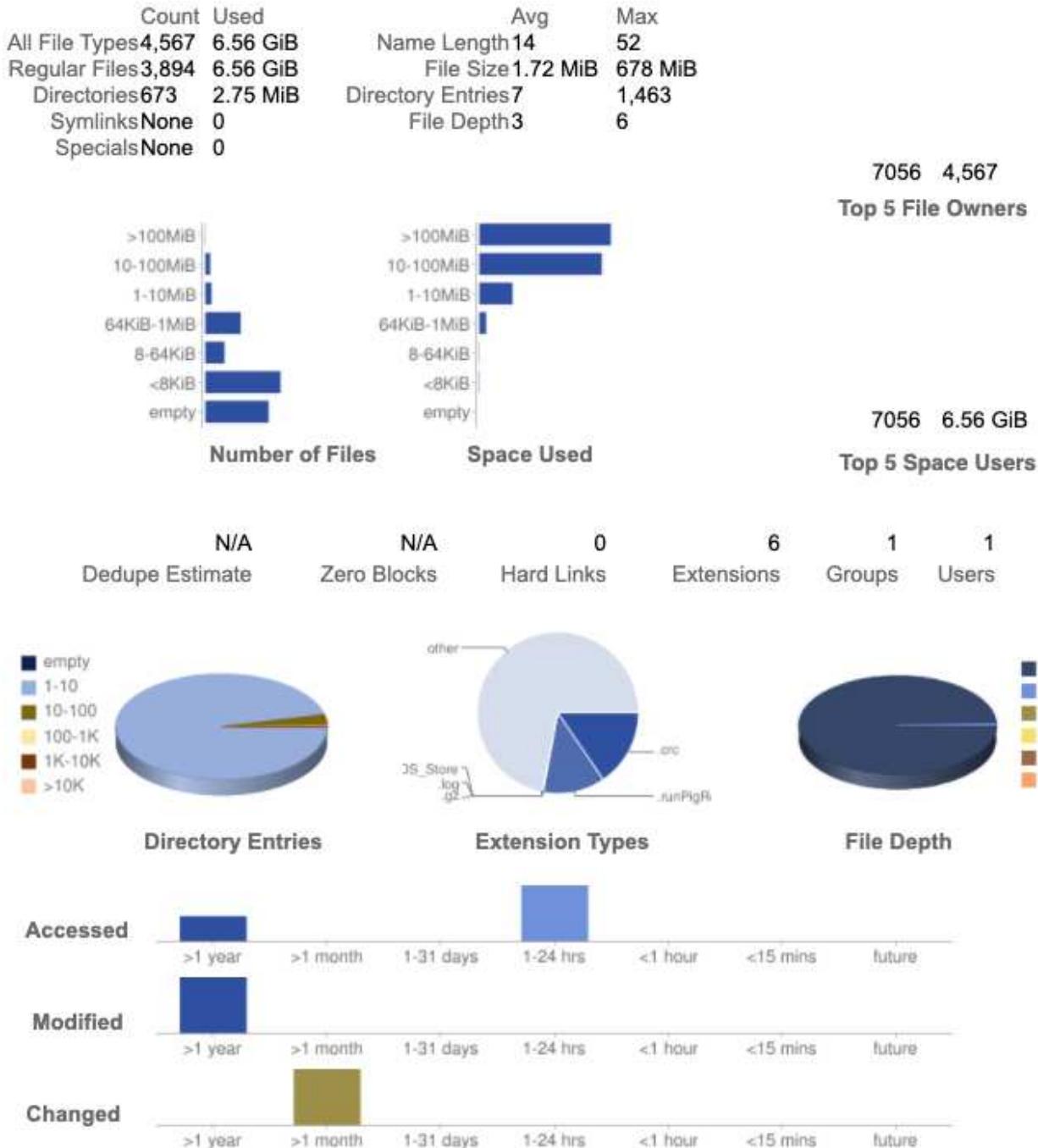
```
[root@ch-vm-cent7-2 linux]# ./xcp -stats -match "modified > 1*year"
-html 192.168.89.110:/ifs/data_for_analysis/ >
modified_morethan_year_stats.html
XCP 1.6.1; (c) 2020 NetApp, Inc.; Licensed to Karthikeyan Nagalingam
[NetApp Inc] until Wed Sep 9 13:19:35 2020

xcp: WARNING: CPU count is only 1!

Xcp command : xcp -stats -match modified > 1*year -html
192.168.89.110:/ifs/data_for_analysis/
Stats        : 5,055 scanned, 4,567 matched
Speed        : 1.10 MiB in (919 KiB/s), 110 KiB out (89.1 KiB/s)
Total Time   : 1s.
STATUS       : PASSED
[root@ch-vm-cent7-2 linux]#
```

The following report is a custom example scan of files that were modified more than one year ago.

Command scan 192.168.89.110:/ifs/data\_for\_analysis  
 Options '-stats': True, '-match': 'modified > 1\*year'  
 Unreadable directories None Unreadable files None  
 Filters: Unmatched None  
 Summary 5,055 scanned, 4,567 matched, 1.10 MiB in (924 KiB/s), 110 KiB out (89.7 KiB/s), 1s.



## Deployment steps

Previous: [File analytics](#).

### Test bed details

The following table provides the details of the test bed that was used for this deployment and performance validation.

Solution components	Details
XCP version 1.7	<ul style="list-style-type: none"><li>• One Linux server - Linux (RHEL 7.9 or RHEL 8)</li><li>• One Windows server – Windows Server 2019 standard</li></ul>
NetApp AFF storage array HA pair for the source volume	<ul style="list-style-type: none"><li>• AFF8080</li><li>• NetApp ONTAP 9</li><li>• NFS protocol</li></ul>
NetApp AFF storage array HA pair for destination volume	<ul style="list-style-type: none"><li>• AFF A800</li><li>• ONTAP 9</li><li>• NFS protocol</li></ul>
Fujitsu PRIMERGY RX2540 server	Each equipped with: * 48 CPUs * Intel Xeon * 256GB physical memory * 10GbE dual port
Networking	10GbE

### Deployment steps - NAS

To deploy NetApp XCP for data transfer, first install and activate the XCP software on the destination location. You can review the details in the [NetApp XCP User Guide](#). To do so, complete the following steps:

1. Meet the prerequisites as detailed in the section “[Prerequisites for XCP](#).”
2. Download the XCP software from the [NetApp XCP \(Downloads\)](#) page.
3. Copy the downloaded XCP tar files to the XCP server.

```
# scp Documents/OneDrive\ -\ NetApp\  
Inc/XCP/software/1.6.1/NETAPP_XCP_1.6.1.tgz  
mailto:root@10.63.150.53:/usr/src
```

4. Untar the tarfile.

```
[root@mastr-53 src]# tar -zxvf NETAPP_XCP_1.6.1.tgz
```

5. Download the license from <https://xcp.netapp.com/license/xcp.xwic> and copy to the XCP server.
6. Activate the license.

```
[root@mastr-53 linux]# ./xcp activate  
[root@mastr-53 src]# cp license /opt/NetApp/xFiles/xcp/license  
[root@mastr-53 src]# cd /usr/src/xcp/linux/  
[root@mastr-53 linux]# ./xcp activate
```

7. Find the source NFS port and destination NFS server. The default port is 2049.

```
[root@mastr-53 ~]# rpcinfo -p 10.63.150.213  
[root@mastr-53 ~]# rpcinfo -p 10.63.150.63
```

8. Check the NFS connection. Check the NFS server (for both source and destination) by using telnet to the NFS server port.

```
[root@mastr-53 ~]# telnet 10.63.150.127 2049  
[root@mastr-53 ~]# telnet 10.63.150.63 2049
```

9. Configure the catalog.

- a. Create an NFS volume and export NFS for the XCP catalog. You can also leverage the operating system NFS export for XCP catalog.

```
A800-Node1-2::> volume create -vserver Hadoop_SVM -volume xcpcatalog  
-aggregate aggr_Hadoop_1 -size 50GB -state online -junction-path  
/xcpcatalog -policy default -unix-permissions ---rwxr-xr-x -type RW  
-snapshot-policy default -foreground true  
A800-Node1-2::> volume mount -vserver Hadoop_SVM -volume  
xcpcatalog_vol -junction-path /xcpcatalog
```

- b. Check the NFS export.

```
[root@mastr-53 ~]# showmount -e 10.63.150.63 | grep xcpcatalog  
/xcpcatalog (everyone)
```

- c. Update xcp.ini.

```
[root@mastr-53 ~]# cat /opt/NetApp/xFiles/xcp/xcp.ini
# Sample xcp config
[xcp]
catalog = 10.63.150.64:/xcpcatalog

[root@mastr-53 ~]#
```

10. Find the source NAS exports by using `xcp show`. Look for:

```
== NFS Exports ==
== Attributes of NFS Exports ==
```

```
[root@mastr-53 linux]# ./xcp show 10.63.150.127
== NFS Exports ==
<check here>
== Attributes of NFS Exports ==
<check here>
```

11. (Optional) Scan the source NAS data.

```
[root@mastr-53 linux]# ./xcp scan -newid xcpscantest4 -stats
10.63.150.127:/xcpsrc_vol
```

Scanning the source NAS data helps you understand the data layout and find any potential issues for migration. The XCP scanning operation time is proportional to the number of files and the directory depth. You can skip this step if you are familiar with your NAS data.

12. Check the report created by `xcp scan`. Search mainly for unreadable folders and unreadable files.

```
[root@mastr-53 linux]# mount 10.63.150.64:/xcpcatalog /xcpcatalog
base) nkarthik-mac-0:~ karthikeyannagalingam$ scp -r
root@10.63.150.53:/xcpcatalog/catalog/indexes/xcpscantest4
Documents/OneDrive\ -\ NetApp\ Inc/XCP/customers/reports/
```

13. (Optional) Change the inode. View the number of inodes and modify the number based on the number of files to migrate or copy for both catalog and destination volumes (if required).

```
A800-Node1-2::> volume show -volume xcpcatalog -fields files,files-used  
A800-Node1-2::> volume show -volume xcpdest -fields files,files-used  
A800-Node1-2::> volume modify -volume xcpcatalog -vserver A800-Node1_vs1  
-files 2000000  
Volume modify successful on volume xcpcatalog of Vserver A800-Node1_vs1.  
  
A800-Node1-2::> volume show -volume xcpcatalog -fields files,files-used
```

14. Scan the destination volume.

```
[root@mastr-53 linux]# ./xcp scan -stats 10.63.150.63:/xcpdest
```

15. Check the source and destination volume space.

```
[root@mastr-53 ~]# df -h /xcpsrc_vol  
[root@mastr-53 ~]# df -h /xcpdest/
```

16. Copy the data from source to destination by using `xcp copy` and check the summary.

```
[root@mastr-53 linux]# ./xcp copy -newid create_Sep091599198212  
10.63.150.127:/xcpsrc_vol 10.63.150.63:/xcpdest  
<command inprogress results removed>  
Xcp command : xcp copy -newid create_Sep091599198212 -parallel 23  
10.63.150.127:/xcpsrc_vol 10.63.150.63:/xcpdest  
Stats : 9.07M scanned, 9.07M copied, 118 linked, 9.07M indexed,  
173 giants  
Speed : 1.57 TiB in (412 MiB/s), 1.50 TiB out (392 MiB/s)  
Total Time : 1h6m.  
STATUS : PASSED  
[root@mastr-53 linux]#
```



By default, XCP creates seven parallel processes to copy the data. This can be tuned.



NetApp recommends that the source volume be read only. In real time, the source volume is a live, active file system. The `xcp copy` operation might fail because NetApp XCP does not support a live source that is continuously changed by an application.

For Linux, XCP requires an Index ID because XCP Linux performs cataloging.

17. (Optional) Check the inodes on the destination NetApp volume.

```
A800-Node1-2::> volume show -volume xcpdest -fields files,files-used
vserver          volume   files   files-used
-----
A800-Node1_vs1  xcpdest  21251126 15039685

A800-Node1-2::>
```

18. Perform the incremental update by using `xcp sync`.

```
[root@mastr-53 linux]# ./xcp sync -id create_Sep091599198212
Xcp command : xcp sync -id create_Sep091599198212
Stats        : 9.07M reviewed, 9.07M checked at source, no changes, 9.07M
reindexed
Speed        : 1.73 GiB in (8.40 MiB/s), 1.98 GiB out (9.59 MiB/s)
Total Time   : 3m31s.
STATUS       : PASSED
```

For this document, to simulate real-time, the one million files in the source data were renamed, and then the updated files were copied to the destination by using `xcp sync`. For Windows, XCP needs both source and destination paths.

19. Validate data transfer. You can validate that the source and destination have the same data by using `xcp verify`.

```
Xcp command : xcp verify 10.63.150.127:/xcpsrc_vol 10.63.150.63:/xcpdest
Stats        : 9.07M scanned, 9.07M indexed, 173 giants, 100% found
(6.01M have data), 6.01M compared, 100% verified (data, attrs, mods)
Speed        : 3.13 TiB in (509 MiB/s), 11.1 GiB out (1.76 MiB/s)
Total Time   : 1h47m.
STATUS       : PASSED
```

XCP documentation provides multiple options (with examples) for the `scan`, `copy`, `sync`, and `verify` operations. For more information, see the [NetApp XCP User Guide](#).

 Windows customers should copy the data by using access control lists (ACLs). NetApp recommends using the command `xcp copy -acl -fallbackuser\<username> -fallbackgroup\<username or groupname> <source> <destination>`. To maximum performance, considering the source volume that has SMB data with ACL and the data accessible by both NFS and SMB, the target must be an NTFS volume. Using XCP (NFS version), copy the data from the Linux server and execute the XCP (SMB version) sync with the `-acl` and `-nodata` options from the Windows server to copy the ACLs from source data to the target SMB data.

For detailed steps, see [Configuring 'Manage Auditing and Security Log' Policy](#).

## Deployment steps - HDFS/MapRFS data migration

In this section, we discuss the new XCP feature called Hadoop Filesystem Data Transfer to NAS, which migrates data from HDFS/MapRFS to NFS and vice versa.

### Prerequisites

For the MapRFS/HDFS feature, you must perform the following procedure in a non-root user environment. Normally the non-root user is hdfs, mapr, or a user who has permission to make changes in the HDFS and MapRFS filesystem.

1. Set the CLASSPATH, HADOOP\_HOME, NHDFS\_LIBJVM\_PATH, LB\_LIBRARY\_PATH, and NHDFS\_LIBHDFS\_PATH variables in the CLI or the .bashrc file of the user along with the xcp command.
  - NHDFS\_LIBHDFS\_PATH points to the libhdfs.so file. This file provides HDFS APIs to interact and manipulate the HDFS/MapRFS files and filesystem as a part of the Hadoop distribution.
  - NHDFS\_LIBJVM\_PATH points to the libjvm.so file. This is a shared JAVA virtual machine library in the jre location.
  - CLASSPATH points to all jars files using (Hadoop classpath --glob) values.
  - LD\_LIBRARY\_PATH points to the Hadoop native library folder location.

See the following sample based on a Cloudera cluster.

```
export CLASSPATH=$(hadoop classpath --glob)
export LD_LIBRARY_PATH=/usr/java/jdk1.8.0_181-
cloudera/jre/lib/amd64/server/
export HADOOP_HOME=/opt/cloudera/parcels/CDH-6.3.4-
1.cdh6.3.4.p0.6751098/
#export HADOOP_HOME=/opt/cloudera/parcels/CDH/
export NHDFS_LIBJVM_PATH=/usr/java/jdk1.8.0_181-
cloudera/jre/lib/amd64/server/libjvm.so
export NHDFS_LIBHDFS_PATH=$HADOOP_HOME/lib64/libhdfs.so
```

In this release, we support XCP scan, copy, and verify operations and data migration from HDFS to NFS. You can transfer data from a data lake cluster single worker node and multiple worker nodes. In the 1.8 release, root and non-root users can perform data migration.

## Deployment steps - Non-root user migrates HDFS/MaprFS data to NetApp NFS

1. Follow the same steps mentioned from 1-9 steps from steps for deployment section.
2. In the following example, the user migrates data from HDFS to NFS.
  - a. Create a folder and files (using hadoop fs -copyFromLocal) in HDFS.

```
[root@n138 ~]# su - tester -c 'hadoop fs -mkdir /tmp/testerfolder_src/util-linux-2.23.2/mohankarthikhdfs_src'
[root@n138 ~]# su - tester -c 'hadoop fs -ls -d /tmp/testerfolder_src/util-linux-2.23.2/mohankarthikhdfs_src'
drwxr-xr-x  - tester supergroup          0 2021-11-16 16:52 /tmp/testerfolder_src/util-linux-2.23.2/mohankarthikhdfs_src
[root@n138 ~]# su - tester -c "echo 'testfile hdfs' > /tmp/a_hdfs.txt"
[root@n138 ~]# su - tester -c "echo 'testfile hdfs 2' > /tmp/b_hdfs.txt"
[root@n138 ~]# ls -ltrah /tmp/*_hdfs.txt
-rw-rw-r-- 1 tester tester 14 Nov 16 17:00 /tmp/a_hdfs.txt
-rw-rw-r-- 1 tester tester 16 Nov 16 17:00 /tmp/b_hdfs.txt
[root@n138 ~]# su - tester -c 'hadoop fs -copyFromLocal /tmp/*_hdfs.txt hdfs:///tmp/testerfolder_src/util-linux-2.23.2/mohankarthikhdfs_src'
[root@n138 ~]#
```

b. Check permissions in the HDFS folder.

```
[root@n138 ~]# su - tester -c 'hadoop fs -ls
hdfs:///tmp/testerfolder_src/util-linux-2.23.2/mohankarthikhdfs_src'
Found 2 items
-rw-r--r--  3 tester supergroup          14 2021-11-16 17:01
hdfs:///tmp/testerfolder_src/util-linux-
2.23.2/mohankarthikhdfs_src/a_hdfs.txt
-rw-r--r--  3 tester supergroup          16 2021-11-16 17:01
hdfs:///tmp/testerfolder_src/util-linux-
2.23.2/mohankarthikhdfs_src/b_hdfs.txt
```

c. Create a folder in NFS and check permissions.

```
[root@n138 ~]# su - tester -c 'mkdir /xcpsrc_vol/mohankarthiknfs_dest'
[root@n138 ~]# su - tester -c 'ls -l /xcpsrc_vol/mohankarthiknfs_dest'
total 0
[root@n138 ~]# su - tester -c 'ls -d /xcpsrc_vol/mohankarthiknfs_dest'
/xcpsrc_vol/mohankarthiknfs_dest
[root@n138 ~]# su - tester -c 'ls -ld /xcpsrc_vol/mohankarthiknfs_dest'
drwxrwxr-x 2 tester tester 4096 Nov 16 14:32
/xcpsrc_vol/mohankarthiknfs_dest
[root@n138 ~]#
```

d. Copy the files from HDFS to NFS using XCP, and check permissions.

```
[root@n138 ~]# su - tester -c '/usr/src/hdfs_nightly/xcp/linux/xcp
copy -chown hdfs:///tmp/testerfolder_src/util-linux-
2.23.2/mohankarthikhdfs_src/
10.63.150.126:/xcpsrc_vol/mohankarthiknfs_dest'
XCP Nightly_dev; (c) 2021 NetApp, Inc.; Licensed to Karthikeyan
Nagalingam [NetApp Inc] until Wed Feb 9 13:38:12 2022

xcp: WARNING: No index name has been specified, creating one with
name: autoname_copy_2021-11-16_17.04.03.652673

Xcp command : xcp copy -chown hdfs:///tmp/testerfolder_src/util-
linux-2.23.2/mohankarthikhdfs_src/
10.63.150.126:/xcpsrc_vol/mohankarthiknfs_dest
Stats       : 3 scanned, 2 copied, 3 indexed
Speed       : 3.44 KiB in (650/s), 80.2 KiB out (14.8 KiB/s)
Total Time  : 5s.
STATUS      : PASSED
[root@n138 ~]# su - tester -c 'ls -l
/xcpsrc_vol/mohankarthiknfs_dest'
total 0
-rw-r--r-- 1 tester supergroup 14 Nov 16 17:01 a_hdfs.txt
-rw-r--r-- 1 tester supergroup 16 Nov 16 17:01 b_hdfs.txt
[root@n138 ~]# su - tester -c 'ls -ld
/xcpsrc_vol/mohankarthiknfs_dest'
drwxr-xr-x 2 tester supergroup 4096 Nov 16 17:01
/xcpsrc_vol/mohankarthiknfs_dest
[root@n138 ~]#
```

[Next: Sizing guidelines.](#)

## Sizing guidelines

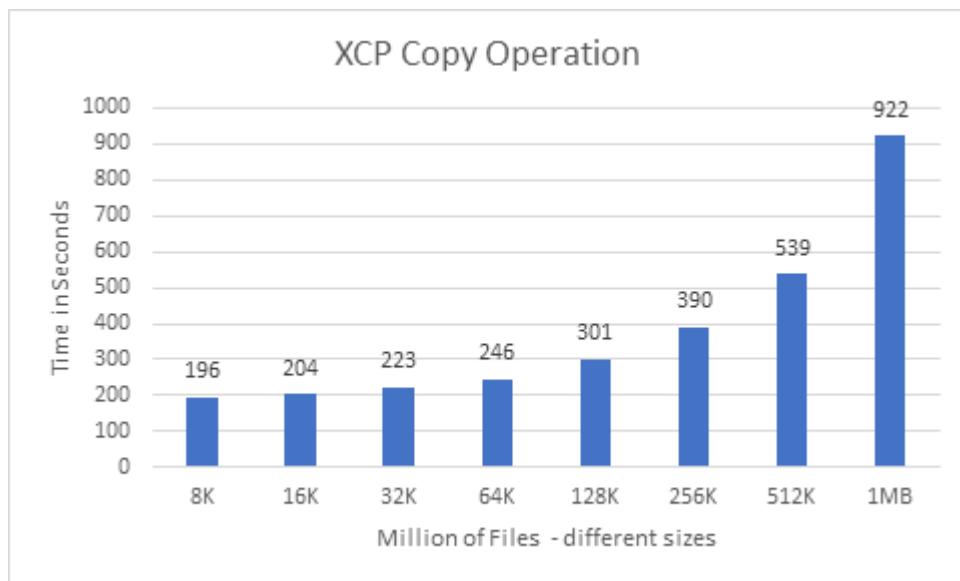
[Previous: Deployment steps.](#)

This section provides the approximate time to perform the XCP copy and XCP sync operations with a different file size of one million files for NFS.

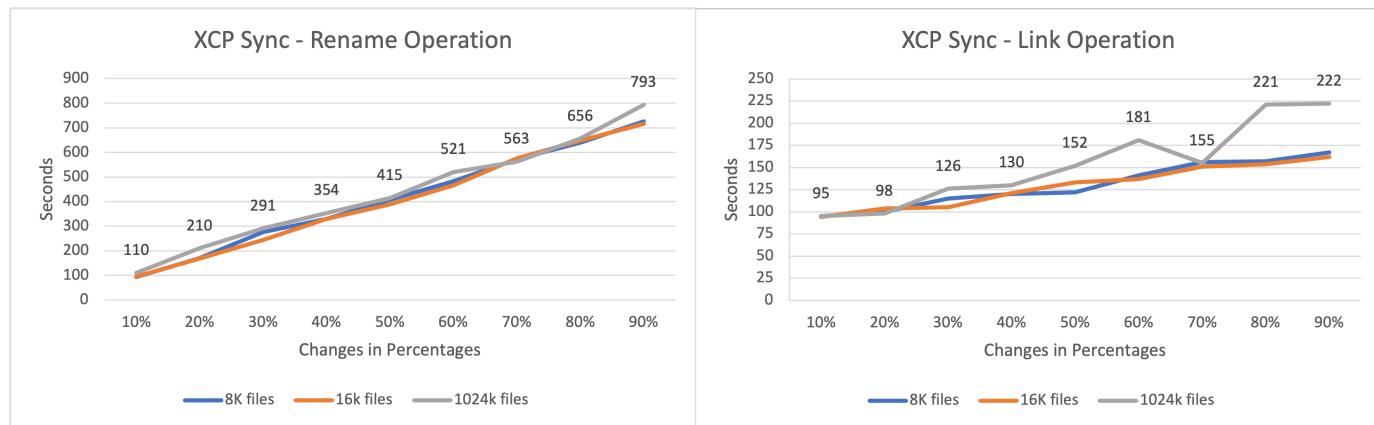
### Time estimate based on testing

The tests for the XCP copy and sync operations used the same test bed that was used for deployment. One million files of three sets of 8K, 16K, and 1MB files were created and the changes were performed in real time. The XCP sync function performed the differential incremental updates from the source to the target at the file level. The incremental update operation is one or more of these four operations: rename existing files and folders, append data to existing files, delete files and folders, and include additional hard, soft, and multilinks. For test purposes, we focused on the rename, append, delete, and links operations. In other words, the modification operations such as rename, append, and delete were performed at a change rate of 10% to 90% on one million files.

The following figure shows the results of the XCP copy operation.



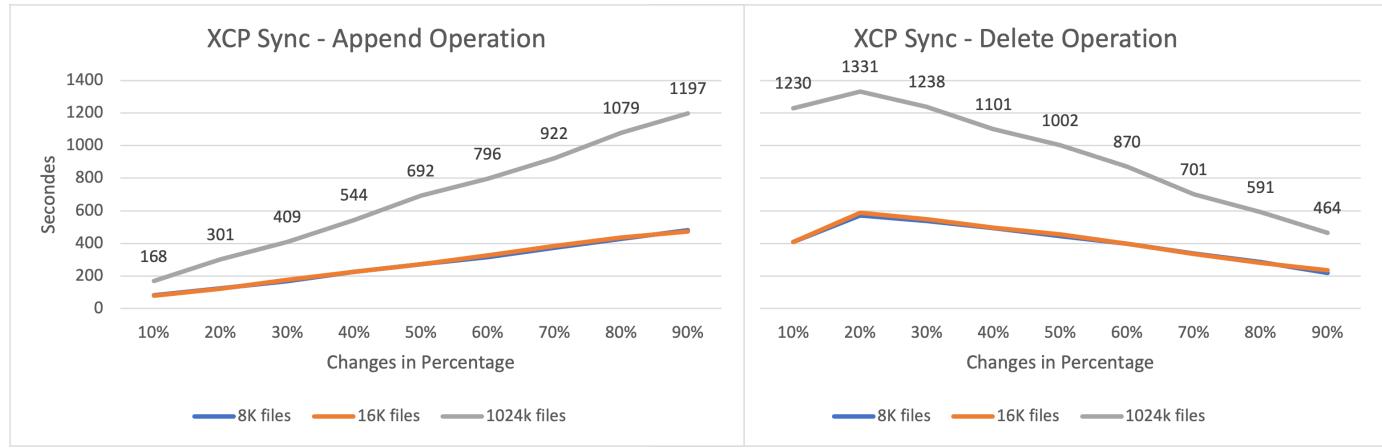
The following figure shows the results of the XCP Sync rename and link operations.



The file size is not propositional to the `xcp sync` completion time for transferring the renamed source files; the graphs are linear.

The link types are soft links, hard links, and multi-links. Soft links are considered normal files. The size of the files is not relevant for the time to complete the XCP sync operation.

The following figures show the results of the XCP sync append and delete operations.

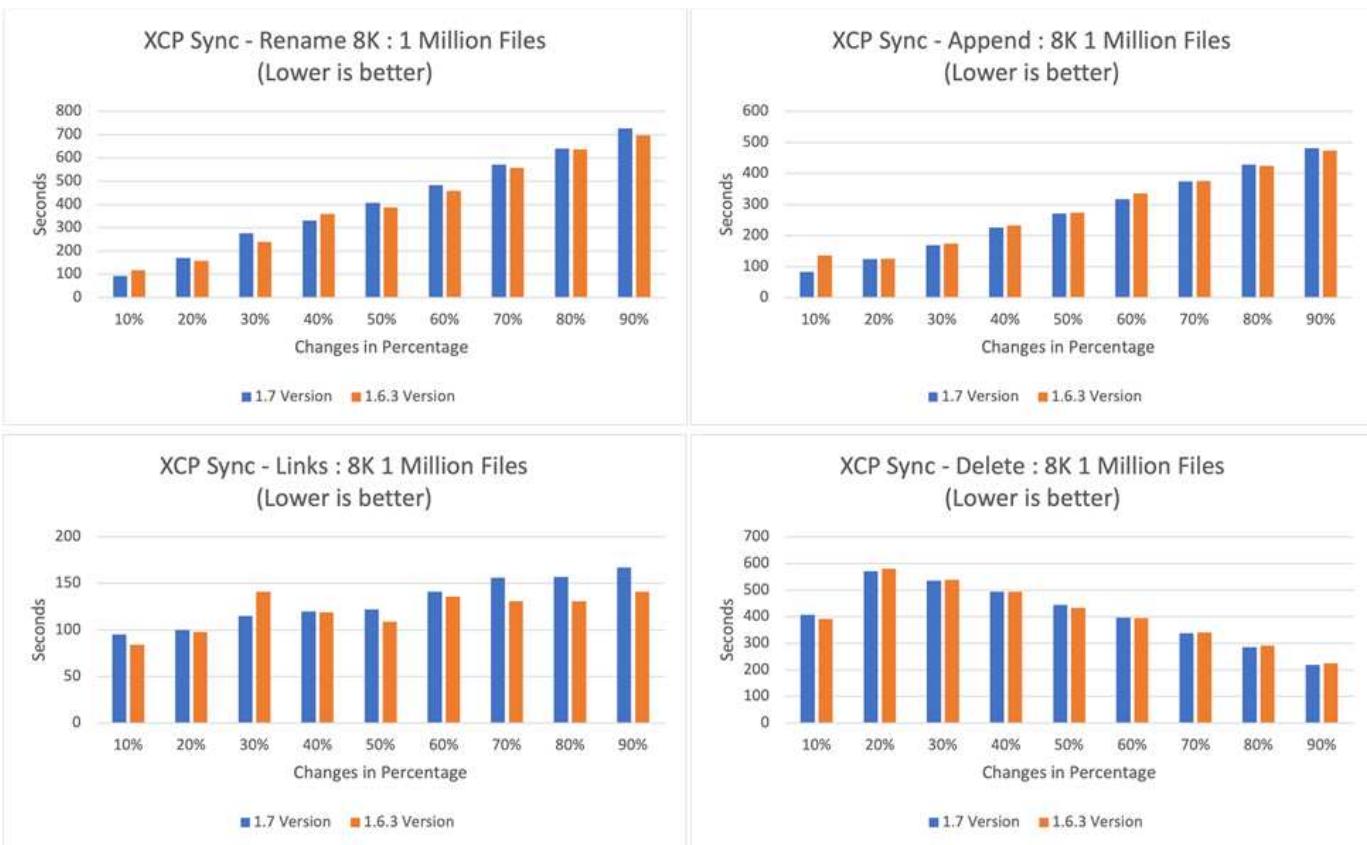


For the append and delete operations, large file sizes take more time compared to small file sizes. The time to complete the operation is linear to the percentage of append and delete changes.

#### Comparing XCP 1.6.1 to XCP 1.5

Compared to previous versions, XCP 1.6.3 and 1.7 provides improved performance. The following section shows a sync performance comparison between XCP 1.6.3 and 1.7 for 8K, 16K, and 1MB sizes of one million files.

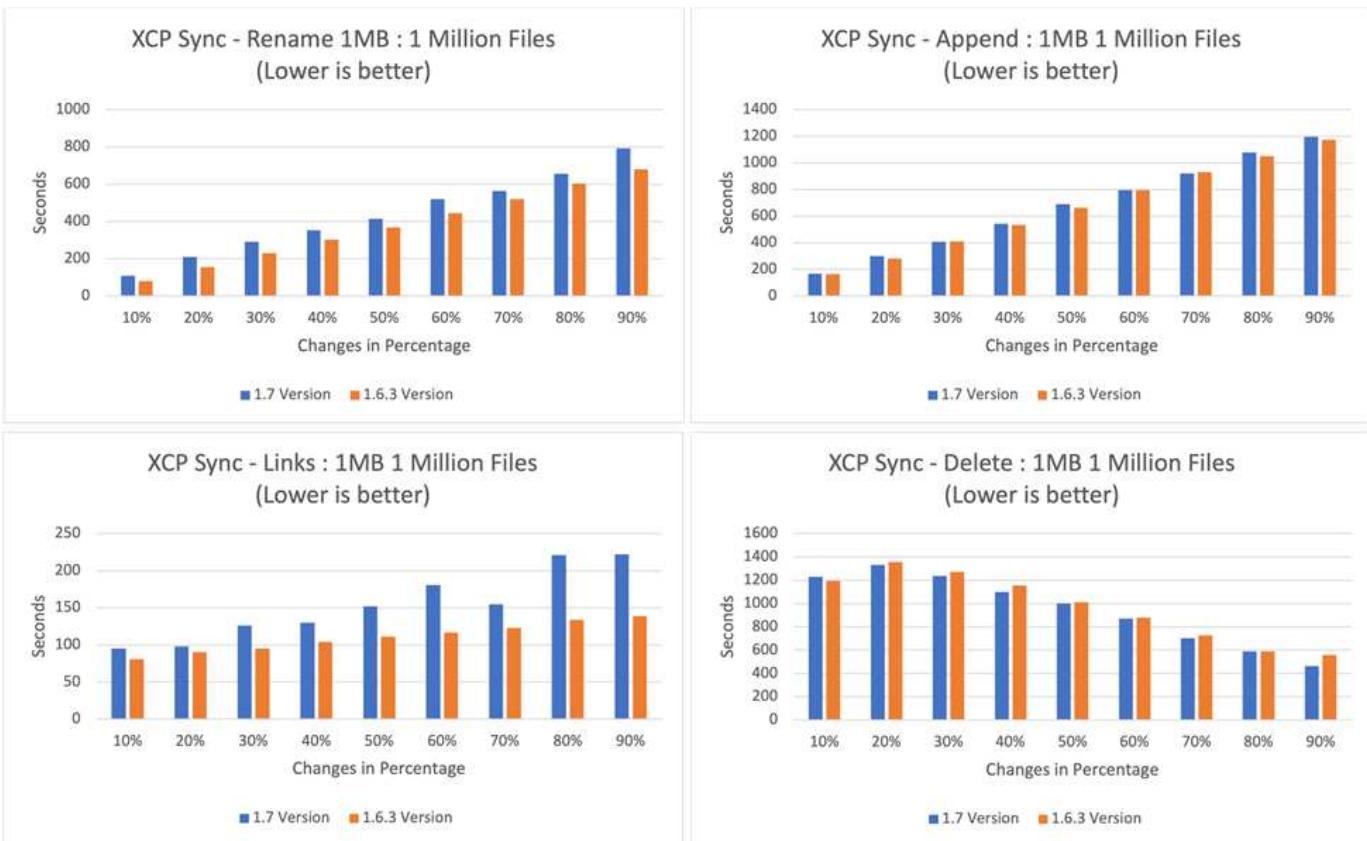
The following figures shows the results of the XCP sync performance for XCP 1.6.3 versus 1.7 (with an 8K size of one million files).



The following figure shows the results of the XCP sync performance for XCP 1.6.1 versus 1.5 (with a 16K size of one million files).



The following figure shows the results of the XCP sync performance for XCP 1.6.1 versus 1.5 with a 1MB size of one million files.



On average, the XCP 1.7 performance improved on or was similar to XCP 1.6.3 for the `xcp_sync` differential incremental update–rename, append, link, and delete operations with a 1MB size of one million files.

Based on this performance validation, NetApp recommends using XCP 1.7 for your data migration on-premises and in the cloud.

[Next: Performance tuning.](#)

## Performance tuning

[Previous: Sizing guidelines.](#)

This section provides some of the tuning parameters that help to improve the performance of XCP operations:

- For better scaling and to distribute the workload across multiple XCP instances, split the subfolders for each XCP instance for the migration and data transfer.
- XCP can use maximum CPU resources—the more the CPU cores, the better the performance. Therefore, you should have more CPUs in the XCP server. We lab tested 128GB RAM and 48x core CPUs, which provided better performance than 8x CPUs and 8GB RAM.
- XCP copy with the `-parallel` option is based on the number of CPUs. The default number of parallel threads (seven) is sometimes sufficient for most XCP data transfer and migration operations. For XCP Windows by default, the number of parallel processes is equal to the number of CPUs. The maximum number for the `-parallel` option should be less than or equal to the number of cores.
- 10GbE is a good start for data transfer. However, we tested with 25GbE and 100GbE, which provided better data transfer and are recommended for large file-size data transfer.
- For Azure NetApp Files, the performance varies based on the service level. For more information, see the following table, which shows Azure NetApp Files service levels and performance details.

Service level	Standard	Premium	Ultra
Throughput	16MBps/terabyte (TB)	64MBps/TB	128MBps/TB
Workload types	General purpose file shares, email, and web	BMs, databases, and applications	Latency-sensitive applications
Performance explained	Standard performance: 1,000 IOPS per TB (16K I/O) and 16MBps/TB	Premium performance – 4,000 IOPS per TB (16k I/O) and 64MBps/TB	Extreme performance: 8,000 IOPS per TB (16k I/O) and 128MBps/TB

You must choose the right service level based on the throughput and workload types. Most customers start with the Premium level and change the service level based on the workload.

[Next: Customer scenarios.](#)

## Customer scenarios

### Overview

[Previous: Performance tuning.](#)

This section describes customer scenarios and their architectures.

[Next: Data lake to ONTAP NFS.](#)

### Data lake to ONTAP NFS

[Previous: Customer scenarios.](#)

This use case is based on the largest financial customer proof of concept (CPOC) that we have done. Historically, we used the NetApp In-Place Analytics Module (NIPAM) to move analytics data to NetApp ONTAP AI. However, because of recent enhancements and the improved performance of NetApp XCP as well as the unique NetApp data mover solution approach, we reran the data migration using NetApp XCP.

## Customer challenges and requirements

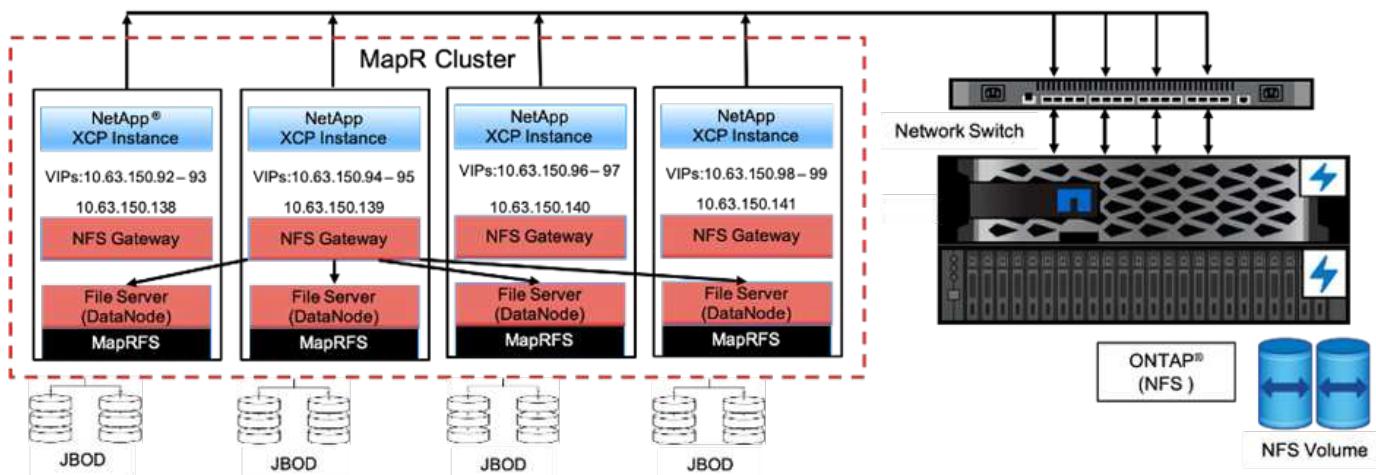
Customer challenges and requirements that are worth noting include the following:

- Customers have different types of data, including structured, unstructured, and semistructured data, logs, and machine-to-machine data in data lakes. AI systems require all these types of data to process for prediction operations. When data is in a data lake-native file system, it is difficult to process.
- The customer's AI architecture is not able to access data from Hadoop Distributed File System (HDFS) and Hadoop Compatible File System (HCFS), so the data is not available to AI operations. AI requires data in an understandable file system format such as NFS.
- Some special processes are required to move data from the data lake because of the large amount of data and high-throughput, and a cost-effective method is required to move the data to the AI system.

## Data mover solution

In this solution, the MapR File System (MapR-FS) is created from local disks in the MapR cluster. The MapR NFS Gateway is configured on each data node with virtual IPs. The file server service stores and manages the MapR-FS data. NFS Gateway makes Map-FS data accessible from the NFS client through the virtual IP. An XCP instance is running on each MapR data node to transfer the data from the Map NFS Gateway to NetApp ONTAP NFS. Each XCP instance transfers a specific set of source folders to the destination location.

The following figure illustrates the NetApp data mover solution for MapR cluster using XCP.



For detailed customer use cases, recorded demos, and test results, see the [Using XCP to Move Data from a Data Lake and High-Performance Computing to ONTAP NFS](#) blog.

For detailed steps on moving MapR-FS data into ONTAP NFS by using NetApp XCP, see Appendix B in [TR-4732: Big Data Analytics Data to Artificial Intelligence](#).

[Next: High-performance computing to ONTAP NFS.](#)

[High-performance computing to ONTAP NFS](#)

[Previous: Data lake to ONTAP NFS.](#)

This use case is based on requests from field organizations. Some NetApp customers have their data in a high-performance computing environment, which provides data analytics for training models and enables research organizations to gain insight and understanding of large amount of digital data. NetApp field engineers need a detailed procedure to extract the data from IBM's GPFS to NFS. We used NetApp XCP to migrate the data from GPFS to NFS so that GPUs can process the data. AI typically processes data from a network file system.

For more information about the high-performance computing to ONTAP NFS use case, a recorded demo, and test results, see the [Using XCP to Move Data from a Data Lake and High-Performance Computing to ONTAP NFS](#) blog.

For detailed steps on moving MapR-FS data into ONTAP NFS by using NetApp XCP, see Appendix A: GPFS to NFS—Detailed Steps in [TR-4732: Big Data Analytics Data to Artificial Intelligence](#).

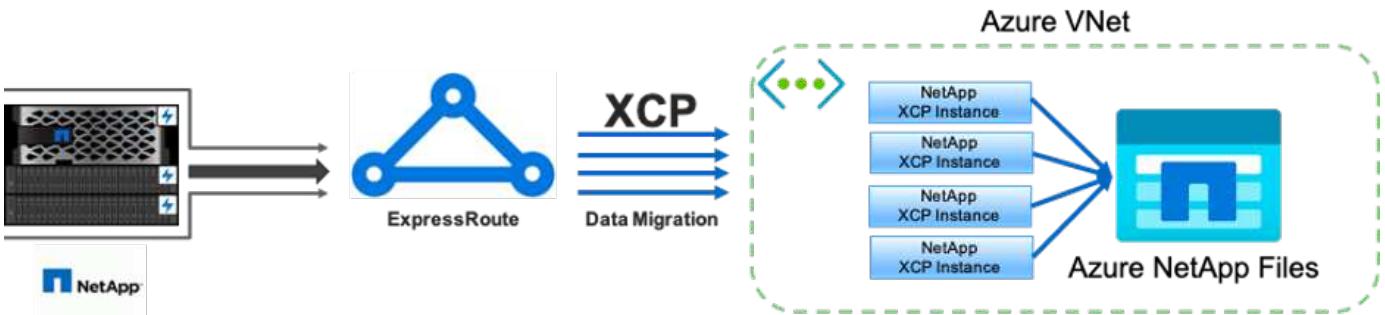
[Next: Using the XCP Data Mover to migrate millions of small files to flexible storage.](#)

[Using the XCP Data Mover to migrate millions of small files to flexible storage](#)

[Previous: High-performance computing to ONTAP NFS.](#)

This use case is based on the largest NetApp tourism industry customer for on-premises-to-cloud data migration. Because COVID-19 has reduced demand in the travel industry, customers want to save capital expenses on high-end storage in their on-premises environment for the demand pricing application. This customer has a tight SLA to migrate millions of small files to the cloud.

The following figure depicts data migration from on-premises to Azure NetApp Files for small files.



For more information, see the [NetApp XCP Data Mover Solution: On Premises to Cloud](#) blog.

[Next: Using the XCP Data Mover to migrate large files.](#)

#### Using the XCP Data Mover to migrate large files

[Previous: Using the XCP Data Mover to migrate millions of small files to flexible storage.](#)

This use case is based on a television network customer. The customer wanted to migrate Oracle Recovery Manager (RMAN) backup files to the cloud and run the Oracle E-Business Suite (EBS) application by using Azure NetApp Files with Pacemaker software. The customer also wanted to migrate their database backup files to on-demand cloud storage and transfer large files (in the range of 25GB to 50GB each) to Azure.

The following figure illustrates the data migration from on-premises to Azure NetApp Files for large files.

For more information, see the [NetApp XCP Data Mover Solution: On Premises to Cloud](#) blog.

[Next: Duplicate files.](#)

#### Duplicate files

[Previous: Using the XCP Data Mover to migrate large files.](#)

NetApp received a request to find duplicate files from a single volume or multiple volumes. NetApp provided the following solution.

For single volume, run the following commands:

```
[root@mastr-51 linux]# ./xcp -md5 -match 'type==f and nlinks==1 and size != 0' 10.63.150.213:/common_volume/nfsconnector_hw_cert/ | sort | uniq -cd --check-chars=32
XCP 1.5; (c) 2020 NetApp, Inc.; Licensed to Calin Salagean [NetApp Inc]
until Mon Dec 31 00:00:00 2029

176,380 scanned, 138,116 matched, 138,115 summed, 10 giants, 61.1 GiB in
(763 MiB/s), 172 MiB out (2.57 MiB/s), 1m5s

Filtered: 38264 did not match
176,380 scanned, 138,116 matched, 138,116 summed, 10 giants, 62.1 GiB in
(918 MiB/s), 174 MiB out (2.51 MiB/s), 1m9s.

    3 00004964ca155ecala71d0949c82e37e
nfsconnector_hw_cert/grid_01082017_174316/0/hadoopqe/accumulo/shell/pom.xml
    2 000103fbcd06d8071410c59047738389
nfsconnector_hw_cert/usr_hdp/2.5.3.0-37/hive2/doc/examples/files/dim-
data.txt
    2 000131053a46d67557d27bb678d5d4a1
nfsconnector_hw_cert/grid_01082017_174316/0/log/cluster/mahout_1/artifacts
/classifier/20news_reduceddata/20news-bydate-test/alt.atheism/53265
```

For multiple volumes, run the following commands:

```
[root@mastr-51 linux]# cat multiplevolume_duplicate.sh
#!/usr/bin/bash

#user input
JUNCTION_PATHS='/nc_volume1 /nc_volume2 /nc_volume3 /oplogarchivevolume'
NFS_DATA_LIF='10.63.150.213'

#xcp operation
for i in $JUNCTION_PATHS
do
echo "start - $i" >> /tmp/duplicate_results
/usr/src/xcp/linux/xcp -md5 -match 'type==f and nlinks==1 and size != 0' ${NFS_DATA_LIF}:$i | sort | uniq -cd --check-chars=32 | tee -a /tmp/duplicate_results
echo "end - $i" >> /tmp/duplicate_results
done

[root@mastr-51 linux]# nohup bash +x multiplevolume_duplicate.sh &
[root@mastr-51 linux]# cat /tmp/duplicate_results
```

[Next: Specific date-based scan and copy of data.](#)

#### Specific date-based scan and copy of data

[Previous: Duplicate files.](#)

This solution is based on a customer who needs to copy data based on a specific date. Verify the following details:

Created a file in Y: and checked the scan command to list them.

```
c:\XCP>dir Y:\karthik_test
Volume in drive Y is from
Volume Serial Number is 80F1-E201

Directory of Y:\karthik_test

05/26/2020  02:51 PM    <DIR>        .
05/26/2020  02:50 PM    <DIR>        ..
05/26/2020  02:51 PM            2,295 testfile.txt
                           1 File(s)       2,295 bytes
                           2 Dir(s)      658,747,392 bytes free
```

```
c:\XCP>
```

```
c:\XCP>xcp scan -match "strftime(ctime, '%Y-%m-%d') > '2020-05-01'" -fmt
'{} , {}'.format(iso(mtime), name) Y:\

XCP SMB 1.6; (c) 2020 NetApp, Inc.; Licensed to Calin Salagean [NetApp
Inc] until Mon Dec 31 00:00:00 2029
```

It appears that you are not running XCP as Administrator. To avoid access issues please run XCP as Administrator.

```
2020-05-26_14:51:13.132465,testfile.txt
2020-05-26_14:51:00.074216,karthik_test
```

```
xcp scan -match strftime(ctime, '%Y-%m-%d') > '2020-05-01' -fmt
'{} , {}'.format(iso(mtime), name) Y:\ : PASSED
30,205 scanned, 2 matched, 0 errors
Total Time : 4s
STATUS : PASSED
```

Copy the files based on date (2020 YearMay month first date) from Y: to Z:

```
c:\XCP>xcp copy -match "strftime(ctime, '%Y-%m-%d') > '2020-05-01'" Y:
Z:\dest_karthik
XCP SMB 1.6; (c) 2020 NetApp, Inc.; Licensed to Calin Salagean [NetApp
```

```
Inc] until Mon Dec 31 00:00:00 2029
```

It appears that you are not running XCP as Administrator. To avoid access issues please run XCP as Administrator.

```
30,205 scanned, 3 matched, 0 copied, 0 errors, 5s
xcp copy -match strftime(ctime, '%Y-%m-%d') > '2020-05-01' Y: Z:\dest_karthik
: PASSED
30,205 scanned, 3 matched, 2 copied, 0 errors
Total Time : 6s
STATUS : PASSED
```

```
c:\XCP>
```

Check the destination Z:

```
c:\XCP>dir Z:\dest_karthik\karthik_test
Volume in drive Z is to
Volume Serial Number is 80F1-E202

Directory of Z:\dest_karthik\karthik_test

05/26/2020  02:51 PM    <DIR> .
05/26/2020  02:50 PM    <DIR> ..
05/26/2020  02:51 PM           2,295 testfile.txt
                      1 File(s)        2,295 bytes
                      2 Dir(s)   659,316,736 bytes free
```

```
c:\XCP>
```

[Next: Creating a CSV file from SMB/CIFS share.](#)

**Creating a CSV file from SMB/CIFS share**

[Previous: Specific date-based scan and copy of data.](#)

The following command dumps data in the CSV format. You can sum up the size column to get the total size of the data.

```
xcp scan -match "((now-x.atime) / 3600) > 31*day" -fmt "'{}, {}, {}, {}'.
format(relpath, name, strftime(x.atime, '%y-%m-%d-%H:%M:%S'), humanize_size(size))" -preserve-atime >file.csv
```

The output should look similar to this example:

```
erase\report_av_fp_cdot_crosstab.csvreport_av_fp_cdot_crosstab.csv20-01-  
29-10:26:2449.6MiB
```

To scan up to the depth of three subdirectories and provide the result in sorting order, run the `xcp -du` command and dump the size at each directory level up to the depth of three subdirectories.

```
./xcp scan -du -depth 3 NFS_Server_IP:/source_vol
```

To sort, dump the information to a CSV file and sort the information.

```
xcp scan -match "type == d" -depth 3 -fmt "'{}, {}, {}, {}'.format(name,  
relpath, size)" NFS_Server_IP:/share > directory_report.csv
```

This is a custom report that uses the `-fmt` command. It scans all the directories and dumps the name of the directory, path, and size of directory into a CSV file. You can sort the size column from the spreadsheet application.

[Next: Data migration from 7-Mode to ONTAP.](#)

**Data migration from 7-Mode to ONTAP**

[Previous: Creating a CSV file from SMB/CIFS share.](#)

This section provides detailed steps for migrating data from NetApp Data ONTAP operating in 7-Mode to ONTAP.

### **Transitioning 7-Mode NFSv3 storage to ONTAP for NFS data**

This section provides the step-by-step procedure in the following table for transitioning a source 7-Mode NFSv3 export to an ONTAP system.

NetApp assumes that the source 7-Mode NFSv3 volume is exported and mounted on the client system and that XCP is already installed on a Linux system.

1. Verify that the target ONTAP system is healthy.

```

CLUSTER::> cluster show
Node          Health  Eligibility
-----
CLUSTER-01      true    true
CLUSTER-02      true    true
2 entries were displayed.

CLUSTER::> node show
Node      Health Eligibility Uptime      Model      Owner      Location
-----
CLUSTER-01
           true    true      78 days 21:01 FAS8060      RTP
CLUSTER-02
           true    true      78 days 20:50 FAS8060      RTP
2 entries were displayed.

CLUSTER::> storage failover show
                           Takeover
Node      Partner      Possible State Description
-----
CLUSTER-01  CLUSTER-02  true    Connected to CLUSTER-02
CLUSTER-02  CLUSTER-01  true    Connected to CLUSTER-01
2 entries were displayed.

```

2. Verify that at least one nonroot aggregate exists on the target system. The aggregate is normal.

```

CLUSTER::> storage aggregate show
Aggregate      Size Available Used% State    #Vols  Nodes          RAID
Status
-----
-----
aggr0        368.4GB   17.85GB   95% online       1 CLUSTER-01
raid_dp,
normal
aggr0_CLUSTER_02_0
            368.4GB   17.85GB   95% online       1 CLUSTER-02
raid_dp,
normal
source       1.23TB    1.10TB    11% online      6 CLUSTER-01
raid_dp,
normal
3 entries were displayed.

```

If there is no data aggregate, create a new one using the `storage aggr create` command.

3. Create a storage virtual machine (SVM) on the target cluster system.

```

CLUSTER::> vserver create -vserver dest -rootvolume dest_root -aggregate
poc -rootvolume-security-style mixed
[Job 647] Job succeeded:
Vserver creation completed
Verify the security style and language settings of the source

Verify that the SVM was successfully created.
CLUSTER::> vserver show -vserver dest
          Vserver: dest
          Vserver Type: data
          Vserver Subtype: default
          Vserver UUID: 91f6d786-0063-11e5-b114-
00a09853a969
          Root Volume: dest_root
          Aggregate: poc
          NIS Domain: -
          Root Volume Security Style: mixed
          LDAP Client: -
          Default Volume Language Code: C.UTF-8
          Snapshot Policy: default
          Comment:
          Quota Policy: default
          List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
          Vserver Admin State: running
          Vserver Operational State: running
          Vserver Operational State Stopped Reason: -
          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
          Disallowed Protocols: -
          Is Vserver with Infinite Volume: false
          QoS Policy Group: -
          Config Lock: false
          IPspace Name: Default

```

#### 4. Remove the FCP, iSCSI, NDMP, and CIDS protocols from the target SVM.

```

CLUSTER::> vserver remove-protocols -vserver dest -protocols
fcp,iscsi,ndmp,cifs

```

Verify that NFS is the allowed protocol for this SVM.

```
CLUSTER::> vserver show -vserver dest -fields allowed-protocols  
vserver allowed-protocols  
-----  
dest nfs
```

5. Create a new read-write data volume on the destination SVM. Verify that the security style, language settings, and capacity requirements match the source volume.

```
CLUSTER::> vol create -vserver dest -volume dest_nfs -aggregate poc  
-size 150g -type RW -state online -security-style mixed  
[Job 648] Job succeeded: Successful
```

6. Create a data LIF to serve NFS client requests.

```
CLUSTER::> network interface create -vserver dest -lif dest_lif -address  
10.61.73.115 -netmask 255.255.255.0 -role data -data-protocol nfs -home  
-node CLUSTER-01 -home-port e01
```

Verify that the LIF was successfully created.

```
CLUSTER::> network interface show -vserver dest  
Logical Status Network Current  
Current Is  
Vserver Interface Admin/Oper Address/Mask Node Port  
Home  
-----  
----  
dest  
dest_lif  
up/up 10.61.73.113/24 CLUSTER-01 e0i  
true
```

7. Create a static route with the SVM, if required.

```
CLUSTER::> network route create -vserver dest -destination 0.0.0.0/0  
-gateway 192.168.100.111
```

Verify that the route was successfully created.

```
CLUSTER::> network route show -vserver source
Vserver           Destination      Gateway        Metric
-----
dest              0.0.0.0/0       10.61.73.1    20
```

8. Mount the target NFS data volume in the SVM namespace.

```
CLUSTER::> volume mount -vserver dest -volume dest_nfs -junction-path
/des_nfs -active true
```

Verify that the volume is successfully mounted.

```
CLUSTER::> volume show -vserver dest -fields junction-path
vserver volume   junction-path
-----
dest      dest_nfs /dest_nfs
dest      dest_root
/
2 entries were displayed.
```

You can also specify volume mount options (junction path) with the `volume create` command.

9. Start the NFS service on the target SVM.

```
CLUSTER::> vserver nfs start -vserver dest
```

Verify that the service is started and running.

```
CLUSTER::> vserver nfs status
The NFS server is running on Vserver "dest".
CLUSTER::> nfs show
Vserver: dest
          General Access:  true
                      v3:  enabled
                      v4.0: disabled
                      4.1: disabled
                      UDP:  enabled
                      TCP:  enabled
          Default Windows User: -
          Default Windows Group: -
```

10. Verify that the default NFS export policy was applied to the target SVM.

```
CLUSTER::> vserver export-policy show -vserver dest
Vserver          Policy Name
-----
dest            default
```

11. If required, create a new custom export policy for the target SVM.

```
CLUSTER::> vserver export-policy create -vserver dest -policyname
xcpexportpolicy
```

Verify that the new custom export policy was successfully created.

```
CLUSTER::> vserver export-policy show -vserver dest
Vserver          Policy Name
-----
dest            default
dest            xcpexportpolicy
2 entries were displayed.
```

12. Modify the export policy rules to allow access to NFS clients.

```
CLUSTER::> export-policy rule modify -vserver dest -ruleindex 1
-policyname xcpexportpolicy -clientmatch 0.0.0.0/0 -rorule any -rwrule
any -anon 0
Verify the policy rules have modified
CLUSTER::> export-policy rule show -instance
                           Vserver: dest
                           Policy Name: xcpexportpolicy
                           Rule Index: 1
                           Access Protocol: nfs3
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                           RO Access Rule: none
                           RW Access Rule: none
User ID To Which Anonymous Users Are Mapped: 65534
                           Superuser Security Types: none
                           Honor SetUID Bits in SETATTR: true
                           Allow Creation of Devices: true
```

13. Verify that the client is allowed access to the volume.

```

CLUSTER::> export-policy check-access -vserver dest -volume dest_nfs
-client-ip 10.61.82.215 -authentication-method none -protocol nfs3
-access-type read-write

Path          Policy      Policy      Rule
Access        Policy      Owner       Owner Type   Index
-----        -----
-----        /
           xclexportpolicy
                   dest_root volume      1
read
/dest_nfs     xclexportpolicy
                   dest_nfs  volume      1
read-write
2 entries were displayed.

```

14. Connect to the Linux NFS server. Create a mount point for the NFS exported volume.

```
[root@localhost /]# cd /mnt
[root@localhost mnt]# mkdir dest
```

15. Mount the target NFSv3 exported volume at this mount point.



The NFSv3 volumes should be exported but not necessarily mounted by the NFS server. If they can be mounted, the XCP Linux host client mounts these volumes.

```
[root@localhost mnt]# mount -t nfs 10.61.73.115:/dest_nfs /mnt/dest
```

Verify that the mount point was successfully created.

```
[root@ localhost /]# mount | grep nfs
10.61.73.115:/dest_nfs on /mnt/dest type nfs
(rw,relatime,vers=3,rsize=65536,wsize=65536,namlen=255,proto=tcp,timeo=600,retrans=2,sec=sys,mountaddr=10.61.82.215,mountvers=3,mountport=4046,mountproto=udp,local_lock=none,addr=10.61.73.115)
```

16. Create a test file on the NFS exported mount point to enable read-write access.

```
[root@localhost dest]# touch test.txt  
Verify the file is created  
[root@localhost dest]# ls -l  
total 0  
-rw-r--r-- 1 root bin 0 Jun 2 03:16 test.txt
```



After the read-write test is complete, delete the file from the target NFS mount point.

17. Connect to the Linux client system in which XCP is installed. Browse to the XCP install path.

```
[root@localhost ~]# cd /linux/  
[root@localhost linux]#
```

18. Query the source 7-Mode NFSv3 exports by running the `xcp show` command on the XCP Linux client host system.

```
[root@localhost]#./xcp show 10.61.82.215  
== NFS Exports ==  
Mounts Errors Server  
        4      0 10.61.82.215  
Space   Files   Space   Files  
Free     Free    Used    Used Export  
23.7 GiB 778,134 356 KiB    96 10.61.82.215:/vol/nfsvol1  
17.5 GiB 622,463 1.46 GiB   117 10.61.82.215:/vol/nfsvol  
328 GiB   10.8M  2.86 GiB  7,904 10.61.82.215:/vol/vol0/home  
328 GiB   10.8M  2.86 GiB  7,904 10.61.82.215:/vol/vol0  
== Attributes of NFS Exports ==  
drwxr-xr-x --- root wheel 4KiB 4KiB 2d21h 10.61.82.215:/vol/nfsvol1  
drwxr-xr-x --- root wheel 4KiB 4KiB 2d21h 10.61.82.215:/vol/nfsvol  
drwxrwxrwx --t root wheel 4KiB 4KiB 9d22h 10.61.82.215:/vol/vol0/home  
drwxr-xr-x --- root wheel 4KiB 4KiB 4d0h 10.61.82.215:/vol/vol0  
3.89 KiB in (5.70 KiB/s), 7.96 KiB out (11.7 KiB/s), 0s.
```

19. Scan the source NFSv3 exported paths and print the statistics of their file structure.

NetApp recommends putting the source NFSv3 exports in read-only mode during `xcp scan`, `copy`, and `sync` operations.

```
[root@localhost /]# ./xcp scan 10.61.82.215:/vol/nfsvol
nfsvol
nfsvol/n5000-uk9.5.2.1.N1.1.bin
nfsvol/821_q_image.tgz
nfsvol/822RC2_q_image.tgz
nfsvol/NX5010_12_node_RCF_v1.3.txt
nfsvol/n5000-uk9-kickstart.5.2.1.N1.1.bin
nfsvol/NetApp_CN1610_1.1.0.5.stk
nfsvol/glibc-common-2.7-2.x86_64.rpm
nfsvol/glibc-2.7-2.x86_64.rpm
nfsvol/rhel-server-5.6-x86_64-dvd.iso.filepart
nfsvol/xcp
nfsvol/xcp_source
nfsvol/catalog
23 scanned, 7.79 KiB in (5.52 KiB/s), 1.51 KiB out (1.07 KiB/s), 1s.
```

20. Copy the source 7-Mode NFSv3 exports to NFSv3 exports on the target ONTAP system.

```
[root@localhost /]# ./xcp copy 10.61.82.215:/vol/nfsvol
10.61.73.115:/dest_nfs
44 scanned, 39 copied, 264 MiB in (51.9 MiB/s), 262 MiB out (51.5
MiB/s), 5s
44 scanned, 39 copied, 481 MiB in (43.3 MiB/s), 479 MiB out (43.4
MiB/s), 10s
44 scanned, 40 copied, 748 MiB in (51.2 MiB/s), 747 MiB out (51.3
MiB/s), 16s
44 scanned, 40 copied, 1.00 GiB in (55.9 MiB/s), 1.00 GiB out (55.9
MiB/s), 21s
44 scanned, 40 copied, 1.21 GiB in (42.8 MiB/s), 1.21 GiB out (42.8
MiB/s), 26s
Sending statistics...
44 scanned, 43 copied, 1.46 GiB in (47.6 MiB/s), 1.45 GiB out (47.6
MiB/s), 31s.
```

21. After the copy is finished, verify that the source and destination NFSv3 exports have identical data. Run the `xcp verify` command.

```
[root@localhost /]# ./xcp verify 10.61.82.215:/vol/nfsvol  
10.61.73.115:/dest_nfs  
44 scanned, 44 found, 28 compared, 27 same data, 2.41 GiB in (98.4  
MiB/s), 6.25 MiB out (255 KiB/s), 26s  
44 scanned, 44 found, 30 compared, 29 same data, 2.88 GiB in (96.4  
MiB/s), 7.46 MiB out (249 KiB/s), 31s  
44 scanned, 100% found (43 have data), 43 compared, 100% verified (data,  
attrs, mods), 2.90 GiB in (92.6 MiB/s), 7.53 MiB out (240 KiB/s), 32s.
```

If `xcp verify` finds differences between the source and destination data, then the error `no such file or directory` is reported in the summary. To fix that issue, run the `xcp sync` command to copy the source changes to the destination.

22. Before and during the cutover, run `verify` again. If the source has new or updated data, then perform incremental updates. Run the `xcp sync` command.

For this operation, the previous copy index name or number is required.

```
[root@localhost /]# ./xcp sync -id 3  
Index: {source: '10.61.82.215:/vol/nfsvol', target:  
'10.61.73.115:/dest_nfs1'}  
64 reviewed, 64 checked at source, 6 changes, 6 modifications, 51.7 KiB  
in (62.5 KiB/s), 22.7 KiB out (27.5 KiB/s), 0s.  
xcp: sync '3': Starting search pass for 1 modified directory...  
xcp: sync '3': Found 6 indexed files in the 1 changed directory  
xcp: sync '3': Rereading the 1 modified directory to find what's new...  
xcp: sync '3': Deep scanning the 1 directory that changed...  
11 scanned, 11 copied, 12.6KiB in (6.19KiBps), 9.50 KiB out (4.66KiBps),  
2s.
```

23. To resume a previously interrupted copy operation, run the `xcp resume` command.

```
[root@localhost /]# ./xcp resume -id 4
Index: {source: '10.61.82.215:/vol/nfsvol', target:
'10.61.73.115:/dest_nfs7'}
xcp: resume '4': WARNING: Incomplete index.
xcp: resume '4': Found 18 completed directories and 1 in progress
106 reviewed, 24.2 KiB in (30.3 KiB/s), 7.23 KiB out (9.06 KiB/s), 0s.
xcp: resume '4': Starting second pass for the in-progress directory...
xcp: resume '4': Found 3 indexed directories and 0 indexed files in the
1 in-progress directory
xcp: resume '4': In progress dirs: unindexed 1, indexed 0
xcp: resume '4': Resuming the 1 in-progress directory...
20 scanned, 7 copied, 205 MiB in (39.6 MiB/s), 205 MiB out (39.6
MiB/s), 5s
20 scanned, 14 copied, 425 MiB in (42.1 MiB/s), 423 MiB out (41.8
MiB/s), 11s
20 scanned, 14 copied, 540 MiB in (23.0 MiB/s), 538 MiB out (23.0
MiB/s), 16s
20 scanned, 14 copied, 721 MiB in (35.6 MiB/s), 720 MiB out (35.6
MiB/s), 21s
20 scanned, 15 copied, 835 MiB in (22.7 MiB/s), 833 MiB out (22.7
MiB/s), 26s
20 scanned, 16 copied, 1007 MiB in (34.3 MiB/s), 1005 MiB out (34.3
MiB/s), 31s
20 scanned, 17 copied, 1.15 GiB in (33.9 MiB/s), 1.15 GiB out (33.9
MiB/s), 36s
20 scanned, 17 copied, 1.27 GiB in (25.5 MiB/s), 1.27 GiB out (25.5
MiB/s), 41s
20 scanned, 17 copied, 1.45 GiB in (36.1 MiB/s), 1.45 GiB out (36.1
MiB/s), 46s
20 scanned, 17 copied, 1.69 GiB in (48.7 MiB/s), 1.69 GiB out (48.7
MiB/s), 51s
Sending statistics...
20 scanned, 20 copied, 21 indexed, 1.77 GiB in (33.5 MiB/s), 1.77 GiB
out (33.4 MiB/s), 54s.
```

After resume finishes copying files, run verify again so that the source and destination storage have identical data.

24. The NFSv3 client host needs to unmount the source NFSv3 exports provisioned from the 7-Mode storage and mounts the target NFSv3 exports from ONTAP. Cutover requires an outage.

### **Transitioning 7-Mode volume Snapshot copies to ONTAP**

This section covers the procedure for transitioning a source 7-Mode volume NetApp Snapshot copy to ONTAP.



NetApp assumes that the source 7-Mode volume is exported and mounted on the client system and that XCP is already installed on a Linux system. A Snapshot copy is a point-in-time image of a volume that records incremental changes since the last Snapshot copy. Use the `-snap` option with a 7-Mode system as the source.

**Warning:** Keep the base Snapshot copy. Do not delete the base Snapshot copy after the baseline copy is complete. The base Snapshot copy is required for further sync operations.

1. Verify that the target ONTAP system is healthy.

```
CLUSTER::> cluster show
Node          Health  Eligibility
-----
CLUSTER-01      true    true
CLUSTER-02      true    true
2 entries were displayed.

CLUSTER::> node show
Node      Health Eligibility Uptime      Model      Owner      Location
-----
CLUSTER-01
      true    true      78 days 21:01 FAS8060      RTP
CLUSTER-02
      true    true      78 days 20:50 FAS8060      RTP
2 entries were displayed.

CLUSTER::> storage failover show
                           Takeover
Node      Partner      Possible State Description
-----
CLUSTER-01    CLUSTER-02    true    Connected to CLUSTER-02
CLUSTER-02    CLUSTER-01    true    Connected to CLUSTER-01
2 entries were displayed.
```

2. Verify that at least one nonroot aggregate exists on the target system. The aggregate is normal.

```

CLUSTER::> storage aggregate show
Aggregate      Size Available Used% State    #Vols  Nodes          RAID
Status
-----
-----
aggr0        368.4GB   17.85GB   95% online       1 CLUSTER-01
raid_dp,
normal
aggr0_CLUSTER_02_0
            368.4GB   17.85GB   95% online       1 CLUSTER-02
raid_dp,
normal
source       1.23TB    1.10TB    11% online      6 CLUSTER-01
raid_dp,
normal
3 entries were displayed.

```

If there is no data aggregate, create a new one using the `storage aggr create` command.

3. Create an SVM on the target cluster system.

```

CLUSTER::> vserver create -vserver dest -rootvolume dest_root -aggregate
poc -rootvolume-security-style mixed
[Job 647] Job succeeded:
Vserver creation completed
Verify the security style and language settings of the source

Verify that the SVM was successfully created.
CLUSTER::> vserver show -vserver dest
          Vserver: dest
          Vserver Type: data
          Vserver Subtype: default
          Vserver UUID: 91f6d786-0063-11e5-b114-
00a09853a969
          Root Volume: dest_root
          Aggregate: poc
          NIS Domain: -
          Root Volume Security Style: mixed
          LDAP Client: -
          Default Volume Language Code: C.UTF-8
          Snapshot Policy: default
          Comment:
          Quota Policy: default
          List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
          Vserver Admin State: running
          Vserver Operational State: running
          Vserver Operational State Stopped Reason: -
          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
          Disallowed Protocols: -
          Is Vserver with Infinite Volume: false
          QoS Policy Group: -
          Config Lock: false
          IPspace Name: Default

```

#### 4. Remove the FCP, iSCSI, NDMP, and CIFS protocols from the target SVM.

```

CLUSTER::> vserver remove-protocols -vserver dest -protocols
fcp,iscsi,ndmp,cifs
Verify that NFS is the allowed protocol for this SVM.
CLUSTER::> vserver show -vserver dest -fields allowed-protocols
vserver allowed-protocols
-----
dest      nfs

```

5. Create a new read-write data volume on the destination SVM. Verify that the security style, language settings, and capacity requirements match the source volume.

```
CLUSTER::> vol create -vserver dest -volume dest_nfs -aggregate poc  
-size 150g -type RW -state online -security-style mixed  
[Job 648] Job succeeded: Successful
```

6. Create a data LIF to serve NFS client requests.

```
CLUSTER::> network interface create -vserver dest -lif dest_lif -address  
10.61.73.115 -netmask 255.255.255.0 -role data -data-protocol nfs -home  
-node CLUSTER-01 -home-port e01
```

Verify that the LIF was successfully created.

```
CLUSTER::> network interface show -vserver dest  
Logical Status Network Current  
Current Is  
Vserver Interface Admin/Oper Address/Mask Node Port  
Home  
-----  
dest dest_lif up/up 10.61.73.113/24 CLUSTER-01 e0i  
true
```

7. If required, create a static route with the SVM.

```
CLUSTER::> network route create -vserver dest -destination 0.0.0.0/0  
-gateway 192.168.100.111
```

Verify that the route was successfully created.

```
CLUSTER::> network route show -vserver source  
Vserver Destination Gateway Metric  
-----  
dest 0.0.0.0/0 10.61.73.1 20
```

8. Mount the target NFS data volume in the SVM namespace.

```
CLUSTER::> volume mount -vserver dest -volume dest_nfs -junction-path  
/dest_nfs -active true
```

Verify that the volume was successfully mounted.

```
CLUSTER::> volume show -vserver dest -fields junction-path  
vserver volume junction-path  
-----  
dest      dest_nfs /dest_nfs  
dest      dest_root  
          /  
2 entries were displayed.
```

You can also specify the volume mount options (junction path) with the `volume create` command.

#### 9. Start the NFS service on the target SVM.

```
CLUSTER::> vserver nfs start -vserver dest
```

Verify that the service is started and running.

```
CLUSTER::> vserver nfs status  
The NFS server is running on Vserver "dest".  
CLUSTER::> nfs show  
Vserver: dest  
    General Access:  true  
                  v3:  enabled  
                  v4.0: disabled  
                  4.1:  disabled  
                  UDP:  enabled  
                  TCP:  enabled  
    Default Windows User: -  
    Default Windows Group: -
```

#### 10. Verify that the default NFS export policy is applied to the target SVM.

```
CLUSTER::> vserver export-policy show -vserver dest  
Vserver          Policy Name  
-----  
dest            default
```

11. If required, create a new custom export policy for the target SVM.

```
CLUSTER::> vserver export-policy create -vserver dest -policynname  
xcpexportpolicy
```

Verify that the new custom export policy was successfully created.

```
CLUSTER::> vserver export-policy show -vserver dest  
Vserver          Policy Name  
-----  
dest            default  
dest            xcpexportpolicy  
2 entries were displayed.
```

12. Modify the export policy rules to allow access to NFS clients on the target system.

```
CLUSTER::> export-policy rule modify -vserver dest -ruleindex 1  
-policynname xcpexportpolicy -clientmatch 0.0.0.0/0 -rorule any -rwrule  
any -anon 0  
Verify the policy rules have modified  
CLUSTER::> export-policy rule show -instance  
          Vserver: dest  
          Policy Name: xcpexportpolicy  
          Rule Index: 1  
          Access Protocol: nfs3  
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0  
          RO Access Rule: none  
          RW Access Rule: none  
User ID To Which Anonymous Users Are Mapped: 65534  
          Superuser Security Types: none  
          Honor SetUID Bits in SETATTR: true  
          Allow Creation of Devices: true
```

13. Verify that the client has access to the target volume.

```

CLUSTER::> export-policy check-access -vserver dest -volume dest_nfs
-client-ip 10.61.82.215 -authentication-method none -protocol nfs3
-access-type read-write

Path          Policy      Policy      Rule
Access        Policy      Owner       Owner Type   Index
-----        -----      -----      -----
-----        -----      -----      -----
/           xclexportpolicy
                  dest_root volume      1
read
/dest_nfs     xclexportpolicy
                  dest_nfs  volume      1
read-write
2 entries were displayed.

```

14. Connect to the Linux NFS server. Create a mount point for the NFS exported volume.

```

[root@localhost /]# cd /mnt
[root@localhost mnt]# mkdir dest

```

15. Mount the target NFSv3 exported volume at this mount point.



The NFSv3 volumes should be exported but not necessarily mounted by the NFS server. If they can be mounted, the XCP Linux host client mounts these volumes.

```
[root@localhost mnt]# mount -t nfs 10.61.73.115:/dest_nfs /mnt/dest
```

Verify that the mount point was successfully created.

```

[root@localhost /]# mount | grep nfs
10.61.73.115:/dest_nfs on /mnt/dest type nfs

```

16. Create a test file on the NFS exported mount point to enable read-write access.

```

[root@localhost dest]# touch test.txt
Verify the file is created
[root@localhost dest]# ls -l
total 0
-rw-r--r-- 1 root bin 0 Jun  2 03:16 test.txt

```



After the read-write test is complete, delete the file from the target NFS mount point.

17. Connect to the Linux client system in which XCP is installed. Browse to the XCP install path.

```
[root@localhost ~]# cd /linux/  
[root@localhost linux]#
```

18. Query the source 7-Mode NFSv3 exports by running the `xcp show` command on the XCP Linux client host system.

```
[root@localhost]#./xcp show 10.61.82.215  
== NFS Exports ==  
Mounts Errors Server  
    4      0  10.61.82.215  
Space   Files     Space   Files  
Free     Free     Used     Used Export  
23.7 GiB 778,134  356 KiB    96 10.61.82.215:/vol/nfsvol1  
17.5 GiB 622,463  1.46 GiB   117 10.61.82.215:/vol/nfsvol  
  328 GiB   10.8M  2.86 GiB  7,904 10.61.82.215:/vol/vol0/home  
  328 GiB   10.8M  2.86 GiB  7,904 10.61.82.215:/vol/vol0  
== Attributes of NFS Exports ==  
drwxr-xr-x --- root wheel 4KiB 4KiB 2d21h 10.61.82.215:/vol/nfsvol1  
drwxr-xr-x --- root wheel 4KiB 4KiB 2d21h 10.61.82.215:/vol/nfsvol  
drwxrwxrwx --t root wheel 4KiB 4KiB 9d22h 10.61.82.215:/vol/vol0/home  
drwxr-xr-x --- root wheel 4KiB 4KiB 4d0h 10.61.82.215:/vol/vol0  
  3.89 KiB in (5.70 KiB/s), 7.96 KiB out (11.7 KiB/s), 0s.
```

19. Scan the source NFSv3 exported paths and print the statistics of their file structure.

NetApp recommends putting the source NFSv3 exports in read-only mode during `xcp scan`, `copy`, and `sync` operations. In `sync` operation, you must pass the `-snap` option with a corresponding value.

```
[root@localhost /]# ./xcp scan 10.61.82.215:/vol/nfsvol/.snapshot/snap1
nfsvol
nfsvol/n5000-uk9.5.2.1.N1.1.bin
nfsvol/821_q_image.tgz
nfsvol/822RC2_q_image.tgz
nfsvol/NX5010_12_node_RCF_v1.3.txt
nfsvol/n5000-uk9-kickstart.5.2.1.N1.1.bin
nfsvol/catalog
23 scanned, 7.79 KiB in (5.52 KiB/s), 1.51 KiB out (1.07 KiB/s), 1s.
[root@scspr1202780001 vol_acl4]# ./xcp sync -id 7msnap1 -snap
10.236.66.199:/vol/nfsvol/.snapshot/snap10
(show scan and sync)
```

20. Copy the source 7-Mode NFSv3 snapshot (base) to NFSv3 exports on the target ONTAP system.

```
[root@localhost /]# /xcp copy 10.61.82.215:/vol/nfsvol/.snapshot/snap1
10.61.73.115:/dest_nfs
44 scanned, 39 copied, 264 MiB in (51.9 MiB/s), 262 MiB out (51.5
MiB/s), 5s
44 scanned, 39 copied, 481 MiB in (43.3 MiB/s), 479 MiB out (43.4
MiB/s), 10s
44 scanned, 40 copied, 748 MiB in (51.2 MiB/s), 747 MiB out (51.3
MiB/s), 16s
44 scanned, 40 copied, 1.00 GiB in (55.9 MiB/s), 1.00 GiB out (55.9
MiB/s), 21s
44 scanned, 40 copied, 1.21 GiB in (42.8 MiB/s), 1.21 GiB out (42.8
MiB/s), 26s
Sending statistics...
44 scanned, 43 copied, 1.46 GiB in (47.6 MiB/s), 1.45 GiB out (47.6
MiB/s), 31s.
```



Keep this base snapshot for further sync operations.

21. After copy is complete, verify that the source and destination NFSv3 exports have identical data. Run the **xcp verify** command.

```
[root@localhost /]# ./xcp verify 10.61.82.215:/vol/nfsvol  
10.61.73.115:/dest_nfs  
44 scanned, 44 found, 28 compared, 27 same data, 2.41 GiB in (98.4  
MiB/s), 6.25 MiB out (255 KiB/s), 26s  
44 scanned, 44 found, 30 compared, 29 same data, 2.88 GiB in (96.4  
MiB/s), 7.46 MiB out (249 KiB/s), 31s  
44 scanned, 100% found (43 have data), 43 compared, 100% verified (data,  
attrs, mods), 2.90 GiB in (92.6 MiB/s), 7.53 MiB out (240 KiB/s), 32s.
```

If verify finds differences between the source and destination data, then the error no such file or directory is reported in the summary. To fix that issue, run the `xcp sync command to copy the source changes to the destination.

22. Before and during the cutover, run verify again. If the source has new or updated data, then perform incremental updates. If there are incremental changes, create a new Snapshot copy for these changes and pass that snapshot path with the -snap option for sync operations.

Run the xcp sync command with the -snap option and snapshot path.

```
[root@localhost /]# ./xcp sync -id 3  
Index: {source: '10.61.82.215:/vol/nfsvol/.snapshot/snap1', target:  
'10.61.73.115:/dest_nfs1'}  
64 reviewed, 64 checked at source, 6 changes, 6 modifications, 51.7 KiB  
in (62.5  
KiB/s), 22.7 KiB out (27.5 KiB/s), 0s.  
xcp: sync '3': Starting search pass for 1 modified directory...  
xcp: sync '3': Found 6 indexed files in the 1 changed directory  
xcp: sync '3': Rereading the 1 modified directory to find what's new...  
xcp: sync '3': Deep scanning the 1 directory that changed...  
11 scanned, 11 copied, 12.6 KiB in (6.19 KiB/s), 9.50 KiB out (4.66  
KiB/s), 2s..
```



For this operation, the base snapshot is required.

23. To resume a previously interrupted copy operation, run the xcp resume command.

```
[root@scspr1202780001 534h_dest_vol]# ./xcp resume -id 3
XCP <version>; (c) 2020 NetApp, Inc.; Licensed to xxxxx [NetApp Inc]
until Mon Dec 31 00:00:00 2029
xcp: Index: {source: '10.61.82.215:/vol/nfsvol',/.snapshot/snap1,
target: 10.237.160.55:/dest_vol}
xcp: resume '7msnap_res1': Reviewing the incomplete index...
xcp: diff '7msnap_res1': Found 143 completed directories and 230 in
progress
39,688 reviewed, 1.28 MiB in (1.84 MiB/s), 13.3 KiB out (19.1 KiB/s),
0s.
xcp: resume '7msnap_res1': Starting second pass for the in-progress
directories...
xcp: resume '7msnap_res1': Resuming the in-progress directories...
xcp: resume '7msnap_res1': Resumed command: copy {-newid:
u'7msnap_res1'}
xcp: resume '7msnap_res1': Current options: {-id: '7msnap_res1'}
xcp: resume '7msnap_res1': Merged options: {-id: '7msnap_res1', -newid:
u'7msnap_res1'}
xcp: resume '7msnap_res1': Values marked with a * include operations
before resume
68,848 scanned*, 54,651 copied*, 39,688 indexed*, 35.6 MiB in (7.04
MiB/s), 28.1 MiB out (5.57 MiB/s), 5s
```

24. The NFSv3 client host must unmount the source NFSv3 exports provisioned from the 7-Mode storage and mount the target NFSv3 exports from ONTAP. This cutover requires an outage.

## Migrating ACLv4 from NetApp 7-Mode to a NetApp storage system

This section covers the step-by-step procedure for transitioning a source NFSv4 export to an ONTAP system.

 NetApp assumes that the source NFSv4 volume is exported and mounted on the client system and that XCP is already installed on a Linux system. The source should be a NetApp 7-Mode system that support ACLs. ACL migration is supported from NetApp to NetApp only. To copy files with a special character in the name, make sure the source and destination support UTF- 8 encoded language.

### Prerequisites for migrating a source NFSv4 export to ONTAP

Before you migrate a source NFSv4 export to ONTAP, the following prerequisites must be met:

- The destination system must have NFSv4 configured.
- The NFSv4 source and target must be mounted on the XCP host. Select NFS v4.0 to match the source and target storage and verify that the ACLs are enabled on the source and target system.
- XCP requires the source/target path to be mounted on the XCP host for ACL processing.In the following example, vol1(10.63.5.56:/vol1) is mounted on the /mnt/vol1 path:

```
[root@localhost ~]# df -h
Filesystem                                Size  Used
Avail Use% Mounted on
10.63.5.56:/vol1                           973M  4.2M
969M   1% /mnt/vol1

[root@localhost ~]# ./xcp scan -l -acl4 10.63.5.56:/vol1/
XCP <version>; (c) 2020 NetApp, Inc.; Licensed to XXX [NetApp Inc] until
Sun Mar 31 00:00:00 2029
drwxr-xr-x --- root root 4KiB 4KiB 23h42m vol1
rw-r--r-- --- root root    4      0 23h42m vol1/DIR1/FILE
drwxr-xr-x --- root root 4KiB 4KiB 23h42m vol1/DIR1/DIR11
drwxr-xr-x --- root root 4KiB 4KiB 23h42m vol1/DIR1
rw-r--r-- --- root root    4      0 23h42m vol1/DIR1/DIR11/FILE
drwxr-xr-x --- root root 4KiB 4KiB 23h42m vol1/DIR1/DIR11/DIR2
rw-r--r-- --- root root    4      0 23h42m vol1/DIR1/DIR11/DIR2/FILE
drwxr-xr-x --- root root 4KiB 4KiB 17m43s vol1/DIR1/DIR11/DIR2/DIR22
8 scanned, 8 getacls, 1 v3perm, 7 acls, 3.80 KiB in (3.86 KiB/s), 1.21 KiB
out (1.23 KiB/s), 0s.
```

## Subdirectories options

The two options to work with subdirectories are as follows:

- For XCP to work on a subdirectory (/vol1/DIR1/DIR11), mount the complete path (10.63.5.56:/vol1/DIR1/DIR11) on the XCP host.

If the complete path is not mounted, XCP reports the following error:

```
[root@localhost ~]# ./xcp scan -l -acl4 10.63.5.56:/vol1/DIR1/DIR11
XCP <version>; (c) 2020 NetApp, Inc.; Licensed to XXX [NetApp Inc] until
Sun Mar 31 00:00:00 2029
xcp: ERROR: For xcp to process ACLs, please mount
10.63.5.56:/vol1/DIR1/DIR11 using the OS nfs4 client.
```

- Use the subdirectory syntax (mount: subdirectory/qtree/.snapshot), as shown in the example below:

```
[root@localhost ~]# ./xcp scan -l -acl4 10.63.5.56:/vol11:/DIR1/DIR11
XCP <version>; (c) 2020 NetApp, Inc.; Licensed to XXX [NetApp Inc] until
Sun Mar 31 00:00:00 2029
drwxr-xr-x --- root root 4KiB 4KiB 23h51m DIR11
rw-r--r-- --- root root 4 0 23h51m DIR11/DIR2/FILE
drwxr-xr-x --- root root 4KiB 4KiB 26m9s DIR11/DIR2/DIR22
rw-r--r-- --- root root 4 0 23h51m DIR11/FILE
drwxr-xr-x --- root root 4KiB 4KiB 23h51m DIR11/DIR2
5 scanned, 5 getacls, 5 accls, 2.04 KiB in (3.22 KiB/s), 540 out (850/s),
0s.
```

Complete the following steps to migrate ACLv4 from NetApp 7-Mode to a NetApp storage system.

1. Verify that the target ONTAP system is healthy.

```
CLUSTER::> cluster show
Node          Health  Eligibility
-----
CLUSTER-01      true    true
CLUSTER-02      true    true
2 entries were displayed.

CLUSTER::> node show
Node      Health Eligibility Uptime      Model      Owner      Location
-----
CLUSTER-01
          true    true      78 days 21:01 FAS8060      RTP
CLUSTER-02
          true    true      78 days 20:50 FAS8060      RTP
2 entries were displayed.

CLUSTER::> storage failover show
                           Takeover
Node      Partner      Possible State Description
-----
CLUSTER-01  CLUSTER-02  true    Connected to CLUSTER-02
CLUSTER-02  CLUSTER-01  true    Connected to CLUSTER-01
2 entries were displayed.
```

2. Verify that at least one nonroot aggregate exists on the target system. The aggregate is normal.

```

CLUSTER::> storage aggregate show
Aggregate      Size Available Used% State    #Vols  Nodes          RAID
Status
-----
-----
aggr0        368.4GB   17.85GB   95% online       1 CLUSTER-01
raid_dp,
normal
aggr0_CLUSTER_02_0
            368.4GB   17.85GB   95% online       1 CLUSTER-02
raid_dp,
normal
source       1.23TB    1.10TB    11% online      6 CLUSTER-01
raid_dp,
normal
3 entries were displayed.

```

If there is no data aggregate, create a new one using the `storage aggr create` command.

### 3. Create an SVM on the target cluster system.

```

CLUSTER::> vserver create -vserver dest -rootvolume dest_root -aggregate
poc -rootvolume-security-style mixed
[Job 647] Job succeeded:
Vserver creation completed
Verify the security style and language settings of the source

```

Verify that the SVM was successfully created.

```

CLUSTER::> vserver show -vserver dest
              Vserver: dest
              Vserver Type: data
              Vserver Subtype: default
              Vserver UUID: 91f6d786-0063-11e5-b114-
00a09853a969
              Root Volume: dest_root
              Aggregate: poc
              NIS Domain: -
              Root Volume Security Style: mixed
              LDAP Client: -
              Default Volume Language Code: C.UTF-8
              Snapshot Policy: default
              Comment:
              Quota Policy: default
              List of Aggregates Assigned: -
              Limit on Maximum Number of Volumes allowed: unlimited
              Vserver Admin State: running
              Vserver Operational State: running
              Vserver Operational State Stopped Reason: -
              Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
              Disallowed Protocols: -
              Is Vserver with Infinite Volume: false
              QoS Policy Group: -
              Config Lock: false
              IPspace Name: Default

```

4. Remove the FCP, iSCSI, NDMP, and CIFS protocols from the target SVM.

```

CLUSTER::> vserver remove-protocols -vserver dest -protocols
fcp,iscsi,ndmp,cifs

```

Verify that NFS is the allowed protocol for this SVM.

```

CLUSTER::> vserver show -vserver dest -fields allowed-protocols
vserver allowed-protocols
-----
dest      nfs

```

5. Create a new read-write data volume on the destination SVM. Verify that the security style, language settings, and capacity requirements match the source volume.

```
CLUSTER::> vol create -vserver dest -volume dest_nfs -aggregate poc  
-size 150g -type RW -state online -security-style mixed  
[Job 648] Job succeeded: Successful
```

6. Create a data LIF to serve NFS client requests.

```
CLUSTER::> network interface create -vserver dest -lif dest_lif -address  
10.61.73.115 -netmask 255.255.255.0 -role data -data-protocol nfs -home  
-node CLUSTER-01 -home-port e01
```

Verify that the LIF was successfully created.

```
CLUSTER::> network interface show -vserver dest  
Logical Status Network Current  
Current Is  
Vserver Interface Admin/Oper Address/Mask Node Port  
Home  
-----  
----  
dest  
dest_lif  
up/up 10.61.73.113/24 CLUSTER-01 e0i  
true
```

7. If required, create a static route with the SVM.

```
CLUSTER::> network route create -vserver dest -destination 0.0.0.0/0  
-gateway 192.168.100.111
```

Verify that the route was successfully created.

```
CLUSTER::> network route show -vserver source  
Vserver Destination Gateway Metric  
-----  
dest 0.0.0.0/0 10.61.73.1 20
```

8. Mount the target NFS data volume in the SVM namespace.

```
CLUSTER::> volume mount -vserver dest -volume dest_nfs -junction-path  
/dest_nfs -active true
```

Verify that the volume was successfully mounted.

```
CLUSTER::> volume show -vserver dest -fields junction-path  
vserver volume junction-path  
-----  
dest      dest_nfs /dest_nfs  
dest      dest_root  
          /  
2 entries were displayed.
```

You can also specify the volume mount options (junction path) with the `volume create` command.

#### 9. Start the NFS service on the target SVM.

```
CLUSTER::> vserver nfs start -vserver dest
```

Verify that the service is started and running.

```
CLUSTER::> vserver nfs status  
The NFS server is running on Vserver "dest".  
CLUSTER::> nfs show  
Vserver: dest  
    General Access:  true  
                  v3:  enabled  
                  v4.0:  enabled  
                  4.1:  disabled  
                  UDP:  enabled  
                  TCP:  enabled  
    Default Windows User:  -  
    Default Windows Group:  -
```

#### 10. Check that the default NFS export policy is applied to the target SVM.

```
CLUSTER::> vserver export-policy show -vserver dest  
Vserver          Policy Name  
-----  
dest            default
```

11. If required, create a new custom export policy for the target SVM.

```
CLUSTER::> vserver export-policy create -vserver dest -policynname  
xcpexportpolicy
```

Verify that the new custom export policy was successfully created.

```
CLUSTER::> vserver export-policy show -vserver dest  
Vserver          Policy Name  
-----  
dest            default  
dest            xcpexportpolicy  
2 entries were displayed.
```

12. Modify the export policy rules to allow access to NFS clients.

```
CLUSTER::> export-policy rule modify -vserver dest -ruleindex 1  
-policynname xcpexportpolicy -clientmatch 0.0.0.0/0 -rorule any -rwrule  
any -anon 0
```

Verify that the policy rules have been modified.

```
CLUSTER::> export-policy rule show -instance  
          Vserver: dest  
          Policy Name: xcpexportpolicy  
          Rule Index: 1  
          Access Protocol: nfs3  
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0  
          RO Access Rule: none  
          RW Access Rule: none  
User ID To Which Anonymous Users Are Mapped: 65534  
          Superuser Security Types: none  
          Honor SetUID Bits in SETATTR: true  
          Allow Creation of Devices: true
```

13. Verify that the client is allowed access to the volume.

```

CLUSTER::> export-policy check-access -vserver dest -volume dest_nfs
-client-ip 10.61.82.215 -authentication-method none -protocol nfs3
-access-type read-write

Path          Policy      Policy      Rule
Access        Policy      Owner       Owner Type  Index
-----  -----
-----  -----
/           xclexportpolicy      dest_root volume      1
read
/dest_nfs    xclexportpolicy      dest_nfs   volume      1
read-write
2 entries were displayed.

```

14. Connect to the Linux NFS server. Create a mount point for the NFS exported volume.

```
[root@localhost /]# cd /mnt
[root@localhost mnt]# mkdir dest
```

15. Mount the target NFSv4 exported volume at this mount point.



The NFSv4 volumes should be exported but not necessarily mounted by the NFS server. If they can be mounted, the XCP Linux host client mounts these volumes.

```
[root@localhost mnt]# mount -t nfs4 10.63.5.56:/vol1 /mnt/vol1
```

Verify that the mount point was successfully created.

```
[root@localhost mnt]# mount | grep nfs
10.63.5.56:/vol1 on /mnt/vol1 type nfs4
(rw,relatime,vers=4.0,rsize=65536,wsize=65536,namlen=255,hard,proto=tcp,
timeo=600,
retrans=2,sec=sys,clientaddr=10.234.152.84,local_lock=none,addr=10.63.5.
56)
```

16. Create a test file on the NFS exported mount point to enable read-write access.

```
[root@localhost dest]# touch test.txt
```

Verify the file is created.

```
[root@localhost dest]# ls -l  
total 0  
-rw-r--r-- 1 root bin 0 Jun 2 03:16 test.txt
```



After the read-write test is complete, delete the file from the target NFS mount point.

17. Connect to the Linux client system in which XCP is installed. Browse to the XCP install path.

```
[root@localhost ~]# cd /linux/  
[root@localhost linux]#
```

18. Query the source NFSv4 exports by running the `xcp show` command on the XCP Linux client host system.

```

root@localhost]# ./xcp show 10.63.5.56
XCP <version>; (c) 2020 NetApp, Inc.; Licensed to xxx [NetApp Inc] until
Mon Dec 31 00:00:00 2029
getting pmap dump from 10.63.5.56 port 111...
getting export list from 10.63.5.56...
sending 6 mounts and 24 nfs requests to 10.63.5.56...
== RPC Services ==
'10.63.5.56': UDP rpc services: MNT v1/2/3, NFS v3, NLM v4, PMAP v2/3/4,
STATUS v1
'10.63.5.56': TCP rpc services: MNT v1/2/3, NFS v3/4, NLM v4, PMAP
v2/3/4, STATUS v1
== NFS Exports ==
Mounts Errors Server
      6        0 10.63.5.56
      Space    Files     Space    Files
      Free     Free     Used     Used Export
94.7 MiB  19,883   324 KiB    107 10.63.5.56:/
  971 MiB  31,023   2.19 MiB    99 10.63.5.56:/vol2
  970 MiB  31,024   2.83 MiB    98 10.63.5.56:/vol1
  9.33 GiB 310,697   172 MiB   590 10.63.5.56:/vol_005
  43.3 GiB   1.10M   4.17 GiB   1.00M 10.63.5.56:/vol3
  36.4 GiB   1.10M   11.1 GiB   1.00M 10.63.5.56:/vol4
== Attributes of NFS Exports ==
drwxr-xr-x --- root root 4KiB 4KiB 6d2h 10.63.5.56:/
drwxr-xr-x --- root root 4KiB 4KiB 3d2h 10.63.5.56:/vol2
drwxr-xr-x --- root root 4KiB 4KiB 3d2h 10.63.5.56:/vol1
drwxr-xr-x --- root root 4KiB 4KiB 9d2h 10.63.5.56:/vol_005
drwxr-xr-x --- root root 4KiB 4KiB 9d4h 10.63.5.56:/vol3
drwxr-xr-x --- root root 4KiB 4KiB 9d4h 10.63.5.56:/vol4
  6.09 KiB in (9.19 KiB/s), 12.2 KiB out (18.3 KiB/s), 0s.

```

#### 19. Scan the source NFSv4 exported paths and print the statistics of their file structure.

NetApp recommends putting the source NFSv4 exports in read-only mode during `xcp scan`, `copy`, and `sync` operations.

```

[root@localhost]# ./xcp scan -acl4 10.63.5.56:/vol1
XCP <version>; (c) 2020 NetApp, Inc.; Licensed to xxx [NetApp Inc] until
Mon Dec 31 00:00:00 2029
vol1
vol1/test/f1
vol1/test
3 scanned, 3 getacls, 3 v3perms, 1.59 KiB in (1.72 KiB/s), 696 out
(753/s), 0s.

```

20. Copy source NFSv4 exports to NFSv4 exports on the target ONTAP system.

```
[root@localhost]# ./xcp copy -acl4 -newid id1 10.63.5.56:/vol1  
10.63.5.56:/vol2  
XCP <version>; (c) 2020 NetApp, Inc.; Licensed to xxx [NetApp Inc] until  
Mon Dec 31 00:00:00 2029  
3 scanned, 2 copied, 3 indexed, 3 getacls, 3 v3perms, 1 setacl, 14.7 KiB  
in (11.7 KiB/s), 61 KiB out (48.4 KiB/s), 1s..
```

21. After `copy` is complete, verify that the source and destination NFSv4 exports have identical data. Run the `xcp verify` command.

```
[root@localhost]# ./xcp verify -acl4 -noid 10.63.5.56:/vol1  
10.63.5.56:/vol2  
XCP <version>; (c) 2020 NetApp, Inc.; Licensed to xxx [NetApp Inc] until  
Mon Dec 31 00:00:00 2029  
3 scanned, 100% found (0 have data), 100% verified (data, attrs, mods,  
acls), 6 getacls, 6 v3perms, 2.90 KiB in (4.16 KiB/s), 2.94 KiB out  
(4.22 KiB/s), 0s.
```

If `verify` finds differences between the source and destination data, then the error `no such file or directory` is reported in the summary. To fix that issue, run the `xcp sync` command to copy the source changes to the destination.

22. Before and during the cutover, run `verify` again. If the source has new or updated data, then perform incremental updates. Run the `xcp sync` command.

```
[root@ root@localhost]# ./xcp sync -id id1  
XCP <version>; (c) 2020 NetApp, Inc.; Licensed to xxx [NetApp Inc] until  
Mon Dec 31 00:00:00 2029  
xcp: Index: {source: 10.63.5.56:/vol1, target: 10.63.5.56:/vol2}  
3 reviewed, 3 checked at source, no changes, 3 reindexed, 25.6 KiB in  
(32.3 KiB/s), 23.3 KiB out (29.5 KiB/s), 0s.
```



For this operation, the previous copy index name or number is required.

23. To resume a previously interrupted `copy` operation, run the `xcp resume` command.

```
[root@localhost]# ./xcp resume -id id1
XCP <version>; (c) 2020 NetApp, Inc.; Licensed to xxx [NetApp Inc] until
Mon Dec 31 00:00:00 2029
xcp: Index: {source: 10.63.5.56:/vol3, target: 10.63.5.56:/vol4}
xcp: resume 'id1': Reviewing the incomplete index...
xcp: diff 'id1': Found 0 completed directories and 8 in progress
39,899 reviewed, 1.64 MiB in (1.03 MiB/s), 14.6 KiB out (9.23 KiB/s),
1s.
xcp: resume 'id1': Starting second pass for the in-progress
directories...
xcp: resume 'id1': Resuming the in-progress directories...
xcp: resume 'id1': Resumed command: copy {-acl4: True}
xcp: resume 'id1': Current options: {-id: 'id1'}
xcp: resume 'id1': Merged options: {-acl4: True, -id: 'id1'}
xcp: resume 'id1': Values marked with a * include operations before
resume
86,404 scanned, 39,912 copied, 39,899 indexed, 13.0 MiB in (2.60
MiB/s), 78.4 KiB out (15.6 KiB/s), 5s 86,404 scanned, 39,912 copied,
39,899 indexed, 13.0 MiB in (0/s), 78.4 KiB out (0/s), 10s
1.00M scanned, 100% found (1M have data), 1M compared, 100% verified
(data, attrs, mods, acls), 2.00M getacls, 202 v3perms, 1.00M same acls,
2.56 GiB in (2.76 MiB/s), 485 MiB out (524 KiB/s), 15m48s.
```

After resume finishes copying files, run verify again so that the source and destination storage have identical data.

### Transitioning 7-Mode SMB storage to ONTAP for CIFS data

This section covers the step-by-step procedure for transitioning a source 7-Mode SMB share to an ONTAP system.

 NetApp assumes that the 7-Mode and ONTAP systems are SMB licensed. The destination SVM is created, the source and destination SMB shares are exported, and XCP is installed and licensed.

1. Scan the SMB shares for the files and directories.

```

C:\xcp>xcp scan -stats \\10.61.77.189\performance_SMB_home_dirs
XCP SMB 1.6; (c) 2020 NetApp, Inc.; Licensed to xxxx xxxx[NetApp Inc]
until Mon Dec 31 00:00:00 2029
== Maximum Values ==
Size Depth Namelen Dirsize
15.6MiB 2 8 200
== Average Values ==
Size Depth Namelen Dirsize
540KiB 2 7 81
== Top File Extensions ==
.txt .tmp
5601 2200
== Number of files ==
empty <8KiB 8-64KiB 64KiB-1MiB 1-10MiB 10-100MiB >100MiB
46 6301 700 302 200 252
== Space used ==
empty <8KiB 8-64KiB 64KiB-1MiB 1-10MiB 10-100MiB >100MiB
0 6.80MiB 8.04MiB 120MiB 251MiB 3.64GiB 0
== Directory entries ==
empty 1-10 10-100 100-1K 1K-10K >10k
18 1 77 1
== Depth ==
0-5 6-10 11-15 16-20 21-100 >100
7898
== Modified ==
>1 year >1 month 1-31 days 1-24 hrs <1 hour <15 mins future
2167 56 322 5353
== Created ==
>1 year >1 month 1-31 days 1-24 hrs <1 hour <15 mins future
2171 54 373 5300
Total count: 7898
Directories: 97
Regular files: 7801
Symbolic links:
Junctions:
Special files:
Total space for regular files: 4.02GiB
Total space for directories: 0
Total space used: 4.02GiB
7,898 scanned, 0 errors, 0s

```

2. Copy the files (with or without ACL) from the source to the destination SMB share. The following example shows a copy with ACL.

```
C:\xcp>xcp copy -acl -fallback-user "DOMAIN\gabi" -fallback-group  
"DOMAIN\Group" \\10.61.77.189\performance_SMB_home_dirs  
\\10.61.77.56\performance_SMB_home_dirs  
XCP SMB 1.6; (c) 2020 NetApp, Inc.; Licensed to xxxx xxxx[NetApp Inc]  
until Mon Dec 31 00:00:00 2029  
7,898 scanned, 0 errors, 0 skipped, 184 copied, 96.1MiB (19.2MiB/s), 5s  
7,898 scanned, 0 errors, 0 skipped, 333 copied, 519MiB (84.7MiB/s), 10s  
7,898 scanned, 0 errors, 0 skipped, 366 copied, 969MiB (89.9MiB/s), 15s  
7,898 scanned, 0 errors, 0 skipped, 422 copied, 1.43GiB (99.8MiB/s), 20s  
7,898 scanned, 0 errors, 0 skipped, 1,100 copied, 1.69GiB (52.9MiB/s),  
25s  
7,898 scanned, 0 errors, 0 skipped, 1,834 copied, 1.94GiB (50.4MiB/s),  
30s  
7,898 scanned, 0 errors, 0 skipped, 1,906 copied, 2.43GiB (100MiB/s),  
35s  
7,898 scanned, 0 errors, 0 skipped, 2,937 copied, 2.61GiB (36.6MiB/s),  
40s  
7,898 scanned, 0 errors, 0 skipped, 2,969 copied, 3.09GiB (100.0MiB/s),  
45s  
7,898 scanned, 0 errors, 0 skipped, 3,001 copied, 3.58GiB (100.0MiB/s),  
50s  
7,898 scanned, 0 errors, 0 skipped, 3,298 copied, 4.01GiB (88.0MiB/s),  
55s  
7,898 scanned, 0 errors, 0 skipped, 5,614 copied, 4.01GiB (679KiB/s),  
1m0s  
7,898 scanned, 0 errors, 0 skipped, 7,879 copied, 4.02GiB (445KiB/s),  
1m5s  
7,898 scanned, 0 errors, 0 skipped, 7,897 copied, 4.02GiB (63.2MiB/s),  
1m5s
```



If there is no data aggregate, create a new one using the storage aggr create command.

### 3. Sync the files on the source and destination.

```
C:\xcp>xcp sync -acl -fallback-user "DOMAIN\gabi" -fallback-group  
"DOMAIN\Group" \\10.61.77.189\performance_SMB_home_dirs  
\\10.61.77.56\performance_SMB_home_dirs  
XCP SMB 1.6; (c) 2020 NetApp, Inc.; Licensed to xxxx xxxx[NetApp Inc]  
until Mon Dec 31 00:00:00 2029  
10,796 scanned, 4,002 compared, 0 errors, 0 skipped, 0 copied, 0  
removed, 5s  
15,796 scanned, 8,038 compared, 0 errors, 0 skipped, 0 copied, 0  
removed, 10s  
15,796 scanned, 8,505 compared, 0 errors, 0 skipped, 0 copied, 0
```

```
removed, 15s
15,796 scanned, 8,707 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 20s
15,796 scanned, 8,730 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 25s
15,796 scanned, 8,749 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 30s
15,796 scanned, 8,765 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 35s
15,796 scanned, 8,786 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 40s
15,796 scanned, 8,956 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 45s
8 XCP v1.6 User Guide © 2020 NetApp, Inc. All rights reserved.
```

Step Description

```
15,796 scanned, 9,320 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 50s
15,796 scanned, 9,339 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 55s
15,796 scanned, 9,363 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 1m0s
15,796 scanned, 10,019 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 1m5s
15,796 scanned, 10,042 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 1m10s
15,796 scanned, 10,059 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 1m15s
15,796 scanned, 10,075 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 1m20s
15,796 scanned, 10,091 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 1m25s
15,796 scanned, 10,108 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 1m30s
15,796 scanned, 10,929 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 1m35s
15,796 scanned, 12,443 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 1m40s
15,796 scanned, 13,963 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 1m45s
15,796 scanned, 15,488 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 1m50s
15,796 scanned, 15,796 compared, 0 errors, 0 skipped, 0 copied, 0
removed, 1m51s
```

4. Verify that the files were copied correctly.

```
C:\xcp> xcp verify \\10.61.77.189\performance_SMB_home_dirs  
\\10.61.77.56\performance_SMB_home_dir  
XCP SMB 1.6; (c) 2020 NetApp, Inc.; Licensed to xxxx xxxx[NetApp Inc]  
until Mon Dec 31 00:00:00 2029  
8 compared, 8 same, 0 different, 0 missing, 5s  
24 compared, 24 same, 0 different, 0 missing, 10s  
41 compared, 41 same, 0 different, 0 missing, 15s  
63 compared, 63 same, 0 different, 0 missing, 20s  
86 compared, 86 same, 0 different, 0 missing, 25s  
423 compared, 423 same, 0 different, 0 missing, 30s  
691 compared, 691 same, 0 different, 0 missing, 35s  
1,226 compared, 1,226 same, 0 different, 0 missing, 40s  
1,524 compared, 1,524 same, 0 different, 0 missing, 45s  
1,547 compared, 1,547 same, 0 different, 0 missing, 50s  
1,564 compared, 1,564 same, 0 different, 0 missing, 55s  
2,026 compared, 2,026 same, 0 different, 0 missing, 1m0s  
2,045 compared, 2,045 same, 0 different, 0 missing, 1m5s  
2,061 compared, 2,061 same, 0 different, 0 missing, 1m10s  
2,081 compared, 2,081 same, 0 different, 0 missing, 1m15s  
2,098 compared, 2,098 same, 0 different, 0 missing, 1m20s  
2,116 compared, 2,116 same, 0 different, 0 missing, 1m25s  
3,232 compared, 3,232 same, 0 different, 0 missing, 1m30s  
4,817 compared, 4,817 same, 0 different, 0 missing, 1m35s  
6,267 compared, 6,267 same, 0 different, 0 missing, 1m40s  
7,844 compared, 7,844 same, 0 different, 0 missing, 1m45s  
7,898 compared, 7,898 same, 0 different, 0 missing, 1m45s,cifs
```

[Next: CIFS data migration with ACLs From a source storage box to ONTAP.](#)

**CIFS data migration with ACLs from a source storage box to ONTAP**

[Previous: Data migration from 7-Mode to ONTAP.](#)

This section covers the step-by-step procedure for migrating CIFS data with security information from a source to a target ONTAP system.

1. Verify that the target ONTAP system is healthy.

```

C1_sti96-vsime-ucs540m_cluster::> cluster show
Node           Health   Eligibility
-----
sti96-vsime-ucs540m    true     true
sti96-vsime-ucs540n    true     true
2 entries were displayed.

C1_sti96-vsime-ucs540m_cluster::> node show
Node       Health   Eligibility   Uptime      Model      Owner      Location
-----
-
-
sti96-vsime-ucs540m
    true     true        15 days 21:17 SIMBOX      ahammed    sti
sti96-vsime-ucs540n
    true     true        15 days 21:17 SIMBOX      ahammed    sti
2 entries were displayed.

cluster::> storage failover show
                                Takeover
Node          Partner      Possible State Description
-----
-
-
sti96-vsime-ucs540m
    sti96-vsime-ucs540n    true     Connected to sti96-vsime-ucs540n
sti96-vsime-ucs540n
    sti96-vsime-ucs540m    true     Connected to sti96-vsime-ucs540m
2 entries were displayed.

C1_sti96-vsime-ucs540m_cluster::>

```

- Verify that at least one nonroot aggregate exists on the target system. The aggregate is normal.

```

cluster::*> storage aggregate show
Aggregate      Size Available Used% State    #Vols  Nodes          RAID
Status

-----
-----

aggr0_sti96_vsim_ucs540o
    7.58GB    373.3MB    95% online        1 sti96-vsim-
raid_dp,
                                         ucs540o
normal
aggr0_sti96_vsim_ucs540p
    7.58GB    373.3MB    95% online        1 sti96-vsim-
raid_dp,
                                         ucs540p
normal
aggr_001    103.7GB   93.63GB    10% online       1 sti96-vsim-
raid_dp,
                                         ucs540p
normal
sti96_vsim_ucs540o_aggr1
    23.93GB   23.83GB    0% online        1 sti96-vsim-
raid_dp,
                                         ucs540o
normal
sti96_vsim_ucs540p_aggr1
    23.93GB   23.93GB    0% online       0 sti96-vsim-
raid_dp,
                                         ucs540p
normal
5 entries were displayed.

```



If there is no data aggregate, create a new one using the `storage aggr create` command.

3. Create an SVM on the target cluster system.

```

cluster::*> vserver create -vserver vs1 -rootvolume root_vs1 -aggregate
sti96_vsim_ucs540o_aggr1 -rootvolume-security-style mixed

Verify that the SVM was successfully created.
C2_sti96-vsime-ucs540o_cluster::*> vserver show -vserver vs1
    Vserver: vs1
        Vserver Type: data
        Vserver Subtype: default
        Vserver UUID: f8bc54be-d91b-11e9-b99c-
005056a7e57e
            Root Volume: root_vs1
            Aggregate: sti96_vsime_ucs540o_aggr1
            NIS Domain: NSQA-RTP-NIS1
            Root Volume Security Style: mixed
            LDAP Client: esisconfig
            Default Volume Language Code: C.UTF-8
            Snapshot Policy: default
            Data Services: data-nfs, data-cifs,
                           data-flexcache, data-iscsi
            Comment: vs1
            Quota Policy: default
            List of Aggregates Assigned: -
            Limit on Maximum Number of Volumes allowed: unlimited
                Vserver Admin State: running
                Vserver Operational State: running
            Vserver Operational State Stopped Reason: -
                Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                Disallowed Protocols: -
            Is Vserver with Infinite Volume: false
                QoS Policy Group: -
                Caching Policy Name: -
                Config Lock: false
            Volume Delete Retention Period: 0
                IPspace Name: Default
                Foreground Process: -
            Is Msid Preserved for DR: false
Force start required to start Destination in multiple IDP fan-out case:
false
                Logical Space Reporting: false
                Logical Space Enforcement: false

```

4. Create a new read-write data volume on the destination SVM. Verify that the security style, language settings, and capacity requirements match the source volume.

```
CLUSTER CLUSTER::> vol create -vserver vs1 -volume dest_vol -aggregate aggr_001 -size 150g type RW -state online -security-style ntfs
```

5. Create a data LIF to serve SMB client requests.

```
CLUSTER::> network interface create -vserver vs1 -lif sti96-vsimsim-ucs540o_data1 -address 10.237.165.87 -netmask 255.255.240.0 -role data -data-protocol nfs,cifs -home-node sti96-vsimsim-ucs540o -home-port e0d
```

Verify that the LIF was successfully created.

```
cluster::*> network interface show -vserver vs1
      Logical      Status      Network          Current
Current Is
Vserver     Interface   Admin/Oper Address/Mask      Node      Port
Home
-----
-----
vs1
      sti96-vsimsim-ucs540o_data1
      up/up      10.237.165.87/20    sti96-vsimsim-ucs540o
                                         e0d
true
```

6. If required, create a static route with the SVM.

```
Network route create -vserver dest -destination 0.0.0.0/0 -gateway
10.237.160.1
```

Verify that the route was successfully created.

```
cluster::*> network route show -vserver vs1
Vserver          Destination      Gateway          Metric
-----
vs1
      0.0.0.0/0        10.237.160.1      20
      ::/0            fd20:8b1e:b255:9155::1
                                         20
2 entries were displayed.
```

7. Mount the target data volume in the SVM namespace.

```
CLUSTER::> volume mount -vserver vs1 -volume dest_vol -junction-path  
/dest_vol -active true
```

Verify that the volume is successfully mounted.

```
cluster::*> volume show -vserver vs1 -fields junction-path  
vserver volume junction-path  
-----  
vs1 dest_vol /dest_vol  
vs1 root_vs1 /  
2 entries were displayed.  
Note: You can also specify the volume mount options (junction path) with  
the volume create command.
```

#### 8. Start the CIFS service on the target SVM.

```
cluster::*> vserver cifs start -vserver vs1  
Warning: The admin status of the CIFS server for Vserver "vs1" is  
already "up".
```

Verify that the service is started and running.

```
cluster::*>  
Verify the service is started and running  
C2_sti96-vs1m-ucs540o_cluster::*> cifs show  
          Server          Status   Domain/Workgroup Authentication  
Vserver    Name        Admin     Name           Style  
-----  
vs1        D60AB15C2AFC4D6 up       CTL             domain
```

#### 9. Verify that the default export policy is applied to the target SVM.

```
CLUSTER::> vserver export-policy show -vserver dest  
Vserver      Policy Name  
-----  
dest         default
```

If required, create a new custom export policy for the target SVM.

```
CLUSTER::> vserver export-policy create -vserver vs1 -policynname  
xcpexport
```

10. Modify the export policy rules to allow access to CIFs clients.

```
CLUSTER::> export-policy rule modify -vserver dest -ruleindex 1  
-policynname xcpexportpolicy -clientmatch 0.0.0.0/0 -rorule any -rwrule  
any -anon 0
```

Verify that the policy rules are modified.

```

cluster::*> export-policy rule show -instance
                  Vserver: vs1
                  Policy Name: default
                  Rule Index: 1
                  Access Protocol: any
List of Client Match Hostnames, IP Addresses, Netgroups, or Domains:
0.0.0.0/0
                  RO Access Rule: any
                  RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                  Superuser Security Types: any
                  Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
                  NTFS Unix Security Options: fail
Vserver NTFS Unix Security Options: use_export_policy
                  Change Ownership Mode: restricted
Vserver Change Ownership Mode: use_export_policy
                  Policy ID: 12884901889
                  Vserver: vs1
                  Policy Name: default
                  Rule Index: 2
                  Access Protocol: any
List of Client Match Hostnames, IP Addresses, Netgroups, or Domains:
0:0:0:0:0:0:0:0/0
                  RO Access Rule: any
                  RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                  Superuser Security Types: none
                  Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
                  NTFS Unix Security Options: fail
Vserver NTFS Unix Security Options: use_export_policy
                  Change Ownership Mode: restricted
Vserver Change Ownership Mode: use_export_policy
                  Policy ID: 12884901889
2 entries were displayed.

```

11. Verify that the client is allowed access to the volume.

```

cluster::*> export-policy check-access -vserver vs1 -volume dest_vol
-client-ip 10.234.17.81 -authentication-method none -protocol cifs
-access-type read-write

          Policy      Policy      Rule
Path          Policy      Owner     Owner Type  Index
Access

-----
-----
/           default    root_vs1  volume   1
read
/dest_vol   default    dest_vol  volume   1
read-write
2 entries were displayed.

```

12. Connect to the Windows client system where XCP is installed. Browse to the XCP install path.

```

C:\WRSHDNT>dir c:\netapp\xcp
dir c:\netapp\xcp
Volume in drive C has no label.
Volume Serial Number is 5C04-C0C7
Directory of c:\netapp\xcp
09/18/2019  09:30 AM    <DIR>        .
09/18/2019  09:30 AM    <DIR>        ..
06/25/2019  06:27 AM            304 license
09/18/2019  09:30 AM    <DIR>        Logs
09/29/2019  08:45 PM            12,143,105 xcp.exe
                           2 File(s)   12,143,409 bytes
                           3 Dir(s)  29,219,549,184 bytes free

```

13. Query the source node SMB exports by running the xcp show command on the XCP Windows client host system.

```

C:\WRSHDNT>c:\netapp\xcp\xcp show \\10.237.165.71
c:\netapp\xcp\xcp show \\10.237.165.71
XCP SMB 1.6; (c) 2020 NetApp, Inc.; Licensed to XXX [NetApp Inc] until
Mon Dec 31 00:00:00 2029
Shares Errors Server
    6      0      10.237.165.71
== SMB Shares ==
Space Space Current
Free Used Connections Share Path          Folder Path
9.50GiB 4.57MiB 1      \\10.237.165.71\source_share C:\source_vol
94.3MiB 716KiB 0      \\10.237.165.71\ROOTSHARE C:\
0      0      N/A      \\10.237.165.71\ipc$      N/A
94.3MiB 716KiB 0      \\10.237.165.71\c$      C:\
== Attributes of SMB Shares ==
Share Types
Remark
source_share DISKTREE
test share DISKTREE
test_sh DISKTREE
ROOTSHARE DISKTREE      \"Share mapped
to top of Vserver global namespace, created bydeux_init \
ipc$ PRINTQ,SPECIAL,IPC,DEVICE
c$ SPECIAL
== Permissions of SMB Shares ==
Share Entity
Type
source_share Everyone
Allow/Full Control
ROOTSHARE Everyone
Allow/Full Control
ipc$ Everyone
Allow/Full Control
c$ Administrators
Allow/Full Control/

```

14. Run the `help` command for copy.

```

C:\WRSHDNT>c:\netapp\xcp\xcp help copy
c:\netapp\xcp\xcp help copy
XCP SMB 1.6; (c) 2020 NetApp, Inc.; Licensed to XXX [NetApp Inc] until
Mon Dec 31 00:00:00 2029
usage: xcp copy [-h] [-v] [-parallel <n>] [-match <filter>] [-preserve-
atime]
                  [-acl] [-fallback-user FALBACK_USER]
                  [-fallback-group FALBACK_GROUP] [-root]
                  source target

positional arguments:
  source
  target

optional arguments:
  -h, --help            show this help message and exit
  -v                   increase debug verbosity
  -parallel <n>        number of concurrent processes (default: <cpu-
count>)
  -match <filter>       only process files and directories that match
the
                      filter (see `xcp help -match` for details)
  -preserve-atime      restore last accessed date on source
  -acl                 copy security information
  -fallback-user FALBACK_USER
                      the name of the user on the target machine to
receive
                      the permissions of local (non-domain) source
machine
                      users (eg. domain\administrator)
  -fallback-group FALBACK_GROUP
                      the name of the group on the target machine to
receive
                      the permissions of local (non-domain) source
machine
                      groups (eg. domain\administrators)
  -root                copy acl for root directorytxt

```

15. On the target ONTAP system, get the list of local user and local group names that you need to provide as values for the `fallback-user` and `fallback-group` arguments path.

```

cluster::*> local-user show
  (vserver cifs users-and-groups local-user show)
Vserver      User Name          Full Name
Description

-----
-----
vs1          D60AB15C2AFC4D6\Administrator
                           Built-in
administrator account
C2_sti96-vs1m-ucs540o_cluster::*> local-group show
  (vserver cifs users-and-groups local-group show)
Vserver      Group Name        Description
-----
-----
vs1          BUILTIN\Administrators   Built-in Administrators
group
vs1          BUILTIN\Backup Operators  Backup Operators group
vs1          BUILTIN\Guests           Built-in Guests Group
vs1          BUILTIN\Power Users     Restricted
administrative privileges
vs1          BUILTIN\Users           All users
5 entries were displayed

```

16. To migrate the CIFs data with ACLs from the source to target, run the `xcp copy` command with the `-acl` and `-fallback-user/group` options.

For the `fallback-user/group` options, specify any user or group that can be found in Active Directory or local user/group to target system.

```

C:\WRSHDNT>c:\netapp\xcp\xcp copy -acl -fallback-user
D60AB15C2AFC4D6\Administrator -fallback-group BUILTIN\Users
\\10.237.165.79\source_share \\10.237.165.89\dest_share
c:\netapp\xcp\xcp copy -acl -fallback-user D60AB15C2AFC4D6\Administrator
-fallback-group BUILTIN\Users \\10.237.165.79\source_share
\\10.237.165.89\dest_share
XCP SMB 1.6; (c) 2020 NetApp, Inc.; Licensed to XXX [NetApp Inc] until
Mon Dec 31 00:00:00 2029
753 scanned, 0 errors, 0 skipped, 0 copied, 0 (0/s), 8s
753 scanned, 0 errors, 0 skipped, 0 copied, 0 (0/s), 13s
753 scanned, 0 errors, 0 skipped, 0 copied, 0 (0/s), 18s
ERROR failed to obtain fallback security principal "BUILTIN\Users".
Please check if the principal with the name "BUILTIN\Users" exists on
"D60AB15C2AFC4D6".
ERROR failed to obtain fallback security principal
"D60AB15C2AFC4D6\Administrator". Please check if the principal with the
name "D60AB15C2AFC4D6\Administrator" exists on "D60AB15C2AFC4D6".
ERROR failed to obtain fallback security principal "BUILTIN\Users".
Please check if the principal with the name "BUILTIN\Users" exists on
"D60AB15C2AFC4D6".
ERROR failed to obtain fallback security principal "BUILTIN\Users".
Please check if the principal with the name "BUILTIN\Users" exists on
"D60AB15C2AFC4D6".
ERROR failed to obtain fallback security principal "BUILTIN\Users".
Please check if the principal with the name "BUILTIN\Users" exists on
"D60AB15C2AFC4D6".
753 scanned, 0 errors, 0 skipped, 0 copied, 0 (0/s), 23s
ERROR failed to obtain fallback security principal
"D60AB15C2AFC4D6\Administrator". Please check if the principal with the
name "D60AB15C2AFC4D6\Administrator" exists on "D60AB15C2AFC4D6".
ERROR failed to obtain fallback security principal
"D60AB15C2AFC4D6\Administrator". Please check if the principal with the
name "D60AB15C2AFC4D6\Administrator" exists on "D60AB15C2AFC4D6".
ERROR failed to obtain fallback security principal
"D60AB15C2AFC4D6\Administrator". Please check if the principal with the
name "D60AB15C2AFC4D6\Administrator" exists on "D60AB15C2AFC4D6".
753 scanned, 0 errors, 0 skipped, 0 copied, 0 (0/s), 28s
753 scanned, 0 errors, 0 skipped, 249 copied, 24.0KiB (4.82KiB/s), 33s
753 scanned, 0 errors, 0 skipped, 744 copied, 54.4KiB (6.07KiB/s), 38s
753 scanned, 0 errors, 0 skipped, 746 copied, 54.5KiB (20/s), 43s
753 scanned, 0 errors, 0 skipped, 752 copied, 54.7KiB (1.23KiB/s), 44s
C:\WRSHDNT>

```

17. If `xcp copy` results in the error message `ERROR failed to obtain fallback security principal`, add the destination box in the hosts file (`C:\Windows\System32\drivers\etc\hosts`).

Use the following format for the NetApp storage destination box entry.

```
<data vserver data interface ip> 1 or more white spaces <cifs server name>
```

```
cluster::*> cifs show
      Server          Status   Domain/Workgroup Authentication
Vserver    Name        Admin     Name           Style
-----
vs1        D60AB15C2AFC4D6 up       CTL             domain
C2_sti96-vsimm-ucs540o_cluster::*> network interface show
      Logical      Status   Network           Current
Current Is
Cluster
      sti96-vsimm-ucs540p_clus1
      up/up       192.168.148.136/24 sti96-vsimm-ucs540p
                           e0a
true
      sti96-vsimm-ucs540p_clus2
      up/up       192.168.148.137/24 sti96-vsimm-ucs540p
                           e0b
true
vs1
      sti96-vsimm-ucs540o_data1
      up/up       10.237.165.87/20   sti96-vsimm-ucs540o
                           e0d
true
      sti96-vsimm-ucs540o_data1_inet6
      up/up       fd20:8b1e:b255:9155::583/64
                           sti96-vsimm-ucs540o
                           e0d
true
      sti96-vsimm-ucs540o_data2
      up/up       10.237.165.88/20   sti96-vsimm-ucs540o
                           e0e
true
10.237.165.87  D60AB15C2AFC4D6  -> destination box entry to be added in
hosts file.
```

18. If you still get the error message **ERROR failed to obtain fallback security principal** after adding the destination box entry in the hosts files, then the user/group does not exist in the target system.

```
C:\WRSHDNT>c:\netapp\xcp\xcp copy -acl -fallback-user  
D60AB15C2AFC4D6\unknown_user -fallback-group BUILTIN\Users  
\\"10.237.165.79\source_share \\"10.237.165.89\dest_share  
c:\netapp\xcp\xcp copy -acl -fallback-user D60AB15C2AFC4D6\unknown_user  
-fallback-group BUILTIN\Users \\"10.237.165.79\source_share  
\\"10.237.165.89\dest_share  
XCP SMB 1.6; (c) 2020 NetApp, Inc.; Licensed to XXX [NetApp Inc] until  
Mon Dec 31 00:00:00 2029  
ERROR failed to obtain fallback security principal  
"D60AB15C2AFC4D6\unknown_user". Please check if the principal with the  
name "D60AB15C2AFC4D6\unknown_user" exists on "D60AB15C2AFC4D6".  
ERROR failed to obtain fallback security principal  
"D60AB15C2AFC4D6\unknown_user". Please check if the principal with the  
name "D60AB15C2AFC4D6\unknown_user" exists on "D60AB15C2AFC4D6".  
ERROR failed to obtain fallback security principal  
"D60AB15C2AFC4D6\unknown_user". Please check if the principal with the  
name "D60AB15C2AFC4D6\unknown_user" exists on "D60AB15C2AFC4D6".  
ERROR failed to obtain fallback security principal  
"D60AB15C2AFC4D6\unknown_user". Please check if the principal with the  
name "D60AB15C2AFC4D6\unknown_user" exists on "D60AB15C2AFC4D6".  
753 scanned, 0 errors, 0 skipped, 0 copied, 0 (0/s), 5s  
753 scanned, 0 errors, 0 skipped, 0 copied, 0 (0/s), 10s  
753 scanned, 0 errors, 0 skipped, 0 copied, 0 (0/s), 15s  
753 scanned, 0 errors, 0 skipped, 284 copied, 27.6KiB (5.54KiB/s), 20s  
753 scanned, 0 errors, 0 skipped, 752 copied, 54.7KiB (2.44KiB/s), 22s  
C:\WRSHDNT>
```

19. Use `xcp copy` to migrate CIFs data with ACLs (with or without the root folder).

Without the root folder, run the following commands:

```
C:\WRSHDNT>c:\netapp\xcp\xcp copy -acl -fallback-user  
D60AB15C2AFC4D6\Administrator -fallback-group BUILTIN\Users  
\\"10.237.165.79\source_share \\"10.237.165.89\dest_share  
c:\netapp\xcp\xcp copy -acl -fallback-user  
D60AB15C2AFC4D6\Administrator -fallback-group BUILTIN\Users  
\\"10.237.165.79\source_share \\"10.237.165.89\dest_share  
XCP SMB 1.6; (c) 2020 NetApp, Inc.; Licensed to XXX [NetApp Inc] until  
Mon Dec 31 00:00:00 2029  
753 scanned, 0 errors, 0 skipped, 0 copied, 0 (0/s), 5s  
753 scanned, 0 errors, 0 skipped, 0 copied, 0 (0/s), 10s  
753 scanned, 0 errors, 0 skipped, 0 copied, 0 (0/s), 15s  
753 scanned, 0 errors, 0 skipped, 210 copied, 20.4KiB (4.08KiB/s), 20s  
753 scanned, 0 errors, 0 skipped, 752 copied, 54.7KiB (2.38KiB/s), 22s  
C:\WRSHDNT>
```

With the root folder, run the following commands:

```
C:\WRSHDNT>c:\netapp\xcp\xcp copy -acl -root -fallback-user  
D60AB15C2AFC4D6\Administrator -fallback-group BUILTIN\Users  
\\"10.237.165.79\source_share \\"10.237.165.89\dest_share  
c:\netapp\xcp\xcp copy -acl -root -fallback-user  
D60AB15C2AFC4D6\Administrator -fallback-group BUILTIN\Users  
\\"10.237.165.79\source_share \\"10.237.165.89\dest_share  
XCP SMB 1.6; (c) 2020 NetApp, Inc.; Licensed to XXX [NetApp Inc] until  
Mon Dec 31 00:00:00 2029  
753 scanned, 0 errors, 0 skipped, 0 copied, 0 (0/s), 5s  
753 scanned, 0 errors, 0 skipped, 0 copied, 0 (0/s), 10s  
753 scanned, 0 errors, 0 skipped, 0 copied, 0 (0/s), 15s  
753 scanned, 0 errors, 0 skipped, 243 copied, 23.6KiB (4.73KiB/s), 20s  
753 scanned, 0 errors, 0 skipped, 752 copied, 54.7KiB (6.21KiB/s), 25s  
753 scanned, 0 errors, 0 skipped, 752 copied, 54.7KiB (0/s), 30s  
753 scanned, 0 errors, 0 skipped, 752 copied, 54.7KiB (0/s), 35s  
753 scanned, 0 errors, 0 skipped, 752 copied, 54.7KiB (0/s), 40s  
753 scanned, 0 errors, 0 skipped, 752 copied, 54.7KiB (0/s), 45s  
753 scanned, 0 errors, 0 skipped, 752 copied, 54.7KiB (0/s), 50s  
753 scanned, 0 errors, 0 skipped, 752 copied, 54.7KiB (0/s), 55s  
753 scanned, 0 errors, 0 skipped, 752 copied, 54.7KiB (0/s), 1m0s  
753 scanned, 0 errors, 0 skipped, 752 copied, 54.7KiB (0/s), 1m5s  
753 scanned, 0 errors, 0 skipped, 752 copied, 54.7KiB (817/s), 1m8s  
C:\WRSHDNT>
```

[Next: Best practice guidelines and recommendations.](#)

## Best practice guidelines and recommendations

Previous: [CIFS data migration with ACLs From a source storage box to ONTAP.](#)

- Use the XCP client operating system, which is IMT supported. The IMT supported client is qualified by NetApp.
- Run XCP as a root user in the Linux operating system to perform migration. you can run the xcp command as the sudo user, but it is not supported by XCP.
- Run only one instance of XCP per client. Technically you can run multiple instances of XCP on the same host from a different location, however this is not a supported practice. Indeed, running many instances might result in failure.
- In the current XCP version, Live Source is not supported. If the source NetApp volume is active and continuously changed by applications and users, you should take a snapshot of the source volume to perform a migration.
- It is a best practice to create a new snapshot with a different name for every incremental sync so that it is easy to create an incremental migration path based on the snapshot name in the event of failure.
- If you are performing a snapshot-based migration, it is a best practice to continue snapshot-based migration until cutover.
- If you have more than 10 million files and you have incremental data change of more than 50%, it is a best practice to use a higher core count and more memory than the minimum recommendation in the installation and administration guide.

Next: [Troubleshooting.](#)

## Troubleshooting

Previous: [Best practice guidelines and recommendations.](#)

### Error 1: XCP Failed with nfs3 error 70: stale filehandle Error in the xcp.log

#### Reason and guidance.

Mount the source folder and verify that the folder exists. If it does not exist or if it has been removed, you will receive a stale filehandle error, in which case, you can ignore the error.

### Error 2: NetApp NFS Destination Volume Has Space, but XCP Failed with nfs3 error 28: no space left on device

#### Reason and guidance.

1. Check the space of the NFS destination volume by running the df command or check the storage.

```
root@workr-140: USER3# df -h /xcpdest
Filesystem           Size   Used Avail Use% Mounted on
10.63.150.127:/xcpsrc_vol  4.3T  1.7T  2.6T  40% /xcpsrc_vol
```

2. Check the inodes in the storage controller.

```
A800-Node1-2::> volume show -volume xcpdest -fields files,files-used
vserver          volume   files   files-used
-----
A800-Node1_vs1  xcpdest  21251126 21251126
A800-Node1-2::>
```

3. If inode is used, increase the number of inodes by running the following command:

```
A800-Node1-2::> volume modify -volume xcpdest -vserver A800-Node1_vs1
-files 40000000
Volume modify successful on volume xcpdest of Vserver A800-Node1_vs1.
A800-Node1-2::> volume show -volume xcpdest -fields files,files-used
vserver          volume   files   files-used
-----
A800-Node1_vs1  xcpdest  39999990 21251126
A800-Node1-2::>
```

[Next: Where to find additional information.](#)

## Where to find additional information

[Previous: Troubleshooting.](#)

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

- NetApp XCP blogs  
<https://blog.netapp.com/tag/netapp-xcp/>
- NetApp XCP user guide  
<https://library-clnt.dmv.netapp.com/documentation/productlibrary/index.html?productID=63064>
- Bigdata Analytics data to Artificial Intelligence – Data mover solution for AI  
<https://www.netapp.com/us/media/tr-4732.pdf>

[Next: Version history.](#)

## Version history

[Previous: Where to find additional information.](#)

Version	Date	Document version history
Version 1.0	October 2020	Initial release.

# Data Protection

# **Security**

# Enterprise Applications

# NetApp Enterprise Database Solutions

## Oracle Database

### Deploying Oracle Database

#### Solution Overview

##### Automated Deployment of Oracle19c for ONTAP on NFS

Organizations are automating their environments to gain efficiencies, accelerate deployments, and reduce manual effort. Configuration management tools like Ansible are being used to streamline enterprise database operations. In this solution, we demonstrate how you can use Ansible to automate the provisioning and configuration of Oracle 19c with NetApp ONTAP. By enabling storage administrators, systems administrators, and DBAs to consistently and rapidly deploy new storage, configure database servers, and install Oracle 19c software, you achieve the following benefits:

- Eliminate design complexities and human errors, and implement a repeatable consistent deployment and best practices
- Decrease time for provisioning of storage, configuration of DB hosts, and Oracle installation
- Increase database administrators, systems and storage administrators productivity
- Enable scaling of storage and databases with ease

NetApp provides customers with validated Ansible modules and roles to accelerate deployment, configuration, and lifecycle management of your Oracle database environment. This solution provides instruction and Ansible playbook code, to help you:

- Create and configure ONTAP NFS storage for Oracle Database
- Install Oracle 19c on RedHat Enterprise Linux 7/8 or Oracle Linux 7/8
- Configure Oracle 19c on ONTAP NFS storage

For more details or to begin, please see the overview videos below.

#### AWX/Tower Deployments

- Part 1: Getting Started, Requirements, Automation Details and Initial AWX/Tower Configuration
- [https://docs.netapp.com/us-en/netapp-solutions/media/oracle\\_deployment\\_auto\\_v1.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/oracle_deployment_auto_v1.mp4) (video)
- Part 2: Variables and Running the Playbook
- [https://docs.netapp.com/us-en/netapp-solutions/media/oracle\\_deployment\\_auto\\_v2.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/oracle_deployment_auto_v2.mp4) (video)

#### CLI Deployment

- Part 1: Getting Started, Requirements, Automation Details and Ansible Control Host Setup
- [https://docs.netapp.com/us-en/netapp-solutions/media/oracle\\_deployment\\_auto\\_v4.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/oracle_deployment_auto_v4.mp4) (video)
- Part 2: Variables and Running the Playbook

► <https://docs.netapp.com/us-en/netapp-solutions/media/oracle3.mp4> (video)

## Getting started

This solution has been designed to be run in an AWX/Tower environment or by CLI on an Ansible control host.

## AWX/Tower

For AWX/Tower environments, you are guided through creating an inventory of your ONTAP cluster management and Oracle server (IPs and hostnames), creating credentials, configuring a project that pulls the Ansible code from NetApp Automation Github, and the Job Template that launches the automation.

1. Fill out the variables specific to your environment, and copy and paste them into the Extra Vars fields in your job template.
2. After the extra vars have been added to your job template, you can launch the automation.
3. The job template is run in three phases by specifying tags for `ontap_config`, `linux_config`, and `oracle_config`.

## CLI via the Ansible control host

1. To configure the Linux host so that it can be used as an Ansible control host  
[click here for RHEL 7/8 or CentOS 7/8](#), or  
[here for Ubuntu/Debian](#)
2. After the Ansible control host is configured, you can git clone the Ansible Automation repository.
3. Edit the hosts file with the IPs and/or hostnames of your ONTAP cluster management and Oracle server's management IPs.
4. Fill out the variables specific to your environment, and copy and paste them into the `vars.yml` file.
5. Each Oracle host has a variable file identified by its hostname that contains host-specific variables.
6. After all variable files have been completed, you can run the playbook in three phases by specifying tags for `ontap_config`, `linux_config`, and `oracle_config`.

## Requirements

Environment	Requirements
<b>Ansible environment</b>	AWX/Tower or Linux host to be the Ansible control host Ansible v.2.10 and higher Python 3 Python libraries - <code>netapp-lib</code> - <code>xmldict</code> - <code>jmespath</code>
<b>ONTAP</b>	ONTAP version 9.3 - 9.7 Two data aggregates NFS vlan and ifgrp created

Environment	Requirements
Oracle server(s)	RHEL 7/8
	Oracle Linux 7/8
	Network interfaces for NFS, public, and optional mgmt
	Oracle installation files on Oracle servers

## Automation Details

This automated deployment is designed with a single Ansible playbook that consists of three separate roles. The roles are for ONTAP, Linux, and Oracle configurations.

The following table describes which tasks are being automated.

Role	Tasks
ontap_config	Pre-check of the ONTAP environment
	Creation of NFS based SVM for Oracle
	Creation of export policy
	Creation of volumes for Oracle
	Creation of NFS LIFs
linux_config	Create mount points and mount NFS volumes
	Verify NFS mounts
	OS specific configuration
	Create Oracle directories
	Configure hugepages
	Disable SELinux and firewall daemon
	Enable and start chronyd service
	increase file descriptor hard limit
oracle_config	Create pam.d session file
	Oracle software installation
	Create Oracle listener
	Create Oracle databases
	Oracle environment configuration
	Save PDB state
	Enable instance archive mode
	Enable DNFS client
	Enable database auto startup and shutdown between OS reboots

## Default parameters

To simplify automation, we have preset many required Oracle deployment parameters with default values. It is generally not necessary to change the default parameters for most deployments. A more advanced user can make changes to the default parameters with caution. The default parameters are located in each role folder under defaults directory.

## Deployment instructions

Before starting, download the following Oracle installation and patch files and place them in the /tmp/archive directory with read, write, and execute access for all users on each DB server to be deployed. The automation tasks look for the named installation files in that particular directory for Oracle installation and configuration.

```
LINUX.X64_193000_db_home.zip -- 19.3 base installer  
p31281355_190000_Linux-x86-64.zip -- 19.8 RU patch  
p6880880_190000_Linux-x86-64.zip -- opatch version 12.2.0.1.23
```

## License

You should read license information as stated in the Github repository. By accessing, downloading, installing, or using the content in this repository, you agree the terms of the license laid out [here](#).

Note that there are certain restrictions around producing and/or sharing any derivative works with the content in this repository. Please make sure you read the terms of the [License](#) before using the content. If you do not agree to all of the terms, do not access, download, or use the content in this repository.

After you are ready, click [here for detailed AWX/Tower deployment procedures](#) or [here for CLI deployment](#).

## Step-by-step deployment procedure

### AWX/Tower deployment Oracle 19c Database

#### 1. Create the inventory, group, hosts, and credentials for your environment

This section describes the setup of inventory, groups, hosts, and access credentials in AWX/Ansible Tower that prepare the environment for consuming NetApp automated solutions.

1. Configure the inventory.
  - a. Navigate to Resources → Inventories → Add, and click Add Inventory.
  - b. Provide the name and organization details, and click Save.
  - c. On the Inventories page, click the inventory created.
  - d. If there are any inventory variables, paste them in the variables field.
  - e. Navigate to the Groups sub-menu and click Add.
  - f. Provide the name of the group for ONTAP, paste the group variables (if any) and click Save.
  - g. Repeat the process for another group for Oracle.
  - h. Select the ONTAP group created, go to the Hosts sub-menu and click Add New Host.
  - i. Provide the IP address of the ONTAP cluster management IP, paste the host variables (if any), and

click Save.

- j. This process must be repeated for the Oracle group and Oracle host(s) management IP/hostname.
- 2. Create credential types. For solutions involving ONTAP, you must configure the credential type to match username and password entries.
  - a. Navigate to Administration → Credential Types, and click Add.
  - b. Provide the name and description.
  - c. Paste the following content in Input Configuration:

```
fields:

- id: username
- type: string
- label: Username
- id: password
- type: string
- label: Password
- secret: true
- id: vsadmin_password
- type: string
- label: vsadmin_password
- secret: true

```

- d. Paste the following content into Injector Configuration:

```
extra_vars:

- password: '{{ password }}'
- username: '{{ username }}'
- vsadmin_password: '{{ vsadmin_password }}'

```

- 3. Configure the credentials.
  - a. Navigate to Resources → Credentials, and click Add.
  - b. Enter the name and organization details for ONTAP.
  - c. Select the custom Credential Type you created for ONTAP.
  - d. Under Type Details, enter the username, password, and vsadmin\_password.
  - e. Click Back to Credential and click Add.
  - f. Enter the name and organization details for Oracle.
  - g. Select the Machine credential type.
  - h. Under Type Details, enter the Username and Password for the Oracle hosts.
  - i. Select the correct Privilege Escalation Method, and enter the username and password.

## 2. Create a project

- 1. Go to Resources → Projects, and click Add.

- a. Enter the name and organization details.
- b. Select Git in the Source Control Credential Type field.
- c. enter [https://github.com/NetApp-Automation/na\\_oracle19c\\_deploy.git](https://github.com/NetApp-Automation/na_oracle19c_deploy.git) as the source control URL.
- d. Click Save.
- e. The project might need to sync occasionally when the source code changes.

### 3. Configure Oracle host\_vars

The variables defined in this section are applied to each individual Oracle server and database.

1. Input your environment-specific parameters in the following embedded Oracle hosts variables or host\_vars form.



The items in blue must be changed to match your environment.

#### Host VARS Config

```
<style>
div {
position: relative;
}
div button {
position: absolute;
top: 0;
right: 0;
}
button {
transition-duration: 0.4s;
background-color: white;
color: #1563a3;
border: 2px solid #1563a3;
}
button:hover {
background-color: #1563a3;
color: white;
}
#more_datastores_nfs {
display: block;
}
#more_datastores_nfs_button {
display: none;
}
</style>
<div class="listingblock"><div class="content"><div><button id="copy-
button1" onclick="CopyClassText1()">Copy</button></div><pre><code><div
class="CopyMeClass1" id="CopyMeID1">
```

```

#####
#####          Host Variables Configuration          #####
#####

# Add your Oracle Host
ansible_host: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>10.61.180.15</i></span>

# Oracle db log archive mode: true - ARCHIVELOG or false - NOARCHIVELOG
log_archive_mode: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>true</i></span>

# Number of pluggable databases per container instance identified by sid.
Pdb_name specifies the prefix for container database naming in this case
cdb2_pdb1, cdb2_pdb2, cdb2_pdb3
oracle_sid: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>cdb2</i></span>
pdb_num: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>3</i></span>
pdb_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>"{{ oracle_sid }}_pdb"</i></span>

# CDB listener port, use different listener port for additional CDB on same host
listener_port: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>1523</i></span>

# CDB is created with SGA at 75% of memory_limit, MB. Consider how many databases to be hosted on the node and how much ram to be allocated to each DB. The grand total SGA should not exceed 75% available RAM on node.
memory_limit: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>5464</i></span>

# Set "em_configuration: DBEXPRESS" to install enterprise manager express and choose a unique port from 5500 to 5599 for each sid on the host.
# Leave them black if em express is not installed.
em_configuration: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;"><i>DBEXPRESS</i></span>
```

```

em_express_port: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline; text-decoration:underline;" /><i>5501</i></span>

# "{{groups.oracle[0]}}" represents first Oracle DB server as defined in Oracle hosts group [oracle]. For concurrent multiple Oracle DB servers deployment, [0] will be incremented for each additional DB server. For example, "{{groups.oracle[1]}}" represents DB server 2, "{{groups.oracle[2]}}" represents DB server 3 ... As a good practice and the default, minimum three volumes is allocated to a DB server with corresponding /u01, /u02, /u03 mount points, which store oracle binary, oracle data, and oracle recovery files respectively. Additional volumes can be added by click on "More NFS volumes" but the number of volumes allocated to a DB server must match with what is defined in global vars file by volumes_nfs parameter, which dictates how many volumes are to be created for each DB server.

host_datastores_nfs:
  - {vol_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;' /><i>{{groups.oracle[0]}}_u01</i></span>", aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>aggr01_node01</i></span>, lif: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>172.21.94.200</i></span>, size: <span <div contenteditable="true"/><i>25</i></span>}
  - {vol_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;' /><i>{{groups.oracle[0]}}_u02</i></span>", aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>aggr01_node01</i></span>, lif: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>172.21.94.200</i></span>, size: <span <div contenteditable="true"/><i>25</i></span>}
  - {vol_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;' /><i>{{groups.oracle[0]}}_u03</i></span>", aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>aggr01_node01</i></span>, lif: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;" /><i>172.21.94.200</i></span>, size: <span <div contenteditable="true"/><i>25</i></span>}
<a id="more_datastores_nfs" href="javascript:datastoredropdown();">More NFS volumes</a><div id="select_more_datastores_nfs"></div><a

```

```

id="more_datastores_nfs_button"
href="javascript:adddatastorevolumes();">Enter NFS volumes'
details</a><div id="extra_datastores_nfs"></div>
</div></code></pre></div></div>
<script>
function CopyClassText1() {
    var textToCopy = document.getElementById("CopyMeID1");
    var currentRange;
    if(document.getSelection().rangeCount > 0)
    {
        currentRange = document.getSelection().getRangeAt(0);
        window.getSelection().removeRange(currentRange);
    }
    else
    {
        currentRange = false;
    }
    var CopyRange = document.createRange();
    CopyRange.selectNode(textToCopy);
    window.getSelection().addRange(CopyRange);
    document.getElementById("more_datastores_nfs").style.display = "none";
    var command = document.execCommand("copy");
    if (command)
    {
        document.getElementById("copy-button1").innerHTML = "Copied!";
        setTimeout(revert_copy, 3000);
    }
    window.getSelection().removeRange(CopyRange);
    if(currentRange)
    {
        window.getSelection().addRange(currentRange);
    }
}
function revert_copy() {
    document.getElementById("copy-button1").innerHTML = "Copy";
    document.getElementById("more_datastores_nfs").style.display =
"block";
}

function datastoredropdown() {
    document.getElementById("more_datastores_nfs").style.display = "none";
    document.getElementById("more_datastores_nfs_button").style.display =
"block";
    var x=1;
    var myHTML = '';
    var buildup = '';

```

```

var wrapper = document.getElementById("select_more_datastores_nfs");
while (x < 100) {
    buildup += '<option value="' + x + '">' + x + '</option>';
    x++;
}
myHTML += '<a id="more_datastores_nfs">How many extra NFS volumes do
you wish to add?</a><select name="number_of_extra_datastores_nfs"
id="number_of_extra_datastores_nfs">' + buildup + '</select>';
wrapper.innerHTML = myHTML;
}

function adddatastorevolumes() {
    var y =
document.getElementById("number_of_extra_datastores_nfs").value;
    var j=0;
    var myHTML = '';
    var wrapper = document.getElementById("extra_datastores_nfs");
    while (j < y) {
        j++;
        myHTML += ' - {vol_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>{{groups.oracle[0]}}_u01</i></span>,
aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>aggr01_node02</i></span>, lif: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>172.21.94.201</i></span>,
size: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>25</i></span>}<br>';
    }
    wrapper.innerHTML = myHTML;
    document.getElementById("select_more_datastores_nfs").style.display =
"none";
    document.getElementById("more_datastores_nfs_button").style.display =
"none";
}

</script>

```

- Fill in all variables in the blue fields.
- After completing variables input, click the Copy button on the form to copy all variables to be transferred to AWX or Tower.
- Navigate back to AWX or Tower and go to Resources → Hosts, and select and open the Oracle server configuration page.
- Under the Details tab, click edit and paste the copied variables from step 1 to the Variables field under the YAML tab.

- e. Click Save.
- f. Repeat this process for any additional Oracle servers in the system.

#### 4. Configure global variables

Variables defined in this section apply to all Oracle hosts, databases, and the ONTAP cluster.

1. Input your environment-specific parameters in following embedded global variables or vars form.



The items in blue must be changed to match your environment.

##### VARS

```
<style>
div {
position: relative;
}
div button {
position: absolute;
top: 0;
right: 0;
}
button {
transition-duration: 0.4s;
background-color: white;
color: #1563a3;
border: 2px solid #1563a3;
}
button:hover {
background-color: #1563a3;
color: white;
}
#more_storage_vlans {
display: block;
}
#more_storage_vlans_button {
display: none;
}
#more_nfs_volumes {
display: block;
}
#more_nfs_volumes_button {
display: none;
}
</style>
<div class="listingblock"><div class="content"><div><button id="copy-
```

```

button" onclick="CopyClassText()">Copy</button></div><pre><code><div
class="CopyMeClass" id="CopyMeID">
#####
##### Oracle 19c deployment global user configuration variables #####
#####
##### Consolidate all variables from ontap, linux and oracle #####
#####

#####
### Ontap env specific config variables ##
#####

#Inventory group name
#Default inventory group name - 'ontap'
#Change only if you are changing the group name either in inventory/hosts
file or in inventory groups in case of AWX/Tower
hosts_group: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>ontap</i></span>

#CA_signed_certificates (ONLY CHANGE to 'true' IF YOU ARE USING CA SIGNED
CERTIFICATES)
ca_signed_certs: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>false</i></span>

#Names of the Nodes in the ONTAP Cluster
nodes:
- <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline;"><i>AFF-
01</i></span>
- <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline;"><i>AFF-
02</i></span>

#Storage VLANs
#Add additional rows for vlans as necessary
storage_vlans:
- {vlan_id: "<span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>203</i></span>", name: "<span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>infra_NFS</i></span>", protocol: "<span <div
contenteditable="true"/><i>NFS</i></span>"}
<a id="more_storage_vlans" href="javascript:storagevlandropdown();">More

```

```

Storage VLANs</a><div id="select_more_storage_vlans"></div><a id="more_storage_vlans_button" href="javascript:addstoragevlans();">Enter Storage VLANs details</a><div id="extra_storage_vlans"></div>

#Details of the Data Aggregates that need to be created
#If Aggregate creation takes longer, subsequent tasks of creating volumes may fail.
#There should be enough disks already zeroed in the cluster, otherwise aggregate create will zero the disks and will take long time
data_aggregates:
  - {aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>aggr01_node01</i></span>}
  - {aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>aggr01_node02</i></span>}

#SVM name
svm_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>ora_svm</i></span>

# SVM Management LIF Details
svm_mgmt_details:
  - {address: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>172.21.91.100</i></span>, netmask: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>255.255.255.0</i></span>, home_port: <span <div contenteditable="true"/><i>e0M</i></span>}

# NFS storage parameters when data_protocol set to NFS. Volume named after Oracle hosts name identified by mount point as follow for oracle DB server 1. Each mount point dedicated to a particular Oracle files: u01 - Oracle binary, u02 - Oracle data, u03 - Oracle redo. Add additional volumes by click on "More NFS volumes" and also add the volumes list to corresponding host_vars as host_datastores_nfs variable. For multiple DB server deployment, additional volumes sets needs to be added for additional DB server. Input variable "{{groups.oracle[1]}}_u01", "{{groups.oracle[1]}}_u02", and "{{groups.oracle[1]}}_u03" as vol_name for second DB server. Place volumes for multiple DB servers alternatingly between controllers for balanced IO performance, e.g. DB server 1 on controller node1, DB server 2 on controller node2 etc. Make sure match lif address with controller node.
volumes_nfs:

```

```

    - {vol_name: ""<span <div contenteditable='true"
      style="color:#004EFF; font-weight:bold; font-style:italic; text-
      decoration:underline;"><i>{{groups.oracle[0]}}_u01</i></span>",
      aggr_name: <span <div contenteditable='true" style="color:#004EFF; font-
      weight:bold; font-style:italic; text-
      decoration:underline;"><i>aggr01_node01</i></span>, lif: <span <div
      contenteditable='true" style="color:#004EFF; font-weight:bold; font-
      style:italic; text-decoration:underline;"><i>172.21.94.200</i></span>,
      size: <span <div contenteditable='true"/><i>25</i></span>}
    - {vol_name: ""<span <div contenteditable='true"
      style="color:#004EFF; font-weight:bold; font-style:italic; text-
      decoration:underline;"><i>{{groups.oracle[0]}}_u02</i></span>",
      aggr_name: <span <div contenteditable='true" style="color:#004EFF; font-
      weight:bold; font-style:italic; text-
      decoration:underline;"><i>aggr01_node01</i></span>, lif: <span <div
      contenteditable='true" style="color:#004EFF; font-weight:bold; font-
      style:italic; text-decoration:underline;"><i>172.21.94.200</i></span>,
      size: <span <div contenteditable='true"/><i>25</i></span>}
    - {vol_name: ""<span <div contenteditable='true"
      style="color:#004EFF; font-weight:bold; font-style:italic; text-
      decoration:underline;"><i>{{groups.oracle[0]}}_u03</i></span>",
      aggr_name: <span <div contenteditable='true" style="color:#004EFF; font-
      weight:bold; font-style:italic; text-
      decoration:underline;"><i>aggr01_node01</i></span>, lif: <span <div
      contenteditable='true" style="color:#004EFF; font-weight:bold; font-
      style:italic; text-decoration:underline;"><i>172.21.94.200</i></span>,
      size: <span <div contenteditable='true"/><i>25</i></span>}
<a id="more_nfs_volumes" href="javascript:nfsvolumesdropdown();">More NFS
volumes</a><div id="select_more_nfs_volumes"></div><a
id="more_nfs_volumes_button" href="javascript:adnnfsvolumes();">Enter NFS
volumes' details</a><div id="extra_nfs_volumes"></div>

#NFS LIFs IP address and netmask
nfs_lifs_details:
  - address: <span <div contenteditable='true" style="color:#004EFF; font-
      weight:bold; font-style:italic; text-
      decoration:underline;"><i>172.21.94.200</i></span> #for node-1
      netmask: <span <div contenteditable='true" style="color:#004EFF; font-
      weight:bold; font-style:italic; text-
      decoration:underline;"><i>255.255.255.0</i></span>
  - address: <span <div contenteditable='true" style="color:#004EFF; font-
      weight:bold; font-style:italic; text-
      decoration:underline;"><i>172.21.94.201</i></span> #for node-2
      netmask: <span <div contenteditable='true" style="color:#004EFF; font-
      weight:bold; font-style:italic; text-
      decoration:underline;"><i>255.255.255.0</i></span>

```

```

#NFS client match
client_match: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;" /><i>172.21.94.0/24</i></span>

#####
### Linux env specific config variables #####
#####

#NFS Mount points for Oracle DB volumes
mount_points:
  - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;" /><i>/u01</i></span>
  - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;" /><i>/u02</i></span>
  - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;" /><i>/u03</i></span>

# Up to 75% of node memory size divided by 2mb. Consider how many
databases to be hosted on the node and how much ram to be allocated to
each DB.
# Leave it blank if hugepage is not configured on the host.
hugepages_nr: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;" /><i>1234</i></span>

# RedHat subscription username and password
redhat_sub_username: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;" /><i>xxx</i></span>
redhat_sub_password: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;" /><i>xxx</i></span>

#####
### DB env specific install and config variables #####
#####

db_domain: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;" /><i>your.domain.com</i></span>

```

```

# Set initial password for all required Oracle passwords. Change them
after installation.

initial_pwd_all: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>netapp123</i></span>

</div></code></pre></div></div>
<script>
function CopyClassText () {
    var textToCopy = document.getElementById("CopyMeID");
    var currentRange;
    if(document.getSelection().rangeCount > 0)
    {
        currentRange = document.getSelection().getRangeAt(0);
        window.getSelection().removeRange(currentRange);
    }
    else
    {
        currentRange = false;
    }
    var CopyRange = document.createRange();
    CopyRange.selectNode(textToCopy);
    window.getSelection().addRange(CopyRange);
    document.getElementById("more_storage_vlans").style.display = "none";
    document.getElementById("more_nfs_volumes").style.display = "none";
    var command = document.execCommand("copy");
    if (command)
    {
        document.getElementById("copy-button").innerHTML = "Copied!";
        setTimeout(revert_copy, 3000);
    }
    window.getSelection().removeRange(CopyRange);
    if(currentRange)
    {
        window.getSelection().addRange(currentRange);
    }
}
function revert_copy() {
    document.getElementById("copy-button").innerHTML = "Copy";
    document.getElementById("more_storage_vlans").style.display =
"block";
    document.getElementById("more_nfs_volumes").style.display = "block";
}
function storagevlandropdown() {
    document.getElementById("more_storage_vlans").style.display = "none";
    document.getElementById("more_storage_vlans_button").style.display =

```

```

"block";
    var x=1;
    var myHTML = '';
    var buildup = '';
    var wrapper = document.getElementById("select_more_storage_vlans");
    while (x < 10) {
        buildup += '<option value="' + x + '">' + x + '</option>';
        x++;
    }
    myHTML += '<a id="more_storage_vlans_info">How many extra VLANs do you
wish to add?</a><select name="number_of_extra_storage_vlans"
id="number_of_extra_storage_vlans">' + buildup + '</select>';
    wrapper.innerHTML = myHTML;
}
function addstoragevlans() {
    var y =
document.getElementById("number_of_extra_storage_vlans").value;
    var j=0;
    var myHTML = '';
    var wrapper = document.getElementById("extra_storage_vlans");
    while (j < y) {
        j++;
        myHTML += ' - {vlan_id: ""<span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>203</i></span>", name: ""<span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>infra_NFS</i></span>",
protocol: ""<span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"><i>NFS</i></span>"}<br>';
    }
    wrapper.innerHTML = myHTML;
    document.getElementById("select_more_storage_vlans").style.display =
"none";
    document.getElementById("more_storage_vlans_button").style.display =
"none";
}
function nfsvolumesdropdown() {
    document.getElementById("more_nfs_volumes").style.display = "none";
    document.getElementById("more_nfs_volumes_button").style.display =
"block";
    var x=1;
    var myHTML = '';
    var buildup = '';
    var wrapper = document.getElementById("select_more_nfs_volumes");
    while (x < 100) {

```

```

        buildup += '<option value="' + x + '">' + x + '</option>';
        x++;
    }
    myHTML += '<a id="more_nfs_volumes_info">How many extra NFS volumes do
you wish to add?</a><select name="number_of_extra_nfs_volumes"
id="number_of_extra_nfs_volumes">' + buildup + '</select>';
    wrapper.innerHTML = myHTML;
}

function addnfsvolumes() {
    var y = document.getElementById("number_of_extra_nfs_volumes").value;
    var j=0;
    var myHTML = '';
    var wrapper = document.getElementById("extra_nfs_volumes");
    while (j < y) {
        j++;
        myHTML += ' - {vol_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>rtpora04_u01</i></span>, aggr_name: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>aggr01_node02</i></span>,
lif: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>172.21.94.201</i></span>, size: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>25</i></span>}<br>';
    }
    wrapper.innerHTML = myHTML;
    document.getElementById("select_more_nfs_volumes").style.display =
"none";
    document.getElementById("more_nfs_volumes_button").style.display =
"none";
}

</script>

```

1. Fill in all variables in blue fields.
2. After completing variables input, click the Copy button on the form to copy all variables to be transferred to AWX or Tower into the following job template.

## 5. Configure and launch the job template.

1. Create the job template.
  - a. Navigate to Resources → Templates → Add and click Add Job Template.
  - b. Enter the name and description
  - c. Select the Job type; Run configures the system based on a playbook, and Check performs a dry run of a playbook without actually configuring the system.

- d. Select the corresponding inventory, project, playbook, and credentials for the playbook.
  - e. Select the all\_playbook.yml as the default playbook to be executed.
  - f. Paste global variables copied from step 4 into the Template Variables field under the YAML tab.
  - g. Check the box Prompt on Launch in the Job Tags field.
  - h. Click Save.
2. Launch the job template.
- a. Navigate to Resources → Templates.
  - b. Click the desired template and then click Launch.
  - c. When prompted on launch for Job Tags, type in requirements\_config. You might need to click the Create Job Tag line below requirements\_config to enter the job tag.
-  requirements\_config ensures that you have the correct libraries to run the other roles.
- d. Click Next and then Launch to start the job.
  - e. Click View → Jobs to monitor the job output and progress.
  - f. When prompted on launch for Job Tags, type in ontap\_config. You might need to click the Create "Job Tag" line right below ontap\_config to enter the job tag.
  - g. Click Next and then Launch to start the job.
  - h. Click View → Jobs to monitor the job output and progress
  - i. After the ontap\_config role has completed, run the process again for linux\_config.
  - j. Navigate to Resources → Templates.
  - k. Select the desired template and then click Launch.
  - l. When prompted on launch for the Job Tags type in linux\_config, you might need to select the Create "job tag" line right below linux\_config to enter the job tag.
  - m. Click Next and then Launch to start the job.
  - n. Select View → Jobs to monitor the job output and progress.
  - o. After the linux\_config role has completed, run the process again for oracle\_config.
  - p. Go to Resources → Templates.
  - q. Select the desired template and then click Launch.
  - r. When prompted on launch for Job Tags, type oracle\_config. You might need to select the Create "Job Tag" line right below oracle\_config to enter the job tag.
  - s. Click Next and then Launch to start the job.
  - t. Select View → Jobs to monitor the job output and progress.

## 6. Deploy additional database on same Oracle host

The Oracle portion of the playbook creates a single Oracle container database on an Oracle server per execution. To create additional container databases on the same server, complete the following steps.

1. Revise host\_vars variables.
  - a. Go back to step 2 - Configure Oracle host\_vars.
  - b. Change the Oracle SID to a different naming string.

- c. Change the listener port to different number.
  - d. Change the EM Express port to a different number if you are installing EM Express.
  - e. Copy and paste the revised host variables to the Oracle Host Variables field in the Host Configuration Detail tab.
2. Launch the deployment job template with only the oracle\_config tag.

### Validate Oracle installation

1. Log in to Oracle server as oracle user and execute the following commands:

```
ps -ef | grep ora
```



This will list oracle processes if installation completed as expected and oracle DB started

2. Log in to the database to check the db configuration settings and the PDBs created with the following command sets.

```
sqlplus / as sysdba
```

```
[oracle@localhost ~]$ sqlplus / as sysdba
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Thu May 6 12:52:51 2021
Version 19.8.0.0.0
```

```
Copyright (c) 1982, 2019, Oracle. All rights reserved.
```

```
Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0
```

```
SQL>
```

```
select name, log_mode from v$database;
```

```
SQL> select name, log_mode from v$database;
NAME LOG_MODE
-----
```

```
CDB2 ARCHIVELOG
```

```
show pdbs;
```

```
SQL> show pdbs
```

CON_ID	CON_NAME	OPEN	MODE	RESTRICTED
2	PDB\$SEED	READ ONLY	NO	
3	CDB2_PDB1	READ WRITE	NO	
4	CDB2_PDB2	READ WRITE	NO	
5	CDB2_PDB3	READ WRITE	NO	

```
col svrname form a30
col dirname form a30
select svrname, dirname, nfsversion from v$dnfs_servers;
```

```
SQL> col svrname form a30
SQL> col dirname form a30
SQL> select svrname, dirname, nfsversion from v$dnfs_servers;
```

SVRNAME DIRNAME NFSVERSION

```
-----  
172.21.126.200 /rhelora03_u02 NFSv3.0  
172.21.126.200 /rhelora03_u03 NFSv3.0  
172.21.126.200 /rhelora03_u01 NFSv3.0
```

This confirms that dNFS is working properly.

3. Connect to database via listener to check the Oracle listener configuration with the following command. Change to the appropriate listener port and database service name.

```
sqlplus system@//localhost:1523/cdb2_pdb1.cie.netapp.com
```

```
[oracle@localhost ~]$ sqlplus system@//localhost:1523/cdb2_pdb1.cie.netapp.com
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Thu May 6 13:19:57 2021
Version 19.8.0.0.0
```

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Enter password:

Last Successful login time: Wed May 05 2021 17:11:11 -04:00

Connected to:

Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0

```
SQL> show user
USER is "SYSTEM"
SQL> show con_name
CON_NAME
CDB2_PDB1
```

This confirms that Oracle listener is working properly.

## Where to go for help?

If you need help with the toolkit, please join the [NetApp Solution Automation community support slack channel](#) and look for the solution-automation channel to post your questions or inquiries.

### Step-by-step deployment procedure

#### CLI deployment Oracle 19c Database

This section covers the steps required to prepare and deploy Oracle19c Database with the CLI. Make sure that you have reviewed the [Getting Started and Requirements section](#) and prepared your environment accordingly.

#### Download Oracle19c repo

1. From your ansible controller, run the following command:

```
git clone https://github.com/NetApp-Automation/na_oracle19c_deploy.git
```

2. After downloading the repository, change directories to na\_oracle19c\_deploy <cd na\_oracle19c\_deploy>.

#### Edit the hosts file

Complete the following before deployment:

1. Edit your hosts file na\_oracle19c\_deploy directory.
2. Under [ontap], change the IP address to your cluster management IP.
3. Under the [oracle] group, add the oracle hosts names. The host name must be resolved to its IP address either through DNS or the hosts file, or it must be specified in the host.
4. After you have completed these steps, save any changes.

The following example depicts a host file:

```
#ONTAP Host<div>
[ontap]
<div>
<span <div contenteditable="false" style="color:#7EAF97
; font-weight:bold; font-style:italic; text-
decoration:;"/>10.61.184.183<i></i></span>
</div>
#Oracle hosts<div>
<div>
[oracle]<div>
<span <div contenteditable="false" style="color:#7EAF97
; font-weight:bold; font-style:italic; text-
decoration:;"/>rtpora01<i></i></span>
<div>
<span <div contenteditable="false" style="color:#7EAF97
; font-weight:bold; font-style:italic; text-
decoration:;"/>rtpora02<i></i></span>
</div>
```

This example executes the playbook and deploys oracle 19c on two oracle DB servers concurrently. You can also test with just one DB server. In that case, you only need to configure one host variable file.



The playbook executes the same way regardless of how many Oracle hosts and databases you deploy.

### Edit the host\_name.yml file under host\_vars

Each Oracle host has its host variable file identified by its host name that contains host-specific variables. You can specify any name for your host. Edit and copy the host\_vars from the Host VARS Config section and paste it into your desired host\_name.yml file.



The items in blue must be changed to match your environment.

### Host VARS Config

```
<style>
div {
position: relative;
}
div button {
position: absolute;
top: 0;
right: 0;
}
button {
```

```

transition-duration: 0.4s;
background-color: white;
color: #1563a3;
border: 2px solid #1563a3;
}
button:hover {
background-color: #1563a3;
color: white;
}
#more_datastores_nfs {
display: block;
}
#more_datastores_nfs_button {
display: none;
}
</style>
<div class="listingblock"><div class="content"><div><button id="copy-
button1" onclick="CopyClassText1()">Copy</button></div><pre><code><div
class="CopyMeClass1" id="CopyMeID1">
#####
#####          Host Variables Configuration          #####
#####
# Add your Oracle Host
ansible_host: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>10.61.180.15</i></span>

# Oracle db log archive mode: true - ARCHIVELOG or false - NOARCHIVELOG
log_archive_mode: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>true</i></span>

# Number of pluggable databases per container instance identified by sid.
Pdb_name specifies the prefix for container database naming in this case
cdb2_pdb1, cdb2_pdb2, cdb2_pdb3
oracle_sid: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>cdb2</i></span>
pdb_num: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>3</i></span>
pdb_name: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>"{{ oracle_sid }}_pdb"</i></span>

```

```

# CDB listener port, use different listener port for additional CDB on
same host
listener_port: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>1523</i></span>

# CDB is created with SGA at 75% of memory_limit, MB. Consider how many
databases to be hosted on the node and how much ram to be allocated to
each DB. The grand total SGA should not exceed 75% available RAM on node.
memory_limit: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>5464</i></span>

# Set "em_configuration: DBEXPRESS" to install enterprise manager express
and choose a unique port from 5500 to 5599 for each sid on the host.
# Leave them black if em express is not installed.
em_configuration: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>DBEXPRESS</i></span>
em_express_port: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>5501</i></span>

# "{{groups.oracle[0]}}" represents first Oracle DB server as defined in
Oracle hosts group [oracle]. For concurrent multiple Oracle DB servers
deployment, [0] will be incremented for each additional DB server. For
example, "{{groups.oracle[1]}}" represents DB server 2,
"{{groups.oracle[2]}}" represents DB server 3 ... As a good practice and
the default, minimum three volumes is allocated to a DB server with
corresponding /u01, /u02, /u03 mount points, which store oracle binary,
oracle data, and oracle recovery files respectively. Additional volumes
can be added by click on "More NFS volumes" but the number of volumes
allocated to a DB server must match with what is defined in global vars
file by volumes_nfs parameter, which dictates how many volumes are to be
created for each DB server.
host_datastores_nfs:
  - {vol_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>{{groups.oracle[0]}}_u01</i></span>",
    aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>aggr01_node01</i></span>, lif: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>172.21.94.200</i></span>,
    size: <span <div contenteditable="true"/><i>25</i></span>}
  - {vol_name: ""<span <div contenteditable="true"

```

```

style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"/><i>{{groups.oracle[0]}}_u02</i></span>" ,
aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"/><i>aggr01_node01</i></span>, lif: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"/><i>172.21.94.200</i></span>,
size: <span <div contenteditable="true"/><i>25</i></span>
- {vol_name: ""<span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"/><i>{{groups.oracle[0]}}_u03</i></span>" ,
aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"/><i>aggr01_node01</i></span>, lif: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"/><i>172.21.94.200</i></span>,
size: <span <div contenteditable="true"/><i>25</i></span>}
<a id="more_datastores_nfs" href="javascript:datastoredropdown();">More NFS volumes</a><div id="select_more_datastores_nfs"></div><a id="more_datastores_nfs_button"
href="javascript:adddatastorevolumes();">Enter NFS volumes' details</a><div id="extra_datastores_nfs"></div>
</div></code></pre></div>
<script>
function CopyClassText1() {
    var textToCopy = document.getElementById("CopyMeID1");
    var currentRange;
    if(document.getSelection().rangeCount > 0)
    {
        currentRange = document.getSelection().getRangeAt(0);
        window.getSelection().removeRange(currentRange);
    }
    else
    {
        currentRange = false;
    }
    var CopyRange = document.createRange();
    CopyRange.selectNode(textToCopy);
    window.getSelection().addRange(CopyRange);
    document.getElementById("more_datastores_nfs").style.display = "none";
    var command = document.execCommand("copy");
    if (command)
    {
        document.getElementById("copy-button1").innerHTML = "Copied!";
        setTimeout(revert_copy, 3000);
    }
}

```

```

        window.getSelection().removeRange(CopyRange);
        if(currentRange)
        {
            window.getSelection().addRange(currentRange);
        }
    }

function revert_copy() {
    document.getElementById("copy-button1").innerHTML = "Copy";
    document.getElementById("more_datastores_nfs").style.display =
"block";
}

function datastoredropdown() {
    document.getElementById("more_datastores_nfs").style.display = "none";
    document.getElementById("more_datastores_nfs_button").style.display =
"block";
    var x=1;
    var myHTML = '';
    var buildup = '';
    var wrapper = document.getElementById("select_more_datastores_nfs");
    while (x < 100) {
        buildup += '<option value="' + x + '">' + x + '</option>';
        x++;
    }
    myHTML += '<a id="more_datastores_nfs">How many extra NFS volumes do
you wish to add?</a><select name="number_of_extra_datastores_nfs"
id="number_of_extra_datastores_nfs">' + buildup + '</select>';
    wrapper.innerHTML = myHTML;
}

function adddatastorevolumes() {
    var y =
document.getElementById("number_of_extra_datastores_nfs").value;
    var j=0;
    var myHTML = '';
    var wrapper = document.getElementById("extra_datastores_nfs");
    while (j < y) {
        j++;
        myHTML += ' - {vol_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>{{groups.oracle[0]}}_u01</i></span>,
aggr_name: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline;"><i>aggr01_node02</i></span>, lif: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>172.21.94.201</i></span>,
size: <span <div contenteditable="true" style="color:#004EFF; font-

```

```

        weight:bold; font-style:italic; text-
        decoration:underline;" /><i>25</i></span>}<br>';
    }
    wrapper.innerHTML = myHTML;
    document.getElementById("select_more_datastores_nfs").style.display =
    "none";
    document.getElementById("more_datastores_nfs_button").style.display =
    "none";
}

</script>

```

## Edit the vars.yml file

The `vars.yml` file consolidates all environment-specific variables (ONTAP, Linux, or Oracle) for Oracle deployment.

- Edit and copy the variables from the VARS section and paste these variables into your `vars.yml` file.

## VARS

```

<style>
div {
position: relative;
}
div button {
position: absolute;
top: 0;
right: 0;
}
button {
transition-duration: 0.4s;
background-color: white;
color: #1563a3;
border: 2px solid #1563a3;
}
button:hover {
background-color: #1563a3;
color: white;
}
#more_storage_vlans {
display: block;
}
#more_storage_vlans_button {
display: none;
}

```

```

#more_nfs_volumes {
    display: block;
}
#more_nfs_volumes_button {
    display: none;
}
</style>
<div class="listingblock"><div class="content"><div><button id="copy-
button" onclick="CopyClassText()">Copy</button></div><pre><code><div
class="CopyMeClass" id="CopyMeID">
#####
##### Oracle 19c deployment global user configuration variables #####
##### Consolidate all variables from ontap, linux and oracle #####
#####

#####
### Ontap env specific config variables ##
#####

#Inventory group name
#Default inventory group name - 'ontap'
#Change only if you are changing the group name either in inventory/hosts
file or in inventory groups in case of AWX/Tower
hosts_group: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>ontap</i></span>

#CA_signed_certificates (ONLY CHANGE to 'true' IF YOU ARE USING CA SIGNED
CERTIFICATES)
ca_signed_certs: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-decoration:underline; text-
decoration:underline;"><i>false</i></span>

#Names of the Nodes in the ONTAP Cluster
nodes:
    - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline;"><i>AFF-
01</i></span>
    - <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-decoration:underline;"><i>AFF-
02</i></span>

#Storage VLANs
#Add additional rows for vlans as necessary
storage_vlans:

```

```

- {vlan_id: ""<span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>203</i></span>", name: ""<span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"/><i>infra_NFS</i></span>", protocol: ""<span <div
contenteditable="true"/><i>NFS</i></span>" }

<a id="more_storage_vlans" href="javascript:storagevlandropdown();">More
Storage VLANs</a><div id="select_more_storage_vlans"></div><a
id="more_storage_vlans_button" href="javascript:addstoragevlans();">Enter
Storage VLANs details</a><div id="extra_storage_vlans"></div>

#Details of the Data Aggregates that need to be created
#If Aggregate creation takes longer, subsequent tasks of creating volumes
may fail.

#There should be enough disks already zeroed in the cluster, otherwise
aggregate create will zero the disks and will take long time
data_aggregates:
- {aggr_name: "<span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>aggr01_node01</i></span>"}
- {aggr_name: "<span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>aggr01_node02</i></span>"}

#SVM name
svm_name: "<span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"/><i>ora_svm</i></span>"

# SVM Management LIF Details
svm_mgmt_details:
- {address: "<span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>172.21.91.100</i></span>, netmask: "<span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"/><i>255.255.255.0</i></span>,
home_port: "<span <div contenteditable="true"/><i>e0M</i></span>"}

# NFS storage parameters when data_protocol set to NFS. Volume named after
Oracle hosts name identified by mount point as follow for oracle DB server
1. Each mount point dedicated to a particular Oracle files: u01 - Oracle
binary, u02 - Oracle data, u03 - Oracle redo. Add additional volumes by
click on "More NFS volumes" and also add the volumes list to corresponding
host_vars as host_datastores_nfs variable. For multiple DB server

```

deployment, additional volumes sets needs to be added for additional DB server. Input variable "{{groups.oracle[1]}}\_u01", "{{groups.oracle[1]}}\_u02", and "{{groups.oracle[1]}}\_u03" as vol\_name for second DB server. Place volumes for multiple DB servers alternatingly between controllers for balanced IO performance, e.g. DB server 1 on controller node1, DB server 2 on controller node2 etc. Make sure match lif address with controller node.

volumes\_nfs:

- {vol\_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>{{groups.oracle[0]}}\_u01</i></span>", aggr\_name: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>aggr01\_node01</i></span>, lif: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>172.21.94.200</i></span>, size: <span <div contenteditable='true'><i>25</i></span>}"}
- {vol\_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>{{groups.oracle[0]}}\_u02</i></span>", aggr\_name: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>aggr01\_node01</i></span>, lif: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>172.21.94.200</i></span>, size: <span <div contenteditable='true'><i>25</i></span>}"}
- {vol\_name: ""<span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>{{groups.oracle[0]}}\_u03</i></span>", aggr\_name: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>aggr01\_node01</i></span>, lif: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>172.21.94.200</i></span>, size: <span <div contenteditable='true'><i>25</i></span>}"}

<a id="more\_nfs\_volumes" href="javascript:nfsvolumesdropdown();">More NFS volumes</a><div id="select\_more\_nfs\_volumes"></div><a id="more\_nfs\_volumes\_button" href="javascript:addnfsvolumes();">Enter NFS volumes' details</a><div id="extra\_nfs\_volumes"></div>

#NFS LIFs IP address and netmask

nfs\_lifs\_details:

- address: <span <div contenteditable='true' style='color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;'><i>172.21.94.200</i></span> #for node-1
- netmask: <span <div contenteditable='true' style='color:#004EFF; font-

```

weight:bold; font-style:italic; text-
decoration:underline;"/><i>255.255.255.0</i></span>
- address: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"/><i>172.21.94.201</i></span> #for node-2
    netmask: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"/><i>255.255.255.0</i></span>

#NFS client match
client_match: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>172.21.94.0/24</i></span>

#####
### Linux env specific config variables ###
#####

#NFS Mount points for Oracle DB volumes
mount_points:
- <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"/><i>/u01</i></span>
- <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"/><i>/u02</i></span>
- <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"/><i>/u03</i></span>

# Up to 75% of node memory size divided by 2mb. Consider how many
databases to be hosted on the node and how much ram to be allocated to
each DB.
# Leave it blank if hugepage is not configured on the host.
hugepages_nr: <span <div contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>1234</i></span>

# RedHat subscription username and password
redhat_sub_username: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>xxx</i></span>
redhat_sub_password: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"/><i>xxx</i></span>

```

```

#####
### DB env specific install and config variables #####
#####

db_domain: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>your.domain.com</i></span>

# Set initial password for all required Oracle passwords. Change them after installation.
initial_pwd_all: <span <div contenteditable="true" style="color:#004EFF; font-weight:bold; font-style:italic; text-decoration:underline;"><i>netapp123</i></span>

</div></code></pre></div></div>
<script>
function CopyClassText() {
    var textToCopy = document.getElementById("CopyMeID");
    var currentRange;
    if(document.getSelection().rangeCount > 0)
    {
        currentRange = document.getSelection().getRangeAt(0);
        window.getSelection().removeRange(currentRange);
    }
    else
    {
        currentRange = false;
    }
    var CopyRange = document.createRange();
    CopyRange.selectNode(textToCopy);
    window.getSelection().addRange(CopyRange);
    document.getElementById("more_storage_vlans").style.display = "none";
    document.getElementById("more_nfs_volumes").style.display = "none";
    var command = document.execCommand("copy");
    if (command)
    {
        document.getElementById("copy-button").innerHTML = "Copied!";
        setTimeout(revert_copy, 3000);
    }
    window.getSelection().removeRange(CopyRange);
    if(currentRange)
    {
        window.getSelection().addRange(currentRange);
    }
}
function revert_copy() {

```

```

        document.getElementById("copy-button").innerHTML = "Copy";
        document.getElementById("more_storage_vlans").style.display =
"block";
        document.getElementById("more_nfs_volumes").style.display = "block";
    }
    function storagevlandropdown() {
        document.getElementById("more_storage_vlans").style.display = "none";
        document.getElementById("more_storage_vlans_button").style.display =
"block";
        var x=1;
        var myHTML = '';
        var buildup = '';
        var wrapper = document.getElementById("select_more_storage_vlans");
        while (x < 10) {
            buildup += '<option value="' + x + '">' + x + '</option>';
            x++;
        }
        myHTML += '<a id="more_storage_vlans_info">How many extra VLANs do you
wish to add?</a><select name="number_of_extra_storage_vlans"
id="number_of_extra_storage_vlans">' + buildup + '</select>';
        wrapper.innerHTML = myHTML;
    }
    function addstoragevlans() {
        var y =
document.getElementById("number_of_extra_storage_vlans").value;
        var j=0;
        var myHTML = '';
        var wrapper = document.getElementById("extra_storage_vlans");
        while (j < y) {
            j++;
            myHTML += ' - {vlan_id: ""<span contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>203</i></span>", name: ""<span contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>infra_NFS</i></span>", protocol:
"&quot;<span contenteditable="true" style="color:#004EFF;
font-weight:bold; font-style:italic; text-
decoration:underline;"><i>NFS</i></span>&quot;}<br>';
        }
        wrapper.innerHTML = myHTML;
        document.getElementById("select_more_storage_vlans").style.display =
"none";
        document.getElementById("more_storage_vlans_button").style.display =
"none";
    }
    function nfsvolumesdropdown() {

```

```

document.getElementById("more_nfs_volumes").style.display = "none";
document.getElementById("more_nfs_volumes_button").style.display =
"block";
var x=1;
var myHTML = '';
var buildup = '';
var wrapper = document.getElementById("select_more_nfs_volumes");
while (x < 100) {
    buildup += '<option value="' + x + '">' + x + '</option>';
    x++;
}
myHTML += '<a id="more_nfs_volumes_info">How many extra NFS volumes do
you wish to add?</a><select name="number_of_extra_nfs_volumes"
id="number_of_extra_nfs_volumes">' + buildup + '</select>';
wrapper.innerHTML = myHTML;
}

function addnfsvolumes() {
var y = document.getElementById("number_of_extra_nfs_volumes").value;
var j=0;
var myHTML = '';
var wrapper = document.getElementById("extra_nfs_volumes");
while (j < y) {
    j++;
    myHTML += ' - {vol_name: <span <div contenteditable="true"
style="color:#004EFF; font-weight:bold; font-style:italic; text-
decoration:underline;"><i>rtpora04_u01</i></span>, aggr_name: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>aggr01_node02</i></span>,
lif: <span <div contenteditable="true" style="color:#004EFF; font-
weight:bold; font-style:italic; text-
decoration:underline;"><i>172.21.94.201</i></span>, size: <span <div
contenteditable="true" style="color:#004EFF; font-weight:bold; font-
style:italic; text-decoration:underline;"><i>25</i></span>}<br>';
}
wrapper.innerHTML = myHTML;
document.getElementById("select_more_nfs_volumes").style.display =
"none";
document.getElementById("more_nfs_volumes_button").style.display =
"none";
}

</script>

```

## Run the playbook

After completing the required environment prerequisites and copying the variables into `vars.yml` and

`your_host.yml`, you are now ready to deploy the playbooks.



<username> must be changed to match your environment.

1. Run the ONTAP playbook by passing the correct tags and ONTAP cluster username. Fill the password for ONTAP cluster, and vsadmin when prompted.

```
ansible-playbook -i hosts all_playbook.yml -u username -k -K -t  
ontap_config -e @vars/vars.yml
```

2. Run the Linux playbook to execute Linux portion of deployment. Input for admin ssh password as well as sudo password.

```
ansible-playbook -i hosts all_playbook.yml -u username -k -K -t  
linux_config -e @vars/vars.yml
```

3. Run the Oracle playbook to execute Oracle portion of deployment. Input for admin ssh password as well as sudo password.

```
ansible-playbook -i hosts all_playbook.yml -u username -k -K -t  
oracle_config -e @vars/vars.yml
```

## Deploy Additional Database on Same Oracle Host

The Oracle portion of the playbook creates a single Oracle container database on an Oracle server per execution. To create additional container database on the same server, complete the following steps:

1. Revise the `host_vars` variables.
  - a. Go back to step 3 - Edit the `host_name.yml` file under `host_vars`.
  - b. Change the Oracle SID to a different naming string.
  - c. Change the listener port to different number.
  - d. Change the EM Express port to a different number if you have installed EM Express.
  - e. Copy and paste the revised host variables to the Oracle host variable file under `host_vars`.
2. Execute the playbook with the `oracle_config` tag as shown above in [Run the playbook](#).

## Validate Oracle installation

1. Log in to Oracle server as oracle user and execute the following commands:

```
ps -ef | grep ora
```



This will list oracle processes if installation completed as expected and oracle DB started

2. Log in to the database to check the db configuration settings and the PDBs created with the following command sets.

```
sqlplus / as sysdba
```

```
[oracle@localhost ~]$ sqlplus / as sysdba
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Thu May 6 12:52:51 2021
Version 19.8.0.0.0
```

```
Copyright (c) 1982, 2019, Oracle. All rights reserved.
```

```
Connected to:
```

```
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0
```

```
SQL>
```

```
select name, log_mode from v$database;
```

```
SQL> select name, log_mode from v$database;
NAME LOG_MODE
-----
```

```
CDB2 ARCHIVELOG
```

```
show pdbs;
```

```
SQL> show pdbs
```

CON_ID	CON_NAME	OPEN	MODE	RESTRICTED
2	PDB\$SEED	READ	ONLY	NO
3	CDB2_PDB1	READ	WRITE	NO
4	CDB2_PDB2	READ	WRITE	NO
5	CDB2_PDB3	READ	WRITE	NO

```
col svrname form a30
col dirname form a30
select svrname, dirname, nfsversion from v$dnfs_servers;
```

SQL> col svrname form a30  
SQL> col dirname form a30  
SQL> select svrname, dirname, nfsversion from v\$dnfs\_servers;

SVRNAME DIRNAME NFSVERSION

```
-----  

172.21.126.200 /rhelora03_u02 NFSv3.0  

172.21.126.200 /rhelora03_u03 NFSv3.0  

172.21.126.200 /rhelora03_u01 NFSv3.0
```

This confirms that dNFS is working properly.

3. Connect to database via listener to check the Oracle listener configuration with the following command. Change to the appropriate listener port and database service name.

```
sqlplus system@//localhost:1523/cdb2_pdb1.cie.netapp.com
```

[oracle@localhost ~]\$ sqlplus system@//localhost:1523/cdb2\_pdb1.cie.netapp.com

SQL\*Plus: Release 19.0.0.0.0 - Production on Thu May 6 13:19:57 2021  
Version 19.8.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Enter password:  
Last Successful login time: Wed May 05 2021 17:11:11 -04:00

Connected to:  
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production  
Version 19.8.0.0.0

SQL> show user

```
USER is "SYSTEM"
SQL> show con_name
CON_NAME
CDB2_PDB1
```

This confirms that Oracle listener is working properly.

## Where to go for help?

If you need help with the toolkit, please join the [NetApp Solution Automation community support slack channel](#) and look for the solution-automation channel to post your questions or inquiries.

# Oracle Database Data Protection

## Solution Overview

### Automated Data Protection for Oracle Databases

Organizations are automating their environments to gain efficiencies, accelerate deployments, and reduce manual effort. Configuration management tools like Ansible are being used to streamline enterprise database operations. In this solution, we demonstrate how you can use Ansible to automate the data protection of Oracle with NetApp ONTAP. By enabling storage administrators, systems administrators, and DBAs to consistently and rapidly setup data replication to an offsite data center or to public cloud, you achieve the following benefits:

- Eliminate design complexities and human errors, and implement a repeatable consistent deployment and best practices
- Decrease time for configuration of Intercluster replication, CVO instantiation, and recovery of Oracle databases
- Increase database administrators, systems and storage administrators productivity
- Provides database recovery workflow for ease of testing a DR scenario.

NetApp provides customers with validated Ansible modules and roles to accelerate deployment, configuration, and lifecycle management of your Oracle database environment. This solution provides instruction and Ansible playbook code, to help you:

### On Prem to on prem replication

- Create intercluster lifs on source and destination
- Establish cluster and vserver peering
- Create and initialize SnapMirror of Oracle volumes
- Create a replication schedule through AWX/Tower for Oracle binaries, databases, and logs
- Restore Oracle DB on the destination, and bring database online

### On Prem to CVO in AWS

- Create AWS connector
- Create CVO instance in AWS
- Add On-Prem cluster to Cloud Manager

- Create intercluster lifs on source
- Establish cluster and vserver peering
- Create and initialize SnapMirror of Oracle volumes
- Create a replication schedule through AWX/Tower for Oracle binaries, databases, and logs
- Restore Oracle DB on the destination, and bring database online

For more details or to begin, please see the overview videos below.

## **AWX/Tower Deployments**

- Part 1: TBD

**video**

- Part 2: TBD

**video**

After you are ready, click [here](#) for getting started with the solution.

## **Getting started**

This solution has been designed to be run in an AWX/Tower environment.

## **AWX/Tower**

For AWX/Tower environments, you are guided through creating an inventory of your ONTAP cluster management and Oracle server (IPs and hostnames), creating credentials, configuring a project that pulls the Ansible code from NetApp Automation Github, and the Job Template that launches the automation.

1. The solution has been designed to run in a private cloud scenario (on-premise to on-premise), and hybrid cloud (on-premise to public cloud Cloud Volumes ONTAP [CVO])
2. Fill out the variables specific to your environment, and copy and paste them into the Extra Vars fields in your job template.
3. After the extra vars have been added to your job template, you can launch the automation.
4. The automation is set to be ran three phases (Setup, Replication Schedule for Oracle Binaries, Database, Logs, and Replication Schedule just for Logs), and a forth phase to recovering the database at a DR site.
5. For detailed instructions for obtaining the keys and tokens necessary for the CVO Data Protection visit [Gather Pre-requisites For CVO and Connector Deployments](#)

## **Requirements**

## On-Prem |

Environment	Requirements
<b>Ansible environment</b>	AWX/Tower Ansible v.2.10 and higher Python 3 Python libraries - netapp-lib - xmltodict - jmespath
<b>ONTAP</b>	ONTAP version 9.8 + Two data aggregates NFS vlan and ifgrp created
<b>Oracle server(s)</b>	RHEL 7/8 Oracle Linux 7/8 Network interfaces for NFS, public, and optional mgmt Existing Oracle environment on source, and the equivalent Linux operating system at the destination (DR Site or Public Cloud)

## CVO

Environment	Requirements
<b>Ansible environment</b>	AWX/Tower Ansible v.2.10 and higher Python 3 Python libraries - netapp-lib - xmltodict - jmespath
<b>ONTAP</b>	ONTAP version 9.8 + Two data aggregates NFS vlan and ifgrp created
<b>Oracle server(s)</b>	RHEL 7/8 Oracle Linux 7/8 Network interfaces for NFS, public, and optional mgmt Existing Oracle environment on source, and the equivalent Linux operating system at the destination (DR Site or Public Cloud) Set appropriate swap space on the Oracle EC2 instance, by default some EC2 instances are deployed with 0 swap

Environment	Requirements
Cloud Manager/AWS	AWS Access/Secret Key
	NetApp Cloud Manager Account
	NetApp Cloud Manager Refresh Token

## Automation Details

## On-Prem |

This automated deployment is designed with a single Ansible playbook that consists of three separate roles. The roles are for ONTAP, Linux, and Oracle configurations. The following table describes which tasks are being automated.

Playbook	Tasks
ontap_setup	Pre-check of the ONTAP environment
	Creation of Intercluster LIFs on source cluster (OPTIONAL)
	Creation of Intercluster LIFs on destination cluster (OPTIONAL)
	Creation of Cluster and SVM Peering
	Creation of destination SnapMirror and Initialization of designated Oracle volumes
ora_replication_cg	Enable backup mode for each database in /etc/oratab
	Snapshot taken of Oracle Binary and Database volumes
	Snapmirror Updated
	Turn off backup mode for each database in /etc/oratab
ora_replication_log	Switch current log for each database in /etc/oratab
	Snapshot taken of Oracle Log volume
	Snapmirror Updated
ora_recovery	Break SnapMirror
	Enable NFS and create junction path for Oracle volumes on the destination
	Configure DR Oracle Host
	Mount and verify Oracle volumes
	Recover and start Oracle database

## CVO

This automated deployment is designed with a single Ansible playbook that consists of three separate roles. The roles are for ONTAP, Linux, and Oracle configurations. The following table describes which tasks are being automated.

Playbook	Tasks
cvo_setup	Pre-check of the environment AWS Configure/AWS Access Key ID/Secret Key/Default Region Creation of AWS Role Creation of NetApp Cloud Manager Connector instance in AWS Creation of Cloud Volumes ONTAP (CVO) instance in AWS Add On-Prem Source ONTAP Cluster to NetApp Cloud Manager Creation of destination SnapMirror and Initialization of designated Oracle volumes
ora_replication_cg	Enable backup mode for each database in /etc/oratab Snapshot taken of Oracle Binary and Database volumes Snapmirror Updated Turn off backup mode for each database in /etc/oratab
ora_replication_log	Switch current log for each database in /etc/oratab Snapshot taken of Oracle Log volume Snapmirror Updated
ora_recovery	Break SnapMirror Enable NFS and create junction path for Oracle volumes on the destination CVO Configure DR Oracle Host Mount and verify Oracle volumes Recover and start Oracle database

## Default parameters

To simplify automation, we have preset many required Oracle parameters with default values. It is generally not necessary to change the default parameters for most deployments. A more advanced user can make changes to the default parameters with caution. The default parameters are located in each role folder under defaults directory.

## License

You should read license information as stated in the Github repository. By accessing, downloading, installing, or using the content in this repository, you agree the terms of the license laid out [here](#).

Note that there are certain restrictions around producing and/or sharing any derivative works with the content in this repository. Please make sure you read the terms of the [License](#) before using the content. If you do not agree to all of the terms, do not access, download, or use the content in this repository.

After you are ready, click [here for detailed AWX/Tower procedures](#).

# Microsoft SQL Server

## TR-4897: SQL Server on Azure NetApp Files - Real Deployment View

Niyaz Mohamed, NetApp

IT organizations face constant change. Gartner reports nearly 75% of all databases will require cloud-based storage by 2022. As a leading relational database management system (RDBMS), Microsoft SQL Server is the go-to choice for Windows platform-designed applications and organizations that rely on SQL Server for everything from enterprise resource planning (ERP) to analytics to content management. SQL Server has helped to revolutionize the way enterprises manage massive data sets and power their applications to meet the schema and query performance demands.

Most IT organizations follow a cloud-first approach. Customers in a transformation phase evaluate their current IT landscape and then migrate their database workloads to the cloud based on an assessment and discovery exercise. Some factors driving customers toward cloud migration include elasticity/burst, data center exit, data center consolidation, end-of-life scenarios, mergers, acquisitions, and so on. The reason for migration can vary based on each organization and their respective business priorities. When moving to the cloud, choosing the right cloud storage is very important in order to unleash the power of SQL Server database cloud deployment.

### Use case

Moving the SQL Server estate to Azure and integrating SQL Server with Azure's vast array of platform-as-a-service (PaaS) features such as Azure Data Factory, Azure IoT Hub, and Azure Machine Learning creates tremendous business value to support digital transformation. Adopting the cloud also enables the respective business unit to focus on productivity and delivering new features and enhancements faster (Dev/Test use case) than relying on the CAPEX model or traditional private cloud models. This document covers a real-time deployment of SQL Server Always On availability group (AOAG) on Azure NetApp Files leveraging Azure Virtual Machines.

Azure NetApp Files provides enterprise-grade storage with continuously available file shares. Continuously available shares are required by SQL Server production databases on SMB file share to make sure that the node always has access to the database storage, including during disruptive scenarios such as controller upgrades or failures. Continuously available file shares eliminate the need to replicate data between storage nodes. Azure NetApp Files uses SMB 3.0 scale-out, persistent handles, and transparent failover to support nondisruptive operations (NDOs) for planned and unplanned downtime events, including many administrative tasks.

When planning cloud migrations, you should always evaluate the best approach to use. The most common and easiest approach for application migration is rehosting (also known as lift and shift). The example scenario provided in this document uses the rehosting method. SQL Server on Azure virtual machines with Azure NetApp Files allows you to use full versions of SQL Server in the cloud without having to manage on-premises hardware. SQL Server virtual machines (VMs) also simplify licensing costs when you pay as you go and provides elasticity and bursting capabilities for development, test, and estate refresh scenarios.

### Factors to consider

#### VM performance

Selecting the right VM size is important for optimal performance of a relational database in a public cloud. Microsoft recommends that you continue using the same database performance-tuning options that are applicable to SQL Server in on-premises server environments. Use [memory-optimized](#) VM sizes for the best performance of SQL Server workloads. Collect the performance data of existing deployment to identify the RAM and CPU utilization while choosing the right instances. Most deployments choose between the D, E, or M

series.

## Notes:

- For the best performance of SQL Server workloads, use memory-optimized VM sizes.
- NetApp and Microsoft recommend that you identify the storage performance requirements before choosing the instance type with the appropriate memory-to-vCore ratio. This also helps select a lower-instance type with the right network bandwidth to overcome storage throughput limits of the VM.

## VM redundancy

To increase redundancy and high availability, SQL Server VMs should either be in the same [availability set](#) or different [availability zones](#). When creating Azure VMs, you must choose between configuring availability sets versus availability zones; an Azure VM cannot participate in both.

## High availability

For high availability, configuring SQL Server AOAG or Always On Failover Cluster Instance (FCI) is the best option. For AOAG, this involves multiple instances of SQL Server on Azure Virtual Machines in a virtual network. If high availability is required at the database level, consider configuring SQL Server availability groups.

## Storage configuration

Microsoft SQL Server can be deployed with an SMB file share as the storage option. Starting with SQL Server 2012, system databases (master, model, msdb, or tempdb), and user databases can be installed with Server Message Block (SMB) file server as a storage option. This applies to both SQL Server stand-alone and SQL Server FCI.



File share storage for SQL Server databases should support continuously available property. This provides uninterrupted access to the file-share data.

Azure NetApp Files provides high performing file storage to meet any demanding workload, and it reduces SQL Server TCO as compared to block storage solutions. With block storage, VMs have imposed limits on I/O and bandwidth for disk operations; network bandwidth limits alone are applied against Azure NetApp Files. In other words, no VM-level I/O limits are applied to Azure NetApp Files. Without these I/O limits, SQL Server running on smaller VMs connected to Azure NetApp Files can perform as well as SQL Server running on much larger VMs. Azure NetApp Files reduce SQL Server deployment costs by reducing compute and software licensing costs. For detailed cost analysis and performance benefits of using Azure NetApp Files for SQL Server deployment, see the [Benefits of using Azure NetApp Files for SQL Server deployment](#).

## Benefits

The benefits of using Azure NetApp Files for SQL Server include the following:

- Using Azure NetApp Files allows you to use smaller instances, thus reducing compute cost.
- Azure NetApp Files also reduces software licensing costs, which reduce the overall TCO.
- Volume reshaping and dynamic service level capability optimizes cost by sizing for steady-state workloads and avoiding overprovisioning.

## Notes:

- To increase redundancy and high availability, SQL Server VMs should either be in the same [availability set](#)

or in different [availability zones](#). Consider file path requirements if user-defined data files are required; in which case, select SQL FCI over SQL AOAG.

- The following UNC path is supported: `\ANFSMB-b4ca.anf.test\SQLDB` and `\ANFSMB-b4ca.anf.test\SQLDB\`.
- The loopback UNC path is not supported.
- For sizing, use historic data from your on-premises environment. For OLTP workloads, match the target IOPS with performance requirements using workloads at average and peak times along with the disk reads/sec and disk writes/sec performance counters. For data warehouse and reporting workloads, match the target throughput using workloads at average and peak times and the disk read bytes/sec and disk write bytes/sec. Average values can be used in conjunction with volume reshaping capabilities.

#### Create continuously available shares

Create continuously available shares with the Azure portal or Azure CLI. In the portal, select the Enable Continuous Availability property option. for the Azure CLI, specify the share as a continuously available share by using the `az netappfiles volume create` with the `smb-continuously-avl` option set to `$True`. To learn more about creating a new, continuous availability-enabled volume, see [Creating a Continuously Available Share](#).

#### Notes:

- Enable continuous availability for the SMB volume as shown in the following image.
- If a non-administrator domain account is used, make sure the account has the required security privilege assigned.
- Set the appropriate permissions at the share level and proper file-level permissions.
- A continuously available property cannot be enabled on existing SMB volumes. To convert an existing volume to use a continuously available share, use NetApp Snapshot technology. For more information, see [Convert existing SMB volumes to use Continuous Availability](#).

# Create a volume

X

Basics    **Protocol**    Tags    Review + create

Configure access to your volume.

## Access

Protocol type

NFS  SMB  Dual-protocol (NFSv3 and SMB)

## Configuration

Active Directory \* ⓘ

10.0.0.100 - anf.test/join



Share name \* ⓘ

SQLDB

Enable Continuous Availability ⓘ



**Review + create**

< Previous

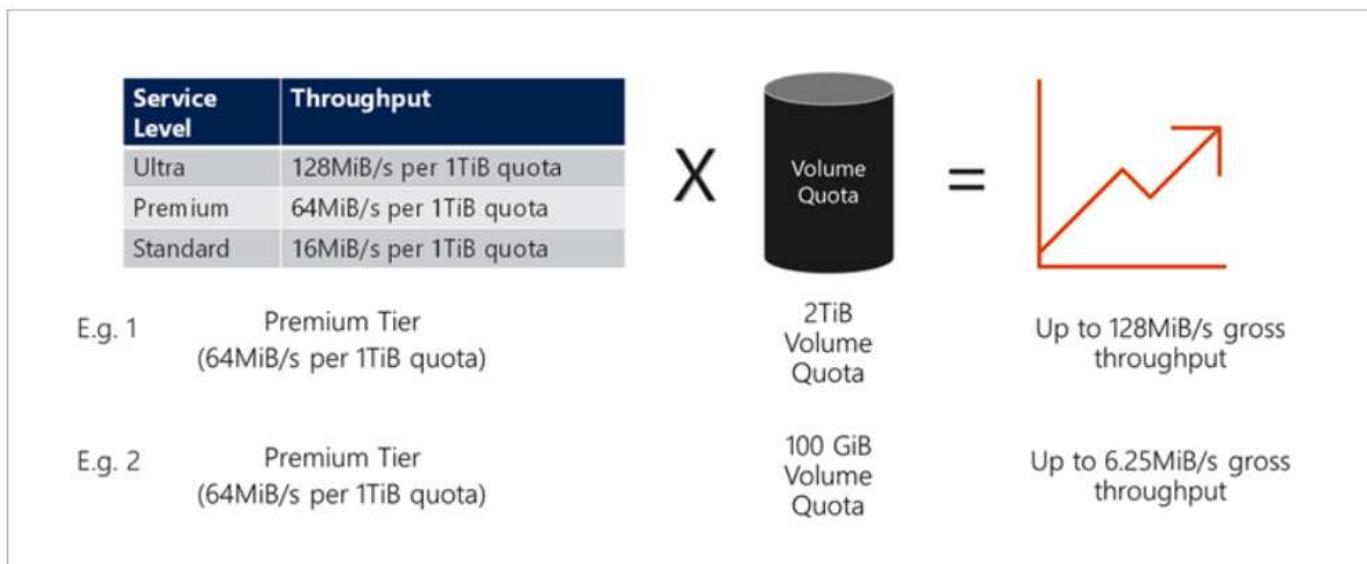
Next : Tags >

## Performance

Azure NetApp Files supports three service levels: Standard (16MBps per terabyte), Premium (64MBps per terabyte), and Ultra (128MBps per terabyte). Provisioning the right volume size is important for optimal performance of the database workload. With Azure NetApp Files, volume performance and the throughput limit are based on a combination of the following factors:

- The service level of the capacity pool to which the volume belongs
- The quota assigned to the volume
- The quality of service (QoS) type (auto or manual) of the capacity pool

For more information, see [Service levels for Azure NetApp Files](#).



### Performance validation

As with any deployment, testing the VM and storage is critical. For storage validation, tools such as HammerDB, Apploader, the [SQL Server storage benchmark \(SB\) tool](#), or any custom script or FIO with the appropriate read/write mix should be used. Keep in mind however that most SQL Server workloads, even busy OLTP workloads, are closer to 80%–90% read and 10%–20% write.

To showcase performance, a quick test was performed against a volume using premium service levels. In this test, the volume size was increased from 100GB to 2TB on the fly without any disruption to application access and zero data migration.



Here is another example of real time performance testing with HammerDB performed for the deployment covered in this paper. For this testing, we used a small instance with eight vCPUs, a 500GB Premium SSD, and a 500GB SMB Azure NetApp Files volume. HammerDB was configured with 80 warehouses and eight

users.

The following chart shows that Azure NetApp Files was able to deliver 2.6x the number of transactions per minute at 4x lower latency when using a comparable sized volume (500GB).

An additional test was performed by resizing to a larger instance with 32x vCPUs and a 16TB Azure NetApp Files volume. There was a significant increase in transactions per minute with consistent 1ms latency. HammerDB was configured with 80 warehouses and 64 users for this test.



### Cost optimization

Azure NetApp Files allows nondisruptive, transparent volume resizing and the ability to change the service levels with zero downtime and no effect on applications. This is a unique capability allowing dynamic cost management that avoids the need to perform database sizing with peak metrics. Rather, you can use steady state workloads, which avoids upfront costs. The volume reshaping and dynamic service-level change allows you to adjust the bandwidth and service level of Azure NetApp Files volumes on demand almost instantaneously without pausing I/O, while retaining data access.

Azure PaaS offerings such as LogicApp or Functions can be used to easily resize the volume based on a specific webhook or alert rule trigger to meet the workload demands while dynamically handling the cost.

For example, consider a database that needs 250MBps for steady state operation; however, it also requires a peak throughput of 400MBps. In this case, the deployment should be performed with a 4TB volume within the Premium service level to meet the steady-state performance requirements. To handle the peak workload, increase the volume size using Azure functions to 7TB for that specific period, and then downsize the volume to make the deployment cost effective. This configuration avoids overprovisioning of the storage.

### Real-time, high-level reference design

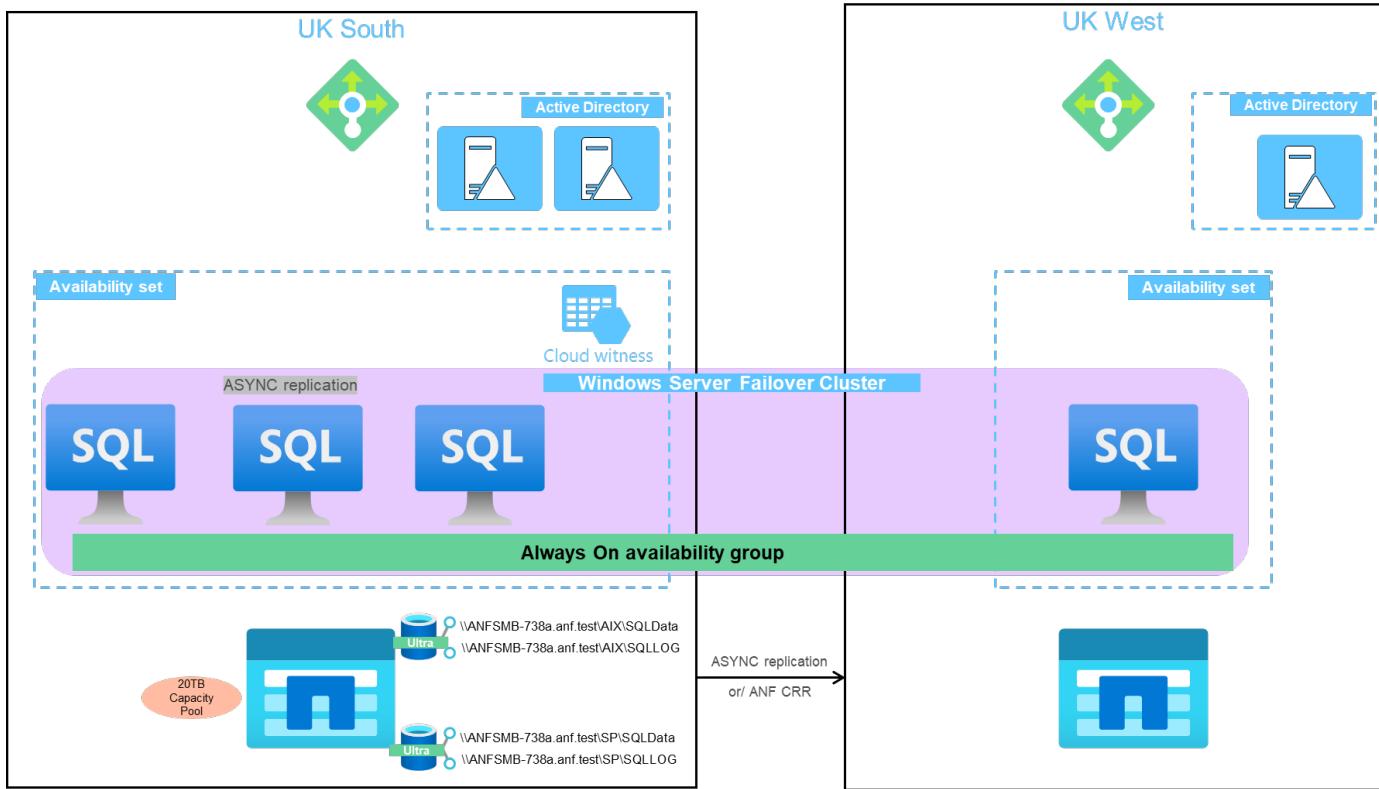
This section covers a real-time deployment of a SQL database estate in an AOAG configuration using an Azure NetApp Files SMB volume.

- Number of nodes: 4
- Number of databases: 21
- Number of availability groups: 4

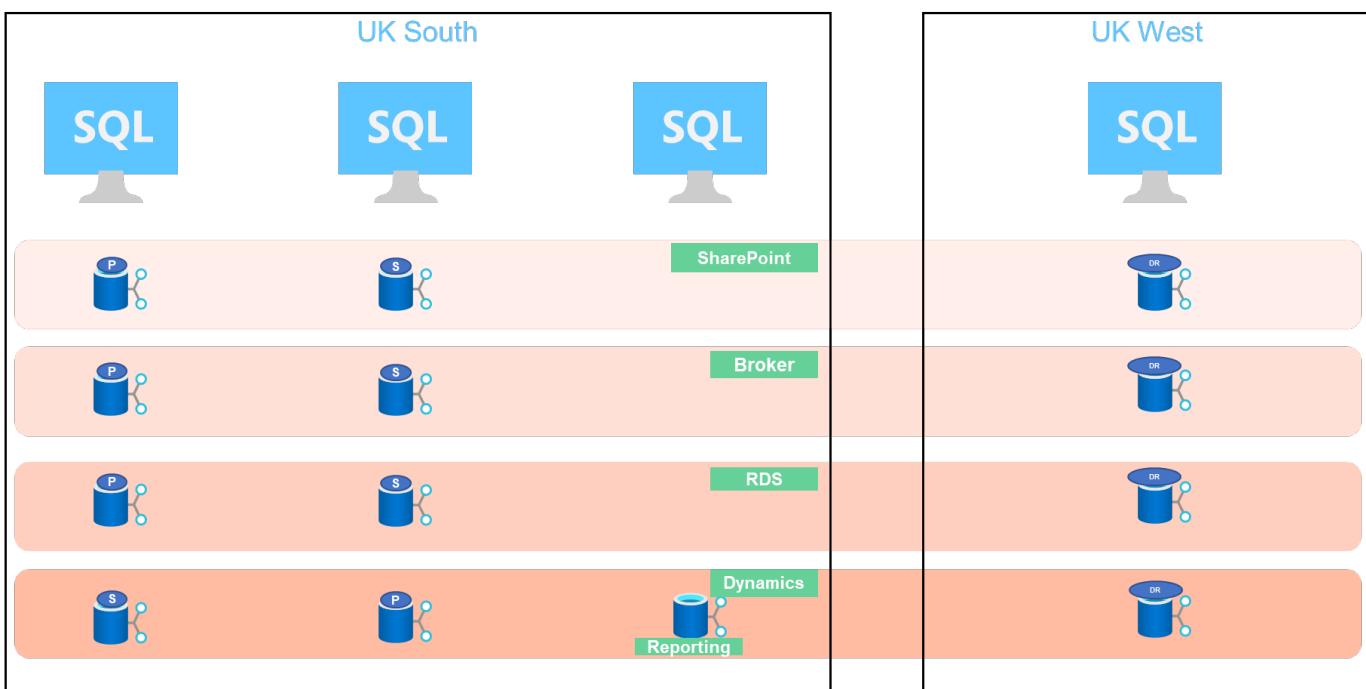
- Backup retention: 7 days
- Backup archive: 365 days



Deploying FCI with SQL Server on Azure virtual machines with an Azure NetApp Files share provides a cost-efficient model with a single copy of the data. This solution can prevent add-file operation issues if the file path differs from the secondary replica.



The following image shows the databases within AOAG spread across the nodes.



### Data layout

The user database files (.mdf) and user database transaction log files (.ldf) along with tempDB are stored on the same volume. The service level is Ultra.

The configuration consists of four nodes and four AGs. All 21 databases (part of Dynamic AX, SharePoint, RDS connection broker, and indexing services) are stored on the Azure NetApp Files volumes. The databases are balanced between the AOAG nodes to use the resources on the nodes effectively. Four D32 v3 instances are added in the WSFC, which participates in the AOAG configuration. These four nodes are provisioned in the Azure virtual network and are not migrated from on-premises.

### Notes:

- If the logs require more performance and throughput depending on the nature of the application and the queries executed, the database files can be placed on the Premium service level, and the logs can be stored at the Ultra service level.
- If the tempdb files have been placed on Azure NetApp Files, then the Azure NetApp Files volume should be separated from the user database files. Here is an example distribution of the database files in AOAG.

### Notes:

- To retain the benefits of Snapshot copy-based data protection, NetApp recommends not combining data and log data into the same volume.
- An add-file operation performed on the primary replica might fail on the secondary databases if the file path of a secondary database differs from the path of the corresponding primary database. This can happen if the share path is different on primary and secondary nodes (due to different computer accounts). This failure could cause the secondary databases to be suspended. If the growth or performance pattern cannot be predicted and the plan is to add files later, a SQL Server failover cluster with Azure NetApp Files is an acceptable solution. For most deployments, Azure NetApp Files meets the performance requirements.

## Migration

There are several ways to migrate an on-premises SQL Server user database to SQL Server in an Azure virtual machine. The migration can be either online or offline. The options chosen depend on the SQL Server version, business requirements, and the SLAs defined within the organization. To minimize downtime during the database migration process, NetApp recommends using either the AlwaysOn option or the transactional replication option. If it is not possible to use these methods, you can migrate the database manually.

The simplest and most thoroughly tested approach for moving databases across machines is backup and restore. Typically, you can start with a database backup followed by a copy of the database backup into Azure. You can then restore the database. For the best data transfer performance, migrate the database files into the Azure VM using a compressed backup file. The high-level design referenced in this document uses the backup approach to Azure file storage with Azure file sync and then restore to Azure NetApp files.



Azure Migrate can be used to discover, assess, and migrate SQL Server workloads.

To perform a migration, complete the following high-level steps:

1. Based on your requirements, set up connectivity.
2. Perform a full database backup to an on-premises file-share location.
3. Copy the backup files to an Azure file share with Azure file sync.
4. Provision the VM with the desired version of SQL Server.
5. Copy the backup files to the VM by using the `copy` command from a command prompt.
6. Restore the full databases to SQL Server on Azure virtual machines.



To restore 21 databases, it took approximately nine hours. This approach is specific to this scenario. However, other migration techniques listed below can be used based on your situation and requirements.

Other migration options to move data from an on-premises SQL Server to Azure NetApp Files include the following:

- Detach the data and log files, copy them to Azure Blob storage, and then attach them to SQL Server in the Azure VM with an ANF file share mounted from the URL.
- If you are using Always On availability group deployment on-premises, use the [Add Azure Replica Wizard](#) to create a replica in Azure and then perform failover.
- Use SQL Server [transactional replication](#) to configure the Azure SQL Server instance as a subscriber, disable replication, and point users to the Azure database instance.
- Ship the hard drive using the Windows Import/Export Service.

## Backup and recovery

Backup and recovery are an important aspect of any SQL Server deployment. It is mandatory to have the appropriate safety net to quickly recover from various data failure and loss scenarios in conjunction with high availability solutions such as AOAG. SQL Server Database Quiesce Tool, Azure Backup (streaming), or any third-party backup tool such as Commvault can be used to perform an application-consistent backup of the databases,

Azure NetApp Files Snapshot technology allows you to easily create a point-in-time (PiT) copy of the user databases without affecting performance or network utilization. This technology also allows you to restore a

Snapshot copy to a new volume or quickly revert the affected volume to the state it was in when that Snapshot copy was created by using the revert volume function. The Azure NetApp Files snapshot process is very quick and efficient, which allows for multiple daily backups, unlike the streaming backup offered by Azure backup. With multiple Snapshot copies possible in a given day, the RPO and RTO times can be significantly reduced. To add application consistency so that data is intact and properly flushed to the disk before the Snapshot copy is taken, use the SQL Server database quiesce tool ([SCSQLAPI tool](#); access to this link requires NetApp SSO login credentials). This tool can be executed from within PowerShell, which quiesces the SQL Server database and in turn can take the application-consistent storage Snapshot copy for backups.

\*Notes: \*

- The SCSSQLAPI tool only supports the 2016 and 2017 versions of SQL Server.
- The SCSSQLAPI tool only works with one database at a time.
- Isolate the files from each database by placing them onto a separate Azure NetApp Files volume.

Because of SCSSQL API's vast limitations, [Azure Backup](#) was used for data protection in order to meet the SLA requirements. It offers a stream-based backup of SQL Server running in Azure Virtual Machines and Azure NetApp Files. Azure Backup allows a 15-minute RPO with frequent log backups and PiT recovery up to one second.

## Monitoring

Azure NetApp Files is integrated with Azure Monitor for the time series data and provides metrics on allocated storage, actual storage usage, volume IOPS, throughput, disk read bytes/sec, disk write bytes/sec, disk reads/sec and disk writes/sec, and associated latency. This data can be used to identify bottlenecks with alerting and to perform health checks to verify that your SQL Server deployment is running in an optimal configuration.

In this HLD, ScienceLogic is used to monitor Azure NetApp Files by exposing the metrics using the appropriate service principal. The following image is an example of the Azure NetApp Files Metric option.

Avg Total throughput for volume1 [edit]

Add metric Add filter Apply splitting Line chart ▼ Drill into Logs ▼ New alert rule Pin to dashboard ...

Scope	Metric Namespace	Metric	Aggregation
volume1	NetApp Volumes stand...	Total throughput	Avg

Percentage Volume Consumed Size  
Read iops  
Read throughput  
**Total throughput**  
Volume allocated size  
Volume Backup Bytes

## Dev/Test using thick clones

With Azure NetApp Files, you can create instantaneous copies of databases to test functionality that should be implemented by using the current database structure and content during the application development cycles, to use the data extraction and manipulation tools when populating data warehouses, or to even recover data that was mistakenly deleted or changed. This process does not involve copying data from Azure Blob containers, which makes it very efficient. After the volume is restored, it can be used for read/write operations, which significantly reduces validation and time to market. This needs to be used in conjunction with SCSSQLAPI for application consistency. This approach provides yet another continuous cost optimization technique along with

Azure NetApp Files leveraging the Restore to New volume option.

#### Notes:

- The volume created from the Snapshot copy using the Restore New Volume option consumes capacity from the capacity pool.
- You can delete the cloned volumes by using REST or Azure CLI to avoid additional costs (in case the capacity pool must be increased).

#### Hybrid storage options

Although NetApp recommends using the same storage for all the nodes in SQL Server availability groups, there are scenarios in which multiple storage options can be used. This scenario is possible for Azure NetApp Files in which a node in AOAG is connected with an Azure NetApp Files SMB file share and the second node is connected with an Azure Premium disk. In these instances, make sure that the Azure NetApp Files SMB share is holding the primary copy of the user databases and the Premium disk is used as the secondary copy.

#### Notes:

- In such deployments, to avoid any failover issues, make sure that continuous availability is enabled on the SMB volume. With no continuously available attribute, the database can fail if there is any background maintenance at the storage layer.
- Keep the primary copy of the database on the Azure NetApp Files SMB file share.

#### Business continuity

Disaster recovery is generally an afterthought in any deployment. However, disaster recovery must be addressed during the initial design and deployment phase to avoid any impact to your business. With Azure NetApp Files, the cross-region replication (CRR) functionality can be used to replicate the volume data at the block level to the paired region to handle any unexpected regional outage. The CRR-enabled destination volume can be used for read operations, which makes it an ideal candidate for disaster recovery simulations. In addition, the CRR destination can be assigned with the lowest service level (for instance, Standard) to reduce the overall TCO. In the event of a failover, replication can be broken, which makes the respective volume read/write capable. Also, the service level of the volume can be changed by using the dynamic service level functionality to significantly reduce disaster recovery cost. This is another unique feature of Azure NetApp Files with block replication within Azure.

#### Long-term Snapshot copy archive

Many organizations must perform long-term retention of snapshot data from database files as a mandatory compliance requirement. Although this process is not used in this HLD, it can be easily accomplished by using a simple batch script using [AzCopy](#) to copy the snapshot directory to the Azure Blob container. The batch script can be triggered based on a specific schedule by using scheduled tasks. The process is straightforward—it includes the following steps:

1. Download the AzCopy V10 executable file. There is nothing to install because it is an exe file.
2. Authorize AzCopy by using a SAS token at the container level with the appropriate permissions.
3. After AzCopy is authorized, the data transfer begins.

#### Notes:

- In batch files, make sure to escape the % characters that appear in SAS tokens. This can be done by adding an additional % character next to existing % characters in the SAS token string.

- The **Secure Transfer Required** setting of a storage account determines whether the connection to a storage account is secured with Transport Layer Security (TLS). This setting is enabled by default. The following batch script example recursively copies data from the Snapshot copy directory to a designated Blob container:

```
SET source="Z:\~snapshot"
echo %source%
SET
dest="https://testanfacct.blob.core.windows.net/azcopts?sp=racwdl&st=2020
-10-21T18:41:35Z&se=2021-10-22T18:41:00Z&sv=2019-12
-12&sr=c&sig=ZxRUJwF1LXgHS8As7HzXJOaDXXVJ7PxxIX3ACpx56XY%%3D"
echo %dest%
```

The following example cmd is executed in PowerShell:

```
-recursive
```

```
INFO: Scanning...
INFO: Any empty folders will not be processed, because source and/or
destination doesn't have full folder support
Job b3731dd8-da61-9441-7281-17a4db09ce30 has started
Log file is located at: C:\Users\niyaz\.azcopy\b3731dd8-da61-9441-7281-
17a4db09ce30.log
0.0 %, 0 Done, 0 Failed, 2 Pending, 0 Skipped, 2 Total,
INFO: azcopy.exe: A newer version 10.10.0 is available to download
0.0 %, 0 Done, 0 Failed, 2 Pending, 0 Skipped, 2 Total,
Job b3731dd8-da61-9441-7281-17a4db09ce30 summary
Elapsed Time (Minutes): 0.0333
Number of File Transfers: 2
Number of Folder Property Transfers: 0
Total Number of Transfers: 2
Number of Transfers Completed: 2
Number of Transfers Failed: 0
Number of Transfers Skipped: 0
TotalBytesTransferred: 5
Final Job Status: Completed
```

## Notes:

- A similar backup feature for long-term retention will soon be available in Azure NetApp Files.
- The batch script can be used in any scenario that requires data to be copied to Blob container of any region.

## **Cost optimization**

With volume reshaping and dynamic service level change, which is completely transparent to the database, Azure NetApp Files allows continuous cost optimizations in Azure. This capability is used in this HLD extensively to avoid overprovisioning of additional storage to handle workload spikes.

Resizing the volume can be easily accomplished by creating an Azure function in conjunction with the Azure alert logs.

## **Conclusion**

Whether you are targeting an all-cloud or hybrid cloud with stretch databases, Azure NetApp Files provides excellent options to deploy and manage the database workloads while reducing your TCO by making data requirements seamless to the application layer.

This document covers recommendations for planning, designing, optimizing, and scaling Microsoft SQL Server deployments with Azure NetApp Files, which can vary greatly between implementations. The right solution depends on both the technical details of the implementation and the business requirements driving the project.

## **Takeaways**

The key points of this document include:

- You can now use Azure NetApp Files to host the database and file share witness for SQL Server cluster.
- You can boost the application response times and deliver 99.9999% availability to provide access to SQL Server data when and where it is needed.
- You can simplify the overall complexity of the SQL Server deployment and ongoing management, such as raid striping, with simple and instant resizing.
- You can rely on intelligent operations features to help you deploy SQL Server databases in minutes and speed development cycles.
- If Azure Cloud is the destination, Azure NetApp Files is the right storage solution for optimized deployment.

## **Where to find additional information**

To learn more about the information described in this document, refer to the following website links:

- Solution architectures using Azure NetApp Files

<https://docs.microsoft.com/en-us/azure/azure-netapp-files/azure-netapp-files-solution-architectures>

- Benefits of using Azure NetApp Files for SQL Server deployment

<https://docs.microsoft.com/en-us/azure/azure-netapp-files/solutions-benefits-azure-netapp-files-sql-server>

- SQL Server on Azure Deployment Guide Using Azure NetApp Files

<https://www.netapp.com/pdf.html?item=/media/27154-tr-4888.pdf>

- Fault tolerance, high availability, and resilience with Azure NetApp Files

<https://cloud.netapp.com/blog/azure-anf-blr-fault-tolerance-high-availability-and-resilience-with-azure-netapp-files>

# Hybrid Cloud Database Solutions with SnapCenter

## TR-4908: Hybrid Cloud Database Solutions with SnapCenter Overview

Alan Cao, Felix Melligan, NetApp

This solution provides NetApp field and customers with instructions and guidance for configuring, operating, and migrating databases to a hybrid cloud environment using the NetApp SnapCenter GUI-based tool and the NetApp storage service CVO in public clouds for the following use cases:

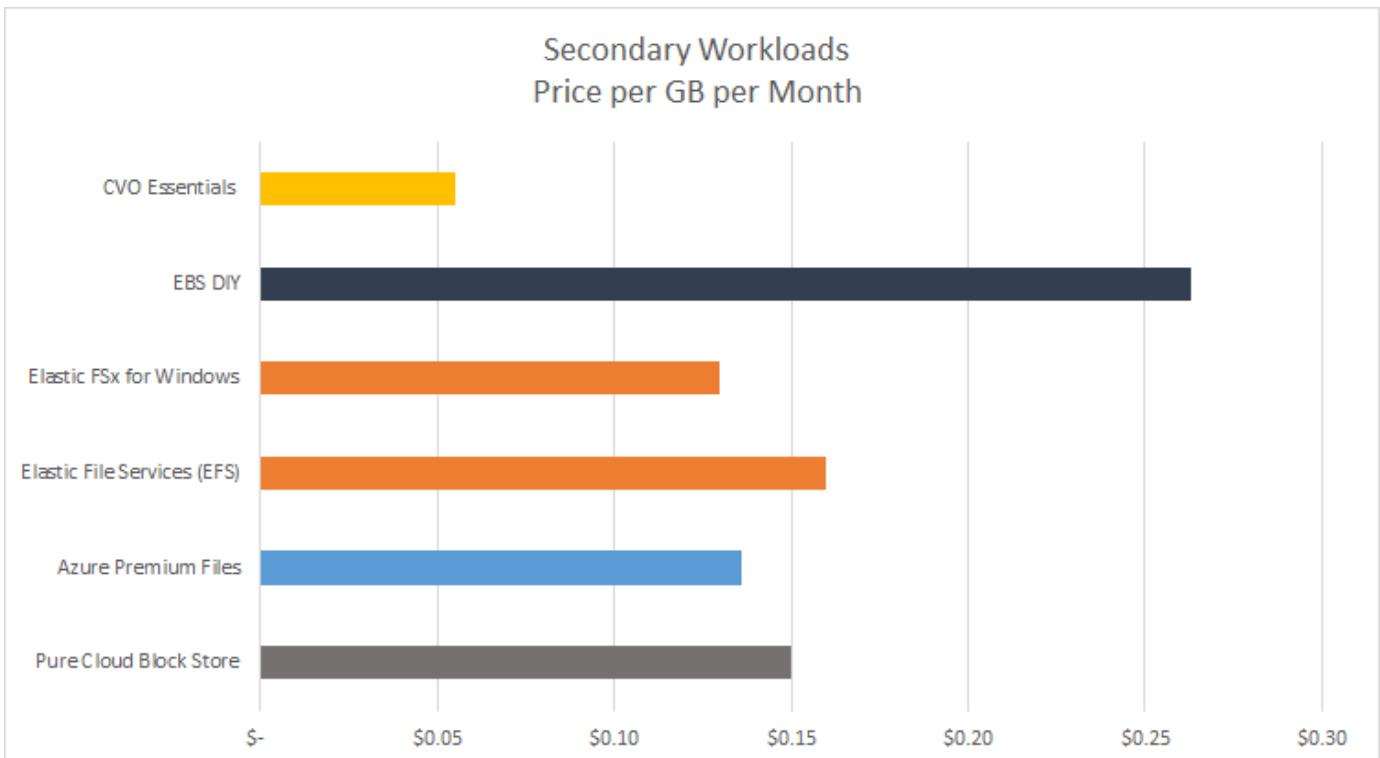
- Database dev/test operations in the hybrid cloud
- Database disaster recovery in the hybrid cloud

Today, many enterprise databases still reside in private corporate data centers for performance, security, and/or other reasons. This hybrid cloud database solution enables enterprises to operate their primary databases on site while using a public cloud for dev/test database operations as well as for disaster recovery to reduce licensing and operational costs.

Many enterprise databases, such as Oracle, SQL Server, SAP HANA, and so on, carry high licensing and operational costs. Many customers pay a one-time license fee as well as annual support costs based on the number of compute cores in their database environment, whether the cores are used for development, testing, production, or disaster recovery. Many of those environments might not be fully utilized throughout the application lifecycle.

The solutions provide an option for customers to potentially reduce their licensable cores count by moving their database environments devoted to development, testing, or disaster recovery to the cloud. By using public-cloud scale, redundancy, high availability, and a consumption-based billing model, the cost saving for licensing and operation can be substantial, while not sacrificing any application usability or availability.

Beyond potential database license-cost savings, the NetApp capacity-based CVO license model allows customers to save storage costs on a per-GB basis while empowering them with high level of database manageability that is not available from competing storage services. The following chart shows a storage cost comparison of popular storage services available in the public cloud.



This solution demonstrates that, by using the SnapCenter GUI-based software tool and NetApp SnapMirror technology, hybrid cloud database operations can be easily setup, implemented, and operated.

The following videos demonstrate SnapCenter in action:

- [Backup of an Oracle database across a Hybrid Cloud using SnapCenter](#)
- [SnapCenter- Clone DEV/TEST to AWS Cloud for an Oracle database](#)

Notably, although the illustrations throughout this document show CVO as a target storage instance in the public cloud, the solution is also fully validated for the new release of the FSx ONTAP storage engine for AWS.

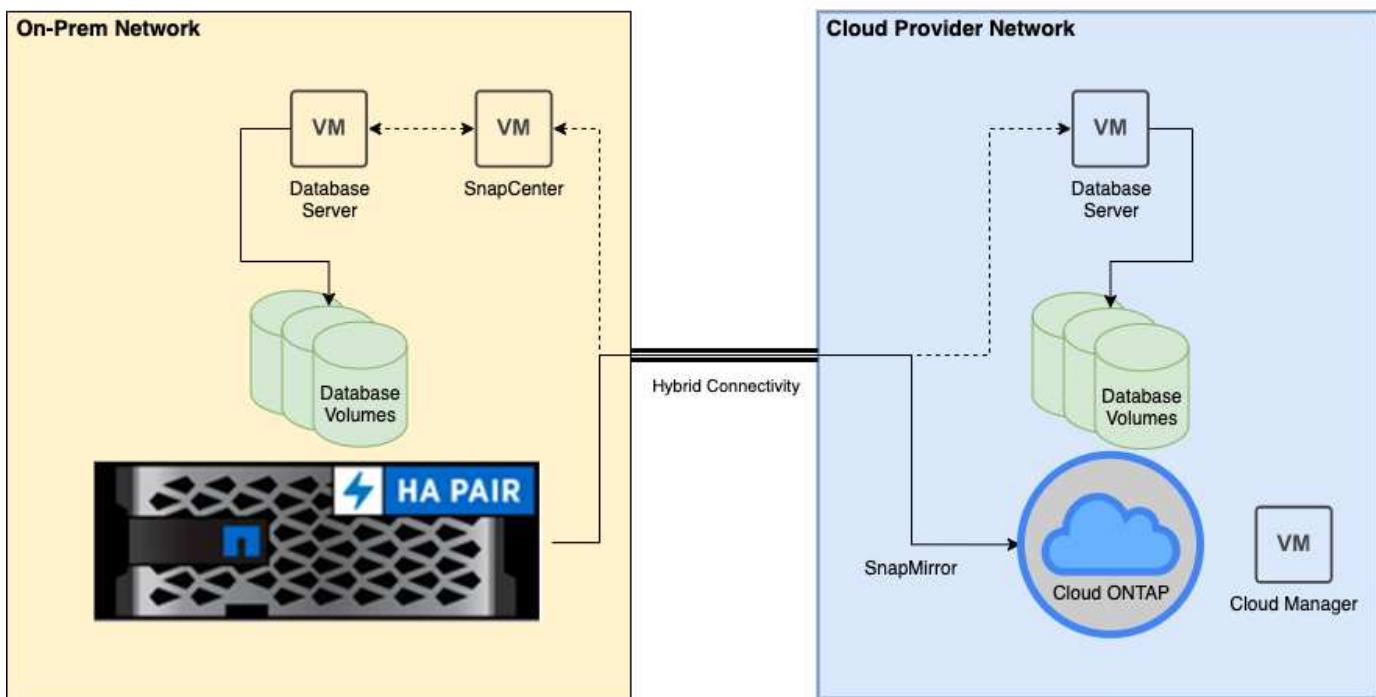
To test drive the solution and use cases for yourself, a NetApp Lab-on-Demand SL10680 can be requested at following xref:[./databases/ TL\\_AWS\\_004 HCoD: AWS - NW,SnapCenter\(OnPrem\)](#).

[Next: Solutions architecture.](#)

## Solution Architecture

[Previous: Introduction.](#)

The following architecture diagram illustrates a typical implementation of enterprise database operation in a hybrid cloud for dev/test and disaster recovery operations.



In normal business operations, synchronized database volumes in the cloud can be cloned and mounted to dev/test database instances for applications development or testing. In the event of a failure, the synchronized database volumes in the cloud can then be activated for disaster recovery.

[Next: Solutions requirements.](#)

## SnapCenter Requirements

[Previous: Solutions architecture.](#)

This solution is designed in a hybrid cloud setting to support on-premises production databases that can burst to all of the popular public clouds for dev/test and disaster recovery operations.

This solution supports all databases that are currently supported by SnapCenter, although only Oracle and SQL Server databases are demonstrated here. This solution is validated with virtualized database workloads, although bare-metal workloads are also supported.

We assume that production database servers are hosted on-premises with DB volumes presented to DB hosts from a ONTAP storage cluster. SnapCenter software is installed on-premises for database backup and data replication to the cloud. An Ansible controller is recommended but not required for database deployment automation or OS kernel and DB configuration syncing with a standby DR instance or dev/test instances in the public cloud.

## Requirements

Environment	Requirements
<b>On-premises</b>	Any databases and versions supported by SnapCenter SnapCenter v4.4 or higher Ansible v2.09 or higher ONTAP cluster 9.x Intercluster LIFs configured Connectivity from on-premises to a cloud VPC (VPN, interconnect, and so on) Networking ports open - ssh 22 - tcp 8145, 8146, 10000, 11104, 11105
<b>Cloud - AWS</b>	<a href="#">Cloud Manager Connector</a> <a href="#">Cloud Volumes ONTAP</a> Matching DB OS EC2 instances to On-prem
<b>Cloud - Azure</b>	<a href="#">Cloud Manager Connector</a> <a href="#">Cloud Volumes ONTAP</a> Matching DB OS Azure Virtual Machines to On-prem
<b>Cloud - GCP</b>	<a href="#">Cloud Manager Connector</a> <a href="#">Cloud Volumes ONTAP</a> Matching DB OS Google Compute Engine instances to on-premises

[Next: Prerequisites configuration.](#)

## Prerequisites configuration

[Previous: Solutions requirements.](#)

Certain prerequisites must be configured both on-premises and in the cloud before the execution of hybrid cloud database workloads. The following section provides a high-level summary of this process, and the following links provide further information about necessary system configuration.

### On premises

- SnapCenter installation and configuration
- On-premises database server storage configuration
- Licensing requirements
- Networking and security
- Automation

### Public cloud

- A NetApp Cloud Central login
- Network access from a web browser to several endpoints

- A network location for a connector
- Cloud provider permissions
- Networking for individual services

Important considerations:

1. Where to deploy the Cloud Manager Connector?
2. Cloud Volume ONTAP sizing and architecture
3. Single node or high availability?

The following links provide further details:

[On Premises](#)

[Public Cloud](#)

[Next: Prerequisites on-premises.](#)

### Prerequisites on-premises

[Previous: Prerequisites configuration.](#)

The following tasks must be completed on-premises to prepare the SnapCenter hybrid-cloud database workload environment.

#### SnapCenter installation and configuration

The NetApp SnapCenter tool is a Windows-based application that typically runs in a Windows domain environment, although workgroup deployment is also possible. It is based on a multitiered architecture that includes a centralized management server (the SnapCenter server) and a SnapCenter plug-in on the database server hosts for database workloads. Here are a few key considerations for hybrid-cloud deployment.

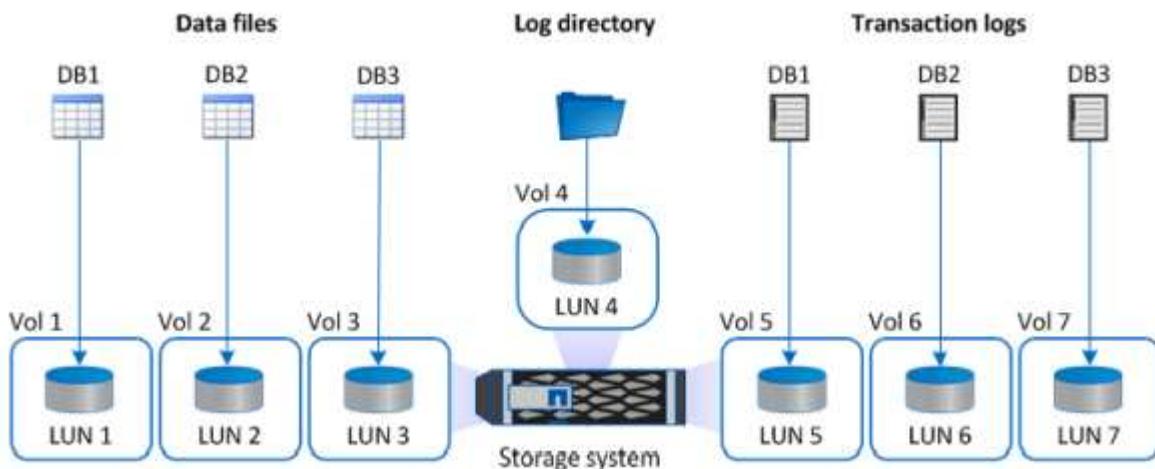
- **Single instance or HA deployment.** HA deployment provides redundancy in the case of a single SnapCenter instance server failure.
- **Name resolution.** DNS must be configured on the SnapCenter server to resolve all database hosts as well as on the storage SVM for forward and reverse lookup. DNS must also be configured on database servers to resolve the SnapCenter server and the storage SVM for both forward and reverse lookup.
- **Role-based access control (RBAC) configuration.** For mixed database workloads, you might want to use RBAC to segregate management responsibility for different DB platform such as an admin for Oracle database or an admin for SQL Server. Necessary permissions must be granted for the DB admin user.
- **Enable policy-based backup strategy.** To enforce backup consistency and reliability.
- **Open necessary network ports on the firewall.** For the on-premises SnapCenter server to communicate with agents installed in the cloud DB host.
- **Ports must be open to allow SnapMirror traffic between on-prem and public cloud.** The SnapCenter server relies on ONTAP SnapMirror to replicate onsite Snapshot backups to cloud CVO storage SVMs.

After careful pre-installation planning and consideration, click this [SnapCenter installation workflow](#) for details of SnapCenter installation and configuration.

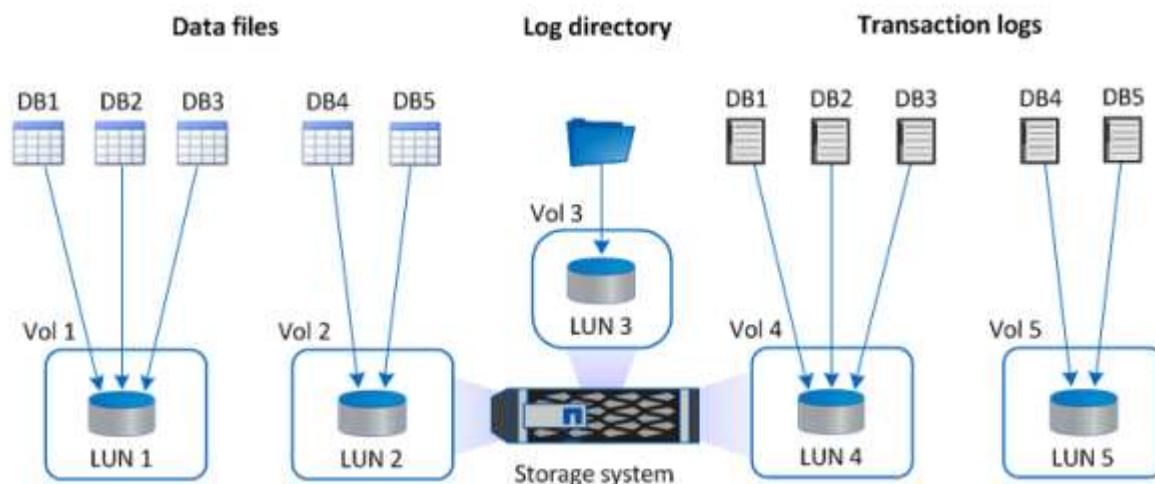
## On-premises database server storage configuration

Storage performance plays an important role in the overall performance of databases and applications. A well-designed storage layout can not only improve DB performance but also make it easy to manage database backup and recovery. Several factors should be considered when defining your storage layout, including the size of the database, the rate of expected data change for the database, and the frequency with which you perform backups.

Directly attaching storage LUNs to the guest VM by either NFS or iSCSI for virtualized database workloads generally provides better performance than storage allocated via VMDK. NetApp recommends the storage layout for a large SQL Server database on LUNs depicted in the following figure.



The following figure shows the NetApp recommended storage layout for small or medium SQL Server database on LUNs.



The Log directory is dedicated to SnapCenter to perform transaction log rollup for database recovery. For an extra large database, multiple LUNs can be allocated to a volume for better performance.

For Oracle database workloads, SnapCenter supports database environments backed by ONTAP storage that are mounted to the host as either physical or virtual devices. You can host the entire database on a single or multiple storage devices based on the criticality of the environment. Typically, customers isolate data files on dedicated storage from all other files such as control files, redo files, and archive log files. This helps administrators to quickly restore (ONTAP single-file SnapRestore) or clone a large critical database (petabyte

scale) using Snapshot technology within few seconds to minutes.



For mission critical workloads that are sensitive to latency, a dedicated storage volume should be deployed to different types of Oracle files to achieve the best latency possible. For a large database, multiple LUNs (NetApp recommends up to eight) per volume should be allocated to data files.



For smaller Oracle databases, SnapCenter supports shared storage layouts in which you can host multiple databases or part of a database on the same storage volume or LUN. As an example of this layout, you can host data files for all the databases on a +DATA ASM disk group or a volume group. The remainder of the files (redo, archive log, and control files) can be hosted on another dedicated disk group or volume group (LVM). Such a deployment scenario is illustrated below.



To facilitate the relocation of Oracle databases, the Oracle binary should be installed on a separate LUN that is included in the regular backup policy. This ensures that in the case of database relocation to a new server host, the Oracle stack can be started for recovery without any potential issues due to an out-of-sync Oracle binary.

#### Licensing requirements

SnapCenter is licensed software from NetApp. It is generally included in an on-premises ONTAP license. However, for hybrid cloud deployment, a cloud license for SnapCenter is also required to add CVO to SnapCenter as a target data replication destination. Please review following links for SnapCenter standard capacity-based license for details:

#### [SnapCenter standard capacity-based licenses](#)

#### Networking and security

In a hybrid database operation that requires an on-premises production database that is burstable to cloud for dev/test and disaster recovery, networking and security is important factor to consider when setting up the

environment and connecting to the public cloud from an on-premises data center.

Public clouds typically use a virtual private cloud (VPC) to isolate different users within a public-cloud platform. Within an individual VPC, security is controlled using measures such as security groups that are configurable based on user needs for the lockdown of a VPC.

The connectivity from the on-premises data center to the VPC can be secured through a VPN tunnel. On the VPN gateway, security can be hardened using NAT and firewall rules that block attempts to establish network connections from hosts on the internet to hosts inside the corporate data center.

For networking and security considerations, review the relevant inbound and outbound CVO rules for your public cloud of choice:

- [Security group rules for CVO - AWS](#)
- [Security group rules for CVO - Azure](#)
- [Firewall rules for CVO - GCP](#)

#### **Using Ansible automation to sync DB instances between on-premises and the cloud - optional**

To simplify management of a hybrid-cloud database environment, NetApp highly recommends but does not require that you deploy an Ansible controller to automate some management tasks, such as keeping compute instances on-premises and in the cloud in sync. This is particular important because an out-of-sync compute instance in the cloud might render the recovered database in the cloud error prone because of missing kernel packages and other issues.

The automation capability of an Ansible controller can also be used to augment SnapCenter for certain tasks, such as breaking up the SnapMirror instance to activate the DR data copy for production.

Follow these instruction to set up your Ansible control node for RedHat or CentOS machines: [RedHat/CentOS Ansible Controller Setup](#).

Follow these instruction to set up your Ansible control node for Ubuntu or Debian machines: [Ubuntu/Debian Ansible Controller Setup](#).

[Next: Public cloud.](#)

#### **Prerequisites for the public cloud**

[Previous: Prerequisites on-premises.](#)

Before we install the Cloud Manager connector and Cloud Volumes ONTAP and configure SnapMirror, we must perform some preparation for our cloud environment. This page describes the work that needs to be done as well as the considerations when deploying Cloud Volumes ONTAP.

#### **Cloud Manager and Cloud Volumes ONTAP deployment prerequisites checklist**

- A NetApp Cloud Central login
- Network access from a web browser to several endpoints
- A network location for a Connector
- Cloud provider permissions
- Networking for individual services

For more information about what you need to get started, visit our [cloud documentation](#).

## Considerations

### 1. What is a Cloud Manager connector?

In most cases, a Cloud Central account admin must deploy a connector in your cloud or on-premises network. The connector enables Cloud Manager to manage resources and processes within your public cloud environment.

For more information about Connectors, visit our [cloud documentation](#).

### 2. Cloud Volumes ONTAP sizing and architecture

When deploying Cloud Volumes ONTAP, you are given the choice of either a predefined package or the creation of your own configuration. Although many of these values can be changed later on nondisruptively, there are some key decisions that need to be made before deployment based on the workloads to be deployed in the cloud.

Each cloud provider has different options for deployment and almost every workload has its own unique properties. NetApp has a [CVO sizing tool](#) that can help size deployments correctly based on capacity and performance, but it has been built around some basic concepts which are worth considering:

- Capacity required
- Network capability of the cloud virtual machine
- Performance characteristics of cloud storage

The key is to plan for a configuration that not only satisfies the current capacity and performance requirements, but also looks at future growth. This is generally known as capacity headroom and performance headroom.

If you would like further information, read the documentation about planning correctly for [AWS](#), [Azure](#), and [GCP](#).

### 3. Single node or high availability?

In all clouds, there is the option to deploy CVO in either a single node or in a clustered high availability pair with two nodes. Depending on the use case, you might wish to deploy a single node to save costs or an HA pair to provide further availability and redundancy.

For a DR use case or spinning up temporary storage for development and testing, single nodes are common since the impact of a sudden zonal or infrastructure outage is lower. However, for any production use case, when the data is in only a single location, or when the dataset must have more redundancy and availability, high availability is recommended.

For further information about the architecture of each cloud's version of high availability, visit the documentation for [AWS](#), [Azure](#) and [GCP](#).

[Next: Getting started overview](#).

## Getting started overview

[Previous: Prerequisites for the public cloud](#).

This section provides a summary of the tasks that must be completed to meet the prerequisite requirements as outlined in previous section. The following section provide a high level tasks list for both on-premises and public cloud operations. The detailed processes and procedures can be accessed by clicking on the relevant

links.

## On-premises

- Setup database admin user in SnapCenter
- SnapCenter plugin installation prerequisites
- SnapCenter host plugin installation
- DB resource discovery
- Setup storage cluster peering and DB volume replication
- Add CVO database storage SVM to SnapCenter
- Setup database backup policy in SnapCenter
- Implement backup policy to protect database
- Validate backup

## AWS public cloud

- Pre-flight check
- Steps to deploy Cloud Manager and Cloud Volumes ONTAP in AWS
- Deploy EC2 compute instance for database workload

Click the following links for details:

[On Premises, Public Cloud - AWS](#)

## Getting started on premises

[Previous: Getting started overview.](#)

### On Premises

#### 1. Setup database admin user in SnapCenter

The NetApp SnapCenter tool uses role-based access control (RBAC) to manage user resources access and permission grants, and SnapCenter installation creates prepopulated roles. You can also create custom roles based on your needs or applications. It makes sense to have a dedicated admin user ID for each database platform supported by SnapCenter for database backup, restoration, and/or disaster recovery. You can also use a single ID to manage all databases. In our test cases and demonstration, we created a dedicated admin user for both Oracle and SQL Server, respectively.

Certain SnapCenter resources can only be provisioned with the SnapCenterAdmin role. Resources can then be assigned to other user IDs for access.

In a pre-installed and configured on-premises SnapCenter environment, the following tasks might have already have been completed. If not, the following steps create a database admin user:

1. Add the admin user to Windows Active Directory.
2. Log into SnapCenter using an ID granted with the SnapCenterAdmin role.
3. Navigate to the Access tab under Settings and Users, and click Add to add a new user. The new user ID is linked to the admin user created in Windows Active Directory in step 1. . Assign the proper role to the user

as needed. Assign resources to the admin user as applicable.

Name	Type	Roles	Domain
administrator	User	SnapCenterAdmin	demo
oradba	User	App Backup and Clone Admin	demo
sqldba	User	App Backup and Clone Admin	demo

## 2. SnapCenter plugin installation prerequisites

SnapCenter performs backup, restore, clone, and other functions by using a plugin agent running on the DB hosts. It connects to the database host and database via credentials configured under the Setting and Credentials tab for plugin installation and other management functions. There are specific privilege requirements based on the target host type, such as Linux or Windows, as well as the type of database.

DB hosts credentials must be configured before SnapCenter plugin installation. Generally, you want to use an administrator user accounts on the DB host as your host connection credentials for plugin installation. You can also grant the same user ID for database access using OS-based authentication. On the other hand, you can also employ database authentication with different database user IDs for DB management access. If you decide to use OS-based authentication, the OS admin user ID must be granted DB access. For Windows domain-based SQL Server installation, a domain admin account can be used to manage all SQL Servers within the domain.

Windows host for SQL server:

1. If you are using Windows credentials for authentication, you must set up your credential before installing plugins.
2. If you are using a SQL Server instance for authentication, you must add the credentials after installing plugins.
3. If you have enabled SQL authentication while setting up the credentials, the discovered instance or database is shown with a red lock icon. If the lock icon appears, you must specify the instance or database credentials to successfully add the instance or database to a resource group.
4. You must assign the credential to a RBAC user without sysadmin access when the following conditions are met:
  - The credential is assigned to a SQL instance.
  - The SQL instance or host is assigned to an RBAC user.
  - The RBAC DB admin user must have both the resource group and backup privileges.

Unix host for Oracle:

1. You must have enabled the password-based SSH connection for the root or non-root user by editing sshd.conf and restarting the sshd service. Password-based SSH authentication on AWS instance is turned off by default.
2. Configure the sudo privileges for the non-root user to install and start the plugin process. After installing the plugin, the processes run as an effective root user.

3. Create credentials with the Linux authentication mode for the install user.
4. You must install Java 1.8.x (64-bit) on your Linux host.
5. Installation of the Oracle database plugin also installs the SnapCenter plugin for Unix.

### 3. SnapCenter host plugin installation



Before attempting to install SnapCenter plugins on cloud DB server instances, make sure that all configuration steps have been completed as listed in the relevant cloud section for compute instance deployment.

The following steps illustrate how a database host is added to SnapCenter while a SnapCenter plugin is installed on the host. The procedure applies to adding both on-premises hosts and cloud hosts. The following demonstration adds a Windows or a Linux host residing in AWS.

#### Configure SnapCenter VMware global settings

Navigate to Settings > Global Settings. Select "VMs have iSCSI direct attached disks or NFS for all the hosts" under Hypervisor Settings and click Update.

The screenshot shows the 'Global Settings' tab selected in the top navigation bar. On the left, there's a sidebar with icons for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings (which is selected), and Alerts. The main content area is titled 'Global Settings' and contains a 'Hypervisor Settings' section. Inside this section, there's a checkbox labeled 'VMs have iSCSI direct attached disks or NFS for all the hosts' which is checked, and a blue 'Update' button next to it. Below this are sections for 'Notification Server Settings', 'Configuration Settings', 'Purge Jobs Settings', 'Domain Settings', and 'CA Certificate Settings', each with a collapse/expand arrow.

#### Add Windows host and installation of plugin on the host

1. Log into SnapCenter with a user ID with SnapCenterAdmin privileges.
2. Click the Hosts tab from the left-hand menu, and then click Add to open the Add Host workflow.
3. Choose Windows for Host Type; the Host Name can be either a host name or an IP address. The host name must be resolved to the correct host IP address from the SnapCenter host. Choose the host credentials created in step 2. Choose Microsoft Windows and Microsoft SQL Server as the plugin packages to be installed.

The screenshot shows the 'Add Host' workflow. On the left, there's a sidebar with icons for Managed Hosts, Search by Name, and a list of existing hosts: 'rhe12.demo.netapp.com' and 'soft.demo.netapp.com'. The main area has a title 'Add Host' and a form with fields: 'Host Type' set to 'Windows', 'Host Name' set to 'sql-standby', and 'Credentials' set to 'Domain Admin'. Below the form is a section titled 'Select Plug-ins to Install' with a note 'SnapCenter Plug-ins Package 4.5 for Windows'. It contains checkboxes for 'Microsoft Windows' (checked) and 'Microsoft SQL Server' (checked). There are also uncheckable options for 'Microsoft Exchange Server' and 'SAP HANA'. At the bottom of this section are 'More Options...', 'Port, gMSA, Install Path, Custom Plug-ins...', 'Submit' (blue button), and 'Cancel' buttons.

- After the plugin is installed on a Windows host, its Overall Status is shown as "Configure log directory."

Name	Type	System	Plug-in	Version	Overall Status
rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	<span style="color: green;">Running</span>
sql1_demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	<span style="color: green;">Running</span>
sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	<span style="color: orange;">Configure log directory</span>

- Click the Host Name to open the SQL Server log directory configuration.

Host Details

Host Name: sql-standby.demo.netapp.com  
Host IP: 10.221.2.56  
Overall Status: Configure log directory  
Host Type: Windows  
System: Stand-alone  
Credentials: Domain Admin  
Plug-ins: SnapCenter Plug-ins package 4.5.0.6123 for Windows  
✓ Microsoft Windows  
✓ Microsoft SQL Server [Remove](#) [Configure log directory](#)

Alerts: No Alerts

- Click "Configure log directory" to open "Configure Plug-in for SQL Server."

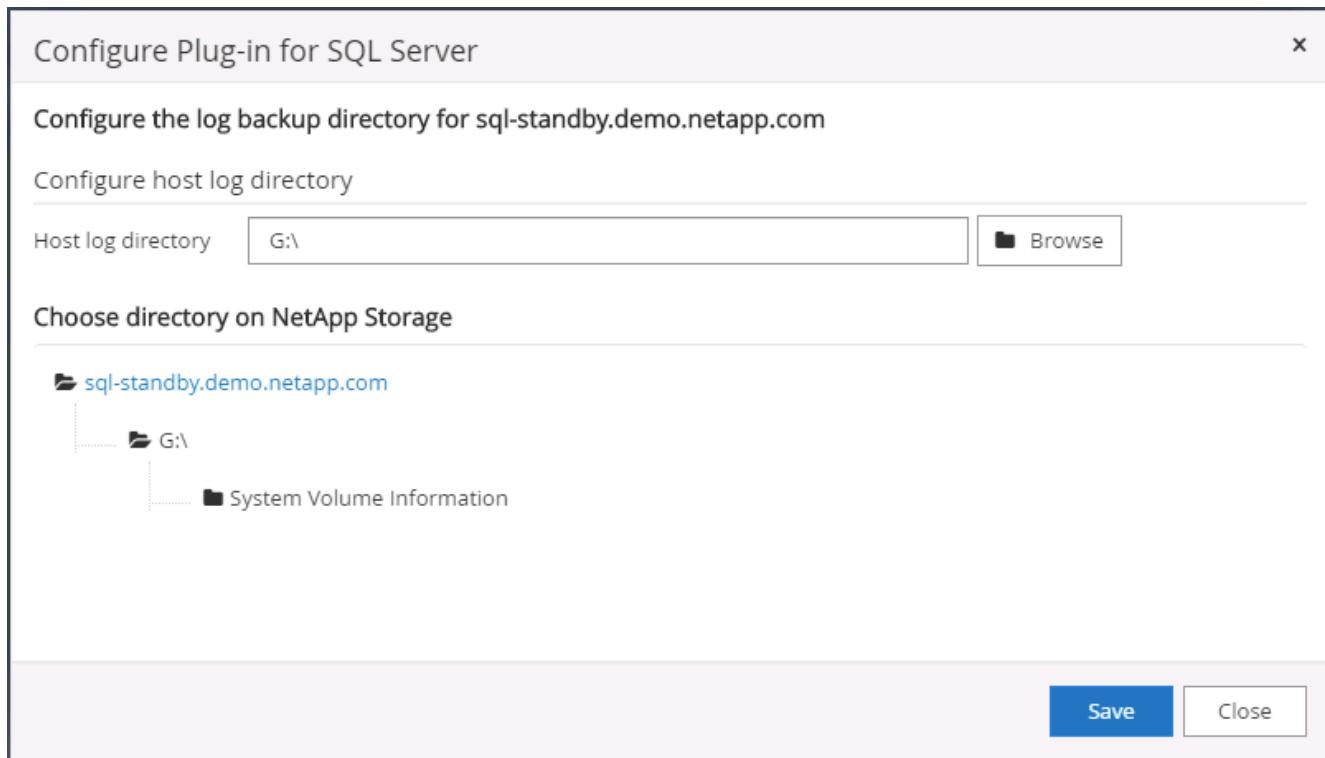
Configure Plug-in for SQL Server

Configure the log backup directory for sql-standby.demo.netapp.com

Configure host log directory

Host log directory: dedicated disk directory path

- Click Browse to discover NetApp storage so that a log directory can be set; SnapCenter uses this log directory to roll up the SQL server transaction log files. Then click Save.



For NetApp storage provisioned to a DB host to be discovered, the storage (on-prem or CVO) must be added to SnapCenter, as illustrated in step 6 for CVO as an example.

- After the log directory is configured, the Windows host plugin Overall Status is changed to Running.

Name	Type	System	Plug-in	Version	Overall Status
rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	<span style="color: green;">Running</span>
sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	<span style="color: green;">Running</span>
sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	<span style="color: green;">Running</span>

- To assign the host to the database management user ID, navigate to the Access tab under Settings and Users, click the database management user ID (in our case the sqldba that the host needs to be assigned to), and click Save to complete host resource assignment.

Name	Type	Roles	Domain
administrator	User	SnapCenterAdmin	demo
oradba	User	App Backup and Clone Admin	demo
sqldba	User	App Backup and Clone Admin	demo

Assign Assets

Asset Type: Host

search

<input type="checkbox"/>	Asset Name	
<input type="checkbox"/>	rhel2.demo.netapp.com	
<input type="checkbox"/>	sql1.demo.netapp.com	
<input checked="" type="checkbox"/>	sql-standby.demo.netapp.com	

**Save** **Close**

### Add Unix host and installation of plugin on the host

1. Log into SnapCenter with a user ID with SnapCenterAdmin privileges.
2. Click the Hosts tab from left-hand menu, and click Add to open the Add Host workflow.
3. Choose Linux as the Host Type. The Host Name can be either the host name or an IP address. However, the host name must be resolved to correct host IP address from SnapCenter host. Choose host credentials created in step 2. The host credentials require sudo privileges. Check Oracle Database as the plug-in to be installed, which installs both Oracle and Linux host plugins.

Add Host

Host Type: Linux

Host Name: ora-standby

Credentials: admin

Select Plug-ins to Install SnapCenter Plug-ins Package 4.5 for Linux

Oracle Database  
 SAP HANA

[More Options](#) : Port, Install Path, Custom Plug-ins...

**Submit** **Cancel**

4. Click More Options and select "Skip preinstall checks." You are prompted to confirm the skipping of the preinstall check. Click Yes and then Save.

More Options

Port	8145	<a href="#">i</a>
Installation Path	/opt/NetApp/snapcenter	<a href="#">i</a>
<input checked="" type="checkbox"/> Skip preinstall checks <input checked="" type="checkbox"/> Add all hosts in the oracle RAC		
Custom Plug-ins		
Choose a File <a href="#">Browse</a> <a href="#">Upload</a>		
No plug-ins found.		
<a href="#">Save</a> <a href="#">Cancel</a>		

5. Click Submit to start the plugin installation. You are prompted to Confirm Fingerprint as shown below.

Confirm Fingerprint

Authenticity of the host cannot be determined [i](#)

Host name	<a href="#">Edit</a>	Fingerprint	Valid
ora-standby.demo.netapp.com		ssh-rsa 3072 5C:02:EF:6B:63:54:59:10:84:DF:4D:6B:AB:FB:61:67	

[Confirm and Submit](#) [Close](#)

6. SnapCenter performs host validation and registration, and then the plugin is installed on the Linux host. The status is changed from Installing Plugin to Running.

Name	Type	System	Plug-in	Version	Overall Status
ora-standby.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running
sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running

7. Assign the newly added host to the proper database management user ID (in our case, oradba).

User Name: oradba  
Domain: demo  
Roles: App Backup and Clone Admin

Asset Name	Type	Asset Type
10.0.0.1	DataOntapCluster	Storage Connection
192.168.0.101	DataOntapCluster	Storage Connection
admin		Credentials
Linux Admin		Credentials
Oracle Archive Log Backup		Policy
Oracle Full Online Backup		Policy
rhel2.demo.netapp.com		host

Asset Type: Host

Asset Name
<input checked="" type="checkbox"/> ora-standby.demo.netapp.com
<input type="checkbox"/> rhel2.demo.netapp.com
<input type="checkbox"/> sql1.demo.netapp.com
<input type="checkbox"/> sql-standby.demo.netapp.com

Save    Close

#### 4. Database resource discovery

With successful plugin installation, the database resources on the host can be immediately discovered. Click the Resources tab in the left-hand menu. Depending on the type of database platform, a number of views are available, such as the database, resources group, and so on. You might need to click the Refresh Resources tab if the resources on the host are not discovered and displayed.

Oracle Database

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com				Not protected

When the database is initially discovered, the Overall Status is shown as "Not protected." The previous screenshot shows an Oracle database not protected yet by a backup policy.

When a backup configuration or policy is set up and a backup has been executed, the Overall Status for the database shows the backup status as "Backup succeeded" and the timestamp of the last backup. The following screenshot shows the backup status of a SQL Server user database.

Name	Instance	Host	Last Backup	Overall Status	Type
master	sql1	sql1.demo.netapp.com		Not available for backup	System database
model	sql1	sql1.demo.netapp.com		Not available for backup	System database
msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tpcc	sql1	sql1.demo.netapp.com	09/14/2021 2:35:07 PM	Backup succeeded	User database

If database access credentials are not properly set up, a red lock button indicates that the database is not accessible. For example, if Windows credentials do not have sysadmin access to a database instance, then database credentials must be reconfigured to unlock the red lock.

Name	Host	Resource Groups	Policies	State	Type
sql-standby	sql-standby.demo.netapp.com			Running	Standalone ()
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)

The Microsoft SQL Server or Windows credentials are necessary to unlock the selected instance. Click Refresh Resources to run a discovery with the associated Auth.

Name	Host	Resource Groups	Policies	State	Type
sql-standby	sql-standby.demo.netapp.com			Running	Standalone ()
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)

After the appropriate credentials are configured either at the Windows level or the database level, the red lock disappears and SQL Server Type information is gathered and reviewed.

Name	Host	Resource Groups	Policies	State	Type
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)
sql-standby	sql-standby.demo.netapp.com			Running	Standalone (15.0.2000)

## 5. Setup storage cluster peering and DB volumes replication

To protect your on-premises database data using a public cloud as the target destination, on-premises ONTAP cluster database volumes are replicated to the cloud CVO using NetApp SnapMirror technology. The replicated target volumes can then be cloned for DEV/OPS or disaster recovery. The following high-level steps enable you to set up cluster peering and DB volumes replication.

1. Configure intercluster LIFs for cluster peering on both the on-premises cluster and the CVO cluster instance. This step can be performed with ONTAP System Manager. A default CVO deployment has inter-cluster LIFs configured automatically.

On-premises cluster:

The screenshot shows the ONTAP System Manager interface with the 'NETWORK' tab selected. In the 'IPspaces' section, there are two entries: 'Cluster' (Broadcast Domains Cluster) and 'Default' (Storage VMs, svm\_onPrem, Broadcast Domains Default). In the 'Broadcast Domains' section, there are two entries: 'Cluster' (9000 MTU, IPspace: Cluster) and 'Default' (1500 MTU, IPspace: Default, onPrem-01 e0a e0b e0c e0d e0e e0f e0g e0h e0g-100 e0e-200 e0f-201). The 'Network Interfaces' section lists three interfaces: 'onPrem-01\_IC' (Status: green, Storage VM: Default, Address: 192.168.0.113, Current Node: onPrem-01, Current Port: e0b, Type: Intercluster), 'onPrem-01\_mgmt1' (Status: green, Storage VM: Default, Address: 192.168.0.111, Current Node: onPrem-01, Current Port: e0c, Type: Cluster/Node Mgmt), and 'cluster\_mgmt' (Status: green, Storage VM: Default, Address: 192.168.0.101, Current Node: onPrem-01, Current Port: e0a, Type: Cluster/Node Mgmt).

Target CVO cluster:

The screenshot shows the ONTAP System Manager interface with the 'NETWORK' tab selected. In the 'IPspaces' section, there are two entries: 'Cluster' (Broadcast Domains Cluster) and 'Default' (Storage VMs, svm\_hybridcvo, Broadcast Domains Default). In the 'Broadcast Domains' section, there are two entries: 'Cluster' (9000 MTU, IPspace: Cluster, hybridcvo-01 e0b, hybridcvo-02 e0b) and 'Default' (9001 MTU, IPspace: Default, hybridcvo-01 e0a, hybridcvo-02 e0a). The 'Network Interfaces' section lists five interfaces: 'hybridcvo-02\_mgmt1' (Status: green, Storage VM: Default, Address: 10.221.2.104, Current Node: hybridcvo-02, Current Port: e0a, Type: Cluster/Node Mgmt), 'inter\_1' (Status: green, Storage VM: Default, Address: 10.221.1.180, Current Node: hybridcvo-01, Current Port: e0a, Type: Intercluster, Cluster/Node Mgmt), 'inter\_2' (Status: green, Storage VM: Default, Address: 10.221.2.250, Current Node: hybridcvo-02, Current Port: e0a, Type: Intercluster, Cluster/Node Mgmt), 'iscsi\_1' (Status: green, Storage VM: svm\_hybridcvo, Address: 10.221.1.5, Current Node: hybridcvo-01, Current Port: e0a, Protocols: iSCSI, Type: Data), and 'iscsi\_2' (Status: green, Storage VM: svm\_hybridcvo, Address: 10.221.2.168, Current Node: hybridcvo-02, Current Port: e0a, Protocols: iSCSI, Type: Data). The 'inter\_1' and 'inter\_2' interfaces are highlighted with a red box.

2. With the intercluster LIFs configured, cluster peering and volume replication can be set up by using drag-and-drop in NetApp Cloud Manager. See "[Getting Started - AWS Public Cloud](#)" for details.

Alternatively, cluster peering and DB volume replication can be performed by using ONTAP System Manager as follows:

3. Log into ONTAP System Manager. Navigate to Cluster > Settings and click Peer Cluster to set up cluster peering with the CVO instance in the cloud.

The screenshot shows the ONTAP System Manager interface. The left sidebar is collapsed. The main area displays the 'Cluster' settings. Under 'UI Settings', the log level is set to 'DEBUG' and the inactivity timeout is '30 minutes'. Below this is the 'Intercluster Settings' section, which includes 'Network Interfaces' (IP address 192.168.0.113), 'Cluster Peers' (peered cluster name 'hybridcvo', with a 'Peer Cluster' button highlighted by a red box), and 'Storage VM Peers' (one peered storage VM). A search bar at the top right says 'Search actions, objects, and pages'.

4. Go to the Volumes tab. Select the database volume to be replicated and click Protect.

The screenshot shows the ONTAP System Manager interface with the 'Volumes' tab selected in the left sidebar. A volume named 'rhel2\_u03' is selected, indicated by a checked checkbox. The 'Protect' button, located in the top navigation bar, is highlighted with a red box. The detailed view for 'rhel2\_u03' shows its status as 'Online', type as 'FlexVol', and various performance metrics like capacity and latency. The 'Overview' tab is active.

5. Set the protection policy to Asynchronous. Select the destination cluster and storage SVM.

**Protect Volumes**

**PROTECTION POLICY**  
Asynchronous

**Source**  
CLUSTER  
onPrem  
STORAGE VM  
svm\_onPrem  
SELECTED VOLUMES  
rhel2\_u03

**Destination**  
CLUSTER  
hybridcvo  
STORAGE VM  
svm\_hybridcvo

**Destination Settings**  
2 matching labels

**VOLUME NAME**  
PREFIX: vol\_ <SourceVolumeName> SUFFIX: \_dest

Override default storage service name

**Configuration Details**  
 Initialize relationship ?  
 Enable FabricPool ?

**Save** **Cancel**

- Validate that the volume is synced between the source and target and that the replication relationship is healthy.

Source	Destination	Protection Policy	Relationship Health	Relationship Status	Lag
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr	MirrorAllSnapshots	<span style="color: green;">Healthy</span>	<span style="color: green;">Mirrored</span>	12 seconds

## 6. Add CVO database storage SVM to SnapCenter

- Log into SnapCenter with a user ID with SnapCenterAdmin privileges.
- Click the Storage System tab from the menu, and then click New to add a CVO storage SVM that hosts replicated target database volumes to SnapCenter. Enter the cluster management IP in the Storage System field, and enter the appropriate username and password.

- Click More Options to open additional storage configuration options. In the Platform field, select Cloud Volumes ONTAP, check Secondary, and then click Save.

Platform	Cloud Volumes ON <sup>TM</sup>	<input checked="" type="checkbox"/> Secondary
Protocol	HTTPS	
Port	443	
Timeout	60	seconds
Preferred IP		

**Save** **Cancel**

- Assign the storage systems to SnapCenter database management user IDs as shown in [3. SnapCenter host plugin installation](#).

Name	IP	Cluster Name	User Name	Platform	Controller License
svm_hybridcvo	10.0.0.1			CVO	✗
svm_onPrem	192.168.0.101			CVO	✓

## 7. Setup database backup policy in SnapCenter

The following procedures demonstrates how to create a full database or log file backup policy. The policy can then be implemented to protect databases resources. The recovery point objective (RPO) or recovery time objective (RTO) dictates the frequency of database and/or log backups.

## Create a full database backup policy for Oracle

1. Log into SnapCenter as a database management user ID, click Settings, and then click Policies.

The screenshot shows the NetApp SnapCenter interface. The left sidebar has links for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings (which is selected), and Alerts. The main area is titled 'Policies' and shows 'Oracle Database'. A search bar says 'Search by Name'. Below is a table with columns: Name, Backup Type, Schedule Type, Replication, and Verification. Two policies are listed:

Name	Backup Type	Schedule Type	Replication	Verification
Oracle Archive Log Backup	LOG, ONLINE	Hourly	SnapMirror	
Oracle Full Online Backup	FULL, ONLINE	Daily	SnapMirror	

Action buttons at the top right include New, Modify, Copy, Details, and Delete.

2. Click New to launch a new backup policy creation workflow or choose an existing policy for modification.

The dialog box is titled 'Modify Oracle Database Backup Policy' with a close button 'x' in the top right. On the left is a vertical navigation bar with steps 1 through 7: 1. Name, 2. Backup Type, 3. Retention, 4. Replication, 5. Script, 6. Verification, 7. Summary. Step 1 is highlighted in blue. The main area is titled 'Provide a policy name' and contains two fields: 'Policy name' with the value 'Oracle Full Online Backup' and 'Details' with the value 'Backup all data and log files'. There is an information icon 'i' next to the details field. At the bottom right are 'Previous' and 'Next' buttons.

3. Select the backup type and schedule frequency.

Modify Oracle Database Backup Policy

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Select Oracle database backup options

Choose backup type

Online backup

Datafiles, control files, and archive logs

Datafiles and control files

Archive logs

Offline backup i

Mount i

Shutdown

Save state of PDBs i

Choose schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

On demand

Hourly

Daily

Previous

Next

This screenshot shows the 'Modify Oracle Database Backup Policy' wizard, specifically Step 2: Backup Type. The left sidebar lists steps 1 through 7. The main area is titled 'Select Oracle database backup options'. Under 'Choose backup type', 'Online backup' and 'Datafiles, control files, and archive logs' are selected. Under 'Choose schedule frequency', 'Daily' is selected. At the bottom right are 'Previous' and 'Next' buttons.

4. Set the backup retention setting. This defines how many full database backup copies to keep.

Modify Oracle Database Backup Policy

**Retention settings**

Daily retention settings  
Data backup retention settings

Total Snapshot copies to keep

Keep Snapshot copies for  days

Archive Log backup retention settings

Total Snapshot copies to keep

Keep Snapshot copies for  days

[Previous](#) [Next](#)

The screenshot shows the 'Retention settings' section of the Oracle Database Backup Policy modification interface. It includes fields for daily data backup retention (14 days) and archive log retention (14 days). The 'Keep Snapshot copies for' option is selected for both.

5. Select the secondary replication options to push local primary snapshots backups to be replicated to a secondary location in cloud.

Modify Oracle Database Backup Policy x

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Select secondary replication options i

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label Daily i

Error retry count 3 i

Previous Next

6. Specify any optional script to run before and after a backup run.

Modify Oracle Database Backup Policy X

Specify optional scripts to run before and after performing a backup job

1 Name	Prescript full path <input type="text" value="/var/opt/snapcenter/spl/scripts/"/> Enter Prescript path	
2 Backup Type	Prescript arguments <input type="text"/>	
3 Retention	Postscript full path <input type="text" value="/var/opt/snapcenter/spl/scripts/"/> Enter Postscript path	
4 Replication	Postscript arguments <input type="text"/>	
5 Script	Script timeout 60	secs
6 Verification		
7 Summary		

Previous **Next**

7. Run backup verification if desired.

Modify Oracle Database Backup Policy X

**1 Name** Select the options to run backup verification

**2 Backup Type** Run Verifications for following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

Daily

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Verification script commands

Script timeout	60	secs
Prescript full path	/var/opt/snapcenter/spl/scripts/	Enter Prescript path
Prescript arguments	Choose optional arguments...	
Postscript full path	/var/opt/snapcenter/spl/scripts/	Enter Postscript path
Postscript arguments	Choose optional arguments...	

Previous Next

8. Summary.

Modify Oracle Database Backup Policy

<b>1 Name</b>	Summary
<b>2 Backup Type</b>	Policy name: Oracle Full Online Backup Details: Backup all data and log files
<b>3 Retention</b>	Backup type: Online backup
<b>4 Replication</b>	Schedule type: Daily RMAN catalog backup: Disabled
<b>5 Script</b>	Archive log pruning: None On demand data backup retention: None
<b>6 Verification</b>	On demand archive log backup retention: None Hourly data backup retention: None Hourly archive log backup retention: None
<b>7 Summary</b>	Daily data backup retention: Delete Snapshot copies older than : 14 days Daily archive log backup retention: Delete Snapshot copies older than : 14 days Weekly data backup retention: None Weekly archive log backup retention: None Monthly data backup retention: None Monthly archive log backup retention: None Replication: SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3

[Previous](#) [Finish](#)

### Create a database log backup policy for Oracle

1. Log into SnapCenter with a database management user ID, click Settings, and then click Policies.
2. Click New to launch a new backup policy creation workflow, or choose an existing policy for modification.

New Oracle Database Backup Policy X

**1 Name**

Provide a policy name

Policy name  i

Details

**2 Backup Type**

**3 Retention**

**4 Replication**

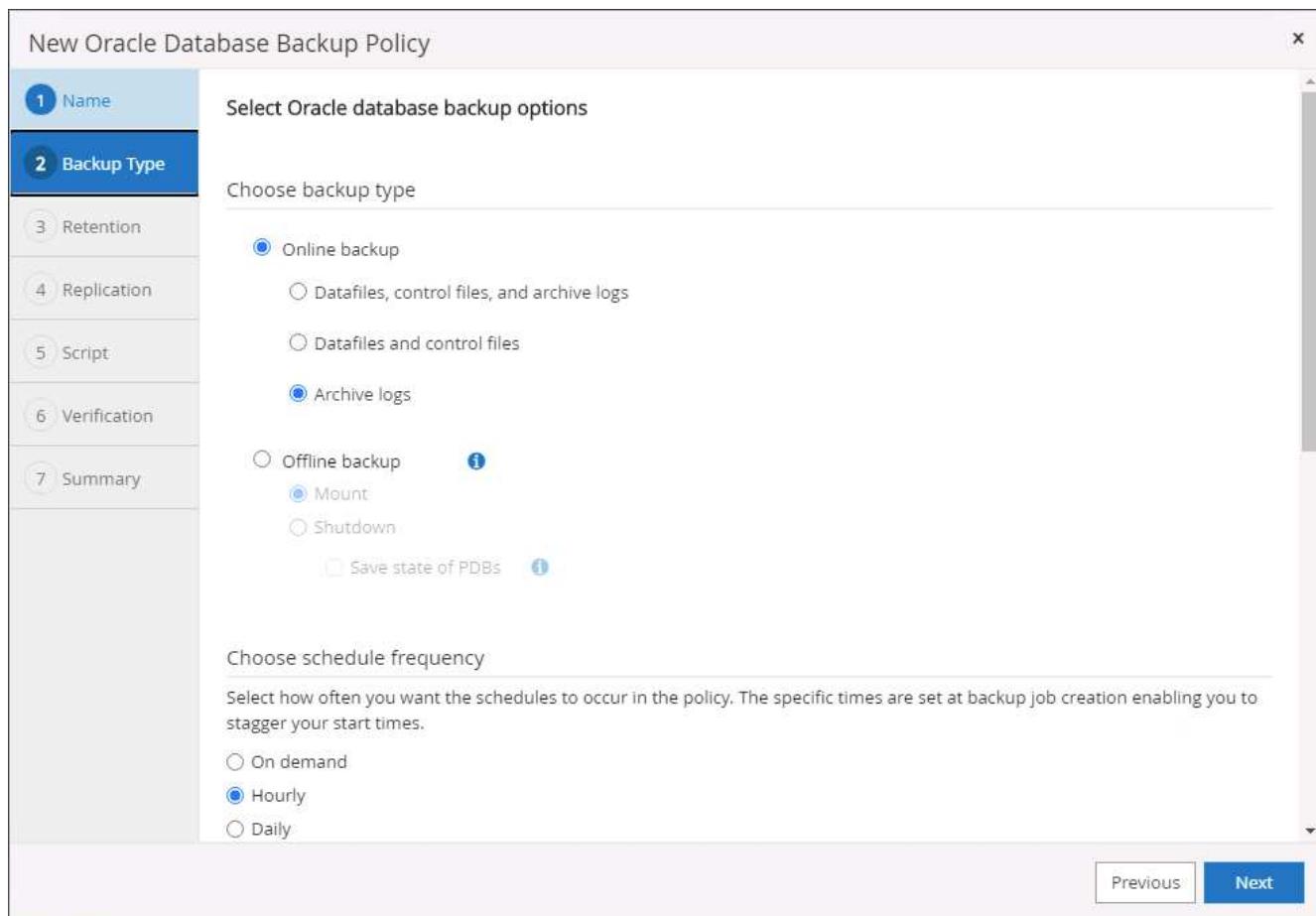
**5 Script**

**6 Verification**

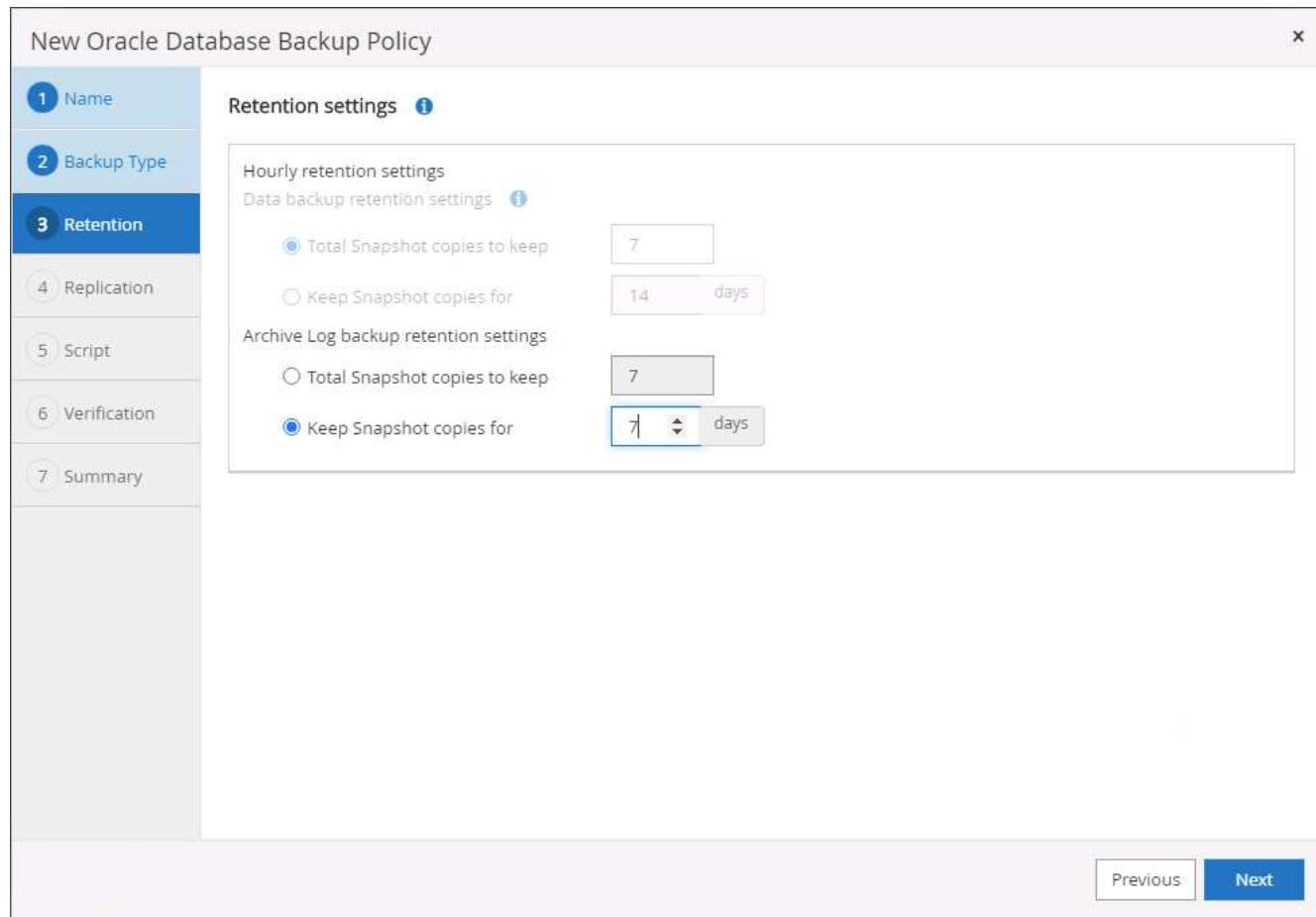
**7 Summary**

Previous Next

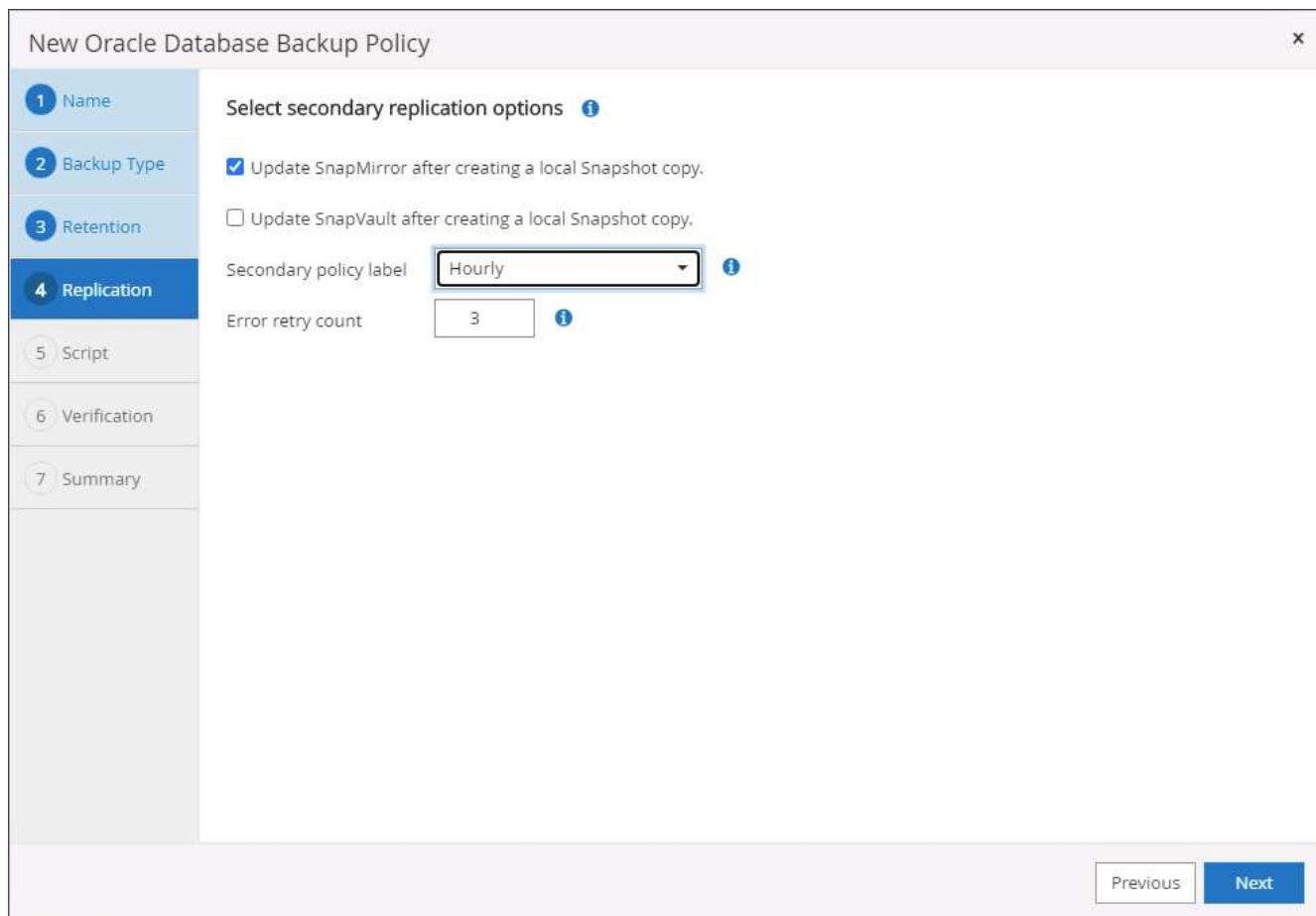
3. Select the backup type and schedule frequency.



4. Set the log retention period.



5. Enable replication to a secondary location in the public cloud.



6. Specify any optional scripts to run before and after log backup.

New Oracle Database Backup Policy X

Specify optional scripts to run before and after performing a backup job

1 Name	Prescript full path <input type="text" value="/var/opt/snapcenter/spl/scripts/"/> Enter Prescript path	
2 Backup Type	Prescript arguments <input type="text"/>	
3 Retention	Postscript full path <input type="text" value="/var/opt/snapcenter/spl/scripts/"/> Enter Postscript path	
4 Replication	Postscript arguments <input type="text"/>	
5 Script	Script timeout <input type="text" value="60"/> secs	
6 Verification		
7 Summary		

Previous Next

7. Specify any backup verification scripts.

New Oracle Database Backup Policy X

**1 Name** Select the options to run backup verification

**2 Backup Type** Run Verifications for following backup schedules

**3 Retention** Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

**4 Replication**

**5 Script**

**6 Verification** Verification script commands

Script timeout 60 secs

Prescript full path /var/opt/snapcenter/spl/scripts/ Enter Prescript path

Prescript arguments Choose optional arguments...

Postscript full path /var/opt/snapcenter/spl/scripts/ Enter Postscript path

Postscript arguments Choose optional arguments...

[Previous](#) [Next](#)

8. Summary.

New Oracle Database Backup Policy

1 Name	Summary
2 Backup Type	Policy name: Oracle Archive Log Backup Details: Backup Oracle archive logs
3 Retention	Backup type: Online backup
4 Replication	Schedule type: Hourly RMAN catalog backup: Disabled
5 Script	Archive log pruning: None
6 Verification	On demand data backup retention: None
7 Summary	On demand archive log backup retention: None Hourly data backup retention: None Hourly archive log backup retention: Delete Snapshot copies older than : 7 days Daily data backup retention: None Daily archive log backup retention: None Weekly data backup retention: None Weekly archive log backup retention: None Monthly data backup retention: None Monthly archive log backup retention: None Replication: SnapMirror enabled , Secondary policy label: Hourly , Error retry count: 3
	<a href="#">Previous</a> <a href="#">Finish</a>

## Create a full database backup policy for SQL

1. Log into SnapCenter with a database management user ID, click Settings, and then click Policies.

The screenshot shows the NetApp SnapCenter interface. On the left, there's a sidebar with icons for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings (which is selected), and Alerts. The main area has a header with 'NetApp SnapCenter®', 'Policies' (selected), 'Credential' (set to Microsoft SQL Server), and user info ('demo@sqldba'). Below the header is a search bar and a message: 'There is no match for your search or data is not available.' To the right are buttons for 'New', 'Modify', 'Copy', 'Details', and 'Delete'.

2. Click New to launch a new backup policy creation workflow, or choose an existing policy for modification.

New SQL Server Backup Policy

**1 Name**

Provide a policy name

Policy name: SQL Server Full Backup i

Details: Backup all data and log files

**2 Backup Type**

**3 Retention**

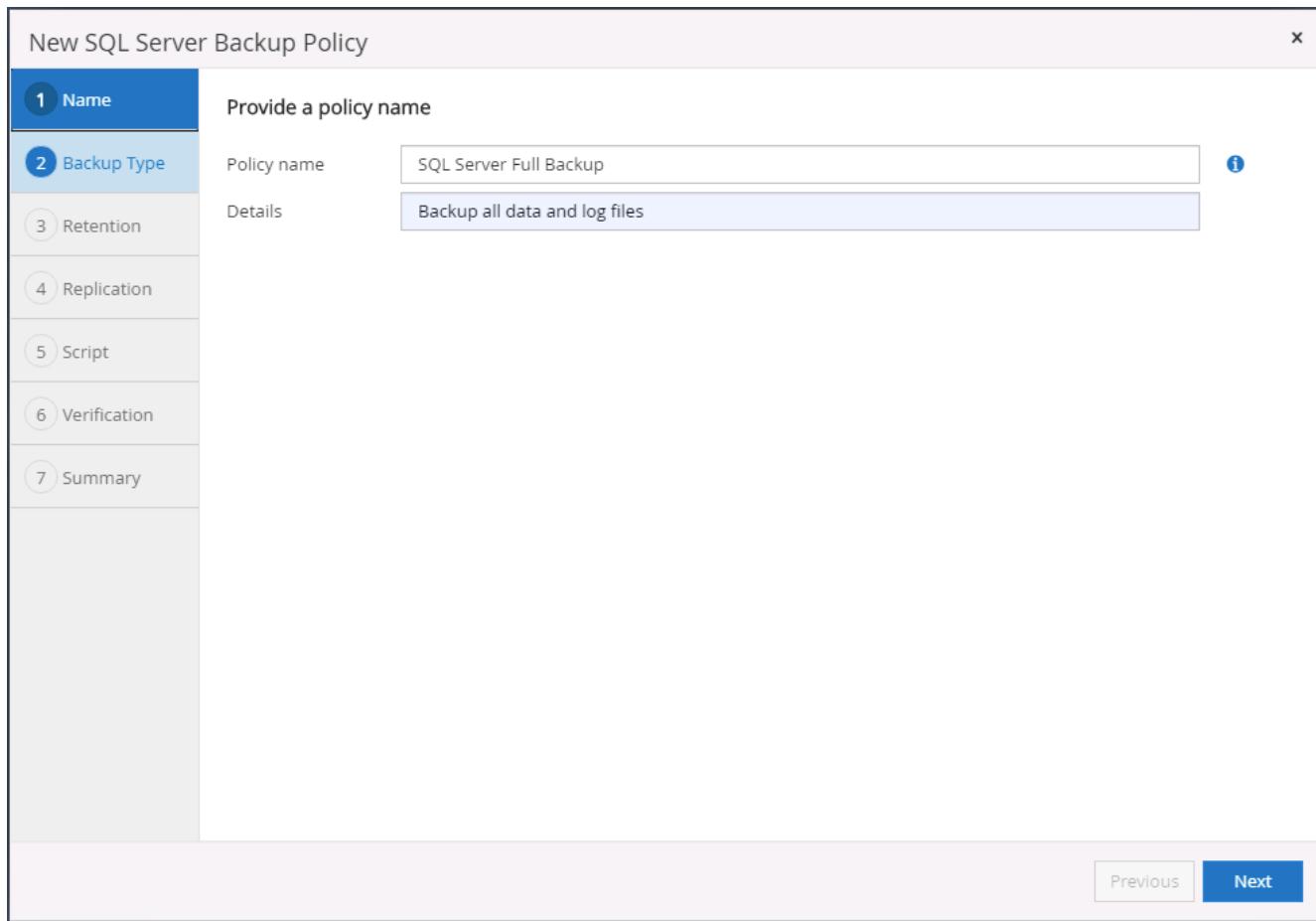
**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Previous Next



3. Define the backup option and schedule frequency. For SQL Server configured with an availability group, a preferred backup replica can be set.

New SQL Server Backup Policy X

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Select SQL server backup options

Choose backup type

Full backup and log backup

Full backup

Log backup

Copy only backup i

Maximum databases backed up per Snapshot copy: 100 i

**Availability Group Settings** ▼

Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

On demand

Hourly

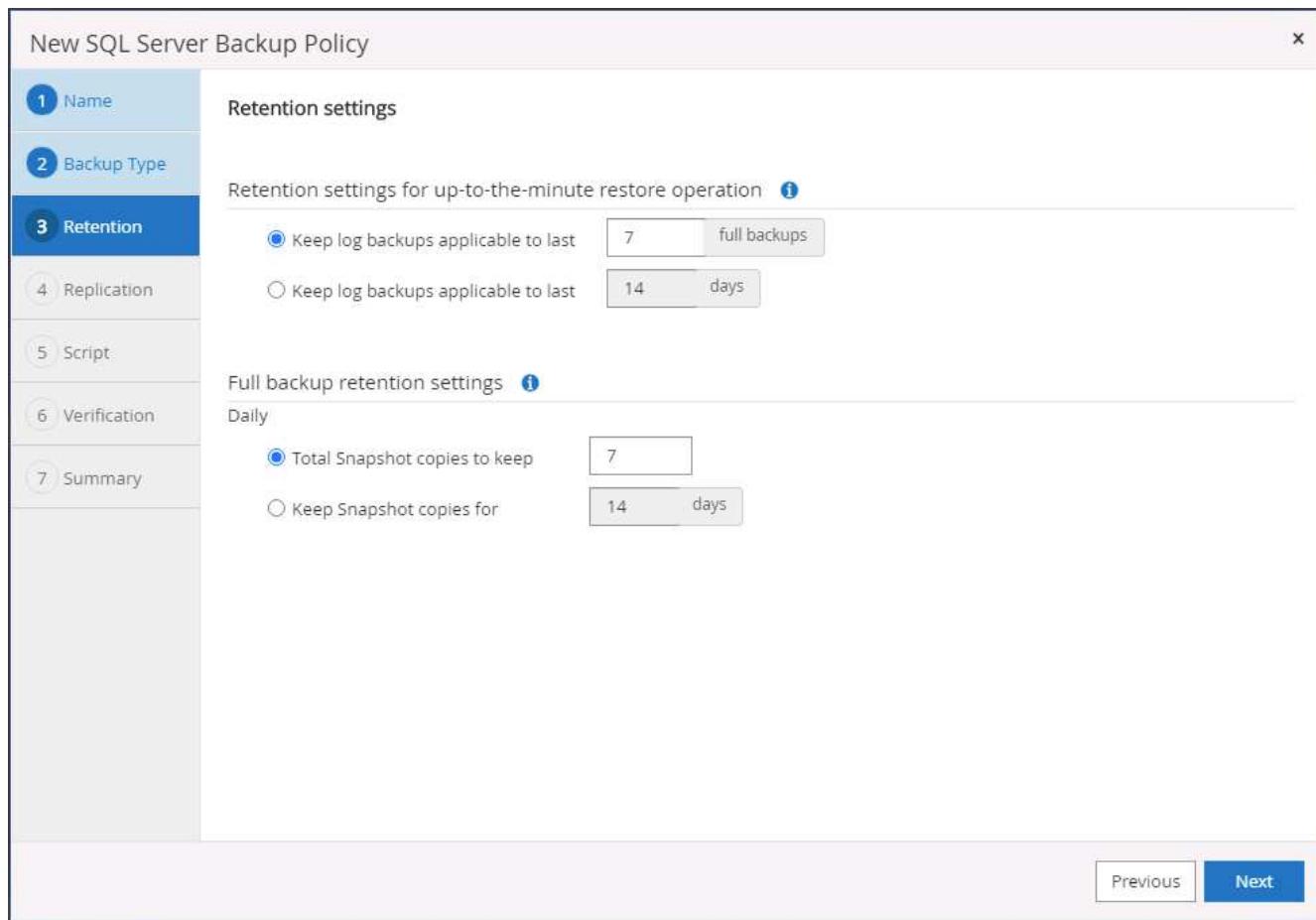
Daily

Weekly

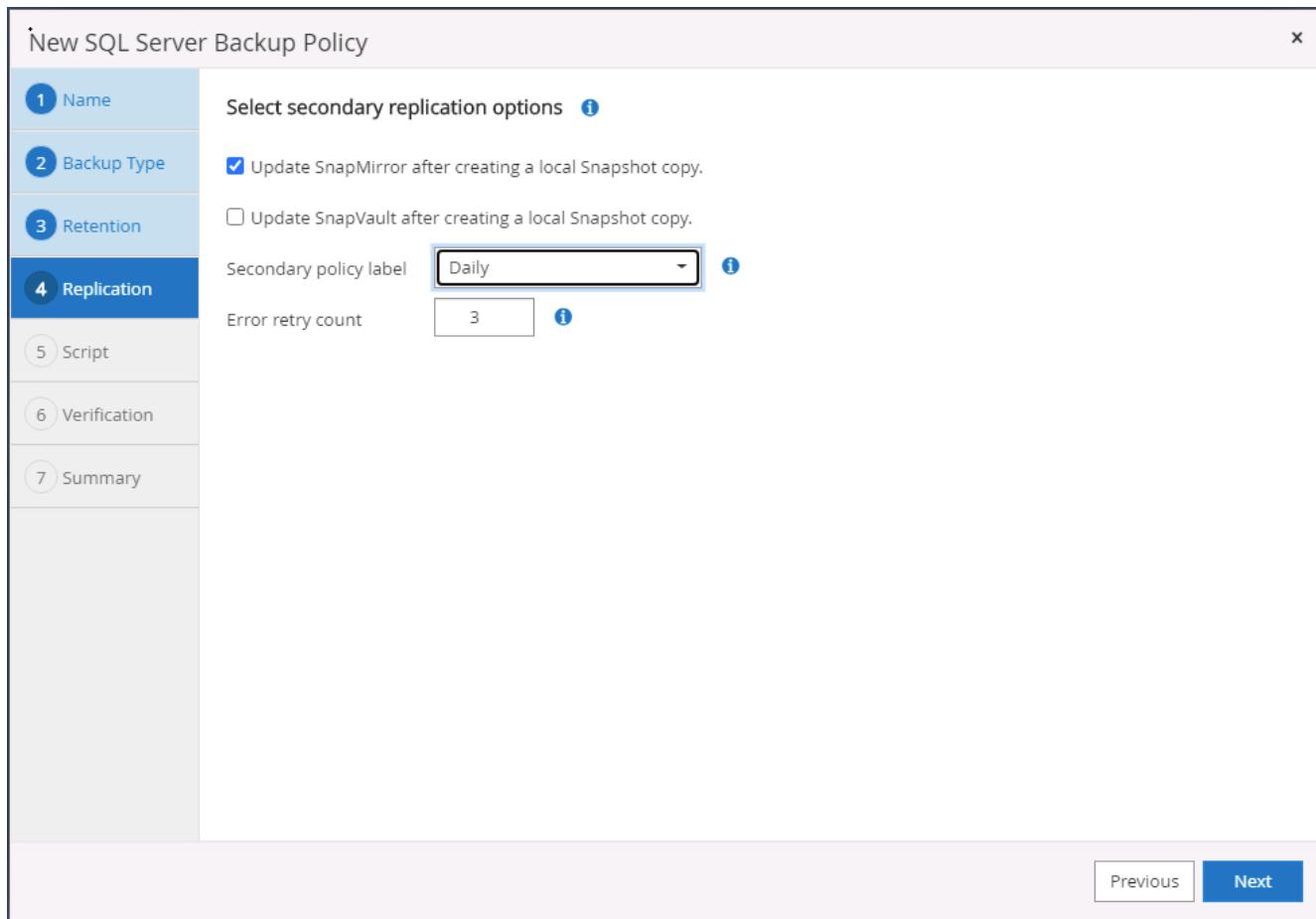
Monthly

Previous Next

4. Set the backup retention period.



5. Enable backup copy replication to a secondary location in cloud.



6. Specify any optional scripts to run before or after a backup job.

New SQL Server Backup Policy X

**1 Name** Specify optional scripts to run before performing a backup job

**2 Backup Type** Prescript full path

**3 Retention** Prescript arguments  Choose optional arguments...

**4 Replication** Specify optional scripts to run after performing a backup job

**5 Script** Postscript full path   
Postscript arguments  Choose optional arguments...

**6 Verification** Script timeout  60  secs

**7 Summary**

Previous Next

7. Specify the options to run backup verification.

New SQL Server Backup Policy

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Select the options to run backup verification

Run verifications for the following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

Daily

Database consistency checks options

Limit the integrity structure to physical structure of the database (PHYSICAL\_ONLY)

Suppress all information message (NO\_INFOMSGS)

Display all reported error messages per object (ALL\_ERRORMSGGS)

Do not check non-clustered indexes (NOINDEX)

Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK)

Log backup

Verify log backup. i

Verification script settings

Script timeout  secs

Previous Next

8. Summary.

New SQL Server Backup Policy X

1 Name	Summary
2 Backup Type	Policy name: SQL Server Full Backup
3 Retention	Details: Backup all data and log files
4 Replication	Backup type: Full backup and log backup
5 Script	Availability group settings: Backup only on preferred backup replica
6 Verification	Schedule Type: Daily UTM retention: Total backup copies to retain : 7 Daily Full backup retention: Total backup copies to retain : 7 Replication: SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3
7 Summary	Backup prescript settings: undefined Prescript arguments: Backup postscript settings: undefined Postscript arguments: Verification for backup schedule type: none Verification prescript settings: undefined Prescript arguments: Verification postscript settings: undefined Postscript arguments:
<a href="#">Previous</a> <span style="background-color: #0070C0; color: white; padding: 2px 10px; border-radius: 5px;">Finish</span>	

### Create a database log backup policy for SQL.

1. Log into SnapCenter with a database management user ID, click Settings > Policies, and then New to launch a new policy creation workflow.

New SQL Server Backup Policy X

Provide a policy name

Policy name	SQL Server Log Backup	<span style="color: blue;">i</span>
Details	Backup SQL server log	

1 Name      2 Backup Type      3 Retention      4 Replication      5 Script      6 Verification      7 Summary

Previous      Next

The screenshot shows the 'New SQL Server Backup Policy' wizard. The 'Name' tab is selected. The 'Policy name' field is filled with 'SQL Server Log Backup'. The 'Details' field contains 'Backup SQL server log'. The 'Next' button is visible at the bottom right.

- Define the log backup option and schedule frequency. For SQL Server configured with a availability group, a preferred backup replica can be set.

New SQL Server Backup Policy X

**1 Name**

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

**6 Verification**

**7 Summary**

Select SQL server backup options

Choose backup type

Full backup and log backup  
 Full backup  
 Log backup  
 Copy only backup i

Maximum databases backed up per Snapshot copy: 100 i

**Availability Group Settings** ▼

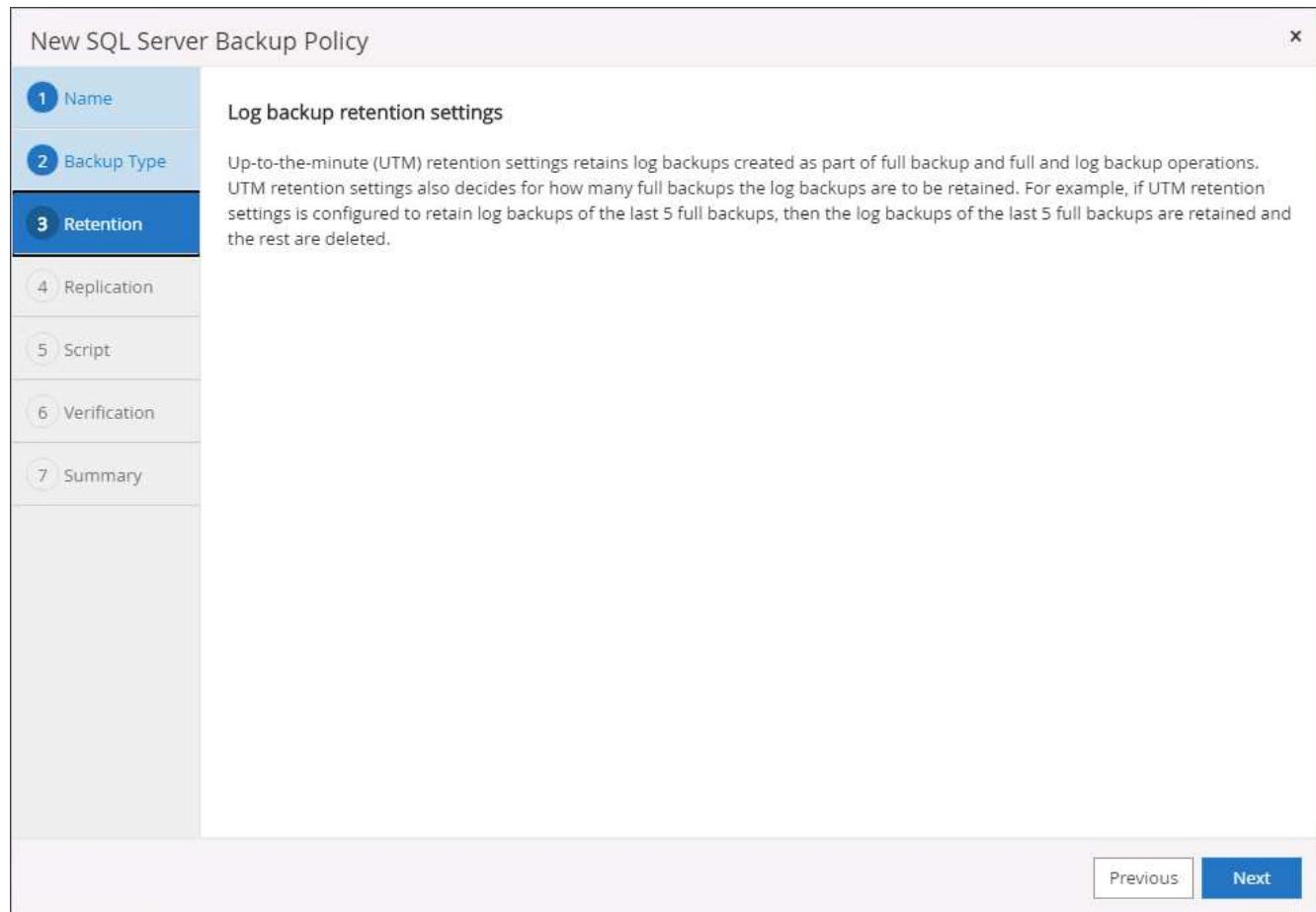
Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

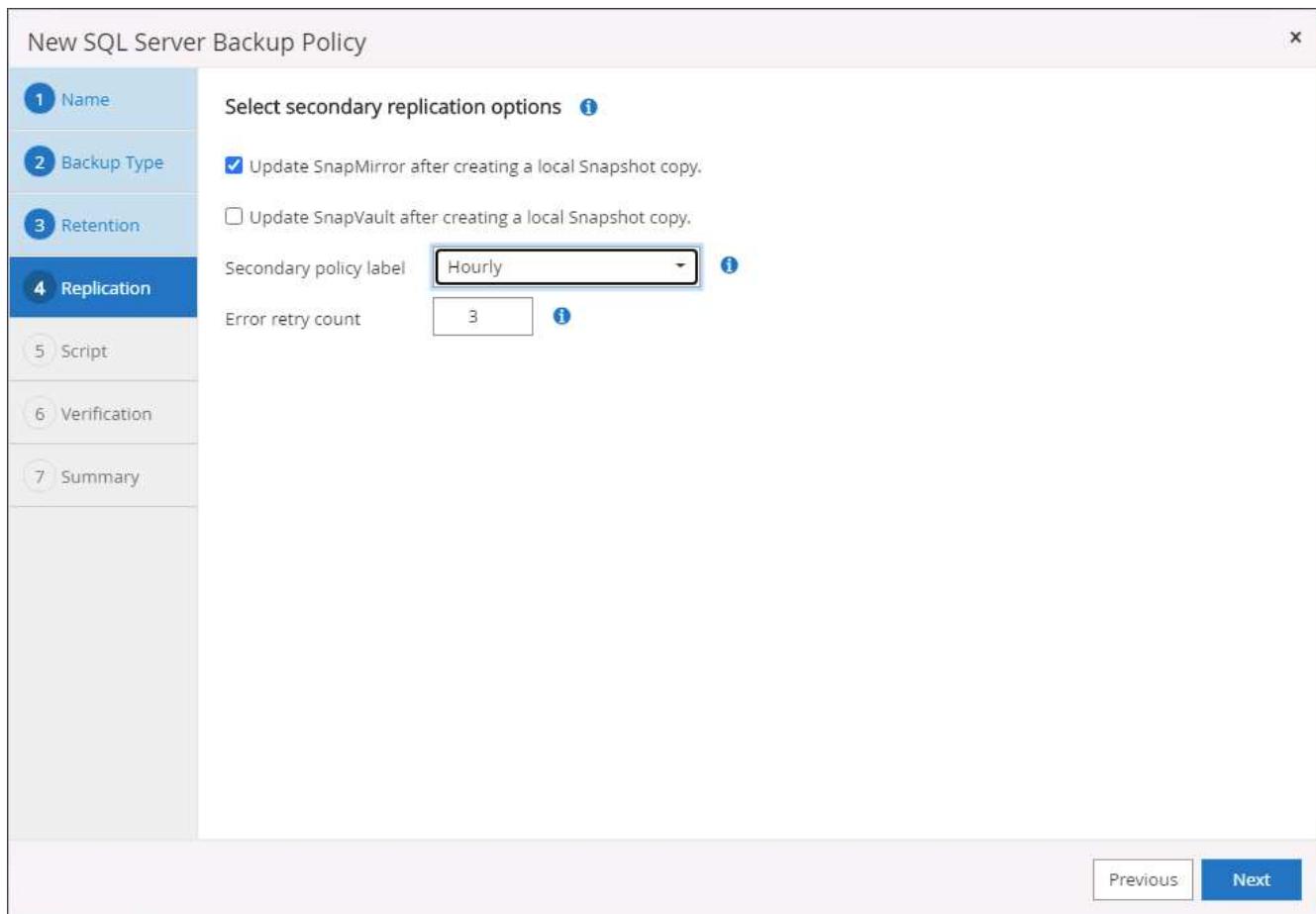
On demand  
 Hourly  
 Daily  
 Weekly  
 Monthly

Previous Next

3. SQL server data backup policy defines the log backup retention; accept the defaults here.



4. Enable log backup replication to secondary in the cloud.



5. Specify any optional scripts to run before or after a backup job.

New SQL Server Backup Policy X

**1 Name**

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments  Choose optional arguments...

**2 Backup Type**

**3 Retention**

**4 Replication**

**5 Script**

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments  Choose optional arguments...

Script timeout  60  secs

**6 Verification**

**7 Summary**

Previous Next

6. Summary.

New SQL Server Backup Policy

Step	Setting
1 Name	Summary
2 Backup Type	Policy name: SQL Server Log Backup Details: Backup SQL server log
3 Retention	Backup type: Log transaction backup
4 Replication	Availability group settings: Backup only on preferred backup replica
5 Script	Schedule Type: Hourly Replication: SnapMirror enabled, Secondary policy label: Hourly, Error retry count: 3
6 Verification	Backup prescript settings: undefined Prescript arguments: Backup postscript settings: undefined Postscript arguments:
7 Summary	Verification for backup schedule type: none Verification prescript settings: undefined Prescript arguments: Verification postscript settings: undefined Postscript arguments:

Previous Finish

## 8. Implement backup policy to protect database

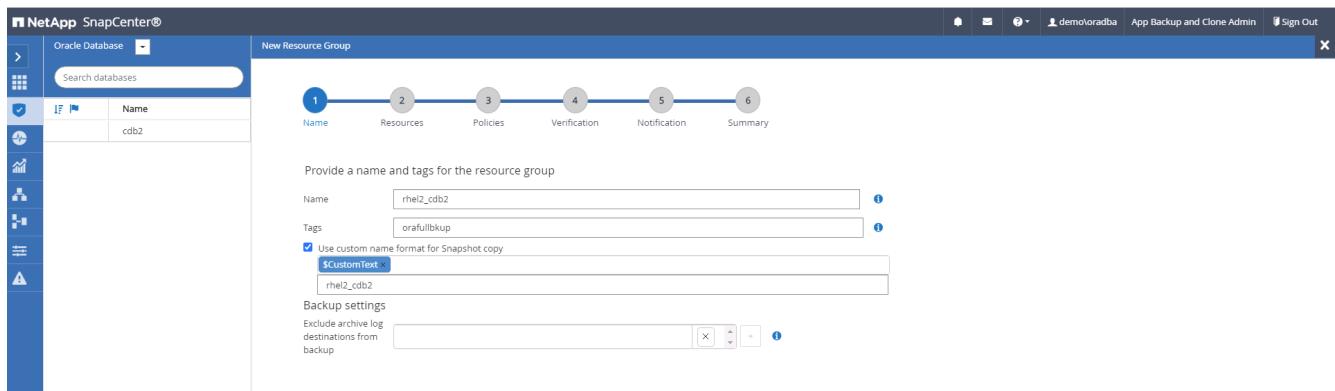
SnapCenter uses a resource group to backup a database in a logical grouping of database resources, such as multiple databases hosted on a server, a database sharing the same storage volumes, multiple databases supporting a business application, and so on. Protecting a single database creates a resource group of its own. The following procedures demonstrate how to implement a backup policy created in section 7 to protect Oracle and SQL Server databases.

### Create a resource group for full backup of Oracle

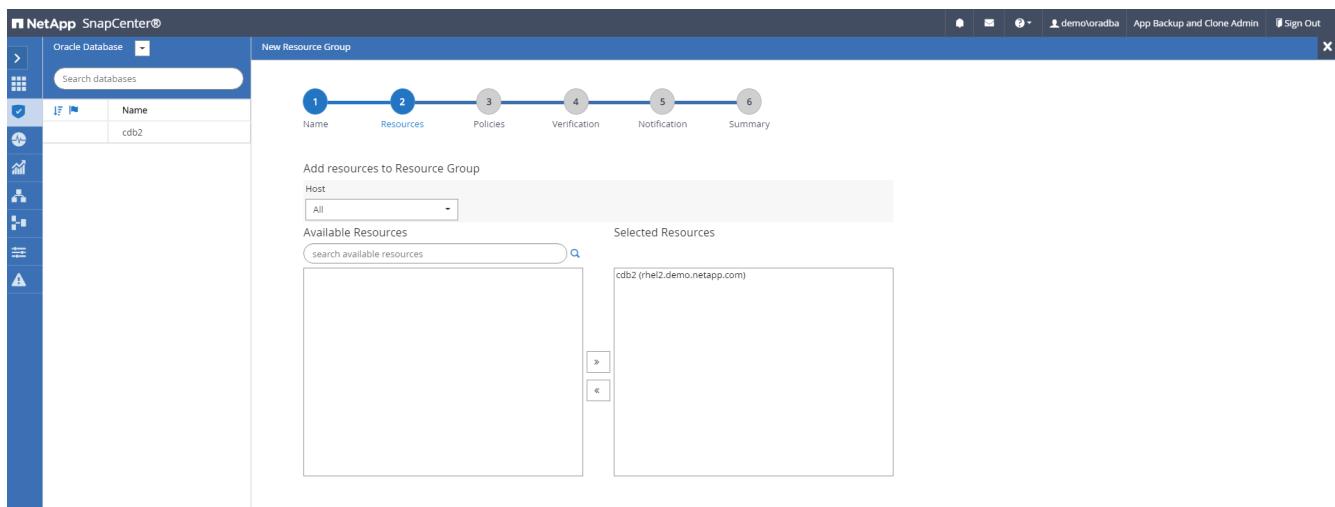
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either Database or Resource Group to launch the resource group creation workflow.

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com				Not protected

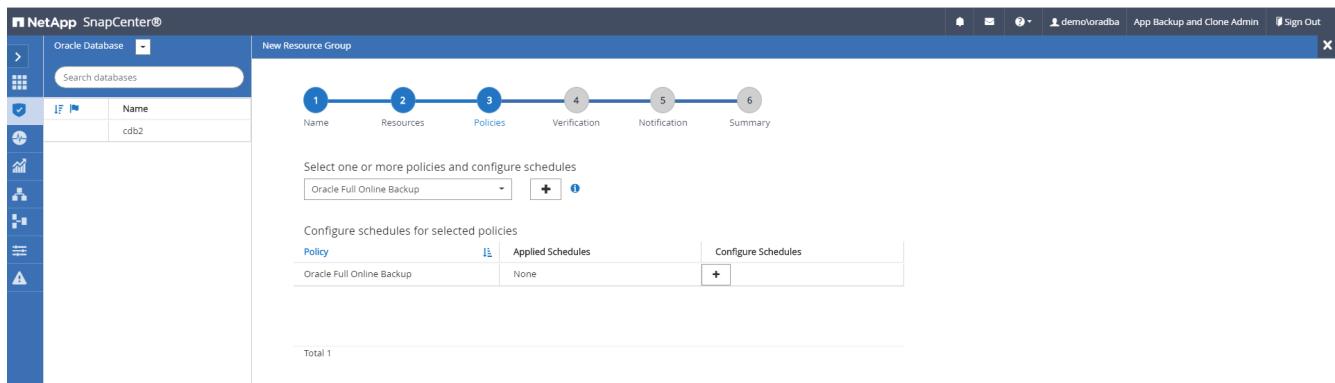
2. Provide a name and tags for the resource group. You can define a naming format for the Snapshot copy and bypass the redundant archive log destination if configured.



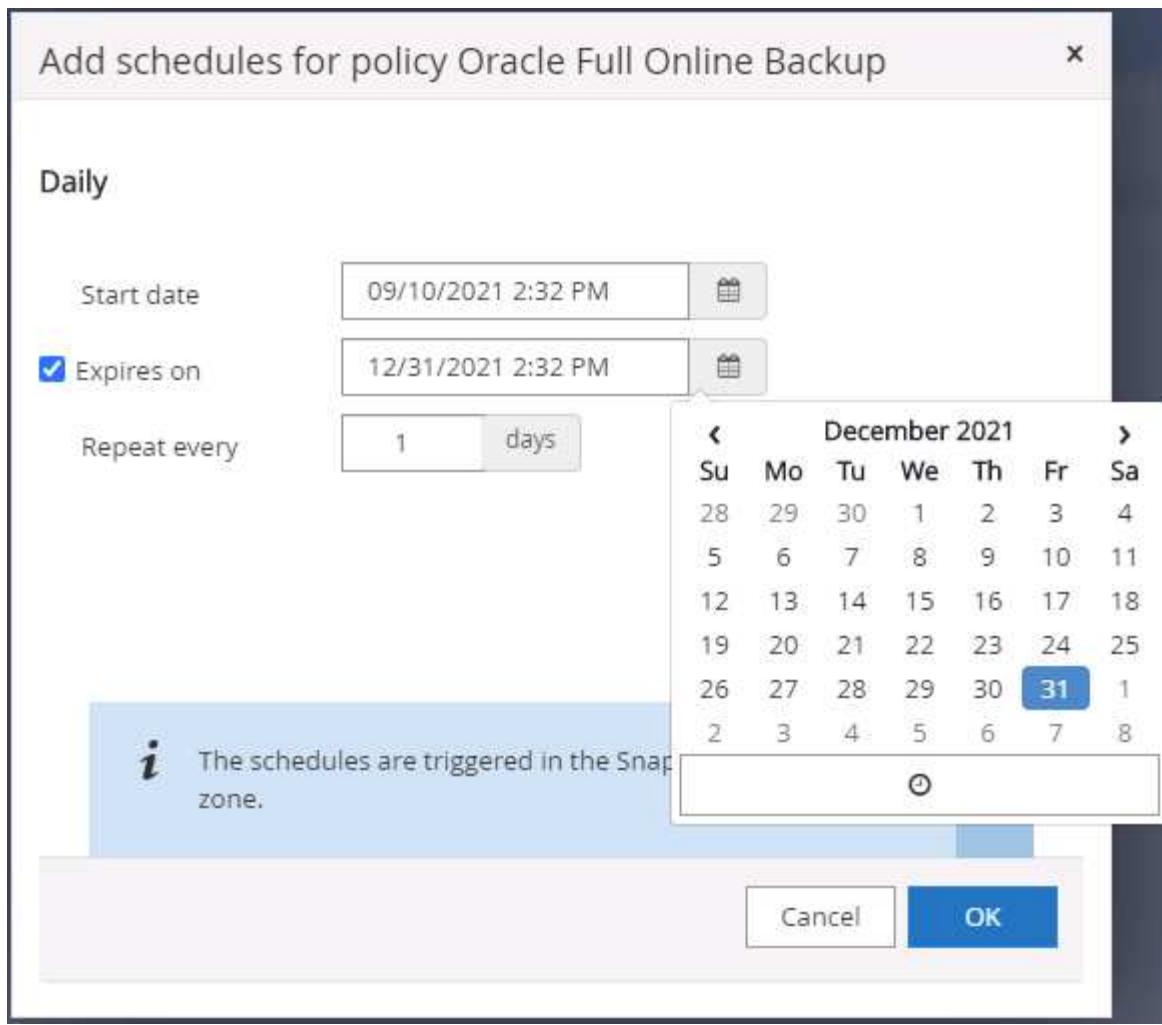
### 3. Add database resources to the resource group.



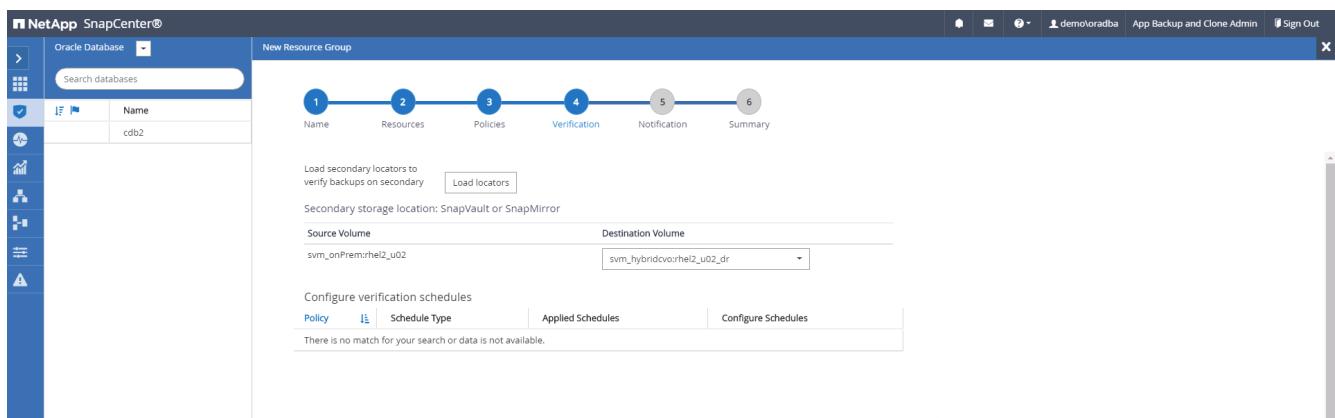
### 4. Select a full backup policy created in section 7 from the drop-down list.



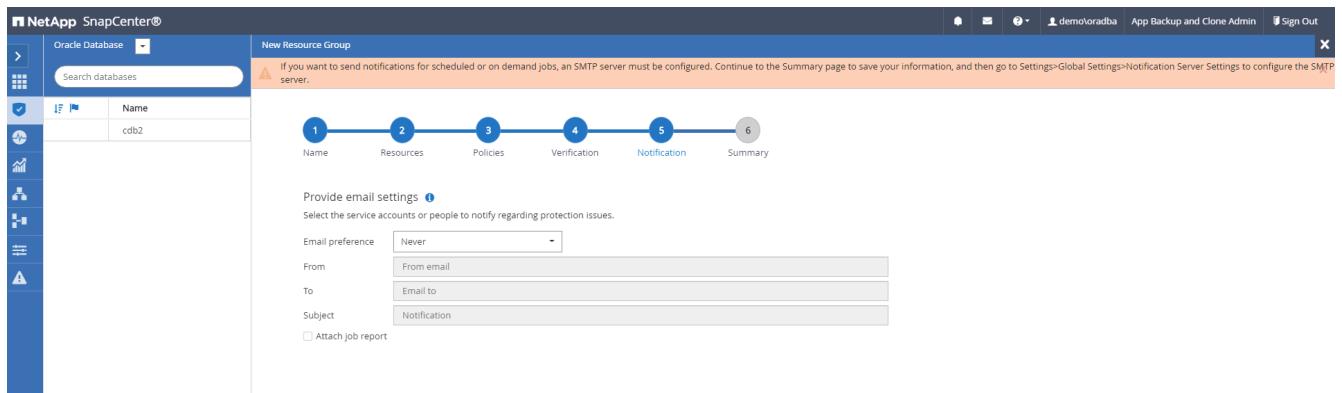
### 5. Click the (+) sign to configure the desired backup schedule.



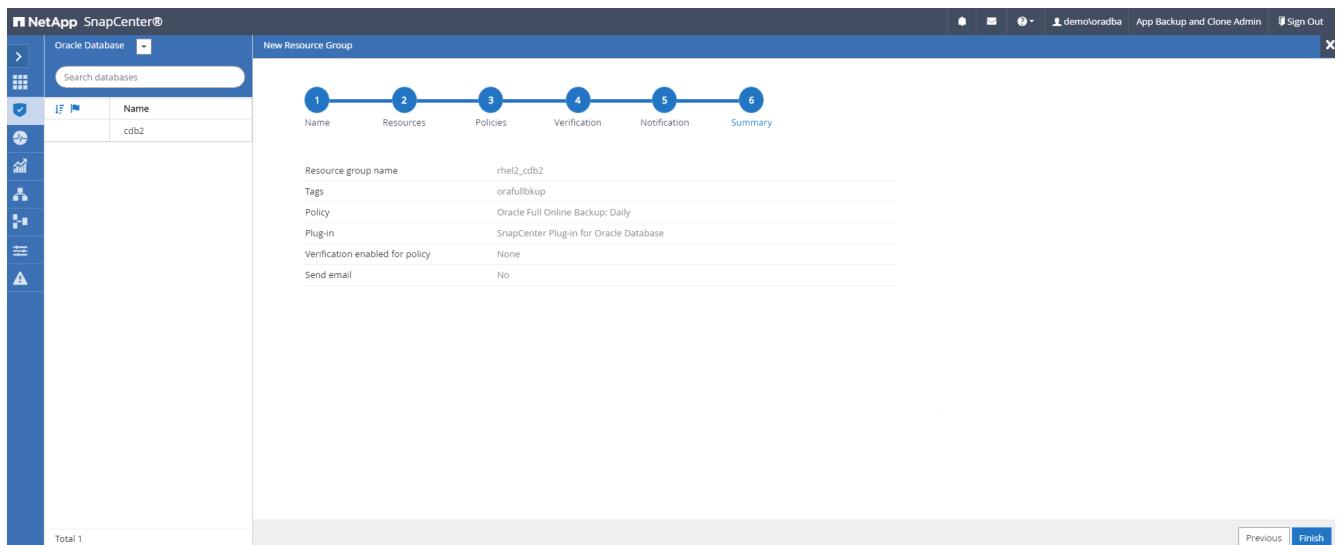
6. Click Load Locators to load the source and destination volume.



7. Configure the SMTP server for email notification if desired.

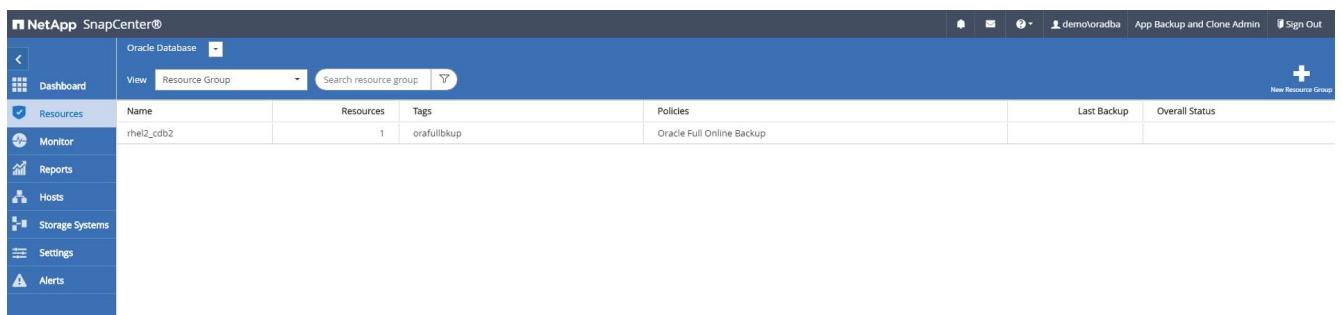


## 8. Summary.

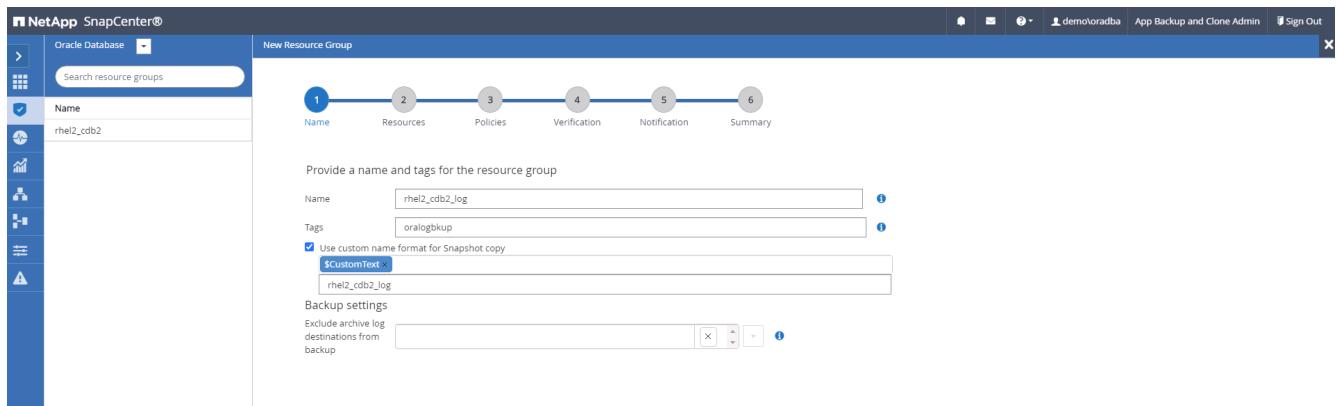


## Create a resource group for log backup of Oracle

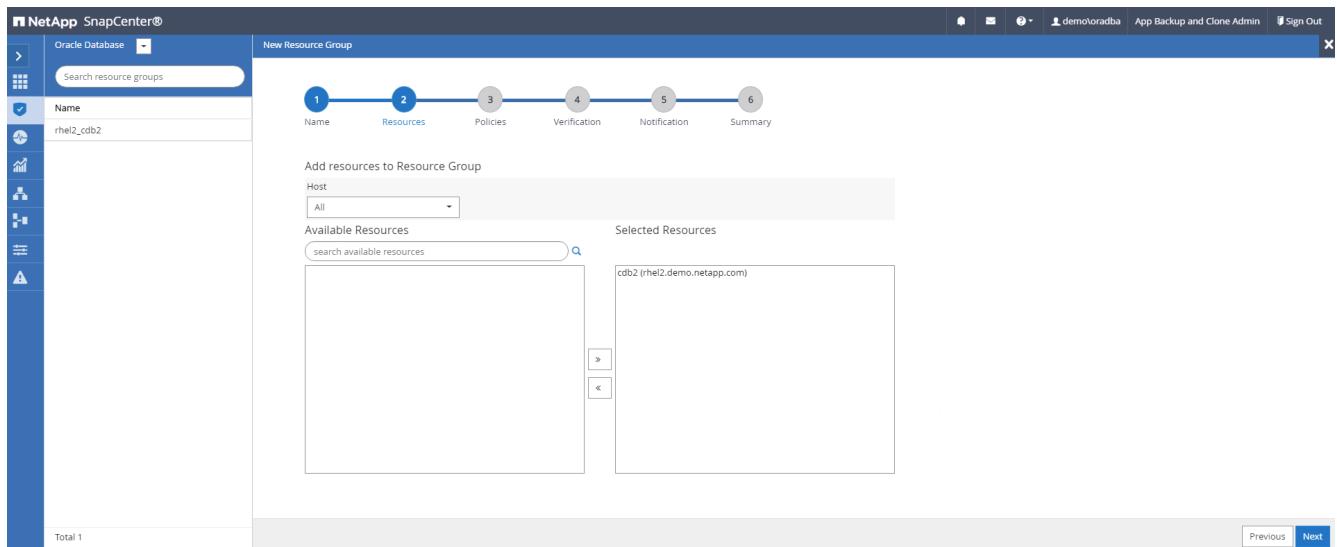
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either Database or Resource Group to launch the resource group creation workflow.



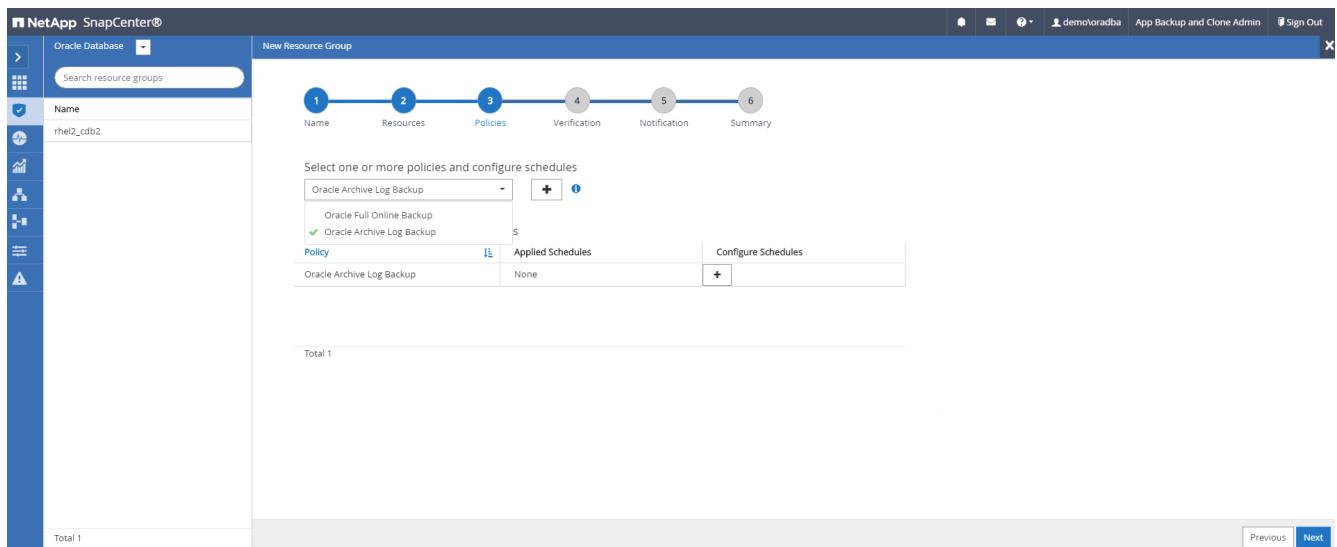
2. Provide a name and tags for the resource group. You can define a naming format for the Snapshot copy and bypass the redundant archive log destination if configured.



3. Add database resources to the resource group.



4. Select a log backup policy created in section 7 from the drop-down list.



5. Click on the (+) sign to configure the desired backup schedule.

Add schedules for policy Oracle Archive Log Backup x

**Hourly**

Start date   

Expires on   

Repeat every  hours  mins

**i** The schedules are triggered in the SnapCenter Server time zone. X

Cancel OK

6. If backup verification is configured, it displays here.

NetApp SnapCenter®

Oracle Database  

New Resource Group

Name

Search resource groups

1 Name      2 Resources      3 Policies      4 Verification      5 Notification      6 Summary

Configure verification schedules

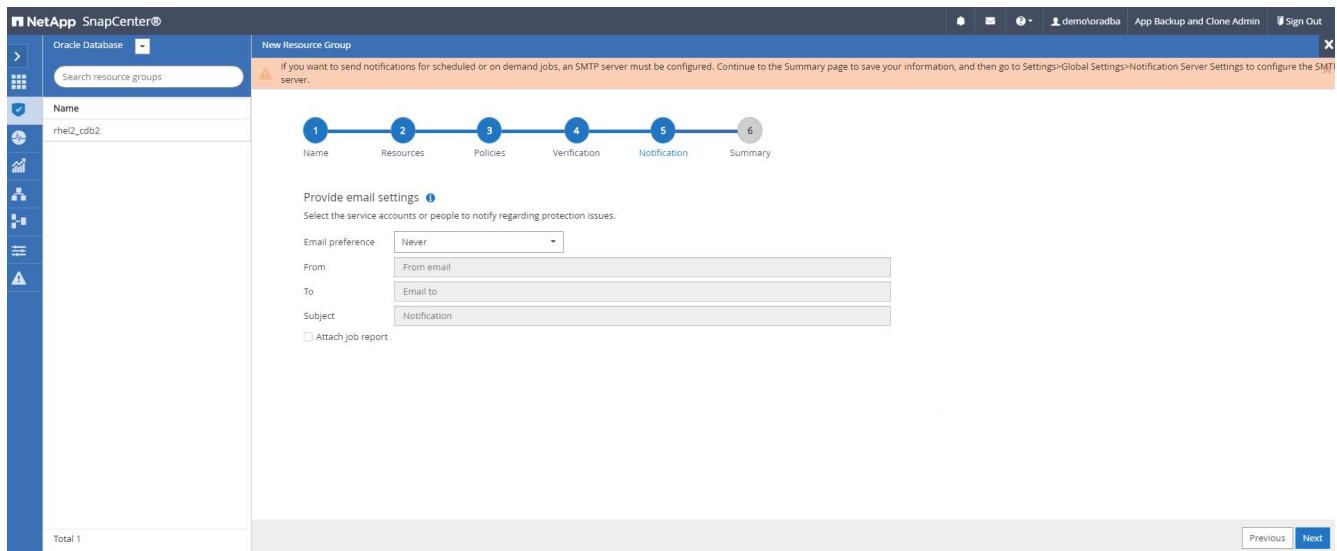
Policy   Schedule Type   Applied Schedules   Configure Schedules

There is no match for your search or data is not available.

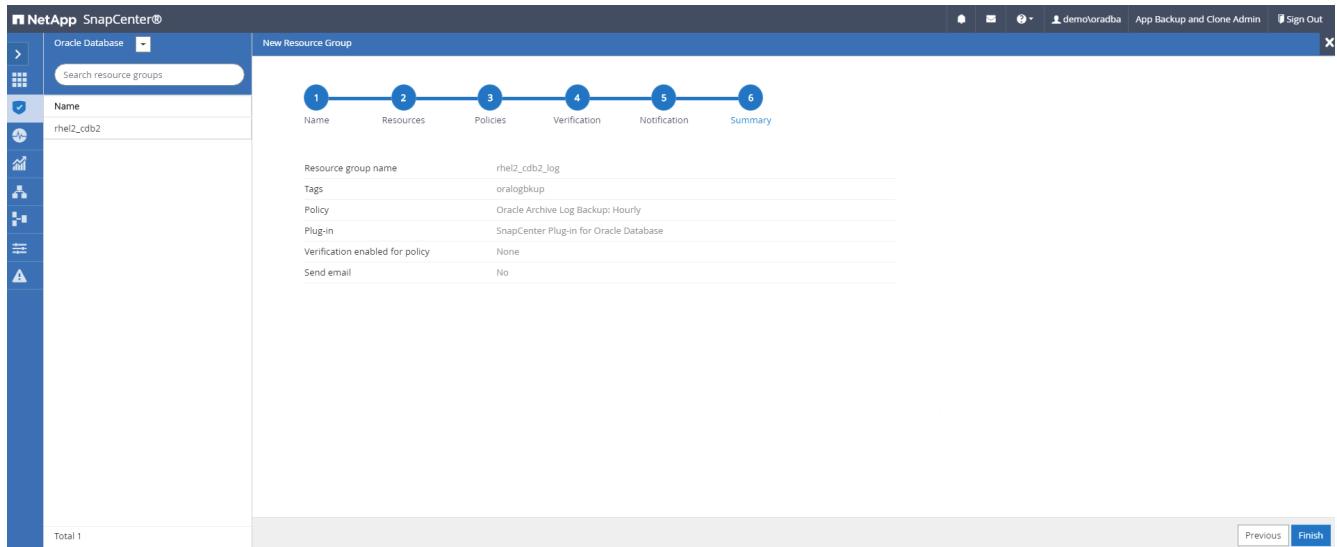
Total 0

Previous Next

7. Configure an SMTP server for email notification if desired.



## 8. Summary.



## Create a resource group for full backup of SQL Server

1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either a Database or Resource Group to launch the resource group creation workflow. Provide a name and tags for the resource group. You can define a naming format for the Snapshot copy.

The screenshot shows the 'New Resource Group' wizard in the NetApp SnapCenter interface. The left sidebar lists databases: master, model, msdb, tempdb, and tpcc. The main area shows the first step of the wizard, 'Name'. The user has entered 'sql1\_tpcc' in the 'Name' field and 'sqlfullbkup' in the 'Tags' field. A checkbox for 'Use custom name format for Snapshot copy' is checked, with '\$CustomText' expanded to show 'sql1\_tpcc'.

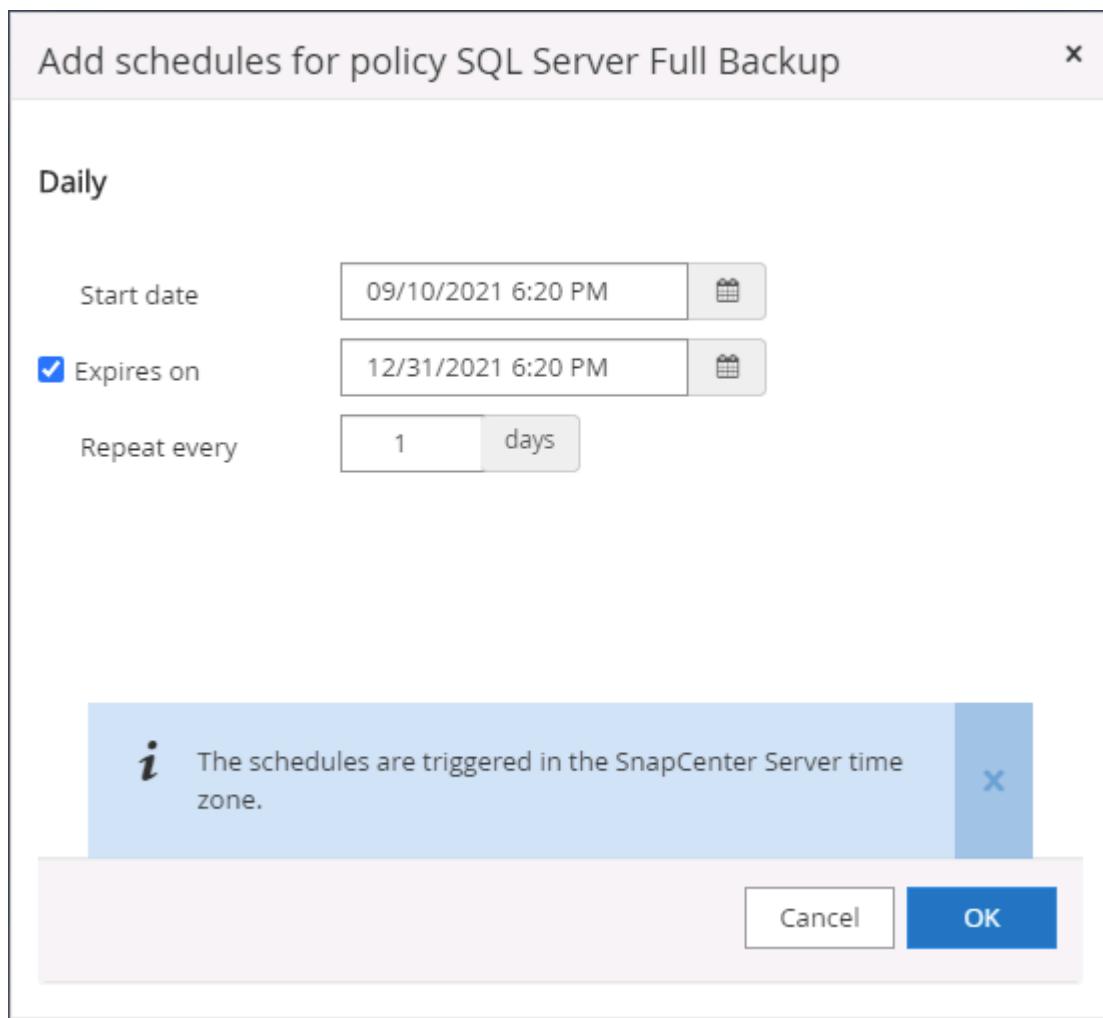
## 2. Select the database resources to be backed up.

The screenshot shows the 'New Resource Group' wizard in the NetApp SnapCenter interface. The left sidebar lists databases: master, model, msdb, tempdb, and tpcc. The main area shows the second step of the wizard, 'Resources'. The 'Host' dropdown is set to 'All', 'Resource Type' to 'Databases', and 'SQL Server Instance' to 'sql1'. Under 'Available Resources', 'tpcc' is listed. Under 'Selected Resources', 'tpcc (sql1)' is selected. A checkbox for 'Auto select all the resources from the same storage volume' is checked.

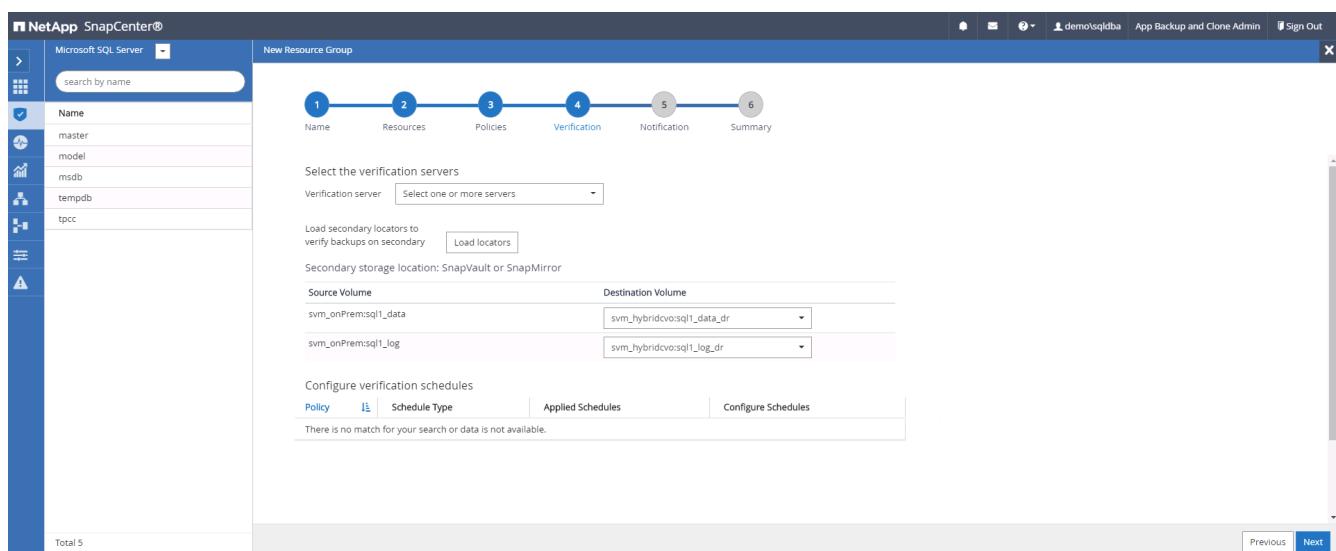
## 3. Select a full SQL backup policy created in section 7.

The screenshot shows the 'New Resource Group' wizard in the NetApp SnapCenter interface. The left sidebar lists databases: master, model, msdb, tempdb, and tpcc. The main area shows the third step of the wizard, 'Policies'. A dropdown menu shows 'SQL Server Full Backup' selected. Below it, a table shows the 'Policy' as 'SQL Server Full Backup', 'Applied Schedules' as 'None', and a 'Configure Schedules' button. A note at the bottom says 'Total 1' and there is a checkbox for 'Use Microsoft SQL Server scheduler'.

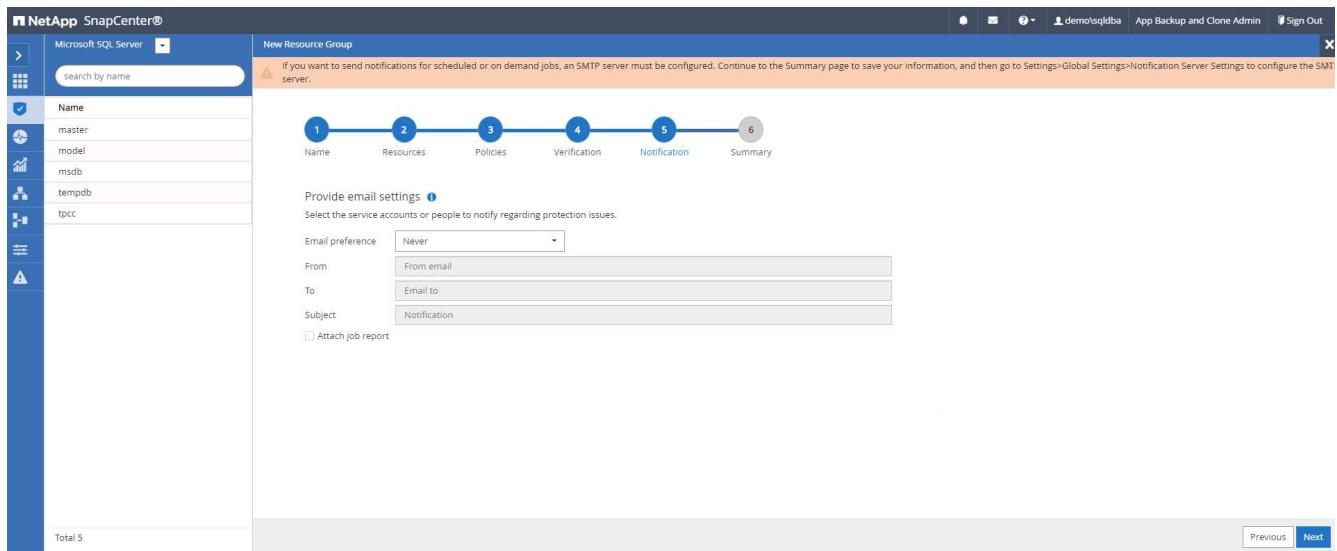
- Add exact timing for backups as well as the frequency.



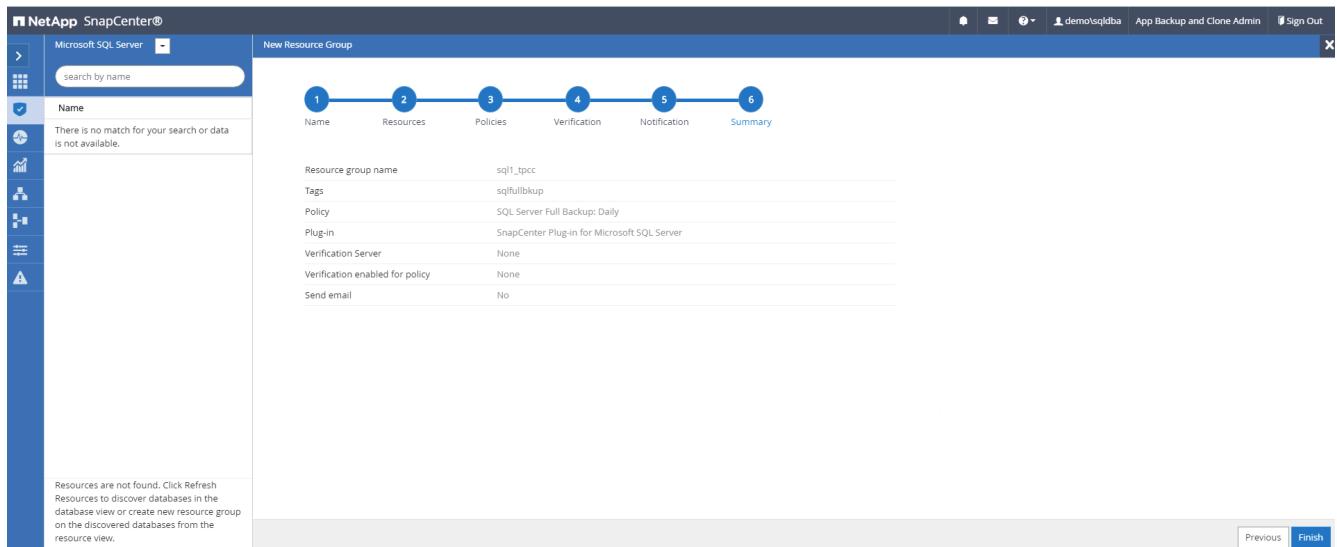
- Choose the verification server for the backup on secondary if backup verification is to be performed. Click Load Locator to populate the secondary storage location.



- Configure the SMTP server for email notification if desired.

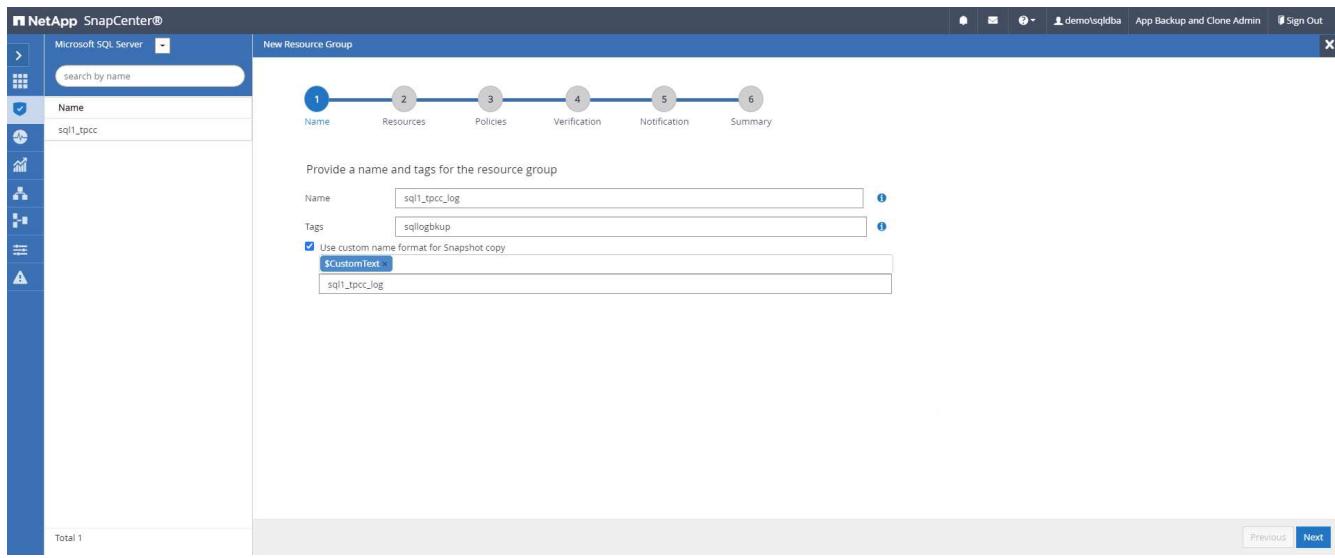


## 7. Summary.

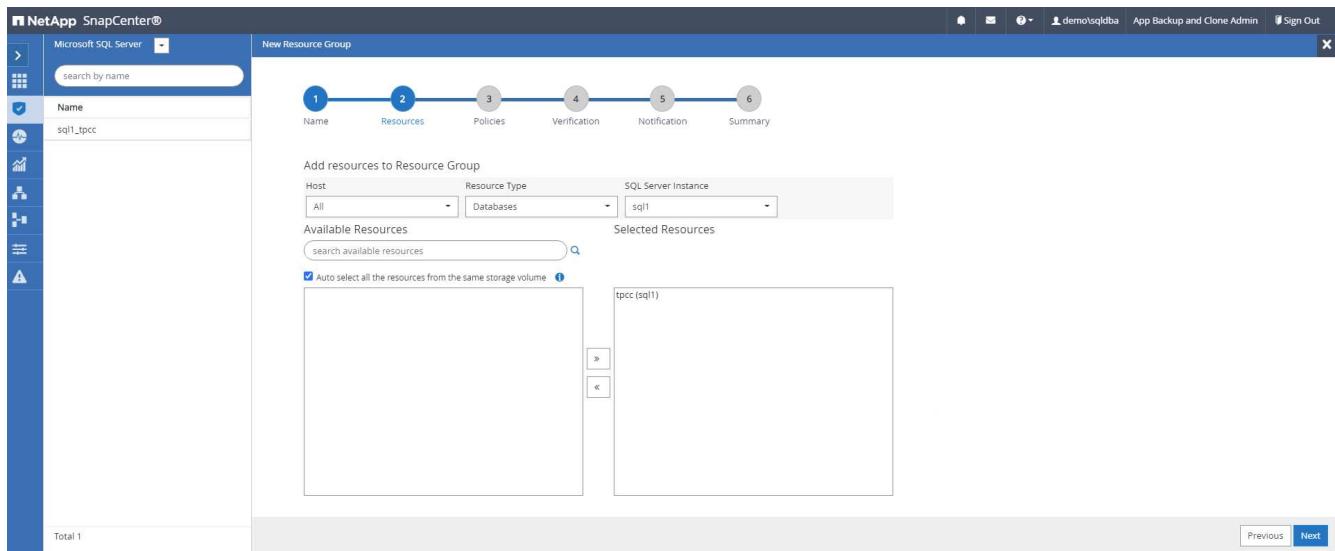


## Create a resource group for log backup of SQL Server

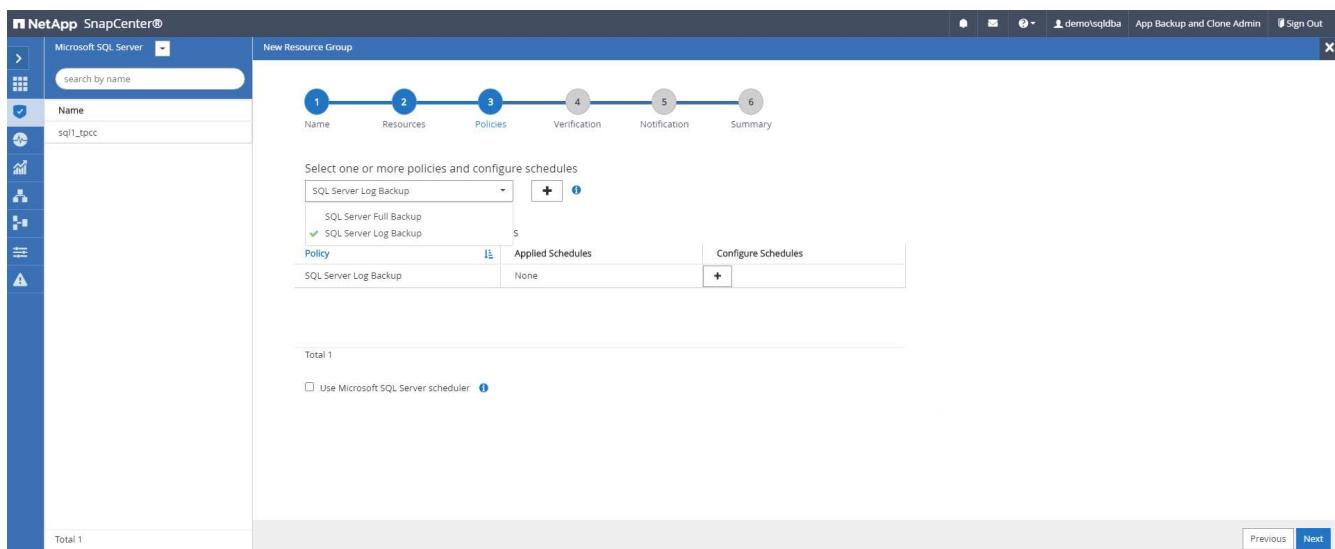
1. Log into SnapCenter with a database management user ID, and navigate to the Resources tab. In the View drop-down list, choose either a Database or Resource Group to launch the resource group creation workflow. Provide the name and tags for the resource group. You can define a naming format for the Snapshot copy.



## 2. Select the database resources to be backed up.



## 3. Select a SQL log backup policy created in section 7.



4. Add exact timing for the backup as well as the frequency.

The screenshot shows the 'New Resource Group' wizard in NetApp SnapCenter. The current step is 'Policies'. A table lists a single policy: 'SQL Server Log Backup' with an applied schedule of 'Hourly: Repeat every 1 hours'. There is also an option to 'Configure Schedules'. The navigation bar at the top includes tabs for Name, Resources, Policies, Verification, Notification, and Summary. On the left, there's a sidebar with various icons and a search bar.

5. Choose the verification server for the backup on secondary if backup verification is to be performed. Click the Load Locator to populate the secondary storage location.

The screenshot shows the 'Verification' step of the 'New Resource Group' wizard. It allows selecting verification servers and configuring verification schedules. The 'Source Volume' and 'Destination Volume' fields are filled with specific volume names. The 'Configure verification schedules' section shows a message: 'There is no match for your search or data is not available.' Navigation tabs include Policy, Schedule Type, Applied Schedules, and Configure Schedules.

6. Configure the SMTP server for email notification if desired.

## 7. Summary.

## 9. Validate backup

After database backup resource groups are created to protect database resources, the backup jobs runs according to the predefined schedule. Check the job execution status under the Monitor tab.

ID	Status	Name	Start date	End date	Owner
532	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 8:35:01 PM	09/14/2021 8:37:10 PM	demo\sqldba
528	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 7:35:01 PM	09/14/2021 7:37:09 PM	demo\sqldba
524	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 6:35:01 PM	09/14/2021 6:37:08 PM	demo\sqldba
521	✓	Backup of Resource Group 'sql1_tpcc' with policy 'SQL Server Full Backup'	09/14/2021 6:25:01 PM	09/14/2021 6:27:14 PM	demo\sqldba
517	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 5:35:01 PM	09/14/2021 5:37:09 PM	demo\sqldba
513	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 4:35:01 PM	09/14/2021 4:37:08 PM	demo\sqldba
509	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 3:35:01 PM	09/14/2021 3:37:09 PM	demo\sqldba
503	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 2:35:01 PM	09/14/2021 2:37:09 PM	demo\sqldba

Go to the Resources tab, click the database name to view details of database backup, and toggle between Local copies and mirror copies to verify that Snapshot backups are replicated to a secondary location in the

public cloud.

The screenshot shows the NetApp SnapCenter interface for Oracle Database. On the left, a sidebar lists databases: cdb2, cdb2dev, cdb2dr, cdb2dr2, and cdb2test. The main area displays 'cdb2 Topology' with a summary card showing 394 Backups, 28 Data Backups, 366 Log Backups, and 3 Clones. It also shows 'Manage Copies' for Local copies (197 Backups, 0 Clones) and Mirror copies (197 Backups, 3 Clones). Below this is a table titled 'Primary Backup(s)' listing five backups:

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_09-23-2021_14.35.03.3242_1	1	Log	09/23/2021 2:35:45 PM	Not Applicable	False	Not Cataloged	6872761
rhel2_cdb2_09-23-2021_14.35.03.3242_0	1	Data	09/23/2021 2:35:30 PM	Unverified	False	Not Cataloged	6872715
rhel2_cdb2_09-22-2021_14.35.02.0014_1	1	Log	09/22/2021 2:35:24 PM	Not Applicable	False	Not Cataloged	6737479
rhel2_cdb2_09-22-2021_14.35.02.0014_0	1	Data	09/22/2021 2:35:14 PM	Unverified	False	Not Cataloged	6737395
rhel2_cdb2_09-21-2021_14.35.02.1884_1	1	Log	09/21/2021 2:35:35 PM	Not Available	False	Not Cataloged	6598735

At this point, database backup copies in the cloud are ready to clone to run dev/test processes or for disaster recovery in the event of a primary failure.

Next: [Getting Started with AWS public cloud](#).

## Getting Started with AWS public cloud

Previous: [Getting started on-premises](#).

### AWS public cloud



To make things easier to follow, we have created this document based on a deployment in AWS. However, the process is very similar for Azure and GCP.

#### 1. Pre-flight check

Before deployment, make sure that the infrastructure is in place to allow for the deployment in the next stage. This includes the following:

- AWS account
- VPC in your region of choice
- Subnet with access to the public internet
- Permissions to add IAM roles into your AWS account
- A secret key and access key for your AWS user

#### 2. Steps to deploy Cloud Manager and Cloud Volumes ONTAP in AWS



There are many methods for deploying Cloud Manager and Cloud Volumes ONTAP; this method is the simplest but requires the most permissions. If this method is not appropriate for your AWS environment, please consult the [NetApp Cloud Documentation](#).

#### Deploy the Cloud Manager connector

1. Navigate to [NetApp Cloud Central](#) and log in or sign up.



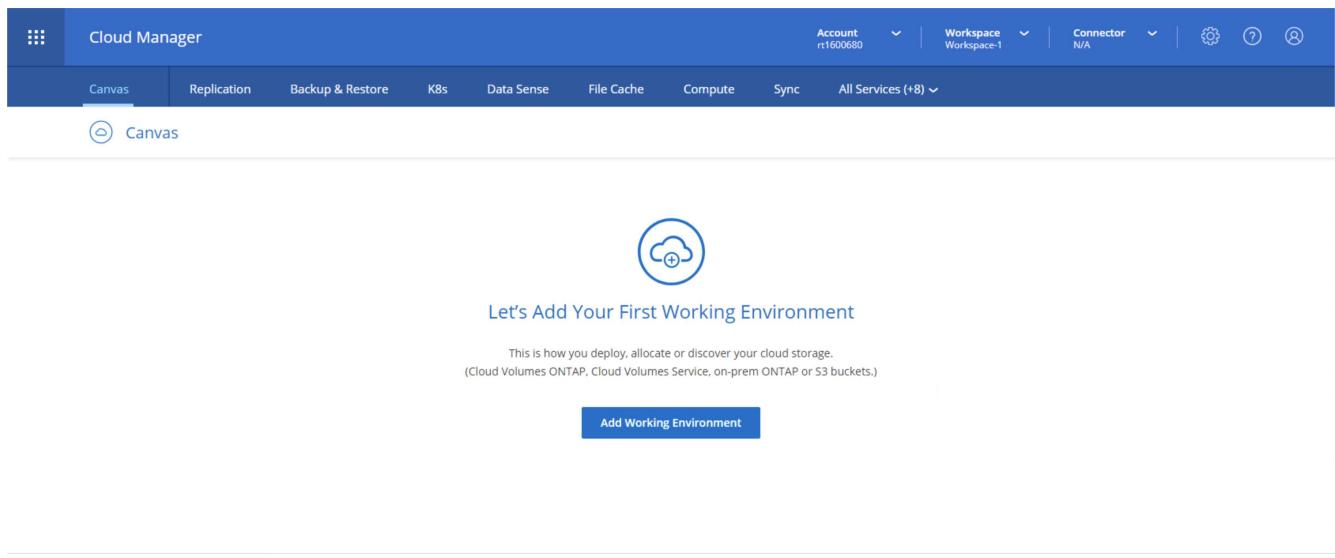
[Continue to Cloud Manager](#)

## Log In to NetApp Cloud Central

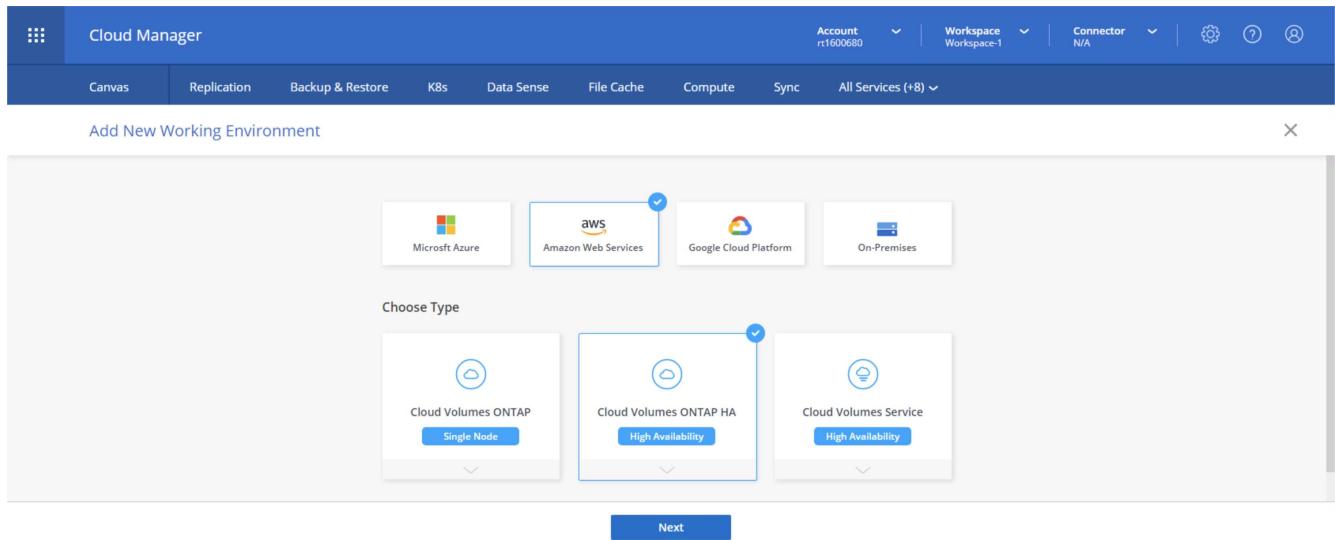
Don't have an account yet? [Sign Up](#)

[Forgot your password?](#)

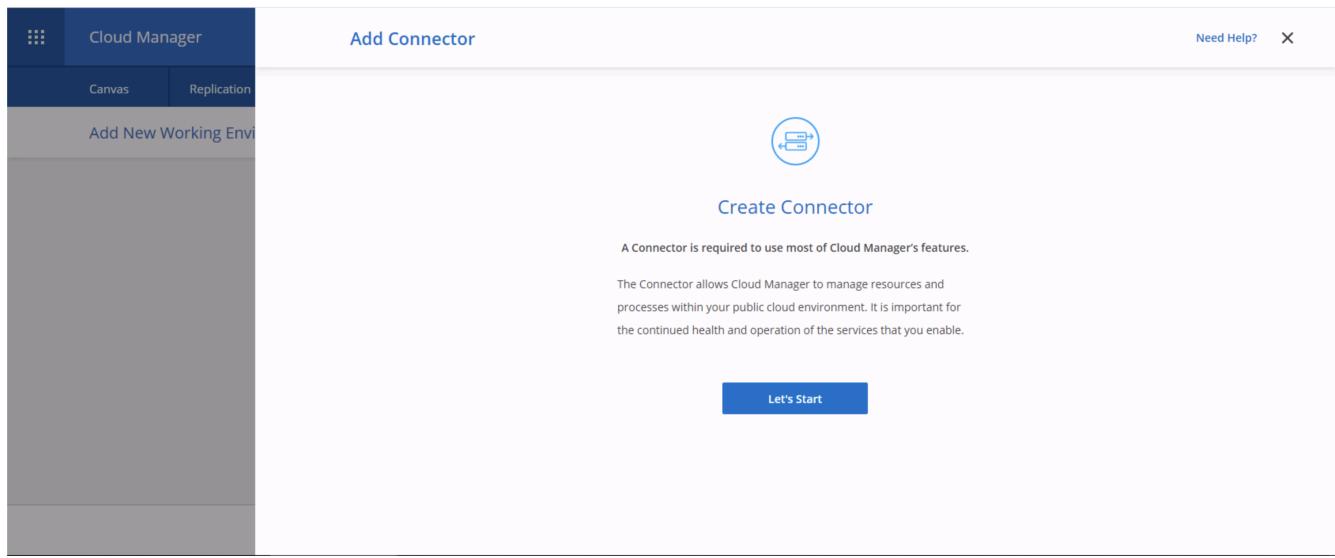
2. After you log in, you should be taken to the Canvas.



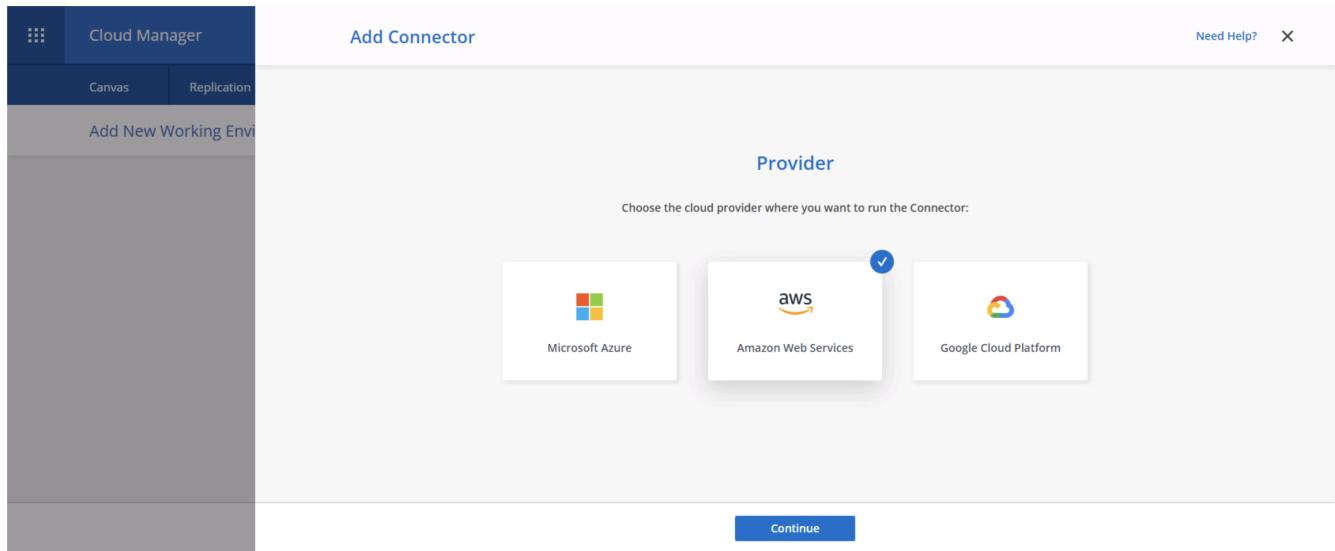
3. Click "Add Working Environment" and choose Cloud Volumes ONTAP in AWS. Here, you also choose whether you want to deploy a single node system or a high availability pair. I have chosen to deploy a high availability pair.



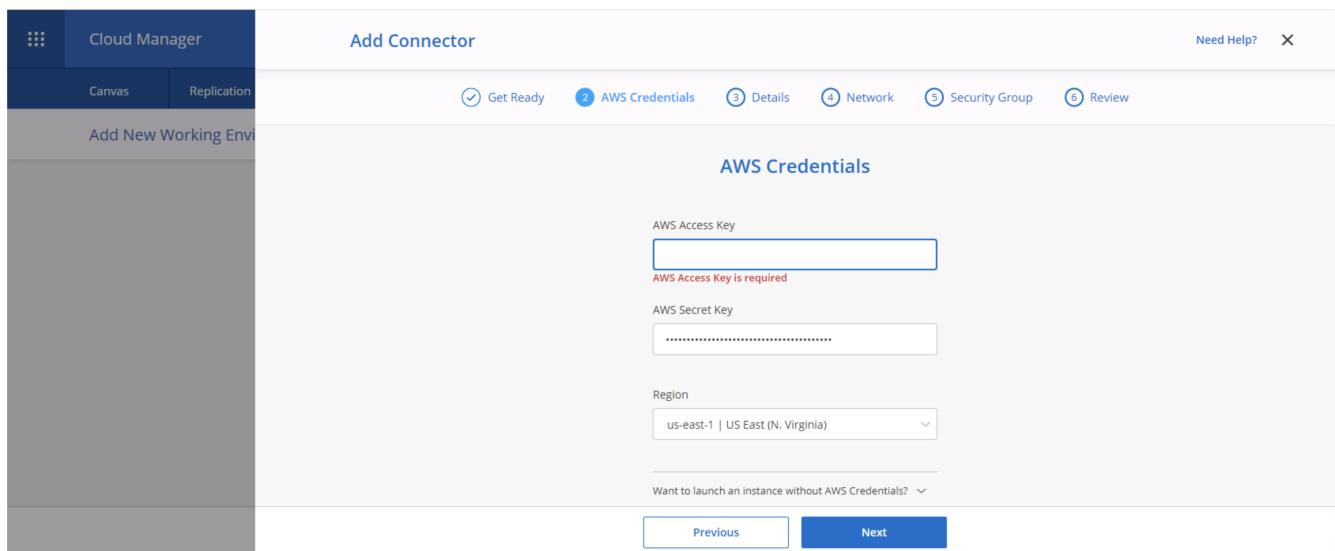
4. If no connector has been created, a pop-up appears asking you to create a connector.



5. Click Lets Start, and then choose AWS.



6. Enter your secret key and access key. Make sure that your user has the correct permissions outlined on the [NetApp policies page](#).



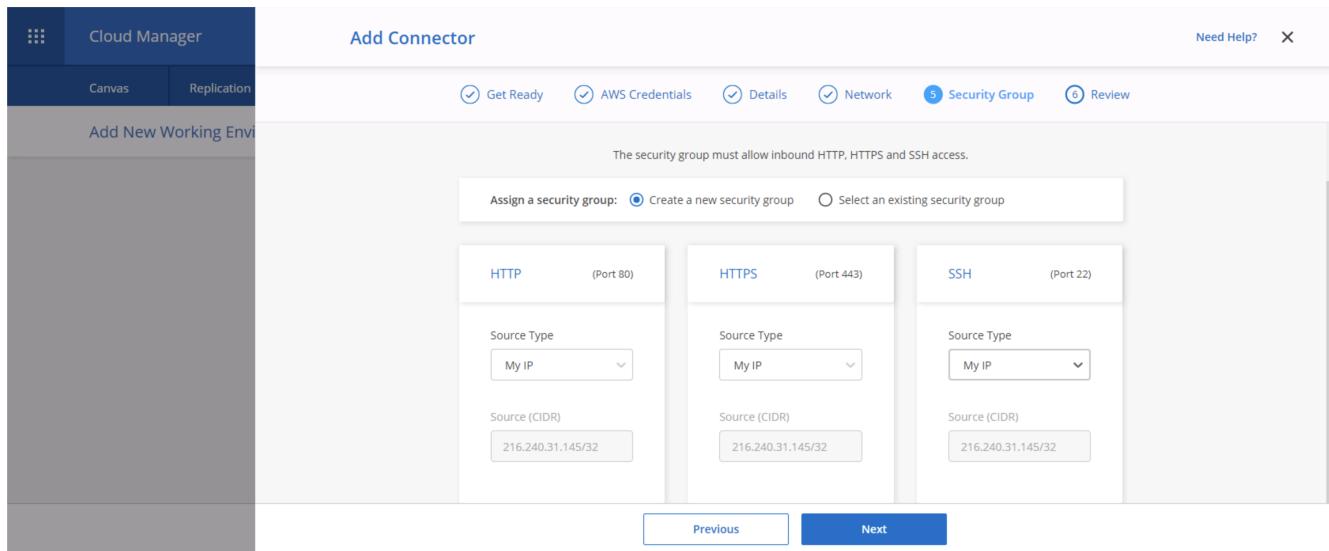
7. Give the connector a name and either use a predefined role as described on the [NetApp policies page](#) or ask Cloud Manager to create the role for you.

The screenshot shows the 'Add Connector' interface in Cloud Manager. The 'Details' step is active, indicated by a blue circle with the number 3. The 'Connector Instance Name' field contains 'awscloudmanager'. Under 'Connector Role', the 'Create Role' radio button is selected. The 'Role Name' field contains 'Cloud-Manager-Operator-IBNt24'. Below these fields is a link to 'Add Tags to Connector Instance'. At the bottom are 'Previous' and 'Next' buttons.

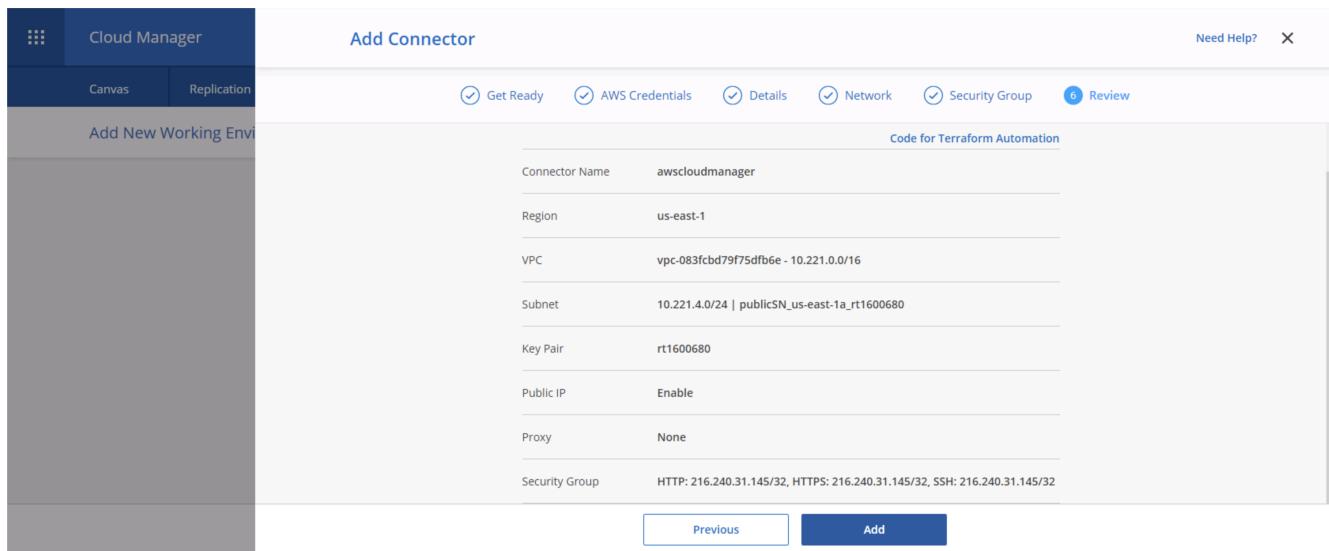
8. Give the networking information needed to deploy the connector. Verify that outbound internet access is enabled by:
- Giving the connector a public IP address
  - Giving the connector a proxy to work through
  - Giving the connector a route to the public internet through an Internet Gateway

The screenshot shows the 'Network' step of the 'Add Connector' process. The 'Network' tab is active, indicated by a blue circle with the number 4. The 'Connectivity' section includes fields for 'VPC' (set to 'vpc-083fcbd79f75dfb6e - 10.221.0.0/16'), 'Subnet' (set to '10.221.4.0/24 | publicSN\_us-east-1a\_rt1600...'), and 'Key Pair' (set to 'rt1600680'). The 'Proxy Configuration (Optional)' section includes a 'HTTP Proxy' field with the placeholder 'Example: http://172.16.254.1:8080'. Below these are dropdowns for 'Define Credentials for this Proxy' and 'Upload a root certificate'. At the bottom are 'Previous' and 'Next' buttons.

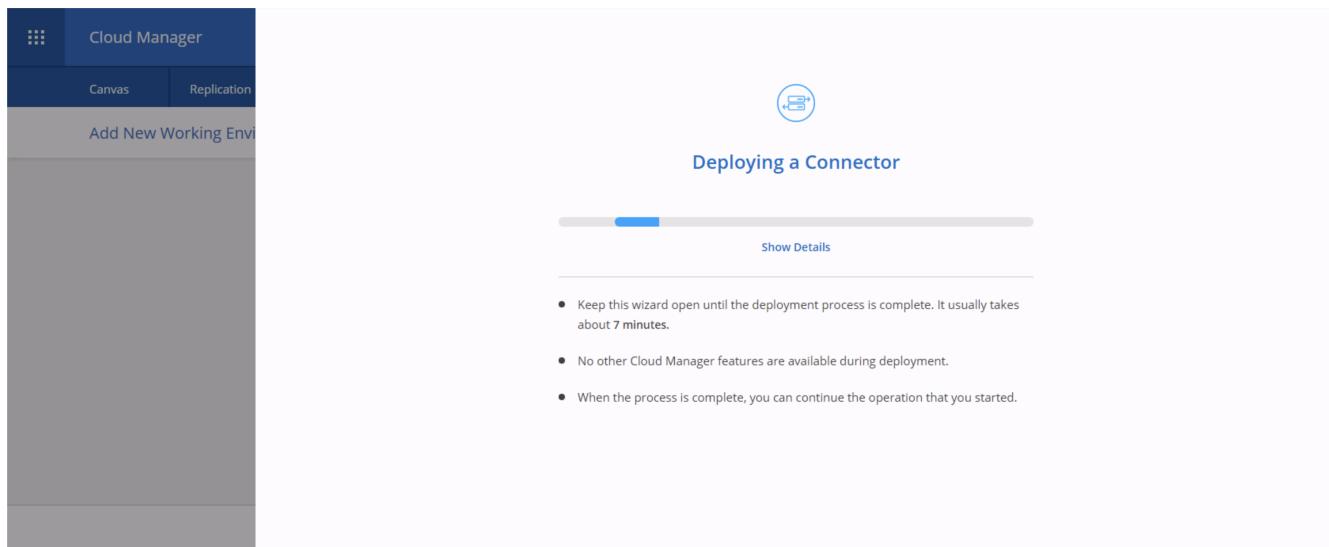
9. Provide communication with the connector via SSH, HTTP, and HTTPS by either providing a security group or creating a new security group. I have enabled access to the connector from my IP address only.



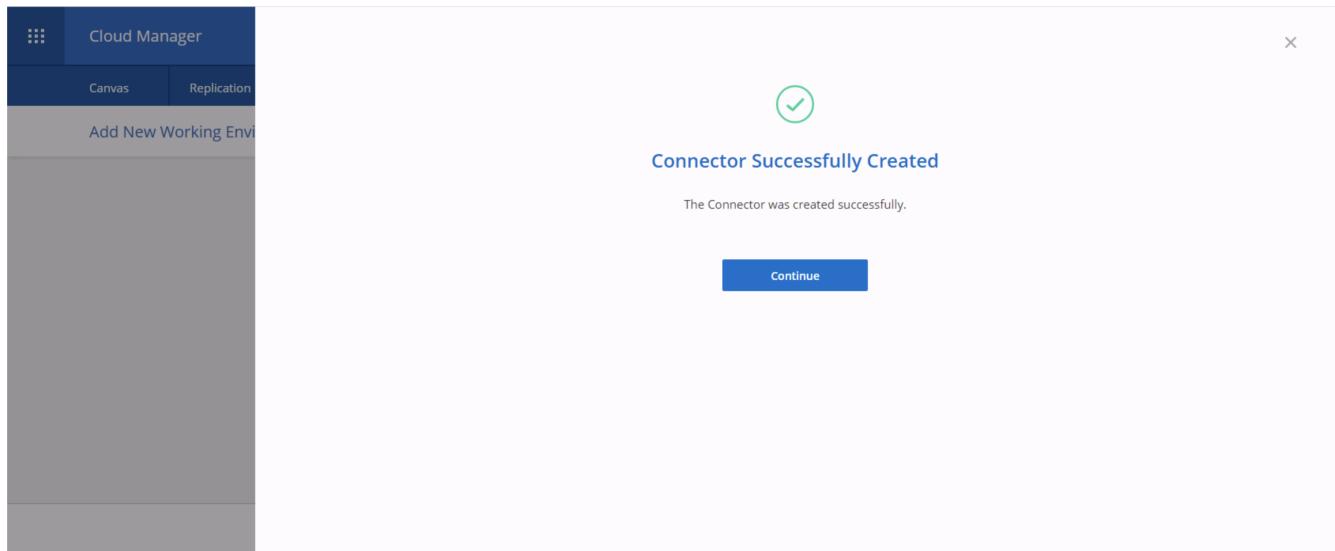
10. Review the information on the summary page and click Add to deploy the connector.



11. The connector now deploys using a cloud formation stack. You can monitor its progress from Cloud Manager or through AWS.

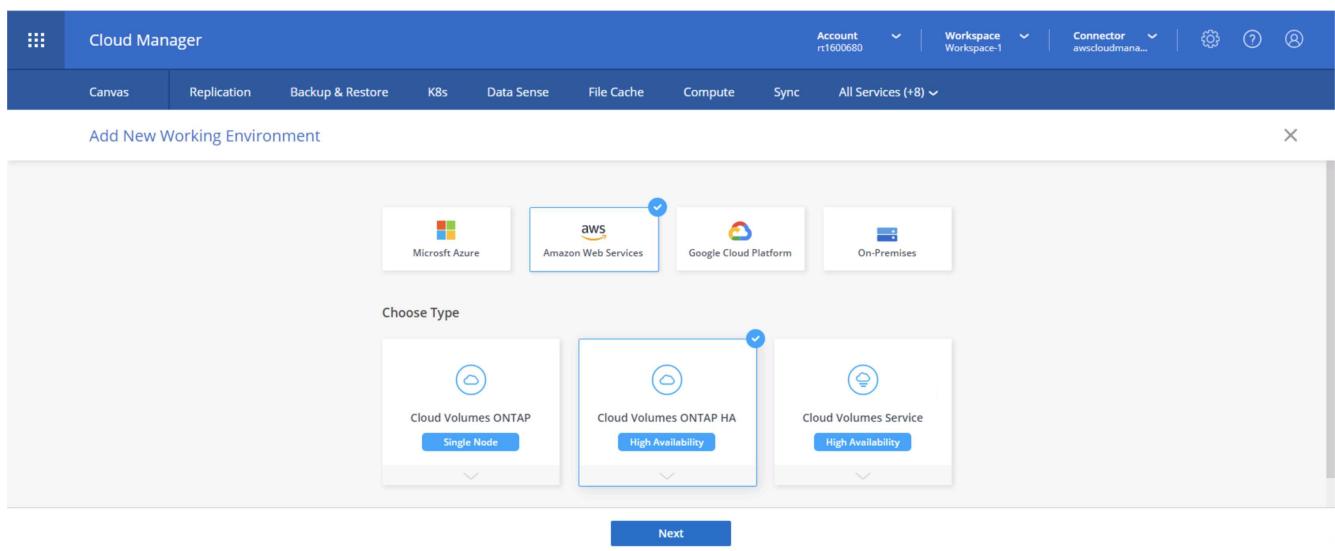


12. When the deployment is complete, a success page appears.



## Deploy Cloud Volumes ONTAP

1. Select AWS and the type of deployment based on your requirements.



2. If no subscription has been assigned and you wish to purchase with PAYGO, choose Edit Credentials.

The screenshot shows the 'Cloud Manager' interface with the title 'Create a New Working Environment'. The top navigation bar includes 'Account: rt1600680', 'Workspace: Workspace-1', 'Connector: awscloudman...', and various icons. The main content area has tabs for 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. The current step is 'Details and Credentials'. It shows an 'Instance Profile' section with 'Credential Name: 322944748816' and 'Account ID: 322944748816'. A note says 'No subscription is associated'. Below this is a 'Details' section with a 'Working Environment Name (Cluster Name)' input field ('Up to 40 characters') and a 'Add Tags' button. To the right is a 'Credentials' section with 'User Name: admin', 'Password' input field, and 'Confirm Password' input field. A 'Continue' button is at the bottom.

### 3. Choose Add Subscription.

The screenshot shows the 'Cloud Manager' interface with the title 'Create a New Working Environment'. The top navigation bar includes 'Account: rt1600680', 'Workspace: Workspace-1', 'Connector: awscloudman...', and various icons. The main content area has tabs for 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. The current step is 'Edit Credentials & Add Subscription'. It shows an 'Associate Subscription to Credentials' section with a dropdown 'Credentials: Instance Profile | Account ID: 322944748816'. Below this is a 'Marketplace Subscription' section with a note 'No subscription is associated with this credential'. A 'Add Subscription' button is present. At the bottom are 'Apply' and 'Cancel' buttons.

### 4. Choose the type of contract that you wish to subscribe to. I chose Pay-as-you-go.

The screenshot shows the 'Cloud Manager' interface with the title 'Create a New Working Environment'. The top navigation bar includes 'Account: rt1600680', 'Workspace: Workspace-1', 'Connector: awscloudman...', and various icons. The main content area has tabs for 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. The current step is 'Edit Credentials & Add Subscription'. It shows a note: 'Select a subscription option and click Continue. The AWS Marketplace enables you to view pricing details and then subscribe.' Below this are two options: 'Pay-Per-TiB - Annual Contract' (radio button not selected) and 'Pay-as-you-go' (radio button selected). A note for 'Pay-as-you-go' says 'Pay for Cloud Volumes ONTAP at an hourly rate.' Below this is a 'The next steps:' section with two numbered steps: 1. AWS Marketplace (note: 'Subscribe and then click Set Up Your Account to configure your account.') and 2. Cloud Manager (note: 'Save your subscription and associate the Marketplace subscription with your AWS credentials.'). At the bottom are 'Continue' and 'Cancel' buttons.

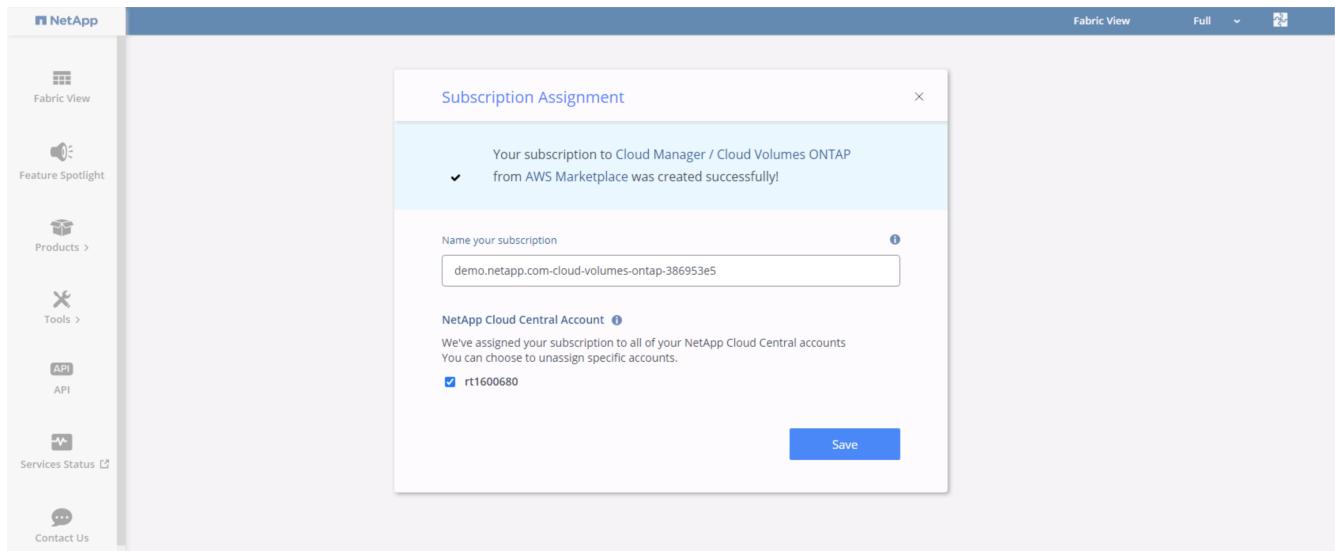
5. You are redirected to AWS; choose Continue to Subscribe.

The screenshot shows the AWS Marketplace interface for the NetApp Cloud Manager product. The product title is 'Cloud Manager - Deploy & Manage NetApp Cloud Data Services'. It is sold by 'NetApp, Inc.'. The 'Continue to Subscribe' button is visible on the right side of the page.

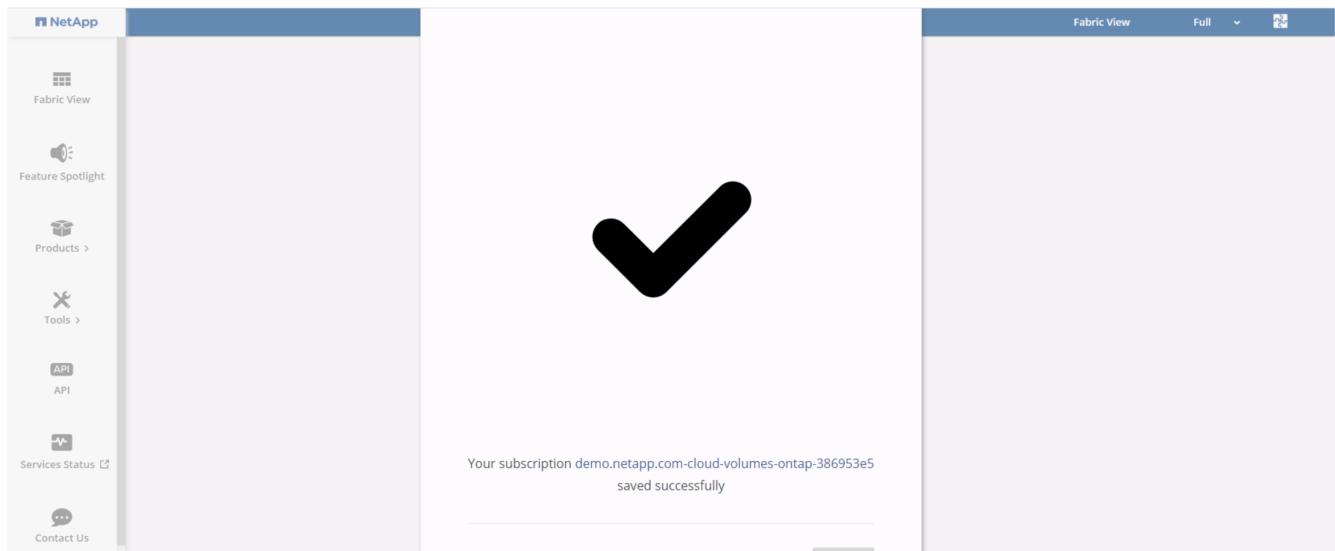
6. Subscribe and you are redirected back to NetApp Cloud Central. If you have already subscribed and don't get redirected, choose the "Click here" link.

The screenshot shows the AWS Marketplace interface for the NetApp Cloud Manager product. A message at the top states: 'You are extended multiple offers! Select an offer first and review the pricing information and EULA.' Below this, it says 'Offer name: NetApp, Inc. for SaaS 2020-07-20- Private Offer - current subscription'. On the right, there is a box titled 'You Have Subscribed to a Private Offer' which contains the text: 'You have subscribed to this private offer on July 21, 2020 UTC. This private offer will expire on August 1, 2022 UTC. Your use of this product after the expiration date of your private offer will be billed at the then current public pricing, which can be found on this product's detail page.' There is also a 'Subscribe' button and a note about agreeing to the End User License Agreement (EULA).

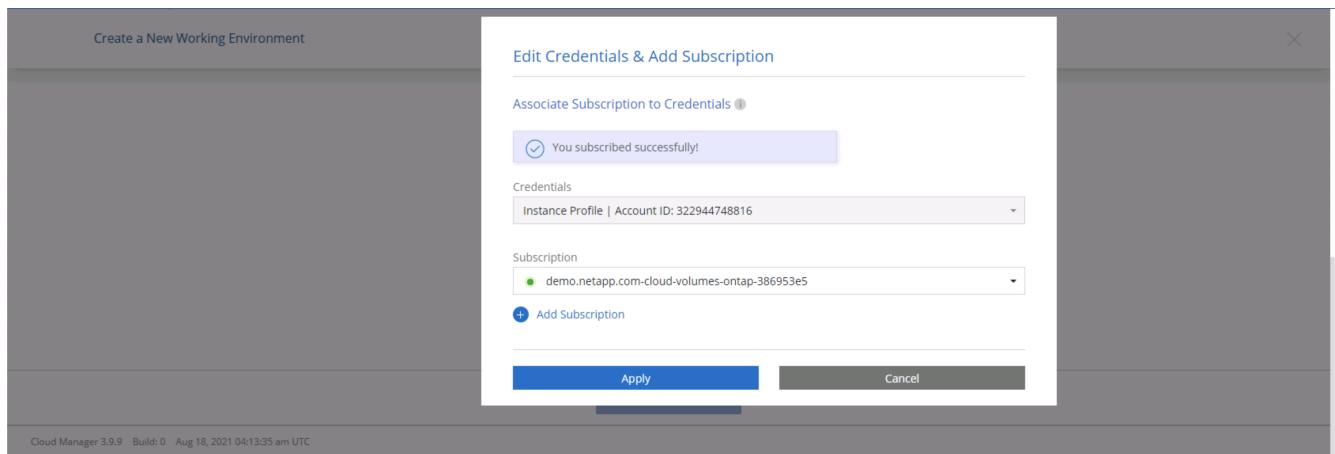
7. You are redirected to Cloud Central where you must name your subscription and assign it to your Cloud Central account.



- When successful, a check mark page appears. Navigate back to your Cloud Manager tab.



- The subscription now appears in Cloud Central. Click Apply to continue.



- Enter the working environment details such as:

- Cluster name

b. Cluster password

c. AWS tags (Optional)

The screenshot shows the 'Cloud Manager' interface with the title 'Create a New Working Environment'. The top navigation bar includes 'Account: rt1600680', 'Workspace: Workspace-1', 'Connector: awscloudman...', and various icons. Below the title, there's a 'Previous Step' link and tabs for 'Instance Profile' (selected), 'Credential Name' (322944748816), 'Account ID' (demo.netapp.com-cloud-vol...), and 'Marketplace Subscription'. A 'Edit Credentials' button is visible. The main area is divided into 'Details' and 'Credentials' sections. In 'Details', there's a 'Working Environment Name (Cluster Name)' field containing 'hybridawscvo' with a note 'Optional Field | Up to four tags'. In 'Credentials', fields for 'User Name' (admin), 'Password' (\*\*\*\*\*), and 'Confirm Password' (\*\*\*\*\*) are shown. A 'Continue' button is at the bottom.

11. Choose which additional services you would like to deploy. To discover more about these services, visit the [NetApp Cloud Homepage](#).

The screenshot shows the 'Cloud Manager' interface with the title 'Create a New Working Environment'. The top navigation bar includes 'Account: rt1600680', 'Workspace: Workspace-1', 'Connector: awscloudman...', and various icons. Below the title, there's a 'Previous Step' link. The main area is titled 'Services' and lists three options: 'Data Sense & Compliance' (with a toggle switch set to on), 'Backup to Cloud' (with a toggle switch set to on), and 'Monitoring' (with a toggle switch set to on). A 'Continue' button is at the bottom.

12. Choose whether to deploy in multiple availability zones (requires three subnets, each in a different AZ), or a single availability zone. I chose multiple AZs.

The screenshot shows the Cloud Manager interface with the title "Create a New Working Environment" and "HA Deployment Models". It compares "Multiple Availability Zones" and "Single Availability Zone".

- Multiple Availability Zones:**
  - Provides maximum protection against AZ failures.
  - Enables selection of 3 availability zones.
  - An HA node serves data if its partner goes offline.
- Single Availability Zone:**
  - Protects against failures within a single AZ.
  - Single availability zone. HA nodes are in a placement group, spread across distinct underlying hardware.
  - An HA node serves data if its partner goes offline.

Both sections have "Extended Info" links at the bottom.

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

13. Choose the region, VPC, and security group for the cluster to be deployed into. In this section, you also assign the availability zones per node (and mediator) as well as the subnets that they occupy.

The screenshot shows the Cloud Manager interface with the title "Create a New Working Environment" and "Region & VPC".

Configuration fields include:
 

- AWS Region: US East | N. Virginia
- VPC: vpc-083fcbd79f75dfb6e - 10.221.0.0/16
- Security group: Use a generated security group
- Node 1:
  - Availability Zone: us-east-1a
  - Subnet: 10.221.1.0/24
- Node 2:
  - Availability Zone: us-east-1b
  - Subnet: 10.221.2.0/24
- Mediator:
  - Availability Zone: us-east-1c
  - Subnet: 10.221.3.0/24

A "Continue" button is at the bottom.

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

14. Choose the connection methods for the nodes as well as the mediator.

The screenshot shows the Cloud Manager interface with the title "Create a New Working Environment" and "Connectivity & SSH Authentication".

Configuration fields include:
 

- Nodes:
  - SSH Authentication Method: Password
- Mediator:
  - Security Group: Use a generated security group
  - Key Pair Name: rt1600680
  - Internet Connection Method: Public IP address

A "Continue" button is at the bottom.

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC



The mediator requires communication with the AWS APIs. A public IP address is not required so long as the APIs are reachable after the mediator EC2 instance has been deployed.

1. Floating IP addresses are used to allow access to the various IP addresses that Cloud Volumes ONTAP uses, including cluster management and data serving IPs. These must be addresses that are not already routable within your network and are added to route tables in your AWS environment. These are required to enable consistent IP addresses for an HA pair during failover. More information about floating IP addresses can be found in the [NetApp Cloud Documentation](#).

The screenshot shows the 'Cloud Manager' interface with the 'Floating IPs' step selected. It includes fields for entering floating IP addresses for cluster management, NFS/CIFS data, SVM management, and an optional floating IP address. A note explains that floating IPs can migrate between HA nodes if failures occur, and it's recommended to set up an AWS transit gateway. A 'Continue' button is at the bottom.

2. Select which route tables the floating IP addresses are added to. These route tables are used by clients to communicate with Cloud Volumes ONTAP.

The screenshot shows the 'Cloud Manager' interface with the 'Route Tables' step selected. It lists two route tables: 'private\_rt\_rt1600680' and 'public\_rt\_rt1600680'. Both are checked. A note states that selecting route tables enables client access to the HA pair. An 'Additional Information' link is available. A 'Continue' button is at the bottom.

3. Choose whether to enable AWS managed encryption or AWS KMS to encrypt the ONTAP root, boot, and data disks.

**Cloud Manager**

Account: rt1600680 | Workspace: Workspace-1 | Connector: awscloudman...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8) ▾

Create a New Working Environment | Data Encryption | X

↑ Previous Step | AWS Managed Encryption

AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.

Default Master Key: aws/ebs

Continue

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

#### 4. Choose your licensing model. If you don't know which to choose, contact your NetApp representative.

**Cloud Manager**

Account: rt1600680 | Workspace: Workspace-1 | Connector: awscloudman...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8) ▾

Create a New Working Environment | Cloud Volumes ONTAP Charging Methods & NSS Account | X

↑ Previous Step | Cloud Volumes ONTAP Charging Methods

Learn more about our charging methods

Pay-As-You-Go by the hour

Bring your own license

Freemium (Up to 500GB)

NetApp Support Site Account (Optional)

Learn more about NetApp Support Site (NSS) accounts

To register this Cloud Volumes ONTAP to support, you should add NetApp Support Site Account.

Don't have a NetApp Support Site account? Select go to finish deploying this system. After it's created, use the Support Registration option to create an NSS account.

Add Netapp Support Site Account

Continue

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

#### 5. Select which configuration best suits your use case. This is related to the sizing considerations covered in the prerequisites page.

**Cloud Manager**

Account: rt1600680 | Workspace: Workspace-1 | Connector: awscloudman...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8) ▾

Create a New Working Environment | Preconfigured Packages | X

↑ Previous Step | Select a preconfigured Cloud Volumes ONTAP system that best matches your needs, or create your own configuration. Preconfigured settings can be modified at a later time. | Change Configuration

POC and small workloads Up to 2TB of storage

Database and application data production workloads Up to 10TB of storage

Cost effective DR Up to 10TB of storage

Highest performance production workloads Up to 368TB of storage

Continue

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

6. Optionally, create a volume. This is not required, because the next steps use SnapMirror, which creates the volumes for us.

Create a New Working Environment

Create Volume

↑ Previous Step

**Details & Protection**

Volume Name:  Size (GB):  Volume size

Snapshot Policy:  default  Default Policy

**Protocol**

NFS  CIFS  iSCSI

Access Control:  Custom export policy

Custom export policy:  10.221.0.0/16

Advanced options

Continue Skip

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

7. Review the selections made and tick the boxes to verify that you understand that Cloud Manager deploys resources into your AWS environment. When ready, click Go.

Create a New Working Environment

Review & Approve

↑ Previous Step **hybridawscvo** Show API request

AWS | us-east-1 | HA

I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. [More information >](#)

I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. [More information >](#)

**Overview** Networking Storage

Storage System:	Cloud Volumes ONTAP HA	HA Deployment Model:	Multiple Availability Zones
License Type:	Cloud Volumes ONTAP Standard	Encryption:	AWS Managed
Capacity Limit:	10TB	Customer Master Key:	aws/ebs

Go

Cloud Manager 3.9.9 Build: 0 Aug 18, 2021 04:13:35 am UTC

8. Cloud Volumes ONTAP now starts its deployment process. Cloud Manager uses AWS APIs and cloud formation stacks to deploy Cloud Volumes ONTAP. It then configures the system to your specifications, giving you a ready-to-go system that can be instantly utilized. The timing for this process varies depending on the selections made.

The screenshot shows the Cloud Manager Canvas interface. At the top, there are tabs for Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The Canvas tab is selected. In the center, there's a diagram illustrating a hybrid environment setup. It shows two clouds: one labeled "hybridawsenvo Cloud Volumes ONTAP" with "HA" and "Initializing" status, and another labeled "Amazon S3" with "1 Buckets" and "1 Region". Below the diagram are "Add Working Environment" and "Working environments" sections. The "Working environments" section lists "1 Cloud Volumes ONTAP (High-Availability)" and "0 B Allocated Capacity" under a cloud icon, and "1 Amazon S3" with "0 Buckets" under a bucket icon. A zoom-in and zoom-out button is at the bottom right.

9. You can monitor the progress by navigating to the Timeline.

The screenshot shows the Cloud Manager main dashboard. At the top, there are tabs for Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The Canvas tab is selected. Below the tabs, there are sections for Resources and Services. The Resources section includes links for Canvas, Digital Wallet, and Timeline. The Services section includes links for Replication, Backup & Restore, K8s, Data Sense, Compliance, Tiering, Monitoring, File Cache, Compute, Sync, SnapCenter, and Active IQ. A link to the Timeline is also present at the bottom left: <https://cloudmanager.netapp.com/timeline>.

10. The Timeline acts as an audit of all actions performed in Cloud Manager. You can view all of the API calls that are made by Cloud Manager during setup to both AWS as well as the ONTAP cluster. This can also be effectively used to troubleshoot any issues that you face.

The screenshot shows the Cloud Manager interface with the 'Timeline' tab selected. At the top, there are filters for Time, Service, Action, Agent, Resource, User, and Status, with 'Agent (1)' currently selected. The timeline table lists three events:

Time	Action	Service	Agent	Resource	User	Status
Aug 18 2021, 9:42:32 pm	Check Connectivity	Cloud Manager	awscloudman...	hybridawscvo	Full Name	Success
Aug 18 2021, 9:42:00 pm	Create Aws Ha Working Environment	Cloud Manager	awscloudma...	hybridawscvo	Full Name	Pending
Aug 18 2021, 10:09:39 pm	Describe Operation Status					Success
Aug 19 2021, 10:00:20 pm	Describe Operation Status					Success

- After deployment is complete, the CVO cluster appears on the Canvas, which the current capacity. The ONTAP cluster in its current state is fully configured to allow a true, out-of-the-box experience.

The screenshot shows the Cloud Manager interface with the 'Canvas' tab selected. On the left, there's a cloud icon labeled 'Add Working Environment'. In the center, there are two clouds representing environments: one for 'Cloud Volumes ONTAP' (labeled 'hybridawscvo' and '1 GiB Capacity') and one for 'Amazon S3' (labeled '2 Buckets' and '1 Region'). On the right, a sidebar titled 'Working environments' lists the deployed resources:

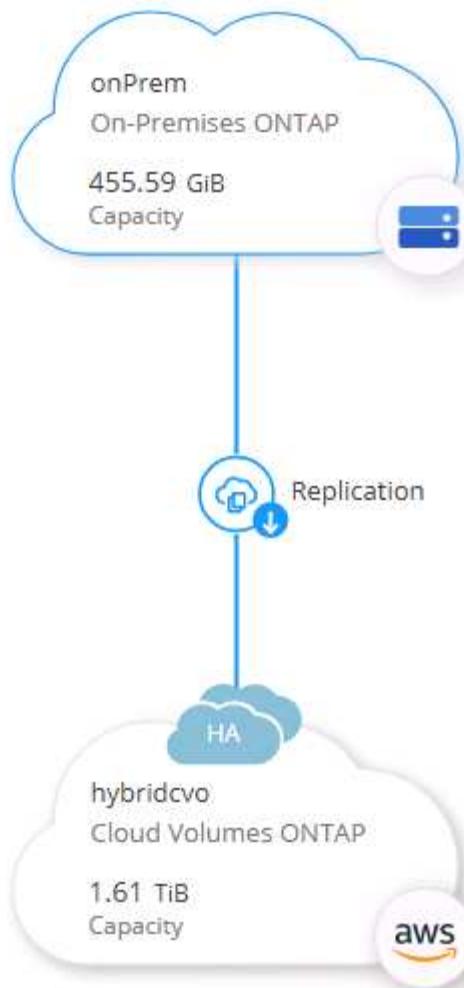
- 1 Cloud Volumes ONTAP (High-Availability)  
1 GiB Allocated Capacity
- 1 Amazon S3  
0 Buckets

## Configure SnapMirror from on-premises to cloud

Now that you have a source ONTAP system and a destination ONTAP system deployed, you can replicate volumes containing database data into the cloud.

For a guide on compatible ONTAP versions for SnapMirror, see the [SnapMirror Compatibility Matrix](#).

- Click the source ONTAP system (on-premises) and either drag and drop it to the destination, select Replication > Enable, or select Replication > Menu > Replicate.



---

Select Enable.



Or Options.

The screenshot shows the configuration for the 'onPrem' cluster. At the top, there's a circular icon with two servers, followed by the text 'onPrem' and a green square indicating 'On'. To the right are three blue circular icons with symbols for information, more options, and delete. Below this, the word 'DETAILS' is in bold. Under 'DETAILS', it says 'On-PremisesONTAP'. In the 'SERVICES' section, there's another server icon followed by 'Replication' and a green square 'On'. To its right, it shows '1 Replication Target' with a blue circular icon containing three dots. A horizontal line separates this from the 'Replicate.' section.

onPrem  
■ On

DETAILS

On-PremisesONTAP

SERVICES

Replication  
■ On 1 Replication Target

Replicate.

This screenshot is similar to the first one but includes a dropdown menu. The 'Replication' service row has a blue arrow pointing down to a dropdown menu. The menu contains two items: 'View Replications' with a list icon and 'Replicate' with a circular arrow icon. The rest of the interface is identical to the first screenshot.

onPrem  
■ On

DETAILS

On-PremisesONTAP

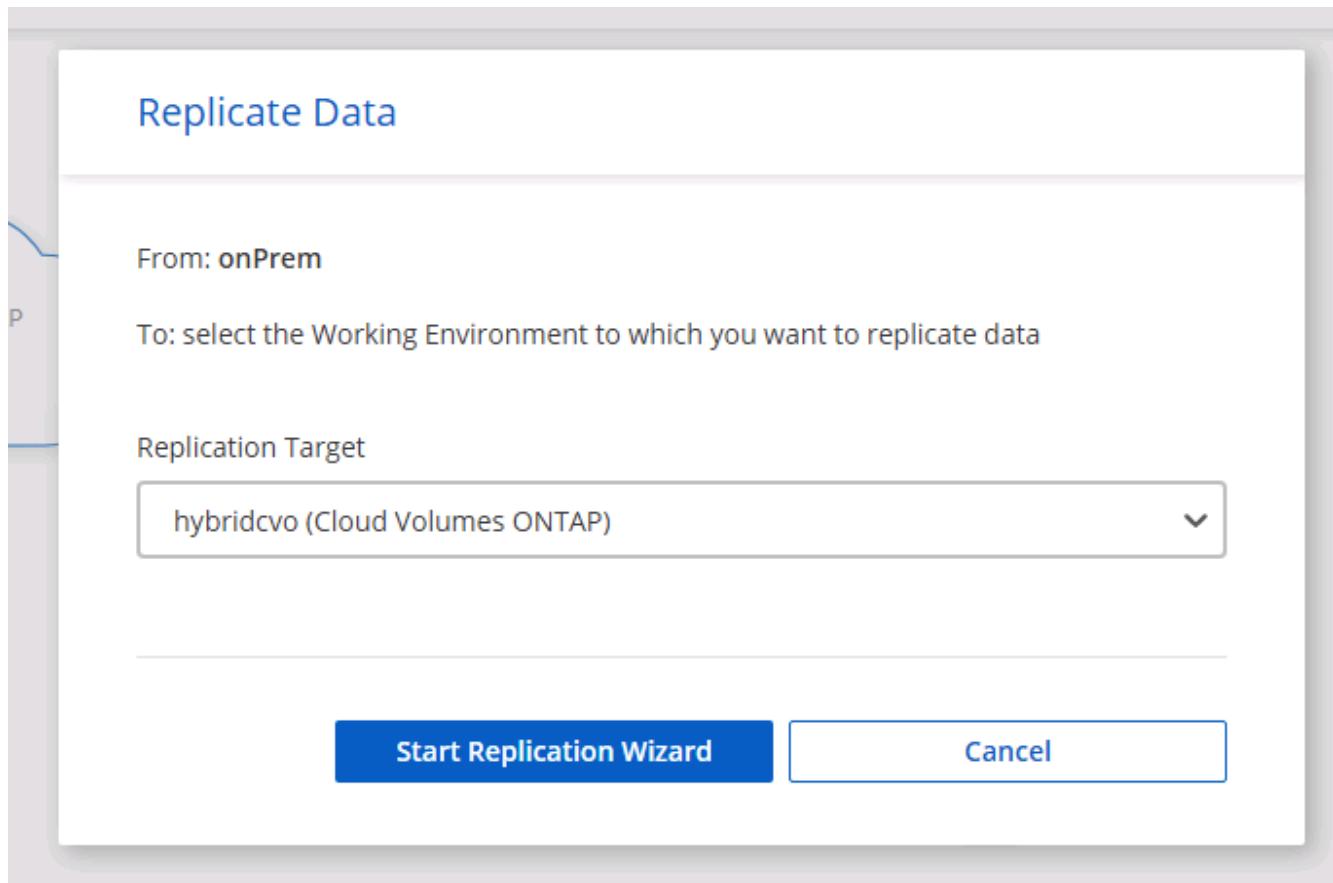
SERVICES

Replication  
■ On 1 Replication Target

View Replications

Replicate

2. If you did not drag and drop, choose the destination cluster to replicate to.



3. Choose the volume that you'd like to replicate. We replicated the data and all log volumes.

Replication Setup				Source Volume Selection			
<b>rhel2_u03</b>	INFO Storage VM Name: <b>svm_onPrem</b> Tiering Policy: <b>None</b> Volume Type: <b>RW</b>	CAPACITY <b>100 GB Allocated</b> / <b>7.29 GB Disk Used</b>	ONLINE	<b>rhel2_u03</b> <b>09232119421203118</b>	INFO Storage VM Name: <b>svm_onPrem</b> Tiering Policy: <b>None</b> Volume Type: <b>RW</b>	CAPACITY <b>100 GB Allocated</b> / <b>35.83 MB Disk Used</b>	ONLINE
<b>sql1_data</b>	INFO Storage VM Name: <b>svm_onPrem</b> Tiering Policy: <b>None</b> Volume Type: <b>RW</b>	CAPACITY <b>53.37 GB Allocated</b> / <b>45.09 GB Disk Used</b>	ONLINE	<b>sql1_log</b>	INFO Storage VM Name: <b>svm_onPrem</b> Tiering Policy: <b>None</b> Volume Type: <b>RW</b>	CAPACITY <b>21.35 GB Allocated</b> / <b>18.16 GB Disk Used</b>	ONLINE
<b>sql1_snapctr</b>	INFO Storage VM Name: <b>svm_onPrem</b> Tiering Policy: <b>None</b> Volume Type: <b>RW</b>	CAPACITY <b>24.87 GB Allocated</b> / <b>21.23 GB Disk Used</b>	ONLINE				
Cloud Manager 3.9.10 Build: 2 Sep 12, 2021 06:47:41 am UTC							

4. Choose the destination disk type and tiering policy. For disaster recovery, we recommend an SSD as the disk type and to maintain data tiering. Data tiering tiers the mirrored data into low-cost object storage and saves you money on local disks. When you break the relationship or clone the volume, the data uses the fast, local storage.

[↑ Previous Step](#)

## Destination Disk Type



## S3 Tiering

[What are storage tiers?](#) Enabled    DisabledNote: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.[Continue](#)

Cloud Manager 3.9.10 Build:2 Sep 12, 2021 06:47:41 am UTC

5. Select the destination volume name: we chose [source\_volume\_name]\_dr.

## Destination Volume Name

## Destination Volume Name

sql1\_data\_dr

## Destination Aggregate

Automatically select the best aggregate ▾

6. Select the maximum transfer rate for the replication. This enables you to save bandwidth if you have a low bandwidth connection to the cloud such as a VPN.

## Max Transfer Rate

You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your Internet performance.

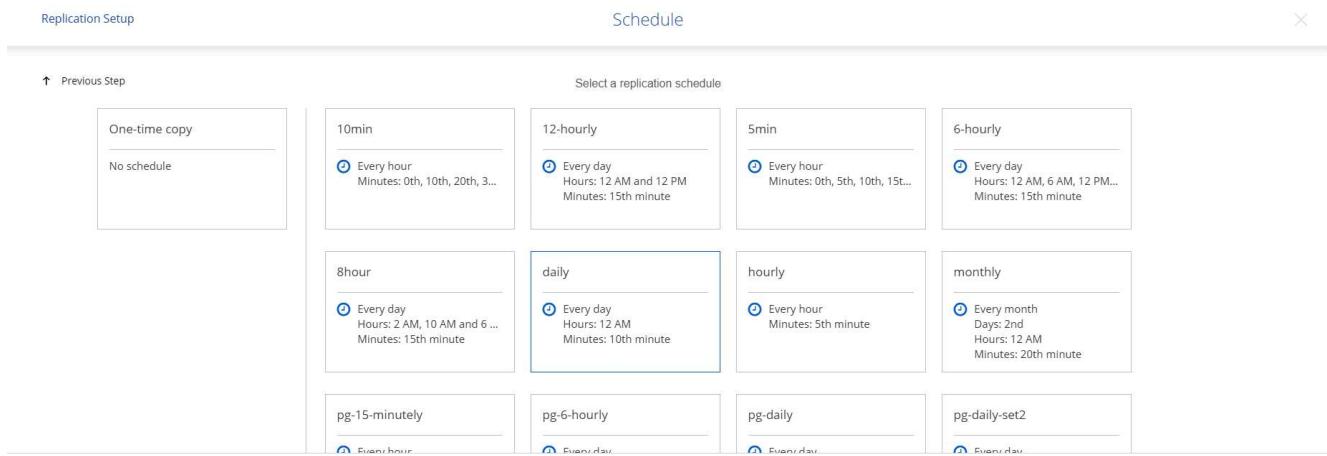
- Limited to:  MB/s
- Unlimited (recommended for DR only machines)

7. Define the replication policy. We chose a Mirror, which takes the most recent dataset and replicates that into the destination volume. You could also choose a different policy based on your requirements.

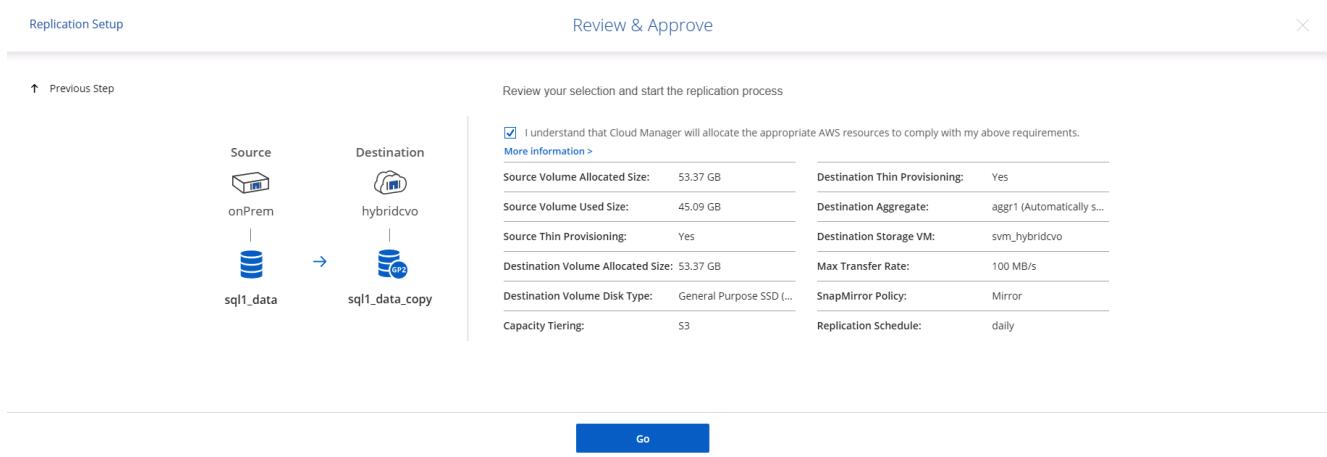
### Replication Policy

Default Policies	Additional Policies
<p> <b>Mirror</b></p> <p>Typically used for disaster recovery</p> <p><a href="#">More info</a></p>	<p> <b>Mirror and Backup (1 month retention)</b></p> <p>Configures disaster recovery and long-term retention of backups on the same destination volume</p> <p><a href="#">More info</a></p>

8. Choose the schedule for triggering replication. NetApp recommends setting a "daily" schedule of for the data volume and an "hourly" schedule for the log volumes, although this can be changed based on requirements.



9. Review the information entered, click Go to trigger the cluster peer and SVM peer (if this is your first time replicating between the two clusters), and then implement and initialize the SnapMirror relationship.



10. Continue this process for data volumes and log volumes.

11. To check all of your relationships, navigate to the Replication tab inside Cloud Manager. Here you can manage your relationships and check on their status.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
<span>✓</span>	rhel2_u01 onPrem	rhel2_u01_dr hybridcvo	43 minutes 43 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:50 AM 19.73 MiB
<span>✓</span>	rhel2_u02 onPrem	rhel2_u02_dr hybridcvo	1 hour 37 minutes 59 seconds	idle	snapmirrored	Sep 30, 2021, 2:37:08 PM 239.78 MiB
<span>✓</span>	rhel2_u03 onPrem	rhel2_u03_dr hybridcvo	16 hours 1 minute 9 seconds	idle	snapmirrored	Sep 30, 2021, 4:07:14 PM 225.37 KiB
<span>✓</span>	sql1_data onPrem	sql1_data_dr hybridcvo	1 hour 6 minutes 50 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:28 AM 24.56 KiB
<span>✓</span>	rhel2_u04 onPrem	rhel2_u04_dr hybridcvo	1 hour 1 minute 40 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:30 AM 24.56 KiB
<span>✓</span>	rhel2_u05 onPrem	rhel2_u05_dr hybridcvo	1 hour 1 minute 40 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:30 AM 24.56 KiB
<span>✓</span>	rhel2_u06 onPrem	rhel2_u06_dr hybridcvo	1 hour 1 minute 40 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:30 AM 24.56 KiB

12. After all the volumes have been replicated, you are in a steady state and ready to move on to the disaster recovery and dev/test workflows.

### **3. Deploy EC2 compute instance for database workload**

AWS has preconfigured EC2 compute instances for various workloads. The choice of instance type determines the number of CPU cores, memory capacity, storage type and capacity, and network performance. For the use cases, with the exception of the OS partition, the main storage to run database workload is allocated from CVO or the FSx ONTAP storage engine. Therefore, the main factors to consider are the choice of CPU cores, memory, and network performance level. Typical AWS EC2 instance types can be found here: [EC2 Instance Type](#).

#### **Sizing the compute instance**

1. Select the right instance type based on the required workload. Factors to consider include the number of business transactions to be supported, the number of concurrent users, data set sizing, and so on.
2. EC2 instance deployment can be launched through the EC2 Dashboard. The exact deployment procedures are beyond the scope of this solution. See [Amazon EC2](#) for details.

#### **Linux instance configuration for Oracle workload**

This section contain additional configuration steps after an EC2 Linux instance is deployed.

1. Add an Oracle standby instance to the DNS server for name resolution within the SnapCenter management domain.
2. Add a Linux management user ID as the SnapCenter OS credentials with sudo permissions without a password. Enable the ID with SSH password authentication on the EC2 instance. (By default, SSH password authentication and passwordless sudo is turned off on EC2 instances.)
3. Configure Oracle installation to match with on-premises Oracle installation such as OS patches, Oracle versions and patches, and so on.
4. NetApp Ansible DB automation roles can be leveraged to configure EC2 instances for database dev/test and disaster recovery use cases. The automation code can be download from the NetApp public GitHub site: [Oracle 19c Automated Deployment](#). The goal is to install and configure a database software stack on an EC2 instance to match on-premises OS and database configurations.

#### **Windows instance configuration for SQL Server workload**

This section lists additional configuration steps after an EC2 Windows instance is initially deployed.

1. Retrieve the Windows administrator password to log in to an instance via RDP.
2. Disable the Windows firewall, join the host to Windows SnapCenter domain, and add the instance to the DNS server for name resolution.
3. Provision a SnapCenter log volume to store SQL Server log files.
4. Configure iSCSI on the Windows host to mount the volume and format the disk drive.
5. Again, many of the previous tasks can be automated with the NetApp automation solution for SQL Server. Check the NetApp automation public GitHub site for newly published roles and solutions: [NetApp Automation](#).

Next: [Workflow for dev/test bursting to cloud](#).

## **Workflow for dev/test bursting to cloud**

Previous: [Getting Started with AWS public cloud](#).

The agility of the public cloud, the time to value, and the cost savings are all meaningful value propositions for enterprises adopting the public cloud for database application development and testing effort. There is no better tool than SnapCenter to make this a reality. SnapCenter can not only protect your production database on-premises, but can also quickly clone a copy for application development or code testing in the public cloud while consuming very little extra storage. Following are details of the step-by-step processes for using this tool.

## Clone an Oracle Database for dev/test from a replicated snapshot backup

1. Log into SnapCenter with a database management user ID for Oracle. Navigate to the Resources tab, which shows the Oracle databases being protected by SnapCenter.

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com	rhel2_cdb2 rhel2_cdb2_log	Oracle Archive Log Backup Oracle Full Online Backup	09/17/2021 3:00:09 PM	Backup succeeded

2. Click the intended on-premises database name for the backup topology and the detailed view. If a secondary replicated location is enabled, it shows linked mirror backups.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log	09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log	09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data	09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log	09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388
rhel2_cdb2_log_09-17-2021_13.00.01.7389_1	1	Log	09/17/2021 1:00:11 PM	Not Applicable	False	Not Cataloged	5971535
rhel2_cdb2_log_09-17-2021_12.00.01.1142_1	1	Log	09/17/2021 12:00:10 PM	Not Applicable	False	Not Cataloged	5971773
rhel2_cdb2_log_09-17-2021_11.00.01.0895_1	1	Log	09/17/2021 11:00:10 AM	Not	False	Not Cataloged	5968474

3. Toggled to the mirrored backups view by clicking mirrored backups. The secondary mirror backup(s) is then displayed.

NetApp SnapCenter®

Oracle Database ▾

Search databases

cdb2 Topology

Manage Copies

Local copies

Mirror copies

Summary Card

368 Backups

16 Data Backups

352 Log Backups

0 Clones

Backup Name

	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5980203
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log		09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388
rhel2_cdb2_log_09-17-2021_13.00.01.7389_1	1	Log		09/17/2021 1:00:11 PM	Not Applicable	False	Not Cataloged	5975135
rhel2_cdb2_log_09-17-2021_12.00.01.1142_1	1	Log		09/17/2021 12:00:10 PM	Not Applicable	False	Not Cataloged	5971773
rhel2_cdb2_log_09-17-2021_11.00.01.0895_1	1	Log		09/17/2021 11:00:10 AM	Not Applicable	False	Not Cataloged	5968474

Total 1

- Choose a mirrored secondary database backup copy to be cloned and determine a recovery point either by time and system change number or by SCN. Generally, the recovery point should be trailing the full database backup time or SCN to be cloned. After a recovery point is decided, the required log file backup must be mounted for recovery. The log file backup should be mounted to target DB server where the clone database is to be hosted.

Mount backups

Choose the host to mount the backup : ora-standby.demo.netapp.com

Mount path : /var/opt/snapcenter/sco/backup\_mount/rhel2\_cdb2\_09-17-2021\_14.35.01.4997\_1/cdb2

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr

Mount Cancel

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log	09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log	09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log	09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data	09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log	09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388



If log pruning is enabled and the recovery point is extended beyond the last log pruning, multiple archive log backups might need to be mounted.

5. Highlight the full database backup copy to be cloned, and then click the clone button to start the DB clone Workflow.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log	09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log	09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log	09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data	09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log	09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388

6. Choose a proper clone DB SID for a complete container database or CDB clone.

Clone from cdb2

**1 Name**

Complete Database Clone

Clone SID: cdb2test

Exclude PDBs: Type to find PDBs

PDB Clone

Secondary storage location : Snap Vault / Snap Mirror

**Data**

Source Volume	Destination Volume
svm_onPrem:rhel2_u02	svm_hybridcvo:rhel2_u02_dr

**Logs**

Source Volume	Destination Volume
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr

[Previous](#) [Next](#)

7. Select the target clone host in the cloud, and datafile, control file, and redo log directories are created by the clone workflow.

Clone from cdb2

**1 Name**

Select the host to create a clone

Clone host ora-standby.demo.netapp.com

**2 Locations**

**3 Credentials**

**4 PreOps**

**5 PostOps**

**6 Notification**

**7 Summary**

**Datafile locations**

/u02\_cdb2test

**Control files**

/u02\_cdb2test/cdb2test/control/control01.ctl  
/u02\_cdb2test/cdb2test/control/control02.ctl

**Redo logs**

Group	Size	Unit	Number of files
RedoGroup 1	200	MB	1
/u02_cdb2test/cdb2test/redolog redo03.log			
RedoGroup 2	200	MB	1

Previous Next

- The None credential name is used for OS-based authentication, which renders the database port irrelevant. Fill in the proper Oracle Home, Oracle OS User, and Oracle OS Group as configured in the target clone DB server.

Clone from cdb2

**1 Name**

**2 Locations**

**3 Credentials**

**4 PreOps**

**5 PostOps**

**6 Notification**

**7 Summary**

Database Credentials for the clone

Credential name for sys user  + ?

Database port

Oracle Home Settings ?

Oracle Home

Oracle OS User

Oracle OS Group

Previous Next

The screenshot shows the Oracle Database Clone wizard interface. The left sidebar lists steps 1 through 7. Step 3, 'Credentials', is currently selected and highlighted in blue. The main panel shows 'Database Credentials for the clone' with a dropdown for 'Credential name for sys user' set to 'None'. Below it, 'Database port' is set to '1521'. Under 'Oracle Home Settings', the 'Oracle Home' path is '/u01/app/oracle/product/19800/cdb2', and the 'Oracle OS User' and 'Oracle OS Group' are both 'oracle'. At the bottom right are 'Previous' and 'Next' buttons.

9. Specify the scripts to run before clone operation. More importantly, the database instance parameter can be adjusted or defined here.

Clone from cdb2

**Specify scripts to run before clone operation**

Prescript full path	/var/opt/snapcenter/spl/scripts/	Enter Prescript path
Arguments		
Script timeout	60	secs

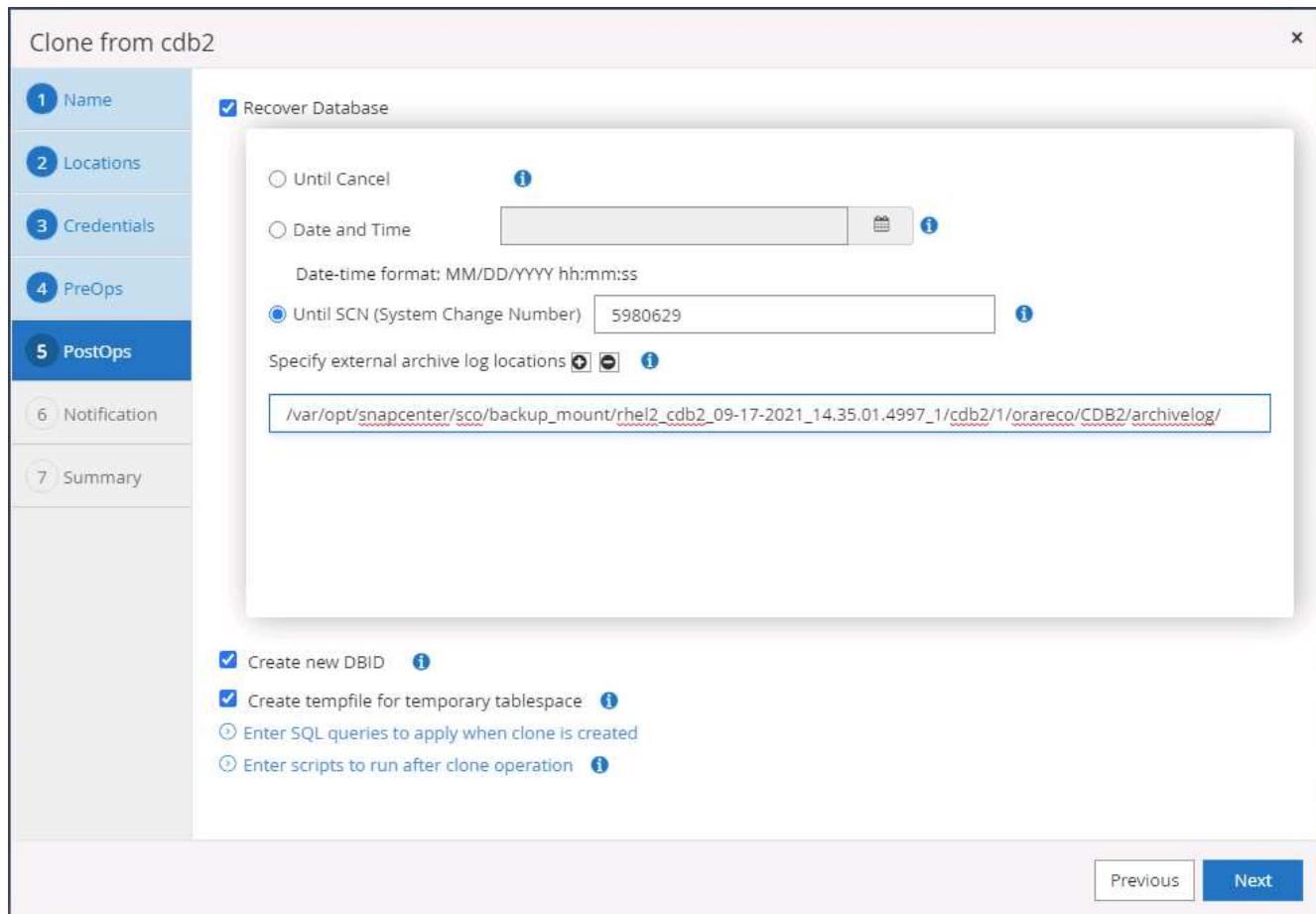
**Database Parameter settings**

processes	320	X
remote_login_passwordfile	EXCLUSIVE	X
sga_target	4311744512	X
undo_tablespace	UNDOTBS1	X

**Buttons:**

- Previous
- Next

- Specify the recovery point either by the date and time or SCN. Until Cancel recovers the database up to the available archive logs. Specify the external archive log location from the target host where the archive log volume is mounted. If target server Oracle owner is different from the on-premises production server, verify that the archive log directory is readable by the target server Oracle owner.



```
oracle@ora-standby:~$ ls /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_09-17-2021_14.35.01.4997_1/cdb2/1/orareco/CDB2/archivelog/
2021_08_26 2021_08_28 2021_08_30 2021_09_01 2021_09_03 2021_09_05 2021_09_07 2021_09_09 2021_09_11 2021_09_13 2021_09_15 2021_09_17
2021_08_27 2021_08_29 2021_08_31 2021_09_02 2021_09_04 2021_09_06 2021_09_08 2021_09_10 2021_09_12 2021_09_14 2021_09_16
[oracle@ora-standby:~]$
```

11. Configure the SMTP server for email notification if desired.

Clone from cdb2

**Provide email settings i**

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach job report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

[Previous](#) [Next](#)

12. Clone summary.

Clone from cdb2

<b>1 Name</b>	Summary
<b>2 Locations</b>	Clone from backup      rhel2_cdb2_09-17-2021_14.35.01.4997_0
<b>3 Credentials</b>	Clone SID      cdb2test
<b>4 PreOps</b>	Clone server      ora-standby.demo.netapp.com
<b>5 PostOps</b>	Exclude PDBs      none
<b>6 Notification</b>	Oracle home      /u01/app/oracle/product/19800/cdb2
<b>7 Summary</b>	Oracle OS user      oracle Oracle OS group      oinstall Datafile mountpaths      /u02_cdb2test Control files      /u02_cdb2test/cdb2test/control/control01.ctl /u02_cdb2test/cdb2test/control/control02.ctl  Redo groups      RedoGroup =1 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog redo03.log RedoGroup =2 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog redo02.log RedoGroup =3 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog redo01.log  Recovery scope      Until SCN 5980629 Prescript full path      none Prescript arguments Postscript full path      none Postscript arguments

[Previous](#) [Finish](#)

13. You should validate after cloning to make sure that the cloned database is operational. Some additional tasks, such as starting up the listener or turning off the DB log archive mode, can be performed on the dev/test database.

```
oracle@ora-standby:/tmp
[oracle@ora-standby tmp]$ export ORACLE_SID=cdb2test
[oracle@ora-standby tmp]$ export ORACLE_HOME=/u01/app/oracle/product/19800/cdb2
[oracle@ora-standby tmp]$ export PATH=$PATH:$ORACLE_HOME/bin
[oracle@ora-standby tmp]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 17 17:49:29 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> select name, log_mode from v$database;
NAME      LOG_MODE
-----
CDB2TEST  ARCHIVELOG

SQL> select instance_name, host_name from v$instance;
INSTANCE_NAME
-----
HOST NAME
-----
cdb2test
ora-standby.demo.netapp.com

SQL> show pdbs
CON_ID CON_NAME          OPEN MODE  RESTRICTED
----- -----
  2 PDB$SEED           READ ONLY NO
  3 CDB2_PDB1          READ WRITE NO
  4 CDB2_PDB2          READ WRITE NO
  5 CDB2_PDB3          READ WRITE NO

SQL>
```

## Clone a SQL database for dev/test from a replicated Snapshot backup

1. Log into SnapCenter with a database management user ID for SQL Server. Navigate to the Resources tab, which shows the SQL Server user databases being protected by SnapCenter and a target standby SQL instance in the public cloud.

Name	Instance	Host	Last Backup	Overall Status	Type
master	sql1	sql1.demo.netapp.com		Not available for backup	System database
model	sql1	sql1.demo.netapp.com		Not available for backup	System database
msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tpcc	sql1	sql1.demo.netapp.com	09/16/2021 7:35:05 PM	Backup succeeded	User database
master	sql1-standby	sql1-standby.demo.netapp.com		Not available for backup	System database
model	sql1-standby	sql1-standby.demo.netapp.com		Not available for backup	System database
msdb	sql1-standby	sql1-standby.demo.netapp.com		Not available for backup	System database
tempdb	sql1-standby	sql1-standby.demo.netapp.com		Not available for backup	System database

2. Click on the intended on-premises SQL Server user database name for the backups topology and detailed view. If a secondary replicated location is enabled, it shows linked mirror backups.

Backup Name	Count	Type	End Date	Verified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup	09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup	09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup	09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup	09/13/2021 6:25:05 PM	Unverified
sql1_tpcc_09-12-2021_18.25.01.4016	1	Full backup	09/12/2021 6:25:05 PM	Unverified
sql1_tpcc_09-11-2021_18.25.01.3753	1	Full backup	09/11/2021 6:25:05 PM	Unverified
sql1_tpcc_09-10-2021_18.36.25.5430	1	Full backup	09/10/2021 6:36:29 PM	Unverified

3. Toggle to the Mirrored Backups view by clicking Mirrored Backups. Secondary Mirror Backup(s) are then displayed. Because SnapCenter backs up the SQL Server transaction log to a dedicated drive for recovery, only full database backups are displayed here.

Backup Name	Count	Type	End Date	Verified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup	09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup	09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup	09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup	09/13/2021 6:25:05 PM	Unverified
sql1_tpcc_09-12-2021_18.25.01.4016	1	Full backup	09/12/2021 6:25:05 PM	Unverified
sql1_tpcc_09-11-2021_18.25.01.3753	1	Full backup	09/11/2021 6:25:05 PM	Unverified
sql1_tpcc_09-10-2021_18.36.25.5430	1	Full backup	09/10/2021 6:36:29 PM	Unverified

4. Choose a backup copy, and then click the Clone button to launch the Clone from Backup workflow.

The screenshot shows the NetApp SnapCenter interface for a Microsoft SQL Server topology named 'tpcc (sql1)'. On the left, a sidebar lists databases: master, model, msdb, tempdb, tpcc, and tpcc\_clone. The 'tpcc' database is selected. The main pane displays 'Manage Copies' with a summary: 7 Backups, 0 Clones, and 1 Clone. Below this, it shows 'Secondary Mirror Backup(s)' with a search bar. A table lists backup details:

Backup Name	Count	Type	End Date	Verified
sql1_tpcc_09-19-2021_18.25.01.4134	1	Full backup	09/19/2021 6:25:05 PM	Unverified
sql1_tpcc_09-18-2021_18.25.01.3963	1	Full backup	09/18/2021 6:25:05 PM	Unverified
sql1_tpcc_09-17-2021_18.25.01.4218	1	Full backup	09/17/2021 6:25:05 PM	Unverified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup	09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup	09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup	09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup	09/13/2021 6:25:05 PM	Unverified

The screenshot shows the 'Clone from backup' wizard, Step 1: Clone Options. The left sidebar shows steps 1 through 5: 1. Clone Options (selected), 2. Logs, 3. Script, 4. Notification, and 5. Summary. The main pane is titled 'Clone settings' and includes fields for 'Clone server' (Choose), 'Clone instance' (Nothing selected), and 'Clone name' (tpcc). Below this, it says 'Choose mount option' with two radio buttons: 'Auto assign mount point' (selected) and 'Auto assign volume mount point under path' (full file path). The next section is titled 'Secondary storage location : Snap Vault / Snap Mirror' and shows mappings for 'Source Volume' and 'Destination Volume':

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

At the bottom right are 'Previous' and 'Next' buttons.

5. Select a cloud server as the target clone server, clone instance name, and clone database name. Choose either an auto-assign mount point or a user-defined mount point path.

Clone from backup x

**1 Clone Options**

**Clone settings**

Clone server	sql-standby.demo.netapp.com	<span style="color: blue;">i</span>
Clone instance	sql-standby	<span style="color: blue;">i</span>
Clone name	tpcc_clone	

Choose mount option

Auto assign mount point i

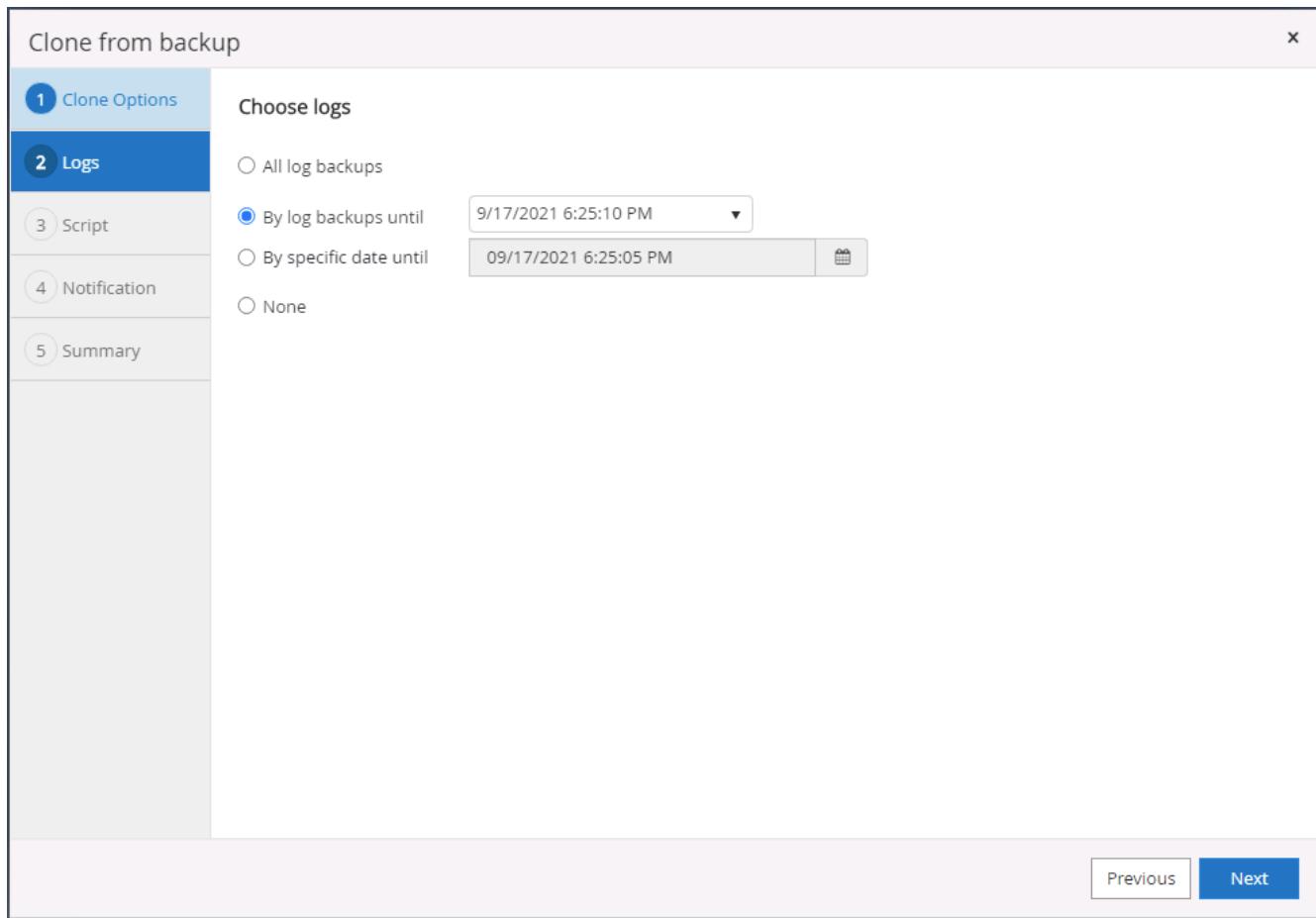
Auto assign volume mount point under path full file path i

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

Previous Next

6. Determine a recovery point either by a log backup time or by a specific date and time.



7. Specify optional scripts to run before and after the cloning operation.

Clone from backup x

**1 Clone Options**

**2 Logs**

**3 Script**

**4 Notification**

**5 Summary**

Specify optional scripts to run before and after performing a clone from backup job

Prescript full path

Prescript arguments  Choose optional arguments...

Postscript full path

Postscript arguments  Choose optional arguments...

Script timeout  60 secs

Previous Next

8. Configure an SMTP server if email notification is desired.

Clone from backup X

**1 Clone Options**

**2 Logs**

**3 Script**

**4 Notification**

**5 Summary**

Provide email settings i

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach Job Report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server. X

Previous Next

## 9. Clone Summary.

Clone from backup

**1 Clone Options**

**2 Logs**

**3 Script**

**4 Notification**

**5 Summary**

Summary	
Clone server	sql-standby.demo.netapp.com
Clone instance	sql-standby
Clone name	tpcc_dev
Mount option	Auto assign volume mount point under custom path
Prescript full path	None
Prescript arguments	
Postscript full path	None
Postscript arguments	
Send email	No

[Previous](#) [Finish](#)

- Monitor the job status and validate that the intended user database has been attached to a target SQL instance in the cloud clone server.

ID	Status	Name	Start date	End date	Owner
766	✓	Clone from backup 'sql1_tpcc_09-16-2021_18:25:01.4024'	09/16/2021 8:05:25 PM	09/16/2021 8:06:17 PM	demo\sqldba
763	✓	Discover resources for all hosts	09/16/2021 7:56:49 PM	09/16/2021 7:56:54 PM	demo\sqldba
761	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 7:59:00 PM	09/16/2021 7:57:08 PM	demo\sqldba
760	⚠	Discover resources for all hosts	09/16/2021 7:19:05 PM	09/16/2021 7:19:09 PM	demo\sqldba
759	⚠	Discover resources for all hosts	09/16/2021 7:18:43 PM	09/16/2021 7:18:48 PM	demo\sqldba
756	⚠	Discover resources for all hosts	09/16/2021 6:59:51 PM	09/16/2021 6:59:56 PM	demo\sqldba
753	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 6:35:00 PM	09/16/2021 6:37:07 PM	demo\sqldba
750	✓	Backup of Resource Group 'sql1_tpcc' with policy 'SQL Server Full Backup'	09/16/2021 6:25:01 PM	09/16/2021 6:27:14 PM	demo\sqldba
749	✓	Discover resources for host 'sql-standby.demo.netapp.com'	09/16/2021 6:19:00 PM	09/16/2021 6:19:05 PM	Demo\administrator
745	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 5:35:00 PM	09/16/2021 5:37:08 PM	demo\sqldba

## Post-clone configuration

- An Oracle production database on-premises is usually running in log archive mode. This mode is not necessary for a development or test database. To turn off log archive mode, log into the Oracle DB as sysdba, execute a log mode change command, and start the database for access.
- Configure an Oracle listener, or register the newly cloned DB with an existing listener for user access.
- For SQL Server, change the log mode from Full to Easy so that the SQL Server dev/test log file can be readily shrunk when it is filling up the log volume.

## Refresh clone database

1. Drop cloned databases and clean up the cloud DB server environment. Then follow the previous procedures to clone a new DB with fresh data. It only takes few minutes to clone a new database.
2. Shutdown the clone database, run a clone refresh command by using the CLI. See the following SnapCenter documentation for details: [Refresh a clone](#).

## Where to go for help?

If you need help with this solution and use cases, join the [NetApp Solution Automation community support Slack channel](#) and look for the solution-automation channel to post your questions or inquires.

Next: [Disaster recovery workflow](#).

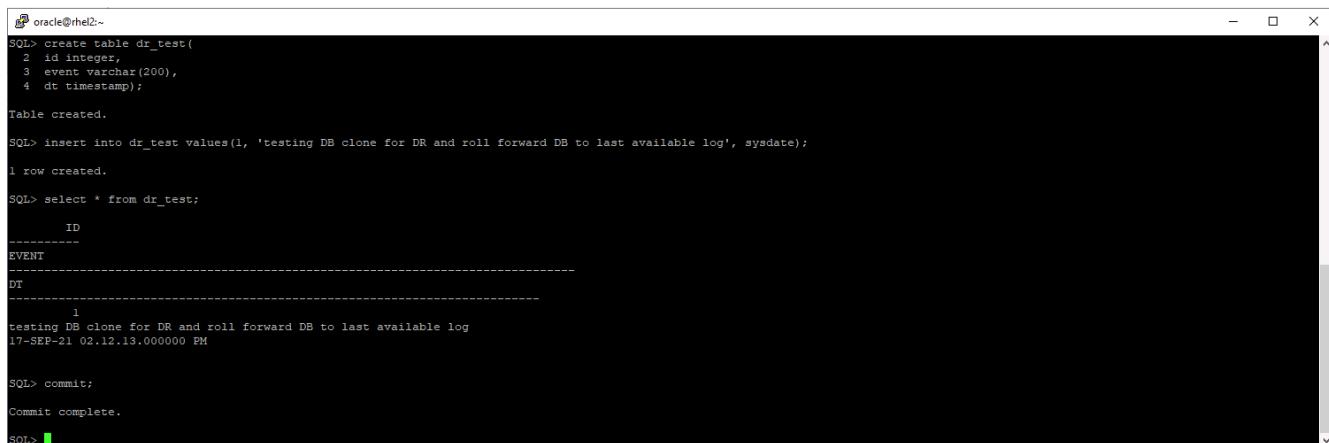
## Disaster recovery workflow

Previous: [Workflow for dev/test bursting to cloud](#).

Enterprises have embraced the public cloud as a viable resource and destination for disaster recovery. SnapCenter makes this process as seamless as possible. This disaster recovery workflow is very similar to the clone workflow, but database recovery runs through the last available log that was replicated to cloud to recover all the business transactions possible. However, there are additional pre-configuration and post-configuration steps specific to disaster recovery.

### Clone an on-premises Oracle production DB to cloud for DR

1. To validate that the clone recovery runs through last available log, we created a small test table and inserted a row. The test data would be recovered after a full recovery to last available log.



```
oracle@rhel2:~$ SQL> create table dr_test(
  2  id integer,
  3  event varchar(200),
  4  dt timestamp);
Table created.

SQL> insert into dr_test values(1, 'testing DB clone for DR and roll forward DB to last available log', sysdate);
1 row created.

SQL> select * from dr_test;
      ID
-----
EVENT
-----
DT
-----
1
testing DB clone for DR and roll forward DB to last available log
17-SEP-21 02.12.13.000000 PM

SQL> commit;
Commit complete.

SQL>
```

2. Log into SnapCenter as a database management user ID for Oracle. Navigate to the Resources tab, which shows the Oracle databases being protected by SnapCenter.

The screenshot shows the NetApp SnapCenter interface. The top navigation bar includes links for App Backup and Clone Admin and Sign Out. On the left, a sidebar menu lists Dashboard, Resources (selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area displays a table of Oracle Database resources. One row is selected, showing details: Name (rhe12\_cdb2), Resources (1), Tags (orafullbkup), Policies (Oracle Full Online Backup), Last Backup (09/17/2021 2:38:16 PM), and Overall Status (Completed). A 'New Resource Group' button is located in the top right corner of the main content area.

3. Select the Oracle log resource group and click Backup Now to manually run an Oracle log backup to flush the latest transaction to the destination in the cloud. In a real DR scenario, the last transaction recoverable depends on the database log volume replication frequency to the cloud, which in turn depends on the RTO or RPO policy of the company.

This screenshot shows the 'rhe12\_cdb2\_log' resource group details page. The top navigation bar and sidebar are identical to the previous screenshot. The main content area shows a table with one row: Name (rhe12\_cdb2), Resource Name (cdb2), Type (Oracle Database), and Host (rhe12.demo.netapp.com). Below the table, there are four buttons: Modify Resource Group, Back up Now (highlighted in blue), Maintenance, and Delete.

This screenshot shows the 'Backup' dialog box. The title bar says 'Backup'. The main content area has two sections: 'Resource Group' (set to 'rhe12\_cdb2\_log') and 'Policy' (set to 'Oracle Archive Log Backup'). At the bottom right are 'Cancel' and 'Backup' buttons. The 'Backup' button is highlighted in blue.



Asynchronous SnapMirror loses data that has not made it to the cloud destination in the database log backup interval in a disaster recovery scenario. To minimize data loss, more frequent log backup can be scheduled. However there is a limit to the log backup frequency that is technically achievable.

4. Select the last log backup on the Secondary Mirror Backup(s), and mount the log backup.

The screenshot shows the NetApp SnapCenter interface for Oracle Database management. On the left, a sidebar lists databases: cdb2, cdb2dev, and cdb2test. The main area displays 'cdb2 Topology' with a diagram showing 'Local copies' (185 Backups, 0 Clones) connected to 'Mirror copies' (185 Backups, 2 Clones). A summary card on the right provides an overview of backup counts: 370 Backups, 16 Data Backups, 354 Log Backups, and 2 Clones. Below this, a table titled 'Secondary Mirror Backup(s)' lists three log backups:

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_18.20.04.1177_1	1	Log	09/17/2021 6:20:13 PM	Not Applicable	False	Not Cataloged	5994710
rhel2_cdb2_log_09-17-2021_18.00.01.2424_1	1	Log	09/17/2021 6:00:09 PM	Not Applicable	False	Not Cataloged	5992079
rhel2_cdb2_log_09-17-2021_17.00.01.1566_1	1	Log	09/17/2021 5:00:20 PM	Not Applicable	False	Not Cataloged	5988842

The dialog box is titled 'Mount backups'. It asks 'Choose the host to mount the backup' and provides a dropdown menu with 'ora-standby.demo.netapp.com'. Below this, 'Mount path' is set to '/var/opt/snapcenter/sco/backup\_mount/rhel2\_cdb2\_log\_09-17-2021\_18.20.04.1177\_1/cdb2'. The next section, 'Secondary storage location : Snap Vault / Snap Mirror', shows 'Source Volume' as 'svm\_onPrem:rhel2\_u03' and 'Destination Volume' as 'svm\_hybridcvo:rhel2\_u03\_dr'. At the bottom are 'Mount' and 'Cancel' buttons.

5. Select the last full database backup and click Clone to initiate the clone workflow.

Total 3

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_18.20.04.1177_1	1	Log		09/17/2021 6:20:13 PM	Not Applicable	True	Not Cataloged	5994710
rhel2_cdb2_log_09-17-2021_18.00.01.2424_1	1	Log		09/17/2021 6:00:09 PM	Not Applicable	False	Not Cataloged	5992079
rhel2_cdb2_log_09-17-2021_17.00.01.1566_1	1	Log		09/17/2021 5:00:20 PM	Not Applicable	False	Not Cataloged	5988842
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log		09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588

## 6. Select a unique clone DB ID on the host.

### Clone from cdb2

**1 Name**

Complete Database Clone

Clone SID:

PDB Clone

**Secondary storage location : Snap Vault / Snap Mirror**

**2 Data**

Source Volume	Destination Volume
svm_onPrem:rhel2_u02	<input type="text" value="svm_hybridcvo:rhel2_u02_dr"/>

**3 Logs**

Source Volume	Destination Volume
svm_onPrem:rhel2_u03	<input type="text" value="svm_hybridcvo:rhel2_u03_dr"/>

**Next**

## 7. Provision a log volume and mount it to the target DR server for the Oracle flash recovery area and online logs.

The screenshot shows the ONTAP System Manager interface. On the left, there's a navigation sidebar with sections like DASHBOARD, STORAGE (Overview, Applications, Volumes), LUNs, Shares, Qtrees, Quotas, Storage VMs, Tiers, NETWORK, EVENTS & JOBS, PROTECTION, and HOSTS. The main area is titled 'Volumes' and lists several volumes: 'ora\_standby\_u01', 'rhel2\_u01\_dr', 'rhel2\_u02\_dr', 'rhel2\_u02\_dr09172116081193\_60', 'rhel2\_u02\_dr09172117035348\_63', 'rhel2\_u03\_dr', and 'rhel2\_u03\_dr09172118245747\_75'. A modal window titled 'Add Volume' is open, prompting for a 'NAME' (set to 'ora\_standby\_u03') and 'CAPACITY' (set to '20 GB'). There are 'More Options' and 'Save' buttons.

```

[ec2-user@ora-standby:tmp]$ sudo mkdir /u03_cdb2dr
[ec2-user@ora-standby tmp]$ chown oracle:oinstall /u03_cdb2dr
chown: changing ownership of '/u03_cdb2dr': Operation not permitted
[ec2-user@ora-standby tmp]$ sudo chown oracle:oinstall /u03_cdb2dr
[ec2-user@ora-standby tmp]$ sudo mount -t nfs 10.221.1.6:/ora_standby_u03 /u03_cdb2dr
[ec2-user@ora-standby tmp]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/tmpfs       7.6G  0    7.6G  0% /dev
tmpfs           7.6G  0    7.6G  0% /dev/shm
tmpfs           7.6G  17M  7.6G  1% /run
tmpfs           7.6G  0    7.6G  0% /sys/fs/cgroup
/dev/nvme0nlp2   10G  9.0G  1.1G  90% /
10.221.1.6:/ora_standby_u01   31G  13G  18G  42% /u01
tmpfs           1.6G  0    1.6G  0% /run/user/1000
10.221.1.6:/Sc28182452-3fa8-448c-9e4a-c5a9e465f353 100G  3.1G  97G  4% /u02_cdb2dev
tmpfs           1.6G  0    1.6G  0% /run/user/54321
10.221.1.6:/Sc39c05df8-4b00-4b3a-853c-9d6d338e5df7 100G  3.7G  97G  4% /u02_cdb2test
10.221.1.6:/Scff88ea5c-3273-475e-ad97-472b2a8dccee 100G  3.8G  97G  4% /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_log_09-17-2021_18.20.04.1177_1/cdb2/1
10.221.1.6:/ora_standby_u03   21G  320K  20G  1% /u03_cdb2dr
[ec2-user@ora-standby tmp]$

```



The Oracle clone procedure does not create a log volume, which needs to be provisioned on the DR server before cloning.

8. Select the target clone host and location to place the data files, control files, and redo logs.

Clone from cdb2

**1 Name**

Select the host to create a clone

Clone host ora-standby.demo.netapp.com

**2 Locations**

Datafile locations /u02\_cdb2dr

Control files /u02\_cdb2dr/cdb2dr/control/control01.ctl  
/u03\_cdb2dr/cdb2dr/control/control02.ctl

Redo logs

Group	Size	Unit	Number of files
RedoGroup 1	200	MB	1
RedoGroup 2	200	MB	1

Previous Next

9. Select the credentials for the clone. Fill in the details of the Oracle home configuration on the target server.

Clone from cdb2

**1 Name**

**2 Locations**

**3 Credentials**

**4 PreOps**

**5 PostOps**

**6 Notification**

**7 Summary**

Database Credentials for the clone

Credential name for sys user  + ?

Database port

Oracle Home Settings ?

Oracle Home

Oracle OS User

Oracle OS Group

Previous Next

The screenshot shows the Oracle Database Clone wizard interface. The left sidebar lists steps 1 through 7. Step 3, 'Credentials', is currently selected and highlighted in blue. The main panel shows 'Database Credentials for the clone' with a dropdown for 'Credential name for sys user' set to 'None' and a port of '1521'. Below that, 'Oracle Home Settings' are configured with the Oracle Home path set to '/u01/app/oracle/product/19800/cdb2', and the Oracle OS User and Group both set to 'oracle'. At the bottom right are 'Previous' and 'Next' buttons.

10. Specify the scripts to run before cloning. Database parameters can be adjusted if needed.

Clone from cdb2

**Specify scripts to run before clone operation** ⓘ

Prescript full path	/var/opt/snapcenter/spl/scripts/	Enter Prescript path
Arguments		
Script timeout	60	secs

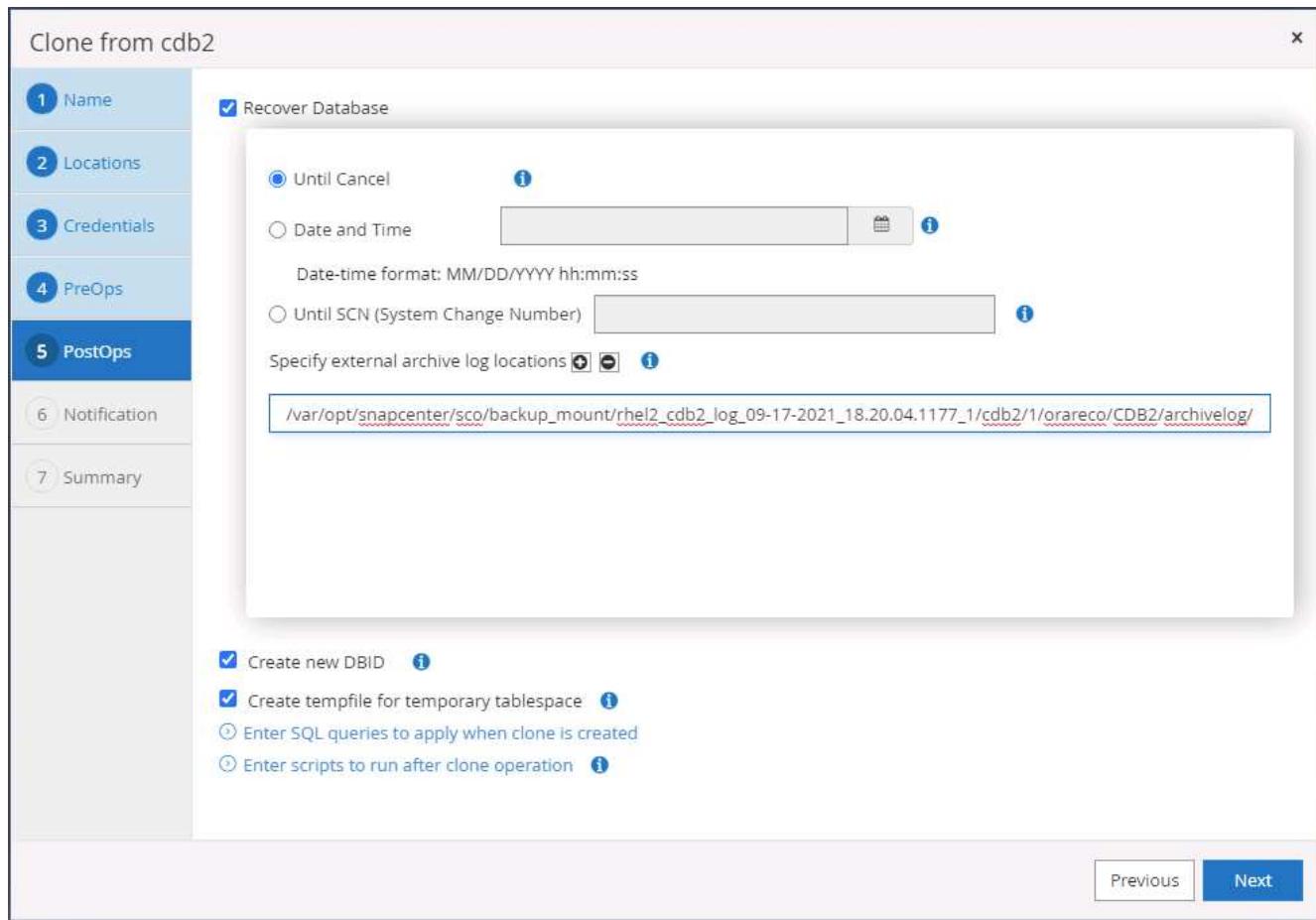
**Database Parameter settings**

audit_file_dest	/u01/app/oracle/admin/cdb2dr/adump	X
audit_trail	DB	X
open_cursors	300	X
pga_aggregate_target	1432354816	X

**Buttons:**

- Previous
- Next

- Select Until Cancel as the recovery option so that the recovery runs through all available archive logs to recoup the last transaction replicated to the secondary cloud location.



12. Configure the SMTP server for email notification if needed.

Clone from cdb2

**Provide email settings i**

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach job report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

[Previous](#) [Next](#)

1. Name  
2. Locations  
3. Credentials  
4. PreOps  
5. PostOps  
**6. Notification**  
7. Summary

13. DR clone summary.

Clone from cdb2

<b>1 Name</b>	Summary
<b>2 Locations</b>	Clone from backup      rhel2_cdb2_09-17-2021_14.35.01.4997_0
<b>3 Credentials</b>	Clone SID      cdb2dr
<b>4 PreOps</b>	Clone server      ora-standby.demo.netapp.com
<b>5 PostOps</b>	Exclude PDBs      none
<b>6 Notification</b>	Oracle home      /u01/app/oracle/product/19800/cdb2
<b>7 Summary</b>	Oracle OS user      oracle
	Oracle OS group      oinstall
	Datafile mountpaths      /u02_cdb2dr
	Control files      /u02_cdb2dr/cdb2dr/control/control01.ctl /u03_cdb2dr/cdb2dr/control/control02.ctl
	Redo groups      RedoGroup =1 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo03.log RedoGroup =2 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo02.log RedoGroup =3 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo01.log
	Recovery scope      Until Cancel
	Prescript full path      none
	Prescript arguments
	Postscript full path      none
	Postscript arguments

[Previous](#) [Finish](#)

14. Cloned DBs are registered with SnapCenter immediately after clone completion and are then available for backup protection.

Oracle Database							
Resources		Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup
		cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com	rhel2_cdb2 rhel2_cdb2_log	Oracle Archive Log Backup Oracle Full Online Backup	09/17/2021 7:00:10 PM
		cdb2dev	Single Instance (Multitenant)	ora-standby.demo.netapp.com			Not protected
		cdb2dr	Single Instance (Multitenant)	ora-standby.demo.netapp.com			Not protected
		cdb2test	Single Instance (Multitenant)	ora-standby.demo.netapp.com			Not protected

## Post DR clone validation and configuration for Oracle

1. Validate the last test transaction that has been flushed, replicated, and recovered at the DR location in the cloud.

```

oracle@ora-standby:/u01/app/oracle/product/19000/cdb2/dbs
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> set lin 200
SQL> select instance_name, host_name from v$instance;

INSTANCE_NAME      HOST_NAME
cdb2dr            ora-standby.demo.netapp.com

SQL> alter pluggable database cdb2_pdb1 open;
Pluggable database altered.

SQL> alter session set container=cdb2_pdb1;
Session altered.

SQL> select * from pdbadmin.dr_test;

ID
EVENT
DT
1
testing DB clone for DR and roll forward DB to last available log
17-SEP-21 02.12.13.000000 PM

SQL>

```

## 2. Configure the flash recovery area.

```

oracle@ora-standby:/u01/app/oracle/product/19000/cdb2/dbs
[oracle@ora-standby dbs]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 17 22:07:11 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> show parameter db_recovery_file_dest

NAME          TYPE        VALUE
-----
db_recovery_file_dest    string
db_recovery_file_dest_size  big integer 17208M
SQL> alter system set db_recovery_file_dest='/u03_cdb2dr/cdb2dr' scope=both;

System altered.

SQL> show parameter db_recovery_file_dest

NAME          TYPE        VALUE
-----
db_recovery_file_dest    string    /u03_cdb2dr/cdb2dr
db_recovery_file_dest_size  big integer 17208M
SQL>

```

## 3. Configure the Oracle listener for user access.

## 4. Split the cloned volume off of the replicated source volume.

## 5. Reverse replication from the cloud to on-premises and rebuild the failed on-premises database server.



Clone split may incur temporary storage space utilization that is much higher than normal operation. However, after the on-premises DB server is rebuilt, extra space can be released.

## Clone an on-premises SQL production DB to cloud for DR

- Similarly, to validate that the SQL clone recovery ran through last available log, we created a small test table and inserted a row. The test data would be recovered after a full recovery to the last available log.

```

Administrator: Command Prompt - sqlcmd - SQLCMD
C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go

-----
SQL1

(1 rows affected)
1> use tpcc
2> go
Changed database context to 'tpcc'.
1> insert into snap_sync values ('test snap mirror DR for SQL', getdate())
2> go

(1 rows affected)
1> select * from snap_sync
2> go
event                                dt
test snap mirror DR for SQL          2021-09-20 14:23:04.533
(1 rows affected)
1> -

```

- Log into SnapCenter with a database management user ID for SQL Server. Navigate to the Resources tab, which shows the SQL Server protection resources group.

The screenshot shows the NetApp SnapCenter interface. The top navigation bar includes links for Microsoft SQL Server, demo/sqldba, App Backup and Clone Admin, and Sign Out. Below the navigation is a search bar labeled 'search by name' and a secondary search bar labeled 'search'. The main area displays a table of resources:

Name	Resource Name	Type	Host
sql1_tpcc	tpcc (sql1)	SQL Database	sql1.demo.netapp.com
sql1_tpcc_log			

On the far right of the table are several icons: Modify Resource Group, Back up Now, Clone Lifecycle, Maintenance, Edit/View Details, and Delete.

- Manually run a log backup to flush the last transaction to be replicated to secondary storage in the public cloud.

The screenshot shows a 'Backup' dialog box. At the top, it says 'Create a backup for the selected resource group'. Below that, there are two input fields: 'Resource Group' containing 'sql1\_tpcc\_log' and 'Policy' containing 'SQL Server Log Backup'. To the right of the policy dropdown is an information icon (blue circle with an 'i'). At the bottom right of the dialog are 'Cancel' and 'Backup' buttons.

- Select the last full SQL Server backup for the clone.

NetApp SnapCenter®

Microsoft SQL Server

tpcc (sql11) Topology

Manage Copies

Local copies: 7 Backups, 0 Clones

Mirror copies: 2 Backups, 2 Clones

Summary Card

14 Backups, 2 Clones

- Set the clone setting such as the Clone Server, Clone Instance, Clone Name, and mount option. The secondary storage location where cloning is performed is auto-populated.

### Clone from backup

**1 Clone Options**

**Clone settings**

Clone server	sql-standby.demo.netapp.com	<i>Info</i>
Clone instance	sql-standby	<i>Info</i>
Clone name	tpcc_dr	

**Choose mount option**

Auto assign mount point *Info*

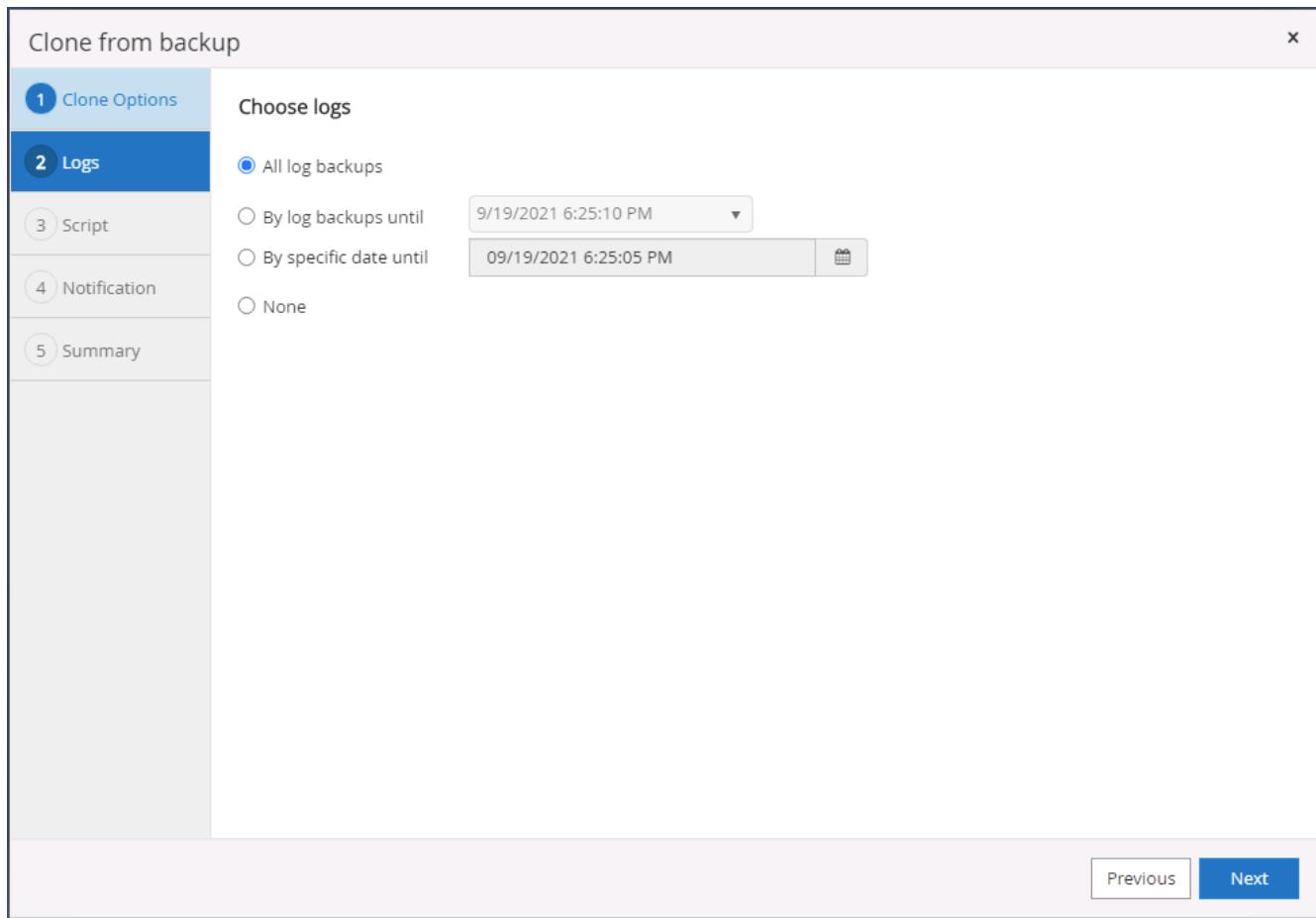
Auto assign volume mount point under path  *Info*

**Secondary storage location : Snap Vault / Snap Mirror**

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

**Next**

- Select all log backups to be applied.



7. Specify any optional scripts to run before or after cloning.

Clone from backup x

**1 Clone Options**

**2 Logs**

**3 Script**

**4 Notification**

**5 Summary**

Specify optional scripts to run before and after performing a clone from backup job

Prescript full path

Prescript arguments  Choose optional arguments...

Postscript full path

Postscript arguments  Choose optional arguments...

Script timeout  60 secs

Previous Next

8. Specify an SMTP server if email notification is desired.

Clone from backup

**Provide email settings i**

Email preference	Never
From	From email
To	Email to
Subject	Notification

Attach Job Report

**⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.**

**Previous** **Next**

1 Clone Options  
2 Logs  
3 Script  
**4 Notification**  
5 Summary

- DR clone summary. Cloned databases are immediately registered with SnapCenter and available for backup protection.

Clone from backup

**1 Clone Options**

**2 Logs**

**3 Script**

**4 Notification**

**5 Summary**

**Summary**

Clone server	sql-standby.demo.netapp.com
Clone instance	sql-standby
Clone name	tpcc_dr
Mount option	Auto Mount
Prescript full path	None
Prescript arguments	
Postscript full path	None
Postscript arguments	
Send email	No

**Previous** **Finish**

NetApp SnapCenter®

Microsoft SQL Server

View Database search by name

Refresh Resources New Resource Group

Resources

Name	Instance	Host	Last Backup	Overall Status	Type
master	sql1	sql1.demo.netapp.com		Not available for backup	System database
model	sql1	sql1.demo.netapp.com		Not available for backup	System database
msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tpcc	sql1	sql1.demo.netapp.com	09/22/2021 5:35:08 PM	Backup failed, Schedules on hold	User database
master	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
model	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
msdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
tempdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
tpcc_clone	sql-standby	sql-standby.demo.netapp.com		Not protected	User database
tpcc_dlev	sql-standby	sql-standby.demo.netapp.com		Not protected	User database
tpcc_dr	sql-standby	sql-standby.demo.netapp.com		Not protected	User database

## Post DR clone validation and configuration for SQL

### 1. Monitor clone job status.

NetApp SnapCenter®

Jobs Schedules Events Logs

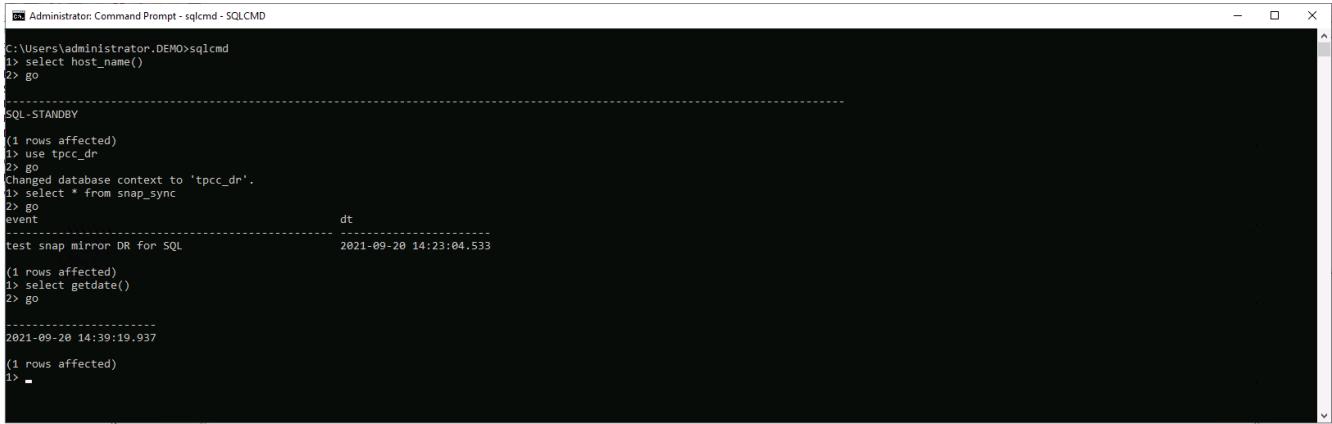
Search by name

Details Reports Download Logs Cancel All

Jobs - Filter

ID	Status	Name	Start date	End date	Owner
1052	✓	Clone from backup 'sql1_tpcc_09-19-2021_18.25.01.4134'	09/20/2021 2:36:17 PM	09/20/2021 2:37:06 PM	demo\sqldba
1047	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 2:35:01 PM	09/20/2021 2:37:08 PM	demo\sqldba
1045	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 2:28:17 PM	09/20/2021 2:30:25 PM	demo\sqldba
1044	✓	Clone from backup 'sql1_tpcc_09-17-2021_18.25.01.4218'	09/20/2021 1:39:24 PM	09/20/2021 1:40:09 PM	demo\sqldba
1042	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 1:35:01 PM	09/20/2021 1:37:08 PM	demo\sqldba
1040	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 1:25:01 PM	09/20/2021 1:27:08 PM	demo\sqldba

### 2. Validate that last transaction has been replicated and recovered with all log file clones and recovery.



```
C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go
-----
SQL STANDBY
(1 rows affected)
1> use tpcc_dr
2> go
Changed database context to 'tpcc_dr'.
1> select * from snap_sync
2> go
event                                dt
test snap mirror DR for SQL          2021-09-20 14:23:04.533
(1 rows affected)
1> select getdate()
2> go
-----
2021-09-20 14:39:19.937
(1 rows affected)
1> -
```

3. Configure a new SnapCenter log directory on the DR server for SQL Server log backup.
4. Split the cloned volume off of the replicated source volume.
5. Reverse replication from the cloud to on-premises and rebuild the failed on-premises database server.

### Where to go for help?

If you need help with this solution and use cases, please join the [NetApp Solution Automation community support Slack channel](#) and look for the solution-automation channel to post your questions or inquiries.

# NetApp Modern Data Analytics Solutions

## Big Data Analytics Data to Artificial Intelligence

### TR-4732: Big data analytics data to artificial intelligence

Karthikeyan Nagalingam, NetApp

This document describes how to move big-data analytics data and HPC data to AI. AI processes NFS data through NFS exports, whereas customers often have their AI data in a big-data analytics platform, such as HDFS, Blob, or S3 storage as well as HPC platforms such as GPFS. This paper provides guidelines for moving big-data-analytics data and HPC data to AI by using NetApp XCP and NIPAM. We also discuss the business benefits of moving data from big data and HPC to AI.

#### Concepts and components

##### Big data analytics storage

Big data analytics is the major storage provider for HDFS. A customer often uses a Hadoop-compatible file system (HCFS) such as Windows Azure Blob Storage, MapR File System (MapR-FS), and S3 object storage.

##### General parallel file system

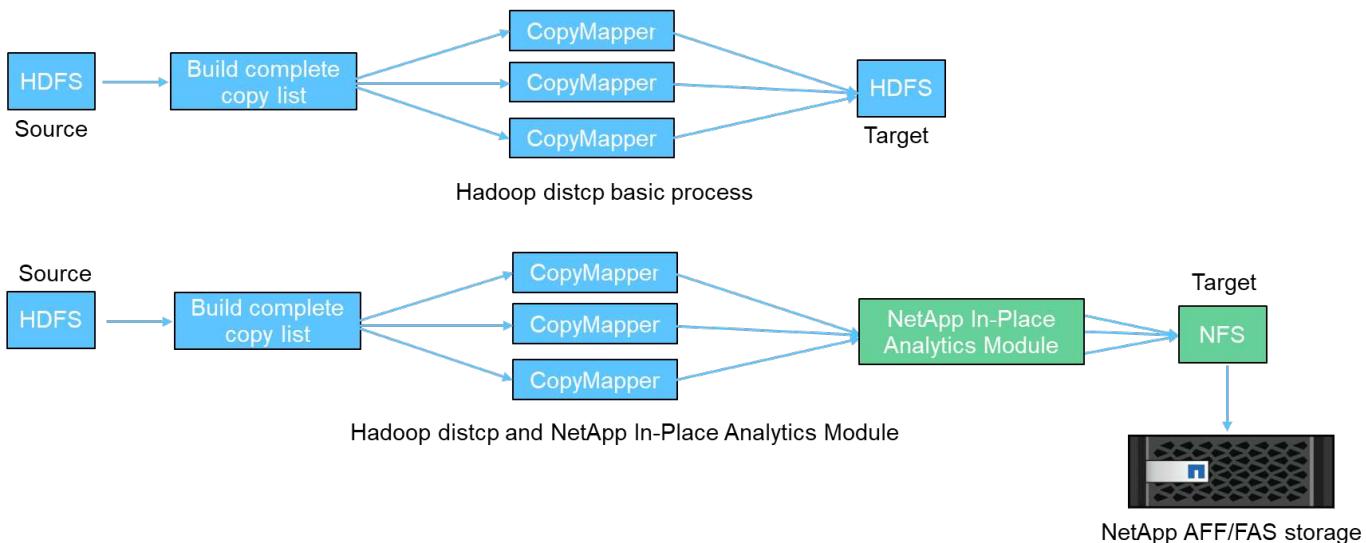
IBM's GPFS is an enterprise file system that provides an alternative to HDFS. GPFS provides flexibility for applications to decide the block size and replication layout, which provide good performance and efficiency.

##### NetApp In-Place Analytics Module

The NetApp In-Place Analytics Module (NIPAM) serves as a driver for Hadoop clusters to access NFS data. It has four components: a connection pool, an NFS InputStream, a file handle cache, and an NFS OutputStream. For more information, see [TR-4382: NetApp In-Place Analytics Module](#).

##### Hadoop Distributed Copy

Hadoop Distributed Copy (DistCp) is a distributed copy tool used for large inter-cluster and intra-cluster coping tasks. This tool uses MapReduce for data distribution, error handling, and reporting. It expands the list of files and directories and inputs them to map tasks to copy the data from the source list. The image below shows the DistCp operation in HDFS and nonHDFS.



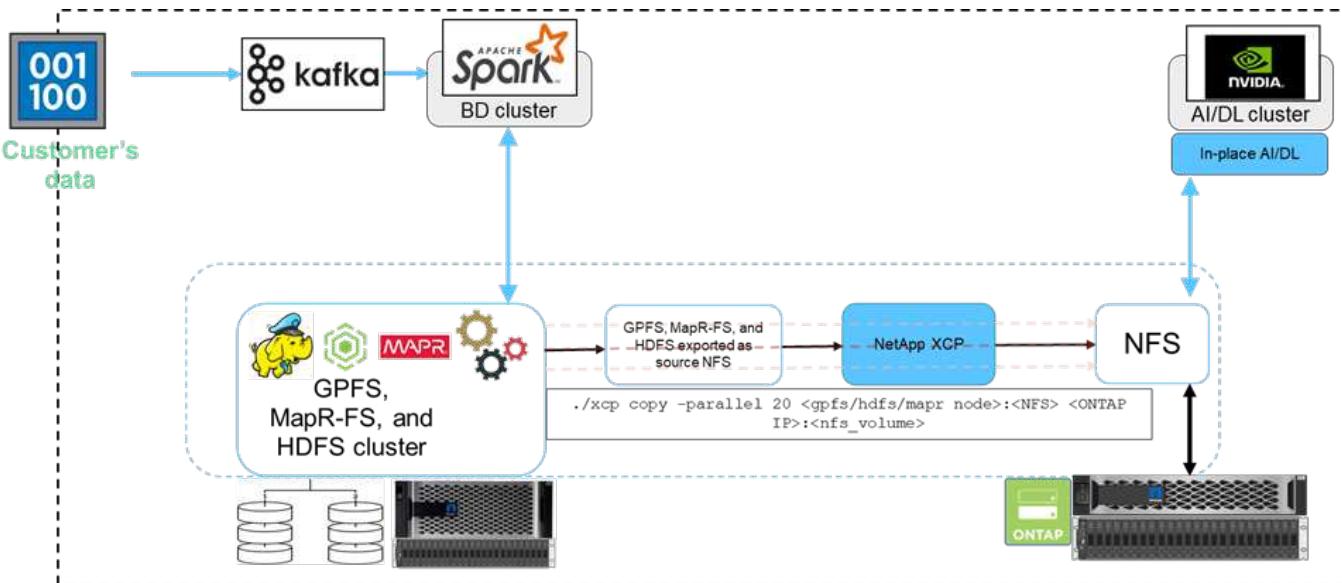
Hadoop DistCp moves data between the two HDFS systems without using an additional driver. NetApp provides the driver for non-HDFS systems. For an NFS destination, NIPAM provides the driver to copy data that Hadoop DistCp uses to communicate with NFS destinations when copying data.

## NetApp Cloud Volumes Service

The NetApp Cloud Volumes Service is a cloud-native file service with extreme performance. This service helps customers accelerate their time-to-market by rapidly spinning resources up and down and using NetApp features to improve productivity and reduce staff downtime. The Cloud Volumes Service is the right alternative for disaster recovery and back up to cloud because it reduces the overall data-center footprint and consumes less native public cloud storage.

## NetApp XCP

NetApp XCP is client software that enables fast and reliable any-to-NetApp and NetApp-to-NetApp data migration. This tool is designed to copy a large amount of unstructured NAS data from any NAS system to a NetApp storage controller. The XCP Migration Tool uses a multicore, multichannel I/O streaming engine that can process many requests in parallel, such as data migration, file or directory listings, and space reporting. This is the default NetApp data Migration Tool. You can use XCP to copy data from a Hadoop cluster and HPC to NetApp NFS storage. The diagram below shows data transfer from a Hadoop and HPC cluster to a NetApp NFS volume using XCP.



## NetApp Cloud Sync

NetApp Cloud Sync is a hybrid data replication software-as-a-service that transfers and synchronizes NFS, S3, and CIFS data seamlessly and securely between on-premises storage and cloud storage. This software is used for data migration, archiving, collaboration, analytics, and more. After data is transferred, Cloud Sync continuously syncs the data between the source and destination. Going forward, it then transfers the delta. It also secures the data within your own network, in the cloud, or on premises. This software is based on a pay-as-you-go model, which provides a cost-effective solution and provides monitoring and reporting capabilities for your data transfer.

[Next: Customer challenges.](#)

## Customer challenges

[Previous: Introduction.](#)

Customers might face the following challenges when trying to access data from big-data analytics for AI operations:

- Customer data is in a data lake repository. The data lake can contain different types of data such as structured, unstructured, semi-structured, logs, and machine-to-machine data. All these data types must be processed in AI systems.
- AI is not compatible with Hadoop file systems. A typical AI architecture is not able to directly access HDFS and HCFS data, which must be moved to an AI-understandable file system (NFS).
- Moving data lake data to AI typically requires specialized processes. The amount of data in the data lake can be very large. A customer must have an efficient, high-throughput, and cost-effective way to move data into AI systems.
- Syncing data. If a customer wants to sync data between the big-data platform and AI, sometimes the data processed through AI can be used with big data for analytical processing.

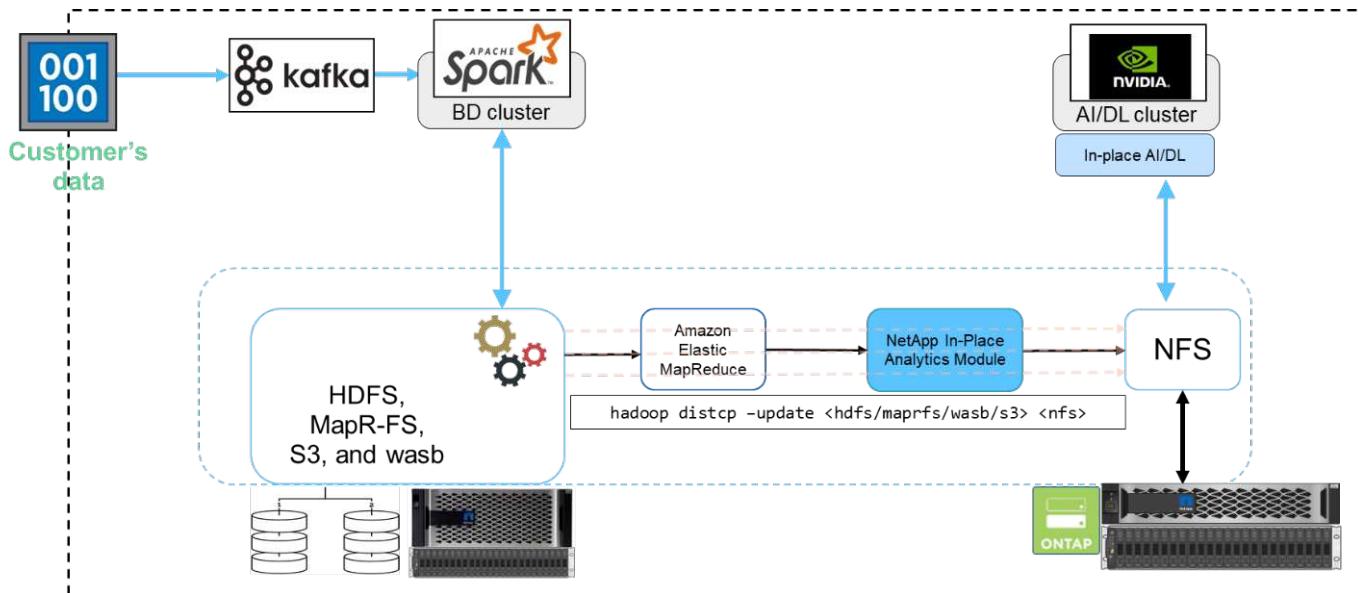
[Next: Data mover solution.](#)

## Data mover solution

[Previous: Customer challenges.](#)

In a big-data cluster, data is stored in HDFS or HCFS, such as MapR-FS, the Windows Azure Storage Blob, S3, or the Google file system. We performed testing with HDFS, MapR-FS, and S3 as the source to copy data to NetApp ONTAP NFS export with the help of NIPAM by using the `hadoop distcp` command from the source.

The following diagram illustrates the typical data movement from a Spark cluster running with HDFS storage to a NetApp ONTAP NFS volume so that NVIDIA can process AI operations.



The `hadoop distcp` command uses the MapReduce program to copy the data. NIPAM works with MapReduce to act as a driver for the Hadoop cluster when copying data. NIPAM can distribute a load across multiple network interfaces for a single export. This process maximizes the network throughput by distributing the data across multiple network interfaces when you copy the data from HDFS or HCFS to NFS.



NIPAM is not supported or certified with MapR.

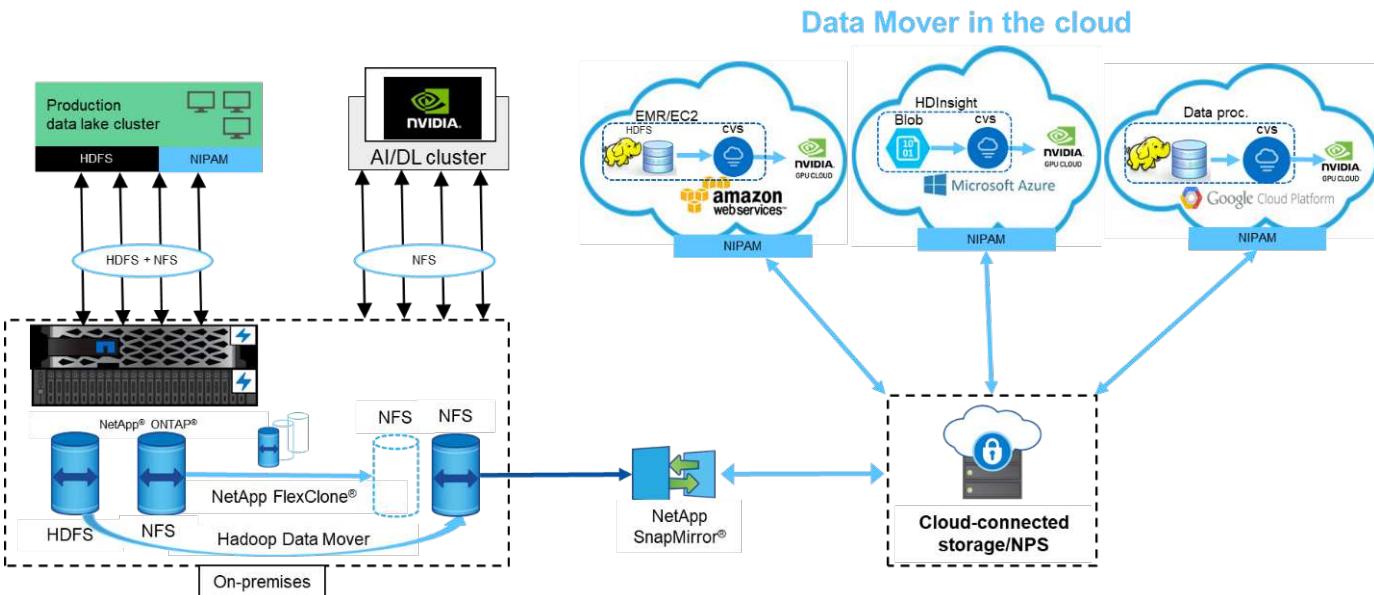
[Next: Data mover solution for AI.](#)

## Data mover solution for AI

[Previous: Data mover solution.](#)

The data mover solution for AI is based on customers' needs to process Hadoop data from AI operations. NetApp moves data from HDFS to NFS by using the NIPAM. In one use case, the customer needed to move data to NFS on the premises and another customer needed to move data from the Windows Azure Storage Blob to Cloud Volumes Service in order to process the data from the GPU cloud instances in the cloud.

The following diagram illustrates the data mover solution details.



The following steps are required to build the data mover solution:

1. ONTAP SAN provides HDFS, and NAS provides the NFS volume through NIPAM to the production data lake cluster.
2. The customer's data is in HDFS and NFS. The NFS data can be production data from other applications that is used for big data analytics and AI operations.
3. NetApp FlexClone technology creates a clone of the production NFS volume and provisions it to the AI cluster on premises.
4. Data from an HDFS SAN LUN is copied into an NFS volume with NIPAM and the `hadoop distcp` command. NIPAM uses the bandwidth of multiple network interfaces to transfer data. This process reduces the data copy time so that more data can be transferred.
5. Both NFS volumes are provisioned to the AI cluster for AI operations.
6. To process on-the-premises NFS data with GPUs in the cloud, the NFS volumes are mirrored to NetApp Private Storage (NPS) with NetApp SnapMirror technology and mounted to cloud service providers for GPUs.
7. The customer wants to process data in EC2/EMR, HDInsight, or DataProc services in GPUs from cloud service providers. The Hadoop data mover moves the data from Hadoop services to the Cloud Volumes Services with NIPAM and the `hadoop distcp` command.
8. The Cloud Volumes Service data is provisioned to AI through the NFS protocol. Data that is processed through AI can be sent on an on-premises location for big data analytics in addition to the NVIDIA cluster through NIPAM, SnapMirror, and NPS.

In this scenario, the customer has large file-count data in the NAS system at a remote location that is required for AI processing on the NetApp storage controller on premises. In this scenario, it's better to use the XCP Migration Tool to migrate the data at a faster speed.

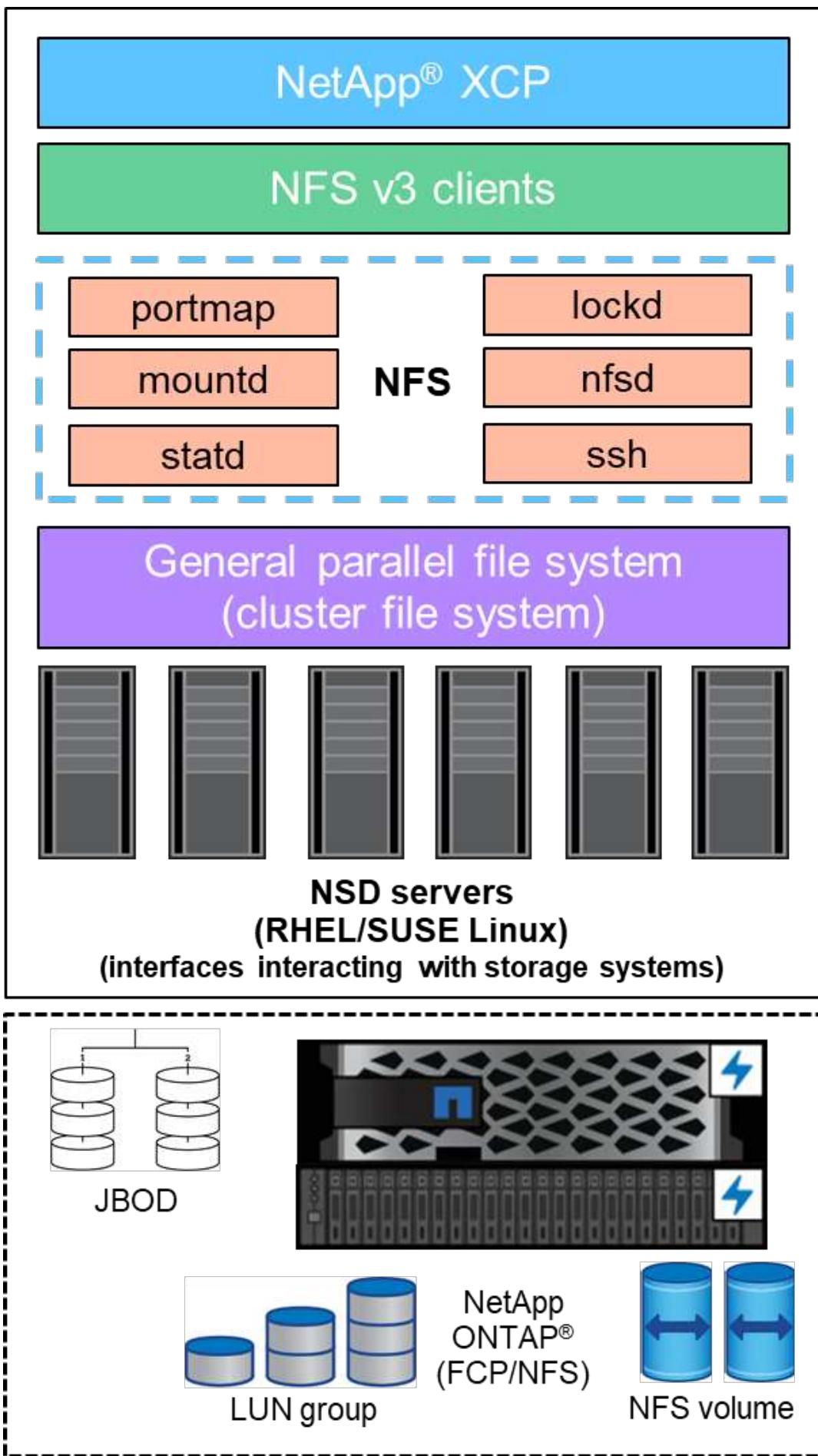
The hybrid-use-case customer can use Cloud Sync to migrate on-premises data from NFS, CIFS, and S3 data to the cloud and vice versa for AI processing by using GPUs such as those in an NVIDIA cluster. Both Cloud Sync and the XCP Migration Tool are used for the NFS data migration to NetApp ONTAP NFS.

[Next: GPFS to NetApp ONTAP NFS.](#)

## GPFS to NetApp ONTAP NFS

[Previous: Data mover solution for AI.](#)

In this validation, we used four servers as Network Shared Disk (NSD) servers to provide physical disks for GPFS. GPFS is created on top of the NSD disks to export them as NFS exports so that NFS clients can access them, as shown in the figure below. We used XCP to copy the data from GPFS- exported NFS to a NetApp NFS volume.



## GPFS essentials

The following node types are used in GPFS:

- **Admin node.** Specifies an optional field containing a node name used by the administration commands to communicate between nodes. For example, the admin node `mastr-51.netapp.com` could pass a network check to all other nodes in the cluster.
- **Quorum node.** Determines whether a node is included in the pool of nodes from which quorum is derived. You need at least one node as a quorum node.
- **Manager Node.** Indicates whether a node is part of the node pool from which file system managers and token managers can be selected. It is a good idea to define more than one node as a manager node. How many nodes you designate as manager depends on the workload and the number of GPFS server licenses you have. If you are running large parallel jobs, you might need more manager nodes than in a four-node cluster supporting a web application.
- **NSD Server.** The server that prepares each physical disk for use with GPFS.
- **Protocol node.** The node that shares GPFS data directly through any Secure Shell (SSH) protocol with the NFS. This node requires a GPFS server license.

## List of operations for GPFS, NFS, and XCP

This section provides the list of operations that create GPFS, export GPFS as an NFS export, and transfer the data by using XCP.

### Create GPFS

To create GPFS, complete the following steps:

1. Download and install spectrum-scale data access for the Linux version on one of the servers.
2. Install the prerequisite package (chef for example) in all nodes and disable Security-Enhanced Linux (SELinux) in all nodes.
3. Set up the install node and add the admin node and the GPFS node to the cluster definition file.
4. Add the manager node, the quorum node, the NSD servers, and the GPFS node.
5. Add the GUI, admin, and GPFS nodes, and add an additional GUI server if required.
6. Add another GPFS node and check the list of all nodes.
7. Specify a cluster name, profile, remote shell binary, remote file copy binary, and port range to be set on all the GPFS nodes in the cluster definition file.
8. View the GPFS configuration settings and add an additional admin node.
9. Disable the data collection and upload the data package to the IBM Support Center.
10. Enable NTP and precheck the configurations before install.
11. Configure, create, and check the NSD disks.
12. Create the GPFS.
13. Mount the GPFS.
14. Verify and provide the required permissions to the GPFS.
15. Verify the GPFS read and write by running the `dd` command.

## Export GPFS into NFS

To export the GPFS into NFS, complete the following steps:

1. Export GPFS as NFS through the `/etc/exports` file.
2. Install the required NFS server packages.
3. Start the NFS service.
4. List the files in the GPFS to validate the NFS client.

## Configure NFS client

To configure the NFS client, complete the following steps:

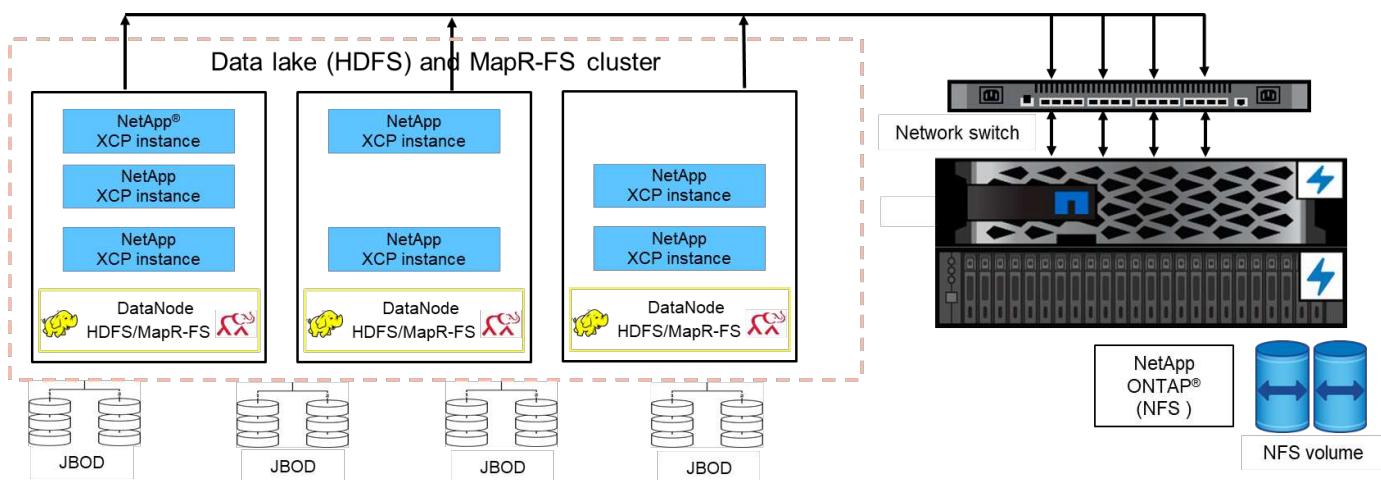
1. Export the GPFS as NFS through the `/etc/exports` file.
2. Start the NFS client services.
3. Mount the GPFS through the NFS protocol on the NFS client.
4. Validate the list of GPFS files in the NFS mounted folder.
5. Move the data from GPFS exported NFS to NetApp NFS by using XCP.
6. Validate the GPFS files on the NFS client.

[Next: HDFS and MapR-FS to ONTAP NFS.](#)

## HDFS and MapR-FS to ONTAP NFS

[Previous: GPFS to NetApp ONTAP NFS.](#)

For this solution, NetApp validated the migration of data from data lake (HDFS) and MapR cluster data to ONTAP NFS. The data resided in MapR-FS and HDFS. NetApp XCP introduced a new feature that directly migrates the data from a distributed file system such as HDFS and MapR-FS to ONTAP NFS. XCP uses async threads and HDFS C API calls to communicate and transfer data from MapR-FS as well as HDFS. The below figure shows the data migration from data lake (HDFS) and MapR-FS to ONTAP NFS. With this new feature, you don't have to export the source as an NFS share.



## Why are customers moving from HDFS and MapR-FS to NFS?

Most of the Hadoop distributions such as Cloudera and Hortonworks use HDFS and MapR distributions uses their own filesystem called Mapr-FS to store data. HDFS and MapR-FS data provides the valuable insights to data scientists that can be leveraged in machine learning (ML) and deep learning (DL). The data in HDFS and MapR-FS is not shared, which means it cannot be used by other applications. Customers are looking for shared data, specifically in the banking sector where customers' sensitive data is used by multiple applications. The latest version of Hadoop (3.x or later) supports NFS data source, which can be accessed without additional third-party software. With the new NetApp XCP feature, data can be moved directly from HDFS and MapR-FS to NetApp NFS in order to provide access to multiple applications

Testing was done in Amazon Web Services (AWS) to transfer the data from MapR-FS to NFS for the initial performance test with 12 MAPR nodes and 4 NFS servers.

	Quantity	Size	vCPU	Memory	Storage	Network
NFS server	4	i3en.24xlarge	96	488GiB	8x 7500 NVMe SSD	100
MapR nodes	12	I3en.12xlarge	48	384GiB	4x 7500 NVMe SSD	50

Based on initial testing, we obtained 20GBps throughput and were able to transfer 2PB per day of data.

For more information about HDFS data migration without exporting HDFS to NFS, see the “Deployment steps - NAS” section in [TR-4863: Best-Practice Guidelines for NetApp XCP - Data Mover, File Migration, and Analytics](#).

[Next: Business benefits.](#)

## Business benefits

[Previous: HDFS and MapR-FS to ONTAP NFS.](#)

Moving data from big data analytics to AI provides the following benefits:

- The ability to extract data from different Hadoop file systems and GPFS into a unified NFS storage system
- A Hadoop-integrated and automated way to transfer data
- A reduction in the cost of library development for moving data from Hadoop file systems
- Maximum performance by aggregated throughput of multiple network interfaces from a single source of data by using NIPAM
- Scheduled and on-demand methods to transfer data
- Storage efficiency and enterprise management capability for unified NFS data by using ONTAP data management software
- Zero cost for data movement with the Hadoop method for data transfer

[Next: GPFS to NFS-Detailed steps.](#)

## GPFS to NFS-Detailed steps

[Previous: Business benefits.](#)

This section provides the detailed steps needed to configure GPFS and move data into NFS by using NetApp XCP.

## Configure GPFS

1. Download and Install Spectrum Scale Data Access for Linux on one of the servers.

```
[root@mastr-51 Spectrum_Scale_Data_Access-5.0.3.1-x86_64-Linux-
install_folder]# ls
Spectrum_Scale_Data_Access-5.0.3.1-x86_64-Linux-install
[root@mastr-51 Spectrum_Scale_Data_Access-5.0.3.1-x86_64-Linux-
install_folder]# chmod +x Spectrum_Scale_Data_Access-5.0.3.1-x86_64-
Linux-install
[root@mastr-51 Spectrum_Scale_Data_Access-5.0.3.1-x86_64-Linux-
install_folder]# ./Spectrum_Scale_Data_Access-5.0.3.1-x86_64-Linux-
install --manifest
manifest
...
<contents removes to save page space>
...
```

2. Install the prerequisite package (including chef and the kernel headers) on all nodes.

```
[root@mastr-51 5.0.3.1]# for i in 51 53 136 138 140 ; do ssh
10.63.150.$i "hostname; rpm -ivh /gpfs_install/chef* "; done
mastr-51.netapp.com
warning: /gpfs_install/chef-13.6.4-1.el7.x86_64.rpm: Header V4 DSA/SHA1
Signature, key ID 83ef826a: NOKEY
Preparing...
#####
package chef-13.6.4-1.el7.x86_64 is already installed
mastr-53.netapp.com
warning: /gpfs_install/chef-13.6.4-1.el7.x86_64.rpm: Header V4 DSA/SHA1
Signature, key ID 83ef826a: NOKEY
Preparing...
#####
Updating / installing...
chef-13.6.4-1.el7
#####
Thank you for installing Chef!
workr-136.netapp.com
warning: /gpfs_install/chef-13.6.4-1.el7.x86_64.rpm: Header V4 DSA/SHA1
Signature, key ID 83ef826a: NOKEY
Preparing...
#####
Updating / installing...
```

```
chef-13.6.4-1.el7
#####
Thank you for installing Chef!
workr-138.netapp.com
warning: /gpfs_install/chef-13.6.4-1.el7.x86_64.rpm: Header V4 DSA/SHA1
Signature, key ID 83ef826a: NOKEY
Preparing...
#####
Updating / installing...
chef-13.6.4-1.el7
#####
Thank you for installing Chef!
workr-140.netapp.com
warning: /gpfs_install/chef-13.6.4-1.el7.x86_64.rpm: Header V4 DSA/SHA1
Signature, key ID 83ef826a: NOKEY
Preparing...
#####
Updating / installing...
chef-13.6.4-1.el7
#####
Thank you for installing Chef!
[root@mastr-51 5.0.3.1]#
[root@mastr-51 installer]# for i in 51 53 136 138 140 ; do ssh
10.63.150.$i "hostname; yumdownloader kernel-headers-3.10.0-
862.3.2.el7.x86_64 ; rpm -Uvh --oldpackage kernel-headers-3.10.0-
862.3.2.el7.x86_64.rpm"; done
mastr-51.netapp.com
Loaded plugins: priorities, product-id, subscription-manager
Preparing...
#####
Updating / installing...
kernel-headers-3.10.0-862.3.2.el7
#####
Cleaning up / removing...
kernel-headers-3.10.0-957.21.2.el7
#####
mastr-53.netapp.com
Loaded plugins: product-id, subscription-manager
Preparing...
#####
Updating / installing...
kernel-headers-3.10.0-862.3.2.el7
#####
Cleaning up / removing...
kernel-headers-3.10.0-862.11.6.el7
#####
```

```

workr-136.netapp.com
Loaded plugins: product-id, subscription-manager
Repository ambari-2.7.3.0 is listed more than once in the configuration
Preparing...
#####
Updating / installing...
kernel-headers-3.10.0-862.3.2.el7
#####
Cleaning up / removing...
kernel-headers-3.10.0-862.11.6.el7
#####
workr-138.netapp.com
Loaded plugins: product-id, subscription-manager
Preparing...
#####
package kernel-headers-3.10.0-862.3.2.el7.x86_64 is already installed
workr-140.netapp.com
Loaded plugins: product-id, subscription-manager
Preparing...
#####
Updating / installing...
kernel-headers-3.10.0-862.3.2.el7
#####
Cleaning up / removing...
kernel-headers-3.10.0-862.11.6.el7
#####
[root@mastr-51 installer]#

```

### 3. Disable SELinux in all nodes.

```

[root@mastr-51 5.0.3.1]# for i in 51 53 136 138 140 ; do ssh
10.63.150.$i "hostname; sudo setenforce 0"; done
mastr-51.netapp.com
setenforce: SELinux is disabled
mastr-53.netapp.com
setenforce: SELinux is disabled
workr-136.netapp.com
setenforce: SELinux is disabled
workr-138.netapp.com
setenforce: SELinux is disabled
workr-140.netapp.com
setenforce: SELinux is disabled
[root@mastr-51 5.0.3.1]#

```

### 4. Set up the install node.

```
[root@mastr-51 installer]# ./spectrumscale setup -s 10.63.150.51
[ INFO ] Installing prerequisites for install node
[ INFO ] Existing Chef installation detected. Ensure the PATH is
configured so that chef-client and knife commands can be run.
[ INFO ] Your control node has been configured to use the IP
10.63.150.51 to communicate with other nodes.
[ INFO ] Port 8889 will be used for chef communication.
[ INFO ] Port 10080 will be used for package distribution.
[ INFO ] Install Toolkit setup type is set to Spectrum Scale (default).
If an ESS is in the cluster, run this command to set ESS mode:
./spectrumscale setup -s server_ip -st ess
[ INFO ] SUCCESS
[ INFO ] Tip : Designate protocol, nsd and admin nodes in your
environment to use during install:./spectrumscale -v node add <node> -p
-a -n
[root@mastr-51 installer]#
```

5. Add the admin node and the GPFS node to the cluster definition file.

```
[root@mastr-51 installer]# ./spectrumscale node add mastr-51 -a
[ INFO ] Adding node mastr-51.netapp.com as a GPFS node.
[ INFO ] Setting mastr-51.netapp.com as an admin node.
[ INFO ] Configuration updated.
[ INFO ] Tip : Designate protocol or nsd nodes in your environment to
use during install:./spectrumscale node add <node> -p -n
[root@mastr-51 installer]#
```

6. Add the manager node and the GPFS node.

```
[root@mastr-51 installer]# ./spectrumscale node add mastr-53 -m
[ INFO ] Adding node mastr-53.netapp.com as a GPFS node.
[ INFO ] Adding node mastr-53.netapp.com as a manager node.
[root@mastr-51 installer]#
```

7. Add the quorum node and the GPFS node.

```
[root@mastr-51 installer]# ./spectrumscale node add workr-136 -q
[ INFO ] Adding node workr-136.netapp.com as a GPFS node.
[ INFO ] Adding node workr-136.netapp.com as a quorum node.
[root@mastr-51 installer]#
```

8. Add the NSD servers and the GPFS node.

```
[root@mastr-51 installer]# ./spectrumscale node add workr-138 -n
[ INFO ] Adding node workr-138.netapp.com as a GPFS node.
[ INFO ] Adding node workr-138.netapp.com as an NSD server.
[ INFO ] Configuration updated.
[ INFO ] Tip :If all node designations are complete, add NSDs to your
cluster definition and define required filessytems:./spectrumscale nsd
add <device> -p <primary node> -s <secondary node> -fs <file system>
[root@mastr-51 installer]#
```

9. Add the GUI, admin, and GPFS nodes.

```
[root@mastr-51 installer]# ./spectrumscale node add workr-136 -g
[ INFO ] Setting workr-136.netapp.com as a GUI server.
[root@mastr-51 installer]# ./spectrumscale node add workr-136 -a
[ INFO ] Setting workr-136.netapp.com as an admin node.
[ INFO ] Configuration updated.
[ INFO ] Tip : Designate protocol or nsd nodes in your environment to
use during install:./spectrumscale node add <node> -p -n
[root@mastr-51 installer]#
```

10. Add another GUI server.

```
[root@mastr-51 installer]# ./spectrumscale node add mastr-53 -g
[ INFO ] Setting mastr-53.netapp.com as a GUI server.
[root@mastr-51 installer]#
```

11. Add another GPFS node.

```
[root@mastr-51 installer]# ./spectrumscale node add workr-140
[ INFO ] Adding node workr-140.netapp.com as a GPFS node.
[root@mastr-51 installer]#
```

12. Verify and list all nodes.

```
[root@mastr-51 installer]# ./spectrumscale node list
[ INFO ] List of nodes in current configuration:
[ INFO ] [Installer Node]
[ INFO ] 10.63.150.51
[ INFO ]
[ INFO ] [Cluster Details]
[ INFO ] No cluster name configured
[ INFO ] Setup Type: Spectrum Scale
[ INFO ]
[ INFO ] [Extended Features]
[ INFO ] File Audit logging : Disabled
[ INFO ] Watch folder : Disabled
[ INFO ] Management GUI : Enabled
[ INFO ] Performance Monitoring : Disabled
[ INFO ] Callhome : Enabled
[ INFO ]
[ INFO ] GPFS Admin Quorum Manager NSD Protocol
GUI Callhome OS Arch
[ INFO ] Node Node Node Server Node
Server Server
[ INFO ] mastr-51.netapp.com X
rhel7 x86_64
[ INFO ] mastr-53.netapp.com X
X rhel7 x86_64
[ INFO ] workr-136.netapp.com X X
X rhel7 x86_64
[ INFO ] workr-138.netapp.com X
rhel7 x86_64
[ INFO ] workr-140.netapp.com
rhel7 x86_64
[ INFO ]
[ INFO ] [Export IP address]
[ INFO ] No export IP addresses configured
[root@mastr-51 installer]#
```

13. Specify a cluster name in the cluster definition file.

```
[root@mastr-51 installer]# ./spectrumscale config gpfs -c mastr-
51.netapp.com
[ INFO ] Setting GPFS cluster name to mastr-51.netapp.com
[root@mastr-51 installer]#
```

14. Specify the profile.

```
[root@mastr-51 installer]# ./spectrumscale config gpfs -p default
[ INFO ] Setting GPFS profile to default
[root@mastr-51 installer]#
Profiles options: default [gpfsProtocolDefaults], random I/O
[gpfsProtocolsRandomIO], sequential I/O [gpfsProtocolDefaults], random
I/O [gpfsProtocolRandomIO]
```

15. Specify the remote shell binary to be used by GPFS; use `-r` argument.

```
[root@mastr-51 installer]# ./spectrumscale config gpfs -r /usr/bin/ssh
[ INFO ] Setting Remote shell command to /usr/bin/ssh
[root@mastr-51 installer]#
```

16. Specify the remote file copy binary to be used by GPFS; use `-rc` argument.

```
[root@mastr-51 installer]# ./spectrumscale config gpfs -rc /usr/bin/scp
[ INFO ] Setting Remote file copy command to /usr/bin/scp
[root@mastr-51 installer]#
```

17. Specify the port range to be set on all GPFS nodes; use `-e` argument.

```
[root@mastr-51 installer]# ./spectrumscale config gpfs -e 60000-65000
[ INFO ] Setting GPFS Daemon communication port range to 60000-65000
[root@mastr-51 installer]#
```

18. View the GPFS config settings.

```
[root@mastr-51 installer]# ./spectrumscale config gpfs --list
[ INFO ] Current settings are as follows:
[ INFO ] GPFS cluster name is mastr-51.netapp.com.
[ INFO ] GPFS profile is default.
[ INFO ] Remote shell command is /usr/bin/ssh.
[ INFO ] Remote file copy command is /usr/bin/scp.
[ INFO ] GPFS Daemon communication port range is 60000-65000.
[root@mastr-51 installer]#
```

19. Add an admin node.

```
[root@mastr-51 installer]# ./spectrumscale node add 10.63.150.53 -a
[ INFO ] Setting mastr-53.netapp.com as an admin node.
[ INFO ] Configuration updated.
[ INFO ] Tip : Designate protocol or nsd nodes in your environment to
use during install:./spectrumscale node add <node> -p -n
[root@mastr-51 installer]#
```

20. Disable the data collection and upload the data package to the IBM Support Center.

```
[root@mastr-51 installer]# ./spectrumscale callhome disable
[ INFO ] Disabling the callhome.
[ INFO ] Configuration updated.
[root@mastr-51 installer]#
```

21. Enable NTP.

```
[root@mastr-51 installer]# ./spectrumscale config ntp -e on
[root@mastr-51 installer]# ./spectrumscale config ntp -l
[ INFO ] Current settings are as follows:
[ WARN ] No value for Upstream NTP Servers(comma separated IP's with NO
space between multiple IPs) in clusterdefinition file.
[root@mastr-51 installer]# ./spectrumscale config ntp -s 10.63.150.51
[ WARN ] The NTP package must already be installed and full
bidirectional access to the UDP port 123 must be allowed.
[ WARN ] If NTP is already running on any of your nodes, NTP setup will
be skipped. To stop NTP run 'service ntpd stop'.
[ WARN ] NTP is already on
[ INFO ] Setting Upstream NTP Servers(comma separated IP's with NO
space between multiple IPs) to 10.63.150.51
[root@mastr-51 installer]# ./spectrumscale config ntp -e on
[ WARN ] NTP is already on
[root@mastr-51 installer]# ./spectrumscale config ntp -l
[ INFO ] Current settings are as follows:
[ INFO ] Upstream NTP Servers(comma separated IP's with NO space
between multiple IPs) is 10.63.150.51.
[root@mastr-51 installer]#
[root@mastr-51 installer]# service ntpd start
Redirecting to /bin/systemctl start ntpd.service
[root@mastr-51 installer]# service ntpd status
Redirecting to /bin/systemctl status ntpd.service
● ntpd.service - Network Time Service
    Loaded: loaded (/usr/lib/systemd/system/ntp.service; enabled; vendor
    preset: disabled)
```

```
Active: active (running) since Tue 2019-09-10 14:20:34 UTC; 1s ago
  Process: 2964 ExecStart=/usr/sbin/ntpd -u ntp:ntp $OPTIONS
  (code=exited, status=0/SUCCESS)
 Main PID: 2965 (ntpd)
    CGroup: /system.slice/ntpd.service
              └─2965 /usr/sbin/ntpd -u ntp:ntp -g

Sep 10 14:20:34 mastr-51.netapp.com ntpd[2965]: ntp_io: estimated max
descriptors: 1024, initial socket boundary: 16
Sep 10 14:20:34 mastr-51.netapp.com ntpd[2965]: Listen and drop on 0
v4wildcard 0.0.0.0 UDP 123
Sep 10 14:20:34 mastr-51.netapp.com ntpd[2965]: Listen and drop on 1
v6wildcard :: UDP 123
Sep 10 14:20:34 mastr-51.netapp.com ntpd[2965]: Listen normally on 2 lo
127.0.0.1 UDP 123
Sep 10 14:20:34 mastr-51.netapp.com ntpd[2965]: Listen normally on 3
enp4s0f0 10.63.150.51 UDP 123
Sep 10 14:20:34 mastr-51.netapp.com ntpd[2965]: Listen normally on 4 lo
::1 UDP 123
Sep 10 14:20:34 mastr-51.netapp.com ntpd[2965]: Listen normally on 5
enp4s0f0 fe80::219:99ff:feef:99fa UDP 123
Sep 10 14:20:34 mastr-51.netapp.com ntpd[2965]: Listening on routing
socket on fd #22 for interface updates
Sep 10 14:20:34 mastr-51.netapp.com ntpd[2965]: 0.0.0.0 c016 06 restart
Sep 10 14:20:34 mastr-51.netapp.com ntpd[2965]: 0.0.0.0 c012 02 freq_set
kernel 11.890 PPM
[root@mastr-51 installer]#
```

## 22. Precheck the configurations before Install.

```
[root@mastr-51 installer]# ./spectrumscale install -pr
[ INFO ] Logging to file: /usr/lpp/mmfs/5.0.3.1/installer/logs/INSTALL-
PRECHECK-10-09-2019_14:51:43.log
[ INFO ] Validating configuration
[ INFO ] Performing Chef (deploy tool) checks.
[ WARN ] NTP is already running on: mastr-51.netapp.com. The install
toolkit will no longer setup NTP.
[ INFO ] Node(s): ['workr-138.netapp.com'] were defined as NSD node(s)
but the toolkit has not been told about any NSDs served by these node(s)
nor has the toolkit been told to create new NSDs on these node(s). The
install will continue and these nodes will be assigned server licenses.
If NSDs are desired, either add them to the toolkit with
<./spectrumscale nsd add> followed by a <./spectrumscale install> or add
them manually afterwards using mmcrnsd.
[ INFO ] Install toolkit will not configure file audit logging as it
has been disabled.
[ INFO ] Install toolkit will not configure watch folder as it has been
disabled.
[ INFO ] Checking for knife bootstrap configuration...
[ INFO ] Performing GPFS checks.
[ INFO ] Running environment checks
[ INFO ] Skipping license validation as no existing GPFS cluster
detected.
[ INFO ] Checking pre-requisites for portability layer.
[ INFO ] GPFS precheck OK
[ INFO ] Performing Performance Monitoring checks.
[ INFO ] Running environment checks for Performance Monitoring
[ INFO ] Performing GUI checks.
[ INFO ] Performing FILE AUDIT LOGGING checks.
[ INFO ] Running environment checks for file Audit logging
[ INFO ] Network check from admin node workr-136.netapp.com to all
other nodes in the cluster passed
[ INFO ] Network check from admin node mastr-51.netapp.com to all other
nodes in the cluster passed
[ INFO ] Network check from admin node mastr-53.netapp.com to all other
nodes in the cluster passed
[ INFO ] The install toolkit will not configure call home as it is
disabled. To enable call home, use the following CLI command:
./spectrumscale callhome enable
[ INFO ] Pre-check successful for install.
[ INFO ] Tip : ./spectrumscale install
[root@mastr-51 installer]#
```

## 23. Configure the NSD disks.

```
[root@mastr-51 cluster-test]# cat disk.1st
%nsd: device=/dev/sdf
nsd=nsd1
servers=workr-136
usage=dataAndMetadata
failureGroup=1

%nsd: device=/dev/sdf
nsd=nsd2
servers=workr-138
usage=dataAndMetadata
failureGroup=1
```

24. Create the NSD disks.

```
[root@mastr-51 cluster-test]# mmcrnsd -F disk.1st -v no
mmcrnsd: Processing disk sdf
mmcrnsd: Processing disk sdf
mmcrnsd: Propagating the cluster configuration data to all
affected nodes. This is an asynchronous process.
[root@mastr-51 cluster-test]#
```

25. Check the NSD disk status.

```
[root@mastr-51 cluster-test]# mmlsnsd

File system      Disk name      NSD servers
-----
---
(free disk)    nsd1          workr-136.netapp.com
(free disk)    nsd2          workr-138.netapp.com

[root@mastr-51 cluster-test]#
```

26. Create the GPFS.

```
[root@mastr-51 cluster-test]# mmcrfs gpfs1 -F disk.1st -B 1M -T /gpfs1  
  
The following disks of gpfs1 will be formatted on node workr-  
136.netapp.com:  
    nsd1: size 3814912 MB  
    nsd2: size 3814912 MB  
Formatting file system ...  
Disks up to size 33.12 TB can be added to storage pool system.  
Creating Inode File  
Creating Allocation Maps  
Creating Log Files  
Clearing Inode Allocation Map  
Clearing Block Allocation Map  
Formatting Allocation Map for storage pool system  
Completed creation of file system /dev/gpfs1.  
mmcrfs: Propagating the cluster configuration data to all  
affected nodes. This is an asynchronous process.  
[root@mastr-51 cluster-test]#
```

## 27. Mount the GPFS.

```
[root@mastr-51 cluster-test]# mmmount all -a  
Tue Oct  8 18:05:34 UTC 2019: mmmount: Mounting file systems ...  
[root@mastr-51 cluster-test]#
```

## 28. Check and provide the required permissions to the GPFS.

```

[root@mastr-51 cluster-test]# mmlsdisk gpfs1
disk      driver   sector    failure holds    holds
storage
name       type     size      group metadata data  status
availability pool
-----
----- nsd1      nsd      512       1 Yes     Yes  ready   up
system
nsd2      nsd      512       1 Yes     Yes  ready   up
system
[root@mastr-51 cluster-test]#
[root@mastr-51 cluster-test]# for i in 51 53 136 138 ; do ssh
10.63.150.$i "hostname; chmod 777 /gpfs1" ; done;
mastr-51.netapp.com
mastr-53.netapp.com
workr-136.netapp.com
workr-138.netapp.com
[root@mastr-51 cluster-test]#

```

29. Check the GPFS read and write by running the dd command.

```

[root@mastr-51 cluster-test]# dd if=/dev/zero of=/gpfs1/testfile
bs=1024M count=5
5+0 records in
5+0 records out
5368709120 bytes (5.4 GB) copied, 8.3981 s, 639 MB/s
[root@mastr-51 cluster-test]# for i in 51 53 136 138 ; do ssh
10.63.150.$i "hostname; ls -ltrh /gpfs1" ; done;
mastr-51.netapp.com
total 5.0G
-rw-r--r-- 1 root root 5.0G Oct  8 18:10 testfile
mastr-53.netapp.com
total 5.0G
-rw-r--r-- 1 root root 5.0G Oct  8 18:10 testfile
workr-136.netapp.com
total 5.0G
-rw-r--r-- 1 root root 5.0G Oct  8 18:10 testfile
workr-138.netapp.com
total 5.0G
-rw-r--r-- 1 root root 5.0G Oct  8 18:10 testfile
[root@mastr-51 cluster-test]#

```

## Export GPFS into NFS

To export GPFS into NFS, complete the following steps:

1. Export the GPFS as NFS through the /etc/exports file.

```
[root@mastr-51 gpfsl]# cat /etc/exports  
/gpfsl          *(rw,fsid=745)  
[root@mastr-51 gpfsl]
```

- ## 2. Install the required NFS server packages.

```
[root@mastr-51 ~]# yum install rpcbind
Loaded plugins: priorities, product-id, search-disabled-repos,
subscription-manager
Resolving Dependencies
--> Running transaction check
---> Package rpcbind.x86_64 0:0.2.0-47.el7 will be updated
---> Package rpcbind.x86_64 0:0.2.0-48.el7 will be an update
--> Finished Dependency Resolution
```

## Dependencies Resolved

## Transaction Summary

Wavelength Dependence

```
Total download size: 60 k
Is this ok [y/d/N]: y
Downloading packages:
No Presto metadata available for rhel-7-server-rpms
rpcbind-0.2.0-48.el7.x86_64.rpm
| 60 kB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Updating    : rpcbind-0.2.0-48.el7.x86_64
1/2
  Cleanup      : rpcbind-0.2.0-47.el7.x86_64
2/2
  Verifying    : rpcbind-0.2.0-48.el7.x86_64
1/2
  Verifying    : rpcbind-0.2.0-47.el7.x86_64
2/2

Updated:
  rpcbind.x86_64 0:0.2.0-48.el7

Complete!
[root@mastr-51 ~] #
```

### 3. Start the NFS service.

```

[root@mastr-51 ~]# service nfs status
Redirecting to /bin/systemctl status nfs.service
● nfs-server.service - NFS server and services
  Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; disabled;
  vendor preset: disabled)
  Drop-In: /run/systemd/generator/nfs-server.service.d
            └─order-with-mounts.conf

    Active: inactive (dead)

[root@mastr-51 ~]# service rpcbind start
Redirecting to /bin/systemctl start rpcbind.service
[root@mastr-51 ~]# service nfs start
Redirecting to /bin/systemctl start nfs.service
[root@mastr-51 ~]# service nfs status
Redirecting to /bin/systemctl status nfs.service
● nfs-server.service - NFS server and services
  Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; disabled;
  vendor preset: disabled)
  Drop-In: /run/systemd/generator/nfs-server.service.d
            └─order-with-mounts.conf

    Active: active (exited) since Wed 2019-11-06 16:34:50 UTC; 2s ago
      Process: 24402 ExecStartPost=/bin/sh -c if systemctl -q is-active
      gssproxy; then systemctl reload gssproxy ; fi (code=exited,
      status=0/SUCCESS)
      Process: 24383 ExecStart=/usr/sbin/rpc.nfsd $RPCNFSDARGS (code=exited,
      status=0/SUCCESS)
      Process: 24379 ExecStartPre=/usr/sbin/exportfs -r (code=exited,
      status=0/SUCCESS)
      Main PID: 24383 (code=exited, status=0/SUCCESS)
      CGroup: /system.slice/nfs-server.service

Nov 06 16:34:50 mastr-51.netapp.com systemd[1]: Starting NFS server and
services...
Nov 06 16:34:50 mastr-51.netapp.com systemd[1]: Started NFS server and
services.
[root@mastr-51 ~]#

```

4. List the files in GPFS to validate the NFS client.

```

[root@mastr-51 gpfs1]# df -Th
Filesystem                          Type  Size  Used Avail
Use% Mounted on
/dev/mapper/rhel_stlx300s6--22--irmc-root xfs   94G  55G  39G
59% /
devtmpfs                           devtmpfs 32G   0    32G
0% /dev
tmpfs                             tmpfs   32G   0    32G
0% /dev/shm
tmpfs                           tmpfs   32G  3.3G  29G
11% /run
tmpfs                           tmpfs   32G   0    32G
0% /sys/fs/cgroup
/dev/sda7                           xfs   9.4G 210M 9.1G
3% /boot
tmpfs                           tmpfs   6.3G   0   6.3G
0% /run/user/10065
tmpfs                           tmpfs   6.3G   0   6.3G
0% /run/user/10068
tmpfs                           tmpfs   6.3G   0   6.3G
0% /run/user/10069
10.63.150.213:/nc_volume3      nfs4  380G  8.0M 380G
1% /mnt
tmpfs                           tmpfs   6.3G   0   6.3G
0% /run/user/0
gpfs1                            gpfs   7.3T  9.1G  7.3T
1% /gpfs1
[root@mastr-51 gpfs1]#
[root@mastr-51 ~]# cd /gpfs1
[root@mastr-51 gpfs1]# ls
catalog ces gpfs-ces ha testfile
[root@mastr-51 gpfs1]#
[root@mastr-51 ~]# cd /gpfs1
[root@mastr-51 gpfs1]# ls
ces gpfs-ces ha testfile
[root@mastr-51 gpfs1]# ls -ltrha
total 5.1G
dr-xr-xr-x  2 root root 8.0K Jan  1 1970 .snapshots
-rw-r--r--  1 root root 5.0G Oct  8 18:10 testfile
dr-xr-xr-x. 30 root root 4.0K Oct  8 18:19 ..
drwxr-xr-x  2 root root 4.0K Nov  5 20:02 gpfs-ces
drwxr-xr-x  2 root root 4.0K Nov  5 20:04 ha
drwxrwxrwx  5 root root 256K Nov  5 20:04 .
drwxr-xr-x  4 root root 4.0K Nov  5 20:35 ces
[root@mastr-51 gpfs1]#

```

## Configure the NFS client

To configure the NFS client, complete the following steps:

1. Install packages in the NFS client.

```
[root@hdp2 ~]# yum install nfs-utils rpcbind
Loaded plugins: product-id, search-disabled-repos, subscription-manager
HDP-2.6-GPL-repo-4
| 2.9 kB 00:00:00
HDP-2.6-repo-4
| 2.9 kB 00:00:00
HDP-3.0-GPL-repo-2
| 2.9 kB 00:00:00
HDP-3.0-repo-2
| 2.9 kB 00:00:00
HDP-3.0-repo-3
| 2.9 kB 00:00:00
HDP-3.1-repo-1
| 2.9 kB 00:00:00
HDP-3.1-repo-51
| 2.9 kB 00:00:00
HDP-UTILS-1.1.0.22-repo-1
| 2.9 kB 00:00:00
HDP-UTILS-1.1.0.22-repo-2
| 2.9 kB 00:00:00
HDP-UTILS-1.1.0.22-repo-3
| 2.9 kB 00:00:00
HDP-UTILS-1.1.0.22-repo-4
| 2.9 kB 00:00:00
HDP-UTILS-1.1.0.22-repo-51
| 2.9 kB 00:00:00
ambari-2.7.3.0
| 2.9 kB 00:00:00
epel/x86_64/metalink
| 13 kB 00:00:00
epel
| 5.3 kB 00:00:00
mysql-connectors-community
| 2.5 kB 00:00:00
mysql-tools-community
| 2.5 kB 00:00:00
mysql56-community
| 2.5 kB 00:00:00
rhel-7-server-optional-rpms
| 3.2 kB 00:00:00
rhel-7-server-rpms
```

```
| 3.5 kB 00:00:00  
(1/10): mysql-connectors-community/x86_64/primary_db  
| 49 kB 00:00:00  
(2/10): mysql-tools-community/x86_64/primary_db  
| 66 kB 00:00:00  
(3/10): epel/x86_64/group_gz  
| 90 kB 00:00:00  
(4/10): mysql56-community/x86_64/primary_db  
| 241 kB 00:00:00  
(5/10): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo  
| 2.5 MB 00:00:00  
(6/10): rhel-7-server-rpms/7Server/x86_64/updateinfo  
| 3.4 MB 00:00:00  
(7/10): rhel-7-server-optional-rpms/7Server/x86_64/primary_db  
| 8.3 MB 00:00:00  
(8/10): rhel-7-server-rpms/7Server/x86_64/primary_db  
| 62 MB 00:00:01  
(9/10): epel/x86_64/primary_db  
| 6.9 MB 00:00:08  
(10/10): epel/x86_64/updateinfo  
| 1.0 MB 00:00:13
```

#### Resolving Dependencies

```
--> Running transaction check  
---> Package nfs-utils.x86_64 1:1.3.0-0.61.el7 will be updated  
---> Package nfs-utils.x86_64 1:1.3.0-0.65.el7 will be an update  
---> Package rpcbind.x86_64 0:0.2.0-47.el7 will be updated  
---> Package rpcbind.x86_64 0:0.2.0-48.el7 will be an update  
---> Finished Dependency Resolution
```

#### Dependencies Resolved

```
=====  
=====  


| Package Repository | Arch   | Version          |
|--------------------|--------|------------------|
|                    |        | Size             |
| =====              |        |                  |
| =====              |        |                  |
| Updating:          |        |                  |
| nfs-utils          | x86_64 | 1:1.3.0-0.65.el7 |
| rhel-7-server-rpms |        | 412 k            |
| rpcbind            | x86_64 | 0.2.0-48.el7     |
| rhel-7-server-rpms |        | 60 k             |



```
=====  
=====
```


```

#### Transaction Summary

```
=====  
=====
```

```
Upgrade 2 Packages
```

```
Total download size: 472 k
Is this ok [y/d/N]: y
Downloading packages:
No Presto metadata available for rhel-7-server-rpms
(1/2): rpcbind-0.2.0-48.el7.x86_64.rpm
| 60 kB 00:00:00
(2/2): nfs-utils-1.3.0-0.65.el7.x86_64.rpm
| 412 kB 00:00:00
-----
-----
Total
1.2 MB/s | 472 kB 00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
    Updating : rpcbind-0.2.0-48.el7.x86_64
1/4
    service rpcbind start

    Updating : 1:nfs-utils-1.3.0-0.65.el7.x86_64
2/4
    Cleanup   : 1:nfs-utils-1.3.0-0.61.el7.x86_64
3/4
    Cleanup   : rpcbind-0.2.0-47.el7.x86_64
4/4
    Verifying : 1:nfs-utils-1.3.0-0.65.el7.x86_64
1/4
    Verifying : rpcbind-0.2.0-48.el7.x86_64
2/4
    Verifying : rpcbind-0.2.0-47.el7.x86_64
3/4
    Verifying : 1:nfs-utils-1.3.0-0.61.el7.x86_64
4/4

Updated:
nfs-utils.x86_64 1:1.3.0-0.65.el7
rpcbind.x86_64 0:0.2.0-48.el7

Complete!
[root@hdp2 ~]#
```

## 2. Start the NFS client services.

```
[root@hdp2 ~]# service rpcbind start
Redirecting to /bin/systemctl start rpcbind.service
[root@hdp2 ~]#
```

3. Mount the GPFS through the NFS protocol on the NFS client.

```
[root@hdp2 ~]# mkdir /gpfstest
[root@hdp2 ~]# mount 10.63.150.51:/gpfs1 /gpfstest
[root@hdp2 ~]# df -h
Filesystem                      Size  Used Avail Use% Mounted on
/dev/mapper/rhel_stlx300s6--22-root 1.1T  113G  981G  11% /
devtmpfs                         126G    0   126G   0% /dev
tmpfs                            126G   16K  126G   1% /dev/shm
tmpfs                            126G  510M  126G   1% /run
tmpfs                            126G    0   126G   0%
/sys/fs/cgroup
/dev/sdd2                          197M  191M   6.6M  97% /boot
tmpfs                            26G    0   26G   0% /run/user/0
10.63.150.213:/nc_volume2        95G   5.4G   90G   6% /mnt
10.63.150.51:/gpfs1              7.3T  9.1G  7.3T   1% /gpfstest
[root@hdp2 ~]#
```

4. Validate the list of GPFS files in the NFS-mounted folder.

```
[root@hdp2 ~]# cd /gpfstest/
[root@hdp2 gpfstest]# ls
ces  gpfs-ces  ha  testfile
[root@hdp2 gpfstest]# ls -l
total 5242882
drwxr-xr-x 4 root root      4096 Nov  5 15:35 ces
drwxr-xr-x 2 root root      4096 Nov  5 15:02 gpfs-ces
drwxr-xr-x 2 root root      4096 Nov  5 15:04 ha
-rw-r--r-- 1 root root 5368709120 Oct  8 14:10 testfile
[root@hdp2 gpfstest]#
```

5. Move the data from the GPFS- exported NFS to the NetApp NFS by using XCP.

```
[root@hdp2 linux]# ./xcp copy -parallel 20 10.63.150.51:/gpfs1  
10.63.150.213:/nc_volume2/  
XCP 1.4-17914d6; (c) 2019 NetApp, Inc.; Licensed to Karthikeyan  
Nagalingam [NetApp Inc] until Tue Nov 5 12:39:36 2019  
  
xcp: WARNING: your license will expire in less than one week! You can  
renew your license at https://xcp.netapp.com  
xcp: open or create catalog 'xcp': Creating new catalog in  
'10.63.150.51:/gpfs1/catalog'  
xcp: WARNING: No index name has been specified, creating one with name:  
autoname_copy_2019-11-11_12.14.07.805223  
xcp: mount '10.63.150.51:/gpfs1': WARNING: This NFS server only supports  
1-second timestamp granularity. This may cause sync to fail because  
changes will often be undetectable.  
 34 scanned, 32 copied, 32 indexed, 1 giant, 301 MiB in (59.5 MiB/s),  
784 KiB out (155 KiB/s), 6s  
 34 scanned, 32 copied, 32 indexed, 1 giant, 725 MiB in (84.6 MiB/s),  
1.77 MiB out (206 KiB/s), 11s  
 34 scanned, 32 copied, 32 indexed, 1 giant, 1.17 GiB in (94.2 MiB/s),  
2.90 MiB out (229 KiB/s), 16s  
 34 scanned, 32 copied, 32 indexed, 1 giant, 1.56 GiB in (79.8 MiB/s),  
3.85 MiB out (194 KiB/s), 21s  
 34 scanned, 32 copied, 32 indexed, 1 giant, 1.95 GiB in (78.4 MiB/s),  
4.80 MiB out (191 KiB/s), 26s  
 34 scanned, 32 copied, 32 indexed, 1 giant, 2.35 GiB in (80.4 MiB/s),  
5.77 MiB out (196 KiB/s), 31s  
 34 scanned, 32 copied, 32 indexed, 1 giant, 2.79 GiB in (89.6 MiB/s),  
6.84 MiB out (218 KiB/s), 36s  
 34 scanned, 32 copied, 32 indexed, 1 giant, 3.16 GiB in (75.3 MiB/s),  
7.73 MiB out (183 KiB/s), 41s  
 34 scanned, 32 copied, 32 indexed, 1 giant, 3.53 GiB in (75.4 MiB/s),  
8.64 MiB out (183 KiB/s), 46s  
 34 scanned, 32 copied, 32 indexed, 1 giant, 4.00 GiB in (94.4 MiB/s),  
9.77 MiB out (230 KiB/s), 51s  
 34 scanned, 32 copied, 32 indexed, 1 giant, 4.46 GiB in (94.3 MiB/s),  
10.9 MiB out (229 KiB/s), 56s  
 34 scanned, 32 copied, 32 indexed, 1 giant, 4.86 GiB in (80.2 MiB/s),  
11.9 MiB out (195 KiB/s), 1m1s  
Sending statistics...  
 34 scanned, 33 copied, 34 indexed, 1 giant, 5.01 GiB in (81.8 MiB/s),  
12.3 MiB out (201 KiB/s), 1m2s.  
[root@hdp2 linux]#
```

## 6. Validate the GPFS files on the NFS client.

```
[root@hdp2 mnt]# df -Th
Filesystem                                     Type      Size   Used  Avail Use%
Mounted on
/dev/mapper/rhel_stlx300s6--22-root          xfs       1.1T   113G  981G  11% /
devtmpfs                                      devtmpfs  126G     0  126G   0%
/dev
tmpfs                                         tmpfs    126G   16K  126G   1%
/dev/shm
tmpfs                                         tmpfs    126G  518M  126G   1%
/run
tmpfs                                         tmpfs    126G     0  126G   0%
/sys/fs/cgroup
/dev/sdd2                                       xfs     197M  191M  6.6M  97%
/boot
tmpfs                                         tmpfs    26G     0   26G   0%
/run/user/0
10.63.150.213:/nc_volume2                   nfs4     95G  5.4G  90G   6%
/mnt
10.63.150.51:/gpfs1                         nfs4    7.3T  9.1G  7.3T   1%
/gpfstest
[root@hdp2 mnt]#
[root@hdp2 mnt]# ls -ltrha
total 128K
dr-xr-xr-x  2 root      root          4.0K Dec 31 1969 .
.snapshots
drwxrwxrwx  2 root      root          4.0K Feb 14 2018 data
drwxrwxrwx  3 root      root          4.0K Feb 14 2018
wcresult
drwxrwxrwx  3 root      root          4.0K Feb 14 2018
wcresult1
drwxrwxrwx  2 root      root          4.0K Feb 14 2018
wcresult2
drwxrwxrwx  2 root      root          4.0K Feb 16 2018
wcresult3
-rw-r--r--  1 root      root         2.8K Feb 20 2018 READMEdemo
drwxrwxrwx  3 root      root          4.0K Jun 28 13:38 scantg
drwxrwxrwx  3 root      root          4.0K Jun 28 13:39
scancopyFromLocal
-rw-r--r--  1 hdfs     hadoop        1.2K Jul  3 19:28 f3
-rw-r--r--  1 hdfs     hadoop        1.2K Jul  3 19:28 README
-rw-r--r--  1 hdfs     hadoop        1.2K Jul  3 19:28 f9
-rw-r--r--  1 hdfs     hadoop        1.2K Jul  3 19:28 f6
-rw-r--r--  1 hdfs     hadoop        1.2K Jul  3 19:28 f5
-rw-r--r--  1 hdfs     hadoop        1.2K Jul  3 19:30 f4
-rw-r--r--  1 hdfs     hadoop        1.2K Jul  3 19:30 f8
```

```

-rw-r--r--  1 hdfs      hadoop          1.2K Jul  3 19:30 f2
-rw-r--r--  1 hdfs      hadoop          1.2K Jul  3 19:30 f7
drwxrwxrwx  2 root      root           4.0K Jul  9 11:14 test
drwxrwxrwx  3 root      root           4.0K Jul 10 16:35
warehouse
drwxr-xr-x  3         10061 tester1    4.0K Jul 15 14:40 sdd1
drwxrwxrwx  3 testeruser1 hadoopkerberosgroup 4.0K Aug 20 17:00
kermkdir
-rw-r--r--  1 testeruser1 hadoopkerberosgroup 0 Aug 21 14:20 newfile
drwxrwxrwx  2 testeruser1 hadoopkerberosgroup 4.0K Aug 22 10:13
teragen1copy_3
drwxrwxrwx  2 testeruser1 hadoopkerberosgroup 4.0K Aug 22 10:33
teragen2copy_1
-rw-rwxr--  1 root      hdfs           1.2K Sep 19 16:38 R1
drwx----- 3 root      root           4.0K Sep 20 17:28 user
-rw-r--r--  1 root      root           5.0G Oct  8 14:10
testfile
drwxr-xr-x  2 root      root           4.0K Nov  5 15:02 gpfs-
ces
drwxr-xr-x  2 root      root           4.0K Nov  5 15:04 ha
drwxr-xr-x  4 root      root           4.0K Nov  5 15:35 ces
dr-xr-xr-x. 26 root     root           4.0K Nov  6 11:40 ..
drwxrwxrwx  21 root     root           4.0K Nov 11 12:14 .
drwxrwxrwx  7 nobody   nobody         4.0K Nov 11 12:14 catalog
[root@hdp2 mnt]#

```

[Next: MapR-FS to ONTAP NFS.](#)

## MapR-FS to ONTAP NFS

[Previous: GPFS to NFS - Detailed steps.](#)

This section provides the detailed steps needed to move MapR-FS data into ONTAP NFS by using NetApp XCP.

1. Provision three LUNs for each MapR node and give the LUNs ownership of all MapR nodes.
2. During installation, choose newly added LUNs for MapR cluster disks that are used for MapR-FS.
3. Install a MapR cluster according to the [MapR 6.1 documentation](#).
4. Check the basic Hadoop operations using MapReduce commands such as `hadoop jar xxx`.
5. Keep customer data in MapR-FS. For example, we generated approximately a terabyte of sample data in MapR-FS by using Teragen.
6. Configure MapR-FS as NFS export.
  - a. Disable the nlockmgr service on all MapR nodes.

```

root@workr-138: ~$ rpcinfo -p
    program  vers  proto   port  service
  100000    4    tcp    111  portmapper
  100000    3    tcp    111  portmapper
  100000    2    tcp    111  portmapper
  100000    4    udp    111  portmapper
  100000    3    udp    111  portmapper
  100000    2    udp    111  portmapper
  100003    4    tcp    2049  nfs
  100227    3    tcp    2049  nfs_acl
  100003    4    udp    2049  nfs
  100227    3    udp    2049  nfs_acl
  100021    3    udp    55270  nlockmgr
  100021    4    udp    55270  nlockmgr
  100021    3    tcp    35025  nlockmgr
  100021    4    tcp    35025  nlockmgr
  100003    3    tcp    2049  nfs
  100005    3    tcp    2049  mountd
  100005    1    tcp    2049  mountd
  100005    3    udp    2049  mountd
  100005    1    udp    2049  mountd
root@workr-138: ~$

root@workr-138: ~$ rpcinfo -d 100021 3
root@workr-138: ~$ rpcinfo -d 100021 4

```

- b. Export specific folders from MapR-FS on all MapR nodes in the /opt/mapr/conf/exports file. Do not export the parent folder with different permissions when you export sub folders.

```

[mapr@workr-138 ~]$ cat /opt/mapr/conf/exports
# Sample Exports file
# for /mapr exports
# <Path> <exports_control>
#access_control -> order is specific to default
# list the hosts before specifying a default for all
# a.b.c.d,1.2.3.4(ro) d.e.f.g(ro) (rw)
# enforces ro for a.b.c.d & 1.2.3.4 and everybody else is rw
# special path to export clusters in mapr-clusters.conf. To disable
exporting,
# comment it out. to restrict access use the exports_control
#
#/mapr (rw)
#karthik
/mapr/my.cluster.com/tmp/testnfs /maprnfs3 (rw)
#to export only certain clusters, comment out the /mapr & uncomment.
#/mapr/clustername (rw)
#to export /mapr only to certain hosts (using exports_control)
#/mapr a.b.c.d(rw),e.f.g.h(ro)
# export /mapr/cluster1 rw to a.b.c.d & ro to e.f.g.h (denied for
others)
#/mapr/cluster1 a.b.c.d(rw),e.f.g.h(ro)
# export /mapr/cluster2 only to e.f.g.h (denied for others)
#/mapr/cluster2 e.f.g.h(rw)
# export /mapr/cluster3 rw to e.f.g.h & ro to others
#/mapr/cluster2 e.f.g.h(rw) (ro)
#to export a certain cluster, volume or a subdirectory as an alias,
#comment out /mapr & uncomment
#/mapr/clustername      /alias1 (rw)
#/mapr/clustername/vol   /alias2 (rw)
#/mapr/clustername/vol/dir /alias3 (rw)
#only the alias will be visible/exposed to the nfs client not the
mapr path, host options as before
[mapr@workr-138 ~]$

```

## 7. Refresh the MapR-FS NFS service.

```

root@workr-138: tmp$ maprcli nfsmgmt refreshexports
ERROR (22) - You do not have a ticket to communicate with
127.0.0.1:9998. Retry after obtaining a new ticket using maprlogin
root@workr-138: tmp$ su - mapr
[mapr@workr-138 ~]$ maprlogin password -cluster my.cluster.com
[Password for user 'mapr' at cluster 'my.cluster.com': ]
MapR credentials of user 'mapr' for cluster 'my.cluster.com' are written
to '/tmp/maprticket_5000'
[mapr@workr-138 ~]$ maprcli nfsmgmt refreshexports

```

8. Assign a virtual IP range to a specific server or a set of servers in the MapR cluster. Then the MapR cluster assigns an IP to a specific server for NFS data access. The IPs enable high availability, which means that, if a server or network with a particular IP experiences failure, the next IP from the range of IPs can be used for NFS access.



If you would like to provide NFS access from all MapR nodes, then you can assign a set of virtual IPs to each server, and you can use the resources from each MapR node for NFS data access.

VIP Range	Virtual IP	Node Name	Physical IP	MAC Address
10.63.150.92 - 10.63.150.93	(Pending)	--	--	--
10.63.150.96 - 10.63.150.97	10.63.150.96 10.63.150.97	workr-138.netapp.com workr-138.netapp.com	10.63.150.138 10.63.150.138	90:1b:0e:d1:5d:f9 90:1b:0e:d1:5d:f9

**SETTINGS AND AUDITING**

\* Starting Virtual IP: 10.63.150.96      \* NetMask: 255.255.255.0

Ending Virtual IP: 10.63.150.97      Preferred MAC Address:  No

**VIRTUAL IP RANGES**

Use all network interfaces on all nodes that are running the NFS Gateway service.  
 Select network interfaces

Node Name	Physical IP	Mac Address
workr-140.netapp.com	10.63.150.140	90:1b:0:ed:1:5e:03

Node Name	Physical IP	Mac Address
workr-138.netapp.com	10.63.150.138	90:1b:0:ed:1:5d:f9

**Save Changes** **Cancel**

**SETTINGS AND AUDITING**

\* Starting Virtual IP: 10.63.150.92      \* NetMask: 255.255.255.0

Ending Virtual IP: 10.63.150.93      Preferred MAC Address:  No

**VIRTUAL IP RANGES**

Use all network interfaces on all nodes that are running the NFS Gateway service.  
 Select network interfaces

Node Name	Physical IP	Mac Address
workr-138.netapp.com	10.63.150.138	90:1b:0:ed:1:5d:f9

Node Name	Physical IP	Mac Address
workr-140.netapp.com	10.63.150.140	90:1b:0:ed:1:5e:03

**Save Changes** **Cancel**

## 9. Check the virtual IPs assigned on each MapR node and use them for NFS data access.

```
root@workr-138: ~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
```

```

        valid_lft forever preferred_lft forever
2: ens3f0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9000 qdisc mq state UP
group default qlen 1000
    link/ether 90:1b:0e:d1:5d:f9 brd ff:ff:ff:ff:ff:ff
    inet 10.63.150.138/24 brd 10.63.150.255 scope global noprefixroute
ens3f0
        valid_lft forever preferred_lft forever
        inet 10.63.150.96/24 scope global secondary ens3f0:~m0
            valid_lft forever preferred_lft forever
            inet 10.63.150.97/24 scope global secondary ens3f0:~m1
                valid_lft forever preferred_lft forever
                inet6 fe80::921b:eff:fed1:5df9/64 scope link
                    valid_lft forever preferred_lft forever
3: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
group default qlen 1000
    link/ether 90:1b:0e:d1:af:b4 brd ff:ff:ff:ff:ff:ff
4: ens3f1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
group default qlen 1000
    link/ether 90:1b:0e:d1:5d:fa brd ff:ff:ff:ff:ff:ff
5: eno2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state
DOWN group default qlen 1000
    link/ether 90:1b:0e:d1:af:b5 brd ff:ff:ff:ff:ff:ff
[root@workr-138: ~$]
[root@workr-140 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: ens3f0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9000 qdisc mq state UP
group default qlen 1000
    link/ether 90:1b:0e:d1:5e:03 brd ff:ff:ff:ff:ff:ff
    inet 10.63.150.140/24 brd 10.63.150.255 scope global noprefixroute
ens3f0
        valid_lft forever preferred_lft forever
        inet 10.63.150.92/24 scope global secondary ens3f0:~m0
            valid_lft forever preferred_lft forever
            inet6 fe80::921b:eff:fed1:5e03/64 scope link noprefixroute
                valid_lft forever preferred_lft forever
3: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
group default qlen 1000
    link/ether 90:1b:0e:d1:af:9a brd ff:ff:ff:ff:ff:ff
4: ens3f1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
group default qlen 1000

```

```

link/ether 90:1b:0e:d1:5e:04 brd ff:ff:ff:ff:ff:ff
5: eno2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state
DOWN group default qlen 1000
    link/ether 90:1b:0e:d1:af:9b brd ff:ff:ff:ff:ff:ff
[root@workr-140 ~]#

```

10. Mount the NFS- exported MapR-FS using the assigned virtual IP for checking the NFS operation. However, this step is not required for data transfer using NetApp XCP.

```

root@workr-138: tmp$ mount -v -t nfs 10.63.150.92:/maprnfs3
/tmp/testmount/
mount.nfs: timeout set for Thu Dec  5 15:31:32 2019
mount.nfs: trying text-based options
'vers=4.1,addr=10.63.150.92,clientaddr=10.63.150.138'
mount.nfs: mount(2): Protocol not supported
mount.nfs: trying text-based options
'vers=4.0,addr=10.63.150.92,clientaddr=10.63.150.138'
mount.nfs: mount(2): Protocol not supported
mount.nfs: trying text-based options 'addr=10.63.150.92'
mount.nfs: prog 100003, trying vers=3, prot=6
mount.nfs: trying 10.63.150.92 prog 100003 vers 3 prot TCP port 2049
mount.nfs: prog 100005, trying vers=3, prot=17
mount.nfs: trying 10.63.150.92 prog 100005 vers 3 prot UDP port 2049
mount.nfs: portmap query retrying: RPC: Timed out
mount.nfs: prog 100005, trying vers=3, prot=6
mount.nfs: trying 10.63.150.92 prog 100005 vers 3 prot TCP port 2049
root@workr-138: tmp$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda7        84G   48G   37G  57% /
devtmpfs       126G     0  126G  0% /dev
tmpfs          126G     0  126G  0% /dev/shm
tmpfs          126G   19M  126G  1% /run
tmpfs          126G     0  126G  0% /sys/fs/cgroup
/dev/sdd1        3.7T  201G  3.5T  6% /mnt/sdd1
/dev/sda6       946M  220M  726M 24% /boot
tmpfs           26G     0   26G  0% /run/user/5000
gpfs1          7.3T  9.1G  7.3T  1% /gpfs1
tmpfs           26G     0   26G  0% /run/user/0
localhost:/mapr 100G     0  100G  0% /mapr
10.63.150.92:/maprnfs3  53T  8.4G  53T  1% /tmp/testmount
root@workr-138: tmp$
```

11. Configure NetApp XCP to transfer data from the MapR-FS NFS gateway to ONTAP NFS.
  - a. Configure the catalog location for XCP.

```
[root@hdp2 linux]# cat /opt/NetApp/xFiles/xcp/xcp.ini
# Sample xcp config
[xcp]
#catalog = 10.63.150.51:/gpfs1
catalog = 10.63.150.213:/nc_volume1
```

- b. Copy the license file to /opt/NetApp/xFiles/xcp/.

```
root@workr-138: src$ cd /opt/NetApp/xFiles/xcp/
root@workr-138: xcp$ ls -ltrha
total 252K
drwxr-xr-x 3 root    root     16 Apr  4  2019 ..
-rw-r--r-- 1 root    root   105 Dec  5 19:04 xcp.ini
drwxr-xr-x 2 root    root     59 Dec  5 19:04 .
-rw-r--r-- 1 faiz89 faiz89  336 Dec  6 21:12 license
-rw-r--r-- 1 root    root   192 Dec  6 21:13 host
-rw-r--r-- 1 root    root  236K Dec 17 14:12 xcp.log
root@workr-138: xcp$
```

- c. Activate XCP using the xcp activate command.

- d. Check the source for NFS export.

```
[root@hdp2 linux]# ./xcp show 10.63.150.92
XCP 1.4-17914d6; (c) 2019 NetApp, Inc.; Licensed to Karthikeyan
Nagalingam [NetApp Inc] until Wed Feb 5 11:07:27 2020
getting pmap dump from 10.63.150.92 port 111...
getting export list from 10.63.150.92...
sending 1 mount and 4 nfs requests to 10.63.150.92...
== RPC Services ==
'10.63.150.92': TCP rpc services: MNT v1/3, NFS v3/4, NFSACL v3, NLM
v1/3/4, PMAP v2/3/4, STATUS v1
'10.63.150.92': UDP rpc services: MNT v1/3, NFS v4, NFSACL v3, NLM
v1/3/4, PMAP v2/3/4, STATUS v1
== NFS Exports ==
Mounts Errors Server
1 0 10.63.150.92
Space Files Space Files
Free Free Used Used Export
52.3 TiB 53.7B 8.36 GiB 53.7B 10.63.150.92:/maprnfs3
== Attributes of NFS Exports ==
drwxr-xr-x --- root root 2 2 10m51s 10.63.150.92:/maprnfs3
1.77 KiB in (8.68 KiB/s), 3.16 KiB out (15.5 KiB/s), 0s.
[root@hdp2 linux]#
```

- e. Transfer the data using XCP from multiple MapR nodes from multiple source IPs and multiple destination IPs (ONTAP LIFs).

```
root@workr-138: linux$ ./xcp_yatin copy --parallel 20
10.63.150.96,10.63.150.97:/maprnfs3/tg4
10.63.150.85,10.63.150.86:/datapipline_dataset/tg4_dest
XCP 1.6-dev; (c) 2019 NetApp, Inc.; Licensed to Karthikeyan
Nagalingam [NetApp Inc] until Wed Feb 5 11:07:27 2020
xcp: WARNING: No index name has been specified, creating one with
name: autoname_copy_2019-12-06_21.14.38.652652
xcp: mount '10.63.150.96,10.63.150.97:/maprnfs3/tg4': WARNING: This
NFS server only supports 1-second timestamp granularity. This may
cause sync to fail because changes will often be undetectable.
130 scanned, 128 giants, 3.59 GiB in (723 MiB/s), 3.60 GiB out (724
MiB/s), 5s
130 scanned, 128 giants, 8.01 GiB in (889 MiB/s), 8.02 GiB out (890
MiB/s), 11s
130 scanned, 128 giants, 12.6 GiB in (933 MiB/s), 12.6 GiB out (934
MiB/s), 16s
130 scanned, 128 giants, 16.7 GiB in (830 MiB/s), 16.7 GiB out (831
MiB/s), 21s
130 scanned, 128 giants, 21.1 GiB in (907 MiB/s), 21.1 GiB out (908
MiB/s), 26s
```

```
130 scanned, 128 giants, 25.5 GiB in (893 MiB/s), 25.5 GiB out (894
MiB/s), 31s
130 scanned, 128 giants, 29.6 GiB in (842 MiB/s), 29.6 GiB out (843
MiB/s), 36s
...
[root@workr-140 linux]# ./xcp_yatin copy --parallel 20
10.63.150.92:/maprnfs3/tg4_2
10.63.150.85,10.63.150.86:/datapipeline_dataset/tg4_2_dest
XCP 1.6-dev; (c) 2019 NetApp, Inc.; Licensed to Karthikeyan
Nagalingam [NetApp Inc] until Wed Feb 5 11:07:27 2020
xcp: WARNING: No index name has been specified, creating one with
name: autoname_copy_2019-12-06_21.14.24.637773
xcp: mount '10.63.150.92:/maprnfs3/tg4_2': WARNING: This NFS server
only supports 1-second timestamp granularity. This may cause sync to
fail because changes will often be undetectable.
130 scanned, 128 giants, 4.39 GiB in (896 MiB/s), 4.39 GiB out (897
MiB/s), 5s
130 scanned, 128 giants, 9.94 GiB in (1.10 GiB/s), 9.96 GiB out
(1.10 GiB/s), 10s
130 scanned, 128 giants, 15.4 GiB in (1.09 GiB/s), 15.4 GiB out
(1.09 GiB/s), 15s
130 scanned, 128 giants, 20.1 GiB in (953 MiB/s), 20.1 GiB out (954
MiB/s), 20s
130 scanned, 128 giants, 24.6 GiB in (928 MiB/s), 24.7 GiB out (929
MiB/s), 25s
130 scanned, 128 giants, 29.0 GiB in (877 MiB/s), 29.0 GiB out (878
MiB/s), 31s
130 scanned, 128 giants, 33.2 GiB in (852 MiB/s), 33.2 GiB out (853
MiB/s), 36s
130 scanned, 128 giants, 37.8 GiB in (941 MiB/s), 37.8 GiB out (942
MiB/s), 41s
130 scanned, 128 giants, 42.0 GiB in (860 MiB/s), 42.0 GiB out (861
MiB/s), 46s
130 scanned, 128 giants, 46.1 GiB in (852 MiB/s), 46.2 GiB out (853
MiB/s), 51s
130 scanned, 128 giants, 50.1 GiB in (816 MiB/s), 50.2 GiB out (817
MiB/s), 56s
130 scanned, 128 giants, 54.1 GiB in (819 MiB/s), 54.2 GiB out (820
MiB/s), 1m1s
130 scanned, 128 giants, 58.5 GiB in (897 MiB/s), 58.6 GiB out (898
MiB/s), 1m6s
130 scanned, 128 giants, 62.9 GiB in (900 MiB/s), 63.0 GiB out (901
MiB/s), 1m11s
130 scanned, 128 giants, 67.2 GiB in (876 MiB/s), 67.2 GiB out (877
MiB/s), 1m16s
```

f. Check the load distribution on the storage controller.

```
Hadoop-AFF8080::*> statistics show-periodic -interval 2 -iterations 0  
-summary true -object nic_common -counter rx_bytes|tx_bytes -node  
Hadoop-AFF8080-01 -instance e3b  
Hadoop-AFF8080: nic_common.e3b: 12/6/2019 15:55:04  
rx_bytes tx_bytes  
-----  
879MB 4.67MB  
856MB 4.46MB  
973MB 5.66MB  
986MB 5.88MB  
945MB 5.30MB  
920MB 4.92MB  
894MB 4.76MB  
902MB 4.79MB  
886MB 4.68MB  
892MB 4.78MB  
908MB 4.96MB  
905MB 4.85MB  
899MB 4.83MB  
  
Hadoop-AFF8080::*> statistics show-periodic -interval 2 -iterations 0  
-summary true -object nic_common -counter rx_bytes|tx_bytes -node  
Hadoop-AFF8080-01 -instance e9b  
Hadoop-AFF8080: nic_common.e9b: 12/6/2019 15:55:07  
rx_bytes tx_bytes  
-----  
950MB 4.93MB  
991MB 5.84MB  
959MB 5.63MB  
914MB 5.06MB  
903MB 4.81MB  
899MB 4.73MB  
892MB 4.71MB  
890MB 4.72MB  
905MB 4.86MB  
902MB 4.90MB
```

Next: [Where to find additional information.](#)

## Where to find additional information

Previous: [MapR-FS to ONTAP NFS.](#)

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

- NetApp In-Place Analytics Module Best Practices  
<https://www.netapp.com/us/media/tr-4382.pdf>
- NetApp FlexGroup Volume Best Practices and Implementation Guide  
<https://www.netapp.com/us/media/tr-4571.pdf>
- NetApp Product Documentation  
<https://www.netapp.com/us/documentation/index.aspx>

#### **Version history**

<b>Version</b>	<b>Date</b>	<b>Document version history</b>
Version 3.0	January 2022	Directly move data from HDFS and MapR-FS to NFS by using NetApp XCP.
Version 2.0	January 2020	XCP included as the default data mover. Added MapR-FS to NFS and GPFS to NFS data transfer.
Version 1.0	November 2018	Initial release.

## **Best practices for Confluent Kafka**

### **TR-4912: Best practice guidelines for Confluent Kafka tiered storage with NetApp**

Karthikeyan Nagalingam, Joseph Kandatilparambil, NetApp  
 Rankesh Kumar, Confluent

Apache Kafka is a community-distributed event-streaming platform capable of handling trillions of events a day. Initially conceived as a messaging queue, Kafka is based on an abstraction of a distributed commit log. Since it was created and open-sourced by LinkedIn in 2011, Kafka has evolved from a messages queue to a full-fledged event-streaming platform. Confluent delivers the distribution of Apache Kafka with the Confluent Platform. The Confluent Platform supplements Kafka with additional community and commercial features designed to enhance the streaming experience of both operators and developers in production at a massive scale.

This document describes the best-practice guidelines for using Confluent Tiered Storage on a NetApp's Object storage offering by providing the following content:

- Confluent verification with NetApp Object storage – NetApp StorageGRID
- Tiered storage performance tests
- Best-practice guidelines for Confluent on NetApp storage systems

#### **Why Confluent Tiered Storage?**

Confluent has become the default real-time streaming platform for many applications, especially for big data, analytics, and streaming workloads. Tiered Storage enables users to separate compute from storage in the

Confluent platform. It makes storing data more cost effective, enables you to store virtually infinite amounts of data and scale workloads up (or down) on-demand, and makes administrative tasks like data and tenant rebalancing easier. S3 compatible storage systems can take advantage of all these capabilities to democratize data with all events in one place, eliminating the need for complex data engineering. For more info on why you should use tiered storage for Kafka, check [this article by Confluent](#).

## Why NetApp StorageGRID for tiered storage?

StorageGRID is an industry-leading object storage platform by NetApp. StorageGRID is a software-defined, object-based storage solution that supports industry-standard object APIs, including the Amazon Simple Storage Service (S3) API. StorageGRID stores and manages unstructured data at scale to provide secure, durable object storage. Content is placed in the right location, at the right time, and on the right storage tier, optimizing workflows and reducing costs for globally distributed rich media.

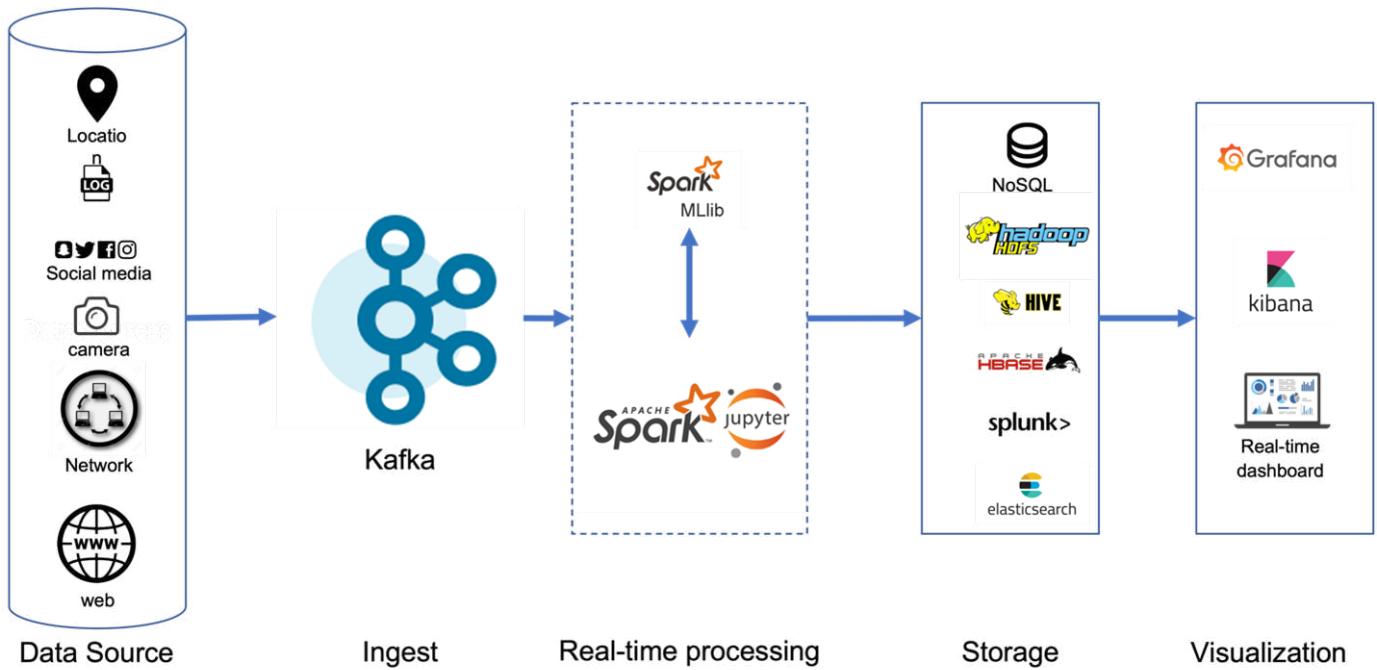
The greatest differentiator for StorageGRID is its Information Lifecycle Management (ILM) policy engine that enables policy-driven data lifecycle management. The policy engine can use metadata to manage how data is stored across its lifetime to initially optimize for performance and automatically optimize for cost and durability as data ages.

## Enabling Confluent Tiered Storage

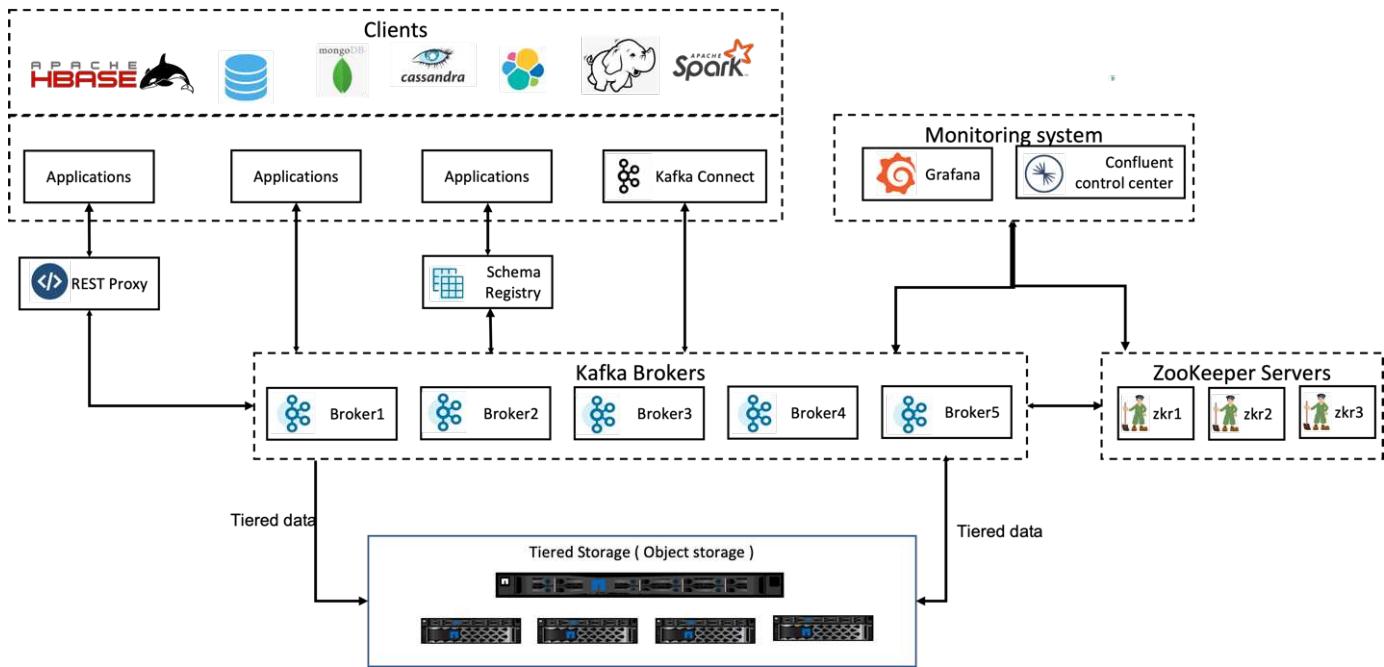
The basic idea of tiered storage is to separate the tasks of data storage from data processing. With this separation, it becomes much easier for the data storage tier and the data processing tier to scale independently.

A tiered storage solution for Confluent must contend with two factors. First, it must work around or avoid common object store consistency and availability properties, such as inconsistencies in LIST operations and occasional object unavailability. Secondly, it must correctly handle the interaction between tiered storage and Kafka's replication and fault tolerance model, including the possibility of zombie leaders continuing to tier offset ranges. NetApp Object storage provides both the consistent object availability and HA model make the tired storage available to tier offset ranges. NetApp object storage provides consistent object availability and an HA model to make the tired storage available to tier offset ranges.

With tiered storage, you can use high-performance platforms for low-latency reads and writes near the tail of your streaming data, and you can also use cheaper, scalable object stores like NetApp StorageGRID for high-throughput historical reads. We also have technical solution for Spark with netapp storage controller and details are here. The following figure shows how Kafka fits into a real-time analytics pipeline.



The following figure depicts how NetApp StorageGRID fits in as Confluent Kafka's object storage tier.



[Next: Solution architecture details.](#)

## Solution architecture details

[Previous: Introduction.](#)

This section covers the hardware and software used for Confluent verification. This information is applicable to Confluent Platform deployment with NetApp storage. The following table covers the tested solution architecture and base components.

Solution components	Details
Confluent Kafka version 6.2	<ul style="list-style-type: none"> <li>• Three zookeepers</li> <li>• Five broker servers</li> <li>• Five tools servers</li> <li>• One Grafana</li> <li>• One control center</li> </ul>
Linux (ubuntu 18.04)	All servers
NetApp StorageGRID for tiered storage	<ul style="list-style-type: none"> <li>• StorageGRID software</li> <li>• 1 x SG1000 (load balancer)</li> <li>• 4 x SGF6024</li> <li>• 4 x 24 x 800 SSDs</li> <li>• S3 protocol</li> <li>• 4 x 100GbE (network connectivity between broker and StorageGRID instances)</li> </ul>
15 Fujitsu PRIMERGY RX2540 servers	<p>Each equipped with:</p> <ul style="list-style-type: none"> <li>* 2 CPUs, 16 physical cores total</li> <li>* Intel Xeon</li> <li>* 256GB physical memory</li> <li>* 100GbE dual port</li> </ul>

[Next: Technology overview.](#)

## Technology overview

[Previous: Solution architecture details.](#)

This section describes the technology used in this solution.

### NetApp StorageGRID

NetApp StorageGRID is a high-performance, cost-effective object storage platform. By using tiered storage, most of the data on Confluent Kafka, which is stored in local storage or the SAN storage of the broker, is offloaded to the remote object store. This configuration results in significant operational improvements by reducing the time and cost to rebalance, expand, or shrink clusters or replace a failed broker. Object storage plays an important role in managing data that resides on the object store tier, which is why picking the right object storage is important.

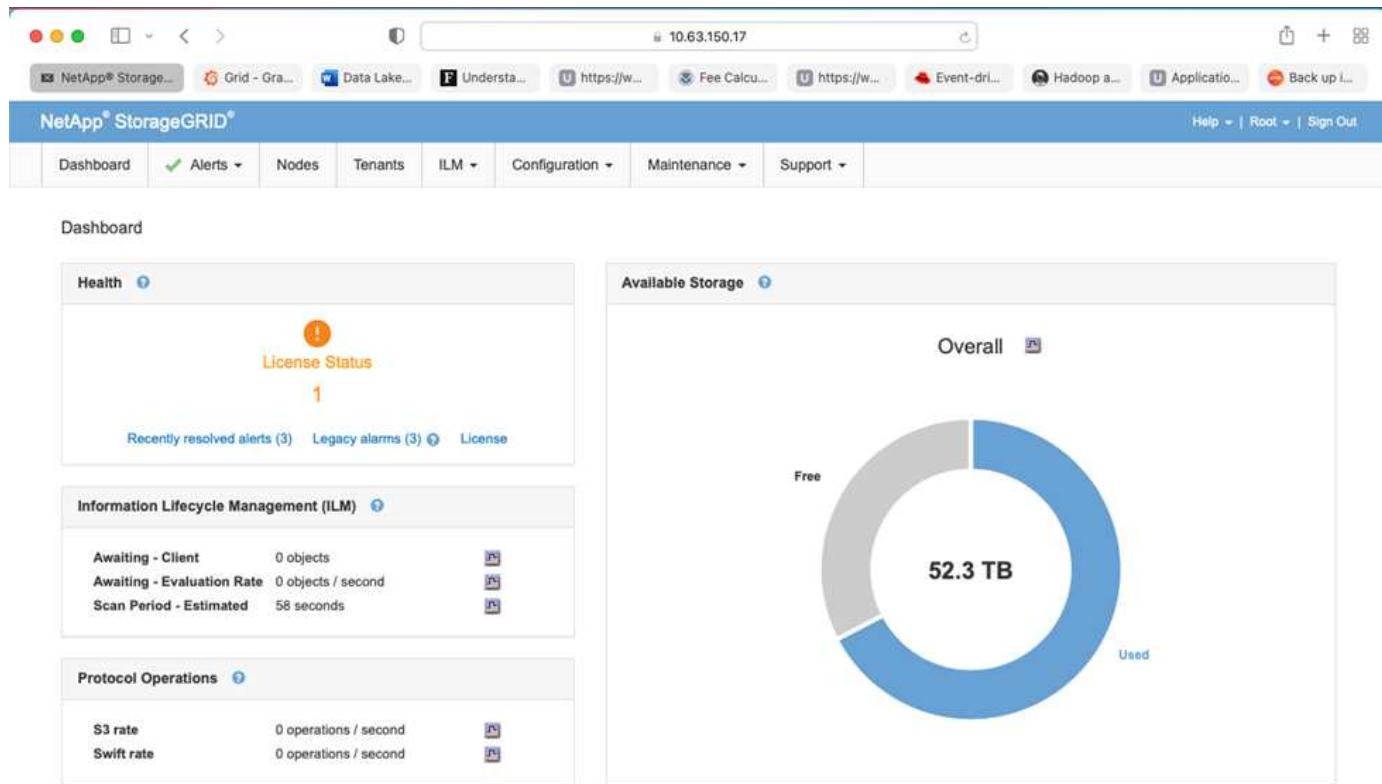
StorageGRID offers intelligent, policy-driven global data management using a distributed, node-based grid architecture. It simplifies the management of petabytes of unstructured data and billions of objects through its ubiquitous global object namespace combined with sophisticated data management features. Single-call object access extends across sites and simplifies high availability architectures while ensuring continual object access, regardless of site or infrastructure outages.

Multitenancy allows multiple unstructured cloud and enterprise data applications to be securely serviced within the same grid, increasing the ROI and use cases for NetApp StorageGRID. You can create multiple service levels with metadata-driven object lifecycle policies, optimizing durability, protection, performance, and locality.

across multiple geographies. Users can adjust data management policies and monitor and apply traffic limits to realign with the data landscape nondisruptively as their requirements change in ever-changing IT environments.

### Simple management with Grid Manager

The StorageGRID Grid Manager is a browser-based graphical interface that allows you to configure, manage, and monitor your StorageGRID system across globally distributed locations in a single pane of glass.



You can perform the following tasks with the StorageGRID Grid Manager interface:

- Manage globally distributed, petabyte-scale repositories of objects such as images, video, and records.
- Monitor grid nodes and services to ensure object availability.
- Manage the placement of object data over time using information lifecycle management (ILM) rules. These rules govern what happens to an object's data after it is ingested, how it is protected from loss, where object data is stored, and for how long.
- Monitor transactions, performance, and operations within the system.

### Information Lifecycle Management policies

StorageGRID has flexible data management policies that include keeping replica copies of your objects and using EC (erasure coding) schemes like 2+1 and 4+2 (among others) to store your objects, depending on specific performance and data protection requirements. As workloads and requirements change over time, it's common that ILM policies must change over time as well. Modifying ILM policies is a core feature, allowing StorageGRID customers to adapt to their ever-changing environment quickly and easily. Please check the [ILM policy](#) and [ILM rules](#) setup in StorageGRID.

## Performance

StorageGRID scales performance by adding more storage nodes, which can be VMs, bare metal, or purpose-built appliances like the [SG5712](#), [SG5760](#), [SG6060](#), or [SGF6024](#). In our tests, we exceeded the Apache Kafka key performance requirements with a minimum-sized, three-node grid using the SGF6024 appliance. As customers scale their Kafka cluster with additional brokers, they can add more storage nodes to increase performance and capacity.

## Load balancer and endpoint configuration

Admin nodes in StorageGRID provide the Grid Manager UI (user interface) and REST API endpoint to view, configure, and manage your StorageGRID system, as well as audit logs to track system activity. To provide a highly available S3 endpoint for Confluent Kafka tiered storage, we implemented the StorageGRID load balancer, which runs as a service on admin nodes and gateway nodes. In addition, the load balancer also manages local traffic and talks to the GSLB (Global Server Load Balancing) to help with disaster recovery.

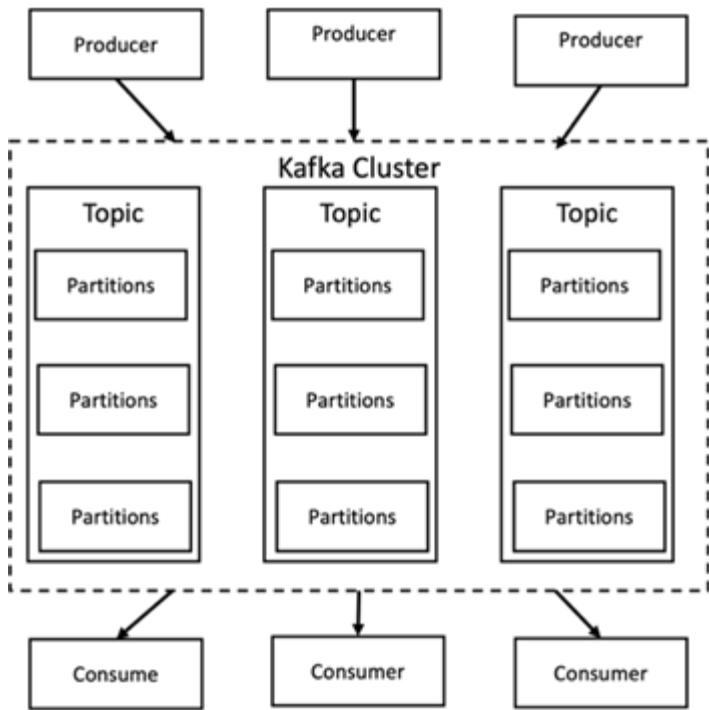
To further enhance endpoint configuration, StorageGRID provides traffic classification policies built into the admin node, lets you monitor your workload traffic, and applies various quality-of-service (QoS) limits to your workloads. Traffic classification policies are applied to endpoints on the StorageGRID Load Balancer service for gateway nodes and admin nodes. These policies can assist with traffic limiting and monitoring.

## Traffic classification in StorageGRID

StorageGRID has built-in QoS functionality. Traffic classification policies can help monitor different types of S3 traffic coming from a client application. You can then create and apply policies to put limits on this traffic based on in/out bandwidth, the number of read/write concurrent requests, or the read/write request rate.

## Apache Kafka

Apache Kafka is a framework implementation of a software bus using stream processing written in Java and Scala. It's aimed to provide a unified, high-throughput, low-latency platform for handling real-time data feeds. Kafka can connect to an external system for data export and import through Kafka Connect and provides Kafka streams, a Java stream processing library. Kafka uses a binary, TCP-based protocol that is optimized for efficiency and relies on a "message set" abstraction that naturally groups messages together to reduce the overhead of the network roundtrip. This enables larger sequential disk operations, larger network packets, and contiguous memory blocks, thereby enabling Kafka to turn a bursty stream of random message writes into linear writes. The following figure depicts the basic data flow of Apache Kafka.



Kafka stores key-value messages that come from an arbitrary number of processes called producers. The data can be partitioned into different partitions within different topics. Within a partition, messages are strictly ordered by their offsets (the position of a message within a partition) and indexed and stored together with a timestamp. Other processes called consumers can read messages from partitions. For stream processing, Kafka offers the Streams API that allows writing Java applications that consume data from Kafka and write results back to Kafka. Apache Kafka also works with external stream processing systems such as Apache Apex, Apache Flink, Apache Spark, Apache Storm, and Apache NiFi.

Kafka runs on a cluster of one or more servers (called brokers), and the partitions of all topics are distributed across the cluster nodes. Additionally, partitions are replicated to multiple brokers. This architecture allows Kafka to deliver massive streams of messages in a fault-tolerant fashion and has allowed it to replace some of the conventional messaging systems like Java Message Service (JMS), Advanced Message Queuing Protocol (AMQP), and so on. Since the 0.11.0.0 release, Kafka offers transactional writes, which provide exactly once stream processing using the Streams API.

Kafka supports two types of topics: regular and compacted. Regular topics can be configured with a retention time or a space bound. If there are records that are older than the specified retention time or if the space bound is exceeded for a partition, Kafka is allowed to delete old data to free storage space. By default, topics are configured with a retention time of 7 days, but it's also possible to store data indefinitely. For compacted topics, records don't expire based on time or space bounds. Instead, Kafka treats later messages as updates to older message with the same key and guarantees never to delete the latest message per key. Users can delete messages entirely by writing a so-called tombstone message with the null value for a specific key.

There are five major APIs in Kafka:

- **Producer API.** Permits an application to publish streams of records.
- **Consumer API.** Permits an application to subscribe to topics and processes streams of records.
- **Connector API.** Executes the reusable producer and consumer APIs that can link the topics to the existing applications.
- **Streams API.** This API converts the input streams to output and produces the result.
- **Admin API.** Used to manage Kafka topics, brokers and other Kafka objects.

The consumer and producer APIs build on top of the Kafka messaging protocol and offer a reference implementation for Kafka consumer and producer clients in Java. The underlying messaging protocol is a binary protocol that developers can use to write their own consumer or producer clients in any programming language. This unlocks Kafka from the Java Virtual Machine (JVM) ecosystem. A list of available non-Java clients is maintained in the Apache Kafka wiki.

### Apache Kafka use cases

Apache Kafka is most popular for messaging, website activity tracking, metrics, log aggregation, stream processing, event sourcing, and commit logging.

- Kafka has improved throughput, built-in partitioning, replication, and fault-tolerance, which makes it a good solution for large-scale message-processing applications.
- Kafka can rebuild a user's activities (page views, searches) in a tracking pipeline as a set of real-time publish-subscribe feeds.
- Kafka is often used for operational monitoring data. This involves aggregating statistics from distributed applications to produce centralized feeds of operational data.
- Many people use Kafka as a replacement for a log aggregation solution. Log aggregation typically collects physical log files off of servers and puts them in a central place (for example, a file server or HDFS) for processing. Kafka abstracts file details and provides a cleaner abstraction of log or event data as a stream of messages. This allows for lower-latency processing and easier support for multiple data sources and distributed data consumption.
- Many users of Kafka process data in processing pipelines consisting of multiple stages, in which raw input data is consumed from Kafka topics and then aggregated, enriched, or otherwise transformed into new topics for further consumption or follow-up processing. For example, a processing pipeline for recommending news articles might crawl article content from RSS feeds and publish it to an "articles" topic. Further processing might normalize or deduplicate this content and publish the cleansed article content to a new topic, and a final processing stage might attempt to recommend this content to users. Such processing pipelines create graphs of real-time data flows based on the individual topics.
- Event sourcing is a style of application design for which state changes are logged as a time-ordered sequence of records. Kafka's support for very large stored log data makes it an excellent backend for an application built in this style.
- Kafka can serve as a kind of external commit-log for a distributed system. The log helps replicate data between nodes and acts as a re-syncing mechanism for failed nodes to restore their data. The log compaction feature in Kafka helps support this use case.

### Confluent

Confluent Platform is an enterprise-ready platform that completes Kafka with advanced capabilities designed to help accelerate application development and connectivity, enable transformations through stream processing, simplify enterprise operations at scale, and meet stringent architectural requirements. Built by the original creators of Apache Kafka, Confluent expands the benefits of Kafka with enterprise-grade features while removing the burden of Kafka management or monitoring. Today, over 80% of the Fortune 100 are powered by data streaming technology – and most of those use Confluent.

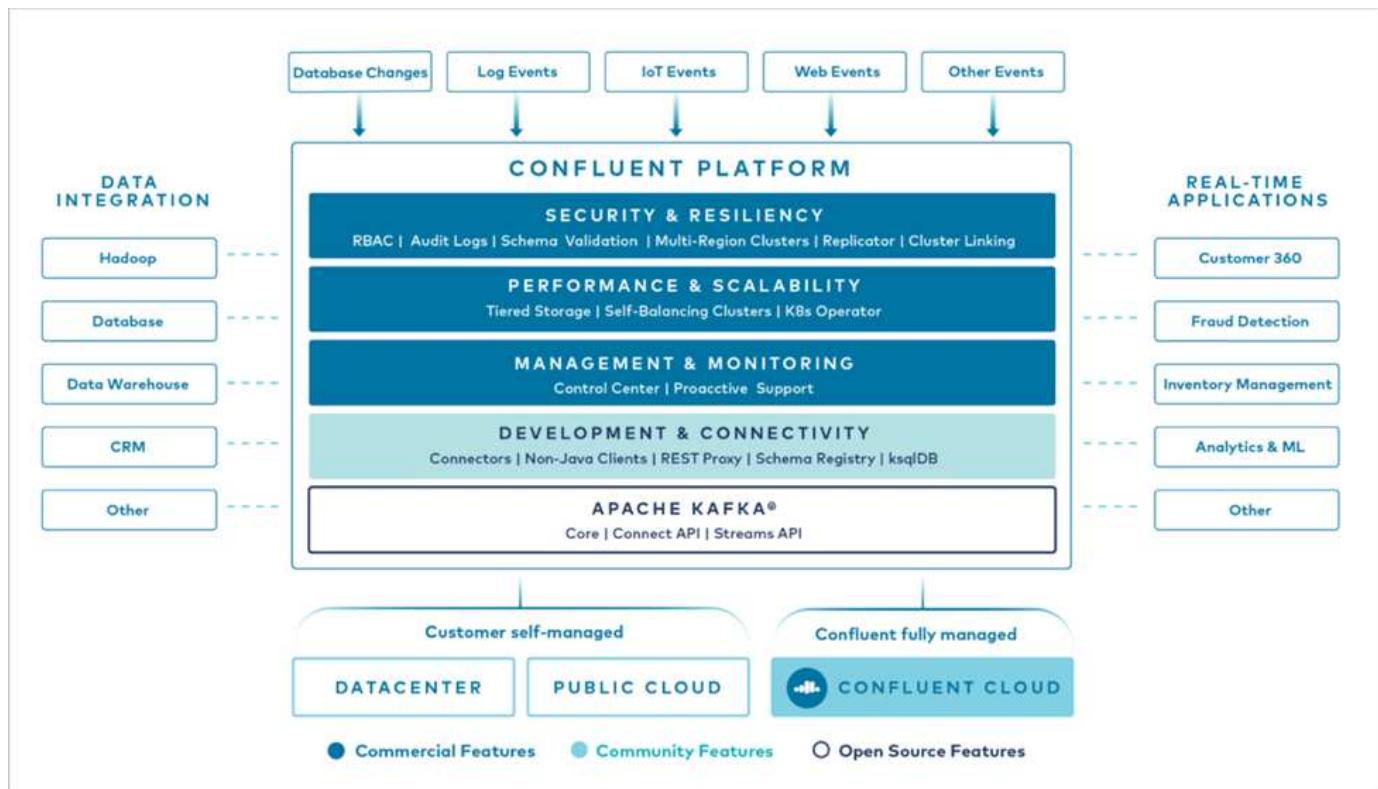
### Why Confluent?

By integrating historical and real-time data into a single, central source of truth, Confluent makes it easy to build an entirely new category of modern, event-driven applications, gain a universal data pipeline, and unlock powerful new use cases with full scalability, performance, and reliability.

## What is Confluent used for?

Confluent Platform lets you focus on how to derive business value from your data rather than worrying about the underlying mechanics, such as how data is being transported or integrated between disparate systems. Specifically, Confluent Platform simplifies connecting data sources to Kafka, building streaming applications, as well as securing, monitoring, and managing your Kafka infrastructure. Today, Confluent Platform is used for a wide array of use cases across numerous industries, from financial services, omnichannel retail, and autonomous cars, to fraud detection, microservices, and IoT.

The following figure shows Confluent Kafka Platform components.



## Overview of Confluent's event streaming technology

At the core of Confluent Platform is [Apache Kafka](#), the most popular open-source distributed streaming platform. The key capabilities of Kafka are as follows:

- Publish and subscribe to streams of records.
- Store streams of records in a fault tolerant way.
- Process streams of records.

Out of the box, Confluent Platform also includes Schema Registry, REST Proxy, a total of 100+ prebuilt Kafka connectors, and ksqlDB.

## Overview of Confluent platform's enterprise features

- **Confluent Control Center.** A GUI-based system for managing and monitoring Kafka. It allows you to easily manage Kafka Connect and to create, edit, and manage connections to other systems.
- **Confluent for Kubernetes.** Confluent for Kubernetes is a Kubernetes operator. Kubernetes operators extend the orchestration capabilities of Kubernetes by providing the unique features and requirements for a specific platform application. For Confluent Platform, this includes greatly simplifying the deployment

process of Kafka on Kubernetes and automating typical infrastructure lifecycle tasks.

- **Confluent connectors to Kafka.** Connectors use the Kafka Connect API to connect Kafka to other systems such as databases, key-value stores, search indexes, and file systems. Confluent Hub has downloadable connectors for the most popular data sources and sinks, including fully tested and supported versions of these connectors with Confluent Platform. More details can be found [here](#).
- **Self-balancing clusters.** Provides automated load balancing, failure detection and self-healing. It provides support for adding or decommissioning brokers as needed, with no manual tuning.
- **Confluent cluster linking.** Directly connects clusters together and mirrors topics from one cluster to another over a link bridge. Cluster linking simplifies setup of multi-datacenter, multi-cluster, and hybrid cloud deployments.
- **Confluent auto data balancer.** Monitors your cluster for the number of brokers, the size of partitions, number of partitions, and the number of leaders within the cluster. It allows you to shift data to create an even workload across your cluster, while throttling rebalance traffic to minimize the effect on production workloads while rebalancing.
- **Confluent replicator.** Makes it easier than ever to maintain multiple Kafka clusters in multiple data centers.
- **Tiered storage.** Provides options for storing large volumes of Kafka data using your favorite cloud provider, thereby reducing operational burden and cost. With tiered storage, you can keep data on cost-effective object storage and scale brokers only when you need more compute resources.
- **Confluent JMS client.** Confluent Platform includes a JMS-compatible client for Kafka. This Kafka client implements the JMS 1.1 standard API, using Kafka brokers as the backend. This is useful if you have legacy applications using JMS and you would like to replace the existing JMS message broker with Kafka.
- **Confluent MQTT proxy.** Provides a way to publish data directly to Kafka from MQTT devices and gateways without the need for a MQTT broker in the middle.
- **Confluent security plugins.** Confluent security plugins are used to add security capabilities to various Confluent Platform tools and products. Currently, there is a plugin available for the Confluent REST proxy that helps to authenticate the incoming requests and propagate the authenticated principal to requests to Kafka. This enables Confluent REST proxy clients to utilize the multitenant security features of the Kafka broker.

[Next: Confluent verification.](#)

## Confluent verification

[Previous: Technology overview.](#)

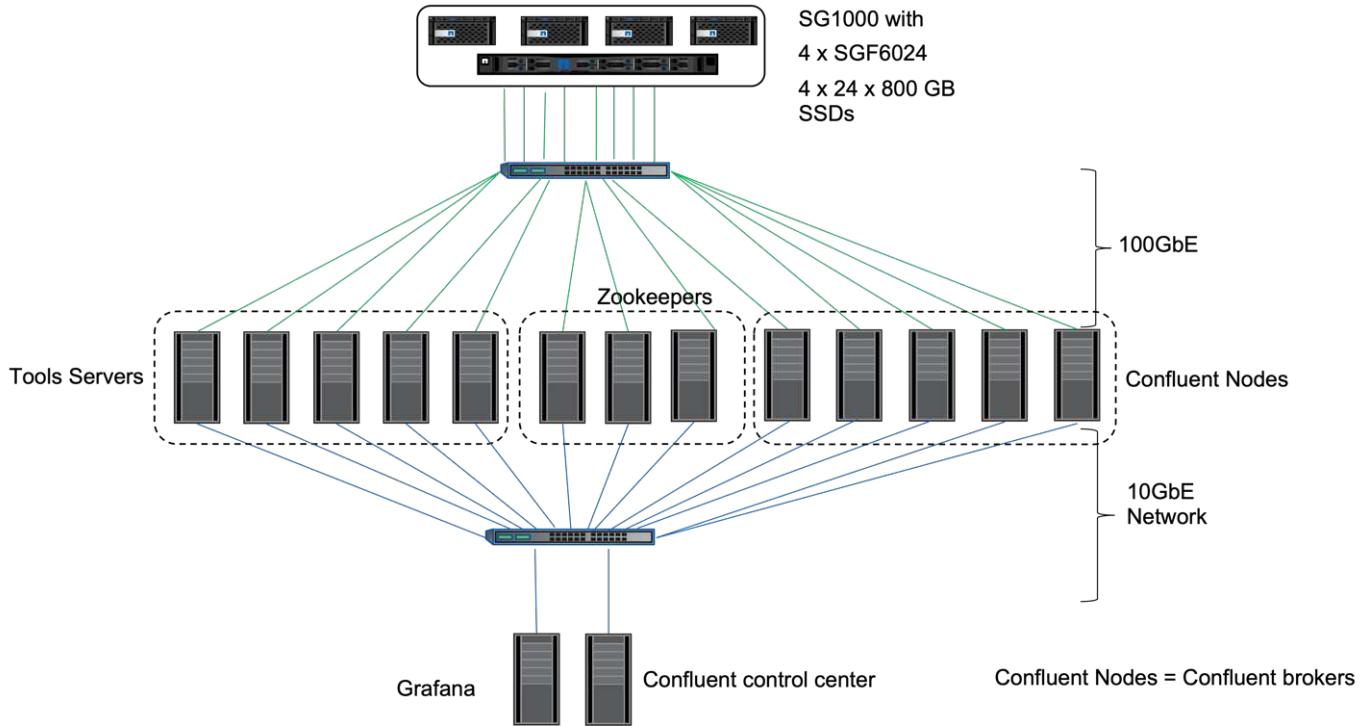
We performed verification with Confluent Platform 6.2 Tiered Storage in NetApp StorageGRID. The NetApp and Confluent teams worked on this verification together and ran the test cases required for verification.

### Confluent Platform setup

We used the following setup for verification.

For verification, we used three zookeepers, five brokers, five test-script executing servers, named tools servers with 256GB RAM, and 16 CPUs. For NetApp storage, we used StorageGRID with an SG1000 load balancer with four SGF6024s. The storage and brokers were connected via 100GbE connections.

The following figure shows the network topology of configuration used for Confluent verification.



The tools servers act as application clients that send requests to Confluent nodes.

### Confluent tiered storage configuration

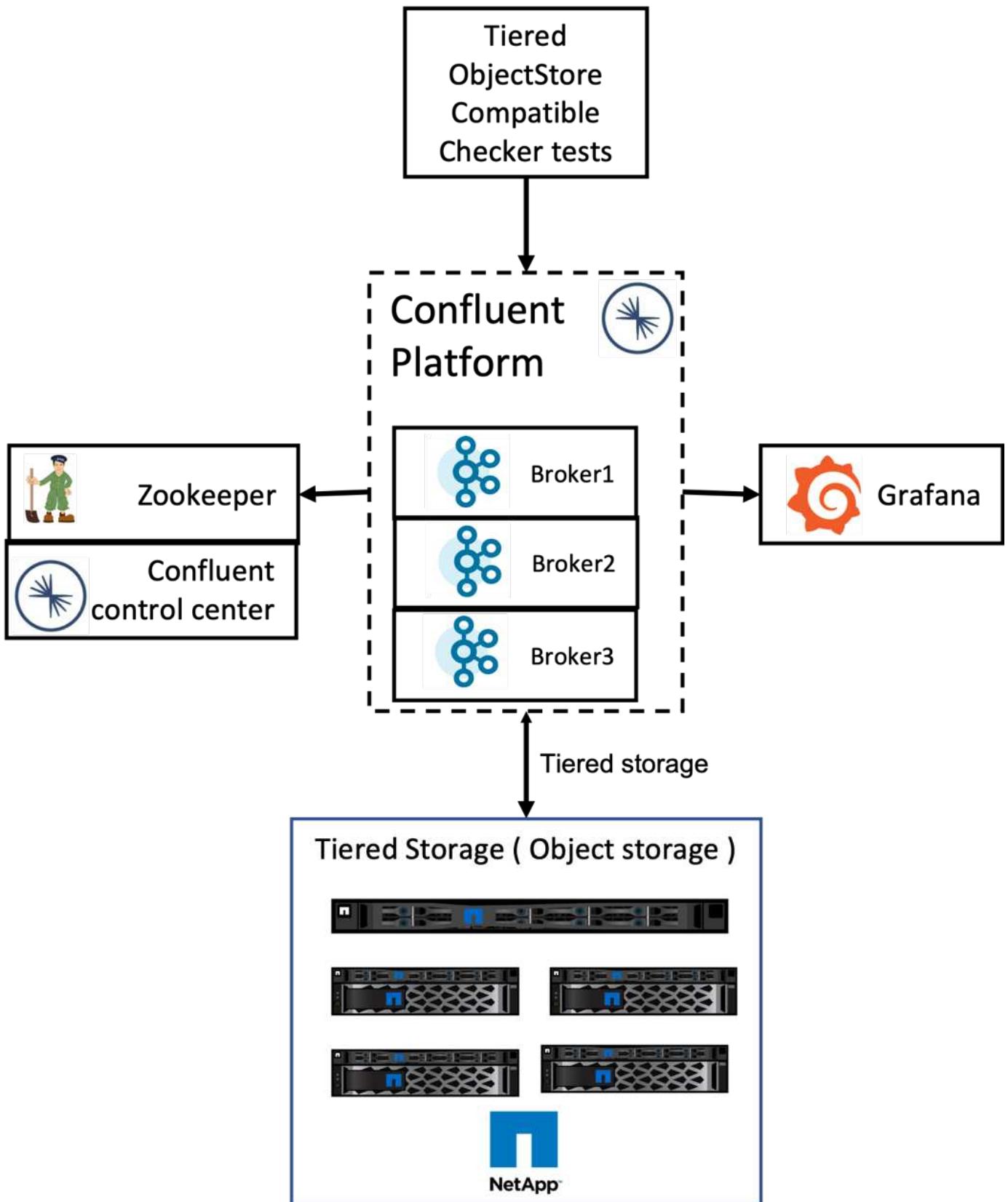
The tiered storage configuration requires the following parameters in Kafka:

```
Confluent.tier.archiver.num.threads=16
confluent.tier.fetcher.num.threads=32
confluent.tier.enable=true
confluent.tier.feature=true
confluent.tier.backend=S3
confluent.tier.s3.bucket=kafkasgdbucket1-2
confluent.tier.s3.region=us-west-2
confluent.tier.s3.cred.file.path=/data/kafka/.ssh/credentials
confluent.tier.s3.aws.endpoint.override=http://kafkasgd.rtpppe.netapp.com:10444/
confluent.tier.s3.force.path.style.access=true
```

For verification, we used StorageGRID with the HTTP protocol, but HTTPS also works. The access key and secret key are stored in the file name provided in the confluent.tier.s3.cred.file.path parameter.

### NetApp object storage - StorageGRID

We configured single-site configuration in StorageGRID for verification.



### Verification tests

We completed the following five test cases for the verification. These tests are executed on the Trogdor framework. The first two were functionality tests and the remaining three were performance tests.

## **Object store correctness test**

This test determines whether all basic operations (for example, get/put/delete) on the object store API work well according to the needs of tiered storage. It is a basic test that every object store service should expect to pass ahead of the following tests. It is an assertive test that either passes or fails.

## **Tiering functionality correctness test**

This test determines if end-to-end tiered storage functionality works well with an assertive test that either passes or fails. The test creates a test topic that by default is configured with tiering enabled and highly a reduced hotset size. It produces an event stream to the newly created test topic, it waits for the brokers to archive the segments to the object store, and it then consumes the event stream and validates that the consumed stream matches the produced stream. The number of messages produced to the event stream is configurable, which lets the user generate a sufficiently large workload according to the needs of testing. The reduced hotset size ensures that the consumer fetches outside the active segment are served only from the object store; this helps test the correctness of the object store for reads. We have performed this test with and without an object-store fault injection. We simulated node failure by stopping the service manager service in one of the nodes in StorageGRID and validating that the end-to-end functionality works with object storage.

## **Tier fetch benchmark**

This test validated the read performance of the tiered object storage and checked the range fetch read requests under heavy load from segments generated by the benchmark. In this benchmark, Confluent developed custom clients to serve the tier fetch requests.

## **Produce-consume workload benchmark**

This test indirectly generated write workload on the object store through the archival of segments. The read workload (segments read) was generated from object storage when consumer groups fetched the segments. This workload was generated by the test script. This test checked the performance of read and write on the object storage in parallel threads. We tested with and without object store fault injection as we did for the tiering functionality correctness test.

## **Retention workload benchmark**

This test checked the deletion performance of an object store under a heavy topic-retention workload. The retention workload was generated using a test script that produces many messages in parallel to a test topic. The test topic was configuring with an aggressive size-based and time-based retention setting that caused the event stream to be continuously purged from the object store. The segments were then archived. This led to a large number of deletions in the object storage by the broker and collection of the performance of the object-store delete operations.

[Next: Performance tests with scalability.](#)

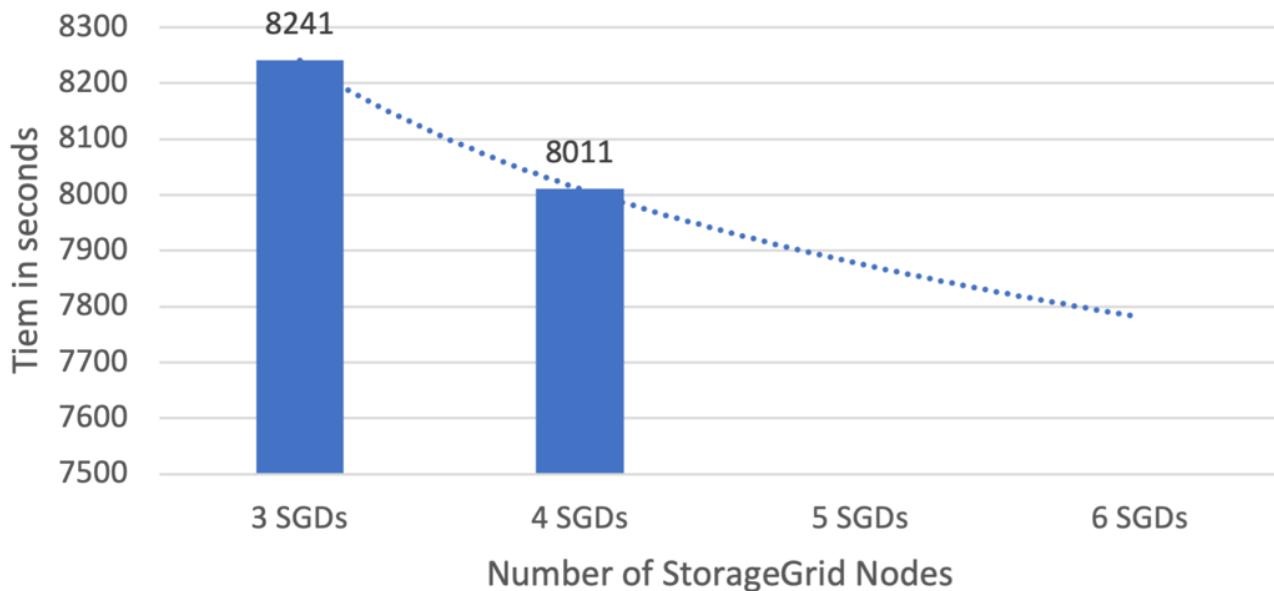
## **Performance tests with scalability**

[Previous: Confluent verification.](#)

We performed the tiered storage testing with three to four nodes for producer and consumer workloads with the NetApp StorageGRID setup. According to our tests, the time to completion and the performance results were directly proportional to the number of StorageGRID nodes. The StorageGRID setup required a minimum of three nodes.

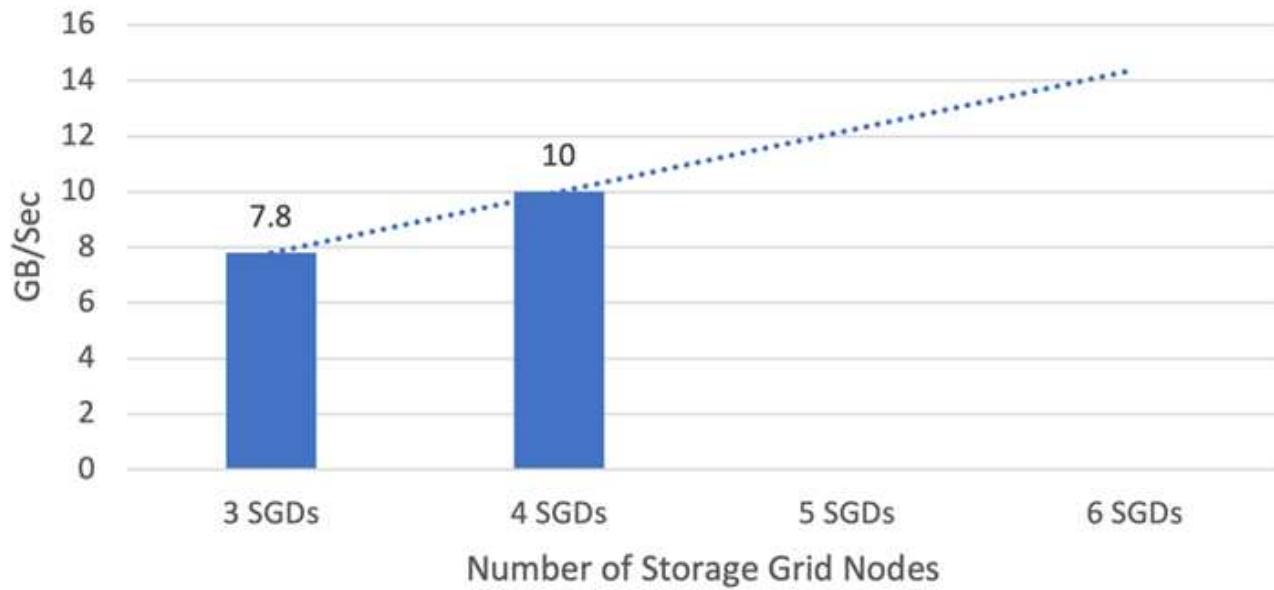
- The time to complete the produce and consumer operation decreased linearly when the number of storage nodes increased.

## Time to complete trends (Lower is better)



- The performance for the s3 retrieve operation increased linearly based on number of StorageGRID nodes. StorageGRID supports up to 200 StorageGRID nodes.

## S3 - Retrieve performance Trend (Higher is better)



Next: Confluent s3 connector.

## Confluent s3 connector

[Previous: Performance tests with scalability.](#)

The Amazon S3 Sink connector exports data from Apache Kafka topics to S3 objects in either the Avro, JSON, or Bytes formats. The Amazon S3 sink connector periodically polls data from Kafka and in turn uploads it to S3. A partitioner is used to split the data of every Kafka partition into chunks. Each chunk of data is represented as an S3 object. The key name encodes the topic, the Kafka partition, and the start offset of this data chunk.

In this setup, we show you how to read and write topics in object storage from Kafka directly using the Kafka s3 sink connector. For this test, we used a stand-alone Confluent cluster, but this setup is applicable to a distributed cluster.

1. Download Confluent Kafka from the Confluent website.
2. Unpack the package to a folder on your server.
3. Export two variables.

```
Export CONFLUENT_HOME=/data/confluent/confluent-6.2.0
export PATH=$PATH:/data/confluent/confluent-6.2.0/bin
```

4. For a stand-alone Confluent Kafka setup, the cluster creates a temporary root folder in /tmp. It also creates Zookeeper, Kafka, a schema registry, connect, a ksql-server, and control-center folders and copies their respective configuration files from \$CONFLUENT\_HOME. See the following example:

```
root@stlrx2540ml-108:~# ls -ltr /tmp/confluent.406980/
total 28
drwxr-xr-x 4 root root 4096 Oct 29 19:01 zookeeper
drwxr-xr-x 4 root root 4096 Oct 29 19:37 kafka
drwxr-xr-x 4 root root 4096 Oct 29 19:40 schema-registry
drwxr-xr-x 4 root root 4096 Oct 29 19:45 kafka-rest
drwxr-xr-x 4 root root 4096 Oct 29 19:47 connect
drwxr-xr-x 4 root root 4096 Oct 29 19:48 ksql-server
drwxr-xr-x 4 root root 4096 Oct 29 19:53 control-center
root@stlrx2540ml-108:~#
```

5. Configure Zookeeper. You don't need to change anything if you use the default parameters.

```
root@stlrx2540m1-108:~# cat
/tmp/confluent.406980/zookeeper/zookeeper.properties | grep -iv ^#
dataDir=/tmp/confluent.406980/zookeeper/data
clientPort=2181
maxClientCnxns=0
admin.enableServer=false
tickTime=2000
initLimit=5
syncLimit=2
server.179=controlcenter:2888:3888
root@stlrx2540m1-108:~#
```

In the above configuration, we updated the `server. xxx` property. By default, you need three Zookeepers for the Kafka leader selection.

6. We created a `myid` file in `/tmp/confluent.406980/zookeeper/data` with a unique ID:

```
root@stlrx2540m1-108:~# cat /tmp/confluent.406980/zookeeper/data/myid
179
root@stlrx2540m1-108:~#
```

We used the last number of IP addresses for the `myid` file. We used default values for the Kafka, connect, control-center, Kafka, Kafka-rest, ksql-server, and schema-registry configurations.

7. Start the Kafka services.

```
root@stlrx2540m1-108:/data/confluent/confluent-6.2.0/bin# confluent
local services start
The local commands are intended for a single-node development
environment only,
NOT for production usage.

Using CONFLUENT_CURRENT: /tmp/confluent.406980
ZooKeeper is [UP]
Kafka is [UP]
Schema Registry is [UP]
Kafka REST is [UP]
Connect is [UP]
ksqlDB Server is [UP]
Control Center is [UP]
root@stlrx2540m1-108:/data/confluent/confluent-6.2.0/bin#
```

There is a log folder for each configuration, which helps troubleshoot issues. In some instances, services take more time to start. Make sure all services are up and running.

8. Install Kafka connect using confluent-hub.

```
root@stlrx2540ml-108:/data/confluent/confluent-6.2.0/bin# ./confluent-hub install confluentinc/kafka-connect-s3:latest
The component can be installed in any of the following Confluent Platform installations:
  1. /data/confluent/confluent-6.2.0 (based on $CONFLUENT_HOME)
  2. /data/confluent/confluent-6.2.0 (where this tool is installed)
Choose one of these to continue the installation (1-2): 1
Do you want to install this into /data/confluent/confluent-6.2.0/share/confluent-hub-components? (yN) y

Component's license:
Confluent Community License
http://www.confluent.io/confluent-community-license
I agree to the software license agreement (yN) y
Downloading component Kafka Connect S3 10.0.3, provided by Confluent, Inc. from Confluent Hub and installing into /data/confluent/confluent-6.2.0/share/confluent-hub-components
Do you want to uninstall existing version 10.0.3? (yN) y
Detected Worker's configs:
  1. Standard: /data/confluent/confluent-6.2.0/etc/kafka/connect-distributed.properties
  2. Standard: /data/confluent/confluent-6.2.0/etc/kafka/connect-standalone.properties
  3. Standard: /data/confluent/confluent-6.2.0/etc/schema-registry/connect-avro-distributed.properties
  4. Standard: /data/confluent/confluent-6.2.0/etc/schema-registry/connect-avro-standalone.properties
  5. Based on CONFLUENT_CURRENT:
/tmp/confluent.406980/connect/connect.properties
  6. Used by Connect process with PID 15904:
/tmp/confluent.406980/connect/connect.properties
Do you want to update all detected configs? (yN) y
Adding installation directory to plugin path in the following files:
  /data/confluent/confluent-6.2.0/etc/kafka/connect-distributed.properties
  /data/confluent/confluent-6.2.0/etc/kafka/connect-standalone.properties
  /data/confluent/confluent-6.2.0/etc/schema-registry/connect-avro-distributed.properties
  /data/confluent/confluent-6.2.0/etc/schema-registry/connect-avro-standalone.properties
  /tmp/confluent.406980/connect/connect.properties
  /tmp/confluent.406980/connect/connect.properties
```

```
Completed
```

```
root@stlrx2540m1-108:/data/confluent/confluent-6.2.0/bin#
```

You can also install a specific version by using `confluent-hub install confluentinc/kafka-connect-s3:10.0.3`.

9. By default, `confluentinc-kafka-connect-s3` is installed in `/data/confluent/confluent-6.2.0/share/confluent-hub-components/confluentinc-kafka-connect-s3`.
10. Update the plug-in path with the new `confluentinc-kafka-connect-s3`.

```
root@stlrx2540m1-108:~# cat /data/confluent/confluent-6.2.0/etc/kafka/connect-distributed.properties | grep plugin.path
#
plugin.path=/usr/local/share/java,/usr/local/share/kafka/plugins,/opt/connectors,
plugin.path=/usr/share/java,/data/zookeeper/confluent/confluent-6.2.0/share/confluent-hub-components,/data/confluent/confluent-6.2.0/share/confluent-hub-components,/data/confluent/confluent-6.2.0/share/confluent-hub-components/confluentinc-kafka-connect-s3
root@stlrx2540m1-108:~#
```

11. Stop the Confluent services and restart them.

```
confluent local services stop
confluent local services start
root@stlrx2540m1-108:/data/confluent/confluent-6.2.0/bin# confluent local services status
The local commands are intended for a single-node development environment only,
NOT for production usage.
```

```
Using CONFLUENT_CURRENT: /tmp/confluent.406980
Connect is [UP]
Control Center is [UP]
Kafka is [UP]
Kafka REST is [UP]
ksqlDB Server is [UP]
Schema Registry is [UP]
ZooKeeper is [UP]
root@stlrx2540m1-108:/data/confluent/confluent-6.2.0/bin#
```

12. Configure the access ID and secret key in the `/root/.aws/credentials` file.

```
root@stlrx2540m1-108:~# cat /root/.aws/credentials
[default]
aws_access_key_id = xxxxxxxxxxxxxxxx
aws_secret_access_key = xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
root@stlrx2540m1-108:~#
```

13. Verify that the bucket is reachable.

```
root@stlrx2540m4-01:~# aws s3 --endpoint-url
http://kafkasgd.rtppe.netapp.com:10444 ls kafkasgdbucket1-2
2021-10-29 21:04:18      1388 1
2021-10-29 21:04:20      1388 2
2021-10-29 21:04:22      1388 3
root@stlrx2540m4-01:~#
```

14. Configure the s3-sink properties file for s3 and bucket configuration.

```
root@stlrx2540m1-108:~# cat /data/confluent/confluent-
6.2.0/share/confluent-hub-components/confluentinc-kafka-connect-
s3/etc/quickstart-s3.properties | grep -v ^#
name=s3-sink
connector.class=io.confluent.connect.s3.S3SinkConnector
tasks.max=1
topics=s3_testtopic
s3.region=us-west-2
s3.bucket.name=kafkasgdbucket1-2
store.url=http://kafkasgd.rtppe.netapp.com:10444/
s3.part.size=5242880
flush.size=3
storage.class=io.confluent.connect.s3.storage.S3Storage
format.class=io.confluent.connect.s3.format.avro.AvroFormat
partitioner.class=io.confluent.connect.storage.partition.DefaultPartitioner
schema.compatibility=NONE
root@stlrx2540m1-108:~#
```

15. Import a few records to the s3 bucket.

```
kafka-console-producer --broker-list localhost:9092 --topic  
s3_topic \  
--property  
value.schema='{"type":"record","name":"myrecord","fields":[{"name":"f1",  
"type":"string"}]}'  
{"f1": "value1"}  
{"f1": "value2"}  
{"f1": "value3"}  
{"f1": "value4"}  
{"f1": "value5"}  
{"f1": "value6"}  
{"f1": "value7"}  
{"f1": "value8"}  
{"f1": "value9"}
```

16. Load the s3-sink connector.

```
root@stlrx2540m1-108:~# confluent local services connect connector load
s3-sink --config /data/confluent/confluent-6.2.0/share/confluent-hub-
components/confluentinc-kafka-connect-s3/etc/quickstart-s3.properties
The local commands are intended for a single-node development
environment only,
NOT for production usage.
https://docs.confluent.io/current/cli/index.html
{
  "name": "s3-sink",
  "config": {
    "connector.class": "io.confluent.connect.s3.S3SinkConnector",
    "flush.size": "3",
    "format.class": "io.confluent.connect.s3.format.avro.AvroFormat",
    "partitioner.class":
      "io.confluent.connect.storage.partition.DefaultPartitioner",
    "s3.bucket.name": "kafkasgdbucket1-2",
    "s3.part.size": "5242880",
    "s3.region": "us-west-2",
    "schema.compatibility": "NONE",
    "storage.class": "io.confluent.connect.s3.storage.S3Storage",
    "store.url": "http://kafkasgd.rtppe.netapp.com:10444/",
    "tasks.max": "1",
    "topics": "s3_testtopic",
    "name": "s3-sink"
  },
  "tasks": [],
  "type": "sink"
}
root@stlrx2540m1-108:~#
```

## 17. Check the s3-sink status.

```
root@stlrx2540m1-108:~# confluent local services connect connector
status s3-sink
The local commands are intended for a single-node development
environment only,
NOT for production usage.
https://docs.confluent.io/current/cli/index.html
{
  "name": "s3-sink",
  "connector": {
    "state": "RUNNING",
    "worker_id": "10.63.150.185:8083"
  },
  "tasks": [
    {
      "id": 0,
      "state": "RUNNING",
      "worker_id": "10.63.150.185:8083"
    }
  ],
  "type": "sink"
}
root@stlrx2540m1-108:~#
```

18. Check the log to make sure that s3-sink is ready to accept topics.

```
root@stlrx2540m1-108:~# confluent local services connect log
```

19. Check the topics in Kafka.

```
kafka-topics --list --bootstrap-server localhost:9092
...
connect-configs
connect-offsets
connect-statuses
default_ksql_processing_log
s3_testtopic
s3_topic
s3_topic_new
root@stlrx2540m1-108:~#
```

20. Check the objects in the s3 bucket.

```
root@stlrx2540m1-108:~# aws s3 --endpoint-url
http://kafkasgd.rtppe.netapp.com:10444 ls --recursive kafkasgdbucket1-
2/topics/
2021-10-29 21:24:00      213
topics/s3_testtopic/partition=0/s3_testtopic+0+0000000000.avro
2021-10-29 21:24:00      213
topics/s3_testtopic/partition=0/s3_testtopic+0+0000000003.avro
2021-10-29 21:24:00      213
topics/s3_testtopic/partition=0/s3_testtopic+0+0000000006.avro
2021-10-29 21:24:08      213
topics/s3_testtopic/partition=0/s3_testtopic+0+0000000009.avro
2021-10-29 21:24:08      213
topics/s3_testtopic/partition=0/s3_testtopic+0+0000000012.avro
2021-10-29 21:24:09      213
topics/s3_testtopic/partition=0/s3_testtopic+0+0000000015.avro
root@stlrx2540m1-108:~#
```

21. To verify the contents, copy each file from S3 to your local filesystem by running the following command:

```
root@stlrx2540m1-108:~# aws s3 --endpoint-url
http://kafkasgd.rtppe.netapp.com:10444 cp s3://kafkasgdbucket1-
2/topics/s3_testtopic/partition=0/s3_testtopic+0+0000000000.avro
tes.avro
download: s3://kafkasgdbucket1-
2/topics/s3_testtopic/partition=0/s3_testtopic+0+0000000000.avro to
./tes.avro
root@stlrx2540m1-108:~#
```

22. To print the records, use avro-tools-1.11.0.1.jar (available in the [Apache Archives](#)).

```
root@stlrx2540m1-108:~# java -jar /usr/src/avro-tools-1.11.0.1.jar
tojson tes.avro
21/10/30 00:20:24 WARN util.NativeCodeLoader: Unable to load native-
hadoop library for your platform... using builtin-java classes where
applicable
{"f1":"value1"}
{"f1":"value2"}
{"f1":"value3"}
root@stlrx2540m1-108:~#
```

[Next: Confluent self-rebalancing clusters.](#)

## Confluent Self-balancing Clusters

[Previous: Kafka s3 connector.](#)

If you have managed a Kafka cluster before, you are likely familiar with the challenges that come with manually reassigning partitions to different brokers to make sure that the workload is balanced across the cluster. For organizations with large Kafka deployments, reshuffling large amounts of data can be daunting, tedious, and risky, especially if mission-critical applications are built on top of the cluster. However, even for the smallest Kafka use cases, the process is time consuming and prone to human error.

In our lab, we tested the Confluent self-balancing clusters feature, which automates rebalancing based on cluster topology changes or uneven load. The Confluent rebalance test helps to measure the time to add a new broker when node failure or the scaling node requires rebalancing data across brokers. In classic Kafka configurations, the amount of data to be rebalanced grows as the cluster grows, but, in tiered storage, rebalancing is restricted to a small amount of data. Based on our validation, rebalancing in tiered storage takes seconds or minutes in a classic Kafka architecture and grows linearly as the cluster grows.

In self-balancing clusters, partition rebalances are fully automated to optimize Kafka's throughput, accelerate broker scaling, and reduce the operational burden of running a large cluster. At steady-state, self-balancing clusters monitor the skew of data across the brokers and continuously reassigned partitions to optimize cluster performance. When scaling the platform up or down, self-balancing clusters automatically recognize the presence of new brokers or the removal of old brokers and trigger a subsequent partition reassignment. This enables you to easily add and decommission brokers, making your Kafka clusters fundamentally more elastic. These benefits come without any need for manual intervention, complex math, or the risk of human error that partition reassessments typically entail. As a result, data rebalances are completed in far less time, and you are free to focus on higher-value event-streaming projects rather than needing to constantly supervise your clusters.

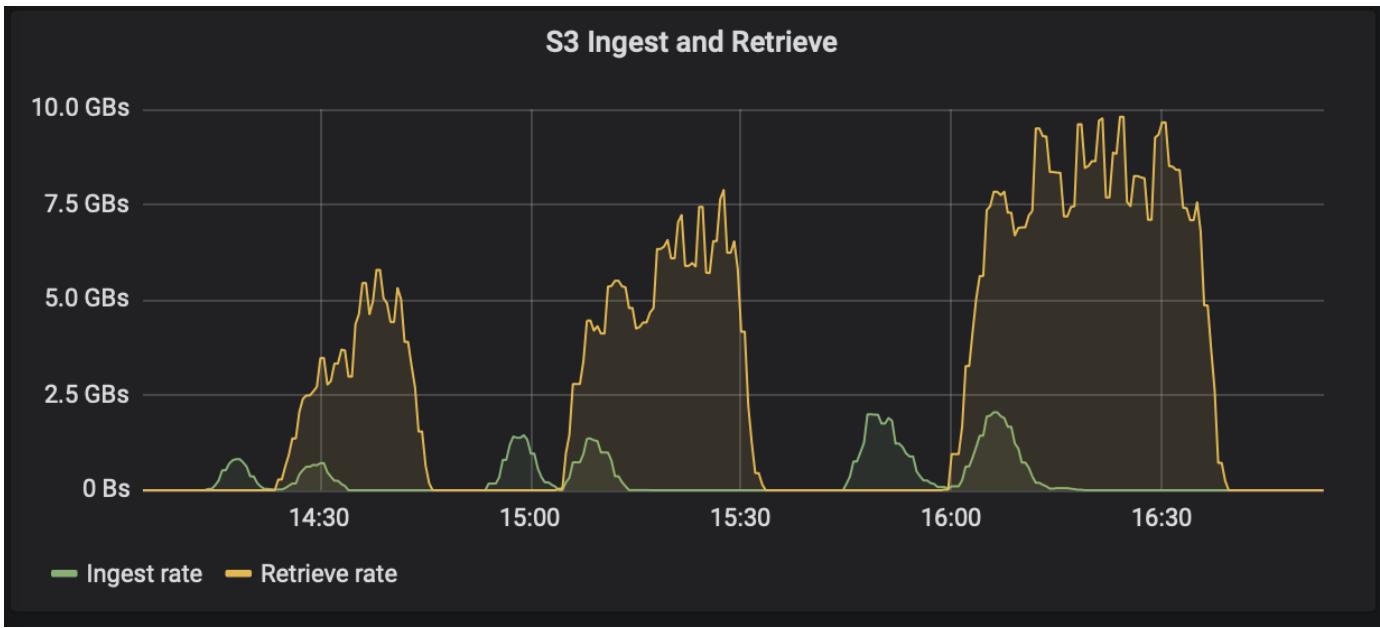
[Next: Best practice guidelines.](#)

## Best practice guidelines

[Previous: Confluent self-rebalancing clusters.](#)

- Based on our validation, S3 object storage is best for Confluent to keep data.
- We can use high-throughput SAN (specifically FC) to keep the broker hot data or local disk, because, in the Confluent tiered storage configuration, the size of the data held in the brokers data directory is based on the segment size and retention time when the data is moved to object storage.
- Object stores provide better performance when segment.bytes is higher; we tested 512MB.
- In Kafka, the length of the key or value (in bytes) for each record produced to the topic is controlled by the length.key.value parameter. For StorageGRID, S3 object ingest and retrieve performance increased to higher values. For example, 512 bytes provided a 5.8GBps retrieve, 1024 bytes provided a 7.5GBps s3 retrieve, and 2048 bytes provided close to 10GBps.

The following figure presents the S3 object ingest and retrieve based on length.key.value.



- **Kafka tuning.** To improve the performance of tiered storage, you can increase `TierFetcherNumThreads` and `TierArchiverNumThreads`. As a general guideline, you want to increase `TierFetcherNumThreads` to match the number of physical CPU cores and increase `TierArchiverNumThreads` to half the number of CPU cores. For example, in server properties, if you have a machine with eight physical cores, set `confluent.tier.fetcher.num.threads = 8` and `confluent.tier.archiver.num.threads = 4`.
- **Time interval for topic deletes.** When a topic is deleted, deletion of the log segment files in object storage does not immediately begin. Rather, there is a time interval with a default value of 3 hours before deletion of those files takes place. You can modify the configuration, `confluent.tier.topic.delete.check.interval.ms`, to change the value of this interval. If you delete a topic or cluster, you can also manually delete the objects in the respective bucket.
- **ACLs on tiered storage internal topics.** A recommended best practice for on-premises deployments is to enable an ACL authorizer on the internal topics used for tiered storage. Set ACL rules to limit access on this data to the broker user only. This secures the internal topics and prevents unauthorized access to tiered storage data and metadata.

```
kafka-acls --bootstrap-server localhost:9092 --command-config adminclient-configs.conf \
--add --allow-principal User:<kafka> --operation All --topic "_confluent-tier-state"
```



Replace the user `<kafka>` with the actual broker principal in your deployment.

For example, the command `confluent-tier-state` sets ACLs on the internal topic for tiered storage. Currently, there is only a single internal topic related to tiered storage. The example creates an ACL that provides the principal Kafka permission for all operations on the internal topic.

[Next: Sizing.](#)

## Sizing

[Previous: Best practice guidelines.](#)

Kafka sizing can be performed with four configuration modes: simple, granular, reverse, and partitions.

## Simple

The simple mode is appropriate for the first-time Apache Kafka users or early state use cases. For this mode, you provide requirements such as throughput MBps, read fanout, retention, and the resource utilization percentage (60% is default). You also enter the environment, such as on-premises (bare-metal, VMware, Kubernetes, or OpenStack) or cloud. Based on this information, the sizing of a Kafka cluster provides the number of servers required for the broker, the zookeeper, Apache Kafka connect workers, the schema registry, a REST Proxy, ksqlDB, and the Confluent control center.

For tiered storage, consider the granular configuration mode for sizing a Kafka cluster. Granular mode is appropriate for experienced Apache Kafka users or well-defined use cases. This section describes sizing for producers, stream processors, and consumers.

### Producers

To describe the producers for Apache Kafka (for example a native client, REST proxy, or Kafka connector), provide the following information:

- **Name.** Spark.
- **Producer type.** Application or service, proxy (REST, MQTT, other), and existing database (RDBMS, NOSQL, other). You can also select "I don't know."
- **Average throughput.** In events per second (1,000,000 for example).
- **Peak throughput.** In events per second (4,000,000 for example).
- **Average message size.** In bytes, uncompressed (max 1MB; 1000 for example).
- **Message format.** Options include Avro, JSON, protocol buffers, binary, text, "I don't know," and other.
- **Replication factor.** Options are 1, 2, 3 (Confluent recommendation), 4, 5, or 6.
- **Retention time.** One day (for example). How long do you want your data to be stored in Apache Kafka? Enter -1 with any unit for an infinite time. The calculator assumes a retention time of 10 years for infinite retention.
- Select the check box for "Enable Tiered Storage to Decrease Broker Count and Allow for Infinite Storage?"
- When tiered storage is enabled, the retention fields control the hot set of data that is stored locally on the broker. The archival retention fields control how long data is stored in archival object storage.
- **Archival Storage Retention.** One year (for example). How long do you want your data to be stored in archival storage? Enter -1 with any unit for an infinite duration. The calculator assumes a retention of 10 years for infinite retention.
- **Growth Multiplier.** 1 (for example). If the value of this parameter is based on current throughput, set it to 1. To size based on additional growth, set this parameter to a growth multiplier.
- **Number of producer instances.** 10 (for example). How many producer instances will be running? This input is required to incorporate the CPU load into the sizing calculation. A blank value indicates that CPU load is not incorporated into the calculation.

Based on this example input, sizing has the following effect on producers:

- Average throughput in uncompressed bytes: 1GBps. Peak throughput in uncompressed bytes: 4GBps. Average throughput in compressed bytes: 400MBps. Peak throughput in compressed bytes: 1.6GBps. This is based on a default 60% compression rate (you can change this value).

- Total on-broker hotset storage required: 31,104TB, including replication, compressed. Total off-broker archival storage required: 378,432TB, compressed. Use <https://fusion.netapp.com> for StorageGRID sizing.

Stream Processors must describe their applications or services that consume data from Apache Kafka and produce back into Apache Kafka. In most cases these are built in ksqlDB or Kafka Streams.

- **Name.** Spark streamer.
  - **Processing time.** How long does this processor take to process a single message?
    - 1 ms (simple, stateless transformation) [example], 10ms (stateful in-memory operation).
    - 100ms (stateful network or disk operation), 1000ms (3rd party REST call).
    - I have benchmarked this parameter and know exactly how long it takes.
  - **Output Retention.** 1 day (example). A stream processor produces its output back to Apache Kafka. How long do you want this output data to be stored in Apache Kafka? Enter -1 with any unit for an infinite duration.
  - Select the check box "Enable Tiered Storage to Decrease Broker Count and Allow for Infinite Storage?"
  - **Archival Storage Retention.** 1 year (for example). How long do you want your data to be stored in archival storage? Enter -1 with any unit for an infinite duration. The calculator assumes a retention of 10 years for infinite retention.
  - **Output Passthrough Percentage.** 100 (for example). A stream processor produces its output back to Apache Kafka. What percentage of inbound throughput will be outputted back into Apache Kafka? For example, if inbound throughput is 20MBps and this value is 10, the output throughput will be 2MBps.
  - From which applications does this read from? Select “Spark,” the name used in producer type-based sizing.  
Based on the above input, you can expect the following effects of sizing on stream processor instances and topic partition estimates:
- This stream processor application requires the following number of instances. The incoming topics likely require this many partitions as well. Contact Confluent to confirm this parameter.
    - 1,000 for average throughput with no growth multiplier
    - 4,000 for peak throughput with no growth multiplier
    - 1,000 for average throughput with a growth multiplier
    - 4,000 for peak throughput with a growth multiplier

## Consumers

Describe your applications or services that consume data from Apache Kafka and do not produce back into Apache Kafka; for example, a native client or Kafka Connector.

- **Name.** Spark consumer.
- **Processing time.** How long does this consumer take to process a single message?
  - 1ms (for example, a simple and stateless task like logging)
  - 10ms (fast writes to a datastore)
  - 100ms (slow writes to a datastore)
  - 1000ms (third party REST call)
  - Some other benchmarked process of known duration.

- **Consumer type.** Application, proxy, or sink to an existing datastore (RDBMS, NoSQL, other).
- From which applications does this read from? Connect this parameter with producer and stream sizing determined previously.

Based on the above input, you must determine the sizing for consumer instances and topic partition estimates. A consumer application requires the following number of instances.

- 2,000 for average throughput, no growth multiplier
- 8,000 for peak throughput, no growth multiplier
- 2,000 for average throughput, including growth multiplier
- 8,000 for peak throughput, including growth multiplier

The incoming topics likely need this number of partitions as well. Contact Confluent to confirm.

In addition to the requirements for producers, stream processors, and consumers, you must provide the following additional requirements:

- **Rebuild time.** For example, 4 hours. If an Apache Kafka broker host fails, its data is lost, and a new host is provisioned to replace the failed host, how fast must this new host rebuild itself? Leave this parameter blank if the value is unknown.
- **Resource utilization target (percentage).** For example, 60. How utilized do you want your hosts to be during average throughput? Confluent recommends 60% utilization unless you are using Confluent self-balancing clusters, in which case utilization can be higher.

#### Describe your environment

- **What environment will your cluster be running in?** Amazon Web Services, Microsoft Azure, Google cloud platform, bare-metal on premises, VMware on premises, OpenStack on premises, or Kubernetes on premises?
- **Host details.** Number of cores: 48 (for example), network card type (10GbE, 40GbE, 16GbE, 1GbE, or another type).
- **Storage volumes.** Host: 12 (for example). How many hard drives or SSDs are supported per host? Confluent recommends 12 hard drives per host.
- **Storage capacity/volume (in GB).** 1000 (for example). How much storage can a single volume store in gigabytes? Confluent recommends 1TB disks.
- **Storage configuration.** How are storage volumes configured? Confluent recommends RAID10 to take advantage of all Confluent features. JBOD, SAN, RAID 1, RAID 0, RAID 5, and other types are also supported.
- **Single volume throughput (MBps).** 125 (for example). How fast can a single storage volume read or write in megabytes per second? Confluent recommends standard hard drives, which typically have 125MBps throughput.
- **Memory capacity (GB).** 64 (for example).

After you have determined your environmental variables, select Size my Cluster. Based on the example parameters indicated above, we determined the following sizing for Confluent Kafka:

- **Apache Kafka.** Broker count: 22. Your cluster is storage-bound. Consider enabling tiered storage to decrease your host count and allow for infinite storage.
- **Apache ZooKeeper.** Count: 5; Apache Kafka Connect Workers: Count: 2; Schema Registry: Count: 2;

REST Proxy: Count: 2; ksqlDB: Count: 2; Confluent Control Center: Count: 1.

Use reverse mode for platform teams without a use case in mind. Use partitions mode to calculate how many partitions a single topic requires. See <https://eventsizer.io> for sizing based on the reverse and partitions modes.

Next: Conclusion.

## Conclusion

Previous: Sizing.

This document provides best practice guidelines for using Confluent Tiered Storage with NetApp storage, including verification tests, tiered storage performance results, tuning, Confluent S3 connectors, and the self-balancing feature. Considering ILM policies, Confluent performance with multiple performance tests for verification, and industry-standard S3 APIs, NetApp StorageGRID object storage is an optimal choice for Confluent tiered storage.

## Where to find additional information

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

- What is Apache Kafka

<https://www.confluent.io/what-is-apache-kafka/>

- NetApp Product Documentation

<https://www.netapp.com/support-and-training/documentation/>

- S3-sink parameter details

[https://docs.confluent.io/kafka-connect-s3-sink/current/configuration\\_options.html#s3-configuration-options](https://docs.confluent.io/kafka-connect-s3-sink/current/configuration_options.html#s3-configuration-options)

- Apache Kafka

[https://en.wikipedia.org/wiki/Apache\\_Kafka](https://en.wikipedia.org/wiki/Apache_Kafka)

- Infinite Storage in Confluent Platform

<https://www.confluent.io/blog/infinite-kafka-storage-in-confluent-platform/>

- Confluent Tiered Storage - Best practices and sizing

<https://docs.confluent.io/platform/current/kafka/tiered-storage.html#best-practices-and-recommendations>

- Amazon S3 sink connector for Confluent Platform

<https://docs.confluent.io/kafka-connect-s3-sink/current/overview.html>

- Kafka sizing

<https://eventsizer.io>

- StorageGRID sizing

<https://fusion.netapp.com/>

- Kafka use cases

<https://kafka.apache.org/uses>

- Self-balancing Kafka clusters in confluent platform 6.0

<https://www.confluent.io/blog/self-balancing-kafka-clusters-in-confluent-platform-6-0/>

<https://www.confluent.io/blog/confluent-platform-6-0-delivers-the-most-powerful-event-streaming-platform-to-date/>

## Version history

Version	Date	Document version history
Version 1.0	December 2021	Initial release.

# NetApp hybrid cloud data solutions - Spark and Hadoop based on customer use cases

## TR-4657: NetApp hybrid cloud data solutions - Spark and Hadoop based on customer use cases

Karthikeyan Nagalingam and Sathish Thyagarajan, NetApp

This document describes hybrid cloud data solutions using NetApp AFF and FAS storage systems, NetApp Cloud Volumes ONTAP, NetApp connected storage, and NetApp FlexClone technology for Spark and Hadoop. These solution architectures allow customers to choose an appropriate data protection solution for their environment. NetApp designed these solutions based on interaction with customers and their business use-cases. This document provides the following detailed information:

- Why we need data protection for Spark and Hadoop environments and customer challenges.
- The data fabric powered by NetApp vision and its building blocks and services.
- How these building blocks can be used to architect flexible data protection workflows.
- The pros and cons of several architectures based on real-world customer use cases. Each use case provides the following components:
  - Customer scenarios
  - Requirements and challenges
  - Solutions
  - Summary of the solutions

## Why Hadoop data protection?

In a Hadoop and Spark environment, the following concerns must be addressed:

- **Software or human failures.** Human error in software updates while carrying out Hadoop data operations can lead to faulty behavior that can cause unexpected results from the job. In such case, we need to protect the data to avoid failures or unreasonable outcomes. For example, as the result of a poorly

executed software update to a traffic signal analysis application, a new feature that fails to properly analyze traffic signal data in the form of plain text. The software still analyzes JSON and other non-text file formats, resulting in the real-time traffic control analytics system producing prediction results that are missing data points. This situation can cause faulty outputs that might lead to accidents at the traffic signals. Data protection can address this issue by providing the capability to quickly roll back to the previous working application version.

- **Size and scale.** The size of the analytics data grows day by day due to the ever-increasing numbers of data sources and volume. Social media, mobile apps, data analytics, and cloud computing platforms are the main sources of data in the current big data market, which is increasing very rapidly, and therefore the data needs to be protected to ensure accurate data operations.
- **Hadoop's native data protection.** Hadoop has a native command to protect the data, but this command does not provide consistency of data during backup. It only supports directory-level backup. The snapshots created by Hadoop are read-only and cannot be used to reuse the backup data directly.

### **Data protection challenges for Hadoop and Spark customers**

A common challenge for Hadoop and Spark customers is to reduce the backup time and increase backup reliability without negatively affecting performance at the production cluster during data protection.

Customers also need to minimize recovery point objective (RPO) and recovery time objective (RTO) downtime and control their on-premises and cloud-based disaster recovery sites for optimal business continuity. This control typically comes from having enterprise-level management tools.

The Hadoop and Spark environments are complicated because not only is the data volume huge and growing, but the rate this data arrives is increasing. This scenario makes it difficult to rapidly create efficient, up-to-date DevTest and QA environments from the source data. NetApp recognizes these challenges and offers the solutions presented in this paper.

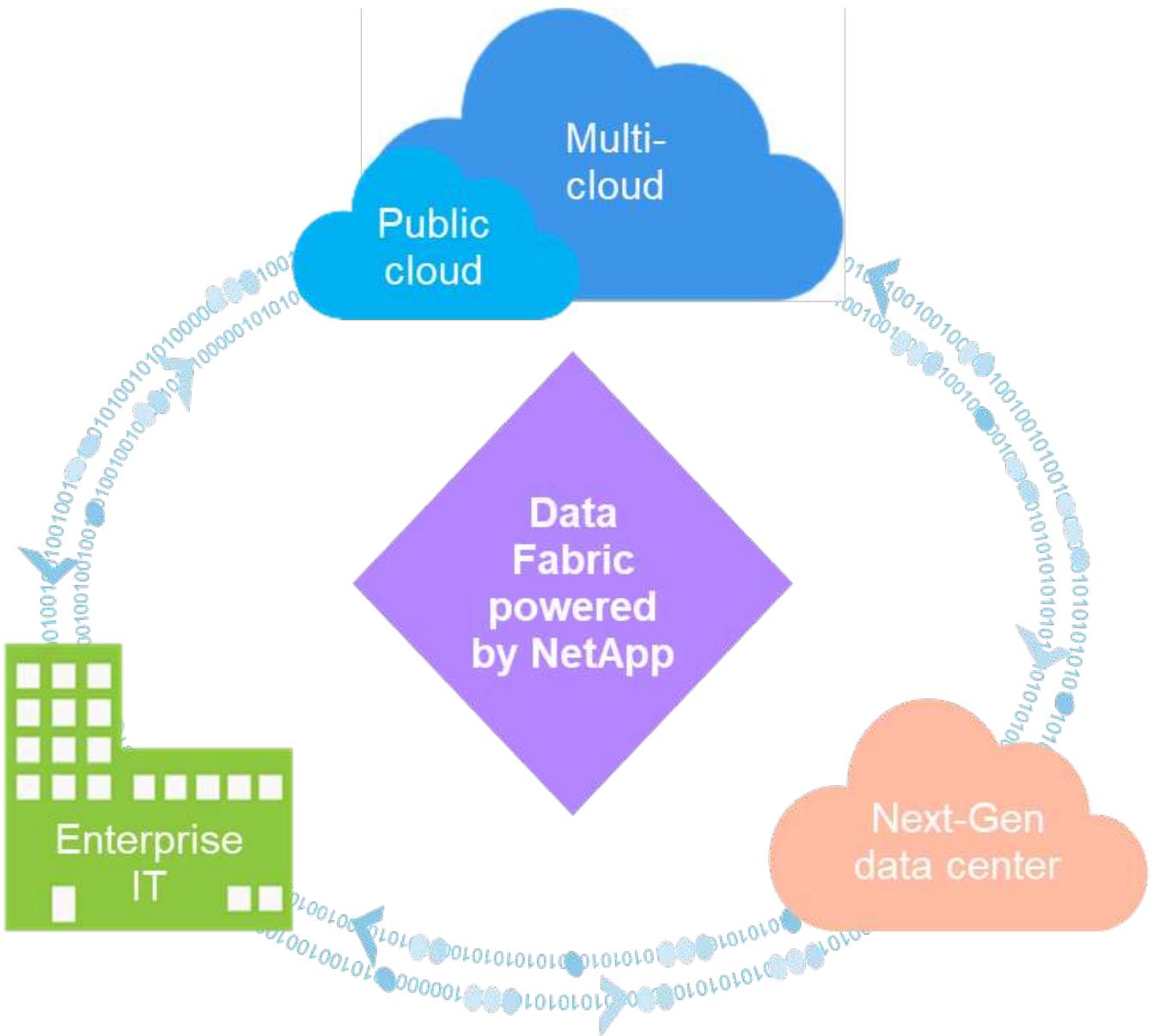
[Next: Data fabric powered by NetApp for big data architecture.](#)

### **Data fabric powered by NetApp for big data architecture**

[Previous: Solution overview.](#)

The data fabric powered by NetApp simplifies and integrates data management across cloud and on-premises environments to accelerate digital transformation.

The data fabric powered by NetApp delivers consistent and integrated data management services and applications (building blocks) for data visibility and insights, data access and control, and data protection and security, as shown in the figure below.



### Proven data fabric customer use cases

The data fabric powered by NetApp provides the following nine proven use cases for customers:

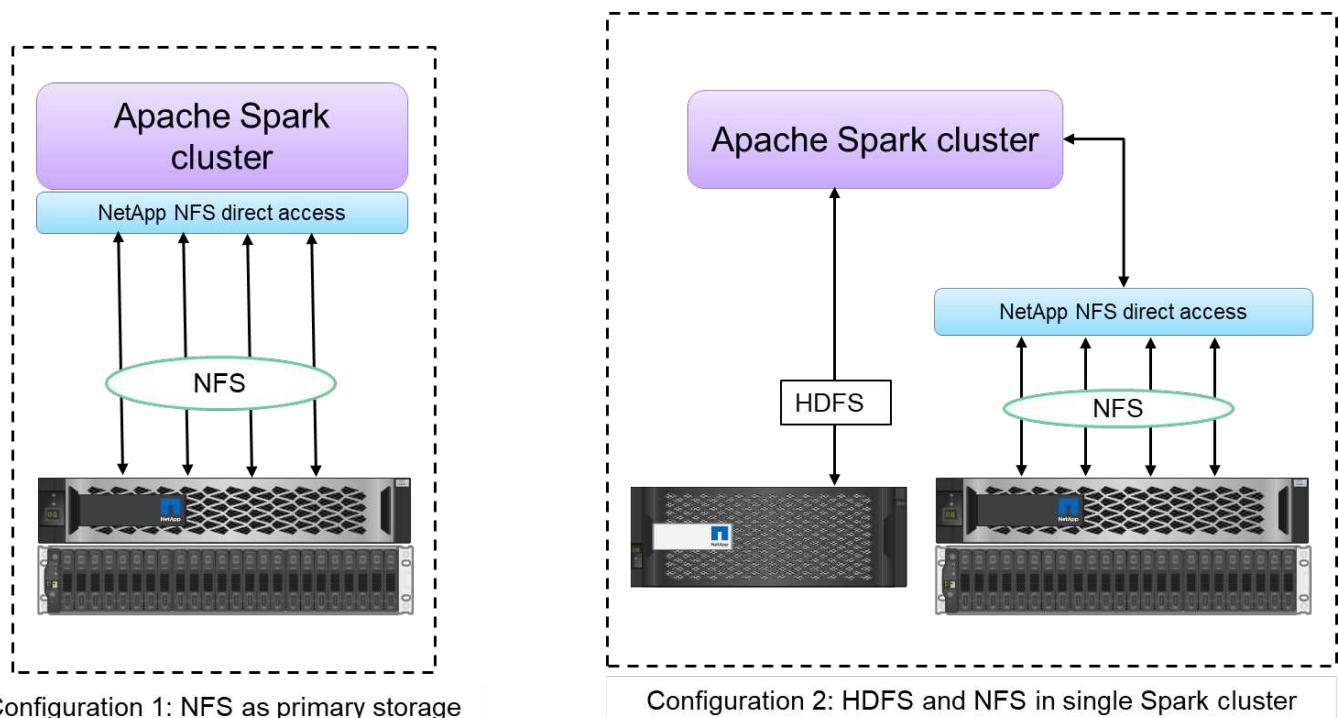
- Accelerate analytics workloads
- Accelerate DevOps transformation
- Build cloud hosting infrastructure
- Integrate cloud data services
- Protect and secure data
- Optimize unstructured data
- Gain data center efficiencies
- Deliver data insights and control
- Simplify and automate

This document covers two of the nine use cases (along with their solutions):

- Accelerate analytics workloads
- Protect and secure data

#### NetApp NFS direct access

The NetApp NFS direct access (formerly known as NetApp In-Place Analytics Module) (shown in the figure below) allows customers to run big data analytics jobs on their existing or new NFSv3 or NFSv4 data without moving or copying the data. It prevents multiple copies of data and eliminates the need to sync the data with a source. For example, in the financial sector, the movement of data from one place to another place must meet legal obligations, which is not an easy task. In this scenario, the NetApp NFS direct access analyzes the financial data from its original location. Another key benefit is that using the NetApp NFS direct access simplifies protecting Hadoop data by using native Hadoop commands and enables data protection workflows leveraging NetApp's rich data management portfolio.



The NetApp NFS direct access provides two kinds of deployment options for Hadoop/Spark clusters:

- By default, the Hadoop/Spark clusters use Hadoop Distributed File System (HDFS) for data storage and the default file system. The NetApp NFS direct access can replace the default HDFS with NFS storage as the default file system, enabling direct analytics operations on NFS data.
- In another deployment option, the NetApp NFS direct access supports configuring NFS as additional storage along with HDFS in a single Hadoop/Spark cluster. In this case, the customer can share data through NFS exports and access it from the same cluster along with HDFS data.

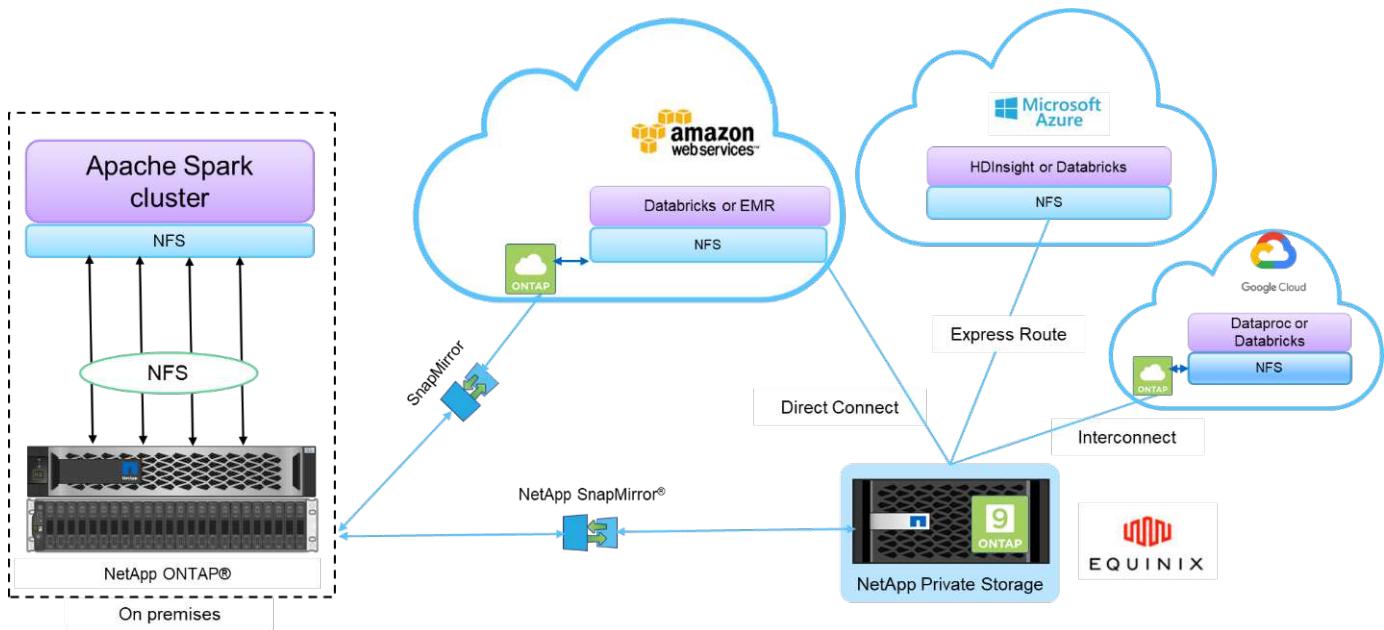
The key benefits of using the NetApp NFS direct access include:

- Analyzes the data from its current location, which prevents the time- and performance-consuming task of moving analytics data to a Hadoop infrastructure such as HDFS.
- Reduces the number of replicas from three to one.
- Enables users to decouple the compute and storage to scale them independently.
- Provides enterprise data protection by leveraging the rich data management capabilities of ONTAP.

- Is certified with the Hortonworks data platform.
- Enables hybrid data analytics deployments.
- Reduces the backup time by leveraging dynamic multithread capability.

### Building blocks for big data

The data fabric powered by NetApp integrates data management services and applications (building blocks) for data access, control, protection, and security, as shown in the figure below.



The building blocks in the figure above include:

- **NetApp NFS direct access.** Provides the latest Hadoop and Spark clusters with direct access to NetApp NFS volumes without additional software or driver requirements.
- **NetApp Cloud Volumes ONTAP and Cloud Volume Services.** Software-defined connected storage based on ONTAP running in Amazon Web Services (AWS) or Azure NetApp Files (ANF) in Microsoft Azure cloud services.
- **NetApp SnapMirror technology.** Provides data protection capabilities between on-premises and ONTAP Cloud or NPS instances.
- **Cloud service providers.** These providers include AWS, Microsoft Azure, Google Cloud, and IBM Cloud.
- **PaaS.** Cloud-based analytics services such as Amazon Elastic MapReduce (EMR) and Databricks in AWS as well as Microsoft Azure HDInsight and Azure Databricks.

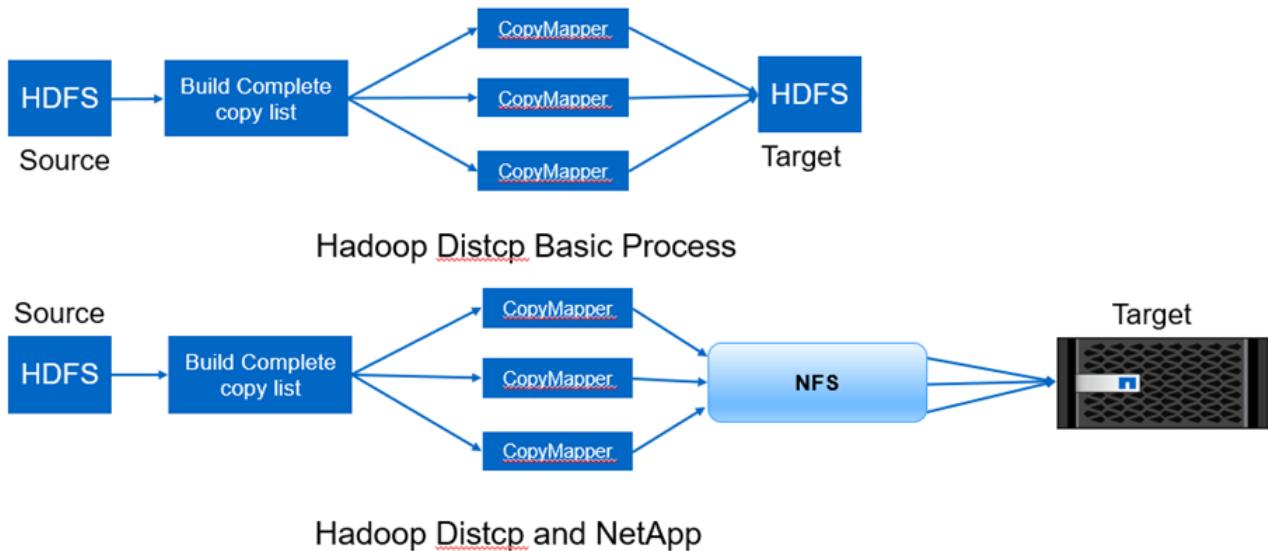
Next: [Hadoop data protection and NetApp](#).

## Hadoop data protection and NetApp

Previous: [Data fabric powered by NetApp for big data architecture](#).

Hadoop DistCp is a native tool used for large intercluster and intracluster copying. The Hadoop DistCp basic process shown in the figure below is a typical backup workflow using Hadoop native tools such as MapReduce to copy Hadoop data from an HDFS source to a corresponding target. The NetApp NFS direct access enables customers to set NFS as the target destination for the Hadoop DistCp tool to copy the data from HDFS source

into an NFS share through MapReduce. The NetApp NFS direct access acts as an NFS driver for the DistCp tool.



[Next: Overview of Hadoop data protection use cases.](#)

## Overview of Hadoop data protection use cases

[Previous: Hadoop data protection and NetApp.](#)

This section provides a high-level description of the data protection use cases, which constitute the focus of this paper. The remaining sections provide more details for each use case, such as the customer problem (scenario), requirements and challenges, and solutions.

### Use case 1: Backing up Hadoop data

For this use case, the In-Place Analytics Module helped a large financial institution reduce the long backup window time from more than 24 hours to just under a few hours.

### Use case 2: Backup and disaster recovery from the cloud to on-premises

By using the data fabric powered by NetApp as building blocks, a large broadcasting company was able to fulfill its requirement of backing up cloud data into its on-premise data center depending on the different modes of data transfers, such as on demand, instantaneous, or based on the Hadoop/Spark cluster load.

### Use case 3: Enabling DevTest on existing Hadoop data

NetApp solutions helped an online music distributor to rapidly build multiple space-efficient Hadoop clusters in different branches to create reports and run daily DevTest tasks by using scheduled policies.

### Use case 4: Data protection and multicloud connectivity

A large service provider used the data fabric powered by NetApp to provide multicloud analytics to its customers from different cloud instances.

## Use case 5: Accelerate analytic workloads

One of the largest financial services and investment banks used the NetApp network-attached storage solution to reduce I/O wait time and accelerate its quantitative financial analytics platform.

Next: Use case 1 - Backing up Hadoop data.

## Use case 1: Backing up Hadoop data

Previous: Overview of Hadoop data protection use cases.

### Scenario

In this scenario, the customer has a large on-premises Hadoop repository and wants to back it up for disaster recovery purposes. However, the customer's current backup solution is costly and is suffering from a long backup window of more than 24 hours.

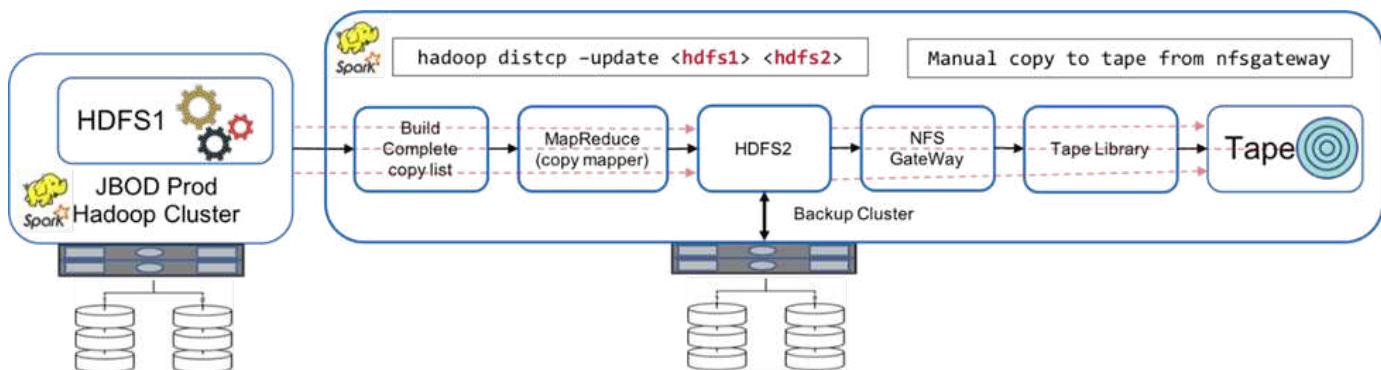
### Requirements and challenges

The main requirements and challenges for this use case include:

- Software backward compatibility:
  - The proposed alternative backup solution should be compatible with the current running software versions used in the production Hadoop cluster.
- To meet the committed SLAs, the proposed alternative solution should achieve very low RPOs and RTOs.
- The backup created by the NetApp backup solution can be used in the Hadoop cluster built locally in the data center as well as the Hadoop cluster running in the disaster recovery location at the remote site.
- The proposed solution must be cost effective.
- The proposed solution must reduce the performance effect on the currently running, in-production analytics jobs during the backup times.

### Customer's existing backup solution

The figure below shows the original Hadoop native backup solution.



The production data is protected to tape through the intermediate backup cluster:

- HDFS1 data is copied to HDFS2 by running the `hadoop distcp -update <hdfs1> <hdfs2>` command.
- The backup cluster acts as an NFS gateway, and the data is manually copied to tape through the Linux `cp`

command through the tape library.

The benefits of the original Hadoop native backup solution include:

- The solution is based on Hadoop native commands, which saves the user from having to learn new procedures.
- The solution leverages industry-standard architecture and hardware.

The disadvantages of the original Hadoop native backup solution include:

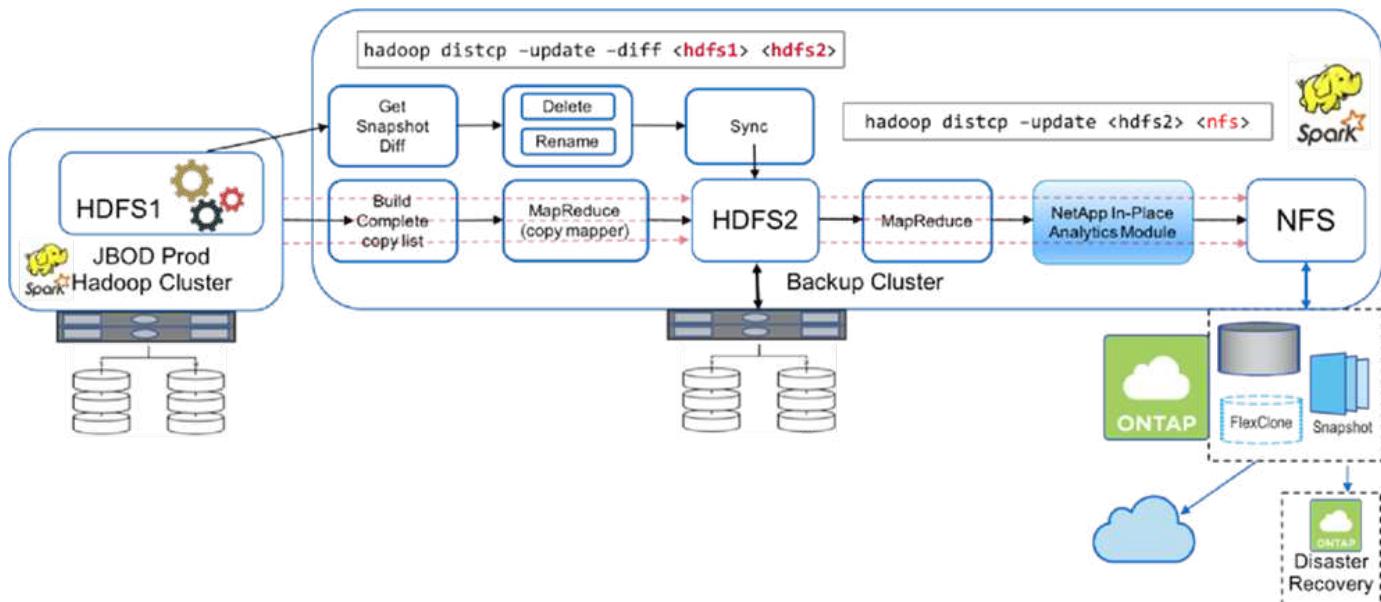
- The long backup window time exceeds 24 hours, which makes the production data vulnerable.
- Significant cluster performance degradation during backup times.
- Copying to tape is a manual process.
- The backup solution is expensive in terms of the hardware required and the human hours required for manual processes.

## Backup solutions

Based on these challenges and requirements, and taking into consideration the existing backup system, three possible backup solutions were suggested. The following subsections describe each of these three different backup solutions, labeled solution A through solution C.

### Solution A

Solution A adds the In-Place Analytics Module to the backup Hadoop cluster, which allows secondary backups to NetApp NFS storage systems, eliminating the tape requirement, as shown in the figure below.



The detailed tasks for solution A include:

- The production Hadoop cluster has the customer's analytics data in the HDFS that requires protection.
- The backup Hadoop cluster with HDFS acts as an intermediate location for the data. Just a bunch of disks (JBOD) provides the storage for HDFS in both the production and backup Hadoop clusters.
- Protect the Hadoop production data is protected from the production cluster HDFS to the backup cluster HDFS by running the Hadoop `distcp -update -diff <hdfs1> <hdfs2>` command.



The Hadoop snapshot is used to protect the data from production to the backup Hadoop cluster.

- The NetApp ONTAP storage controller provides an NFS exported volume, which is provisioned to the backup Hadoop cluster.
- By running the `Hadoop distcp` command leveraging MapReduce and multiple mappers, the analytics data is protected from the backup Hadoop cluster to NFS by using the In-Place Analytics Module.

After the data is stored in NFS on the NetApp storage system, NetApp Snapshot, SnapRestore, and FlexClone technologies are used to back up, restore, and duplicate the Hadoop data as needed.



Hadoop data can be protected to the cloud as well as disaster recovery locations by using SnapMirror technology.

The benefits of solution A include:

- Hadoop production data is protected from the backup cluster.
- HDFS data is protected through NFS enabling protection to cloud and disaster recovery locations.
- Improves performance by offloading backup operations to the backup cluster.
- Eliminates manual tape operations
- Allows for enterprise management functions through NetApp tools.
- Requires minimal changes to the existing environment.
- Is a cost-effective solution.

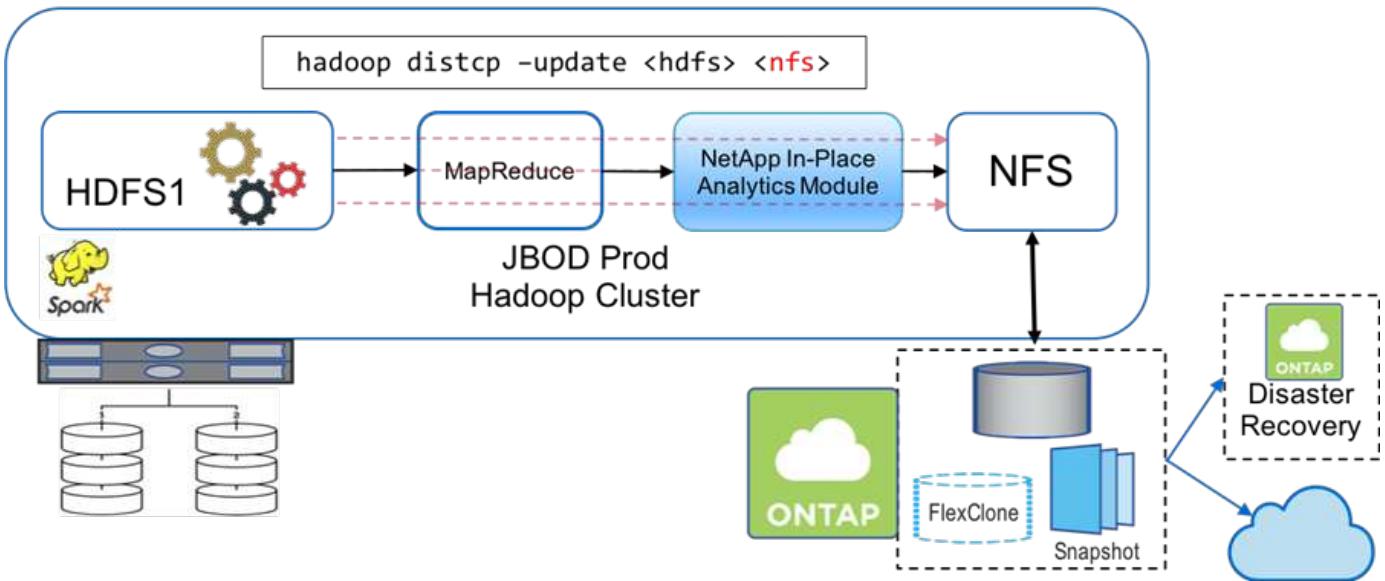
The disadvantage of this solution is that it requires a backup cluster and additional mappers to improve performance.

The customer recently deployed solution A due to its simplicity, cost, and overall performance.

In this solution, SAN disks from ONTAP can be used instead of JBOD. This option offloads the backup cluster storage load to ONTAP; however, the downside is that SAN fabric switches are required.

## Solution B

Solution B adds the In-Place Analytics Module to the production Hadoop cluster, which eliminates the need for the backup Hadoop cluster, as shown in the figure below.



The detailed tasks for solution B include:

- The NetApp ONTAP storage controller provisions the NFS export to the production Hadoop cluster. The Hadoop native `hadoop distcp` command protects the Hadoop data from the production cluster HDFS to NFS through the In-Place Analytics Module.
- After the data is stored in NFS on the NetApp storage system, Snapshot, SnapRestore, and FlexClone technologies are used to back up, restore, and duplicate the Hadoop data as needed.

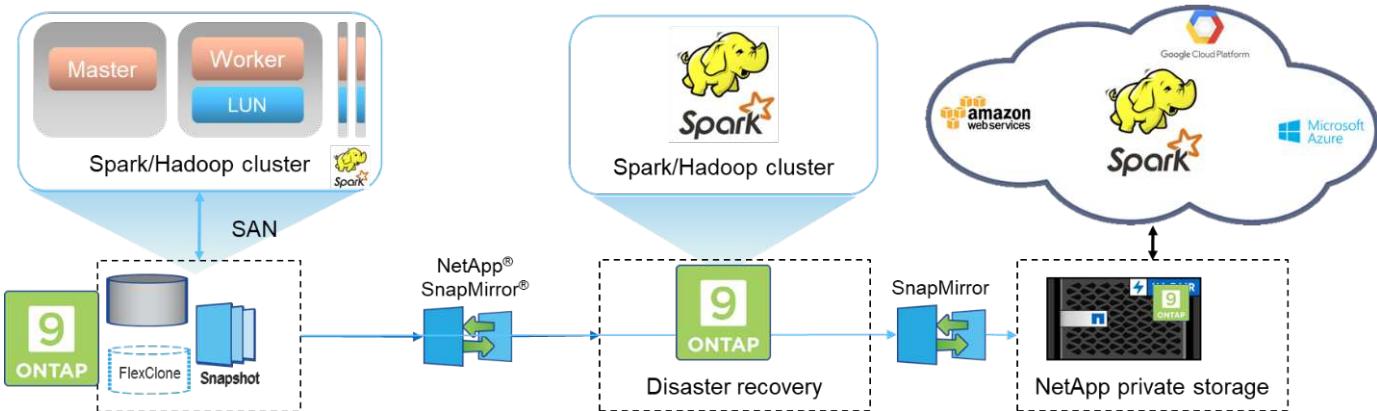
The benefits of solution B include:

- The production cluster is slightly modified for the backup solution, which simplifies implementation and reduces additional infrastructure cost.
- A backup cluster for the backup operation is not required.
- HDFS production data is protected in the conversion to NFS data.
- The solution allows for enterprise management functions through NetApp tools.

The disadvantage of this solution is that it's implemented in the production cluster, which can add additional administrator tasks in the production cluster.

### Solution C

In solution C, the NetApp SAN volumes are directly provisioned to the Hadoop production cluster for HDFS storage, as shown in the figure below.



The detailed steps for solution C include:

- NetApp ONTAP SAN storage is provisioned at the production Hadoop cluster for HDFS data storage.
- NetApp Snapshot and SnapMirror technologies are used to back up the HDFS data from the production Hadoop cluster.
- There is no performance effect to production for the Hadoop/Spark cluster during the Snapshot copy backup process because the backup is at the storage layer.



Snapshot technology provides backups that complete in seconds regardless of the size of the data.

The benefits of solution C include:

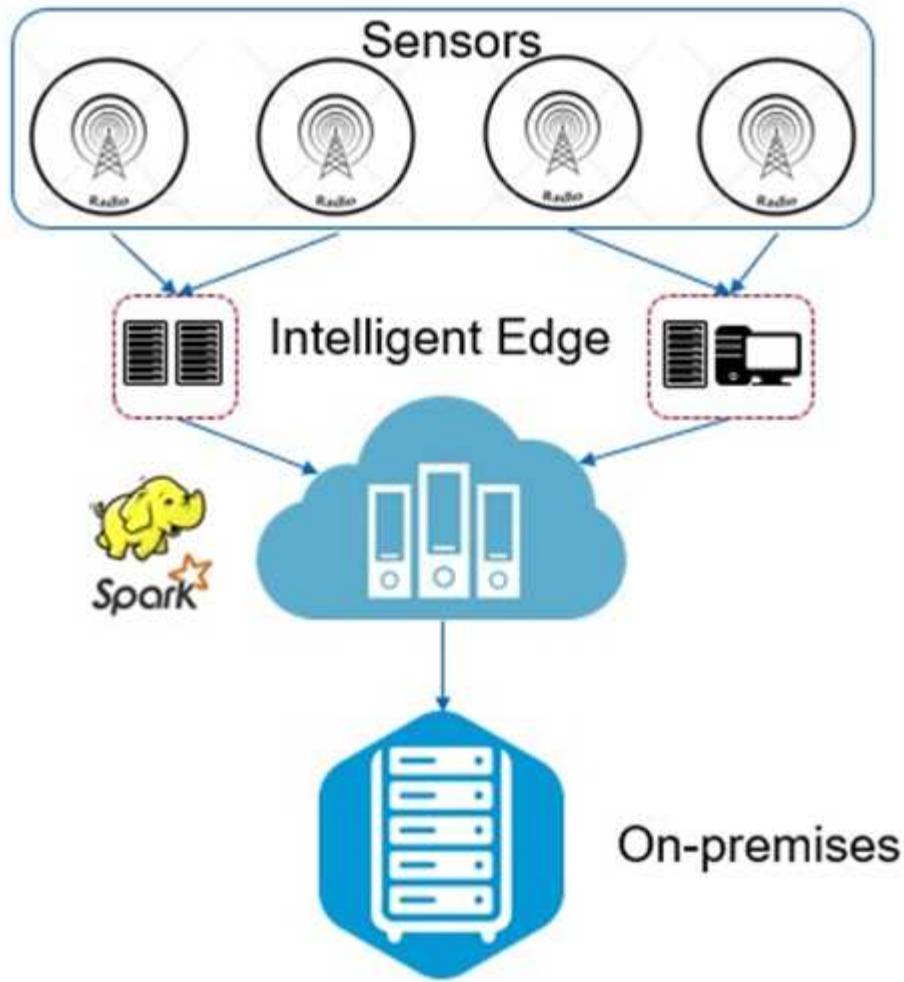
- Space-efficient backup can be created by using Snapshot technology.
- Allows for enterprise management functions through NetApp tools.

Next: [Use case 2 - Backup and disaster recovery from the cloud to on-premises](#).

## Use case 2: Backup and disaster recovery from the cloud to on-premises

[Previous: Use case 1 - Backing up Hadoop data.](#)

This use case is based on a broadcasting customer that needs to back up cloud-based analytics data to its on-premises data center, as illustrated in the figure below.



## Scenario

In this scenario, the IoT sensor data is ingested into the cloud and analyzed by using an open source Apache Spark cluster within AWS. The requirement is to back up the processed data from the cloud to on-premises.

## Requirements and challenges

The main requirements and challenges for this use case include:

- Enabling data protection should not cause any performance effect on the production Spark/Hadoop cluster in the cloud.
- Cloud sensor data needs to be moved and protected to on-premises in an efficient and secure way.
- Flexibility to transfer data from the cloud to on-premises under different conditions, such as on-demand, instantaneous, and during low-cluster load times.

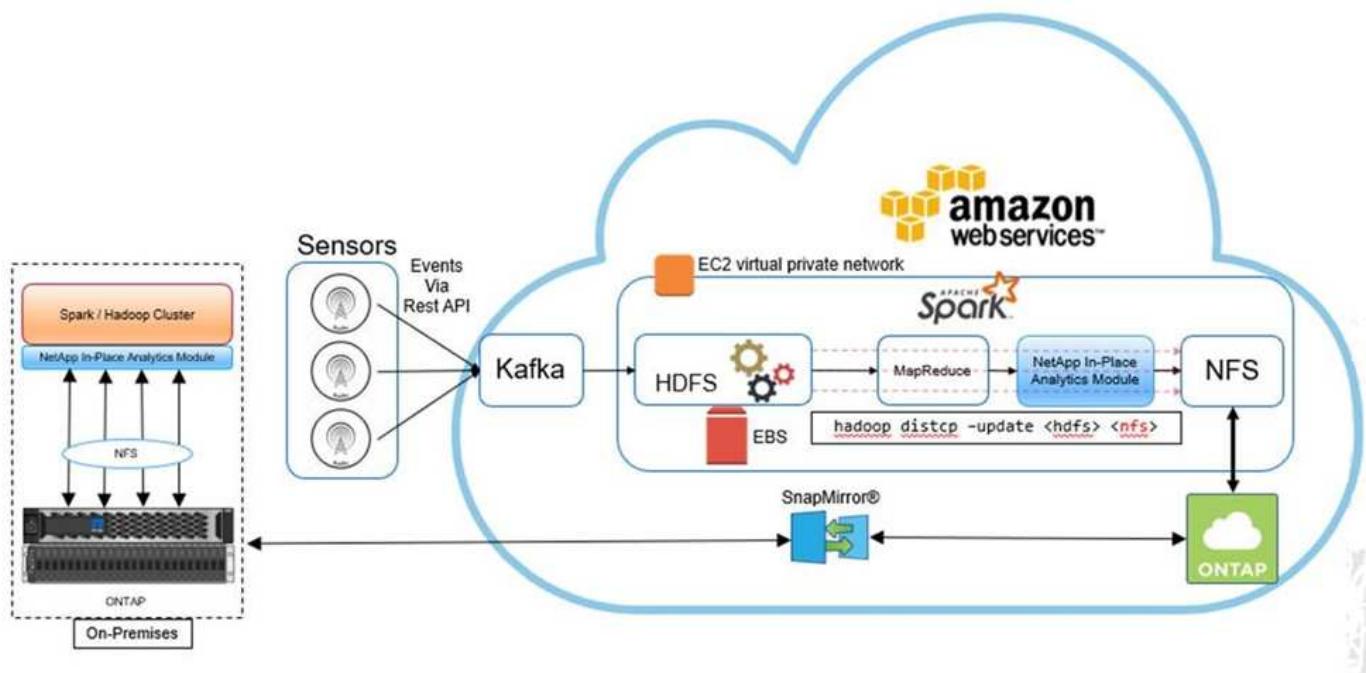
## Solution

The customer uses AWS Elastic Block Store (EBS) for its Spark cluster HDFS storage to receive and ingest data from remote sensors through Kafka. Consequently, the HDFS storage acts as the source for the backup data.

To fulfill these requirements, NetApp ONTAP Cloud is deployed in AWS, and an NFS share is created to act as the backup target for the Spark/Hadoop cluster.

After the NFS share is created, the In-Place Analytics Module is leveraged to copy the data from the HDFS EBS storage into the ONTAP NFS share. After the data resides in NFS in ONTAP Cloud, SnapMirror technology can be used to mirror the data from the cloud into on-premises storage as needed in a secure and efficient way.

This image shows the backup and disaster recovery from cloud to on-premises solution.



[Next: Use case 3 - Enabling DevTest on existing Hadoop data.](#)

## Use case 3: Enabling DevTest on existing Hadoop data

[Previous: Use case 2 - Backup and disaster recovery from the cloud to on-premises.](#)

In this use case, the customer's requirement is to rapidly and efficiently build new Hadoop/Spark clusters based on an existing Hadoop cluster containing a large amount of analytics data for DevTest and reporting purposes in the same data center as well as remote locations.

### Scenario

In this scenario, multiple Spark/Hadoop clusters are built from a large Hadoop data lake implementation on-premises as well as at disaster recovery locations.

### Requirements and challenges

The main requirements and challenges for this use case include:

- Create multiple Hadoop clusters for DevTest, QA, or any other purpose that requires access to the same production data. The challenge here is to clone a very large Hadoop cluster multiple times instantaneously and in a very space-efficient manner.
- Sync the Hadoop data to DevTest and reporting teams for operational efficiency.
- Distribute the Hadoop data by using the same credentials across production and new clusters.

- Use scheduled policies to efficiently create QA clusters without affecting the production cluster.

## Solution

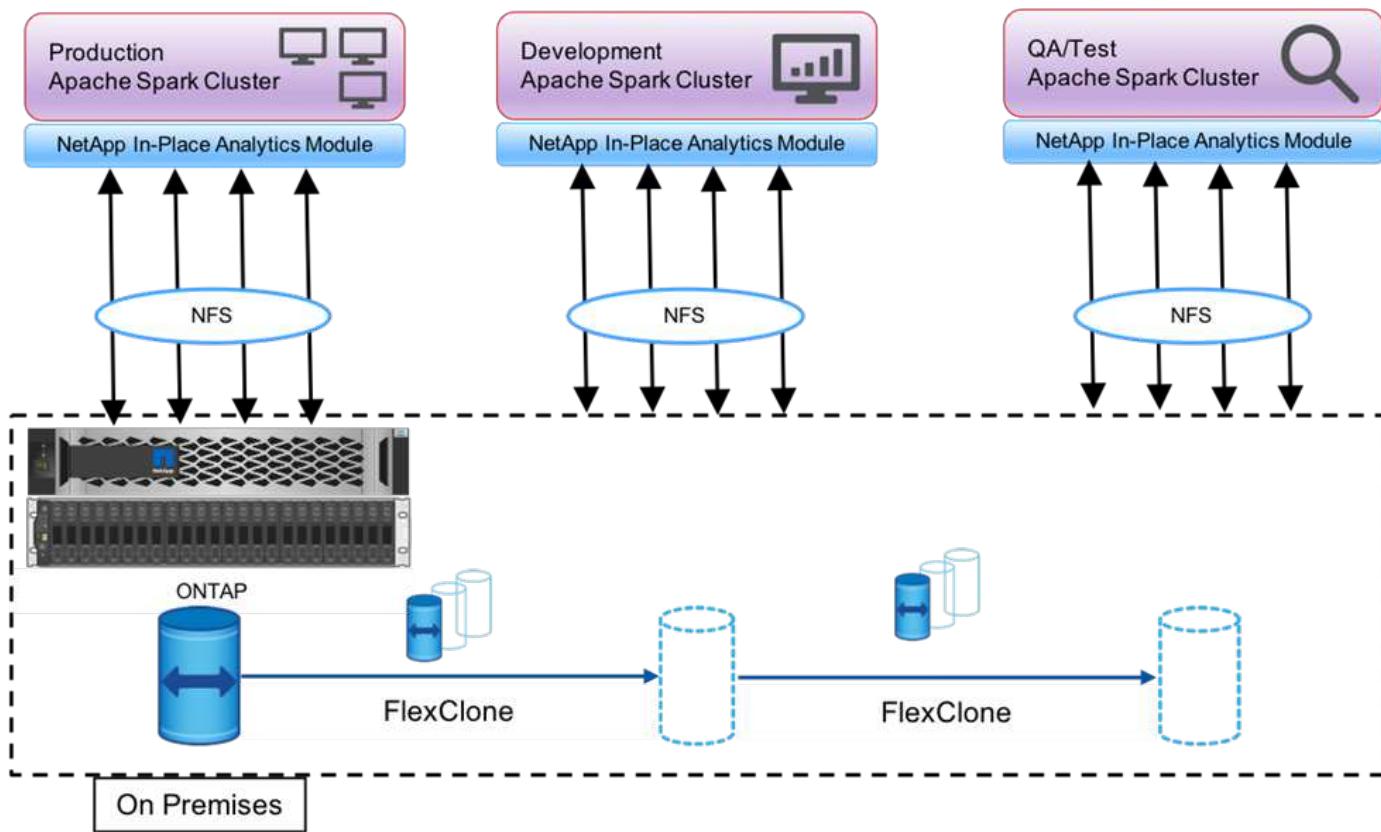
FlexClone technology is used to answer the requirements just described. FlexClone technology is the read/write copy of a Snapshot copy. It reads the data from parent Snapshot copy data and only consumes additional space for new/modified blocks. It is fast and space-efficient.

First, a Snapshot copy of the existing cluster was created by using a NetApp consistency group.

Snapshot copies within NetApp System Manager or the storage admin prompt. The consistency group Snapshot copies are application-consistent group Snapshot copies, and the FlexClone volume is created based on consistency group Snapshot copies. It is worth mentioning that a FlexClone volume inherits the parent volume's NFS export policy. After the Snapshot copy is created, a new Hadoop cluster must be installed for DevTest and reporting purposes, as shown in the figure below. The In-Place Analytics Module accesses the cloned NFS volume from the new Hadoop cluster through In-Place Analytics Module users and group authorization for the NFS data.

To have proper access, the new cluster must have the same UID and GUID for the users configured in the In-Place Analytics Module users and group configurations.

This image shows the Hadoop cluster for DevTest.



[Next: Use case 4 - Data protection and multicloud connectivity.](#)

## Use case 4: Data protection and multicloud connectivity

[Previous: Use case 3 - Enabling DevTest on existing Hadoop data.](#)

This use case is relevant for a cloud service partner tasked with providing multicloud connectivity for customers' big data analytics data.

## Scenario

In this scenario, IoT data received in AWS from different sources is stored in a central location in NPS. The NPS storage is connected to Spark/Hadoop clusters located in AWS and Azure enabling big data analytics applications running in multiple clouds accessing the same data.

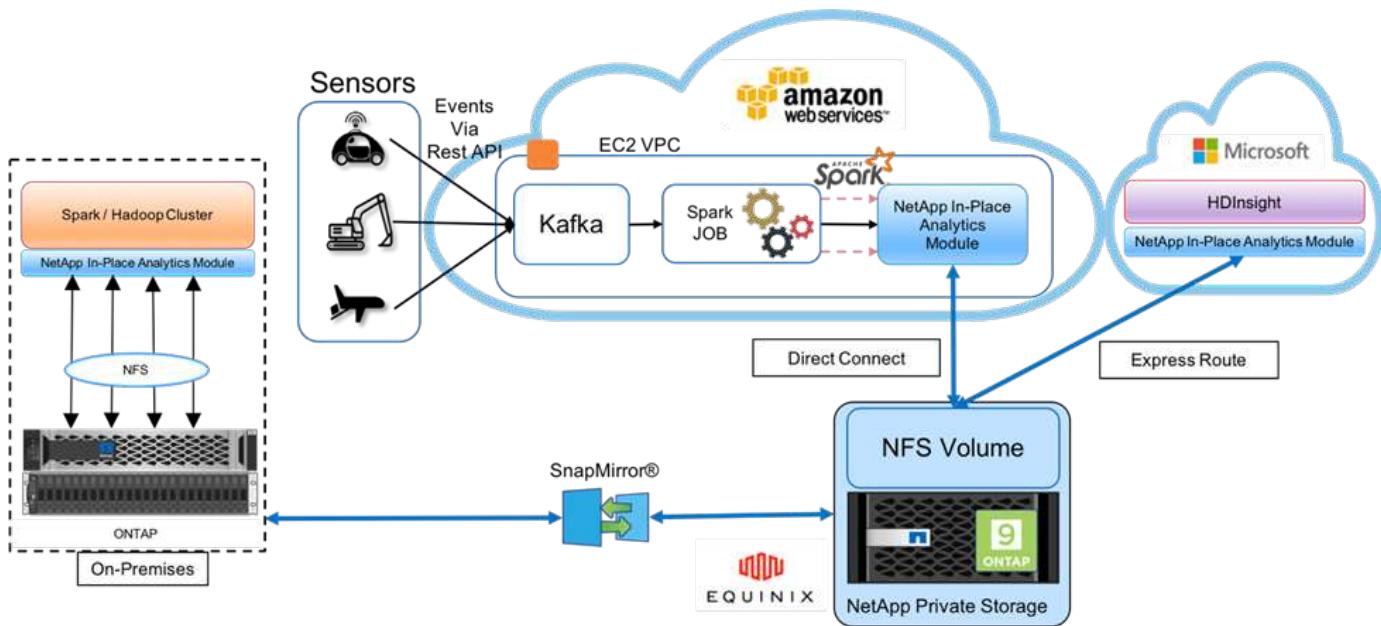
## Requirements and challenges

The main requirements and challenges for this use case include:

- Customers want to run analytics jobs on the same data using multiple clouds.
- Data must be received from different sources such as on-premises and cloud through different sensors and hubs.
- The solution must be efficient and cost-effective.
- The main challenge is to build a cost-effective and efficient solution that delivers hybrid analytics services between on-premises and across different clouds.

## Solution

This image illustrates the data protection and multicloud connectivity solution.



As shown in the figure above, data from sensors is streamed and ingested into the AWS Spark cluster through Kafka. The data is stored in an NFS share residing in NPS, which is located outside of the cloud provider within an Equinix data center. Because NetApp NPS is connected to Amazon AWS and Microsoft Azure through Direct Connect and Express Route connections, respectively, customers can leverage the In-Place Analytics Module to access the data from both Amazon and AWS analytics clusters. This approach solves having cloud analytics across multiple hyperscalers.

Consequently, because both on-premises and NPS storage runs ONTAP software, SnapMirror can mirror the NPS data into the on-premises cluster, providing hybrid cloud analytics across on-premises and multiple clouds.

For the best performance, NetApp typically recommends using multiple network interfaces and direct connection/express routes to access the data from cloud instances.

[Next: Use case 5 - Accelerate analytic workloads.](#)

## Use case 5: Accelerate analytic workloads

[Previous: Use case 4 - Data protection and multicloud connectivity.](#)

In this scenario, a large financial services and investment bank's analytics platform was modernized using the NetApp NFS storage solution to achieve significant improvement in analyzing investment risks and derivatives for its asset management and quantitative business unit.

### Scenario

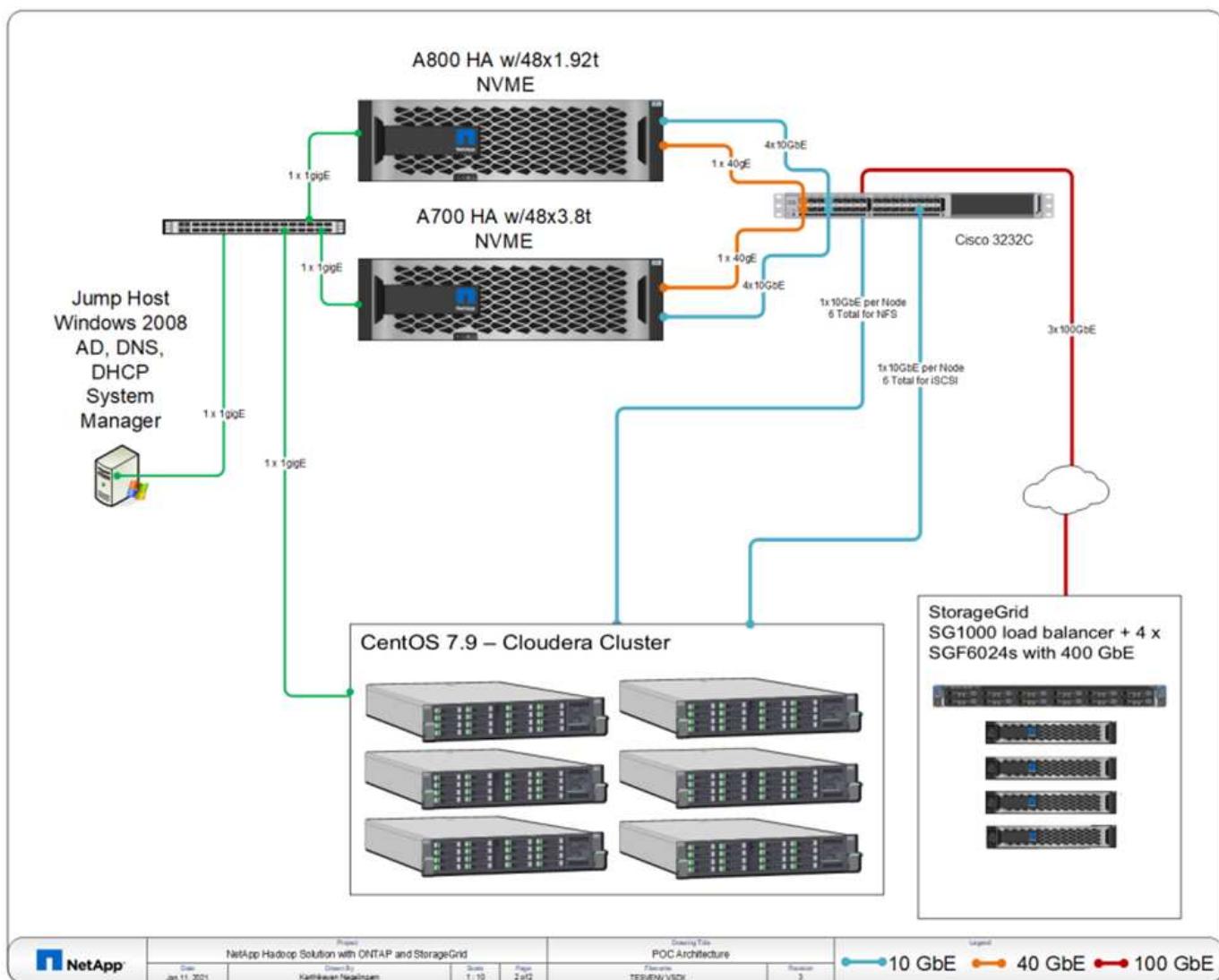
In the customer's existing environment, the Hadoop infrastructure used for the analytics platform leveraged internal storage from the Hadoop servers. Due to proprietary nature of JBOD environment, many internal customers within the organization were unable to take advantage of their Monte Carlo quantitative model, a simulation that relies on the recurring samples of real-time data. The suboptimal ability to understand the effects of uncertainty in market movements was serving unfavorably for the quantitative asset management business unit.

### Requirements and challenges

The quantitative business unit at the bank wanted an efficient forecasting method to attain accurate and timely predictions. To do so, the team recognized the need to modernize the infrastructure, reduce existing I/O wait time and improve performance on the analytic applications such as Hadoop and Spark to efficiently simulate investment models, measure potential gains and analyze risks.

### Solution

The customer had JBOD for their existing Spark solution. NetApp ONTAP, NetApp StorageGRID, and MinIO Gateway to NFS was then leveraged to reduce the I/O wait time for the bank's quantitative finance group that runs simulation and analysis on investment models that assess potential gains and risks. This image shows the Spark solution with NetApp storage.



As shown in figure above, AFF A800, A700 systems, and StorageGRID were deployed to access parquet files through NFS and S3 protocols in a six-node Hadoop cluster with Spark, and YARN and Hive metadata services for data analytic operations.

A direct-attached storage (DAS) solution in the customer's old environment had the disadvantage to scale compute and storage independently. With NetApp ONTAP solution for Spark, the bank's financial analytics business unit was able to decouple storage from compute and seamlessly bring infrastructure resources more effectively as needed.

By using ONTAP with NFS, the compute server CPUs were almost fully utilized for Spark SQL jobs and the I/O wait time was reduced by nearly 70%, therefore providing better compute power and performance boost to Spark workloads. Subsequently, increasing CPU utilization also enabled the customer to leverage GPUs, such as GPUDirect, for further platform modernization. Additionally, StorageGRID provides a low-cost storage option for Spark workloads and MinIO Gateway provides secure access to NFS data through the S3 protocol. For data in the cloud, NetApp recommends Cloud Volumes ONTAP, Azure NetApp Files, and NetApp Cloud Volumes Service.

Next: Conclusion.

## Conclusion

Previous: [Use case 5 - Accelerate analytic workloads.](#)

This section provides a summary of the use cases and solutions provided by NetApp to fulfill various Hadoop data protection requirements. By using the data fabric powered by NetApp, customers can:

- Have the flexibility to choose the right data protection solutions by leveraging NetApp's rich data management capabilities and integration with Hadoop native workflows.
- Reduce their Hadoop cluster backup window time by almost 70%.
- Eliminate any performance effect resulting from Hadoop cluster backups.
- Provide multicloud data protection and data access from different cloud providers simultaneously to a single source of analytics data.
- Create fast and space-efficient Hadoop cluster copies by using FlexClone technology.

## Where to find additional information

To learn more about the information described in this document, see the following documents and/or websites:

- NetApp Big Data Analytics Solutions

<https://www.netapp.com/us/solutions/applications/big-data-analytics/index.aspx>

- Apache Spark Workload with NetApp Storage

<https://www.netapp.com/pdf.html?item=/media/26877-nva-1157-deploy.pdf>

- NetApp Storage Solutions for Apache Spark

<https://www.netapp.com/media/16864-tr-4570.pdf>

- Apache Hadoop on data fabric enabled by NetApp

<https://www.netapp.com/media/16877-tr-4529.pdf>

- NetApp In-Place Analytics Module

[https://library.netapp.com/ecm/ecm\\_download\\_file/ECMLP2854071](https://library.netapp.com/ecm/ecm_download_file/ECMLP2854071)

## Acknowledgements

- Paul Burland, Sales Rep, ANZ Victoria District Sales, NetApp
- Hoseb Dermanilian, Business Development Manager, NetApp
- Lee Dorrier, Director MPSG, NetApp
- David Thiessen, Systems Engineer, ANZ Victoria District SE, NetApp

## Version history

Version	Date	Document version history
Version 1.0	January 2018	Initial release

<b>Version</b>	<b>Date</b>	<b>Document version history</b>
Version 2.0	October 2021	Updated with use case #5: Accelerate analytic workload

# NetApp Hybrid Multi-Cloud Solutions

## VMware for Public Cloud

### Overview of NetApp Hybrid Multi-Cloud with VMware

Most IT organizations follow the hybrid cloud-first approach. These organizations are in a transformation phase and customers are evaluating their current IT landscape and then migrating their workloads to the cloud based on the assessment and discovery exercise.

The factors for customers migrating to the cloud can include elasticity and burst, data center exit, data center consolidation, end-of-life scenarios, mergers, acquisitions, and so on. The reason for this migration can vary based on each organization and their respective business priorities. When moving to the hybrid cloud, choosing the right storage in the cloud is very important in order to unleash the power of cloud deployment and elasticity.

#### VMware Cloud options in Public Cloud

##### Azure VMware Solution



Azure VMware Solution is a hybrid cloud service that allows for fully functioning VMware SDDCs within the Microsoft Azure public cloud. Azure VMware Solution is a first-party solution fully managed and supported by Microsoft, verified by VMware leveraging Azure infrastructure. This means that when Azure VMware Solution is deployed, customer's get VMware's ESXi for compute virtualization, vSAN for hyper-converged storage, and NSX for networking and security, all while taking advantage of Microsoft Azure's global presence, class-leading data center facilities and proximity to the rich ecosystem of native Azure services and solutions.

##### VMware Cloud on AWS



VMware Cloud on AWS brings VMware's enterprise-class SDDC software to the AWS Cloud with optimized access to native AWS services. Powered by VMware Cloud Foundation, VMware Cloud on AWS integrates VMware's compute, storage, and network virtualization products (VMware vSphere, VMware vSAN, and VMware NSX) along with VMware vCenter Server management, optimized to run on dedicated, elastic, bare-metal AWS infrastructure.

##### Google Cloud VMware Engine



Google Cloud VMware Engine is an infrastructure-as-a-service (IaaS) offering built on Google Cloud's highly performant scalable infrastructure and VMware Cloud Foundation stack – VMware vSphere, vCenter, vSAN,

and NSX-T. This service enables a fast path to the cloud, seamlessly migrating or extending existing VMware workloads from on-premises environments to Google Cloud Platform without the cost, effort, or risk of rearchitecting applications or retooling operations. It is a service sold and supported by Google, working closely with VMware.



SDDC private cloud and NetApp Cloud Volumes colocation provides the best performance with minimal network latency.

## Did you know?

Regardless of the cloud used, when a VMware SDDC is deployed, the initial cluster includes the following products:

- VMware ESXi hosts for compute virtualization with a vCenter Server appliance for management
- VMware vSAN hyper-converged storage incorporating the physical storage assets of each ESXi host
- VMware NSX for virtual networking and security with an NSX Manager cluster for management

## Storage configuration

For customers planning to host storage-intensive workloads and scale out on any cloud-hosted VMware solution, the default hyper-converged infrastructure dictates that the expansion should be on both the compute and storage resources.

By integrating with NetApp Cloud Volumes, such as Azure NetApp Files, Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP (available in all three major hyperscalers), and Cloud Volumes Service for Google Cloud, customers now have options to independently scale their storage separately, and only add compute nodes to the SDDC cluster as needed.

### Notes:

- VMware does not recommend unbalanced cluster configurations, hence expanding storage means adding more hosts, which implies more TCO.
- Only one vSAN environment is possible. Therefore, all storage traffic will compete directly with production workloads.
- There is no option to provide multiple performance tiers to align application requirements, performance, and cost.
- It is very easy to reach the limits of storage capacity of vSAN built on top of the cluster hosts. Use NetApp Cloud Volumes to scale storage to either host active datasets or tier cooler data to persistent storage.

Azure NetApp Files, Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP (available in all three major hyperscalers), and Cloud Volumes Service for Google Cloud can be used in conjunction with guest VMs. This hybrid storage architecture consists of a vSAN datastore that holds the guest operating system and application binary data. The application data is attached to the VM through a guest-based iSCSI initiator or the NFS/SMB mounts that communicate directly with Amazon FSx for NetApp ONTAP, Cloud Volume ONTAP, Azure NetApp Files and Cloud Volumes Service for Google Cloud respectively. This configuration allows you to easily overcome challenges with storage capacity as with vSAN, the available free space depends on the slack space and storage policies used.

Let's consider a three-node SDDC cluster on VMware Cloud on AWS:

- The total raw capacity for a three-node SDDC = 31.1TB (roughly 10TB for each node).

- The slack space to be maintained before additional hosts are added = 25% = (.25 x 31.1TB) = 7.7TB.
- The usable raw capacity after slack space deduction = 23.4TB
- The effective free space available depends on the storage policy applied.

For example:

- RAID 0 = effective free space = 23.4TB (usable raw capacity/1)
- RAID 1 = effective free space = 11.7TB (usable raw capacity/2)
- RAID 5 = effective free space = 17.5TB (usable raw capacity/1.33)

Thus, using NetApp Cloud Volumes as guest-connected storage would help in expanding the storage and optimizing the TCO while meeting the performance and data protection requirements.

#### NOTE:

NetApp storage as a datastore is currently available as Public preview for AWS/VMC and Azure/AVS and Private preview for GCP/GSVE. Please visit the following links for more information.

AWS press release for FSx ONTAP as a native datastore COMING SOON!

[Azure NetApp Files \(ANF\) as a native datastore for Azure](#)  
[Cloud Volumes Service \(CVS\) as a native datastore for GCP](#)

#### Points to Remember

- In hybrid storage models, place tier 1 or high priority workloads on vSAN datastore to address any specific latency requirements because they are part of the host itself and within proximity. Use in-guest mechanisms for any workload VMs for which transactional latencies are acceptable.
- Use NetApp SnapMirror® technology to replicate the workload data from the on-premises ONTAP system to Cloud Volumes ONTAP or Amazon FSx for NetApp ONTAP to ease migration using block-level mechanisms. This does not apply to Azure NetApp Files and Cloud Volumes Services. For migrating data to Azure NetApp Files or Cloud Volumes Services, use NetApp XCP, Cloud sync, rysnc or robocopy depending on the file protocol used.
- Testing shows 2-4ms additional latency while accessing storage from the respective SDDCs. Factor this additional latency into the application requirements when mapping the storage.
- For mounting guest-connected storage during test failover and actual failover, make sure iSCSI initiators are reconfigured, DNS is updated for SMB shares, and NFS mount points are updated in fstab.
- Make sure that in-guest Microsoft Multipath I/O (MPIO), firewall, and disk timeout registry settings are configured properly inside the VM.



This applies to guest connected storage only.

#### Benefits of NetApp cloud storage

NetApp cloud storage offers the following benefits:

- Improves compute-to-storage density by scaling storage independently of compute.
- Allows you to reduce the host count, thus reducing the overall TCO.
- Compute node failure does not impact storage performance.
- The volume reshaping and dynamic service-level capability of Azure NetApp Files allows you to optimize

cost by sizing for steady-state workloads, and thus preventing over provisioning.

- The storage efficiencies, cloud tiering, and instance-type modification capabilities of Cloud Volumes ONTAP allow optimal ways of adding and scaling storage.
- Prevents over provisioning storage resources are added only when needed.
- Efficient Snapshot copies and clones allow you to rapidly create copies without any performance impact.
- Helps address ransomware attacks by using quick recovery from Snapshot copies.
- Provides efficient incremental block transfer-based regional disaster recovery and integrated backup block level across regions provides better RPO and RTOs.

## Assumptions

- SnapMirror technology or other relevant data migration mechanisms are enabled. There are many connectivity options, from on-premises to any hyperscaler cloud. Use the appropriate path and work with the relevant networking teams.
- In-guest storage was the only available option at the time this document was written.

### NOTE:

NetApp storage as a datastore is currently available as Public preview for AWS/VMC and Azure/AVS and Private preview for GCP/GSVE. Please visit the following links for more information.

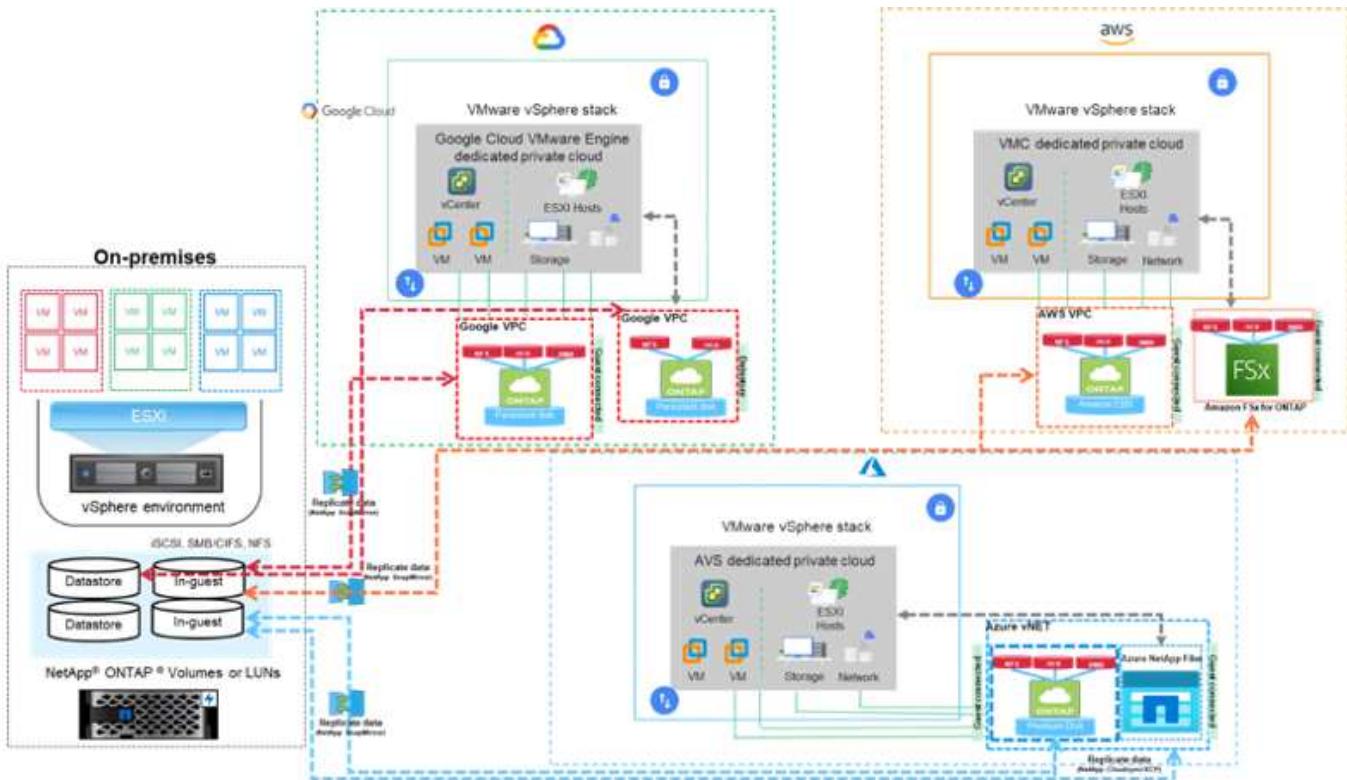
AWS press release for FSx ONTAP as a native datastore COMING SOON!

[Azure NetApp Files \(ANF\) as a native datastore for Azure](#)  
[Cloud Volumes Service \(CVS\) as a native datastore for GCP](#)

 Engage NetApp solution architects and respective hyperscaler cloud architects for planning and sizing of storage and the required number of hosts. NetApp recommends identifying the storage performance requirements before using the Cloud Volumes ONTAP sizer to finalize the storage instance type or the appropriate service level with the right throughput.

## Detailed architecture

From a high-level perspective, this architecture (shown in the figure below) covers how to achieve hybrid multi-cloud connectivity and app portability across multiple cloud providers using NetApp Cloud Volumes ONTAP, Cloud Volumes Service for Google Cloud and Azure NetApp Files as an additional in-guest storage option.



## NetApp Solutions for VMware in Hyperscalers

Learn more about the capabilities that NetApp brings to the three (3) primary hyperscalers - from NetApp as a guest connected storage device or a native datastore to migrating workflows, extending/bursting to the cloud, backup/restore and disaster recovery.

Pick your cloud and let NetApp do the rest!



To see the capabilities for a specific hyperscaler, click on the appropriate tab for that hyperscaler.

Jump to the section for the desired content by selecting from the following options:

- [VMware in the Hyperscalers Configuration](#)

- [NetApp Storage Options](#)
- [NetApp / VMware Cloud Solutions](#)

## **VMware in the Hyperscalers Configuration**

As with on-premises, planning a cloud based virtualization environment is critical for a successful production-ready environment for creating VMs and migration.

## AWS / VMC

This section describes how to set up and manage VMware Cloud on AWS SDDC and use it in combination with the available options for connecting NetApp storage.



In-guest storage is the only supported method of connecting FSx ONTAP and Cloud Volumes ONTAP to AWS VMC.

The setup process can be broken down into the following steps:

- Deploy and Configure VMware Cloud for AWS
- Connect VMware Cloud to FSx ONTAP

View the detailed [configuration steps for VMC](#).

## Azure / AVS

This section describes how to set up and manage Azure VMware Solution and use it in combination with the available options for connecting NetApp storage.



In-guest storage is the only supported method of connecting Azure NetApp Files and Cloud Volumes ONTAP to Azure VMware Solution.

The setup process can be broken down into the following steps:

- Register the resource provider and create a private cloud
- Connect to a new or existing ExpressRoute virtual network gateway
- Validate the network connectivity and access the private cloud

View the detailed [configuration steps for AVS](#).

## GCP / GCVE

This section describes how to set up and manage GCVE and use it in combination with the available options for connecting NetApp storage.



In-guest storage is the only supported method of connecting Cloud Volumes ONTAP and Cloud Volumes Services to GCVE.

The setup process can be broken down into the following steps:

- Deploy and Configure GCVE
- Enable Private Access to GCVE

View the detailed [configuration steps for GCVE](#).

## NetApp Storage Options

NetApp storage can be utilized in several ways - either as guest connected or as a native datastore - within each of the 3 major hyperscalers.

Please visit [Supported NetApp Storage Options](#) for more information.

## AWS / VMC

AWS supports NetApp storage in the following configurations:

- FSx ONTAP as guest connected storage
- Cloud Volumes ONTAP (CVO) as guest connected storage
- FSx ONTAP as a native datastore<sup>1</sup>

View the detailed [guest connect storage options for VMC](#).

Read more about FSx ONTAP as a native datastore public preview from the AWS Press Release (COMING SOON!).

## Azure / AVS

Azure supports NetApp storage in the following configurations:

- Azure NetApp Files (ANF) as guest connected storage
- Cloud Volumes ONTAP (CVO) as guest connected storage
- Azure NetApp Files (ANF) as a native datastore<sup>1</sup>

View the detailed [guest connect storage options for AVS](#).

Read more about [Azure NetApp Files \(ANF\) as a native datastore - Public Preview](#).

## GCP / GCVE

Google Cloud supports NetApp storage in the following configurations:

- Cloud Volumes ONTAP (CVO) as guest connected storage
- Cloud Volumes Service (CVS) as guest connected storage
- Cloud Volumes Service (CVS) as a native datastore<sup>1</sup>

View the detailed [guest connect storage options for GCVE](#).

Read more about [Cloud Volumes Service \(CVS\) as a native datastore<sup>1</sup>](#).



1 - Currently in Private Preview

## NetApp / VMware Cloud Solutions

With NetApp and VMware cloud solutions, many use cases are simple to deploy in your hyperscaler of choice. VMware defines the primary cloud workload use-cases as:

- Protect (includes both Disaster Recovery and Backup / Restore)
- Migrate
- Extend

**AWS / VMC**

[Browse the NetApp solutions for AWS / VMC](#)

**Azure / AVS**

[Browse the NetApp solutions for Azure / AVS](#)

**GCP / GCVE**

[Browse the NetApp solutions for Google Cloud Platform \(GCP\) / GCVE](#)

## Supported Configurations for NetApp Hybrid Multi-Cloud with VMware

Understanding the combinations for NetApp storage support in the major hyperscalers.

	<b>Guest Connected</b>	<b>Native Datastore</b>
<b>AWS</b>	CVO FSx ONTAP <a href="#">Details</a>	FSx ONTAP Press Release coming soon!
<b>Azure</b>	CVO ANF <a href="#">Details</a>	ANF <a href="#">Details</a> <sup>1</sup>
<b>GCP</b>	CVO CVS <a href="#">Details</a>	CVS <a href="#">Details</a> <sup>2</sup>

NOTE:

1 - Currently in Public Preview

2 - Currently in Private Preview

## Configuring the virtualization environment in the cloud provider

Details for how to configure the virtualization environment in each of the supported hyperscalers are covered here.

## AWS / VMC

This section describes how to set up and manage VMware Cloud on AWS SDDC and use it in combination with the available options for connecting NetApp storage.



In-guest storage is the only supported method of connecting FSx ONTAP and Cloud Volumes ONTAP to AWS VMC.

The setup process can be broken down into the following steps:

- Deploy and Configure VMware Cloud for AWS
- Connect VMware Cloud to FSx ONTAP

View the detailed [configuration steps for VMC](#).

## Azure / AVS

This section describes how to set up and manage Azure VMware Solution and use it in combination with the available options for connecting NetApp storage.



In-guest storage is the only supported method of connecting Azure NetApp Files and Cloud Volumes ONTAP to Azure VMware Solution.

The setup process can be broken down into the following steps:

- Register the resource provider and create a private cloud
- Connect to a new or existing ExpressRoute virtual network gateway
- Validate the network connectivity and access the private cloud

View the detailed [configuration steps for AVS](#).

## GCP / GCVE

This section describes how to set up and manage GCVE and use it in combination with the available options for connecting NetApp storage.



In-guest storage is the only supported method of connecting Cloud Volumes ONTAP and Cloud Volumes Services to GCVE.

The setup process can be broken down into the following steps:

- Deploy and Configure GCVE
- Enable Private Access to GCVE

View the detailed [configuration steps for GCVE](#).

## Deploy and configure the Virtualization Environment on AWS

As with on-premises, planning VMware Cloud on AWS is critical for a successful production-ready environment for creating VMs and migration.

This section describes how to set up and manage VMware Cloud on AWS SDDC and use it in combination

with the available options for connecting NetApp storage.



In-guest storage is currently the only supported method of connecting FSx ONTAP and Cloud Volumes ONTAP to AWS VMC.

The setup process can be broken down into the following steps:

## Deploy and configure VMware Cloud for AWS

VMware Cloud on AWS provides for a cloud native experience for VMware based workloads in the AWS ecosystem. Each VMware Software-Defined Data Center (SDDC) runs in an Amazon Virtual Private Cloud (VPC) and provides a full VMware stack (including vCenter Server), NSX-T software-defined networking, vSAN software-defined storage, and one or more ESXi hosts that provide compute and storage resources to your workloads.

This section describes how to set up and manage VMware Cloud on AWS and use it in combination with Amazon FSx for NetApp ONTAP and/or Cloud Volumes ONTAP on AWS with in-guest storage.



In-guest storage is the only supported method of connecting Amazon FSx for NetApp ONTAP and Cloud Volumes ONTAP to VMware Cloud on AWS.

The setup process can be broken down into three parts:

### Register for an AWS Account

Register for an [Amazon Web Services Account](#).

You need an AWS account to get started, assuming there isn't one created already. New or existing, you need administrative privileges in the account for many steps in this procedure. See this [link](#) for more information regarding AWS credentials.

### Register for a My VMware Account

Register for a [My VMware](#) account.

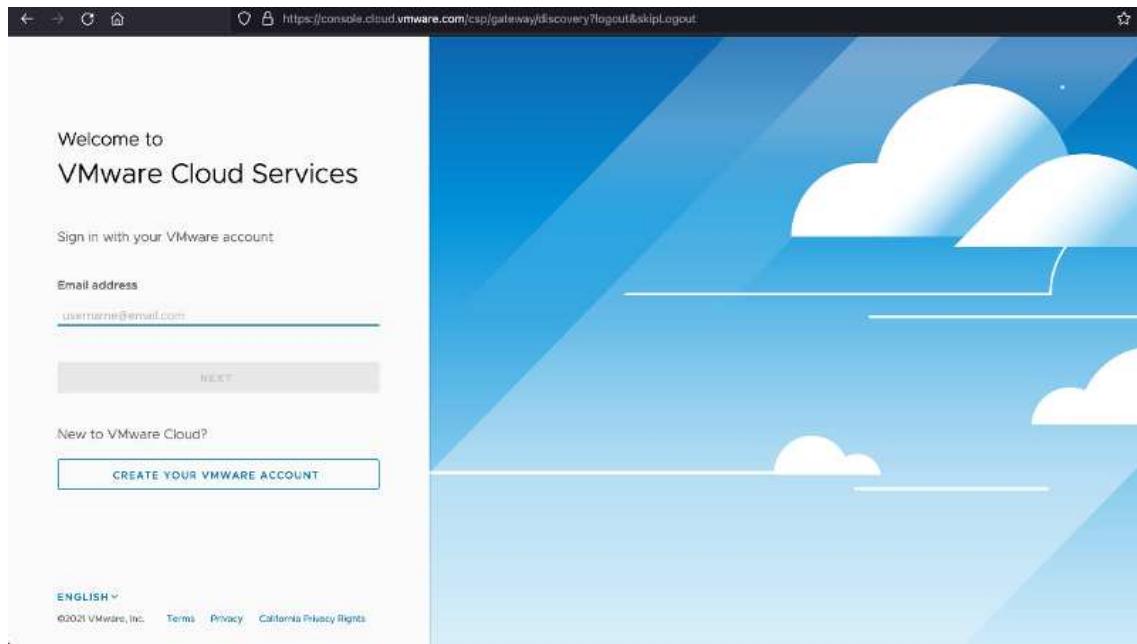
For access to VMware's cloud portfolio (including VMware Cloud on AWS), you need a VMware customer account or a My VMware account. If you have not already done so, create a VMware account [here](#).



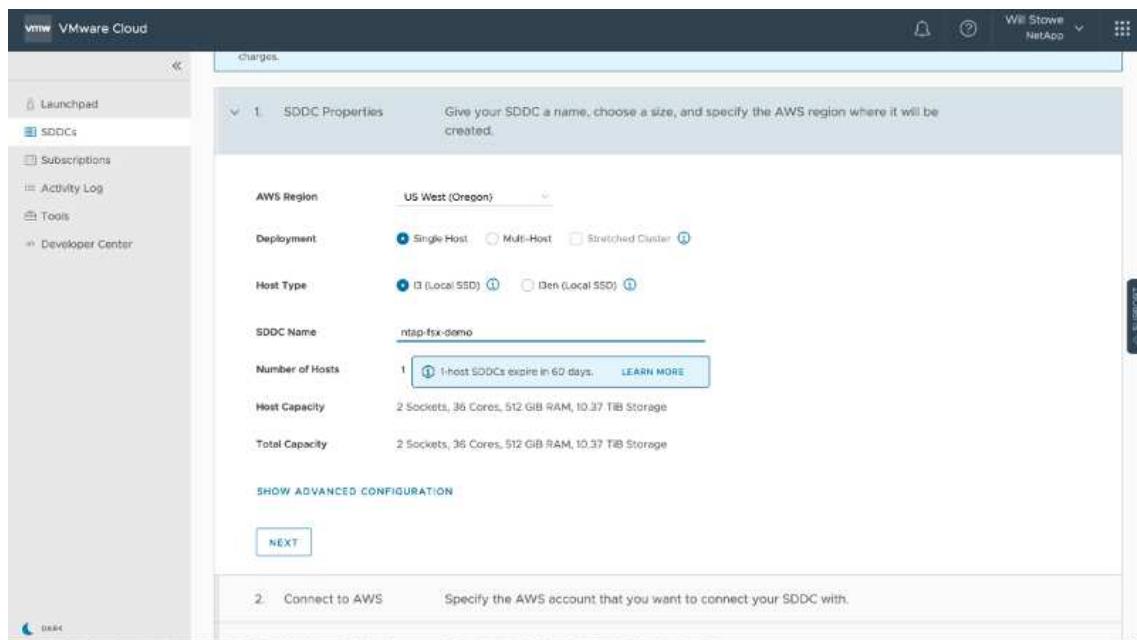
## Provision SDDC in VMware Cloud

After the VMware account is configured and proper sizing is performed, deploying a Software-Defined Data Center is the obvious next step for using the VMware Cloud on AWS service. To create an SDDC, pick an AWS region to host it, give the SDDC a name, and specify how many ESXi hosts you want the SDDC to contain. If you don't already have an AWS account, you can still create a starter configuration SDDC that contains a single ESXi host.

1. Log into the VMware Cloud Console using your existing or newly created VMware credentials.



2. Configure the AWS region, deployment, and host type and the SDDC name:



3. Connect to the desired AWS account and execute the AWS Cloud Formation stack.

Screenshot of the AWS CloudFormation 'Quick create stack' interface.

**Template**

Template URL: <https://vmware-sddc.s3.us-west-2.amazonaws.com/1eb9d184-a706-4489-abb8-692aad0e25d0/mq5ijphtclieoh85b75tegq9icc4bdd7ifq07nv716fk36>

Stack description: This template is created by VMware Cloud on AWS for SDDC deployment and maintenance. Please do not remove.

**Stack name**

Stack name: vmware-sddc-formation-a87f51c9-e5ac-4bb4-9d1e-9a3dahd197b7

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

**Parameters**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**Stack name**

Stack name: vmware-sddc-formation-a87f51c9-e5ac-4bb4-9d1e-9a3dahd197b7

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

**Parameters**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

No parameters

There are no parameters defined in your template.

**Capabilities**

The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. [Learn more](#)

I acknowledge that AWS CloudFormation might create IAM resources.

[Cancel](#) [Create change set](#) [Create stack](#)

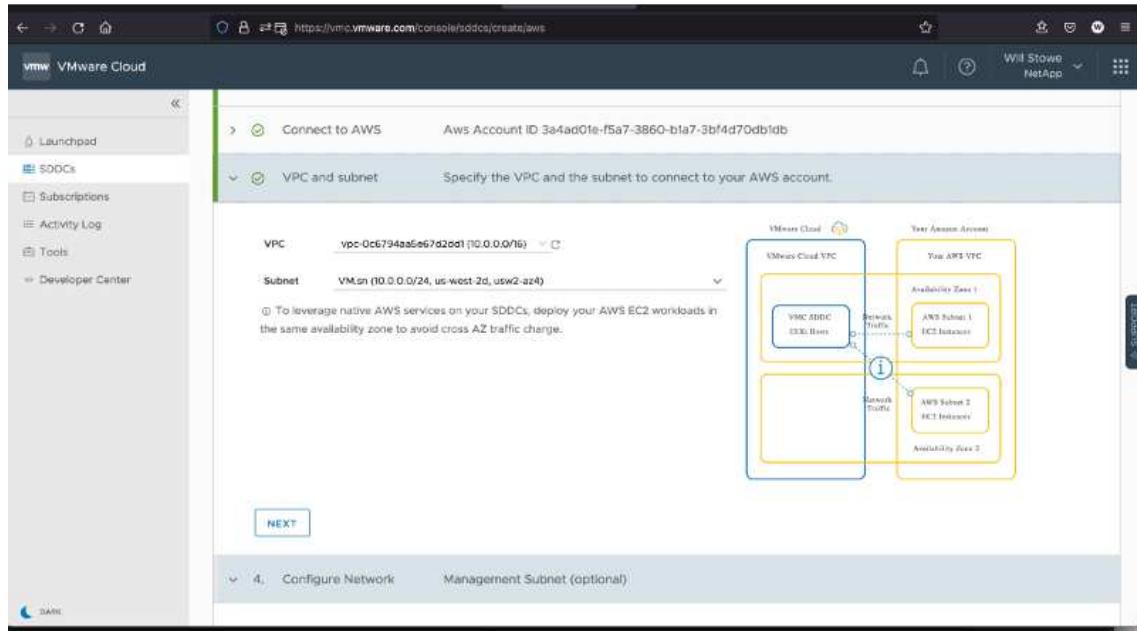
The screenshot shows the VMware Cloud SDDC creation wizard at step 2, titled "Connect to AWS". The page instructs the user to specify the AWS account to connect the SDDC with. It includes a note that VMware will have permission to set up networking correctly. There are two options: "Skip for now" and "Connect to AWS now". The "Connect to AWS now" option is selected. A progress bar indicates the task is 99% complete. Below the progress bar, a "NEXT" button is visible.

The screenshot then shows the result of connecting to the AWS account. A green checkmark icon and the message "Congratulations! Your connection is successfully established." are displayed. It shows the CloudFormation stack name "vmware-iddc-formation-a8731c9-e5ac-4bb4-9dfc-9a3dab097b7" and the AWS Account ID. A network diagram illustrates the connection between AWS and VMware. The "NEXT" button is again visible at the bottom.

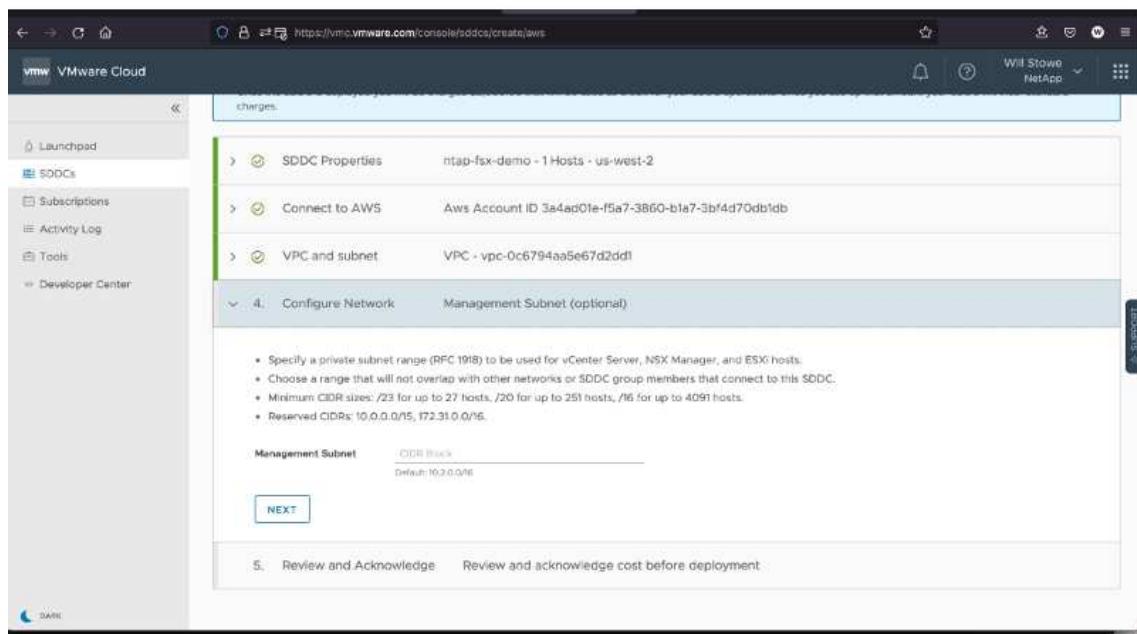


Single-host configuration is used in this validation.

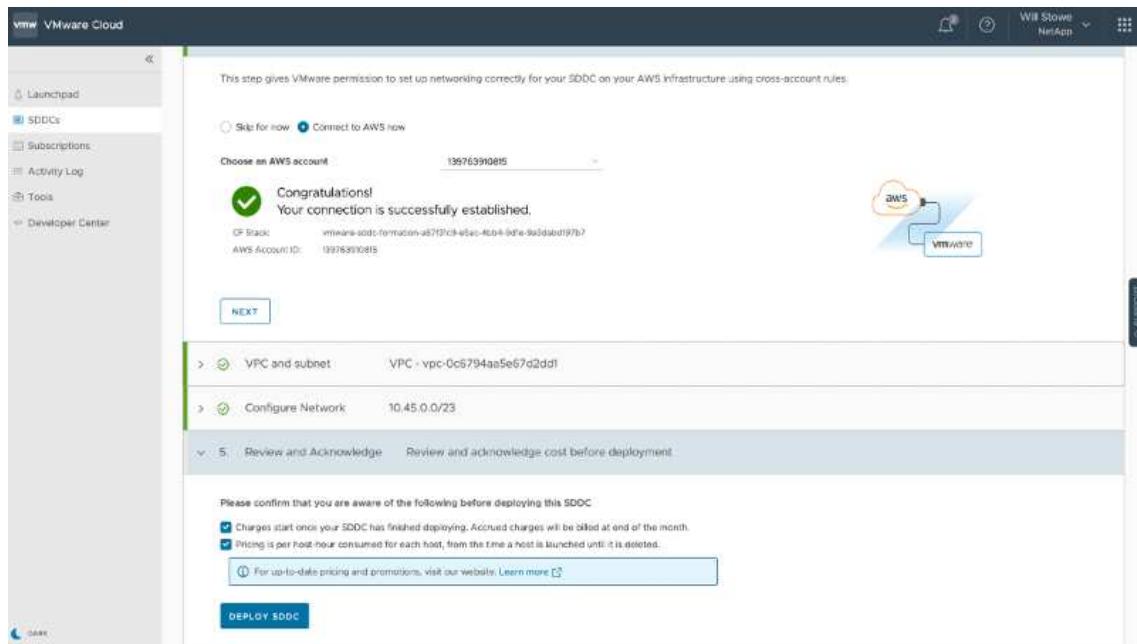
4. Select the desired AWS VPC to connect the VMC environment with.



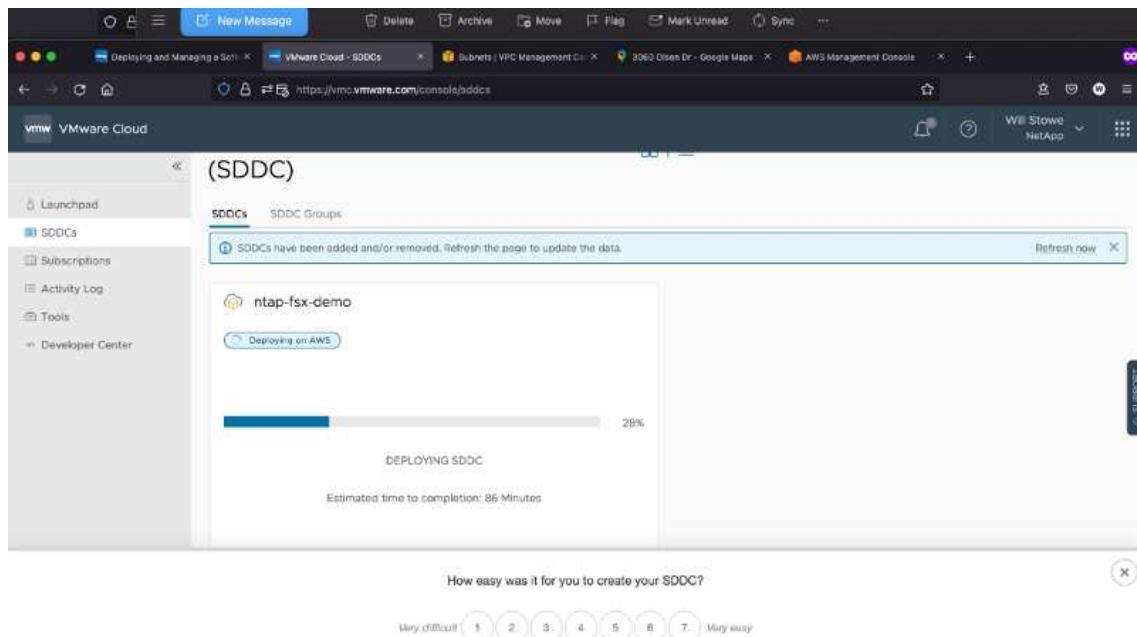
5. Configure the VMC Management Subnet; this subnet contains VMC-managed services like vCenter, NSX, and so on. Do not choose an overlapping address space with any other networks that need connectivity to the SDDC environment. Finally, follow the recommendations for CIDR size notated below.



6. Review and acknowledge the SDDC configuration, and then click deploy the SDDC.



The deployment process typically takes approximately two hours to complete.



7. After completion, the SDDC is ready for use.

The screenshot shows the VMware Cloud interface for managing Software-Defined Data Centers (SDDCs). The main title is "Software-Defined Data Centers (SDDC)". On the left, a sidebar lists "Launched", "SDDCs", "Subscriptions", "Activity Log", "Tools", and "Developer Center". The "SDDCs" item is selected, showing a list with one entry: "ntap-fsx-demo". The entry details are as follows:

Region	US West (Oregon)	Clusters	1		
Type	VMC on AWS SDDC	Hosts	1		
Availability Zones	us-west-2a, us-west-2b, us-west-2c	Volumes	36		
CPU	82.8 GHz	Memory	512 GiB	Storage	10.37 TiB

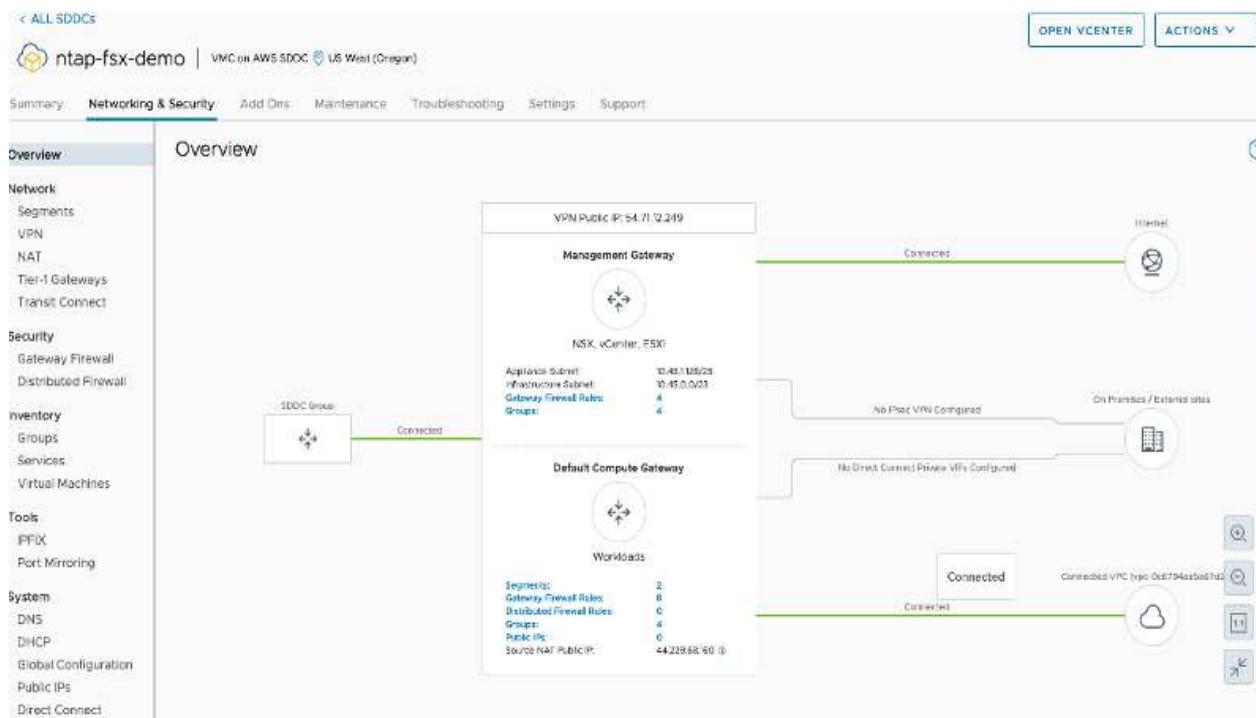
Below the table, there are links: "VIEW DETAILS", "OPEN VCENTER", and "ACTIONS". At the bottom of the page are links: "BACK TO TOP", "GO TO GRID VIEW", and a "DATA" link.

For a step-by-step guide on SDDC deployment, see [Deploy an SDDC from the VMC Console](#).

## Connect VMware Cloud to FSx ONTAP

To connect VMware Cloud to FSx ONTAP, complete the following steps:

- With VMware Cloud deployment completed and connected to AWS VPC, you must deploy Amazon FSx for NetApp ONTAP into a new VPC rather than the original connected VPC (see the screenshot below). FSx (NFS and SMB floating IPs) is not accessible if it is deployed in the connected VPC. Keep in mind that iSCSI endpoints like Cloud Volumes ONTAP work just fine from the connected VPC.



- Deploy an additional VPC in the same region, and then deploy Amazon FSx for NetApp ONTAP into the new VPC.

Configuration of an SDDC group in the VMware Cloud console enables the networking configuration options required to connect to the new VPC where FSx is deployed. In step 3, verify that “Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers” is checked, and then choose Create Group. The process can take a few minutes to complete.

VMware Cloud

### Create SDDC Group

**1. Name and Description** Create a name and description for your group.

Name	sddcgroup01
Description	sddcgroup01

**NEXT**

**2. Membership** Members: 1

**3. Acknowledgement**

Please confirm that you are aware of the following before creating this SDDC Group.

Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.

Create firewall rules to establish connectivity between the SDDCs in the group. [Learn More](#)

**CREATE GROUP**

VMware Cloud

### Create SDDC Group

**1. Name and Description** Name: sddcgroup01

**2. Membership** Select SDDCs to be part of your group.

Name	Sddc ID	Location	Version	Management CIDR
intap-lx-demo	829a6e22-92d1-42db-ad3d-9e4eb7a90fb6	US West (Oregon)	1.14.0.14	10.45.0.0/23
1				

**NEXT**

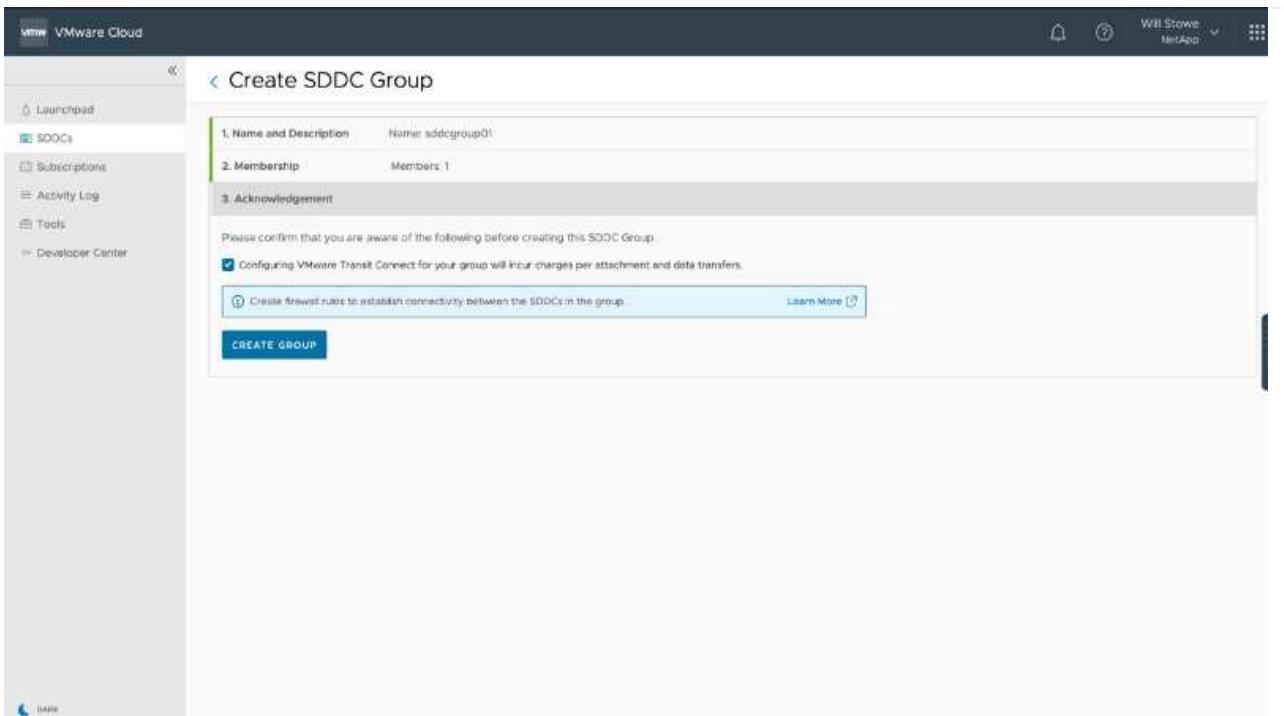
**3. Acknowledgement** Review and acknowledge requirements before creating the group.

Please confirm that you are aware of the following before creating this SDDC Group.

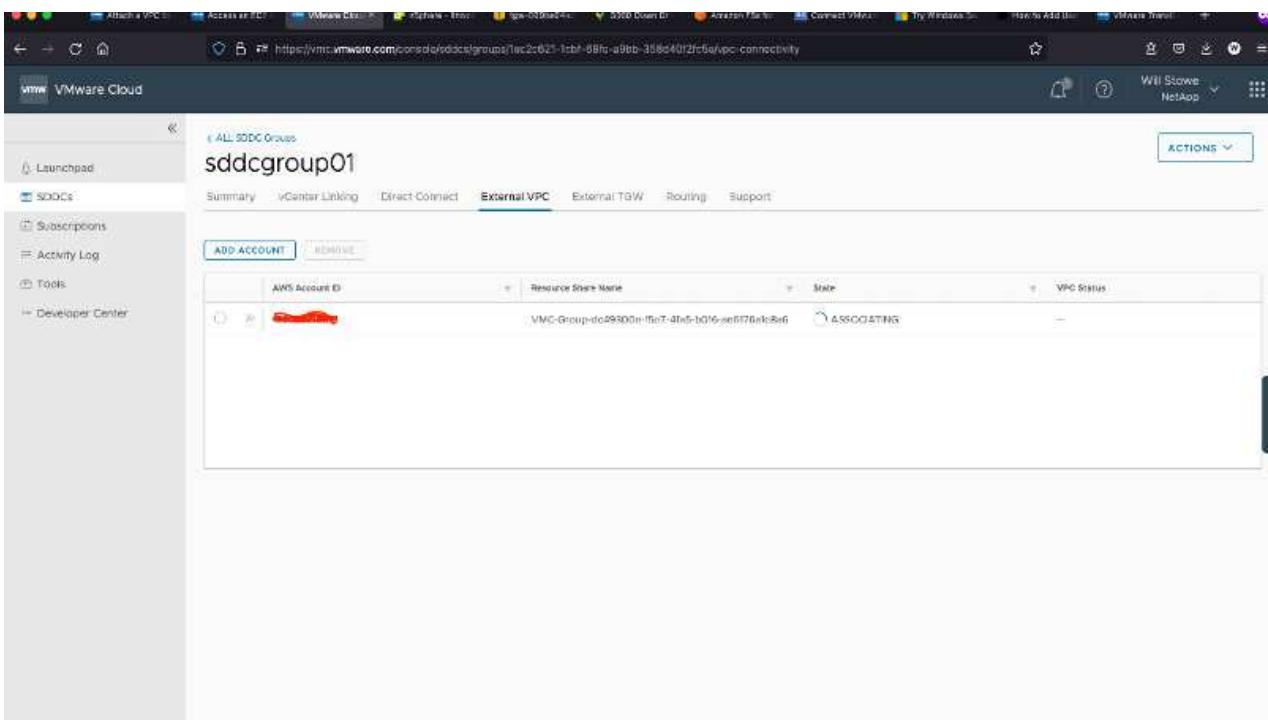
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.

Create firewall rules to establish connectivity between the SDDCs in the group. [Learn More](#)

**CREATE GROUP**



3. Attach the newly created VPC to the just created SDDC group. Select the External VPC tab and follow the [instructions for attaching an External VPC](#) to the group. This process can take 10 to 15 minutes to complete.



The screenshot shows the VMware Cloud interface with the URL <https://mc.vmware.com/core/sddc/groups/fe2c821-lcbf-80fc-a9bb-350a402f5a5c/connectivity>. The 'External VPC' tab is selected. On the left, there's a sidebar with options like 'Launchpad', 'Subscriptions', 'Activity Log', 'Tools', and 'Developer Center'. The main area displays a table titled 'ALL SDDC GROUPS' with one row:

AWS Account ID	Resource Share Name	Status	VPC Status
12345678901234567890	VMC-Group-dc09300e15e74fb5-b016-ee01768e86	ASSOCIATED	...

4. As part of the external VPC process, you are prompted through the AWS console to a new shared resource via the Resource Access Manager. The shared resource is the [AWS Transit Gateway](#) managed by VMware Transit Connect.

The screenshot shows the AWS Resource Access Manager (RAM) console at the URL <https://us-west-2.console.aws.amazon.com/ram/home?region=us-west-2#home>. The 'Resource shares' section is selected. The main area has sections for 'How it works' and 'Use cases'.

**How it works:**

- AWS Resource Access Manager: Share resources across AWS accounts or AWS Organizations by creating a Resource Share.
- Select Resources: Select the resource(s) that you would like to add to a Resource Share.
- Specify Principals: Specify account ID, ARN, or Organization identifier who can access the resources in the Resource Share.
- Share Resources: The specified principals will now have access to resources in the Resource Share.

**Use cases:**

- Manage resources centrally in a multi-account environment
- Increase efficiency, decrease costs

The screenshot shows the AWS Resource Access Manager (RAM) console. On the left, there's a sidebar with navigation links: 'Resource Access Manager', 'Shared by me' (selected), 'Resource shares' (1 invitation), 'Shared resources', 'Principals', and 'Shared with me' (selected). Under 'Shared with me', it shows 'Resource shares' (1 invitation), 'Shared resources', and 'Principals'. Below that are 'Permissions library' and 'Settings'. The main content area shows a 'Resource share' named 'VMC-Group-dc49300e-f5e7-4fa5-b016-ae6176a1e8a6 (051a6fc5-0a1e-4560-853f-e2939d856b0c)'. It has a summary table with columns: Name, Owner, Invitation date, and Status. The status is 'Pending'. There are 'Reject resource share' and 'Accept resource share' buttons at the top of the summary table.

## 5. Create the Transit Gateway Attachment.

The screenshot shows the 'Create transit gateway attachment' wizard in the AWS VPC console. The first step, 'Details', is selected. It contains fields for 'Name tag - optional' (set to 'my-transit-gateway-attachment'), 'Transit gateway ID' (set to 'tgw-001646b36ee07a2cb'), and 'Attachment type' (set to 'VPC'). The second step, 'VPC attachment', is shown below. It includes sections for 'DNS support' (checked), 'IPv6 support' (unchecked), 'VPC ID' (set to 'vpc-0d1c764bcc495e805 (vmctsx2.vpc)'), and 'Subnet IDs' (info link). At the bottom right of the wizard, there's a 'Next Step' button.

## 6. Back on the VMC Console, Accept the VPC attachment. This process can take approximately 10 minutes to complete.

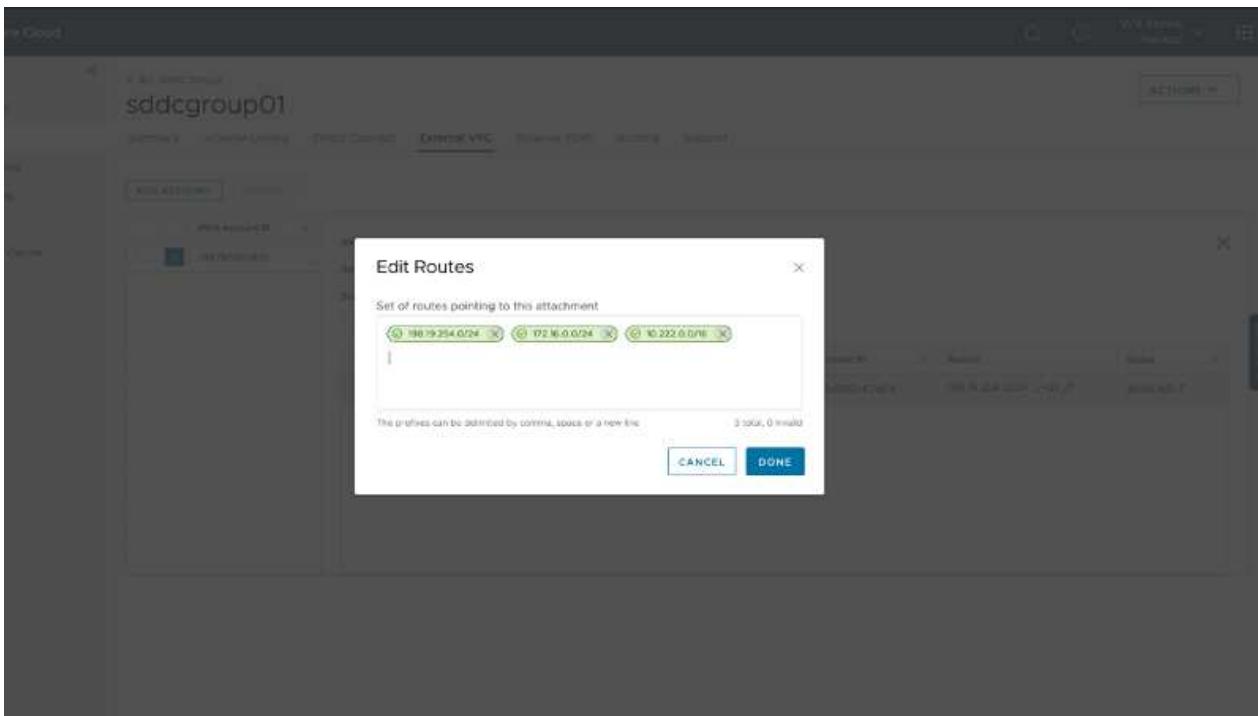
VPC ID	VMC on AWS Region	Transit Gateway Attachment ID	Routes	Status
vpc-0d1c764bcc495e805	US West (Oregon)	tgw-attach-0a4883d6f92c67d64	192.168.0.0/24	PENDING

7. While in the External VPC tab, click the edit icon in the Routes column and add in the following required routes:

- A route for the floating IP range for Amazon FSx for NetApp ONTAP [floating IPs](#).
- A route for the floating IP range for Cloud Volumes ONTAP (if applicable).
- A route for the newly created external VPC address space.

VPC ID	VMC on AWS Region	Transit Gateway Attachment ID	Routes	Status
vpc-0d1c764bcc495e805	US West (Oregon)	tgw-attach-0a4883d6f92c67d64	192.168.0.0/24	AVAILABLE

8. Finally, allow bidirectional traffic [firewall rules](#) for access to FSx/CVO. Follow these [detailed steps](#) for compute gateway firewall rules for SDDC workload connectivity.



9. After the firewall groups are configured for both the Management and Compute gateway, the vCenter can be accessed as follows:

The next step is to verify that Amazon FSx ONTAP or Cloud Volumes ONTAP is configured depending on your requirements and that the volumes are provisioned to offload storage components from vSAN to optimize the deployment.

## Deploy and configure the Virtualization Environment on Azure

As with on-premises, planning Azure VMware Solution is critical for a successful production-ready environment for creating VMs and migration.

This section describes how to set up and manage Azure VMware Solution and use it in combination with the available options for connecting NetApp storage.



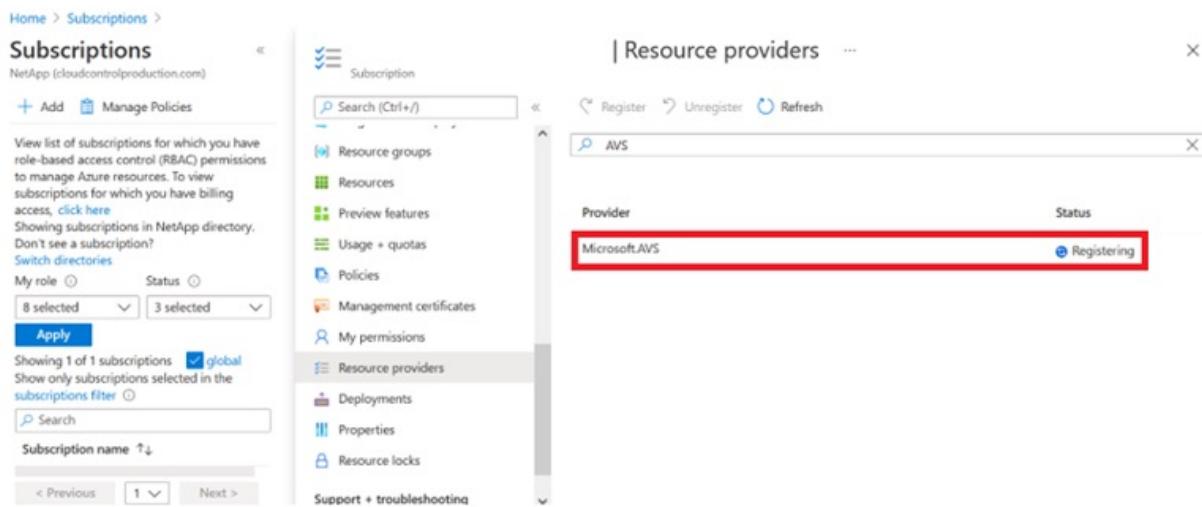
In-guest storage is the only supported method of connecting Azure NetApp Files and Cloud Volumes ONTAP to Azure VMware Solution.

The setup process can be broken down into the following steps:

## Register the resource provider and create a private cloud

To use Azure VMware Solution, first register the resource provider within the identified subscription:

1. Sign in to the Azure portal.
2. On the Azure portal menu, select All Services.
3. In the All Services dialog box, enter the subscription and then select Subscriptions.
4. To view, select the subscription from the subscription list.
5. Select Resource Providers and enter Microsoft.AVS into the search.
6. If the resource provider is not registered, select Register.



Provider	Status
Microsoft.OperationsManagement	Registered
Microsoft.Compute	Registered
Microsoft.ContainerService	Registered
Microsoft.ManagedIdentity	Registered
Microsoft.AVS	Registered
Microsoft.OperationalInsights	Registered
Microsoft.GuestConfiguration	Registered

7. After the resource provider is registered, create an Azure VMware Solution private cloud by using the Azure portal.
8. Sign in to the Azure portal.
9. Select Create a New Resource.
10. In the Search the Marketplace text box, enter Azure VMware Solution and select it from the results.
11. On the Azure VMware Solution page, select Create.
12. From the Basics tab, enter the values in the fields and select Review + Create.

Notes:

- For a quick start, gather the required information during the planning phase.
- Select an existing resource group or create a new resource group for the private cloud. A resource group is a logical container in which the Azure resources are deployed and managed.
- Make sure the CIDR address is unique and does not overlap with other Azure Virtual Networks or on-premises networks. The CIDR represents the private cloud management network and is used for the cluster management services, such as vCenter Server and NSX-T Manager. NetApp recommends using a /22 address space. In this example, 10.21.0.0/22 is used.

## Create a private cloud

Prerequisites   **Basics**   Tags   Review and Create

**Project details**

Subscription \* **SaaS Backup Production**  
Resource group \* **(New) NimoAVSDemo**  
[Create new](#)

**Private cloud details**

Resource name \* **nimoavsppriv**  
Location \* **(US) East US 2**  
Size of host \* **AV36 Trial**  
Number of hosts \* **3** Find out how many hosts you need

There is no metering for the selected subscription, region, and SKU. No cost data to display.

**CIDR address block**  
Provide IP address for private cloud for cluster management. Make sure these are unique and do not overlap with any other Azure vnets or on-premise networks.

Address block for private cloud \* **10.21.0.0/22**

[Review and Create](#)   [Previous](#)   [Next : Tags >](#)

The provisioning process takes approximately 4–5 hours. After the process is complete, verify that the deployment was successful by accessing the private cloud from the Azure portal. A status of Succeeded is displayed when the deployment is complete.

An Azure VMware Solution private cloud requires an Azure Virtual Network. Because Azure VMware Solution doesn't support on-premises vCenter, additional steps are required to integrate with an existing on-premises environment. Setting up an ExpressRoute circuit and a virtual network gateway is also required. While waiting for the cluster provisioning to complete, create a new virtual network or use an existing one to connect to Azure VMware Solution.

Home >

**nimoavsppriv** [AVS Private cloud](#)

[Delete](#)

**Overview**

**Activity log**

**Access control (IAM)**

**Tags**

**Diagnose and solve problems**

**Settings**

**Locks**

**Manage**

**Connectivity**

**Identity**

**Clusters**

**Essentials**

Resource group <a href="#">(change)</a> <b>NimoAVSDemo</b>	Address block for private cloud <b>10.21.0.0/22</b>
Status <b>Succeeded</b>	Primary peering subnet <b>10.21.0.232/30</b>
Location <b>East US 2</b>	Secondary peering subnet <b>10.21.0.236/30</b>
Subscription <a href="#">(change)</a> <b>SaaS Backup Production</b>	Private Cloud Management network <b>10.21.0.0/26</b>
Subscription ID <b>b58a041a-e464-4497-8be9-9048369ee8e1</b>	vMotion network <b>10.21.1.128/25</b>
Tags <a href="#">(change)</a> <a href="#">Click here to add tags</a>	Number of hosts <b>3</b>

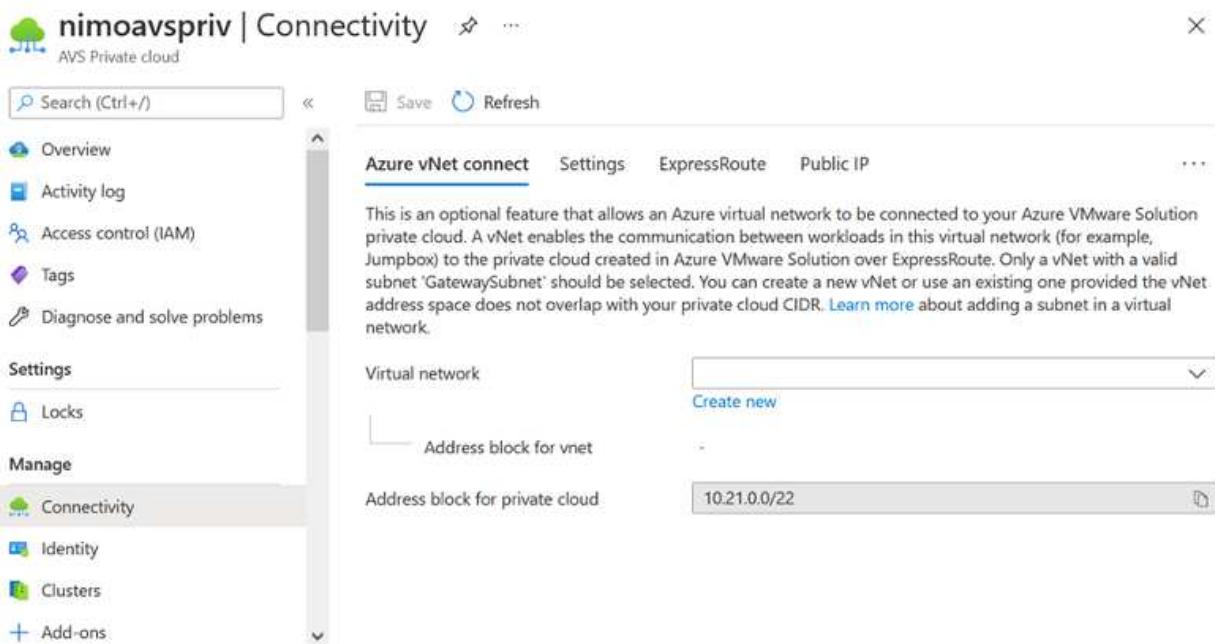
## Connect to a new or existing ExpressRoute virtual network gateway

To create a new Azure Virtual Network (VNet), select the Azure VNet Connect tab. Alternatively, you can create one manually from the Azure portal by using the Create Virtual Network wizard:

1. Go to Azure VMware Solution private cloud and access Connectivity under the Manage option.
2. Select Azure VNet Connect.
3. To create a new VNet, select the Create New option.

This feature allows a VNet to be connected to the Azure VMware Solution private cloud. The VNet enables communication between workloads in this virtual network by automatically creating required components (for example, jump box, shared services such as Azure NetApp Files, and Cloud Volume ONTAP) to the private cloud created in Azure VMware Solution over ExpressRoute.

**Note:** The VNet address space should not overlap with the private cloud CIDR.



4. Provide or update the information for the new VNet and select OK.

## Create virtual network

X

This virtual network enables the communication between workloads in this virtual network (e.g. a Jumphost) to the private cloud created in Azure VMware Solution over an Express route. A default address range and a subnet is selected for this virtual network. For changing the default address range and subnet of this virtual network, follow these steps: Step 1: Change the "Address Range" to desired range (e.g. 172.16.0.0/16). Step 2: Add a subnet under "Subnets" with the name as "GatewaySubnet" and provide subnet's address range in CIDR notation (e.g. 172.16.1.0/24). [Learn more about virtual networks](#)

Name \*

nimoavspiv-vnet

### Address space

The virtual network's address space specified as one or more address prefixes in CIDR notation (e.g. 10.0.0.0/16).

<input type="checkbox"/> Address range	Addresses	Overlap	
<input type="checkbox"/> 172.24.0.0/16	172.24.0.4 - 172.24.255.254 (65531 addresses)	None	
	(0 Addresses)	None	

### Subnets

The subnet's address range in CIDR notation (e.g. 10.0.0.0/24). It must be contained by the address space of the virtual network.

<input type="checkbox"/> Subnet name	Address range	Addresses	
<input type="checkbox"/> GatewaySubnet	172.24.0.0/24	172.24.0.4 - 172.24.0.254 (251 addresses)	
		(0 Addresses)	

The VNet with the provided address range and gateway subnet is created in the designated subscription and resource group.



If you create a VNet manually, create a virtual network gateway with the appropriate SKU and ExpressRoute as the gateway type. After the deployment is complete, connect the ExpressRoute connection to the virtual network gateway containing Azure VMware Solution private cloud using the authorization key. For more information, see [Configure networking for your VMware private cloud in Azure](#).

## Validate the network connect and access to Azure VMware Solution private cloud

Azure VMware Solution does not allow you to manage a private cloud with on-premises VMware vCenter. Instead, jump host is required to connect to the Azure VMware Solution vCenter instance. Create a jump host in the designated resource group and sign in to the Azure VMware Solution vCenter. This jump host should be a Windows VM on the same virtual network that was created for connectivity and should provide access to both vCenter and the NSX Manager.

### Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*  SaaS Backup Production

Resource group \*  NimoAVSDemo [Create new](#)

**Instance details**

Virtual machine name \*  nimAVSRH

Region \*  (US) East US 2

Availability options  No infrastructure redundancy required

Image \*  Windows Server 2012 R2 Datacenter - Gen2 [See all images](#)

Azure Spot instance

Size \*  Standard\_D2s\_v3 - 2 vcpus, 8 GiB memory (\$130.67/month) [See all sizes](#)

After the virtual machine is provisioned, use the Connect option to access RDP.

The screenshot shows the Azure portal interface for a virtual machine named 'nimAVSJH'. On the left, there's a sidebar with various navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Connect, Disks, and Size. The 'Connect' option is currently selected. The main pane is titled 'nimAVSJH | Connect' and shows the 'Virtual machine' section. It includes a search bar, a warning message about enabling just-in-time access, and tabs for RDP, SSH, and BASTION. Under the RDP tab, there's a section titled 'Connect with RDP' with instructions to select an IP address, port number, and download an RDP file. The IP address is set to 'Public IP address (52.138.103.135)' and the port number is '3389'. A blue button labeled 'Download RDP File' is visible.

Sign in to vCenter from this newly created jump host virtual machine by using the cloud admin user . To access the credentials, go to the Azure portal and navigate to Identity (under the Manage option within the private cloud). The URLs and user credentials for the private cloud vCenter and NSX-T Manager can be copied from here.

The screenshot shows the Azure portal interface for an AVS Private cloud named 'nimoavsppriv'. The left sidebar has sections for Connectivity, Identity (which is selected), Clusters, Placement policies (preview), and Add-ons. The main pane is titled 'nimoavsppriv | Identity' and shows 'AVS Private cloud' details. It includes a search bar and a 'Login credentials' section. This section is divided into 'vCenter credentials' and 'NSX-T Manager credentials'. For vCenter, the Web client URL is 'https://10.21.0.2/' and the Admin username is 'cloudadmin@vsphere.local'. For NSX-T Manager, the Web client URL is 'https://10.21.0.3/' and the Admin username is 'admin'. Each credential entry has a copy icon to its right.

In the Windows virtual machine, open a browser and navigate to the vCenter web client URL (<https://10.21.0.2/>) and use the admin user name as **cloudadmin@vsphere.local** and paste the copied password. Similarly, NSX-T manager can also be accessed using the web client URL (<https://10.21.0.3/>) and use the admin user name and paste the copied password to create new segments or modify the existing tier gateways.



The web client URLs are different for each SDDC provisioned.

The screenshot shows two parts of the VMware vSphere interface. The top part is the 'Login' screen, which includes fields for 'Email' (clouadmin@vsphere.local), 'Password', and a checkbox for 'Use Windows session authentication'. The bottom part is the main vSphere Client interface, showing the summary for the 'SDDC-Datacenter' cluster. It displays 0 virtual machines and 3 hosts. Resource usage statistics are shown for CPU, Memory, and Storage. Below this, there are sections for 'Custom Attributes' and 'Tags'. A table of recent tasks shows one task named 'Undeploy plug-in' completed successfully.

The Azure VMware Solution SDDC is now deployed and configured. Leverage ExpressRoute Global Reach to connect the on-premises environment to Azure VMware Solution private cloud. For more information, see [Peer on-premises environments to Azure VMware Solution](#).

## Deploy and configure the Virtualization Environment on Google Cloud Platform (GCP)

As with on-premises, planning Google Cloud VMware Engine (GCVE) is critical for a successful production-ready environment for creating VMs and migration.

This section describes how to set up and manage GCVE and use it in combination with the available options for connecting NetApp storage.



In-guest storage is the only supported method of connecting Cloud Volumes ONTAP and Cloud Volumes Services to GCVE.

The setup process can be broken down into the following steps:

## Deploy and configure GCVE

To configure a GCVE environment on GCP, login to the GCP console and access the VMware Engine portal.

Click on the “New Private Cloud” button and enter the desired configuration for the GCVE Private Cloud. On “Location”, make sure to deploy the private cloud in the same Region/Zone where CVS/CVO is deployed, to ensure the best performance and lowest latency.

Pre-requisites:

- Setup VMware Engine Service Admin IAM role
- [Enable VMWare Engine API access and node quota](#)
- Make sure that the CIDR range doesn't overlap with any of your on-premises or cloud subnets. The CIDR range must be /27 or higher.

Google Cloud VMware Engine

Create Private Cloud

Private Cloud name \*

NIMoGCVE

Location \*

us-east4 > v-zone-a > VE Placement Group 2

Node type \*

ve1-standard-72  
2x2.6 GHz, 36 Cores (72 HT), 768 GB RAM  
19.2 TB Raw, 3.2 TB Cache (All-Flash)

Node count \*

3  
(3 to 3)

vSphere/vSAN subnets CIDR range \*

192.168.100.0 / 22

IP Range: 192.168.100.0 - 192.168.103.255

HCX Deployment Network CIDR range

192.168.104.0 / 26

IP Range: 192.168.104.0 - 192.168.104.63

Note: Private cloud creation can take between 30 minutes to 2 hours.

## Enable Private Access to GCVE

Once the Private Cloud is provisioned, configure private access to the Private Cloud for high-throughput and low-latency data-path connection.

This will ensure that the VPC network where Cloud Volumes ONTAP instances are running is able to communicate with the GCVE Private Cloud. To do so, follow the [GCP documentation](#). For the Cloud Volume Service, establish a connection between VMware Engine and Cloud Volumes Service by performing a one-time peering between the tenant host projects. For detailed steps, follow this [link](#).

Tenant Project ID	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Status	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	● Active	● Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	● Active	● Connected

Sign in to vcenter using the [CloudOwner@gve.local](#) user. To access the credentials, go to the VMware Engine portal, Go to Resources, and select the appropriate private cloud. In the Basic info section, click the View link for either vCenter login info (vCenter Server, HCX Manager) or NSX-T login info (NSX Manager).

In a Windows virtual machine, open a browser and navigate to the vCenter web client URL (<https://10.0.16.6/>) and use the admin user name as [CloudOwner@gve.local](#) and paste the copied password. Similarly, NSX-T manager can also be accessed using the web client URL (<https://10.0.16.11/>) and use the admin user name and paste the copied password to create new segments or modify the existing tier gateways.

For connecting from an on-premises network to VMware Engine private cloud, leverage cloud VPN or Cloud Interconnect for appropriate connectivity and make sure the required ports are open. For detailed steps, follow this [link](#).

The screenshot shows two windows related to VMware vSphere:

- Login Screen:** A browser window titled "Login" with the URL "vcsa-57901.f7458c8f.europe-west3.gve.google/webss/SAML2/SSO/gve.local?SAMLRequest=zVRbb5swFH7fr0B%2B8wMhN6tJITWrVqlds5JN014mxoxwS...". It displays the VMware vSphere logo and a "LOG IN" button.
- vSphere Client Interface:** A separate window titled "vSphere - vcsa-57901.f7458c8f.europe-west3.gve.google". The address bar shows "Not secure | 10.0.16.6/ui/app/folder;nav=h/umvmmomi:Folder:group-d1452e8e7d-3188-4363-9e2c-448bc9b9979a/summary". The interface includes a navigation sidebar with options like Datacenter, Cluster, HCX Management, and Workload. The main pane displays the "Summary" tab for the selected cluster, showing details such as Version: 7.0.1, Build: 18392253, Last Updated: Sep 22, 2021, 6:49 AM, and Last File-Based Backup: Not scheduled. It also shows resource usage statistics for CPU, Memory, and Storage.

## NetApp Storage options for Public Cloud Providers

Explore the options for NetApp as storage in the three major hyperscalers.

## AWS / VMC

AWS supports NetApp storage in the following configurations:

- FSx ONTAP as guest connected storage
- Cloud Volumes ONTAP (CVO) as guest connected storage
- FSx ONTAP as a native datastore<sup>1</sup>

View the detailed [guest connect storage options for VMC](#).

Read more about FSx ONTAP as a native datastore public preview from the AWS Press Release (COMING SOON!).

## Azure / AVS

Azure supports NetApp storage in the following configurations:

- Azure NetApp Files (ANF) as guest connected storage
- Cloud Volumes ONTAP (CVO) as guest connected storage
- Azure NetApp Files (ANF) as a native datastore<sup>1</sup>

View the detailed [guest connect storage options for AVS](#).

Read more about [Azure NetApp Files \(ANF\) as a native datastore - Public Preview](#).

## GCP / GCVE

Google Cloud supports NetApp storage in the following configurations:

- Cloud Volumes ONTAP (CVO) as guest connected storage
- Cloud Volumes Service (CVS) as guest connected storage
- Cloud Volumes Service (CVS) as a native datastore<sup>1</sup>

View the detailed [guest connect storage options for GCVE](#).

Read more about [Cloud Volumes Service \(CVS\) as a native datastore<sup>1</sup>](#).



1 - Currently in Private Preview

## NetApp Guest Connected Storage Options for AWS

AWS supports guest connected NetApp storage with the native FSx service (FSx ONTAP) or with Cloud Volumes ONTAP (CVO).

### FSx ONTAP

Amazon FSx for NetApp ONTAP is a fully managed service that provides highly reliable, scalable, high-performing, and feature-rich file storage built on NetApp's popular ONTAP file system. FSx for ONTAP combines the familiar features, performance, capabilities, and API operations of NetApp file systems with the agility, scalability, and simplicity of a fully managed AWS service.

FSx for ONTAP provides feature-rich, fast, and flexible shared file storage that's broadly accessible from Linux,

Windows, and macOS compute instances running in AWS or on premises. FSx for ONTAP offers high-performance solid state drive (SSD) storage with submillisecond latencies. With FSx for ONTAP, you can achieve SSD levels of performance for your workload while paying for SSD storage for only a small fraction of your data.

Managing your data with FSx for ONTAP is easier because you can snapshot, clone, and replicate your files with the click of a button. In addition, FSx for ONTAP automatically tiers your data to lower-cost, elastic storage, lessening the need for you to provision or manage capacity.

FSx for ONTAP also provides highly available and durable storage with fully managed backups and support for cross-Region disaster recovery. To make it easier to protect and secure your data, FSx for ONTAP supports popular data security and antivirus applications.

## FSx ONTAP as guest connected storage

### Configure Amazon FSx for NetApp ONTAP with VMware Cloud on AWS

Amazon FSx for NetApp ONTAP files shares and LUNs can be mounted from VMs that are created within the VMware SDDC environment at VMware Cloud at AWS. The volumes can also be mounted on the Linux client and mapped on the Windows client using the NFS or SMB protocol, and LUNS can be accessed on Linux or Windows clients as block devices when mounted over iSCSI. Amazon FSx for the NetApp ONTAP file system can be set up quickly with the following steps.



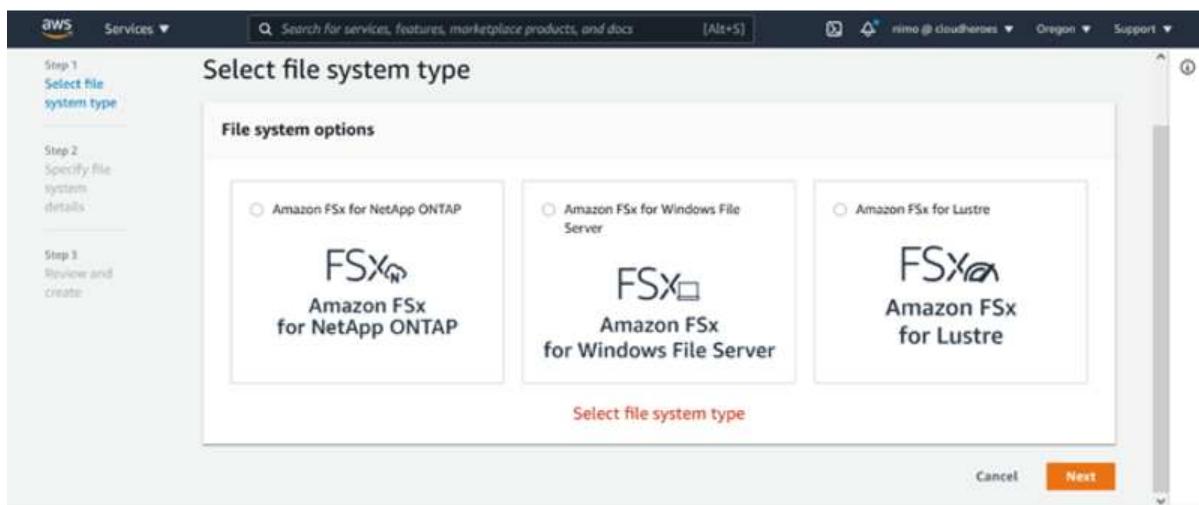
Amazon FSx for NetApp ONTAP and VMware Cloud on AWS must be in the same availability zone to achieve better performance and avoid data transfer charges between availability zones.



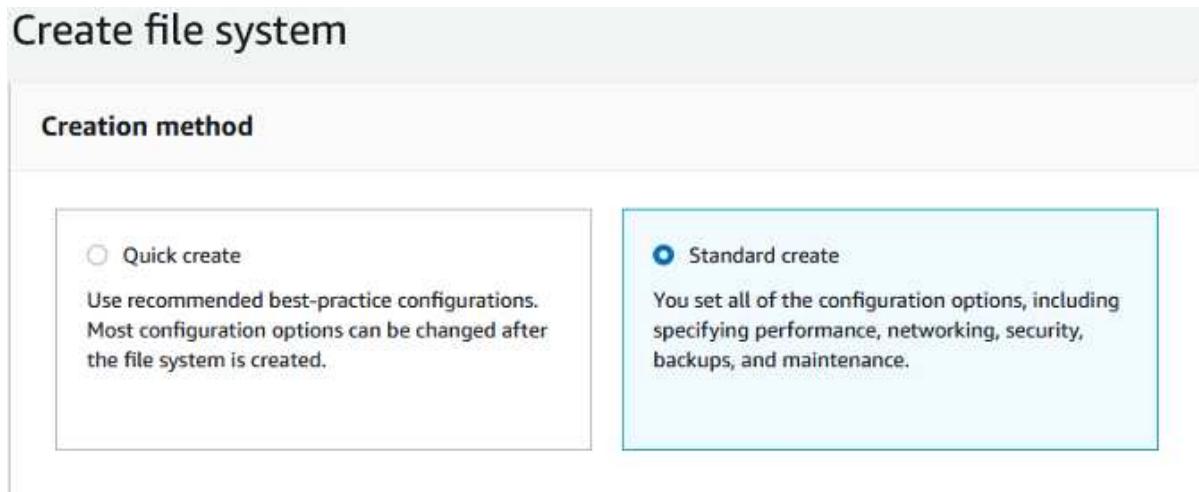
## Create and mount Amazon FSx for ONTAP volumes

To create and mount Amazon FSx for NetApp ONTAP file system, complete the following steps:

1. Open the [Amazon FSx console](#) and choose Create file system to start the file system creation wizard.
2. On the Select File System Type page, choose Amazon FSx for NetApp ONTAP, and then choose Next. The Create File System page appears.



3. In the Networking section, for Virtual Private Cloud (VPC), choose the appropriate VPC and preferred subnets along with the route table. In this case, vmcfsx2.vpc is selected from the dropdown.



4. For the creation method, choose Standard Create. You can also choose Quick Create, but this document uses the Standard create option.

## File system details

File system name - optional [Info](#)

vmcfsxval2

Maximum of 256 Unicode letters, whitespace, and numbers, plus + - = . \_ : /

SSD storage capacity [Info](#)

1024

Minimum 1024 GB; Maximum 192 TB.

Provisioned SSD IOPS

Amazon FSx provides 3 IOPS per GB of storage capacity. You can also provision additional SSD IOPS as needed.

Automatic (3 IOPS per GB of SSD storage)

User-provisioned

Throughput capacity [Info](#)

The sustained speed at which the file server hosting your file system can serve data. The file server can also burst to higher speeds for periods of time.

512 MB/s (Recommended)

5. In the Networking section, for Virtual Private Cloud (VPC), choose the appropriate VPC and preferred subnets along with the route table. In this case, vmcfsx2.vpc is selected from the dropdown.

## Network & security

Virtual Private Cloud (VPC) [Info](#)

Specify the VPC from which your file system is accessible.

vmcfsx2.vpc | vpc-0d1c764bcc495e805

VPC Security Groups [Info](#)

Specify VPC Security Groups to associate with your file system's network interface.

Choose VPC security group(s)

sg-018896ea218164ccb (default) 

Preferred subnet [Info](#)

Specify the preferred subnet for your file system.

subnet02.sn | subnet-013675849a5b99b3c (us-west-2b)

Standby subnet

subnet01.sn | subnet-0ef956cebf539f970 (us-west-2a)

VPC route tables

Specify the VPC route tables associated with your file system.

VPC's default route table

Select one or more VPC route tables

Endpoint IP address range

Specify the IP address range in which the endpoints to access your file system will be created

No preference

Select an IP address range



In the Networking section, for Virtual Private Cloud (VPC), choose the appropriate VPC and preferred subnets along with the route table. In this case, vmcfsx2.vpc is selected from the dropdown.

6. In the Security & Encryption section, for the Encryption Key, choose the AWS Key Management Service (AWS KMS) encryption key that protects the file system's data at rest. For the File System Administrative Password, enter a secure password for the fsxadmin user.

## Security & encryption

### Encryption key [Info](#)

AWS Key Management Service (KMS) encryption key that protects your file system data at rest.

aws/fsx (default)

Description	Account	KMS key ID
Default master key that protects my FSx resources when no other key is defined	139763910815	72745367-7bb0-499c-acc0-4f2c0a80e7c5

### File system administrative password

Password for this file system's "fsxadmin" user, which you can use to access the ONTAP CLI or REST API.

- Don't specify a password  
 Specify a password

Password

\*\*\*\*\*

Confirm password

\*\*\*\*\*

7. In virtual machine and specify the password to use with vsadmin for administering ONTAP using REST APIs or the CLI. If no password is specified, a fsxadmin user can be used for administering the SVM. In the Active Directory section, make sure to join Active Directory to the SVM for provisioning SMB shares. In the Default Storage Virtual Machine Configuration section, provide a name for the storage in this validation, SMB shares are provisioned using a self-managed Active Directory domain.

## Default storage virtual machine configuration

Storage virtual machine name

vmcfsxval2svm

SVM administrative password

Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.

- Don't specify a password
- Specify a password

Password

\*\*\*\*\*

Confirm password

\*\*\*\*\*

Active Directory

Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.

- Do not join an Active Directory
- Join an Active Directory

8. In the Default Volume Configuration section, specify the volume name and size. This is an NFS volume. For Storage Efficiency, choose Enabled to turn on the ONTAP storage efficiency features (compression, deduplication, and compaction) or Disabled to turn them off.

## Default volume configuration

Volume name

vol1

Maximum of 203 alphanumeric characters, plus \_.

Junction path

/vol1

The location within your file system where your volume will be mounted.

Volume size

1024



Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

- Enabled (recommended)
- Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

Auto



9. Review the file system configuration shown on the Create File System page.

10. Click Create File System.

Screenshot of the AWS FSx console showing the creation of a Storage virtual machine (SVM).

**Left Navigation Pane:**

- Amazon FSx
- File systems
- Backups
- ONTAP
  - Storage virtual machines
  - Volumes
- Windows File Server
- Lustre
  - Data repository tasks
- FSx on Service Quotas

**File systems (3) Table:**

File system name	File system ID	Status	Deployment type	Storage type	Size
fsxntapcifs	fs-014c28399be9c1f9f	Available	Multi-AZ	SSD	1.0 TB
vmcfsxval2	fs-040eacc5d0ac31017	Available	Multi-AZ	SSD	1.0 TB
fsxntapsql	fs-0ab4b447ebd6082aa	Available	Multi-AZ	SSD	2.0 TB

**Storage virtual machines (SVMs) (2) Table:**

SVM name	SVM ID	Status	Creation time	Active Directory
fsxsmbtesting01	svm-075dcfbe2cfa2ece9	Created	2021-10-19 15:17:08 UTC +01:00	FSXTESTING.LOCAL
vmcfsxval2svm	svm-095db076341561212	Created	2021-10-15 15:16:54 UTC +01:00	-

**fsxsmbtesting01 (svm-075dcfbe2cfa2ece9) Summary:**

SVM ID svm-075dcfbe2cfa2ece9	Creation time 2021-10-19T15:17:08+01:00	Active Directory FSXTESTING.LOCAL
SVM name fsxsmbtesting01	Lifecycle state Created	Net BIOS name FSXSMBTESTING01
UUID 4a50e659-30e7-11ec-ac4f-f3ad92a6a735	Subtype DEFAULT	Fully qualified domain name FSXTESTING.LOCAL
File system ID fs-040eacc5d0ac31017		Service account username administrator
		Organizational unit distinguished name CN=Computers

For more detailed information, see [Getting started with Amazon FSx for NetApp ONTAP](#).

After the file system is created as above, create the volume with the required size and protocol.

1. Open the [Amazon FSx console](#).
2. In the left navigation pane, choose File systems, and then choose the ONTAP file system that you want to create a volume for.
3. Select the Volumes tab.

4. Select the Create Volume tab.
5. The Create Volume dialog box appears.

For demo purposes, an NFS volume is created in this section that can be easily mounted on VMs running on VMware cloud on AWS. nfsdemovol01 is created as depicted below:

The screenshot shows the 'Create volume' dialog box with the following settings:

- File system:** fs-040eacc5d0ac31017 | vmcfsv12
- Storage virtual machine:** svm-095db076341561212 | vmcfsv12svm
- Volume name:** nfsdemovol01
- Junction path:** /nfsdemovol01
- Volume size:** 1024
- Storage efficiency:** Enabled (recommended) is selected.
- Capacity pool tiering policy:** Auto

At the bottom right, there are 'Cancel' and 'Confirm' buttons, with 'Confirm' being highlighted.

## Mount FSx ONTAP volume on Linux client

To mount the FSx ONTAP volume created in the previous step. from the Linux VMs within VMC on AWS SDDC, complete the following steps:

1. Connect to the designated Linux instance.
2. Open a terminal on the instance using Secure Shell (SSH) and log in with the appropriate credentials.
3. Make a directory for the volume's mount point with the following command:

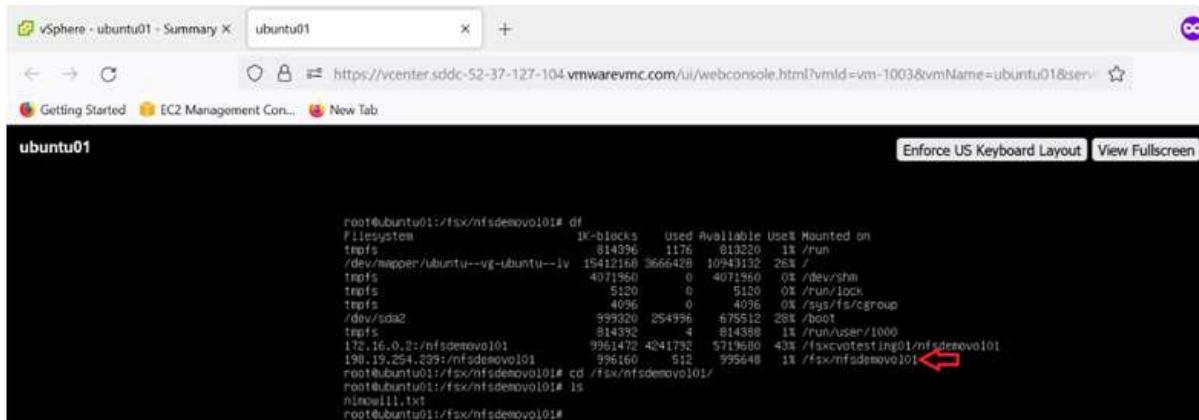
```
$ sudo mkdir /fsx/nfsdemovol01
```

4. Mount the Amazon FSx for NetApp ONTAP NFS volume to the directory that is created in the previous step.

```
sudo mount -t nfs nfsvers=4.1,198.19.254.239:/nfsdemovol01  
/fsx/nfsdemovol01
```

```
root@ubuntu01:/fsx/nfsdemovol01# mount -t nfs 198.19.254.239:/nfsdemovol01 /fsx/nfsdemovol01
```

5. Once executed, run the df command to validate the mount.



```
root@ubuntu01:/fsx/nfsdemovol01# df  
Filesystem 1K-blocks Used Available Use% Mounted on  
tmpfs 814396 1176 813220 1% /run  
/dev/mapper/ubuntu--vg-ubuntu--lv 15412160 3666428 10943132 26% /  
tmpfs 4071960 0 4071960 0% /dev/shm  
tmpfs 5120 0 5120 0% /run/lock  
tmpfs 4096 0 4096 0% /sys/fs/cgroup  
/dev/sda2 599320 254956 675512 28% /boot  
tmpfs 814392 4 814388 1% /run/user/1000  
172.16.0.2:/nfsdemovol01 9961472 4241732 5719680 43% /fsx/vcatesting01/nfsdemovol01  
root@ubuntu01:/fsx/nfsdemovol01# cd /fsx/nfsdemovol01/  
root@ubuntu01:/fsx/nfsdemovol01# ls  
nfsnull1.txt  
root@ubuntu01:/fsx/nfsdemovol01#
```

► [https://docs.netapp.com/us-en/netapp-solutions/media/vmc\\_linux\\_vm\\_nfs.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/vmc_linux_vm_nfs.mp4) (video)



## Attach FSx ONTAP volumes to Microsoft Windows clients

To manage and map file shares on an Amazon FSx file system, the Shared Folders GUI must be used.

1. Open the Start menu and run fsmgmt.msc using Run As Administrator. Doing this opens the Shared Folders GUI tool.
2. Click Action > All tasks and choose Connect to Another Computer.
3. For Another Computer, enter the DNS name for the storage virtual machine (SVM). For example, FSXSMBTESTING01.FSXTESTING.LOCAL is used in this example.



To find the SVM's DNS name on the Amazon FSx console, choose Storage Virtual Machines, choose SVM, and then scroll down to Endpoints to find the SMB DNS name. Click OK. The Amazon FSx file system appears in the list for the Shared Folders.

### Endpoints

Management DNS name	Management IP address
svm-075dcfbe2cfa2ece9.fs-040eacc5d0ac31017.fsx.us-west-2.amazonaws.com	198.19.254.9
NFS DNS name	NFS IP address
svm-075dcfbe2cfa2ece9.fs-040eacc5d0ac31017.fsx.us-west-2.amazonaws.com	198.19.254.9
SMB DNS name	SMB IP address
FSXSMBTESTING01.FSXTESTING.LOCAL	198.19.254.9
iSCSI DNS name	iSCSI IP addresses
iscsi.svm-075dcfbe2cfa2ece9.fs-040eacc5d0ac31017.fsx.us-west-2.amazonaws.com	10.222.2.224, 10.222.1.94

4. In the Shared Folders tool, choose Shares in the left pane to see the active shares for the Amazon FSx file system.

Computer Management

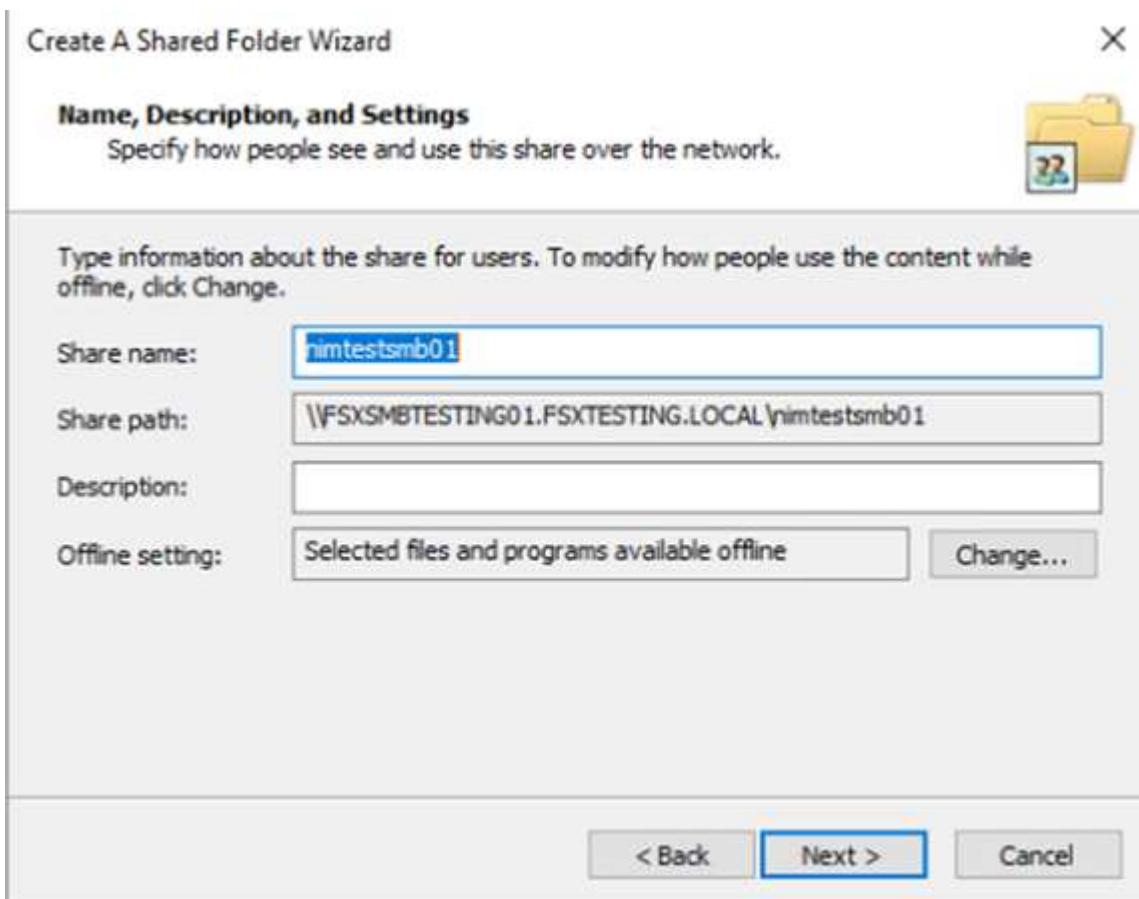
File Action View Help

Computer Management (FSXMBTESTING01.FSXTESTING.LOCAL)

- System Tools
  - Task Scheduler
  - Event Viewer
  - Shared Folders
    - Shares
    - Sessions
    - Open Files
  - Local Users and Groups
  - Performance
  - Device Manager
- Storage
  - Windows Server Backup
  - Disk Management
- Services and Applications

Share Name	Folder Path	Type	# Client Connections	Description
c\$	C:\	Windows	0	
ipc\$		Windows	1	
smbdemo...	C:\smbdemovol01	Windows	1	
testnimvol	C:\testnimvol	Windows	0	

5. Now choose a new share and complete the Create a Shared Folder wizard.



## Create A Shared Folder Wizard



### Sharing was Successful

#### Status:

You have successfully completed the Share a Folder Wizard.

#### Summary:

You have selected the following share settings on \\FSXSMBTESTING01.FSXTESTING.LOCAL:  
Folder path: C:\\nimtestsmb01  
Share name: nimtestsmb01  
Share path: \\FSXSMBTESTING01.FSXTESTING.LOCAL\\nimtestsmb01

When I click Finish, run the wizard again to share another folder

To close this wizard, click Finish.

**Finish**

**Cancel**

To learn more about creating and managing SMB shares on an Amazon FSx file system, see [Creating SMB Shares](#).

- After connectivity is in place, the SMB share can be attached and used for application data. To accomplish this, Copy the share path and use the Map Network Drive option to mount the volume on the VM running on VMware Cloud on the AWS SDDC.

The screenshot shows the VMware Cloud Services - Log In X: vSphere - vmcdc01 - Summary window. The URL is https://vcenter.sddc-52-37-127-104.vmwarevm.com/ui/webconsole.html?vmId=vm-1005&vmName=vmcdc01. The page displays the Computer Management interface for the vmcdc01 VM. On the left, the navigation pane shows System Tools, Storage, and Device Manager. The main pane shows the 'Shares' section under Computer Management. A red arrow points to the 'The PC' share entry, which is highlighted. The 'Actions' column for this share shows options like 'Share', 'More Actions', and 'Unshare'. The table lists the share details:

Name	Items	Date modified	Type	Size
new-folder01	new-item01	10/19/2021 8:21 AM	File/folder	
new-item01	new-item01	10/22/2021 3:25 AM	File/folder	
new-item02	new-item02	10/22/2021 3:25 AM	File/folder	
new-item03	new-item03	10/22/2021 3:25 AM	File/folder	

## Connect a FSx for NetApp ONTAP LUN to a host using iSCSI

- ▶ [https://docs.netapp.com/us-en/netapp-solutions/media/vmc\\_windows\\_vm\\_iscsi.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/vmc_windows_vm_iscsi.mp4) (video)

iSCSI traffic for FSx traverses the VMware Transit Connect/AWS Transit Gateway via the routes provided in the previous section. To configure a LUN in Amazon FSx for NetApp ONTAP, follow the documentation found [here](#).

On Linux clients, make sure that the iSCSI daemon is running. After the LUNs are provisioned, refer to the detailed guidance on iSCSI configuration with Ubuntu (as an example) [here](#).

In this paper, connecting the iSCSI LUN to a Windows host is depicted:



## Provision a LUN in FSx for NetApp ONTAP:

1. Access the NetApp ONTAP CLI using the management port of the FSx for the ONTAP file system.
2. Create the LUNs with the required size as indicated by the sizing output.

```
FsxId040eacc5d0ac31017::> lun create -vserver vmcfsxval2svm  
-volume nimfsxscsivol -lun nimofsslun01 -size 5gb -ostype  
windows -space-reserve enabled
```

In this example, we created a LUN of size 5g (5368709120).

3. Create the necessary igroups to control which hosts have access to specific LUNs.

```
FsxId040eacc5d0ac31017::> igrup create -vserver vmcfsxval2svm  
-igroup winIG -protocol iscsi -ostype windows -initiator  
iqn.1991-05.com.microsoft:vmcdc01.fsxtesting.local

FsxId040eacc5d0ac31017::> igrup show

Vserver      Igroup          Protocol OS Type  Initiators
-----  -----  -----  -----
-----  -----  -----  -----
vmcfsxval2svm

      ubuntu01      iscsi      linux      iqn.2021-
10.com.ubuntu:01:initiator01

vmcfsxval2svm

      winIG      iscsi      windows    iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local
```

Two entries were displayed.

4. Map the LUNs to igroups using the following command:

```

FsxId040eacc5d0ac31017::> lun map -vserver vmcfsxval2svm -path
/vol/nimfsxscsivol/nimofsxlun01 -igroup winIG

FsxId040eacc5d0ac31017::> lun show

Vserver      Path          State   Mapped   Type
Size

-----
-----
vmcfsxval2svm

/vol/blocktest01/lun01      online   mapped   linux
5GB

vmcfsxval2svm

/vol/nimfsxscsivol/nimofsxlun01 online   mapped
windows      5GB

```

Two entries were displayed.

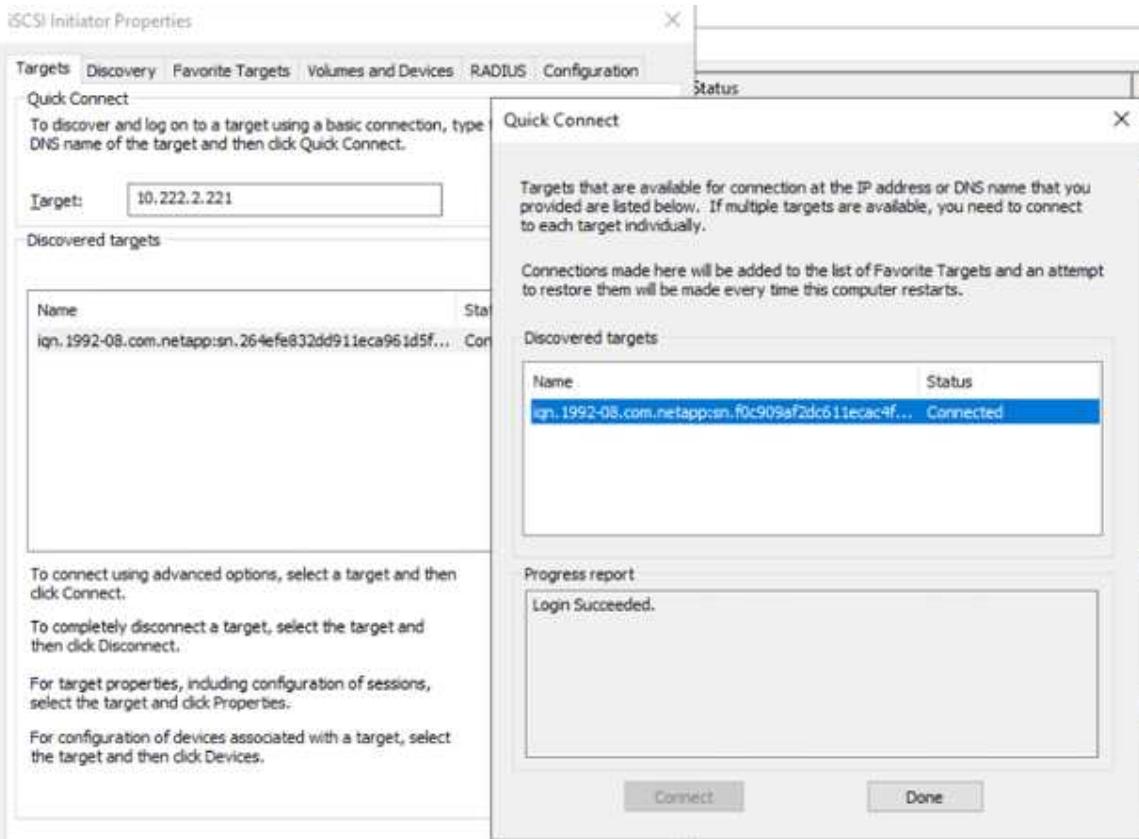
##### 5. Connect the newly provisioned LUN to a Windows VM:

To connect the new LUN to a Windows host residing on VMware cloud on AWS SDDC, complete the following steps:

- RDP to the Windows VM hosted on the VMware Cloud on AWS SDDC.
- Navigate to Server Manager > Dashboard > Tools > iSCSI Initiator to open the iSCSI Initiator Properties dialog box.
- From the Discovery tab, click Discover Portal or Add Portal and then enter the IP address of the iSCSI target port.
- From the Targets tab, select the target discovered and then click Log On or Connect.
- Select Enable Multipath, and then select “Automatically Restore This Connection When the Computer Starts” or “Add This Connection to the List of Favorite Targets”. Click Advanced.

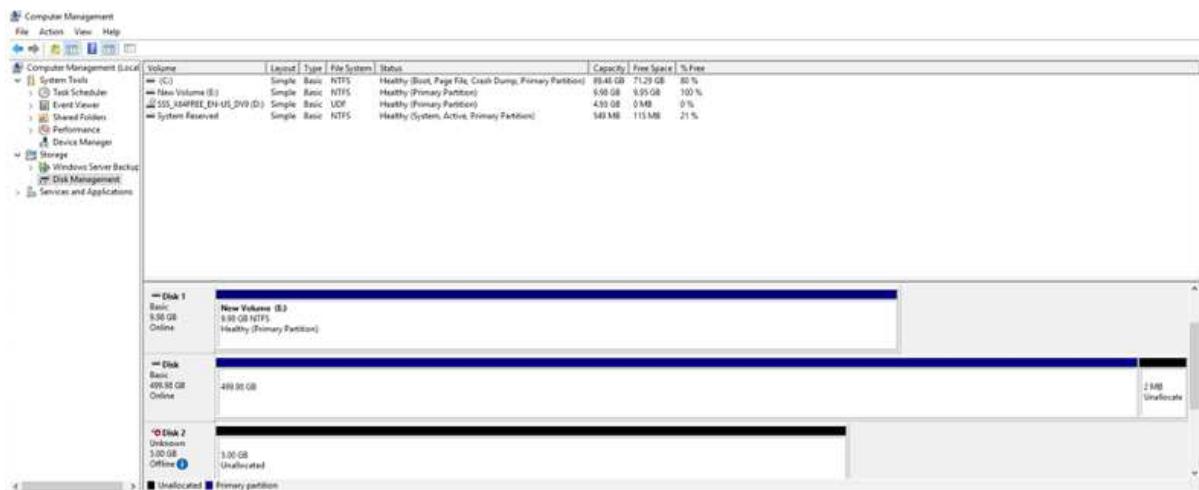


The Windows host must have an iSCSI connection to each node in the cluster. The native DSM selects the best paths to use.



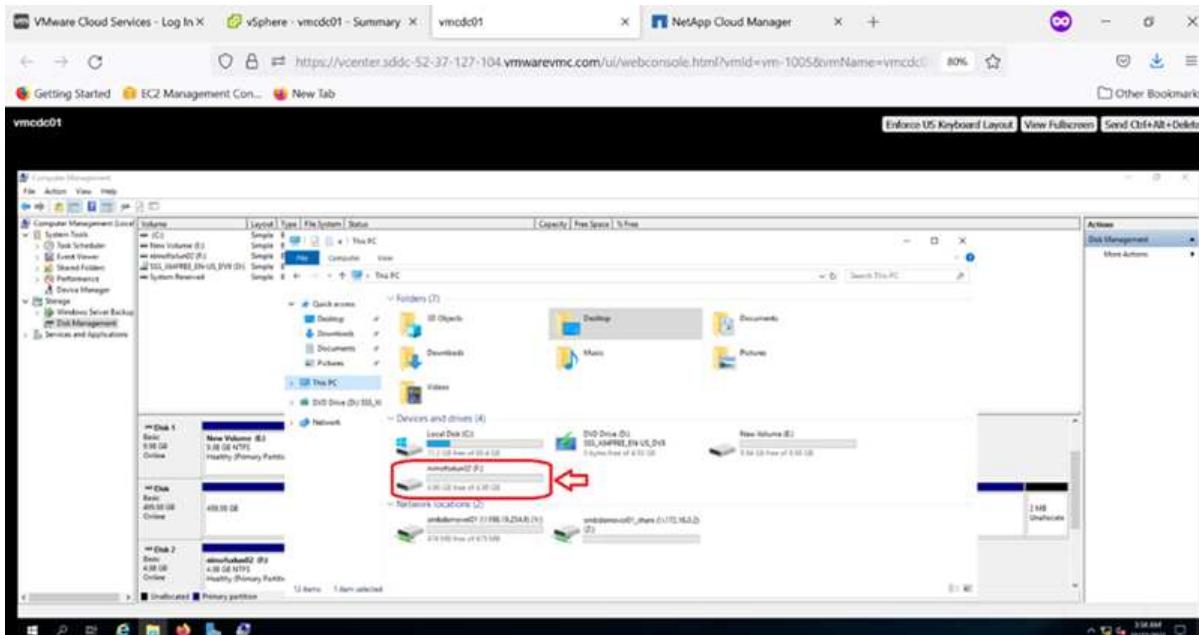
LUNs on the storage virtual machine (SVM) appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

1. Open the Windows Computer Management utility: Start > Administrative Tools > Computer Management.
2. Expand the Storage node in the navigation tree.
3. Click Disk Management.
4. Click Action > Rescan Disks.



When a new LUN is first accessed by the Windows host, it has no partition or file system. Initialize the LUN and, optionally, format the LUN with a file system by completing the following steps:

1. Start Windows Disk Management.
2. Right-click the LUN, and then select the required disk or partition type.
3. Follow the instructions in the wizard. In this example, drive F: is mounted.



## Cloud Volumes ONTAP (CVO)

Cloud volumes ONTAP, or CVO, is the industry-leading cloud data management solution built on NetApp's ONTAP storage software, available natively on Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).

It is a software-defined version of ONTAP that consumes cloud-native storage, allowing you to have the same storage software in the cloud and on-premises, reducing the need to retrain your IT staff in all-new methods to manage your data.

CVO gives customers the ability to seamlessly move data from the edge, to the data center, to the cloud and back, bringing your hybrid cloud together — all managed with a single-pane management console, NetApp Cloud Manager.

By design, CVO delivers extreme performance and advanced data management capabilities to satisfy even your most demanding applications in the cloud

## Cloud Volumes ONTAP (CVO) as guest connected storage



## Deploy new Cloud Volumes ONTAP instance in AWS (do it yourself)

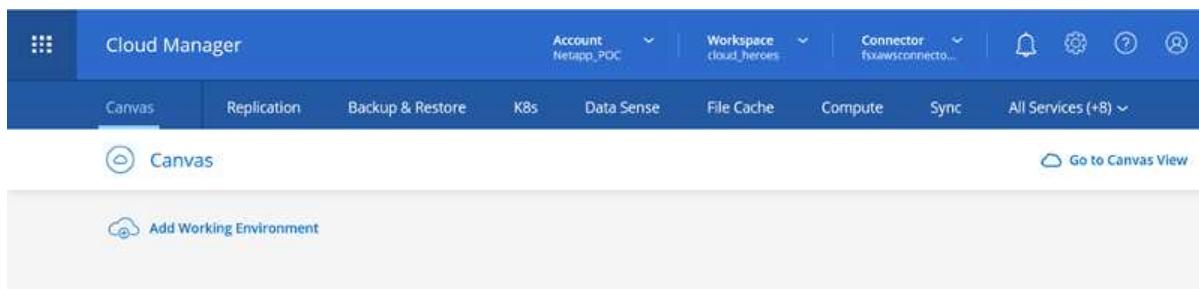
Cloud Volumes ONTAP shares and LUNs can be mounted from VMs that are created in the VMware Cloud on AWS SDDC environment. The volumes can also be mounted on native AWS VM Linux Windows clients, and LUNs can be accessed on Linux or Windows clients as block devices when mounted over iSCSI because Cloud Volumes ONTAP supports iSCSI, SMB, and NFS protocols. Cloud Volumes ONTAP volumes can be set up in a few simple steps.

To replicate volumes from an on-premises environment to the cloud for disaster recovery or migration purposes, establish network connectivity to AWS, either using a site-to-site VPN or DirectConnect. Replicating data from on-premises to Cloud Volumes ONTAP is outside the scope of this document. To replicate data between on-premises and Cloud Volumes ONTAP systems, see [Setting up data replication between systems](#).

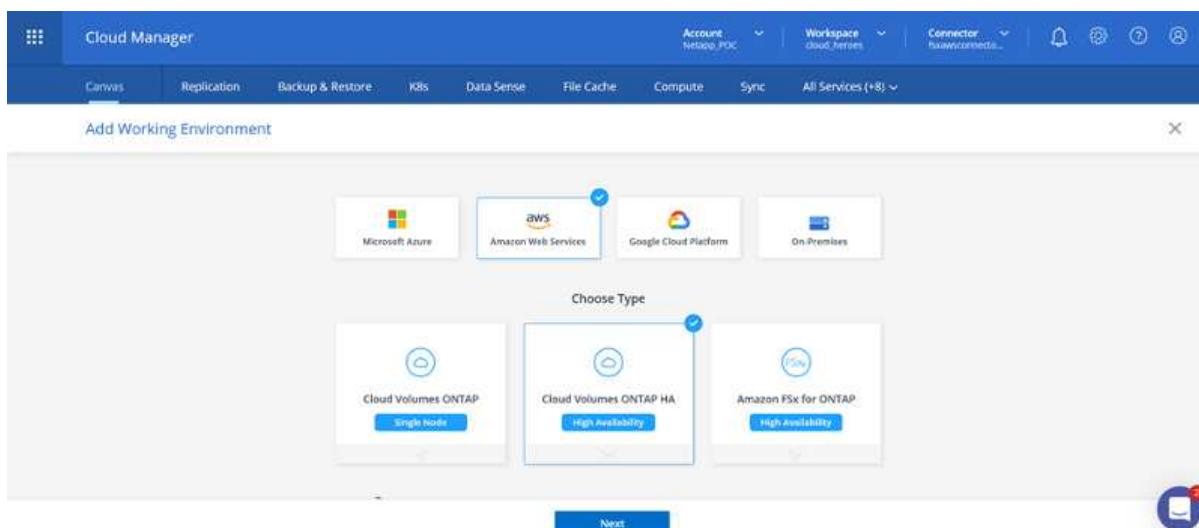


Use the [Cloud Volumes ONTAP sizer](#) to accurately size the Cloud Volumes ONTAP instances. Also, monitor on-premises performance to use as inputs in the Cloud Volumes ONTAP sizer.

1. Log into NetApp Cloud Central; the Fabric View screen is displayed. Locate the Cloud Volumes ONTAP tab and select Go to Cloud Manager. After you are logged in, the Canvas screen is displayed.



2. On the Cloud Manager home page, click Add a Working Environment and then select AWS as the cloud and the type of the system configuration.



3. Provide the details of the environment to be created including the environment name and admin credentials. Click Continue.

#### Create a New Working Environment

#### Details and Credentials

<a href="#">↑ Previous Step</a>	Instance Profile Credential Name	139763910815 Account ID	netapp.com-cloud-volumes-... Marketplace Subscription	<a href="#">Edit Credentials</a>													
<table border="1"><tr><td><b>Details</b></td><td><b>Credentials</b></td></tr><tr><td>Working Environment Name (Cluster Name) <input type="text" value="fsxvcvtesting01"/></td><td>User Name <input type="text" value="admin"/></td></tr><tr><td><a href="#">+ Add Tags</a>      Optional Field   Up to four tags</td><td>Password <input type="password" value="*****"/></td></tr><tr><td></td><td>Confirm Password <input type="password" value="*****"/></td></tr><tr><td colspan="5" style="text-align: center;"><a href="#">Continue</a></td></tr></table>					<b>Details</b>	<b>Credentials</b>	Working Environment Name (Cluster Name) <input type="text" value="fsxvcvtesting01"/>	User Name <input type="text" value="admin"/>	<a href="#">+ Add Tags</a> Optional Field   Up to four tags	Password <input type="password" value="*****"/>		Confirm Password <input type="password" value="*****"/>	<a href="#">Continue</a>				
<b>Details</b>	<b>Credentials</b>																
Working Environment Name (Cluster Name) <input type="text" value="fsxvcvtesting01"/>	User Name <input type="text" value="admin"/>																
<a href="#">+ Add Tags</a> Optional Field   Up to four tags	Password <input type="password" value="*****"/>																
	Confirm Password <input type="password" value="*****"/>																
<a href="#">Continue</a>																	

4. Select the add-on services for Cloud Volumes ONTAP deployment, including Cloud Data Sense, Cloud Backup, and Cloud Insights. Click Continue.

#### Create a New Working Environment

#### Services

 Data Sense & Compliance	<input checked="" type="checkbox"/>
 Backup to Cloud	<input checked="" type="checkbox"/>
 Monitoring	<input checked="" type="checkbox"/>
<a href="#">Continue</a>	

5. On the HA Deployment Models page, choose the Multiple Availability Zones configuration.

#### Create a New Working Environment

#### HA Deployment Models

<a href="#">↑ Previous Step</a>	<table border="1"><tr><td><b>Multiple Availability Zones</b></td></tr><tr><td> Provides maximum protection against AZ failures.</td></tr><tr><td> Enables selection of 3 availability zones.</td></tr><tr><td> An HA node serves data if its partner goes offline.</td></tr><tr><td><a href="#">Extended Info</a></td></tr></table>	<b>Multiple Availability Zones</b>	 Provides maximum protection against AZ failures.	 Enables selection of 3 availability zones.	 An HA node serves data if its partner goes offline.	<a href="#">Extended Info</a>	<table border="1"><tr><td><b>Single Availability Zone</b></td></tr><tr><td> Protects against failures within a single AZ.</td></tr><tr><td> Single availability zone. HA nodes are in a placement group, spread across distinct underlying hardware.</td></tr><tr><td> An HA node serves data if its partner goes offline.</td></tr><tr><td><a href="#">Extended Info</a></td></tr></table>	<b>Single Availability Zone</b>	 Protects against failures within a single AZ.	 Single availability zone. HA nodes are in a placement group, spread across distinct underlying hardware.	 An HA node serves data if its partner goes offline.	<a href="#">Extended Info</a>
<b>Multiple Availability Zones</b>												
 Provides maximum protection against AZ failures.												
 Enables selection of 3 availability zones.												
 An HA node serves data if its partner goes offline.												
<a href="#">Extended Info</a>												
<b>Single Availability Zone</b>												
 Protects against failures within a single AZ.												
 Single availability zone. HA nodes are in a placement group, spread across distinct underlying hardware.												
 An HA node serves data if its partner goes offline.												
<a href="#">Extended Info</a>												
<a href="#">Continue</a>												

6. On the Region & VPC page, enter the network information and then click Continue.

Create a New Working Environment

### Region & VPC

↑ Previous Step

AWS Region	VPC	Security group
US West   Oregon	vpc-0d1c764bcc495e805 - 10.222.0.0/16	Use a generated security group

Node 1:	Node 2:	Mediator:
Availability Zone	Availability Zone	Availability Zone
us-west-2a	us-west-2b	us-west-2c
Subnet	Subnet	Subnet
10.222.1.0/24	10.222.2.0/24	10.222.3.0/24

**Continue**

7. On the Connectivity and SSH Authentication page, choose connection methods for the HA pair and the mediator.

Create a New Working Environment

### Connectivity & SSH Authentication

↑ Previous Step

Nodes	Mediator
SSH Authentication Method	Security Group
Password	Use a generated security group
	Key Pair Name
	nimokey
	Internet Connection Method
	Public IP address

**Continue**

8. Specify the floating IP addresses and then click Continue.

Create a New Working Environment

### Floating IPs

↑ Previous Step

Floating IP addresses are required for cluster and SVM access and for NFS and CIFS data access. These floating IPs can migrate between HA nodes if failures occur. To access the data from outside the VPC, [you can set up an AWS transit gateway](#).

You must specify IP addresses that are outside of the CIDR blocks for all VPCs in the selected AWS region.

Floating IP address for cluster management	172.16.0.1
Floating IP address 1 for NFS and CIFS data	172.16.0.2
Floating IP address 2 for NFS and CIFS data	172.16.0.3
Floating IP address for SVM management (Optional)	172.16.0.4

**Continue**

9. Select the appropriate route tables to include routes to the floating IP addresses and then click Continue.

Create a New Working Environment

Route Tables

↑ Previous Step

Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volumes ONTAP HA pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair.

Additional information ⓘ

Name	Main	ID	Associate with Subnet	Tags
<input checked="" type="checkbox"/>	Yes	rtb-00b2d30c3f68fdbdd	0 Subnets	1 Tags

1 Route Tables | The main route table is the default for the VPC

Continue

10. On the Data Encryption page, choose AWS-managed encryption.

Create a New Working Environment

Data Encryption

↑ Previous Step

 AWS Managed Encryption

AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.

Default Master Key: aws/ebs

 Change Key

Continue

11. Select the license option: Pay-As-You-Go or BYOL for using an existing license. In this example, the Pay-As-You-Go option is used.

## Create a New Working Environment Cloud Volumes ONTAP Charging Methods & NSS Account

The screenshot shows the 'Cloud Volumes ONTAP Charging Methods' section. It includes a link to learn more about charging methods, two options for licensing ('Pay-As-You-Go by the hour' and 'Bring your own license'), and a 'Continue' button.

Cloud Volumes ONTAP Charging Methods

Learn more about our charging methods

Pay-As-You-Go by the hour

Bring your own license

NetApp Support Site Account (*Optional*)

Learn more about NetApp Support Site (NSS) accounts

To register this Cloud Volumes ONTAP to support, you should add NetApp Support Site Account.

Don't have a NetApp Support Site account? Select go to finish deploying this system. After it's created, use the [Support Registration option](#) to create an NSS account.

Continue

12. Select between several preconfigured packages available based on the type of workload to be deployed on the VMs running on the VMware cloud on AWS SDDC.

The screenshot shows the 'Preconfigured Packages' section. It displays four options: 'POC and small workloads' (Up to 500GB of storage), 'Database and application data production workloads', 'Cost effective DR' (Up to 500GB of storage), and 'Highest performance production workloads'. A 'Continue' button is at the bottom.

Create a New Working Environment

Preconfigured Packages

Select a preconfigured Cloud Volumes ONTAP system that best matches your needs, or create your own configuration. Preconfigured settings can be modified at a later time.

Change Configuration

POC and small workloads  
Up to 500GB of storage

Database and application data production workloads

Cost effective DR  
Up to 500GB of storage

Highest performance production workloads

Continue

13. On the Review & Approve page, review and confirm the selections. To create the Cloud Volumes ONTAP instance, click Go.

The screenshot shows the 'Review & Approve' page. It includes a summary of the instance details (e.g., Storage System: Cloud Volumes ONTAP HA, License Type: Cloud Volumes ONTAP Explore, Capacity Limit: 2TB), a note about NSS registration, and a checkbox for understanding resource allocation. A 'Go' button is at the bottom.

Create a New Working Environment

Review & Approve

Previous Step: [tsxcvotesting](#)

AWS | us-west-2 | HA

Show API request

This Cloud Volumes ONTAP instance will be registered with NetApp support under the NSS Account mchad.

I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. [More information >](#)

Overview Networking Storage

Storage System: Cloud Volumes ONTAP HA HA Deployment Model: Multiple Availability Zones

License Type: Cloud Volumes ONTAP Explore Encryption: AWS Managed

Capacity Limit: 2TB Customer Master Key: aws/ebs

Go

14. After Cloud Volumes ONTAP is provisioned, it is listed in the working environments on the Canvas page.

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8) ▾

Canvas Go to Tabular View

Add Working Environment

vmhseval2  
15a for ONTAP  
9 Volumes 26.49 GB Capacity AWS

fsxvotesting01  
Cloud Volumes ONTAP  
46.08 Capacity AWS

Amazon S3  
4 Buckets 2 Regions AWS

fsxvotesting01 Cloud Volumes ONTAP On

Cloud Volumes ONTAP | AWS | HA

DETAILS

SERVICES

Replication Off Enable

Backup & Restore Loading...



## Additional configurations for SMB volumes

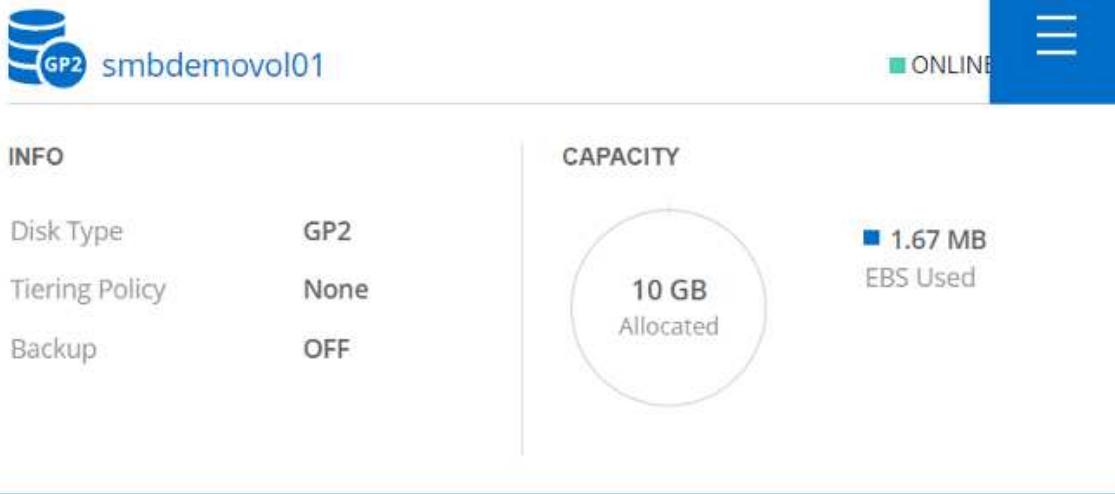
1. After the working environment is ready, make sure the CIFS server is configured with the appropriate DNS and Active Directory configuration parameters. This step is required before you can create the SMB volume.

The screenshot shows the AWS CloudFront console. In the top navigation bar, there is a blue ribbon with 'AWS' and 'AWS Managed Encryption'. Below the ribbon, there are tabs for 'Volumes', 'HA Status', 'Cost', and 'Replications'. On the left, there is a sidebar with a 'Create a CIFS server' button. The main area has fields for 'DNS Primary IP Address' (192.168.1.3), 'Active Directory Domain to join' (fsxtesting.local), 'DNS Secondary IP Address (Optional)', 'Credentials authorized to join the domain' (Username and Password), and 'Save' and 'Cancel' buttons. A small note at the bottom says 'Example: 127.0.0.1'.

2. Select the CVO instance to create the volume and click the Create Volume option. Choose the appropriate size and cloud manager chooses the containing aggregate or use advanced allocation mechanism to place on a specific aggregate. For this demo, SMB is selected as the protocol.

The screenshot shows the 'Create new volume in fsxvotesting01' interface. At the top, it says 'Volume Details, Protection & Protocol'. There are two main sections: 'Details & Protection' and 'Protocol'. In 'Details & Protection', there are fields for 'Volume Name' (smbdemovol01), 'Size (GB)' (100), and 'Snapshot Policy' (default). In 'Protocol', the 'CIFS' tab is selected. It shows 'Share name' (smbdemovol01\_share), 'Permissions' (Full Control), 'Users / Groups' (Everyone), and a note about valid users separated by a semicolon. At the bottom, there is a 'Continue' button.

3. After the volume is provisioned, it is available under the Volumes pane. Because a CIFS share is provisioned, you should give your users or groups permission to the files and folders and verify that those users can access the share and create a file.



4. After the volume is created, use the mount command to connect to the share from the VM running on the VMware Cloud in AWS SDDC hosts.
5. Copy the following path and use the Map Network Drive option to mount the volume on the VM running on the VMware Cloud in AWS SDDC.

**fsxvotesting01 (Multiple AZs)**

AWS | AWS

Volumes	HA Status	Cost	Replications
<a href="#">Mount Volume smbdemovol01</a>	<a href="#">Edit</a>	<a href="#">View Log</a>	<a href="#">Edit</a>

**Access from inside the VPC using Floating IP**

Auto failover between nodes  
The IP address automatically migrates between nodes if failures occur

Go to your machine and enter this command

```
\\"172.16.0.2\smbdemovol01_share
```

[Copy](#)

**Access from outside the VPC using AWS Private IP**

No auto failover between nodes  
The IP address does not migrate between nodes if failures occur

To avoid traffic between nodes, mount the volume by using the primary node's IP address:

```
\\"10.222.1.100\smbdemovol01_share
```

[Copy](#)

If the primary node goes offline, mount the volume by using the HA partner's IP address:

VMware Cloud - ntap-fsx-demo X vsphere - vmcd01 - Summary X vmcd01 X NetApp Cloud Manager X +

Getting Started EC2 Management Con... New Tab https://vcenter.sddc-S2-37-127-104.vmwarevmc.com/ui/webconsole.html?vmid=vm-1005&vmName=vmcd01 80% Other Bookmarks

Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

vmcd01

Server Manager • Dashboard

WELCOME TO SERVER MANAGER

File Home Share View

Dashboard Local Server All Servers AD DS DNS File and Storage Services

QUICKSTART

SEARCH HERE

AD DS

Manageability Events Services Performance DPA results

The PC - smbdemovol01\_share (172.16.0.2) (Z)

Name Date modified Type Size

name01 10/22/2021 11:11 AM File folder

name02 10/22/2021 11:11 AM File folder

name03 10/22/2021 11:11 AM File folder

name04 10/22/2021 11:11 AM File folder

DVD Drive (D) (00\_0)

Network

Manage Task View Help

20 AM 10/22/2021



## Connect the LUN to a host

To connect the Cloud Volumes ONTAP LUN to a host, complete the following steps:

1. On the Cloud Manager Canvas page, double-click the Cloud Volumes ONTAP working environment to create and manage volumes.
2. Click Add Volume > New Volume, select iSCSI, and click Create Initiator Group. Click Continue.

The screenshot shows two windows side-by-side. The top window is titled 'Volume Details, Protection & Protocol' and is part of the 'Create new volume in fsxvotesting01' process. It has tabs for 'Details & Protection' and 'Protocol'. Under 'Protocol', the 'iSCSI' tab is selected. The 'Initiator Group' section contains a radio button for 'Map Existing Initiator Groups' and a checkbox for 'Create Initiator Group'. The 'Operating System Type' dropdown is set to 'Windows'. Below these, a 'Select Initiator Groups:' section shows '1 (of 3) Groups' with a checkbox for 'winIG | windows' and the IQN 'iqn.1991-05.com.microsoft:vmcdc01.fsxtesting01'. The bottom right of this window has a 'Continue' button. The bottom window is a 'Server Manager - Dashboard' window for a server named 'vmcdc01'. It shows the 'File and Storage Services' role is installed. A file browser window is open showing a folder structure with files named 'monkey1', 'monkey2', and 'monkey3'. The status bar at the bottom of the dashboard window indicates the time as 7:25 AM and the date as Wednesday, October 20, 2021.

3. After the volume is provisioned, select the volume, and then click Target IQN. To copy the iSCSI Qualified Name (IQN), click Copy. Set up an iSCSI connection from the host to the LUN.

To accomplish the same for the host residing on the VMware Cloud on AWS SDDC, complete the following steps:

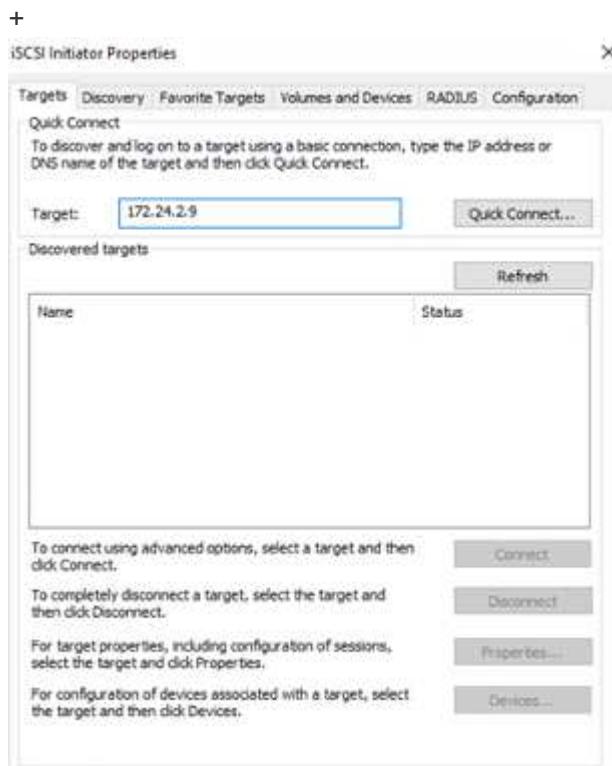
- a. RDP to the VM hosted on VMware cloud on AWS.
- b. Open the iSCSI Initiator Properties dialog box: Server Manager > Dashboard > Tools > iSCSI Initiator.
- c. From the Discovery tab, click Discover Portal or Add Portal and then enter the IP address of the

iSCSI target port.

- d. From the Targets tab, select the target discovered and then click Log On or Connect.
- e. Select Enable Multipath, and then select Automatically Restore This Connection When the Computer Starts or Add This Connection to the List of Favorite Targets. Click Advanced.

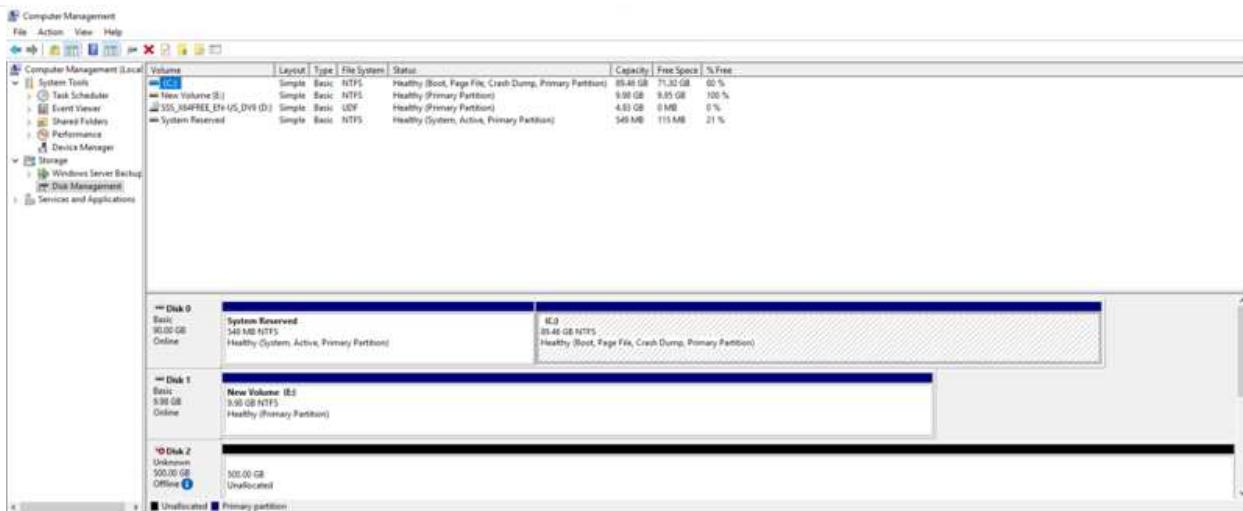


The Windows host must have an iSCSI connection to each node in the cluster. The native DSM selects the best paths to use.



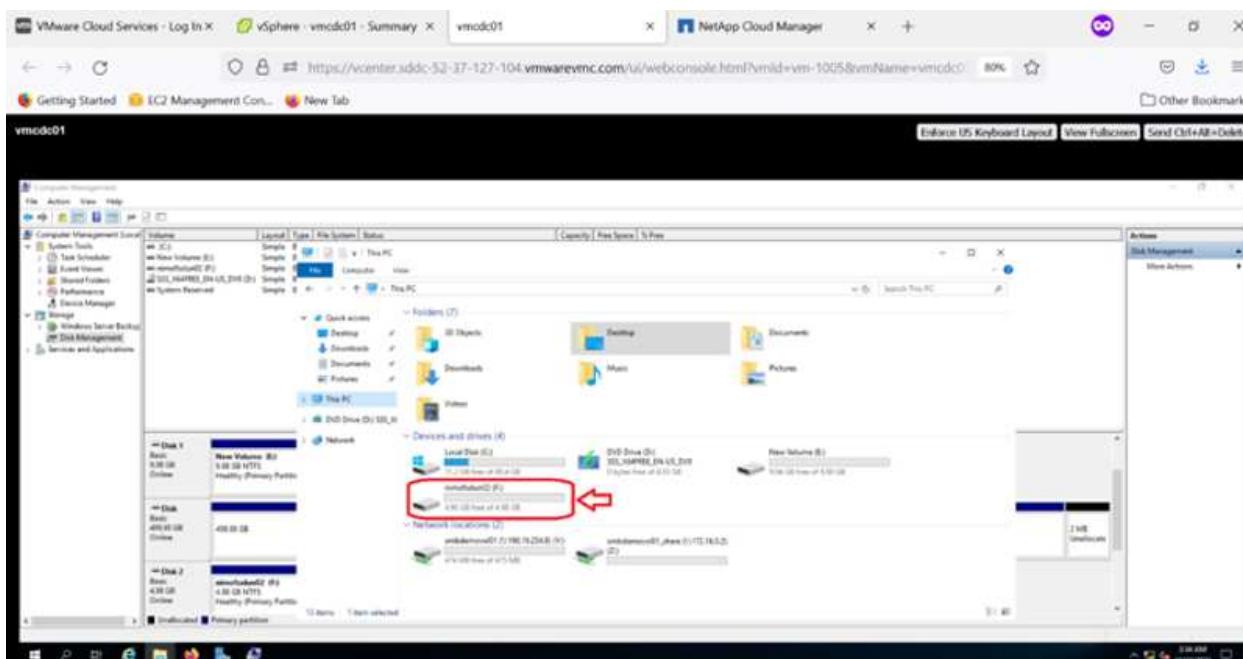
LUNs from the SVM appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

1. Open the Windows Computer Management utility: Start > Administrative Tools > Computer Management.
2. Expand the Storage node in the navigation tree.
3. Click Disk Management.
4. Click Action > Rescan Disks.



When a new LUN is first accessed by the Windows host, it has no partition or file system. Initialize the LUN; and optionally, format the LUN with a file system by completing the following steps:

1. Start Windows Disk Management.
2. Right-click the LUN, and then select the required disk or partition type.
3. Follow the instructions in the wizard. In this example, drive F: is mounted.



On the Linux clients, ensure the iSCSI daemon is running. After the LUNs are provisioned, refer to the detailed guidance on iSCSI configuration for your Linux distribution. For example, Ubuntu iSCSI configuration can be found [here](#). To verify, run lsblk cmd from the shell.

## Mount Cloud Volumes ONTAP NFS volume on Linux client

To mount the Cloud Volumes ONTAP (DIY) file system from VMs within VMC on AWS SDDC, complete the following steps:

1. Connect to the designated Linux instance.
2. Open a terminal on the instance using secure shell (SSH) and log in with the appropriate credentials.
3. Make a directory for the volume's mount point with the following command.

```
$ sudo mkdir /fsxcvotesting01/nfsdemovol01
```

4. Mount the Amazon FSx for NetApp ONTAP NFS volume to the directory that is created in the previous step.

```
sudo mount -t nfs nfsvers=4.1,172.16.0.2:/nfsdemovol01  
/fsxcvotesting01/nfsdemovol01
```

The screenshot shows a terminal window titled 'ubuntu01' running on a VMware host. The terminal displays the command 'root@ubuntu01:/fsx# mount -t nfs 172.16.0.2:/nfsdemovol01 /fsxcvotesting01/nfsdemovol01'. Below this, the 'df' command output is shown, listing the mounted NFS volume at '/fsxcvotesting01/nfsdemovol01'. A red arrow points to this line in the terminal output.

```
root@ubuntu01:/fsx# mount -t nfs 172.16.0.2:/nfsdemovol01 /fsxcvotesting01/nfsdemovol01_
root@ubuntu01:~# df
Filesystem      1K-blocks   Used Available Use% Mounted on
tmpfs            814396    116   813280  1% /run
/dev/mapper/ubuntu--vg-ubuntu--1V 15412168 3666428 10943132 2% /
tmpfs            4071960     0  4071960  0% /dev/shm
tmpfs             5120     0   5120  0% /run/lock
tmpfs              4096     0   4096  0% /sys/fs/cgroup
/dev/sda2        999320 254996  675512 28% /boot
tmpfs            814392     4  814388  1% /run/user/1000
172.16.0.2:/nfsdemovol01  9361472 4241792  5195680 43% /fsxcvotesting01/nfsdemovol01
198.19.254.239:/nfsdemovol01  536160    512   995648  1% /fsx/nfsdemovol01
root@ubuntu01:/fsx/nfsdemovol01# cd /fsx/nfsdemovol01/
root@ubuntu01:/fsx/nfsdemovol01# ls
n1now111.txt
root@ubuntu01:/fsx/nfsdemovol01#
```

## NetApp Guest Connected Storage Options for Azure

Azure supports guest connected NetApp storage with the native Azure NetApp Files (ANF) service or with Cloud Volumes ONTAP (CVO).

### Azure NetApp Files (ANF)

Azure netApp Files brings enterprise-grade data management and storage to Azure so you can manage your workloads and applications with ease. Migrate your workloads to the cloud and run them without sacrificing performance.

Azure netApp Files removes obstacles, so you can move all of your file-based applications to the cloud. For the first time, you do not

have to re-architect your applications, and you get persistent storage for your applications without complexity.

Because the service is delivered through the Microsoft Azure Portal, users experience a fully managed service as part of their Microsoft enterprise Agreement. World-class support, managed by Microsoft, gives you complete peace of mind. This single solution enables you to quickly and easily add multiprotocol workloads. you can build and deploy both Windows and Linux file-based applications, even for legacy environments.

## Azure NetApp Files (ANF) as guest connected storage

### Configure Azure NetApp Files with Azure VMware Solution (AVS)

Azure NetApp Files shares can be mounted from VMs that are created in the Azure VMware Solution SDDC environment. The volumes can also be mounted on the Linux client and mapped on the Windows client because Azure NetApp Files supports SMB and NFS protocols. Azure NetApp Files volumes can be set up in five simple steps.

Azure NetApp Files and Azure VMware Solution must be in the same Azure region.



## Create and mount Azure NetApp Files volumes

To create and mount Azure NetApp Files volumes, complete the following steps:

1. Log in to the Azure Portal and access Azure NetApp Files. Verify access to the Azure NetApp Files service and register the Azure NetApp Files Resource Provider by using the `az provider register --namespace Microsoft.NetApp -wait` command. After registration is complete, create a NetApp account.

For detailed steps, see [Azure NetApp Files shares](#). This page will guide you through the step-by-step process.

The screenshot shows the 'New NetApp account' creation interface in the Azure portal. On the left, there's a sidebar with a 'Create' button and a 'Manage view' dropdown. The main area has fields for 'Name' (set to 'nimoAVSANFdemo'), 'Subscription' (set to 'SaaS Backup Production'), 'Resource group' (set to 'NimoAVSDemo'), and 'Location' (set to 'East US 2'). At the bottom, there are 'Create' and 'Download a template for automation' buttons.

2. After the NetApp account is created, set up the capacity pools with the required service level and size.

For more information, see [Set up a capacity pool](#).

The screenshot shows the Azure NetApp Files interface. On the left, there's a sidebar with options like 'Create', 'Manage view', and a search bar. The main area is titled 'nimoAVSANFdemo | Capacity pools'. It has a table with columns 'Name', 'Capacity', and 'Service level'. Below the table, it says 'You don't have any capacity pools. Click Add pool to get started'. A modal window titled 'New capacity pool' is overlaid, containing fields for 'Name' (set to 'nimcappool'), 'Service level' (set to 'Standard'), 'Size (TiB)' (set to '4'), and 'QoS type' (set to 'Auto'). At the bottom of the modal are 'Create' and 'Discard' buttons.

3. Configure the delegated subnet for Azure NetApp Files and specify this subnet while creating the volumes. For detailed steps to create delegated subnet, see [Delegate a subnet to Azure NetApp Files](#).

The screenshot shows the Azure portal's 'Virtual networks' section. On the left, there's a sidebar with 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Address space', 'Connected devices', 'Subnets' (which is selected), 'DDoS protection', 'Firewall', and 'Security'. The main area is titled 'nimoavspriv-vnet | Subnets'. A modal window titled 'Add subnet' is open, with fields for 'Name' (set to 'anfdel'), 'Subnet address range' (set to '172.24.3.0/28'), 'Add IPv6 address space' (unchecked), 'NAT gateway' (set to 'None'), 'Network security group' (set to 'None'), and 'Route table' (set to 'None'). At the bottom of the modal are 'Save' and 'Cancel' buttons.

4. Add an SMB volume by using the Volumes blade under the Capacity Pools blade. Make sure the Active Directory connector is configured prior to creating the SMB volume.

The screenshot shows the 'Active Directory connections' blade for the 'nimoAVSANFdemo' NetApp account. On the left, there's a sidebar with 'Azure NetApp Files' and 'nimoAVSANFdemo' selected. The main area has a search bar and a table with columns: DNS, AD DNS Domain, and SMB Server. A message says 'No currently joined Active Directories.' On the right, there's a 'Join Active Directory' form with fields for Primary DNS (172.24.1.5), Secondary DNS, AD DNS Domain Name (nimodemo.com), AD Site Name, SMB Server (Computer Account) Prefix (nim smb), and Organizational Unit Path. A 'Join' button is at the bottom.

5. Click Review + Create to create the SMB volume.

If the application is SQL Server, then enable the SMB continuous availability.

The screenshot shows the 'Create a volume' wizard. The 'Basics' tab is selected. It includes a summary of the volume creation: Volume name (nimvoltest1), Capacity pool (nimcappool), Available quota (4096 GB), and Quota (100 GB). Below the summary are buttons for 'Review + create', '< Previous', and 'Next : Protocol >'.

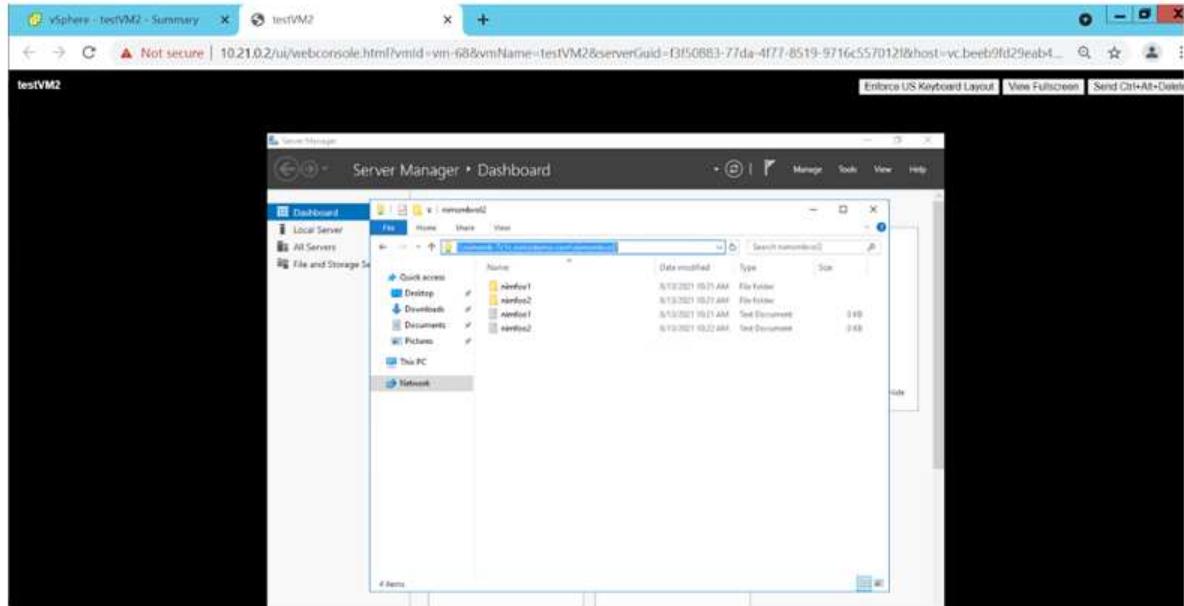
The screenshot shows the Azure portal interface for managing NetApp volumes. On the left, there's a sidebar with options like Quota, Properties, Locks, and Active Directory connections. The main area is titled 'nimoAVSANFDemo | Volumes' and contains a table with the following data:

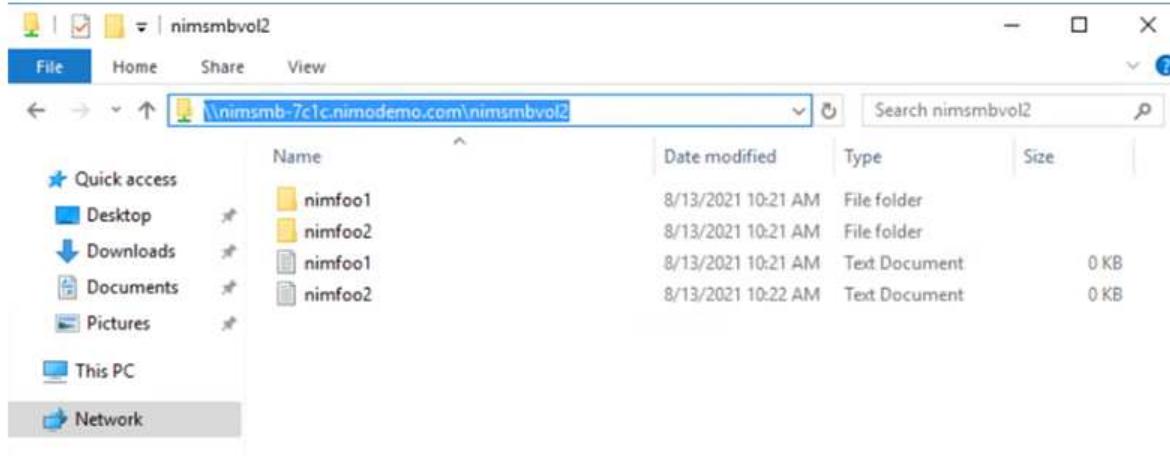
Name	Quota	Throughput	Protocol type	Mount path	Service level	Capacity p
nimsmbvol2	100 GiB	1.6 MiB/s	SMB	\\\nimsmb-7c1c.nimodr	Standard	nimcappoo
nimvoltest1	100 GiB	1.6 MiB/s	NFSv3	172.24.3.4/nimvoltest1	Standard	nimcappoo

To learn more about Azure NetApp Files volume performance by size or quota, see [Performance considerations for Azure NetApp Files](#).

- After the connectivity is in place, the volume can be mounted and used for application data.

To accomplish this, from the Azure portal, click the Volumes blade, and then select the volume to mount and access the mount instructions. Copy the path and use the Map Network Drive option to mount the volume on the VM running on Azure VMware Solution SDDC.





- To mount NFS volumes on Linux VMs running on Azure VMware Solution SDDC, use this same process. Use volume reshaping or dynamic service level capability to meet the workload demands.

```

nimoadmin@nimoadmin-virtual-machine:~$ sudo mount -t nfs -o rw,hard,tcp 172.24.3.4:/nimodemofsv1 /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:~$ df
Filesystem      1K-blocks    Used Available Use% Mounted on
udev             8168112      0   8168112   0% /dev
tmpfs            1639548   1488  1638060   1% /run
/dev/sda5       50824704 7902752 40310496 17% /
tmpfs            8197728      0   8197728   0% /dev/shm
tmpfs             5120       0     5120   0% /run/lock
tmpfs            8197728      0   8197728   0% /sys/fs/cgroup
/dev/loop0        56832    56832          0 100% /snap/core18/2128
/dev/loop2        66688    66688          0 100% /snap/gtk-common-themes/1515
/dev/loop1        224256   224256          0 100% /snap/gnome-3-34-1804/72
/dev/loop3        52224    52224          0 100% /snap/snap-store/547
/dev/loop4        33152    33152          0 100% /snap/snapd/12704
/dev/sda1        523248       4   523244   1% /boot/efi
tmpfs            1639544    52       1639492   1% /run/user/1000
/dev/sr0           54738    54738          0 100% /media/nimoadmin/VMware Tools
172.24.3.4:/nimodemofsv1 104857600          0 104857600   0% /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:~$
```

For more information, see [Dynamically change the service level of a volume](#).

## Cloud Volumes ONTAP (CVO)

Cloud volumes ONTAP, or CVO, is the industry-leading cloud data management solution built on NetApp's ONTAP storage software, available natively on Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).

It is a software-defined version of ONTAP that consumes cloud-native storage, allowing you to have the same storage software in the cloud and on-premises, reducing the need to retrain your IT staff in all-new methods to manage your data.

CVO gives customers the ability to seamlessly move data from the edge, to the data center, to the cloud and back, bringing your hybrid cloud together — all managed with a single-pane management console, NetApp Cloud Manager.

By design, CVO delivers extreme performance and advanced data management capabilities to satisfy even your most demanding applications in the cloud

#### **Cloud Volumes ONTAP (CVO) as guest connected storage**



## Deploy new Cloud Volumes ONTAP in Azure

Cloud Volumes ONTAP shares and LUNs can be mounted from VMs that are created in the Azure VMware Solution SDDC environment. The volumes can also be mounted on the Linux client and on Windows client because Cloud Volumes ONTAP supports iSCSI, SMB, and NFS protocols. Cloud Volumes ONTAP volumes can be set up in a few simple steps.

To replicate volumes from an on-premises environment to the cloud for disaster recovery or migration purposes, establish network connectivity to Azure, either using a site-to-site VPN or ExpressRoute. Replicating data from on-premises to Cloud Volumes ONTAP is outside the scope of this document. To replicate data between on-premises and Cloud Volumes ONTAP systems, see [Setting up data replication between systems](#).

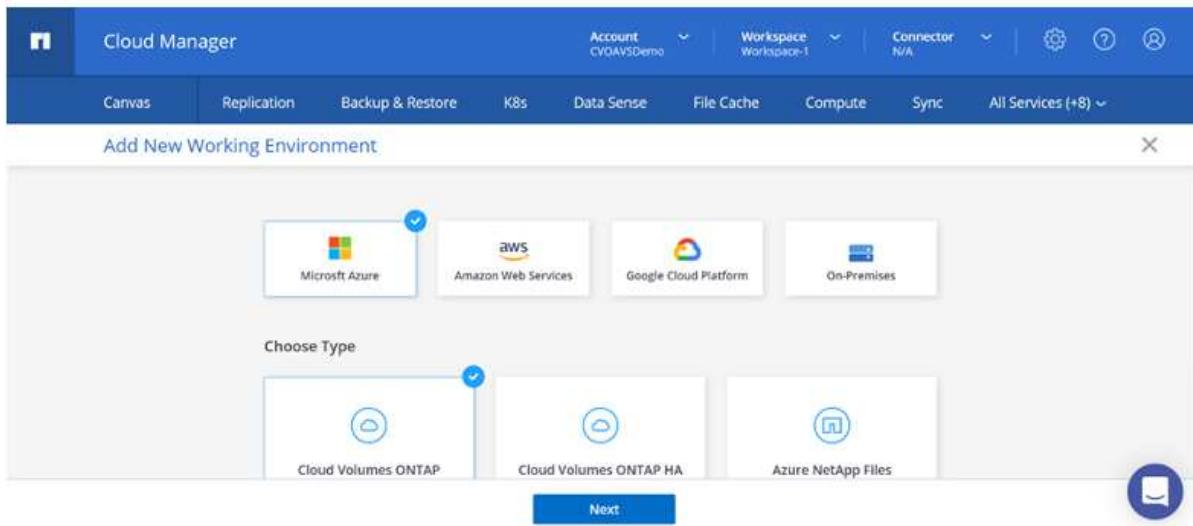


Use [Cloud Volumes ONTAP sizer](#) to accurately size the Cloud Volumes ONTAP instances. Also monitor on-premises performance to use as inputs in the Cloud Volumes ONTAP sizer.

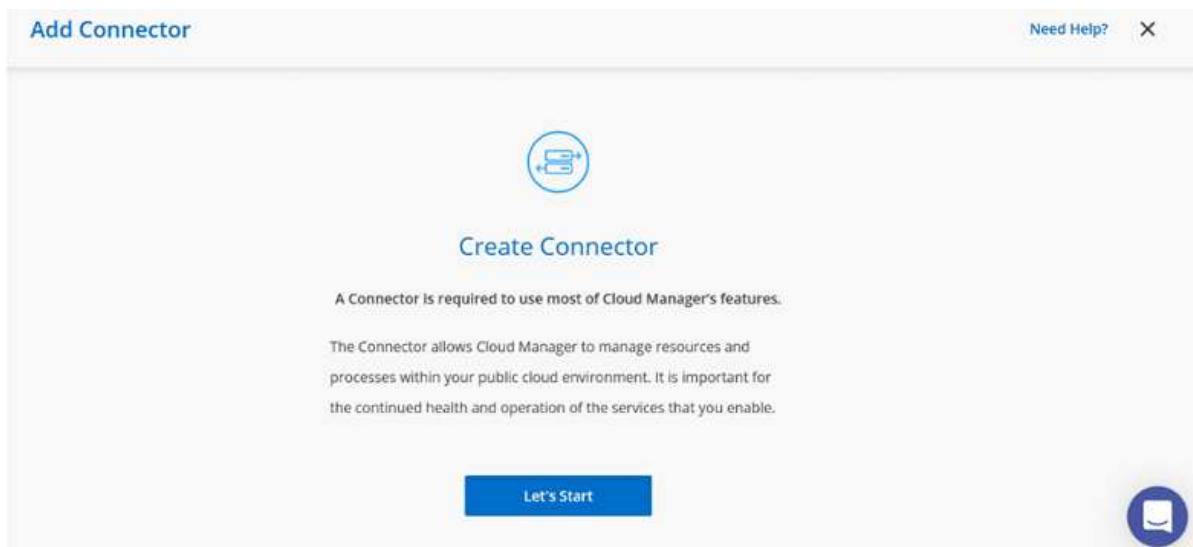
1. Log in to NetApp Cloud Central—the Fabric View screen is displayed. Locate the Cloud Volumes ONTAP tab and select Go to Cloud Manager. After you are logged in, the Canvas screen is displayed.

The screenshot shows the NetApp Cloud Central interface. The top navigation bar includes 'Cloud Manager', 'Account CVOAVSDemo', 'Workspace Workspace-1', 'Connector N/A', and various icons. Below the navigation bar, a horizontal menu bar has tabs for 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. A large blue button labeled 'Canvas' is positioned below the tabs. In the center of the page, there is a circular icon with a cloud and a plus sign, and the text 'Let's Add Your First Working Environment'. A small note below it says 'This is how you deploy, allocate or discover your cloud storage. (Cloud Volumes ONTAP, Cloud Volumes Service, on-prem ONTAP or S3 buckets.)'. At the bottom, a blue button is labeled 'Add Working Environment'.

2. On the Cloud Manager home page, click Add a Working Environment and then select Microsoft Azure as the cloud and the type of the system configuration.



- When creating the first Cloud Volumes ONTAP working environment, Cloud Manager prompts you to deploy a Connector.



- After the connector is created, update the Details and Credentials fields.

Create a New Working Environment		Details and Credentials	
Managed Service Ide...	SaaS Backup Prod...	CMCVOSub	<a href="#">Edit Credentials</a>
Credential Name	Azure Subscription	Marketplace Subscription	
Details Working Environment Name (Cluster Name) <input type="text" value="nimavscvo"/>		Credentials User Name <input type="text" value="admin"/> Password <input type="password"/>	
<a href="#">Continue</a>			

- Provide the details of the environment to be created including the environment name and admin

credentials. Add resource group tags for the Azure environment as an optional parameter. After you are done, click Continue.

Create a New Working Environment      Details and Credentials

Working Environment Name (Cluster Name)	User Name
nimavsCVO	admin
Add Resource Group Tags      Optional Field	
<b>Continue</b>	

6. Select the add-on services for Cloud Volumes ONTAP deployment, including Cloud Data Sense, Cloud Backup, and Cloud Insights. Select the services and then click Continue.

Create a New Working Environment      Services

Data Sense & Compliance	On
Backup to Cloud	On
Monitoring	On
<b>Continue</b>	

7. Configure the Azure location and connectivity. Select the Azure Region, resource group, VNet, and subnet to be used.

Create a New Working Environment      Location & Connectivity

Azure Region	East US 2	Resource Group
Availability Zone	(Optional) Select an Availability Zone	<input checked="" type="radio"/> Create a new group <input type="radio"/> Use an existing group
VNet	nimoavspiv-vnet   NimoAVSDemo	Resource Group Name nimavsCVO-rg
Subnet	172.24.2.0/24	Security Group
<input checked="" type="checkbox"/> I have verified network connectivity between the Cloud Manager server and the selected VNet.		
<b>Continue</b>		

8. Select the license option: Pay-As-You-Go or BYOL for using existing license. In this example, Pay-As-You-Go option is used.

## Create a New Working Environment Cloud Volumes ONTAP Charging Methods & NSS Account

### Cloud Volumes ONTAP Charging Methods

[Learn more about our charging methods](#)



Pay-As-You-Go by the hour



Bring your own license

### NetApp Support Site Account (*Optional*)

[Learn more about NetApp Support Site \(NSS\) accounts](#)

To register this Cloud Volumes ONTAP to support, you should add NetApp Support Site Account.

Don't have a NetApp Support Site account? Select go to finish deploying this system. After it's created, use the [Support Registration option](#) to create an NSS account.

[Continue](#)

9. Select between several preconfigured packages available for the various types of workloads.

### Create a New Working Environment

### Preconfigured Packages

Select a preconfigured Cloud Volumes ONTAP system that best matches your needs, or create your own configuration.  
Preconfigured settings can be modified at a later time.

[Change Configuration](#)



POC and small workloads  
Up to 500GB of storage



Database and application data production workloads



Cost effective DR  
Up to 500GB of storage



Highest performance production workloads

[Continue](#)

10. Accept the two agreements regarding activating support and allocation of Azure resources. To create the Cloud Volumes ONTAP instance, click Go.

### Create a New Working Environment

### Review & Approve

nimavscVO

Azure | East US 2

- I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. [More information](#) >
- I understand that Cloud Manager will allocate the appropriate Azure resources to comply with my above requirements. [More information](#) >

[Overview](#)

[Networking](#)

[Storage](#)

[Go](#)

11. After Cloud Volumes ONTAP is provisioned, it is listed in the working environments on the Canvas page.

Canvas    Replication    Backup & Restore    K8s    Data Sense    File Cache    Compute    Sync    All Services (+8) ▾

Go to Tabular View

Add Working Environment

Cloud Volumes ONTAP

Freemium

nimavscVO

On

DETAILS

Cloud Volumes ONTAP | Azure | Single

SERVICES

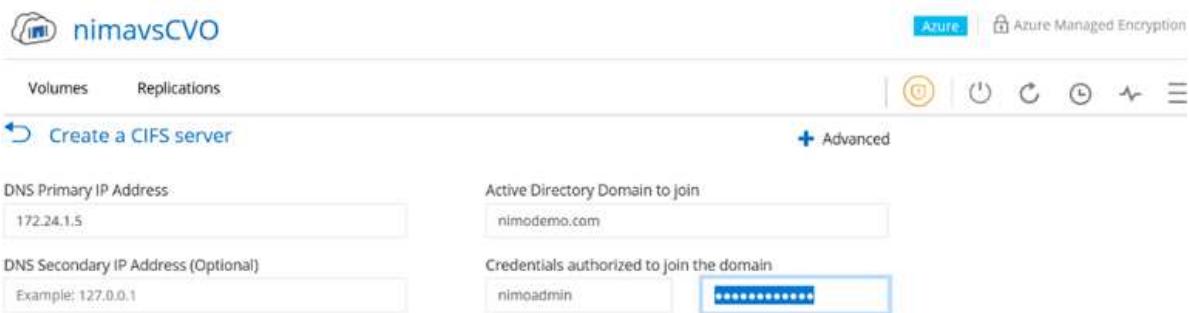
Enter Working Environment

This screenshot shows a user interface for managing cloud storage environments. At the top, there's a navigation bar with tabs like Canvas, Replication, etc. Below the navigation is a section titled 'Add Working Environment' with a 'Cloud Volumes ONTAP' icon. To its right is a detailed view of a single environment named 'nimavscVO', which is currently active ('On'). The details pane shows 'Cloud Volumes ONTAP | Azure | Single'. Below this are sections for 'SERVICES' and a button labeled 'Enter Working Environment'. There are also some small icons for replication and other services.

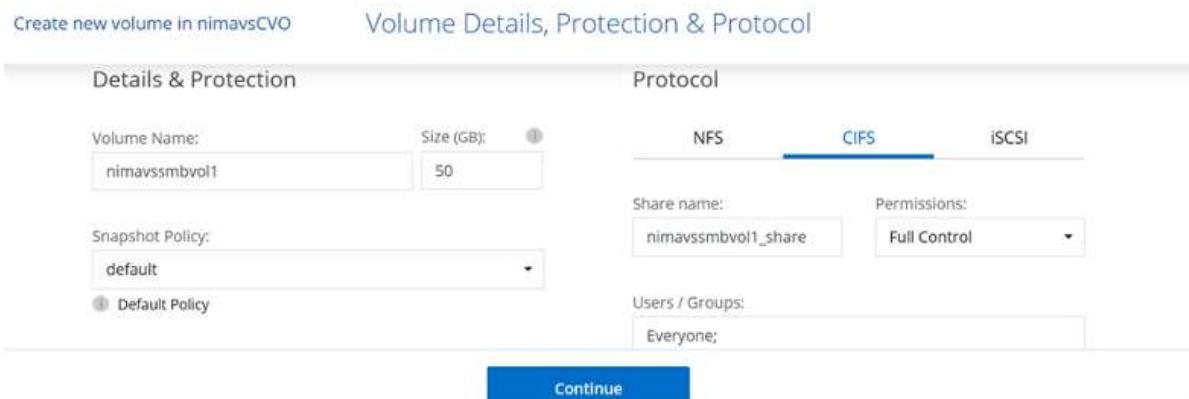


## Additional configurations for SMB volumes

1. After the working environment is ready, make sure the CIFS server is configured with the appropriate DNS and Active Directory configuration parameters. This step is required before you can create the SMB volume.



2. Creating the SMB volume is an easy process. Select the CVO instance to create the volume and click the Create Volume option. Choose the appropriate size and cloud manager chooses the containing aggregate or use advanced allocation mechanism to place on a specific aggregate. For this demo, SMB is selected as the protocol.



3. After the volume is provisioned, it will be available under the Volumes pane. Because a CIFS share is provisioned, give your users or groups permission to the files and folders and verify that those users can access the share and create a file. This step is not required if the volume is replicated from an on-premises environment because the file and folder permissions are all retained as part of SnapMirror replication.

Volumes Replications

Volumes

1 Volume | 50 GB Allocated | 1.74 MB Total Used (1.74 MB In Disk, 0 KB In Blob)

nimavssmbvol1 ONLINE

INFO	
Disk Type	PREMIUM_LRS
Tiering Policy	Auto
Backup	OFF

CAPACITY

Category	Value
Disk Used	1.74 MB
Blob Used	0 GB

- After the volume is created, use the mount command to connect to the share from the VM running on the Azure VMware Solution SDDC hosts.
- Copy the following path and use the Map Network Drive option to mount the volume on the VM running on Azure VMware Solution SDDC.

Volumes Replications

Mount Volume nimavssmbvol1

Go to your machine and enter this command

```
\\"172.24.2.8\\nimavssmbvol1_share
```

File Home Share View

\\172.24.2.8\\nimavssmbvol1\_share

Name	Date modified	Type	Size
Desktop			
Downloads			
Documents			
Pictures			
This PC			
Network			

This folder is empty.



## Connect the LUN to a host

To connect the LUN to a host, complete the following steps:

1. On the Canvas page, double-click the Cloud Volumes ONTAP working environment to create and manage volumes.
2. Click Add Volume > New Volume and select iSCSI and click Create Initiator Group. Click Continue.

The screenshot shows the 'New Volume' configuration interface. On the left, under 'Details & Protection', there are fields for 'Volume Name' (nimavsscsi1) and 'Size (GB)' (500). Below that is a dropdown for 'Snapshot Policy' with 'default' selected. A note below says 'Default Policy'. On the right, under 'Protocol', the 'iSCSI' tab is active, indicated by a blue underline. It shows 'NFS', 'CIFS', and 'iSCSI'. A link 'What about LUNs?' is present. Under 'Initiator Group', there are two options: 'Map Existing Initiator Groups' (radio button) and 'Create Initiator Group' (radio button, which is selected). An input field 'Initiator Group' contains 'avsvmlIG'. At the bottom is a blue 'Continue' button.

3. After the volume is provisioned, select the volume, and then click Target IQN. To copy the iSCSI Qualified Name (IQN), click Copy. Set up an iSCSI connection from the host to the LUN.

To accomplish the same for the host residing on Azure VMware Solution SDDC:

- a. RDP to the VM hosted on Azure VMware Solution SDDC.
- b. Open the iSCSI Initiator Properties dialog box: Server Manager > Dashboard > Tools > iSCSI Initiator.
- c. From the Discovery tab, click Discover Portal or Add Portal and then enter the IP address of the iSCSI target port.
- d. From the Targets tab, select the target discovered and then click Log on or Connect.
- e. Select Enable multipath, and then select Automatically Restore This Connection When the Computer Starts or Add This Connection to the List of Favorite Targets. Click Advanced.

**Note:** The Windows host must have an iSCSI connection to each node in the cluster. The native DSM selects the best paths to use.



LUNs on storage virtual machine (SVM) appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

1. Open the Windows Computer Management utility: Start > Administrative Tools > Computer Management.
2. Expand the Storage node in the navigation tree.
3. Click Disk Management.
4. Click Action > Rescan Disks.

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(C)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	39.51 GB	24.99 GB	63 %
SSS_X64FREE_EN-US_DV9 (D)	Simple	Basic	UDF	Healthy (Primary Partition)	6.49 GB	0 MB	0 %
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	500 MB	169 MB	34 %

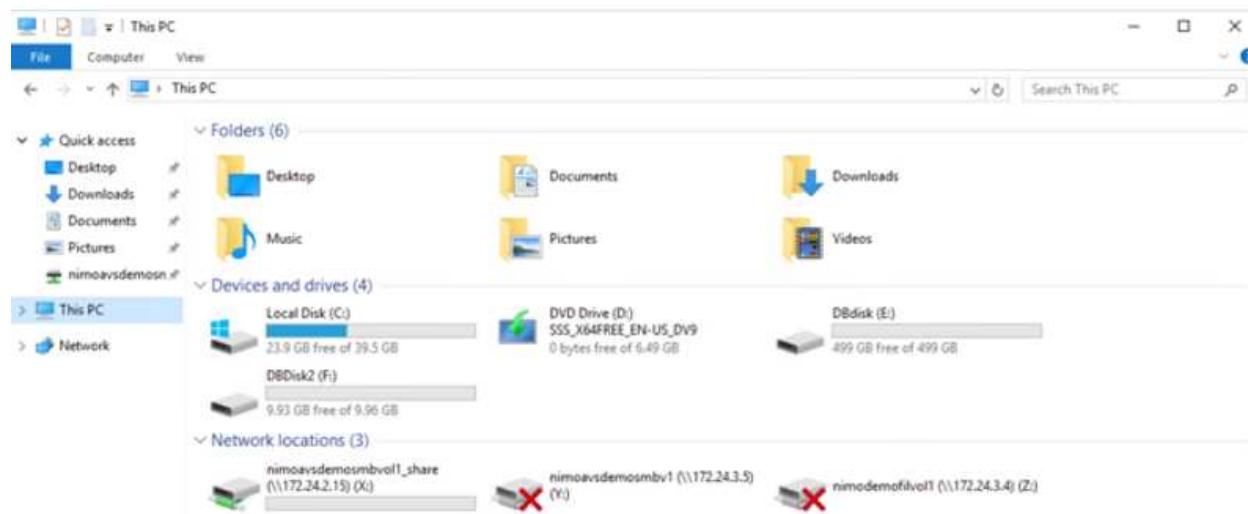
  

Disk	Volume	File System	Status
Disk 0	System Reserved	500 MB NTFS	Healthy (System, Active, Primary Partition)
Disk 1			

When a new LUN is first accessed by the Windows host, it has no partition or file system. Initialize the LUN; and optionally, format the LUN with a file system by completing the following steps:

1. Start Windows Disk Management.

2. Right-click the LUN, and then select the required disk or partition type.
3. Follow the instructions in the wizard. In this example, drive E: is mounted



## NetApp Storage Options for GCP

GCP supports guest connected NetApp storage with Cloud Volumes ONTAP (CVO) or Cloud Volumes Service (CVS).

### Cloud Volumes ONTAP (CVO)

Cloud volumes ONTAP, or CVO, is the industry-leading cloud data management solution built on NetApp's ONTAP storage software, available natively on Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).

It is a software-defined version of ONTAP that consumes cloud-native storage, allowing you to have the same storage software in the cloud and on-premises, reducing the need to retrain your IT staff in all-new methods to manage your data.

CVO gives customers the ability to seamlessly move data from the edge, to the data center, to the cloud and back, bringing your hybrid cloud together — all managed with a single-pane management console, NetApp

Cloud Manager.

By design, CVO delivers extreme performance and advanced data management capabilities to satisfy even your most demanding applications in the cloud

### **Cloud Volumes ONTAP (CVO) as guest connected storage**



## Deploy Cloud Volumes ONTAP in Google Cloud (Do It Yourself)

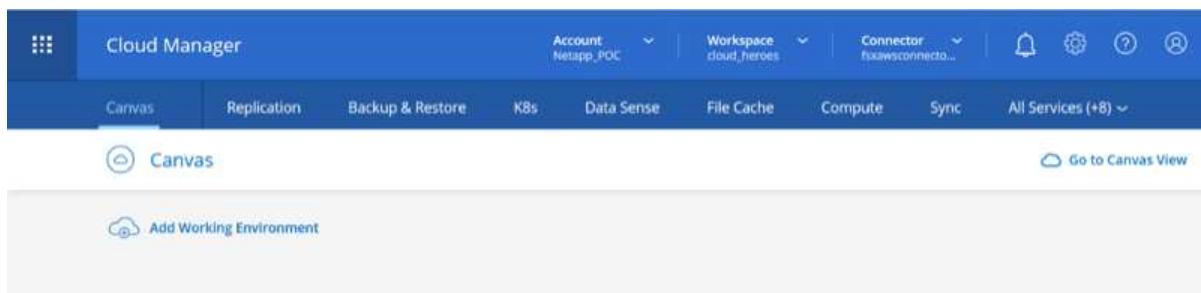
Cloud Volumes ONTAP shares and LUNs can be mounted from VMs that are created in the GCVE private cloud environment. The volumes can also be mounted on the Linux client and on Windows client and LUNS can be accessed on Linux or Windows clients as block devices when mounted over iSCSI because Cloud Volumes ONTAP supports iSCSI, SMB, and NFS protocols. Cloud Volumes ONTAP volumes can be set up in a few simple steps.

To replicate volumes from an on-premises environment to the cloud for disaster recovery or migration purposes, establish network connectivity to Google Cloud, either using a site-to-site VPN or Cloud Interconnect. Replicating data from on-premises to Cloud Volumes ONTAP is outside the scope of this document. To replicate data between on-premises and Cloud Volumes ONTAP systems, see [xref:/ehc/gcp/Setting up data replication between systems](#).

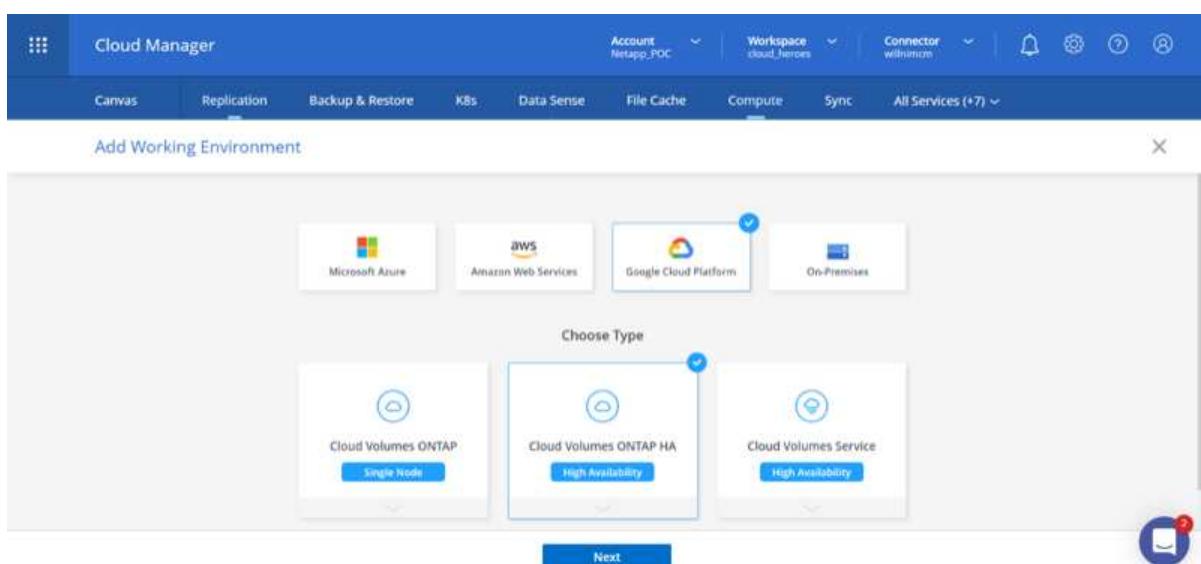


Use [Cloud Volumes ONTAP sizer](#) to accurately size the Cloud Volumes ONTAP instances. Also monitor on-premises performance to use as inputs in the Cloud Volumes ONTAP sizer.

1. Log in to NetApp Cloud Central—the Fabric View screen is displayed. Locate the Cloud Volumes ONTAP tab and select Go to Cloud Manager. After you are logged in, the Canvas screen is displayed.



2. On the Cloud Manager Canvas tab, click Add a Working Environment and then select Google Cloud Platform as the cloud and the type of the system configuration. Then, click Next.



3. Provide the details of the environment to be created including the environment name and admin credentials. After you are done, click Continue.

[↑ Previous Step](#)

CV-Performance-Testing

Google Cloud Project

HCLMainBillingAccountSubs...

Marketplace Subscription

[Edit Project](#)

## Details

Working Environment Name (Cluster Name)

cvogcveva

Service Account



! **Notice:** A Google Cloud service account is required to use two features: backing up data using Backup

## Credentials

User Name

admin

Password

.....

Confirm Password

.....

[Continue](#)

4. Select or deselect the add-on services for Cloud Volumes ONTAP deployment, including Data Sense & Compliance or Backup to Cloud. Then, click Continue.

HINT: A verification pop-up message will be displayed when deactivating add-on services. Add-on services can be added/removed after CVO deployment, consider to deselect them if not needed from the beginning to avoid costs.

[↑ Previous Step](#)

Data Sense &amp; Compliance



Backup to Cloud



⚠ **WARNING:** By turning off Backup to Cloud, future data recovery will not be possible in case of data corruption or loss

[Continue](#)

5. Select a location, choose a firewall policy, and select the checkbox to confirm network connectivity to Google Cloud storage.

## Create a New Working Environment

## Location &amp; Connectivity

[↑ Previous Step](#) Location

GCP Region

europe-west3

Connectivity

VPC

cloud-volumes-vpc

GCP Zone

europe-west3-c

Subnet

10.0.6.0/24

I have verified connectivity between the target VPC and Google Cloud storage.

Firewall Policy

 Generated firewall policy Use existing firewall policy[Continue](#)

6. Select the license option: Pay-As-You-Go or BYOL for using existing license. In this example, Freemium option is used. Then, click on Continue.

## Create a New Working Environment

## Cloud Volumes ONTAP Charging Methods &amp; NSS Account

[↑ Previous Step](#)

## Cloud Volumes ONTAP Charging Methods

[Learn more about our charging methods](#) Pay-As-You-Go by the hour Bring your own license Freemium (Up to 500GB)

NetApp Support Site Account

[Learn more about NetApp Support Site \(NSS\) accounts](#)

NetApp Support Site Account

mchad

To add a new NetApp Support Site account, go to the Support - NSS Management tab.

[Continue](#)

7. Select between several preconfigured packages available based on the type of workload that will be deployed on the VMs running on VMware cloud on AWS SDDC.

HINT: Hoover your mouse over the tiles for details or customize CVO components and ONTAP version by clicking on Change Configuration.

## Create a New Working Environment

## Preconfigured Packages



Select a preconfigured Cloud Volumes ONTAP system that best matches your needs, or create your own configuration.  
Preconfigured settings can be modified at a later time.

[Change Configuration](#)

POC and small workloads

Up to 500GB of storage



Database and application data production workloads



Cost effective DR

Up to 500GB of storage



Highest performance production workloads

[Continue](#)

8. On the Review & Approve page, review and confirm the selections. To create the Cloud Volumes ONTAP instance, click Go.

The screenshot shows the 'Review & Approve' step of a wizard. At the top left is a link to 'Create a New Working Environment'. The main area displays configuration details for a 'cvogcveval' instance in 'GCP | europe-west3'. A note states: 'This Cloud Volumes ONTAP instance will be registered with NetApp support under the NSS Account mchad.' A checkbox is checked, indicating agreement to resource allocation. Below the note are three tabs: 'Overview' (selected), 'Networking', and 'Storage'. Under 'Overview', the following details are listed:

Storage System:	Cloud Volumes ONTAP	Cloud Volumes ONTAP runs on:	n2-standard-4
License Type:	Cloud Volumes ONTAP Freemium	Encryption:	Google Cloud Managed
Capacity Limit:	500GB	Write Speed:	Normal

A large blue 'Go' button is centered at the bottom of the configuration section.

9. After Cloud Volumes ONTAP is provisioned, it is listed in the working environments on the Canvas page.

The screenshot shows the 'Canvas' tab of the Cloud Manager interface. The top navigation bar includes 'Account: NetApp\_POC', 'Workspace: cloud\_tieries', 'Connector: wellnimmci', and various icons for notifications, settings, and help. Below the navigation is a search bar with 'Canvas' selected and a 'Go to Tabular View' link. The main area features two clouds representing working environments:

- cvogcveval**: 'Cloud Volumes ONTAP' (Freemium) with a GCP icon.
- DatacenterDude**: 'Azure NetApp Files' with a Microsoft Azure icon. It shows 31 volumes and 9.71 TiB capacity.

To the right, a sidebar titled 'Working Environments' lists the provisioned capacities:

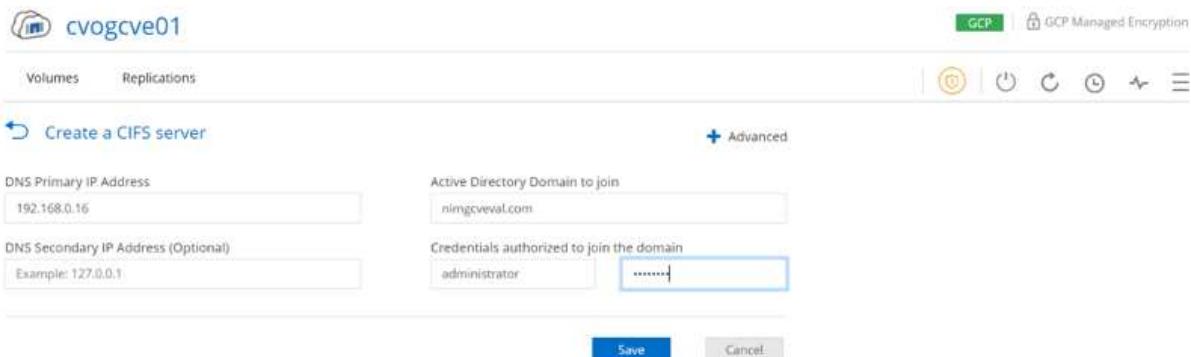
	1 Cloud Volumes ONTAP	43.05 GiB Provisioned Capacity
	1 FSx for ONTAP (High-Availability)	0 B Provisioned Capacity
	1 Azure NetApp Files	9.71 TiB Provisioned Capacity



## Additional configurations for SMB volumes

1. After the working environment is ready, make sure the CIFS server is configured with the appropriate DNS and Active Directory configuration parameters. This step is required before you can create the SMB volume.

HINT: Click on the Menu Icon (°), select Advanced to display more options and select CIFS setup.



2. Creating the SMB volume is an easy process. At Canvas, double-click the Cloud Volumes ONTAP working environment to create and manage volumes and click on the Create Volume option. Choose the appropriate size and cloud manager chooses the containing aggregate or use advanced allocation mechanism to place on a specific aggregate. For this demo, CIFS/SMB is selected as the protocol.

Create new volume in cvogcve01      Volume Details, Protection & Protocol

The screenshot shows the 'Volume Details, Protection & Protocol' configuration page. Under 'Details & Protection', the 'Volume Name' is 'cvogcvesmbvol01' and the 'Size (GB)' is '10'. Under 'Protocol', the 'CIFS' tab is selected. The 'Share name' is 'cvogcvesmbvol01\_share' and the 'Permissions' are set to 'Full Control'. The 'Users / Groups' field contains 'Everyone'. A note below says 'Valid users and groups separated by a semicolon'. A 'Continue' button is at the bottom.

3. After the volume is provisioned, it will be available under the Volumes pane. Because a CIFS share is provisioned, give your users or groups permission to the files and folders and verify that those users can access the share and create a file. This step is not required if the volume is replicated from an on-premises environment because the file and folder permissions are all retained as part of SnapMirror replication.

HINT: Click on the volume menu (°) to display its options.



cvogcvesmbvol01

ONLINE



## INFO

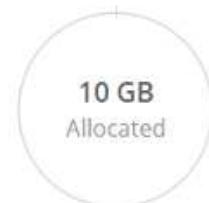
Disk Type

PD-SSD

Tiering Policy

None

## CAPACITY



1.84 MB

Disk Used

- After the volume is created, use the mount command to display the volume connection instructions, then connect to the share from the VMs on Google Cloud VMware Engine.

## cvogcve01

Volumes

Replications

## Mount Volume cvogcvesmbvol01

Go to your machine and enter this command

\\\10.0.6.251\cvogcvesmbvol01\_share

Copy

- Copy the following path and use the Map Network Drive option to mount the volume on the VM running on the Google Cloud VMware Engine.

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Y:

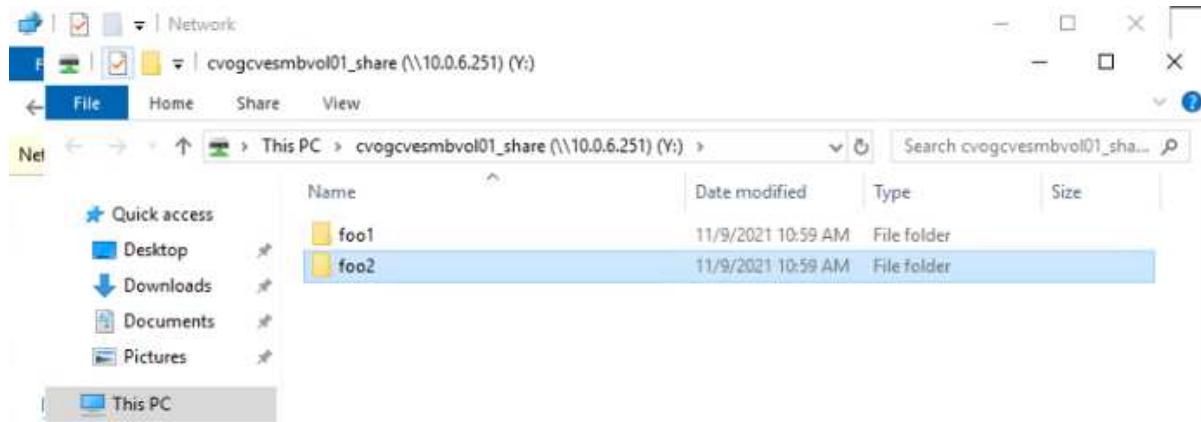
Folder:

\\\10.0.6.251\cvogcvesmbvol01\_share

Example: \\\server\share

 Reconnect at sign-in Connect using different credentials[Connect to a Web site that you can use to store your documents and pictures.](#)

Once mapped, it can be easily accessed, and the NTFS permissions can be set accordingly.





## Connect the LUN on Cloud Volumes ONTAP to a host

To connect the cloud volumes ONTAP LUN to a host, complete the following steps:

1. On the Canvas page, double-click the Cloud Volumes ONTAP working environment to create and manage volumes.
2. Click Add Volume > New Volume and select iSCSI and click Create Initiator Group. Click Continue.

The screenshot shows the 'Create new volume in cvogcve01' wizard in the NetApp Cloud Manager. The 'Volume Name' is 'cvogcvescsilun01' and the 'Size (GB)' is '10'. The 'Protocol' tab is selected, showing 'iSCSI' is chosen. An 'Initiator Group' section contains 'WinIG'. The 'Operating System Type' is set to 'Windows'. A 'Continue' button is at the bottom. Below the wizard is a screenshot of a Windows Server Manager dashboard showing the newly provisioned volume 'cvogcvescsilun01' in File and Storage Services.

3. After the volume is provisioned, select the volume menu (°), and then click Target iQN. To copy the iSCSI Qualified Name (iQN), click Copy. Set up an iSCSI connection from the host to the LUN.

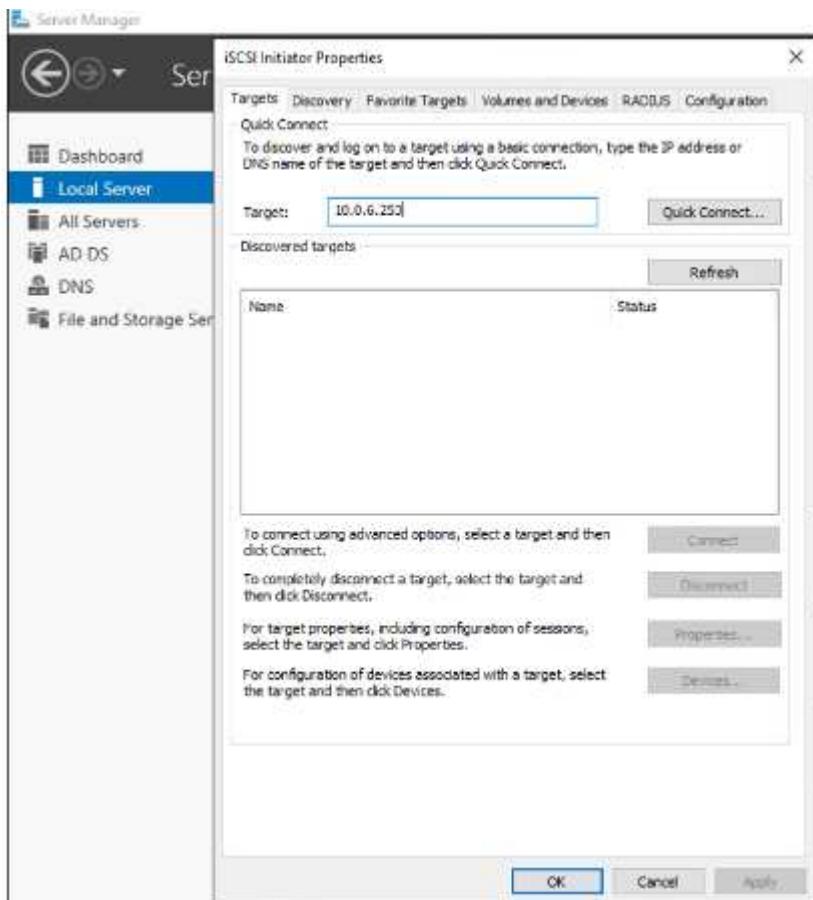
To accomplish the same for the host residing on Google Cloud VMware Engine:

- a. RDP to the VM hosted on Google Cloud VMware Engine.
- b. Open the iSCSI Initiator Properties dialog box: Server Manager > Dashboard > Tools > iSCSI Initiator.

- c. From the Discovery tab, click Discover Portal or Add Portal and then enter the IP address of the iSCSI target port.
- d. From the Targets tab, select the target discovered and then click Log on or Connect.
- e. Select Enable multipath, and then select Automatically Restore This Connection When the Computer Starts or Add This Connection to the List of Favorite Targets. Click Advanced.

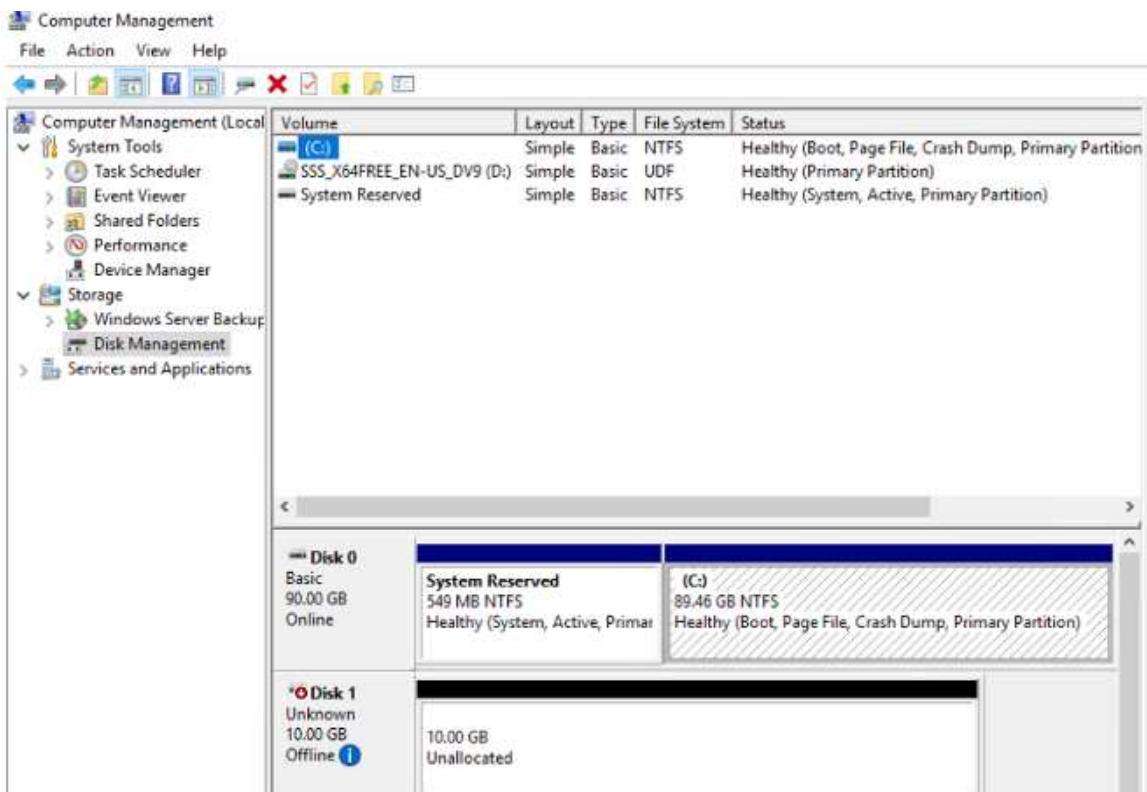


The Windows host must have an iSCSI connection to each node in the cluster.  
The native DSM selects the best paths to use.



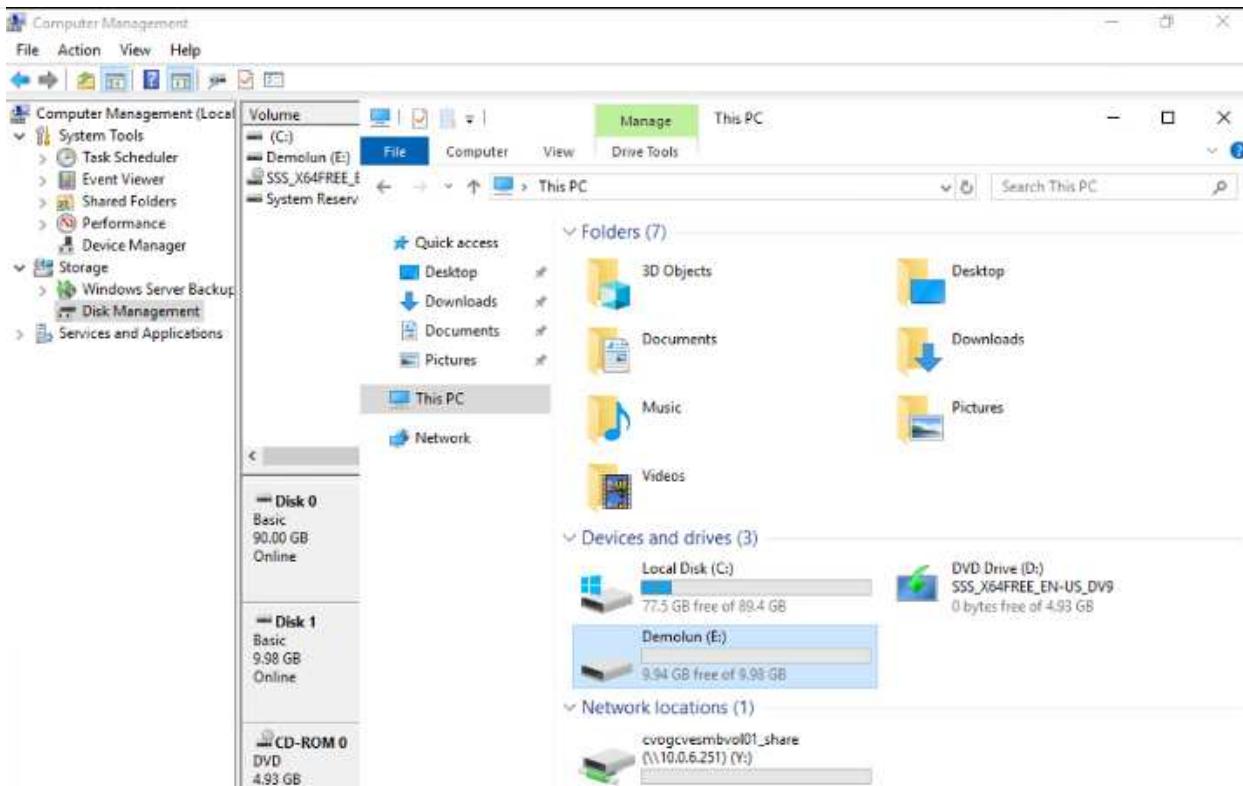
LUNs on storage virtual machine (SVM) appear as disks to the Windows host. Any new disks that are added are not automatically discovered by the host. Trigger a manual rescan to discover the disks by completing the following steps:

1. Open the Windows Computer Management utility: Start > Administrative Tools > Computer Management.
2. Expand the Storage node in the navigation tree.
3. Click Disk Management.
4. Click Action > Rescan Disks.



When a new LUN is first accessed by the Windows host, it has no partition or file system. Initialize the LUN; and optionally, format the LUN with a file system by completing the following steps:

5. Start Windows Disk Management.
6. Right-click the LUN, and then select the required disk or partition type.
7. Follow the instructions in the wizard. In this example, drive F: is mounted.



On the Linux clients, ensure the iSCSI daemon is running. Once the LUNs are provisioned, refer to the detailed guidance on iSCSI configuration with Ubuntu as an example here. To verify, run lsblk cmd from the shell.

```
niyaz@nimubu01:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0 55.4M  1 loop /snap/core18/2128
loop1    7:1    0 219M  1 loop /snap/gnome-3-34-1804/72
loop2    7:2    0 65.1M  1 loop /snap/gtk-common-themes/1515
loop3    7:3    0  51M  1 loop /snap/snap-store/547
loop4    7:4    0 32.3M  1 loop /snap/snapd/12704
loop5    7:5    0 32.5M  1 loop /snap/snapd/13640
loop6    7:6    0 55.5M  1 loop /snap/core18/2246
loop7    7:7    0   4K  1 loop /snap/bare/5
loop8    7:8    0 65.2M  1 loop /snap/gtk-common-themes/1519
sda      8:0    0 16G  0 disk 
└─sda1   8:1    0 512M  0 part /boot/efi
└─sda2   8:2    0   1K  0 part 
└─sda5   8:5    0 15.5G 0 part /
sdb      8:16   0   1G  0 disk
```

```
niyaz@nimubu01:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G   0    1.9G  0% /dev
tmpfs           394M  1.5M  392M  1% /run
/dev/sda5        16G  7.6G  6.9G  53% /
tmpfs           2.0G   0    2.0G  0% /dev/shm
tmpfs           5.0M   0    5.0M  0% /run/lock
tmpfs           2.0G   0    2.0G  0% /sys/fs/cgroup
/dev/loop1       219M  219M   0  100% /snap/gnome-3-34-1804/72
/dev/loop2       66M   66M   0  100% /snap/gtk-common-themes/1515
/dev/loop3       51M   51M   0  100% /snap/snap-store/547
/dev/loop0       56M   56M   0  100% /snap/core18/2128
/dev/loop4       33M   33M   0  100% /snap/snapd/12704
/dev/sda1       511M  4.0K  511M  1% /boot/efi
tmpfs           394M  64K  394M  1% /run/user/1000
/dev/loop5       33M   33M   0  100% /snap/snapd/13640
/dev/loop6       56M   56M   0  100% /snap/core18/2246
/dev/loop7      128K  128K   0  100% /snap/bare/5
/dev/loop8       66M   66M   0  100% /snap/gtk-common-themes/1519
/dev/sdb         976M  2.6M  907M  1% /mnt
```

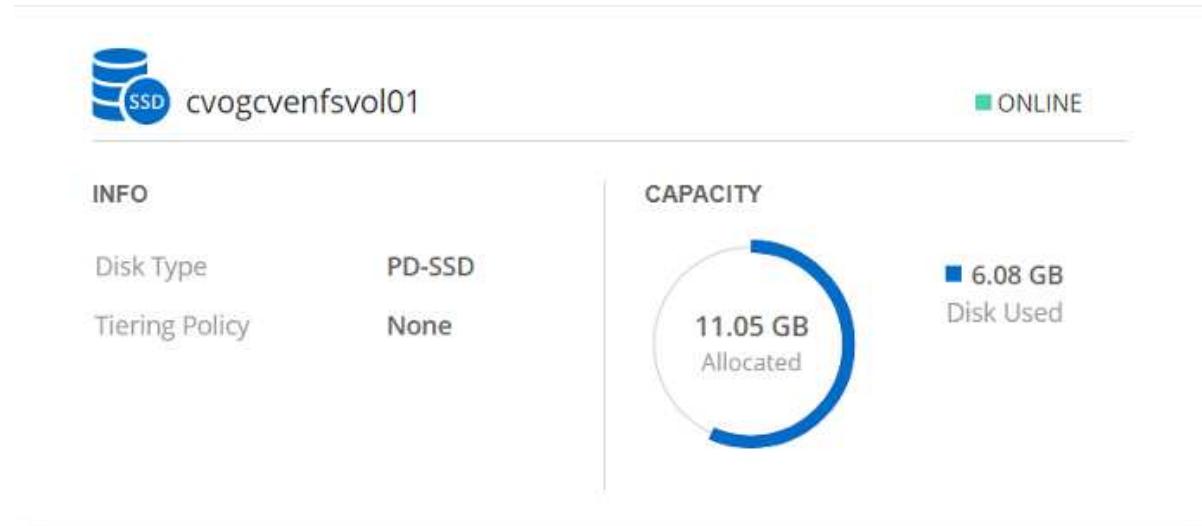


## Mount Cloud Volumes ONTAP NFS volume on Linux client

To mount the Cloud Volumes ONTAP (DIY) file system from VMs within Google Cloud VMware Engine, follow the below steps:

Provision the volume following the below steps

1. In the Volumes tab, click Create New Volume.
2. On the Create New Volume page, select a volume type:



3. In the Volumes tab, place your mouse cursor over the volume, select the menu icon (°), and then click Mount Command.

Volumes      Replications

[Mount Volume cvogcvenfsvol01](#)

Go to your Linux machine and enter this mount command

```
mount 10.0.6.251:/cvogcvenfsvol01 <dest_dir>
```

Copy

4. Click Copy.
5. Connect to the designated Linux instance.
6. Open a terminal on the instance using secure shell (SSH) and log in with the appropriate credentials.
7. Make a directory for the volume's mount point with the following command.

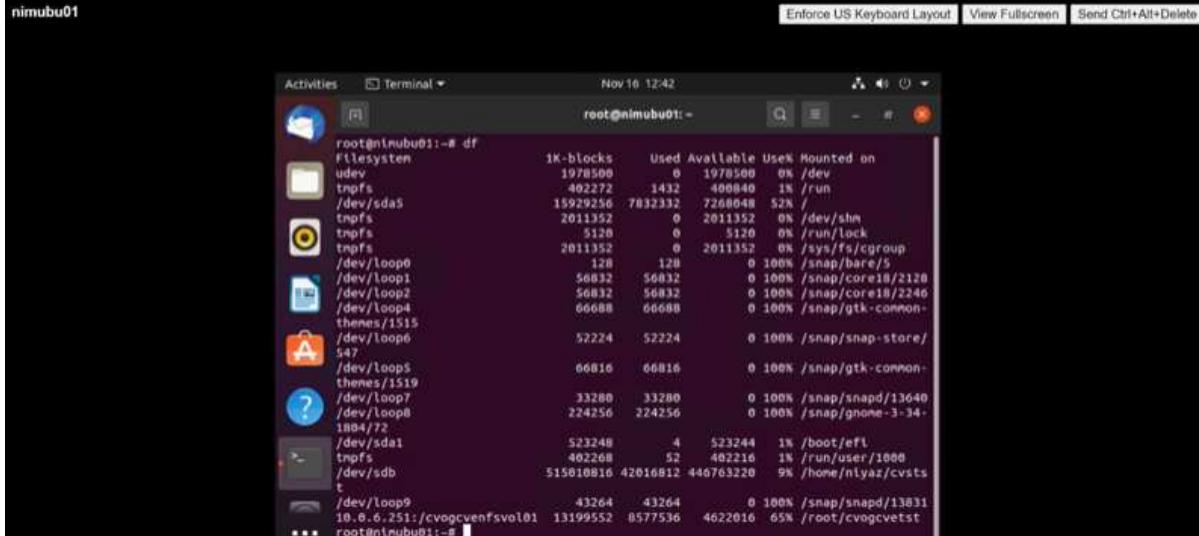
```
$ sudo mkdir /cvogcvetst
```

```
root@nimubu01:~# sudo mkdir cvogcvetst
```

8. Mount the Cloud Volumes ONTAP NFS volume to the directory that is created in the previous step.

```
sudo mount 10.0.6.251:/cvogcvenfsvol01 /cvogcvetst
```

```
root@nimubu01:~# sudo mount -t nfs 10.0.6.251:/cvogcvenfsvol01 cvogcvetst
```



## Cloud Volumes Service (CVS)

Cloud Volumes Services (CVS) is a complete portfolio of data services to deliver advanced cloud solutions. Cloud Volumes Services supports multiple file access protocols for major cloud providers (NFS and SMB support).

Other benefits and features include: data protection and restore with Snapshot; special features to replicate, sync and migrate data destinations on-prem or in the cloud; and consistent high performance at the level of a dedicated flash storage system.

## Cloud Volumes Service (CVS) as guest connected storage

## Configure Cloud Volumes Service with VMware Engine

Cloud Volumes Service shares can be mounted from VMs that are created in the VMware Engine environment. The volumes can also be mounted on the Linux client and mapped on the Windows client because Cloud Volumes Service supports SMB and NFS protocols. Cloud Volumes Service volumes can be set up in simple steps.

Cloud Volume Service and Google Cloud VMware Engine private cloud must be in the same region.

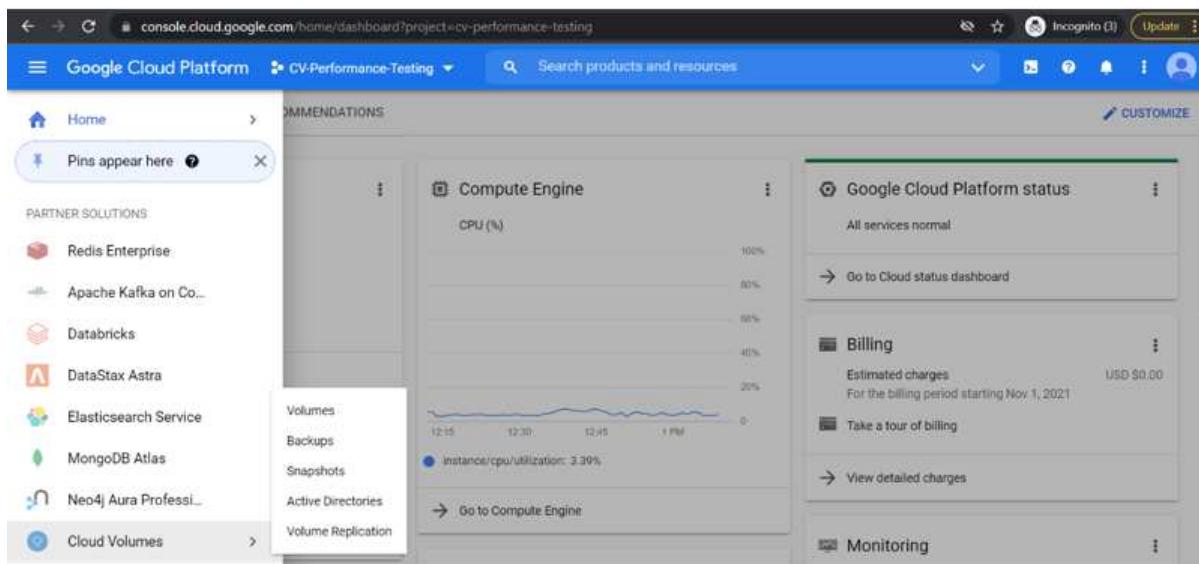
To purchase, enable and configure NetApp Cloud Volumes Service for Google Cloud from the Google Cloud Marketplace, follow this detailed [guide](#).



## Create a CVS NFS volume to GCVE private cloud

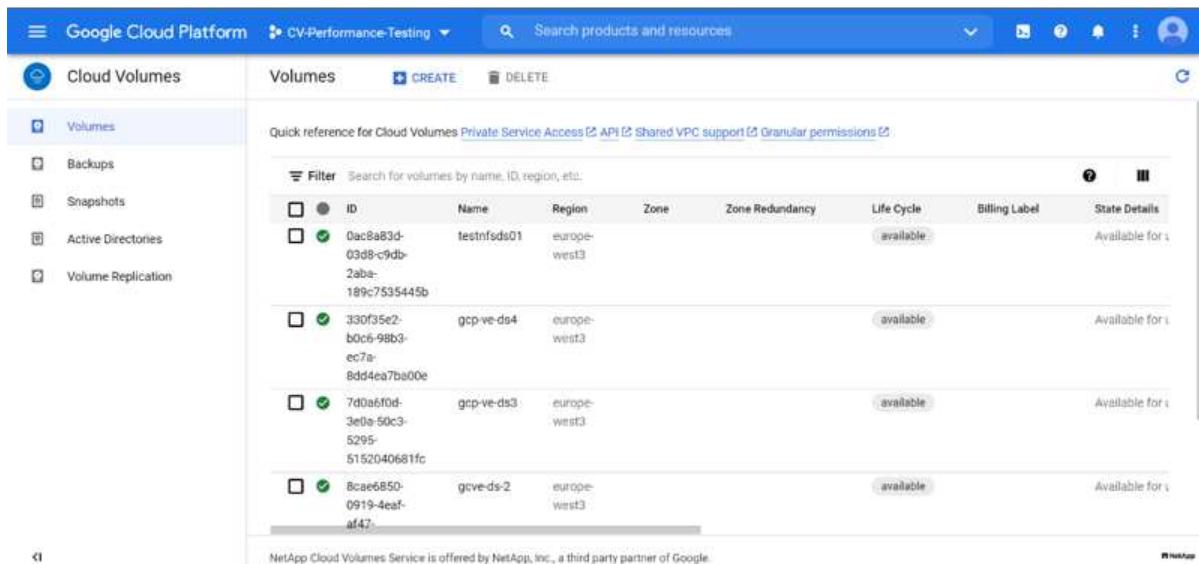
To create and mount NFS volumes, complete the following steps:

1. Access Cloud Volumes from Partner Solutions within the Google cloud console.



The screenshot shows the Google Cloud Platform dashboard for the project 'CV-Performance-Testing'. On the left, there's a sidebar titled 'PARTNER SOLUTIONS' with icons for Redis Enterprise, Apache Kafka on Cloud, Databricks, DataStax Astra, Elasticsearch Service, MongoDB Atlas, Neo4j Aura Professional, and Cloud Volumes. The 'Cloud Volumes' icon is highlighted with a mouse cursor. A dropdown menu for 'Cloud Volumes' is open, showing options: Volumes, Backups, Snapshots, Active Directories, and Volume Replication. The 'Volumes' option is selected. In the main content area, there's a 'Compute Engine' section with a chart showing CPU utilization over time, and a 'Google Cloud Platform status' section indicating 'All services normal'.

2. In the Cloud Volumes Console, go to the Volumes page and click Create.



The screenshot shows the 'Volumes' page within the Cloud Volumes service. The top navigation bar includes 'Cloud Volumes', 'VOLUMES', 'CREATE', and 'DELETE'. The left sidebar has links for 'Volumes', 'Backups', 'Snapshots', 'Active Directories', and 'Volume Replication'. The main area displays a table of existing volumes:

ID	Name	Region	Zone	Zone Redundancy	Life Cycle	Billing Label	State Details
0ac8a83d-03d8-c9db-2ab-189c7535445b	testnfsds01	europe-west3			available		Available for use
330f35e2-b0c6-98b3-ec7a-8dd4ea7ba00e	gcp-ve-ds4	europe-west3			available		Available for use
7d0a610d-3e0a-50c3-5295-5152040681fc	gcp-ve-ds3	europe-west3			available		Available for use
8cae6850-0919-4eaf-af47-	gcve-ds-2	europe-west3			available		Available for use

At the bottom of the page, a note states: 'NetApp Cloud Volumes Service is offered by NetApp, Inc., a third party partner of Google.'

3. On the Create File System page, specify the volume name and billing labels as required for chargeback mechanisms.

 Cloud Volumes <ul style="list-style-type: none"> <li> Volumes</li> <li> Backups</li> <li> Snapshots</li> <li> Active Directories</li> <li> Volume Replication</li> </ul>	<p><a href="#" style="color: inherit; text-decoration: none;">← Create File System</a></p> <hr/> <div style="border-bottom: 1px solid #ccc; margin-bottom: 10px;"></div> <p><b>Volume Name</b></p> <p>Name * <input type="text" value="nimCVNFSvol01"/></p> <p>A human readable name used for display purposes.</p> <hr/> <p><b>Billing Labels</b></p> <p>Label your volumes for billing reports, queries. Supported with CVS-Performance service type; can be set with CVS service type but not available for billing at this time.</p> <p><a href="#" style="border: 1px solid #ccc; padding: 2px 10px; color: inherit; text-decoration: none; margin-right: 10px;">+ ADD LABEL</a></p>
---	---

4. Select the appropriate service. For GCVE, choose CVS-Performance and desired service level for improved latency and higher performance based on the application workload requirements.

 Cloud Volumes <ul style="list-style-type: none"> <li> Volumes</li> <li> Backups</li> <li> Snapshots</li> <li> Active Directories</li> <li> Volume Replication</li> </ul>	<p><a href="#" style="color: inherit; text-decoration: none;">← Create File System</a></p> <hr/> <div style="border-bottom: 1px solid #ccc; margin-bottom: 10px;"></div> <p><b>Service Type</b></p> <p>Cloud Volumes Service is offered as two service types: CVS and CVS-Performance. Select the service type that matches your workload needs. <a href="#">Region availability</a> varies by service type. <a href="#">Learn more</a></p> <p><input checked="" type="radio"/> CVS Offers volumes created with zonal high availability.</p> <p><input checked="" type="radio"/> CVS-Performance Offers 3 performance levels and improved latency to address higher performance application requirements.</p> <hr/> <p><b>Volume Replication</b></p> <p><input type="checkbox"/> Secondary Select to create volume as a destination target for volume replication. Applicable only to CVS-performance volumes.</p>
---	--

5. Specify the Google Cloud region for the volume and volume path (The volume path must be unique across all of cloud volumes in the project)

 Cloud Volumes <ul style="list-style-type: none"> <li> Volumes</li> <li> Backups</li> <li> Snapshots</li> <li> Active Directories</li> <li> Volume Replication</li> </ul>	<p><a href="#" style="color: inherit; text-decoration: none;">← Create File System</a></p> <hr/> <div style="border-bottom: 1px solid #ccc; margin-bottom: 10px;"></div> <p><b>Region</b></p> <p>Region availability varies by service type.</p> <p>Region * <input type="text" value="europe-west3"/></p> <p>Volume will be provisioned in the region you select.</p> <p>Volume Path * <input type="text" value="nimCVSNFSvol01"/></p> <p>Must be unique to the project.</p>
---	---

6. Select the level of performance for the volume.

 Cloud Volumes	<p><a href="#" style="text-decoration: none; color: inherit;">← Create File System</a></p> <p><b>Service Level</b></p> <p>Select the performance level required for your workload.</p> <p><input checked="" type="radio"/> Standard Up to 16 MiB/s per TiB</p> <p><input type="radio"/> Premium Up to 64 MiB/s per TiB</p> <p><input type="radio"/> Extreme Up to 128 MiB/s per TiB</p> <p><input type="button" value="Snapshot"/></p> <p>The snapshot to create the volume from.</p>
---	---

7. Specify the size of the volume and the protocol type. In this testing, NFSv3 is used.

 Cloud Volumes	<p><a href="#" style="text-decoration: none; color: inherit;">← Create File System</a></p> <p><b>Volume Details</b></p> <p>Allocated Capacity * <input type="text" value="1024"/> GiB</p> <p>Allocated size must be between 1 TiB (1024 GiB) and 100 TiB (102400 GiB)</p> <p>Protocol Type * <input type="button" value="NFSv3"/></p> <p><input type="checkbox"/> Make snapshot directory (.snapshot) visible Makes .snapshot directory visible to clients. For NFSv4.1 volumes (CVS-Performance only), the directory itself will not be listed but can be accessed to list contents, etc.</p> <p><input type="checkbox"/> Enable LDAP Enables user look up from AD LDAP server for your NFS volumes</p>
---	--

8. In this step, select the VPC Network from which the volume will be accessible. Ensure VPC peering is in place.

HINT: If VPC peering has not been done, a pop-up button will be displayed to guide you through the peering commands. Open a Cloud Shell session and execute the appropriate commands to peer your VPC with Cloud Volumes Service producer. In case you decide to prepare VPC peering in beforehand, refer to these instructions.

**Cloud Volumes**

**Volumes**

**Network Details**

Shared VPC configuration  
Provide the host project name when deploying in a shared VPC service project.

**VPC Network Name \***

Select the VPC Network from which the volume will be accessible. This cannot be changed later.

Use Custom Address Range  
Reserved Address range

9. Manage the Export policy rules by adding the appropriate rules and Select the checkbox for the corresponding NFS version.

Note: Access to NFS volumes won't be possible unless an export policy is added.

**Cloud Volumes**

**Volumes**

**Export Policy**

**Rules**

**Item 1**

Allowed Clients 1 \*

**Access**

Read & Write  
 Read Only

**Root Access**

On  
 Off

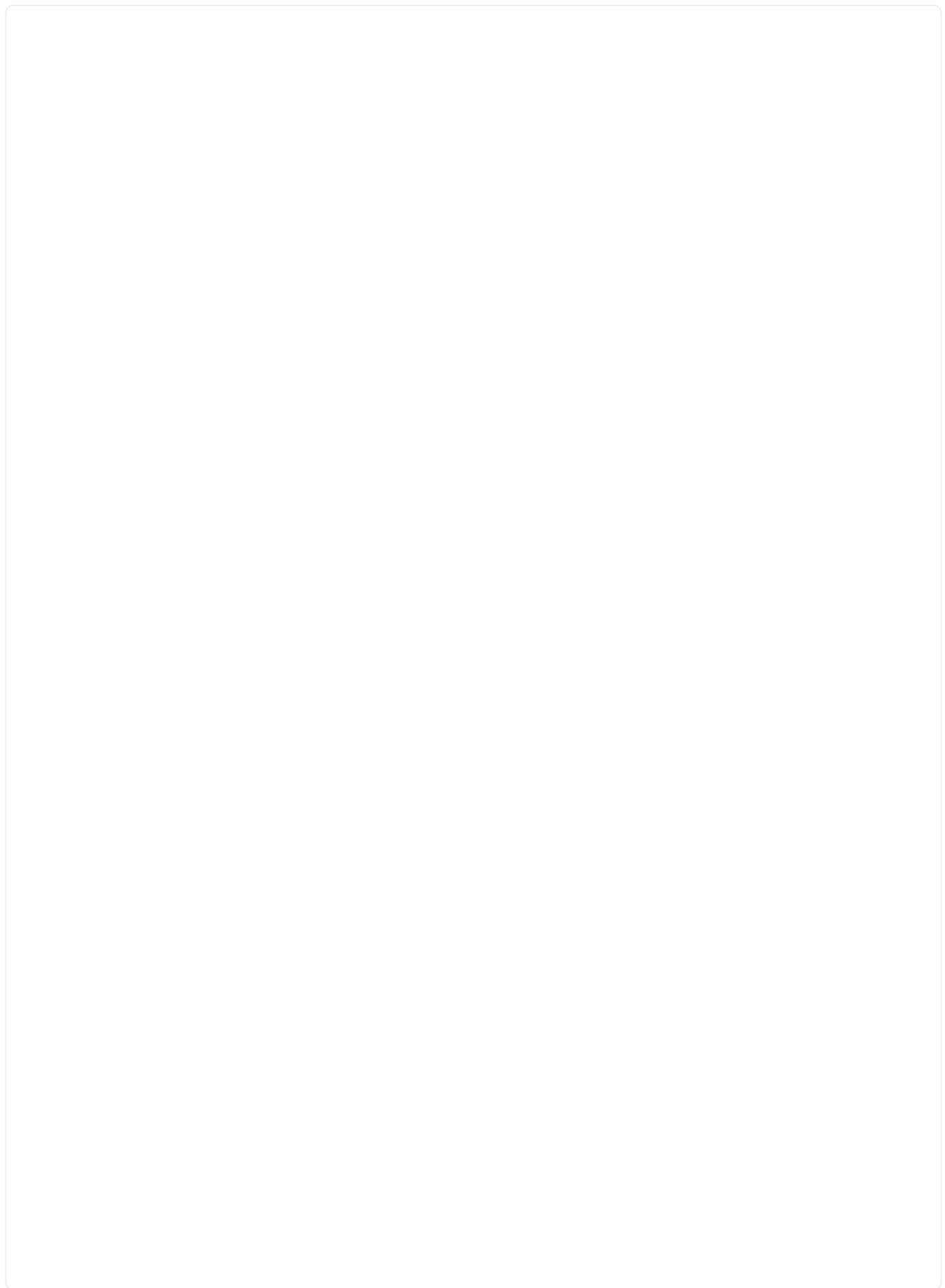
**Protocol Type (Select at least 1 of the below options)**

Must select for Protocol type NFSv3. Optional for Protocol Type Both. Do not select for NFSv4.1

Allows Matching Clients for NFSv3

10. Click Save to create the volume.

	4b8ed9d9- bc6d-f3d5- 5a0f- 7da26aed3ed0	nimnfsdemods02	europe- west3	Available for use	CVS- Performance	Primary	Extreme	NFSv3 : 10.53.0.4/nimnfsdemods02
<input type="checkbox"/>								



## Mounting NFS exports to VMs running on VMware Engine

Before preparing to mount the NFS volume, ensure the peering status of private connection is listed as Active. Once status is Active, use the mount command.

To mount an NFS volume, do the following:

1. In the Cloud Console, go to Cloud Volumes > Volumes.
2. Go to the Volumes page
3. Click the NFS volume for which you want to mount NFS exports.
4. Scroll to the right, under Show More, click Mount Instructions.

To perform the mounting process from within the guest OS of the VMware VM, follow the below steps:

1. Use SSH client and SSH to the virtual machine.
2. Install the nfs client on the instance.
  - a. On Red Hat Enterprise Linux or SuSE Linux instance:

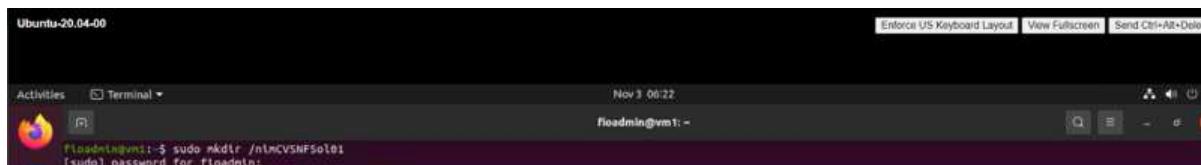
```
sudo yum install -y nfs-utils
```

- b. On an Ubuntu or Debian instance:

```
sudo apt-get install nfs-common
```

3. Create a new directory on the instance, such as "/nimCVSNFS01":

```
sudo mkdir /nimCVSNFS01
```



4. Mount the volume using the appropriate command. Example command from the lab is below:

```
sudo mount -t nfs -o rw,hard,rsize=65536,wszie=65536,vers=3,tcp  
10.53.0.4:/nimCVSNFS01 /nimCVSNFS01
```

```
root@vm1:~# sudo mkdir /nimCVSNFS01  
root@vm1:~# sudo mount -t nfs -o rw,hard,rsize=65536,wszie=65536,vers=3,tcp 10.53.0.4:/nimCVSNFS01 /nimCVSNFS01
```

```
root@vm1:~# df
Filesystem      1K-blocks   Used   Available Use% Mounted on
udev            16409952     0    16409952  0% /dev
tmpfs           3288328    1580    3286748  1% /run
/dev/sdb5        61145932  19231356  38778832  34% /
tmpfs           16441628     0    16441628  0% /dev/shm
tmpfs            5120       0      5120  0% /run/lock
tmpfs           16441628     0    16441628  0% /sys/fs/cgroup
/dev/loop0         128      128      0 100% /snap/bare/5
/dev/loop1        56832     56832      0 100% /snap/core18/2128
/dev/loop2        66688     66688      0 100% /snap/gtk-common-themes/1515
/dev/loop4        66816     66816      0 100% /snap/gtk-common-themes/1519
/dev/loop3        52224     52224      0 100% /snap/snap-store/547
/dev/loop5        224256    224256      0 100% /snap/gnome-3-34-1804/72
/dev/sdb1         523248      4    523244  1% /boot/efi
tmpfs           3288324     28    3288296  1% /run/user/1000
10.53.0.4:/gcve-ds-1 107374182400 1136086016 106238096384  2% /base
/dev/mapper/nfsprdvg1-prod01 419155968 55384972  363770996 14% /datastore1
/dev/loop8         33280     33280      0 100% /snap/snapd/13270
/dev/loop6         33280     33280      0 100% /snap/snapd/13640
/dev/loop7         56832     56832      0 100% /snap/core18/2246
10.53.0.4:/nimCVSNFSol01 107374182400      256 107374182144  1% /nimCVSNFSol01
root@vm1:~#
```



## Creating and Mounting SMB Share to VMs running on VMware Engine

For SMB volumes, make sure the Active Directory connections is configured prior to creating the SMB volume.

The screenshot shows a table of Active Directory connections. There is one entry:

Username	Domain	DNS Servers	NetBIOS Prefix	OU Path	AD Server Name	KDC IP	Region	Status
administrator	nimgcveval.com	192.168.0.16	nimsmb	CN=Computers			europe-west3	In Use

Once the AD connection is in place, create the volume with the desired service level. The steps are like creating NFS volume except selecting the appropriate protocol.

1. In the Cloud Volumes Console, go to the Volumes page and click Create.
2. On the Create File System page, specify the volume name and billing labels as required for chargeback mechanisms.

### [←](#) Create File System

#### Volume Name

Name \* nimCVSMBvol01

A human readable name used for display purposes.

#### Billing Label

Label your volumes for billing reports, queries.

Supported with CVS-Performance service type; can be set with CVS service type but not available for billing at this time.

[+ ADD LABEL](#)

3. Select the appropriate service. For GCVE, choose CVS-Performance and desired service level for improved latency and higher performance based on the workload requirements.

## [Create File System](#)

### Service Type

Cloud Volumes Service is offered as two service types: CVS and CVS-Performance.

Select the service type that matches your workload needs. [Region availability](#) varies by service type. [Learn more](#)

CVS

Offers volumes created with zonal high availability.

CVS-Performance

Offers 3 performance levels and improved latency to address higher performance application requirements.

### Volume Replication

Secondary

Select to create volume as a destination target for volume replication. Applicable only to CVS-performance volumes.

4. Specify the Google Cloud region for the volume and volume path (The volume path must be unique across all of cloud volumes in the project)

## [Create File System](#)

### Region

Region availability varies by service type.

Region \* —

europe-west3



Volume will be provisioned in the region you select.

Volume Path \* —

nimCVSMBvol01



Must be unique to the project.

5. Select the level of performance for the volume.

## [←](#) Create File System

### Service Level

Select the performance level required for your workload.

Standard

Up to 16 MiB/s per TiB

Premium

Up to 64 MiB/s per TiB

Extreme

Up to 128 MiB/s per TiB

Snapshot



The snapshot to create the volume from.

6. Specify the size of the volume and the protocol type. In this testing, SMB is used.

## [←](#) Create File System

### Volume Details

Allocated Capacity \*

1024

GiB

Allocated size must be between 1 TiB (1024 GiB) and 100 TiB (102400 GiB)

Protocol Type \*

SMB



Make snapshot directory (.snapshot) visible

Makes .snapshot directory visible to clients. For NFSv4.1 volumes (CVS-Performance only), the directory itself will not be listed but can be accessed to list contents, etc.

Enable SMB Encryption

Enable this option only if you require encryption of your SMB data traffic.

Enable CA share support for SQL Server, FSLogix

Enable this option only for SQL Server and FSLogix workloads that require continuous availability.

Hide SMB Share

Enable this option to make SMB shares non-browsable

7. In this step, select the VPC Network from which the volume will be accessible. Ensure VPC peering is in place.

HINT: If VPC peering has not been done, a pop-up button will be displayed to guide you through the peering commands. Open a Cloud Shell session and execute the appropriate commands to peer your VPC with Cloud Volumes Service producer. In case you decide to prepare VPC

peering in beforehand, refer to these [instructions](#).

## Network Details

### Shared VPC configuration

Provide the host project name when deploying in a shared VPC service project.

### VPC Network Name \*

cloud-volumes-vpc

Select the VPC Network from which the volume will be accessible. This cannot be changed later.

### Use Custom Address Range

#### Reserved Address range

netapp-addresses

## SHOW SNAPSHOT POLICY

**SAVE**

**CANCEL**

8. Click Save to create the volume.

	6a4552ed-7378-7302-be2b-21a169374f28	nimCVSMBvol01	europe-west3	Available for use	CVS-Performance	Primary	Standard	SMB : \\nimsmb-3830.nimgcveval.com\\nimCVSMBvol01
<input type="checkbox"/>								

To mount the SMB volume, do the following:

1. In the Cloud Console, go to Cloud Volumes > Volumes.
2. Go to the Volumes page
3. Click the SMB volume for which you want to map an SMB share.
4. Scroll to the right, under Show More, click Mount Instructions.

To perform the mounting process from within the Windows guest OS of the VMware VM, follow the below steps:

1. Click the Start button and then click on Computer.
2. Click Map Network Drive.
3. In the Drive list, click any available drive letter.
4. In the folder box, type:

\\nimsmb-3830.nimgcveval.com\\nimCVSMBvol01



### What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\10.53.0.4\ nimcvsmbvol01

Example: \\server\share

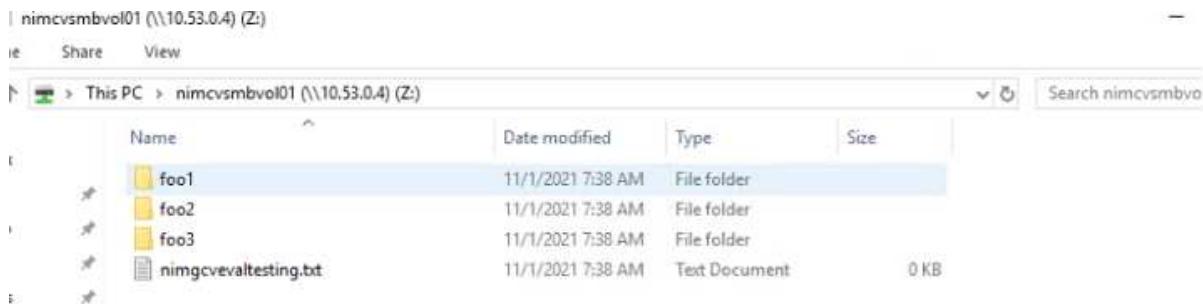
Reconnect at sign-in

Connect using different credentials

[Connect to a Web site that you can use to store your documents and pictures.](#)

To connect every time you log on to your computer, select the Reconnect at sign-in check box.

5. Click Finish.



### Region Availability for NFS datastores on AWS / VMC, Azure / AVS, and GCP / GCVE

Learn more about the Global Region support for NFS datastores on AWS, Azure and Google Cloud Platform (GCP).

#### AWS Region Availability

## Americas

AWS Region	VMC Availability	FSx ONTAP Availability	NFS Datastore Availability
US East (Northern Virginia)	Yes	Yes	Yes
US East (Ohio)	Yes	Yes	Yes
US West (Northern California)	Yes	No	No
US West (Oregon)	Yes	Yes	Yes
GovCloud (US West)	Yes	Yes	Yes
Canada (Central)	Yes	Yes	Yes
South America (Sao Paulo)	Yes	Yes	Yes

Last updated on: June 2, 2022.

## EMEA

AWS Region	VMC Availability	FSx ONTAP Availability	NFS Datastore Availability
Europe (Ireland)	Yes	Yes	Yes
Europe (London)	Yes	Yes	Yes
Europe (Frankfurt)	Yes	Yes	Yes
Europe (Paris)	Yes	Yes	Yes
Europe (Milan)	Yes	Yes	Yes
Europe (Stockholm)	Yes	Yes	Yes

Last updated on: June 2, 2022.

## Asia Pacific

AWS Region	VMC Availability	FSx ONTAP Availability	NFS Datastore Availability
Asia Pacific (Sydney)	Yes	Yes	Yes
Asia Pacific (Tokyo)	Yes	Yes	Yes
Asia Pacific (Osaka)	Yes	No	No
Asia Pacific (Singapore)	Yes	Yes	Yes
Asia Pacific (Seoul)	Yes	Yes	Yes
Asia Pacific (Mumbai)	Yes	Yes	Yes
Asia Pacific (Jakarta)	No	No	No
Asia Pacific (Hong Kong)	No	Yes	No

Last updated on: June 2, 2022.

## Azure Region Availability

## Americas

Azure Region	AVS Availability	ANF Availability	NFS Datastore Availability
Central US	Yes	Yes	Yes
East US	Yes	Yes	Yes
East US 2	No	Yes	No
North Central US	Yes	Yes	Yes
South Central US	Yes	Yes	Yes
West Central US	No	No	No
West US	Yes	Yes	Yes
West US2	No	Yes	No
West US3	GA: H1-2023	Yes	Yes
Canada Central	Yes	Yes	Yes
Canada East	Yes	Yes	Yes
Brazil South	Yes	Yes	Yes
Brazil Southeast	No	GA: Q2-2022	No

Last updated on: June 7, 2022.

## EMEA

Azure Region	AVS Availability	ANF Availability	NFS Datastore Availability
North Europe	Yes	Yes	Yes
West Europe	No	Yes	No
France Central	Yes	Yes	Yes
France South	No	GA: H2-2022	No
Germany North	No	Yes	No
Germany West Central	Yes	Yes	Yes
Norway East	No	Yes	No
Norway West	No	Yes	No
Sweden Central	GA: Q2-2022	GA: Q2-2022	No
Sweden South	No	No	No
Switzerland North	No	Yes	No
Switzerland West	No	Yes	No
UAE Central	No	Yes	No
UAE North	No	Yes	No
UK South	Yes	Yes	Yes

UK West

Yes

Yes

Yes

Last updated on: June 7, 2022.

## Asia Pacific

Azure Region	AVS Availability	ANF Availability	NFS Datastore Availability
Australia East	Yes	Yes	Yes
Australia Southeast	Yes	Yes	Yes
Australia Central	No	Yes	No
Japan East	No	Yes	No
Japan West	Yes	Yes	Yes
East Asia	No	Yes	No
Southeast Asia	Yes	Yes	Yes
Central India	No	Yes	No
South India	No	Yes	No
Korea Central	No	Yes	No

Last updated on: June 7, 2022.

## Summary and Conclusion: Why NetApp Hybrid Multi-Cloud with VMware

NetApp Cloud Volumes along with VMware solutions for the major hyperscalers provides great potential for organizations looking to leverage hybrid cloud. The rest of this section provides the use cases that show integrating NetApp Cloud Volumes enables true hybrid multi-cloud capabilities.

### Use case #1: Optimizing storage

When performing a sizing exercise using RVtools output, it is always evident that the horsepower (vCPU/vMem) scale is parallel with storage. Many times, organizations find themselves in a situation where the storage space requires drives the size of the cluster well beyond what is needed for horsepower.

By integrating NetApp Cloud Volumes, organizations can realize a vSphere-based cloud solution with a simple migration approach, with no re-platforming, no IP changes, and no architectural changes. Additionally, this optimization enables you to scale the storage footprint while keeping the host count to least amount required in vSphere, but no change to the storage hierarchy, security, or files made available. This allows you to optimize the deployment and reduce the overall TCO by 35–45%. This integration also enables you to scale storage from warm storage to production-level performance in seconds.

### Use case #2: Cloud migration

Organizations are under pressure to migrate applications from on-premises data centers to the Public Cloud for multiple reasons: an upcoming lease expiration; a finance directive to move from capital expenditure (capex) spending to operational expenditures (opex) spending; or simply a top-down mandate to move everything to the cloud.

When speed is critical, only a streamlined migration approach is feasible because re-platforming and refactoring applications to adapt to the cloud's particular IaaS platform is slow and expensive, often taking months. By combining NetApp Cloud Volumes with the bandwidth-efficient SnapMirror replication for guest-connected storage (including RDMS in conjunction with application-consistent Snapshot copies and HCX, cloud specific migration (e.g. Azure Migrate), or third-party products for replicating VMs), this transition is even easier than relying on time-consuming I/O filters mechanisms.

#### **Use case #3: Data center expansion**

When a data center reaches capacity limits due to seasonal demand spikes or just steady organic growth, moving to the cloud-hosted VMware along with NetApp Cloud Volumes is an easy solution. Leveraging NetApp Cloud Volumes allows storage creation, replication, and expansion very easily by providing high availability across availability zones and dynamic scaling capabilities. Leveraging NetApp Cloud Volumes helps in minimizing host cluster capacity by overcoming the need for stretch clusters.

#### **Use case #4: Disaster recovery to the cloud**

In a traditional approach, if a disaster occurs, the VMs replicated to the cloud would require conversion to the cloud's own hypervisor platform before they could be restored – not a task to be handled during a crisis.

By using NetApp Cloud Volumes for guest-connected storage using SnapCenter and SnapMirror replication from on-premises along with public cloud virtualization solutions, a better approach for disaster recovery can be devised allowing VM replicas to be recovered on fully consistent VMware SDDC infrastructure along with cloud specific recovery tools (e.g. Azure Site Recovery) or equivalent third-party tools such as Veeam. This approach also enables you to perform disaster recovery drills and recovery from ransomware quickly. This also enables you to scale to full production for testing or during a disaster by adding hosts on-demand.

#### **Use case #5: Application modernization**

After applications are in the public cloud, organizations will want to take advantage of the hundreds of powerful cloud services to modernize and extend them. With the use of NetApp Cloud Volumes, modernization is an easy process because the application data is not locked into vSAN and allows data mobility for a wide range of use cases, including Kubernetes.

### **Conclusion**

Whether you are targeting an all-cloud or hybrid cloud, NetApp Cloud Volumes provides excellent options to deploy and manage the application workloads along with file services and block protocols while reducing the TCO by making the data requirements seamless to the application layer.

Whatever the use case, choose your favorite cloud/hyperscaler together with NetApp Cloud Volumes for rapid realization of cloud benefits, consistent infrastructure, and operations across on-premises and multiple clouds, bidirectional portability of workloads, and enterprise-grade capacity and performance.

It is the same familiar process and procedures that are used to connect the storage. Remember, it is just the position of the data that changed with new names; the tools and processes all remain the same and NetApp Cloud Volumes helps in optimizing the overall deployment.

## **VMware Hybrid Cloud Use Cases**

### **Use Cases for NetApp Hybrid Multi-Cloud with VMware**

An overview of the use cases of importance to IT organization when planning hybrid-

cloud or cloud-first deployments.

## Popular Use Cases

Use cases include:

- Disaster recovery,
- Hosting workloads during data center maintenance, \* quick burst in which additional resources are required beyond what's provisioned in the local data center,
- VMware site expansion,
- Fast migration to the cloud,
- Dev/test, and
- Modernization of apps leveraging cloud native technologies.

Throughout this documentation, cloud workload references will be detailed using the VMware use-cases.

These use-cases are:

- Protect (includes both Disaster Recovery and Backup / Restore)
- Migrate
- Extend

## Inside the IT Journey

Most organizations are on a journey to transformation and modernization. As part of this process, companies are trying use their existing VMware investments while leveraging cloud benefits and exploring ways to make the migration process as seamless as possible. This approach would make their modernization efforts very easy because the data is already in the cloud.

The easiest answer to this scenario is VMware offerings in each hyperscaler. Like NetApp® Cloud Volumes, VMware provides a way to move or extend on-premises VMware environments to any cloud, allowing you to retain existing on-premises assets, skills, and tools while running workloads natively in the cloud. This reduces risk because there will be no service breaks or a need for IP changes and provides the IT team the ability to operate the way they do on-premises using existing skills and tools. This can lead to accelerated cloud migrations and a much smoother transition to a hybrid multi-cloud architecture.

## Understanding the Importance of Native Storage Options

While VMware in any cloud delivers unique hybrid capabilities to every customer, limited native storage options have restricted its usefulness for organizations with storage-heavy workloads. Because storage is directly tied to hosts, the only way to scale storage is to add more hosts—and that can increase costs by 35–40 percent or more for storage intensive workloads. These workloads just need additional storage, not additional horsepower. But that means paying for additional hosts.

Let's consider this scenario:

A customer requires just five hosts for CPU and memory, but has a lot of storage needs, and needs 12 hosts to meet the storage requirement. This requirement ends up really tipping the financial scale by having to buy the additional horsepower, when they only need to increment the storage.

When you're planning cloud adoption and migrations, it's always important to evaluate the best approach and take the easiest path that reduces total investments. The most common and easiest approach for any application migration is rehosting (also known as lift and shift) where there is no virtual machine (VM) or data

conversion. Using NetApp Cloud Volumes with VMware software-defined data center (SDDC), while complementing vSAN, provides an easy lift-and-shift option.

## NetApp Solutions for Amazon VMware Managed Cloud (VMC)

Learn more about the solutions that NetApp brings to AWS.

VMware defines the cloud workloads into one of three categories:

- Protect (including both Disaster Recovery and Backup / Restore)
- Migrate
- Extend

Browse the available solutions in the following sections.

### **Protect**

COMING SOON!!

### **Migrate**

COMING SOON!!

### **Extend**

COMING SOON!!

## NetApp Solutions for Azure VMware Solution (AVS)

Learn more about the solutions that NetApp brings to Azure.

VMware defines the cloud workloads into one of three categories:

- Protect (including both Disaster Recovery and Backup / Restore)
- Migrate
- Extend

Browse the available solutions in the following sections.

### **Protect**

COMING SOON!!

### **Migrate**

COMING SOON!!

### **Extend**

COMING SOON!!

## **NetApp Solutions for Google Cloud Virtualization Engine (GCVE)**

Learn more about the solutions that NetApp brings to GCP.

VMware defines the cloud workloads into one of three categories:

- Protect (including both Disaster Recovery and Backup / Restore)
- Migrate
- Extend

Browse the available solutions in the following sections.

### **Protect**

COMING SOON!!

### **Migrate**

COMING SOON!!

### **Extend**

COMING SOON!!

## **NetApp Hybrid Multi-Cloud Solutions for AWS / VMC**

### **Region Availability – NFS datastore for VMC**

Learn more about the Global Region support for AWS, VMC and FSx ONTAP.



NFS datastore will be available in regions where both services (VMC and FSx ONTAP) are available.

## Americas

AWS Region	VMC Availability	FSx ONTAP Availability	NFS Datastore Availability
US East (Northern Virginia)	Yes	Yes	Yes
US East (Ohio)	Yes	Yes	Yes
US West (Northern California)	Yes	No	No
US West (Oregon)	Yes	Yes	Yes
GovCloud (US West)	Yes	Yes	Yes
Canada (Central)	Yes	Yes	Yes
South America (Sao Paulo)	Yes	Yes	Yes

Last updated on: June 2, 2022.

## EMEA

AWS Region	VMC Availability	FSx ONTAP Availability	NFS Datastore Availability
Europe (Ireland)	Yes	Yes	Yes
Europe (London)	Yes	Yes	Yes
Europe (Frankfurt)	Yes	Yes	Yes
Europe (Paris)	Yes	Yes	Yes
Europe (Milan)	Yes	Yes	Yes
Europe (Stockholm)	Yes	Yes	Yes

Last updated on: June 2, 2022.

## Asia Pacific

AWS Region	VMC Availability	FSx ONTAP Availability	NFS Datastore Availability
Asia Pacific (Sydney)	Yes	Yes	Yes
Asia Pacific (Tokyo)	Yes	Yes	Yes
Asia Pacific (Osaka)	Yes	No	No
Asia Pacific (Singapore)	Yes	Yes	Yes
Asia Pacific (Seoul)	Yes	Yes	Yes
Asia Pacific (Mumbai)	Yes	Yes	Yes
Asia Pacific (Jakarta)	No	No	No
Asia Pacific (Hong Kong)	No	Yes	No

Last updated on: June 2, 2022.

# NetApp Hybrid Multi-Cloud Solutions for Azure / AVS

## NetApp Hybrid Multi-Cloud Solutions for GCP / GCVE

### Security overview - NetApp Cloud Volumes Service (CVS) in Google Cloud

#### TR-4918: Security overview - NetApp Cloud Volumes Service in Google Cloud

Oliver Krause, Justin Parisi, NetApp

#### Document scope

Security, particularly in the cloud where infrastructure is outside of the control of storage administrators, is paramount to trusting your data to service offerings provided by cloud providers. This document is an overview of the security offerings that NetApp [Cloud Volumes Service provides in Google Cloud](#).

#### Intended audience

This document's intended audience includes, but is not limited to, the following roles:

- Cloud providers
- Storage administrators
- Storage architects
- Field resources
- Business decision makers

If you have questions about the content of this technical report, see the section "[Contact us.](#)"

Abbreviation	Definition
CVS-SW	Cloud Volumes Service, Service Type CVS
CVS-Performance	Cloud Volume Service, Service Type CVS-Performance
PSA	

[Next: How Cloud Volumes Service in Google Cloud secures your data.](#)

#### **How Cloud Volumes Service in Google Cloud secures your data**

[Previous: Overview.](#)

Cloud Volumes Service in Google Cloud provides a multitude of ways to natively secure your data.

#### **Secure architecture and tenancy model**

Cloud Volumes Service provides a secure architecture in Google Cloud by segmenting the service management (control plane) and the data access (data plane) across different endpoints so that neither can impact the other (see the section "[Cloud Volumes Service architecture](#)"). It uses Google's [private services access](#) (PSA) framework to provide the service. This framework distinguishes between the service producer, which is provided and operated by NetApp, and the service consumer, which is a Virtual Private Cloud (VPC) in

a customer project, hosting the clients that want to access Cloud Volumes Service file shares.

In this architecture, tenants (see the section “[Tenancy model](#)”) are defined as Google Cloud projects that are completely isolated from each other unless explicitly connected by the user. Tenants allow complete isolation of data volumes, external name services, and other essential pieces of the solution from other tenants using the Cloud Volumes Service volume platform. Because the Cloud Volumes Service platform is connected through VPC peering, that isolation applies to it also. You can enable sharing of Cloud Volumes Service volumes between multiple projects by using a shared-VPC (see the section “[Shared VPCs](#)”). You can apply access controls to SMB shares and NFS exports to limit who or what can view or modify datasets.

### **Strong identity management for the control plane**

In the control plane where Cloud Volumes Service configuration takes place, identity management is managed by using [Identity Access Management \(IAM\)](#). IAM is a standard service that enables you to control authentication (logins) and authorization (permissions) to Google Cloud project instances. All configuration is performed with Cloud Volumes Service APIs over a secure HTTPS transport using TLS 1.2 encryption, and authentication is performed by using JWT tokens for added security. The Google console UI for Cloud Volumes Service translates user input into Cloud Volumes Service API calls.

### **Security hardening - Limiting attack surfaces**

Part of effective security is limiting the number of attack surfaces available in a service. Attack surfaces can include a variety of things, including data at-rest, in-flight transfers, logins, and the datasets themselves.

A managed service removes some of the attack surfaces inherently in its design. Infrastructure management, as described in the section “[Service operation](#),” is handled by a dedicated team and is automated to reduce the number of times a human actually touches configurations, which helps reduce the number of intentional and unintentional errors. Networking is fenced off so that only necessary services can access one another. Encryption is baked into the data storage and only the data plane needs security attention from Cloud Volumes Service administrators. By hiding most of the management behind an API interface, security is achieved by limiting the attack surfaces.

### **Zero Trust model**

Historically, IT security philosophy has been to trust but verify, and manifested as relying solely on external mechanisms (such as firewalls and intrusion detection systems) to mitigate threats. However, attacks and breaches evolved to bypass the verification in environments through phishing, social engineering, insider threats and other methods that provide the verification to enter networks and wreak havoc.

Zero Trust has become a new methodology in security, with the current mantra being “trust nothing while still verifying everything.” Therefore, nothing is allowed access by default. This mantra is enforced in a variety of ways, including standard firewalls and intrusion detection systems (IDS) and also with the following methods:

- Strong authentication methods (such as AES-encrypted Kerberos or JWT tokens)
- Single strong sources of identities (such as Windows Active Directory, Lightweight Directory Access Protocol (LDAP), and Google IAM)
- Network segmentation and secure multitenancy (only tenants are allowed access by default)
- Granular access controls with Least Privileged Access policies
- Small exclusive lists of dedicated, trusted administrators with digital audit and paper trails

Cloud Volumes Service running in Google Cloud adheres to the Zero Trust model by implementing the "trust nothing, verify everything" stance.

## Encryption

Encrypt data at-rest (see the section “[Data encryption at rest](#)”) by using XTS-AES-256 ciphers with NetApp Volume Encryption (NVE) and in-flight with “[SMB encryption](#)” or NFS Kerberos 5p support. Rest easy knowing cross-region replication transfers are protected by TLS 1.2 encryption (see the section “[Cross-region replication](#)”). In addition, Google networking also provides encrypted communications (see the section “[Data encryption in transit](#)”) for an added layer of protection against attacks. For more information about transport encryption, see the section “[Google Cloud network](#)”.

## Data protection and backups

Security isn’t just about the prevention of attacks. It is also about how we recover from attacks if or when they occur. This strategy includes data protection and backups. Cloud Volumes Service provides methods to replicate to other regions in case of outages (see the section “[Cross-region replication](#)”) or if a dataset is affected by a ransomware attack. It can also perform asynchronous backups of data to locations outside of the Cloud Volumes Service instance by using [Cloud Volumes Service backup](#). With regular backups, mitigation of security events can take less time and save money and angst for administrators.

## Fast ransomware mitigation with industry leading Snapshot copies

In addition to data protection and backups, Cloud Volumes Service provides support for immutable Snapshot copies (see the section “[Immutable Snapshot copies](#)”) of volumes that allow recovery from ransomware attacks (see the section “[Service operation](#)”) within seconds of discovering the issue and with minimal disruption. Recovery time and effects depend on the Snapshot schedule, but you can create Snapshot copies that provide as little as one-hour deltas in ransomware attacks. Snapshot copies have a negligible effect on performance and capacity usage and are a low-risk, high-reward approach to protecting your datasets.

[Next: Security considerations and attack surfaces.](#)

## Security considerations and attack surfaces

[Previous: How Cloud Volumes Service in Google Cloud secures your data.](#)

The first step in understanding how to secure your data is identifying the risks and potential attack surfaces. These include (but are not limited to) the following:

- Administration and logins
- Data at rest
- Data in flight
- Network and firewalls
- Ransomware, malware, and viruses

Understanding attack surfaces can help you to better secure your environments. Cloud Volumes Service in Google Cloud already considers many of these topics and implements security functionality by default, without any administrative interaction.

## Ensuring secure logins

When securing your critical infrastructure components, it is imperative to make sure that only approved users can log in and manage your environments. If bad actors breach your administrative credentials, then they have the keys to the castle and can do anything they want—change configurations, delete volumes and backups, create backdoors, or disable Snapshot schedules.

Cloud Volumes Service for Google Cloud provides protection against unauthorized administrative logins

through the obfuscation of storage as a service (StaaS). Cloud Volumes Service is completely maintained by the cloud provider with no availability to login externally. All setup and configuration operations are fully automated, so a human administrator never has to interact with the systems except in very rare circumstances.

If login is required, Cloud Volumes Service in Google Cloud secures logins by maintaining a very short list of trusted administrators that have access to log in to the systems. This gatekeeping helps reduce the number of potential bad actors with access. Additionally, the Google Cloud networking hides the systems behind layers of network security and exposes only what is needed to the outside world. For information about the Google Cloud, Cloud Volumes Service architecture, see the section “[Cloud Volumes Service architecture](#).”

### **Cluster administration and upgrades**

Two areas with potential security risks include cluster administration (what happens if a bad actor has admin access) and upgrades (what happens if a software image is compromised).

### **Storage administration protection**

Storage provided as a service removes the added risk of exposure to administrators by removing that access to end users outside of the cloud data center. Instead, the only configuration done is for the data access plane by customers. Each tenant manages their own volumes, and no tenant can reach other Cloud Volumes Service instances. The service is managed by automation, with a very small list of trusted administrators given access to the systems through the processes covered in the section “[Service operation](#).”

The CVS-Performance service type offers cross-region replication as an option to provide data protection to a different region in the event of a region failure. In those cases, Cloud Volumes Service can be failed over to the unaffected region to maintain data access.

### **Service upgrades**

Updates help protect vulnerable systems. Each update provides security enhancements and bug fixes that minimize attack surfaces. Software updates are downloaded from centralized repositories and are validated before the updates are allowed to verify that official images are used and that the upgrades are not compromised by bad actors.

With Cloud Volumes Service, updates are handled by the cloud provider teams, which removes risk exposure for administrator teams by providing experts well versed in configuration and upgrades that have automated and fully tested the process. Upgrades are nondisruptive, and Cloud Volumes Service maintains the latest updates for best overall results.

For information about the administrator team that performs these service upgrades, see the section “[Service operation](#).”

### **Securing data at-rest**

Data-at-rest encryption is important to protect sensitive data in the event of a disk that is stolen, returned, or repurposed. Data in Cloud Volumes Service is protected at rest by using software-based encryption.

- Google-generated keys are used for CVS-SW.
- For CVS-Performance, the per-volume keys are stored in a key manager built into Cloud Volumes Service, which uses NetApp ONTAP CryptoMod to generate AES-256 encryption keys. CryptoMod is listed on the CMVP FIPS 140-2 validated modules list. See [FIPS 140-2 Cert #4144](#).

Starting in November 2021, preview Customer-managed Encryption (CMEK) functionality was made available for CVS-Performance. This functionality allows you to encrypt the per-volume keys with per-project, per-region master-keys that are hosted in Google Key Management Service (KMS). KMS enables you to attach external

key managers.

For details about how to configure KMS for CVS-Performance, see the [Cloud Volumes Service documentation](#).

For more information about architecture, see the section [“Cloud Volumes Service architecture.”](#)

## Securing data in-flight

In addition to securing data at rest, you must also be able to secure data when it is in flight between the Cloud Volumes Service instance and a client or replication target. Cloud Volumes Service provides encryption for in-flight data over NAS protocols by using encryption methods such as SMB encryption using Kerberos, the signing/sealing of packets, and NFS Kerberos 5p for end-to-end encryption of data transfers.

Replication of Cloud Volumes Service volumes uses TLS 1.2, which takes advantage of AES-GCM encryption methods.

Most insecure in-flight protocols such as telnet, NDMP, and so on are disabled by default. DNS, however, is not encrypted by Cloud Volumes Service (no DNS Sec support) and should be encrypted by using external network encryption when possible. See the section [“Data encryption in transit”](#) for more information about securing data in-flight.

For information about NAS protocol encryption, see the section [“NAS protocols.”](#)

## Users and groups for NAS permissions

Part of securing your data in the cloud involves proper user and group authentication, where the users accessing the data are verified as real users in the environment and the groups contain valid users. These users and groups provide initial share and export access, as well as permission validation for files and folders in the storage system.

Cloud Volumes Service uses standard Active Directory-based Windows user and group authentication for SMB shares and Windows-style permissions. The service can also leverage UNIX identity providers such as LDAP for UNIX users and groups for NFS exports, NFSv4 ID validation, Kerberos authentication, and NFSv4 ACLs.



Currently only Active Directory LDAP is supported with Cloud Volumes Service for LDAP functionality.

## Detection, prevention and mitigation of ransomware, malware, and viruses

Ransomware, malware, and viruses are a persistent threat to administrators, and detection, prevention, and mitigation of those threats are always top of mind for enterprise organizations. A single ransomware event on a critical dataset can potentially cost millions of dollars, so it is beneficial to do what you can to minimize the risk.

Although Cloud Volumes Service currently doesn't include native detection or prevention measures, such as antivirus protection or [automatic ransomware detection](#), there are ways to quickly recover from a ransomware event by enabling regular Snapshot schedules. Snapshot copies are immutable and read only pointers to changed blocks in the file system, are near instantaneous, have minimal impact on performance, and only use up space when data is changed or deleted. You can set schedules for Snapshot copies to match your desired acceptable recovery point objective (RPO)/recovery time objective (RTO) and can keep up to 1,024 Snapshot copies per volume.

Snapshot support is included at no additional cost (beyond data storage charges for changed blocks/data retained by Snapshot copies) with Cloud Volumes Service and, in the event of a ransomware attack, can be used to roll back to a Snapshot copy before the attack occurred. Snapshot restores take just seconds to complete, and you then can get back to serving data as normal. For more information, see [The NetApp](#)

## Solution for Ransomware.

Preventing ransomware from affecting your business requires a multilayered approach that includes one or more of the following:

- Endpoint protection
- Protection against external threats through network firewalls
- Detection of data anomalies
- Multiple backups (onsite and offsite) of critical datasets
- Regular restore tests of backups
- Immutable read-only NetApp Snapshot copies
- Multifactor authentication for critical infrastructure
- Security audits of system logins

This list is far from exhaustive but is a good blueprint to follow when dealing with the potential of ransomware attacks. Cloud Volumes Service in Google Cloud provides several ways to protect against ransomware events and reduce their effects.

### Immutable Snapshot copies

Cloud Volumes Service natively provides immutable read-only Snapshot copies that are taken on a customizable schedule for quick point-in-time recovery in the event of data deletion or if an entire volume has been victimized by a ransomware attack. Snapshot restores to previous good Snapshot copies are fast and minimize data loss based on the retention period of your Snapshot schedules and RTO/RPO. The performance effect with Snapshot technology is negligible.

Because Snapshot copies in Cloud Volumes Service are read-only, they cannot be infected by ransomware unless the ransomware has proliferated into the dataset unnoticed and Snapshot copies have been taken of the data infected by ransomware. This is why you must also consider ransomware detection based on data anomalies. Cloud Volumes Service does not currently provide detection natively, but you can use external monitoring software.

### Backups and restores

Cloud Volumes Service provides standard NAS client backup capabilities (such as backups over NFS or SMB).

- CVS-Performance offers cross-region volume replication to other CVS-Performance volumes. For more information, see [volume replication](#) in the Cloud Volumes Service documentation.
- CVS-SW offers service-native volume backup/restore capabilities. For more information, see [cloud backup](#) in the Cloud Volumes Service documentation.

Volume replication provides an exact copy of the source volume for fast failover in the case of a disaster, including ransomware events.

### Cross-region replication

CVS-Performance enables you to securely replicate volumes across Google Cloud regions for data protection and archive use cases by using TLS1.2 AES 256 GCM encryption on a NetApp-controlled backend service network using specific interfaces used for replication running on Google's network. A primary (source) volume contains the active production data and replicates to a secondary (destination) volume to provide an exact replica of the primary dataset.

Initial replication transfers all blocks, but updates only transmit the changed blocks in a primary volume. For instance, if a 1TB database that resides on a primary volume is replicated to the secondary volume, then 1TB of space is transferred on the initial replication. If that database has a few hundred rows (hypothetically, a few MB) that change between the initialization and the next update, only the blocks with the changed rows are replicated to the secondary (a few MB). This helps to make sure that the transfer times remain low and keeps replication charges down.

All permissions on files and folders are replicated to the secondary volume, but share access permissions (such as export policies and rules or SMB shares and share ACLs) must be handled separately. In the case of a site failover, the destination site should leverage the same name services and Active Directory domain connections to provide consistent handling of user and group identities and permissions. You can use a secondary volume as a failover target in the event of a disaster by breaking the replication relationship, which converts the secondary volume to read-write.

Volume replicas are read-only, which provides an immutable copy of data offsite for quick recovery of data in instances where a virus has infected data or ransomware has encrypted the primary dataset. Read-only data won't be encrypted, but, if the primary volume is affected and replication occurs, the infected blocks also replicate. You can use older, non-affected Snapshot copies to recover, but SLAs might fall out of range of the promised RTO/RPO depending on how quickly an attack is detected.

In addition, you can prevent malicious administrative actions, such as volume deletions, Snapshot deletions, or Snapshot schedule changes, with cross-region replication (CRR) management in Google Cloud. This is done by creating custom roles that separate volume administrators, who can delete source volumes but not break mirrors and therefore cannot delete destination volumes, from CRR administrators, who cannot perform any volume operations. See [Security Considerations](#) in the Cloud Volumes Service documentation for permissions allowed by each administrator group.

## Cloud Volumes Service backup

Although Cloud Volumes Service provides high data durability, external events can cause data loss. In the event of a security event such as a virus or ransomware, backups and restores become critical for resumption of data access in a timely manner. An administrator might accidentally delete a Cloud Volumes Service volume. Or users simply want to retain backup versions of their data for many months and keeping the extra Snapshot copy space inside the volume becomes a cost challenge. Although Snapshot copies should be the preferred way to keep backup versions for the last few weeks to restore lost data from them, they are sitting inside the volume and are lost if the volume goes away.

For all these reasons, NetApp Cloud Volumes Service offers backup services through [Cloud Volumes Service backup](#).

Cloud Volumes Service backup generates a copy of the volume on Google Cloud Storage (GCS). It only backs up the actual data stored within the volume, not the free space. It works as incremental forever, meaning it transfers the volume content once and from there on continues backing up changed data only. Compared to classical backup concepts with multiple full backups, it saves large amounts of backup storage, reducing cost. Because the monthly price of backup space is lower compared to a volume, it is an ideal place to keep backup versions longer.

Users can use a Cloud Volumes Service backup to restore any backup version to the same or a different volume within the same region. If the source volume is deleted, the backup data is retained and needs to be managed (for example, deleted) independently.

Cloud Volumes Service backup is built into Cloud Volumes Service as option. Users can decide which volumes to protect by activating Cloud Volumes Service backup on a per-volume basis. See the [Cloud Volumes Service backup documentation](#) for information about backups, the [number of maximum backup versions supported](#), scheduling, and [pricing](#).

All backup data of a project is stored within a GCS bucket, which is managed by the service and not visible to the user. Each project uses a different bucket. Currently, the buckets are in same region as the Cloud Volumes Service volumes, but more options are being discussed. Consult the documentation for the latest status.

Data transport from a Cloud Volumes Service bucket to GCS uses service-internal Google networks with HTTPS and TLS1.2. Data is encrypted at-rest with Google-managed keys.

To manage Cloud Volumes Service backup (creating, deleting, and restoring backups), a user must have the [roles/netappcloudvolumes.admin](#) role.

[Next: Architecture overview.](#)

## Architecture

### Overview

[Previous: Security considerations and attack surfaces.](#)

Part of trusting a cloud solution is understanding the architecture and how it is secured. This section calls out different aspects of the Cloud Volumes Service architecture in Google to help alleviate potential concerns about how data is secured, as well as call out areas where additional configuration steps might be required to obtain the most secure deployment.

The general architecture of Cloud Volumes Service can be broken down into two main components: the control plane and the data plane.

### Control plane

The control plane in Cloud Volumes Service is the backend infrastructure managed by Cloud Volumes Service administrators and NetApp native automation software. This plane is completely transparent to end users and includes networking, storage hardware, software updates, and so on to help deliver value to a cloud-resident solution such as Cloud Volumes Service.

### Data plane

The data plane in Cloud Volumes Service includes the actual data volumes and the overall Cloud Volumes Service configuration (such as access control, Kerberos authentication, and so on). The data plane is entirely under the control of the end users and the consumers of the Cloud Volumes Service platform.

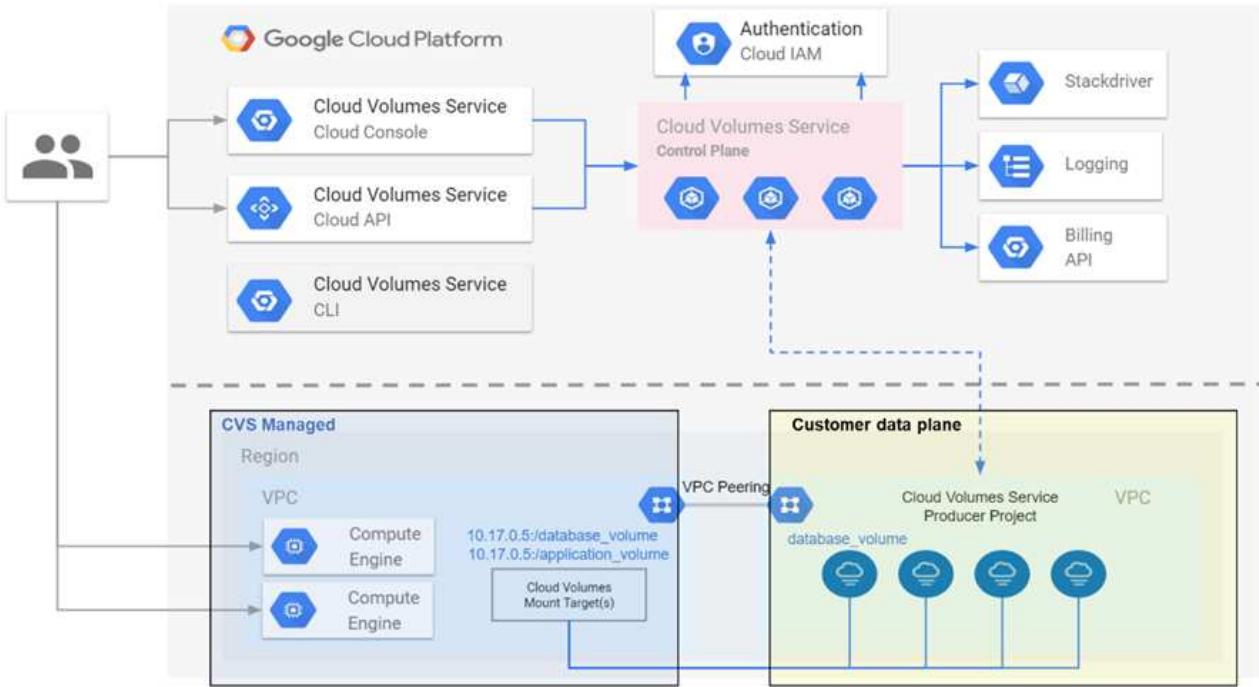
There are distinct differences in how each plane is secured and managed. The following sections cover these differences, starting with a Cloud Volumes Service architecture overview.

[Next: Cloud Volumes Service architecture.](#)

### Cloud Volumes Service architecture

In a manner similar to other Google Cloud native services such as CloudSQL, Google Cloud VMware Engine (GCVE), and FileStore, Cloud Volumes Service uses [Google PSA](#) to deliver the service. In PSA, services are built inside a service producer project, which uses [VPC network peering](#) to connect to the service consumer. The service producer is provided and operated by NetApp, and the service consumer is a VPC in a customer project, hosting the clients that want to access Cloud Volumes Service file shares.

The following figure, referenced from the [architecture section](#) of the Cloud Volumes Service documentation, shows a high-level view.



The part above the dotted line shows the control plane of the service, which controls the volume lifecycle. The part below the dotted line shows the data plane. The left blue box depicts the user VPC (service consumer), the right blue box is the service producer provided by NetApp. Both are connected through VPC peering.

## Tenancy model

In Cloud Volumes Service, individual projects are considered unique tenants. This means that manipulation of volumes, Snapshot copies, and so on are performed on a per-project basis. In other words, all volumes are owned by the project that they were created in and only that project can manage and access the data inside of them by default. This is considered the control plane view of the service.

## Shared VPCs

On the data plane view, Cloud Volumes Service can connect to a shared VPC. You can create volumes in the hosting project or in one of the service projects connected to the shared VPC. All projects (host or service) connected to that shared VPC are able to reach the volumes at the network layer (TCP/IP). Because all clients with network connectivity on the shared- VPC can potentially access the data through NAS protocols, access control on the individual volume (such as user/group access control lists (ACLs) and hostnames/IP addresses for NFS exports) must be used to control who can access the data.

You can connect Cloud Volumes Service to up to five VPCs per customer project. On the control plane, the project enables you to manage all created volumes, no matter which VPC they are connected to. On the data plane, VPCs are isolated from one another, and each volume can only be connected to one VPC.

Access to the individual volumes is controlled by protocol specific (NFS/SMB) access control mechanisms.

In other words, on the network layer, all projects connected to the shared VPC are able to see the volume, while, on the management side, the control plane only allows the owner project to see the volume.

## VPC Service Controls

VPC Service Controls establish an access control perimeter around Google Cloud services that are attached to

the internet and are accessible worldwide. These services provide access control through user identities but cannot restrict which network location requests originate from. VPC Service Controls close that gap by introducing the capabilities to restrict access to defined networks.

The Cloud Volumes Service data plane is not connected to the external internet but to private VPCs with well-defined network boundaries (perimeters). Within that network, each volume uses protocol-specific access control. Any external network connectivity is explicitly created by Google Cloud project administrators. The control plane, however, does not provide the same protections as the data plane and can be accessed by anyone from anywhere with valid credentials ([JWT tokens](#)).

In short, the Cloud Volumes Service data plane provides the capability of network access control, without the requirement to support VPC Service Controls and does not explicitly use VPC Service Controls.

## Packet sniffing/trace considerations

Packet captures can be useful for troubleshooting network issues or other problems (such as NAS permissions, LDAP connectivity, and so on), but can also be used maliciously to gain information about network IP addresses, MAC addresses, user and group names, and what level of security is being used on endpoints. Because of the way Google Cloud networking, VPCs, and firewall rules are configured, unwanted access to network packets should be difficult to obtain without user login credentials or [JWT tokens](#) into the cloud instances. Packet captures are only possible on endpoints (such as virtual machines (VMs)) and only possible on endpoints internal to the VPC unless a shared VPC and/or external network tunnel/IP forwarding is in use to explicitly allow external traffic to endpoints. There is no way to sniff traffic outside of the clients.

When shared VPCs are used, in-flight encryption with NFS Kerberos and/or [SMB encryption](#) can mask much of the information gleaned from traces. However, some traffic is still sent in plaintext, such as [DNS](#) and [LDAP queries](#). The following figure shows a packet capture from a plaintext LDAP query originating from Cloud Volumes Service and the potential identifying information that is exposed. LDAP queries in Cloud Volumes Service currently do not support encryption or LDAP over SSL. Both CVS-SW and CVS-Performance support LDAP signing.

IP addresses of the LDAP server and CVS instance			LDAP base DN and search type, search result			
No.	Time	Source	Destination	Protocol	Length	Info
2320...	366.244071	10.194.0.6	10.19.0.11	LDAP	225	searchRequest(2) "DC=cvsdemo,DC=local" wholeSubtree
2320...	366.244381	10.10.0.11	10.194.0.6	LDAP	330	searchResRef(2)   searchResRef(2)   searchResRef(2)   searchResDone(2) success [0 results]
<pre>▼ searchRequest   baseObject: DC=cvsdemo,DC=local   scope: wholeSubtree (2)   derefAliases: neverDerefAliases (0)   sizeLimit: 0   timeLimit: 3   typesOnly: False   ▼ Filter: (&amp;(objectClass=User)(uidNumber=1025))     ▼ filter: and (0)       ▼ and: (&amp;(objectClass=User)(uidNumber=1025))         ▼ and: 2 items           ▼ Filter: (objectClass=User)             ▼ and: item: equalityMatch (3)               ▼ equalityMatch                 attributeDesc: objectClass                 assertionValue: User             ▼ Filter: (uidNumber=1025)               ▼ and: item: equalityMatch (3)                 ▼ equalityMatch                   attributeDesc: uidNumber                   assertionValue: 1025         ▼ attributes: 7 items           AttributeDescription: uid           AttributeDescription: uidNumber           AttributeDescription: gidNumber           AttributeDescription: unixUserPassword           AttributeDescription: name           AttributeDescription: unixHomeDirectory           AttributeDescription: loginShell</pre>						



unixUserPassword is queried by LDAP and is not sent in plaintext but instead in a salted hash. By default, Windows LDAP does not populate the unixUserPassword fields. This field is only required if you need to leverage Windows LDAP for interactive logins through LDAP to clients. Cloud Volumes Service does not support interactive LDAP logins to the instances.

The following figure shows a packet capture from an NFS Kerberos conversation next to a capture of NFS over AUTH\_SYS. Note how the information available in a trace differs between the two and how enabling in-flight encryption offers greater overall security for NAS traffic.

IP addresses of the NFS client and CVS instance						Generalized NFS call/reply	
No.	Time	Source	Destination	Protocol	Length	Info	
380	9.218014	10.193.67.225	10.193.67.219	NFS	346	V4 Call (Reply In 381)	
381	9.218480	10.193.67.219	10.193.67.225	NFS	426	V4 Reply (Call In 380)	
382	9.218641	10.193.67.225	10.193.67.219	NFS	370	V4 Call (Reply In 397)	
397	9.369035	10.193.67.219	10.193.67.225	NFS	458	V4 Reply (Call In 382)	

> Frame 381: 426 bytes on wire (3408 bits), 426 bytes captured (3408 bits)  
> Ethernet II, Src: IntelCor\_7f:da:bc (90:e2:ba:7f:da:bc), Dst: VMware\_a0:2c:2d (00:50:56:a0:2c:2d)  
> Internet Protocol Version 4, Src: 10.193.67.219, Dst: 10.193.67.225  
> Transmission Control Protocol, Src Port: 2049, Dst Port: 738, Seq: 6305, Ack: 6569, Len: 360  
> Remote Procedure Call, Type:Reply XID:0xef5e998d

▼ GSS-Wrap  
Length: 300  
GSS Data: 050407ff000000000000000025913451ee1d43d298cf3031...  
  > krb5\_blob: 050407ff000000000000000025913451ee1d43d298cf3031...  
▼ Network File System  
[Program Version: 4]  
[V4 Procedure: COMPOUND (1)]

GSS wrapped NFS calls/replies with no other identifying information

IP addresses of the NFS client and CVS instance						Detailed NFS call types and file handle information	
No.	Time	Source	Destination	Protocol	Length	Info	
33	0.958480	10.193.67.201	10.193.67.204	NFS	458	V4 Reply (Call In 32) OPEN StateID: 0x0481	
34	0.958784	10.193.67.204	10.193.67.201	NFS	306	V4 Call (Reply In 35) SETATTR FH: 0x6c07918a	
35	0.959284	10.193.67.201	10.193.67.204	NFS	350	V4 Reply (Call In 34) SETATTR	

> Opcode: PUTFH (22)  
> Opcode: SETATTR (34)  
▼ Opcode: GETATTR (9)  
  Status: NFS4\_OK (0)  
  ▼ Attr mask[0]: 0x0010011a (Type, Change, Size, FSID, fileId)  
    > reqd\_attr: Type (1)  
    > reqd\_attr: Change (3)  
    > reqd\_attr: Size (4)  
    > reqd\_attr: FSID (8)  
      ▼ reco\_attr: fileId (20) File ID  
        fileId: 9232254136597092620  
  ▼ Attr mask[1]: 0x00b00a03a (Mode, NumLinks, Owner, Owner\_Group, Space\_Used, Time\_Access, Time\_Metadata, Time\_Modify, Mounted\_on\_FileId)  
    ▼ reco\_attr: Mode (33) Permission information  
      > mode: 0644, Name: Unknown, Read permission for owner, Write permission for owner, Read permission for group, Read permission for others  
    > reco\_attr: NumLinks (35)  
      ▼ reco\_attr: Owner (36) Owner and group ID strings  
        > fattr4\_owner: root@NTAP.LOCAL  
      ▼ reco\_attr: Owner\_Group (37)  
        > fattr4\_owner\_group: root@NTAP.LOCAL  
    > reco\_attr: Space\_Used (45)  
    > reco\_attr: Time\_Access (47)  
    > reco\_attr: Time\_Metadata (52)  
    > reco\_attr: Time\_Modify (53)  
    > reco\_attr: Mounted\_on\_FileId (55)

## VM network interfaces

One trick attackers might attempt is to add a new network interface card (NIC) to a VM in **promiscuous mode** (port mirroring) or enable promiscuous mode on an existing NIC in order to sniff all traffic. In Google Cloud, adding a new NIC requires a VM to be shut down entirely, which creates alerts, so attackers cannot do this

unnoticed.

In addition, NICs cannot be set to promiscuous mode at all and will trigger alerts in Google Cloud.

[Next: Control plane architecture.](#)

## Control plane architecture

[Previous: Cloud Volumes Service architecture.](#)

All management actions to Cloud Volumes Service are done through API. Cloud Volumes Service management integrated into the GCP Cloud Console also uses the Cloud Volumes Service API.

## Identity and Access Management

Identity and Access Management ([IAM](#)) is a standard service that enables you to control authentication (logins) and authorization (permissions) to Google Cloud project instances. Google IAM provides a full audit trail of permissions authorization and removal. Currently Cloud Volumes Service does not provide control plane auditing.

## Authorization/permission overview

IAM offers built-in, granular permissions for Cloud Volumes Service. You can find a [complete list of granular permissions here](#).

IAM also offers two predefined roles called `netappcloudvolumes.admin` and `netappcloudvolumes.viewer`. These roles can be assigned to specific users or service accounts.

Assign appropriate roles and permission to allow IAM users to manage Cloud Volumes Service.

Examples for using granular permissions include the following:

- Build a custom role with only `get/list/create/update` permissions so that users cannot delete volumes.
- Use a custom role with only `snapshot.*` permissions to create a service account that is used to build application-consistent Snapshot integration.
- Build a custom role to delegate `volumereplication.*` to specific users.

## Service accounts

To make Cloud Volumes Service API calls through scripts or [Terraform](#), you must create a service account with the `roles/netappcloudvolumes.admin` role. You can use this service account to generate the JWT tokens required to authenticate Cloud Volumes Service API requests in two different ways:

- Generate a JSON key and use Google APIs to derive a JWT token from it. This is the simplest approach, but it involves manual secrets (the JSON key) management.
- Use [Service account impersonation](#) with `roles/iam.serviceAccountTokenCreator`. The code (script, Terraform, and so on.) runs with [Application Default Credentials](#) and impersonates the service account to gain its permissions. This approach reflects Google security best practices.

See [Creating your service account and private key](#) in the Google cloud documentation for more information.

## Cloud Volumes Service API

Cloud Volumes Service API uses a REST-based API by using HTTPS (TLSv1.2) as the underlying network transport. You can find the latest API definition [here](#) and information about how to use the API at [Cloud Volumes APIs in the Google cloud documentation](#).

The API endpoint is operated and secured by NetApp using standard HTTPS (TLSv1.2) functionality.

### JWT tokens

Authentication to the API is performed with JWT bearer tokens ([RFC-7519](#)). Valid JWT tokens must be obtained by using Google Cloud IAM authentication. This must be done by fetching a token from IAM by providing a service account JSON key.

### Audit logging

Currently, no user-accessible control plane audit logs are available.

[Next: Data plane architecture.](#)

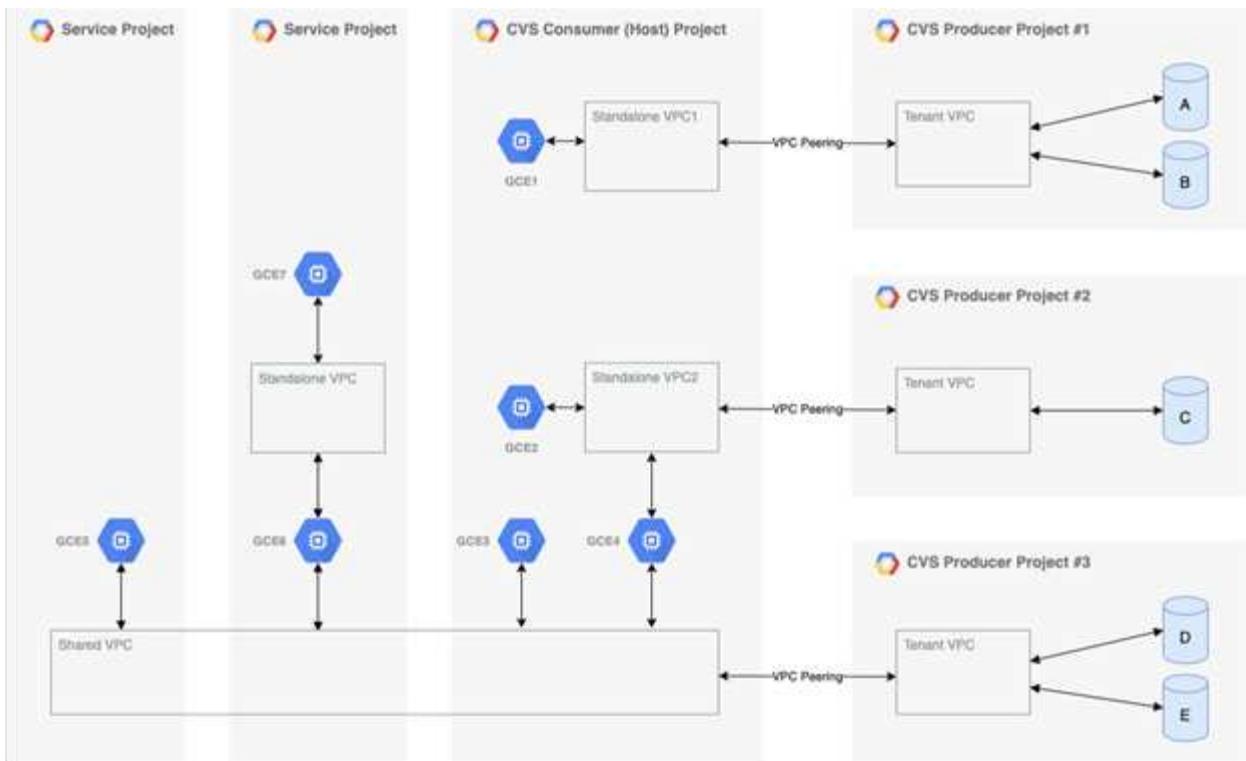
### Data plane architecture

[Previous: Control plane architecture.](#)

Cloud Volumes Service for Google Cloud leverages the Google Cloud [private services access](#) framework. In this framework, users can connect to the Cloud Volumes Service. This framework uses Service Networking and VPC peering constructs like other Google Cloud services, ensuring complete isolation between tenants.

For an architecture overview of Cloud Volumes Service for Google Cloud, see [Architecture for Cloud Volumes Service](#).

User VPCs (standalone or shared) are peered to VPCs within Cloud Volumes Service managed tenant projects, which hosts the volumes.



The preceding figure shows a project (the CVS consumer project in the middle) with three VPC networks connected to Cloud Volumes Service and multiple Compute Engine VMs (GCE1-7) sharing volumes:

- VPC1 allows GCE1 to access volumes A and B.
- VPC2 allows GCE2 and GCE4 to access volume C.
- The third VPC network is a shared VPC, shared with two service projects. It allows GCE3, GCE4, GCE5, and GCE6 to access volumes D and E. Shared VPC networks are only supported for volumes of the CVS-Performance service type.



GCE7 cannot access any volume.

Data can be encrypted both in-transit (using Kerberos and/or SMB encryption) and at-rest in Cloud Volumes Service.

[Next: Data encryption in transit.](#)

#### **Data encryption in transit**

[Previous: Data plane architecture.](#)

Data in transit can be encrypted at the NAS protocol layer, and the Google Cloud network itself is encrypted, as described in the following sections.

#### **Google Cloud network**

Google Cloud encrypts traffic on the network level as described in [Encryption in transit](#) in the Google documentation. As mentioned in the section “Cloud Volumes Services architecture,” Cloud Volumes Service is delivered out of a NetApp-controlled PSA producer project.

In case of CVS-SW, the producer tenant runs Google VMs to provide the service. Traffic between user VMs

and Cloud Volumes Service VMs is encrypted automatically by Google.

Although the data path for CVS-Performance isn't fully encrypted on the network layer, NetApp and Google use a combination of [IEEE 802.1AE encryption \(MACSec\)](#), [encapsulation](#) (data encryption), and physically restricted networks to protect data in transit between the Cloud Volumes Service CVS-Performance service type and Google Cloud.

## NAS protocols

NFS and SMB NAS protocols provide optional transport encryption at the protocol layer.

## SMB encryption

[SMB encryption](#) provides end-to-end encryption of SMB data and protects data from eavesdropping occurrences on untrusted networks. You can enable encryption for both the client/server data connection (only available to SMB3.x capable clients) and the server/domain controller authentication.

When SMB encryption is enabled, clients that do not support encryption cannot access the share.

Cloud Volumes Service supports RC4-HMAC, AES-128-CTS-HMAC-SHA1, and AES-256-CTS-HMAC-SHA1 security ciphers for SMB encryption. SMB negotiates to the highest supported encryption type by the server.

## NFSv4.1 Kerberos

For NFSv4.1, CVS-Performance offers Kerberos authentication as described in [RFC7530](#). You can enable Kerberos on a per-volume basis.

The current strongest available encryption type for Kerberos is AES-256-CTS-HMAC-SHA1. NetApp Cloud Volumes Service supports AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3, and DES for NFS. It also supports ARCFour-HMAC (RC4) for CIFS/SMB traffic, but not for NFS.

Kerberos provides three different security levels for NFS mounts that offer choices for how strong the Kerberos security should be.

As per RedHat's [Common Mount Options](#) documentation:

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to authenticate users.  
sec=krb5i uses Kerberos V5 for user authentication and performs integrity checking of NFS operations using secure checksums to prevent data tampering.  
sec=krb5p uses Kerberos V5 for user authentication, integrity checking, and encrypts NFS traffic to prevent traffic sniffing. This is the most secure setting, but it also involves the most performance overhead.
```

As a general rule, the more the Kerberos security level has to do, the worse the performance is, as the client and server spend time encrypting and decrypting NFS operations for each packet sent. Many clients and NFS servers provide support for AES-NI offloading to the CPUs for a better overall experience, but the performance impact of Kerberos 5p (full end-to-end encryption) is significantly greater than the impact of Kerberos 5 (user authentication).

The following table shows differences in what each level does for security and performance.

Security level	Security	Performance
NFSv3—sys	<ul style="list-style-type: none"> <li>Least secure; plain text with numeric user IDs/group IDs</li> <li>Able to view UID, GID, client IP addresses, export paths, file names, permissions in packet captures</li> </ul>	<ul style="list-style-type: none"> <li>Best for most cases</li> </ul>
NFSv4.x—sys	<ul style="list-style-type: none"> <li>More secure than NFSv3 (client IDs, name string/domain string matching) but still plain text</li> <li>Able to view UID, GID, client IP addresses, name strings, domain IDs, export paths, file names, permissions in packet captures</li> </ul>	<ul style="list-style-type: none"> <li>Good for sequential workloads (such as VMs, databases, large files)</li> <li>Bad with high file count/high metadata (30-50% worse)</li> </ul>
NFS—krb5	<ul style="list-style-type: none"> <li>Kerberos encryption for credentials in every NFS packet—wraps UID/GID of users/groups in RPC calls in GSS wrapper</li> <li>User requesting access to mount needs a valid Kerberos ticket (either through username/password or manual key tab exchange); ticket expires after a specified time period and user must reauthenticate for access</li> <li>No encryption for NFS operations or ancillary protocols like mount/portmapper/nlm (can see export paths, IP addresses, file handles, permissions, file names, atime/mtime in packet captures)</li> </ul>	<ul style="list-style-type: none"> <li>Best in most cases for Kerberos; worse than AUTH_SYS</li> </ul>

Security level	Security	Performance
NFS—krb5i	<ul style="list-style-type: none"> <li>• Kerberos encryption for credentials in every NFS packet—wraps UID/GID of users/groups in RPC calls in GSS wrapper</li> <li>• User requesting access to mount needs a valid Kerberos ticket (either via username/password or manual key tab exchange); ticket expires after a specified time period and user must reauthenticate for access</li> <li>• No encryption for NFS operations or ancillary protocols like mount/portmapper/nlm (can see export paths, IP addresses, file handles, permissions, file names, atime/mtime in packet captures)</li> <li>• Kerberos GSS checksum is added to every packet to ensure nothing intercepts the packets. If checksums match, conversation is allowed.</li> </ul>	<ul style="list-style-type: none"> <li>• Better than krb5p because the NFS payload is not encrypted; only added overhead compared to krb5 is the integrity checksum. Performance of krb5i won't be much worse than krb5 but will see some degradation.</li> </ul>

Security level	Security	Performance
NFS – krb5p	<ul style="list-style-type: none"> <li>• Kerberos encryption for credentials in every NFS packet—wraps UID/GID of users/groups in RPC calls in GSS wrapper</li> <li>• User requesting access to mount needs a valid Kerberos ticket (either via username/password or manual keytab exchange); ticket expires after specified time period and user must reauthenticate for access</li> <li>• All of the NFS packet payloads are encrypted with the GSS wrapper (cannot see file handles, permissions, file names, atime/mtime in packet captures).</li> <li>• Includes integrity check.</li> <li>• NFS operation type is visible (FSINFO, ACCESS, GETATTR, and so on).</li> <li>• Ancillary protocols (mount, portmap, nlm, and so on) are not encrypted - (can see export paths, IP addresses)</li> </ul>	<ul style="list-style-type: none"> <li>• Worst performance of the security levels; krb5p has to encrypt/decrypt more.</li> <li>• Better performance than krb5p with NFSv4.x for high file count workloads.</li> </ul>

In Cloud Volumes Service, a configured Active Directory server is used as Kerberos server and LDAP server (to lookup user identities from an RFC2307 compatible schema). No other Kerberos or LDAP servers are supported. NetApp highly recommends that you use LDAP for identity management in Cloud Volumes Service. For information on how NFS Kerberos is shown in packet captures, see the section [“Packet sniffing/trace considerations.”](#)

[Next: Data encryption at rest.](#)

[Data encryption at rest](#)

[Previous: Data encryption in transit.](#)

All volumes in Cloud Volumes Service are encrypted-at-rest using AES-256 encryption, which means all user data written to media is encrypted and can only be decrypted with a per-volume key.

- For CVS-SW, Google-generated keys are used.
- For CVS-Performance, the per-volume keys are stored in a key manager built into the Cloud Volumes Service.

Starting in November 2021, preview customer-managed encryption keys (CMEK) functionality was made available. This enables you to encrypt the per-volume keys with a per-project, per-region master key that is

hosted in [Google Key Management Service \(KMS\)](#). KMS enables you to attach external key managers.

For information about configuring KMS for CVS-Performance, see [Setting up customer-managed encryption keys](#).

Next: [Firewall](#).

## Firewall

Previous: [Data encryption at rest](#).

Cloud Volumes Service exposes multiple TCP ports to serve NFS and SMB shares:

- [Ports required for NFS access](#)
- [Ports required for SMB access](#)

Additionally, SMB, NFS with LDAP including Kerberos, and dual-protocol configurations require access to a Windows Active Directory domain. Active Directory connections must be [configured](#) on a per-region basis. Active Directory Domain controllers (DC) are identified by using [DNS-based DC discovery](#) using the specified DNS servers. Any of the DCs returned are used. The list of eligible DCs can be limited by specifying an Active Directory site.

Cloud Volumes Service reaches out with IP addresses from the CIDR range allocated with the `gcloud compute address` command while [on-boarding the Cloud Volumes Service](#). You can use this CIDR as source addresses to configure inbound firewalls to your Active Directory domain controllers.

Active Directory Domain Controllers must [expose ports to the Cloud Volumes Service CIDRs as mentioned here](#).

Next: [NAS protocols overview](#).

## NAS protocols

### NAS protocols overview

Previous: [Firewall](#).

NAS protocols include NFS (v3 and v4.1) and SMB/CIFS (2.x and 3.x). These protocols are how CVS allows shared access to data across multiple NAS clients. In addition, Cloud Volumes Service can provide access to NFS and SMB/CIFS clients simultaneously (dual-protocol) while honoring all of the identity and permission settings on files and folders in the NAS shares. To maintain the highest possible data transfer security, Cloud Volumes Service supports protocol encryption in flight using SMB encryption and NFS Kerberos 5p.



Dual-protocol is available with CVS-Performance only.

Next: [Basics of NAS protocols](#).

### Basics of NAS protocols

Previous: [NAS protocols overview](#).

NAS protocols are ways for multiple clients on a network to access the same data on a storage system, such as Cloud Volumes Service on GCP. NFS and SMB are the defined NAS protocols and operate on a client/server basis where Cloud Volumes Service acts as the server. Clients send access, read, and write

requests to the server, and the server is responsible for coordinating the locking mechanisms for files, storing permissions and handling identity and authentication requests.

For example, the following general process is followed if a NAS client wants to create a new file in a folder.

1. The client asks the server for information about the directory (permissions, owner, group, file ID, available space, and so on); the server responds with the information if the requesting client and user have the necessary permissions on the parent folder.
2. If the permissions on the directory allow access, the client then asks the server if the file name being created already exists in the file system. If the file name is already in use, creation fails. If the file name does not exist, the server lets the client know it can proceed.
3. The client issues a call to the server to create the file with the directory handle and file name and sets the access and modified times. The server issues a unique file ID to the file to make sure that no other files are created with the same file ID.
4. The client sends a call to check file attributes before the WRITE operation. If permissions allow it, the client then writes the new file. If locking is used by the protocol/application, the client asks the server for a lock to prevent other clients from accessing the file while locked to prevent data corruption.

[Next: NFS.](#)

## NFS

[Previous: Basics of NAS protocols \\_ overview.](#)

NFS is a distributed file system protocol that is an open IETF standard defined in Request for Comments (RFC) that allows anyone to implement the protocol.

Volumes in Cloud Volumes Service are shared out to NFS clients by exporting a path that is accessible to a client or set of clients. Permissions to mount these exports are defined by export policies and rules, which are configurable by Cloud Volumes Service administrators.

The NetApp NFS implementation is considered a gold standard for the protocol and is used in countless enterprise NAS environments. The following sections cover NFS and specific security features available in Cloud Volumes Service and how they are implemented.

## Default local UNIX users and groups

Cloud Volumes Service contains several default UNIX users and groups for various basic functionalities. These users and groups cannot currently be modified or deleted. New local users and groups cannot currently be added to Cloud Volumes Service. UNIX users and groups outside of the default users and groups need to be provided by an external LDAP name service.

The following table shows the default users and groups and their corresponding numeric IDs. NetApp recommends not creating new users or groups in LDAP or on the local clients that re-use these numeric IDs.

Default users: numeric IDs	Default groups: numeric IDs
<ul style="list-style-type: none"><li>• root:0</li><li>• pcuser:65534</li><li>• nobody:65535</li></ul>	<ul style="list-style-type: none"><li>• root:0</li><li>• daemon:1</li><li>• pcuser:65534</li><li>• nobody:65535</li></ul>



When using NFSv4.1, the root user might display as nobody when running directory listing commands on NFS clients. This is due to the client's ID domain mapping configuration. See the section called [NFSv4.1 and the nobody user/group](#) for details on this issue and how to resolve it.

## The root user

In Linux, the root account has access to all commands, files, and folders in a Linux-based file system. Because of the power of this account, security best practices often require the root user to be disabled or restricted in some fashion. In NFS exports, the power a root user has over the files and folders can be controlled in Cloud Volumes Service through export policies and rules and a concept known as root squash.

Root squashing ensures that the root user accessing an NFS mount is squashed to the anonymous numeric user 65534 (see the section “[The anonymous user](#)”) and is currently only available when using CVS-Performance by selecting Off for root access during export policy rule creation. If the root user is squashed to the anonymous user, it no longer has access to run chown or [setuid/setgid commands \(the sticky bit\)](#) on files or folders in the NFS mount, and files or folders created by the root user show the anon UID as the owner/group. In addition, NFSv4 ACLs cannot be modified by the root user. However, the root user still has access to chmod and deleted files that it does not have explicit permissions for. If you want to limit access to a root user’s file and folder permissions, consider using a volume with NTFS ACLs, creating a Windows user named `root`, and applying the desired permissions to the files or folders.

## The anonymous user

The anonymous (anon) user ID specifies a UNIX user ID or username that is mapped to client requests that arrive without valid NFS credentials. This can include the root user when root squashing is used. The anon user in Cloud Volumes Service is 65534.

This UID is normally associated with the username `nobody` or `nfsnobody` in Linux environments. Cloud Volumes Service also uses 65534 as the local UNIX user ‘pcuser’ (see the section “[Default local UNIX users and groups](#)”), which is also the default fallback user for Windows to UNIX name mappings when no valid matching UNIX user can be found in LDAP.

Because of the differences in usernames across Linux and Cloud Volumes Service for UID 65534, the name string for users mapped to 65534 might not match when using NFSv4.1. As a result, you might see `nobody` as the user on some files and folders. See the section “[NFSv4.1 and the nobody user/group](#)” for information about this issue and how to resolve it.

## Access control/exports

Initial export/share access for NFS mounts is controlled through host- based export policy rules contained within an export policy. A host IP, host name, subnet, netgroup, or domain is defined to allow access to mount the NFS share and the level of access allowed to the host. Export policy rule configuration options depend on the Cloud Volumes Service level.

For CVS-SW, the following options are available for export-policy configuration:

- **Client match.** Comma-separated list of IP addresses, comma-separated list of hostnames, subnets, netgroups, domain names.
- **RO/RW access rules.** Select read/write or read only to control level of access to export.CVS-Performance provides the following options:
- **Client match.** Comma-separated list of IP addresses, comma-separated list of hostnames, subnets, netgroups, domain names.

- **RO/RW access rules.** Select read/write or read only to control level of access to export.
- **Root access (on/off).** Configures root squash (see the section “[The root user](#)” for details).
- **Protocol type.** This limits access to the NFS mount to a specific protocol version. When specifying both NFSv3 and NFSv4.1 for the volume, either leave both blank or check both boxes.
- **Kerberos security level (when Enable Kerberos is selected).** Provides the options of krb5, krb5i, and/or krb5p for read-only or read-write access.

## Change ownership (chown) and change group (chgrp)

NFS on Cloud Volumes Service only allows the root user to run chown/chgrp on files and folders. Other users see an Operation not permitted error—even on files they own. If you use root squash (as covered in the section “[The root user](#)”), the root is squashed to a nonroot user and is not allowed access to chown and chgrp. There are currently no workarounds in Cloud Volumes Service to allow chown and chgrp for non-root users. If ownership changes are required, consider using dual protocol volumes and set the security style to NTFS to control permissions from the Windows side.

## Permission management

Cloud Volumes Service supports both mode bits (such as 644, 777, and so on for rwx) and NFSv4.1 ACLs to control permissions on NFS clients for volumes that use the UNIX security style. Standard permission management is used for these (such as chmod, chown, or nfs4\_setfacl) and work with any Linux client that supports them.

Additionally, when using dual protocol volumes set to NTFS, NFS clients can leverage Cloud Volumes Service name mapping to Windows users, which then are used to resolve the NTFS permissions. This requires an LDAP connection to Cloud Volumes Service to provide numeric-ID-to-username translations because Cloud Volumes Service requires a valid UNIX username to map properly to a Windows username.

## Providing granular ACLs for NFSv3

Mode bit permissions cover only owner, group, and everyone else in the semantics—meaning that there are no granular user access controls in place for basic NFSv3. Cloud Volumes Service does not support POSIX ACLs, nor extended attributes (such as chattr), so granular ACLs are only possible in the following scenarios with NFSv3:

- NTFS security style volumes (CIFS server required) with valid UNIX to Windows user mappings.
- NFSv4.1 ACLs applied using an admin client mounting NFSv4.1 to apply ACLs.

Both methods require an LDAP connection for UNIX identity management and a valid UNIX user and group information populated (see the section “[LDAP](#)”) and are only available with CVS-Performance instances. To use NTFS security style volumes with NFS, you must use dual-protocol (SMB and NFSv3) or dual-protocol (SMB and NFSv4.1), even if no SMB connections are made. To use NFSv4.1 ACLs with NFSv3 mounts, you must select Both (NFSv3/NFSv4.1) as the protocol type.

Regular UNIX mode bits don’t provide the same level of granularity in permissions that NTFS or NFSv4.x ACLs provide. The following table compares the permission granularity between NFSv3 mode bits and NFSv4.1 ACLs. For information about NFSv4.1 ACLs, see [nfs4\\_acl - NFSv4 Access Control Lists](#).

NFSv3 mode bits	NFSv4.1 ACLs
<ul style="list-style-type: none"> <li>• Set user ID on execution</li> <li>• Set group ID on execution</li> <li>• Save swapped text (not defined in POSIX)</li> <li>• Read permission for owner</li> <li>• Write permission for owner</li> <li>• Execute permission for owner on a file; or look up (search) permission for owner in directory</li> <li>• Read permission for group</li> <li>• Write permission for group</li> <li>• Execute permission for group on a file; or look up (search) permission for group in directory</li> <li>• Read permission for others</li> <li>• Write permission for others</li> <li>• Execute permission for others on a file; or look up (search) permission for others in directory</li> </ul>	<p>Access control entry (ACE) types (Allow/Deny/Audit)</p> <ul style="list-style-type: none"> <li>* Inheritance flags</li> <li>* directory-inherit</li> <li>* file-inherit</li> <li>* no-propagate-inherit</li> <li>* inherit-only</li> </ul> <p>Permissions</p> <ul style="list-style-type: none"> <li>* read-data (files) / list-directory (directories)</li> <li>* write-data (files) / create-file (directories)</li> <li>* append-data (files) / create-subdirectory (directories)</li> <li>* execute (files) / change-directory (directories)</li> <li>* delete</li> <li>* delete-child</li> <li>* read-attributes</li> <li>* write-attributes</li> <li>* read-named-attributes</li> <li>* write-named-attributes</li> <li>* read-ACL</li> <li>* write-ACL</li> <li>* write-owner</li> <li>* Synchronize</li> </ul>

Finally, NFS group membership (in both NFSv3 and NFSV4.x) is limited to a default maximum of 16 for AUTH\_SYS as per the RPC packet limits. NFS Kerberos provides up to 32 groups and NFSv4 ACLs remove the limitation by way of granular user and group ACLs (up to 1024 entries per ACE).

Additionally, Cloud Volumes Service provides extended group support to extend the maximum supported groups up to 32. This requires an LDAP connection to an LDAP server that contains valid UNIX user and group identities. For more information about configuring this, see [Creating and managing NFS volumes](#) in the Google documentation.

### NFSv3 user and group IDs

NFSv3 user and group IDs come across the wire as numeric IDs rather than names. Cloud Volumes Service does no username resolution for these numeric IDs with NFSv3, with UNIX security style volumes using just mode bits. When NFSv4.1 ACLs are present, a numeric ID lookup and/or name string lookup is needed to resolve the ACL properly—even when using NFSv3. With NTFS security style volumes, Cloud Volumes Service must resolve a numeric ID to a valid UNIX user and then map to a valid Windows user to negotiate access rights.

### Security limitations of NFSv3 user and group IDs

With NFSv3, the client and server never have to confirm that the user attempting a read or write with a numeric ID is a valid user; it is just implicitly trusted. This opens the file system up to potential breaches simply by spoofing any numeric ID. To prevent security holes like this, there are a few options available to Cloud Volumes Service.

- Implementing Kerberos for NFS forces users to authenticate with a username and password or keytab file to get a Kerberos ticket to allow access into a mount. Kerberos is available with CVS-Performance instances and only with NFSv4.1.

- Limiting the list of hosts in your export policy rules limits which NFSv3 clients have access to the Cloud Volumes Service volume.
- Using dual-protocol volumes and applying NTFS ACLs to the volume forces NFSv3 clients to resolve numeric IDs to valid UNIX usernames to authenticate properly to access mounts. This requires enabling LDAP and configuring UNIX user and group identities.
- Squashing the root user limits the damage a root user can do to an NFS mount but does not completely remove risk. For more information, see the section “[The root user](#).”

Ultimately, NFS security is limited to what the protocol version you are using offers. NFSv3, while more performant in general than NFSv4.1, does not provide the same level of security.

## NFSv4.1

NFSv4.1 provides greater security and reliability as compared to NFSv3, for the following reasons:

- Integrated locking through a lease-based mechanism
- Stateful sessions
- All NFS functionality over a single port (2049)
- TCP only
- ID domain mapping
- Kerberos integration (NFSv3 can use Kerberos, but only for NFS, not for ancillary protocols such as NLM)

## NFSv4.1 dependencies

Because of the additional security features in NFSv4.1, there are some external dependencies involved that were not needed to use NFSv3 (similar to how SMB requires dependencies such as Active Directory).

## NFSv4.1 ACLs

Cloud Volumes Service offers support for NFSv4.x ACLs, which deliver distinct advantages over normal POSIX-style permissions, such as the following:

- Granular control of user access to files and directories
- Better NFS security
- Improved interoperability with CIFS/SMB
- Removal of the NFS limitation of 16 groups per user with AUTH\_SYS security
- ACLs bypass the need for group ID (GID) resolution, which effectively removes the GID limitNFSv4.1 ACLs are controlled from NFS clients—not from Cloud Volumes Service. To use NFSv4.1 ACLs, be sure your client’s software version supports them and the proper NFS utilities are installed.

## Compatibility between NFSv4.1 ACLs and SMB clients

NFSv4 ACLs are different from Windows file-level ACLs (NTFS ACLs) but carry similar functionality. However, in multiprotocol NAS environments, if NFSv4.1 ACLs are present and you are using dual-protocol access (NFS and SMB on the same datasets), clients using SMB2.0 and later won’t be able to view or manage ACLs from Windows security tabs.

## How NFSv4.1 ACLs work

For reference, the following terms are defined:

- **Access control list (ACL).** A list of permissions entries.
- **Access control entry (ACE).** A permission entry in the list.

When a client sets an NFSv4.1 ACL on a file during a SETATTR operation, Cloud Volumes Service sets that ACL on the object, replacing any existing ACL. If there is no ACL on a file, then the mode permissions on the file are calculated from OWNER@, GROUP@, and EVERYONE@. If there are any existing SUID/Sgid/STICKY bits on the file, they are not affected.

When a client gets an NFSv4.1 ACL on a file during the course of a GETATTR operation, Cloud Volumes Service reads the NFSv4.1 ACL associated with the object, constructs a list of ACEs, and returns the list to the client. If the file has an NT ACL or mode bits, then an ACL is constructed from mode bits and is returned to the client.

Access is denied if a DENY ACE is present in the ACL; access is granted if an ALLOW ACE exists. However, access is also denied if neither of the ACEs is present in the ACL.

A security descriptor consists of a security ACL (SACL) and a discretionary ACL (DACL). When NFSv4.1 interoperates with CIFS/SMB, the DACL is one-to-one mapped with NFSv4 and CIFS. The DACL consists of the ALLOW and the DENY ACEs.

If a basic chmod is run on a file or folder with NFSv4.1 ACLs set, existing user and group ACLs are preserved, but the default OWNER@, GROUP@, EVERYONE@ ACLs are modified.

A client using NFSv4.1 ACLs can set and view ACLs for files and directories on the system. When a new file or subdirectory is created in a directory that has an ACL, that object inherits all ACEs in the ACL that have been tagged with the appropriate [inheritance flags](#).

If a file or directory has an NFSv4.1 ACL, that ACL is used to control access no matter which protocol is used to access the file or directory.

Files and directories inherit ACEs from NFSv4 ACLs on parent directories (possibly with appropriate modifications) as long as the ACEs have been tagged with the correct inheritance flags.

When a file or directory is created as the result of an NFSv4 request, the ACL on the resulting file or directory depends on whether the file creation request includes an ACL or only standard UNIX file access permissions. The ACL also depends on whether the parent directory has an ACL.

- If the request includes an ACL, that ACL is used.
- If the request includes only standard UNIX file access permissions and the parent directory does not have an ACL, the client file mode is used to set standard UNIX file access permissions.
- If the request includes only standard UNIX file access permissions and the parent directory has a noninheritable ACL, a default ACL based on the mode bits passed into the request is set on the new object.
- If the request includes only standard UNIX file access permissions but the parent directory has an ACL, the ACEs in the parent directory's ACL are inherited by the new file or directory as long as the ACEs have been tagged with the appropriate inheritance flags.

## ACE permissions

NFSv4.1 ACLs permissions uses a series of upper- and lower-case letter values (such as `rxtncy`) to control access. For more information about these letter values, see [HOW TO: Use NFSv4 ACL](#).

### NFSv4.1 ACL behavior with umask and ACL inheritance

NFSv4 ACLs provide the ability to offer ACL inheritance. ACL inheritance means that files or folders created beneath objects with NFSv4.1 ACLs set can inherit the ACLs based on the configuration of the [ACL inheritance flag](#).

[Umask](#) is used to control the permission level at which files and folders are created in a directory without administrator interaction. By default, Cloud Volumes Service allows umask to override inherited ACLs, which is expected behavior as per [RFC 5661](#).

### ACL formatting

NFSv4.1 ACLs have specific formatting. The following example is an ACE set on a file:

```
A:::ldapuser@domain.netapp.com:rwtTnNcCy
```

The preceding example follows the ACL format guidelines of:

```
type:flags:principal:permissions
```

A type of `A` means “allow.” The inherit flags are not set in this case, because the principal is not a group and does not include inheritance. Also, because the ACE is not an AUDIT entry, there is no need to set the audit flags. For more information about NFSv4.1 ACLs, see [http://linux.die.net/man/5/nfs4\\_acl](http://linux.die.net/man/5/nfs4_acl).

If the NFSv4.1 ACL is not set properly (or a name string cannot be resolved by the client and server), the ACL might not behave as expected, or the ACL change might fail to apply and throw an error.

Sample errors include:

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

### Explicit DENY

NFSv4.1 permissions can include explicit DENY attributes for OWNER, GROUP, and EVERYONE. That is because NFSv4.1 ACLs are default-deny, which means that if an ACL is not explicitly granted by an ACE, then it is denied. Explicit DENY attributes override any ACCESS ACEs, explicit or not.

DENY ACEs are set with an attribute tag of `D`.

In the example below, `GROUP@` is allowed all read and execute permissions, but denied all write access.

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

DENY ACEs should be avoided whenever possible because they can be confusing and complicated; ALLOW ACLs that are not explicitly defined are implicitly denied. When DENY ACEs are set, users might be denied access when they expect to be granted access.

The preceding set of ACEs is equivalent to 755 in mode bits, which means:

- The owner has full rights.
- Groups have read only.
- Others have read only.

However, even if permissions are adjusted to the 775 equivalent, access can be denied because of the explicit DENY set on EVERYONE.

## NFSv4.1 ID domain mapping dependencies

NFSv4.1 leverages ID domain mapping logic as a security layer to help verify that a user attempting access to an NFSv4.1 mount is indeed who they claim to be. In these cases, the username and group name coming from the NFSv4.1 client appends a name string and sends it to the Cloud Volumes Service instance. If that username/group name and ID string combination does not match, then the user and/or group is squashed to the default nobody user specified in the `/etc/idmapd.conf` file on the client.

This ID string is a requirement for proper permission adherence, especially when NFSv4.1 ACLs and/or Kerberos are in use. As a result, name service server dependencies such as LDAP servers are necessary to ensure consistency across clients and Cloud Volumes Service for proper user and group name identity resolution.

Cloud Volumes Service uses a static default ID domain name value of `defaultv4iddomain.com`. NFS clients default to the DNS domain name for its ID domain name settings, but you can manually adjust the ID domain name in `/etc/idmapd.conf`.

If LDAP is enabled in Cloud Volumes Service, then Cloud Volumes Service automates the NFS ID domain to change to what is configured for the search domain in DNS and clients won't need to be modified unless they use different DNS domain search names.

When Cloud Volumes Service can resolve a username or group name in local files or LDAP, the domain string is used and non-matching domain IDs squash to nobody. If Cloud Volumes Service cannot find a username or group name in local files or LDAP, the numeric ID value is used and the NFS client resolves the name properly (this is similar to NFSv3 behavior).

Without changing the client's NFSv4.1 ID domain to match what the Cloud Volumes Service volume is using, you see the following behavior:

- UNIX users and groups with local entries in Cloud Volumes Service (such as root, as defined in local UNIX users and groups) are squashed to the nobody value.
- UNIX users and groups with entries in LDAP (if Cloud Volumes Service is configured to use LDAP) squashes to nobody if DNS domains are different between NFS clients and Cloud Volumes Service.
- UNIX users and groups with no local entries or LDAP entries use the numeric ID value and resolve to the name specified on the NFS client. If no name exists on the client, only the numeric ID is shown.

The following shows the results of the preceding scenario:

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1 9835 9835     0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

When the client and server ID domains match, this is how the same file listing looks:

```
# ls -la
total 8
drwxr-xr-x 2 root   root      4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root      4096 Feb  3 12:06 ..
-rw-r--r-- 1 9835      9835     0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache   apache-group 0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root      0 Feb  3 12:06 root-user-file
```

For more information about this issue and how to resolve it, see the section “[NFSv4.1 and the nobody user/group](#).”

## Kerberos dependencies

If you plan to use Kerberos with NFS, you must have the following with Cloud Volumes Service:

- Active Directory domain for Kerberos Distribution Center services (KDC)
- Active Directory domain with user and group attributes populated with UNIX information for LDAP functionality (NFS Kerberos in Cloud Volumes Service requires a user SPN to UNIX user mapping for proper functionality.)
- LDAP enabled on the Cloud Volumes Service instance
- Active Directory domain for DNS services

## NFSv4.1 and the nobody user/group

One of the most common issues seen with an NFSv4.1 configuration is when a file or folder is shown in a listing using `ls` as being owned by the `user:group` combination of `nobody:nobody`.

For example:

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody 0 Apr 24 13:25 prof1-file
```

And the numeric ID is 99.

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99 0 Apr 24 13:25 prof1-file
```

In some instances, the file might show the correct owner but `nobody` as the group.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1 nobody 0 Oct 9 2019 newfile1
```

Who is `nobody`?

The `nobody` user in NFSv4.1 is different from the `nfsnobody` user. You can view how an NFS client sees each user by running the `id` command:

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

With NFSv4.1, the `nobody` user is the default user defined by the `idmapd.conf` file and can be defined as any user you want to use.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

Why does this happen?

Because security through name string mapping is a key tenet of NFSv4.1 operations, the default behavior when a name string does not match properly is to squash that user to one that won't normally have any access to files and folders owned by users and groups.

When you see `nobody` for the user and/or group in file listings, this generally means something in NFSv4.1 is misconfigured. Case sensitivity can come into play here.

For example, if `user1@CVSDEMO.LOCAL` (uid 1234, gid 1234) is accessing an export, then Cloud Volumes Service must be able to find `user1@CVSDEMO.LOCAL` (uid 1234, gid 1234). If the user in Cloud Volumes Service is `USER1@CVSDEMO.LOCAL`, then it won't match (uppercase USER1 versus lowercase user1). In

many cases, you can see the following in the messages file on the client:

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name  
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'  
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does  
not map into domain 'CVSDEMO.LOCAL'
```

The client and server must both agree that a user is indeed who they are claiming to be, so you must check the following to ensure that the user that the client sees has the same information as the user that Cloud Volumes Service sees.

- **NFSv4.x ID domain.** Client: `idmapd.conf` file; Cloud Volumes Service uses `defaultv4iddomain.com` and cannot be changed manually. If using LDAP with NFSv4.1, Cloud Volumes Service changes the ID domain to what the DNS search domain is using, which is the same as the AD domain.
- **User name and numeric IDs.** This determines where the client is looking for user names and leverages the name service switch configuration—client: `nsswitch.conf` and/or local `passwd` and `group` files; Cloud Volumes Service does not allow modifications to this but automatically adds LDAP to the configuration when it is enabled.
- **Group name and numeric IDs.** This determines where the client is looking for group names and leverages the name service switch configuration—client: `nsswitch.conf` and/or local `passwd` and `group` files; Cloud Volumes Service does not allow modifications to this but automatically adds LDAP to the configuration when it is enabled.

In almost all cases, if you see `nobody` in user and group listings from clients, the issue is user or group name domain ID translation between Cloud Volumes Service and the NFS client. To avoid this scenario, use LDAP to resolve user and group information between clients and Cloud Volumes Service.

### Viewing name ID strings for NFSv4.1 on clients

If you are using NFSv4.1, there is a name-string mapping that takes place during NFS operations, as previously described.

In addition to using `/var/log/messages` to find an issue with NFSv4 IDs, you can use the `nfsidmap -l` command on the NFS client to view which usernames have properly mapped to the NFSv4 domain.

For example, this is output of the command after a user that can be found by the client and Cloud Volumes Service accesses an NFSv4.x mount:

```
# nfsidmap -l  
4 .id_resolver keys found:  
  gid:daemon@CVSDEMO.LOCAL  
  uid:nfs4@CVSDEMO.LOCAL  
  gid:root@CVSDEMO.LOCAL  
  uid:root@CVSDEMO.LOCAL
```

When a user that does not map properly into the NFSv4.1 ID domain (in this case, `netapp-user`) tries to access the same mount and touches a file, they are assigned `nobody:nobody`, as expected.

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx 5 root root 4096 Jan 14 17:13 .
drwxr-xr-x 8 root root 81 Jan 14 10:02 ..
-rw-r--r-- 1 nobody nobody 0 Jan 14 17:13 newfile
drwxrwxrwx 2 root root 4096 Jan 13 13:20 qtree1
drwxrwxrwx 2 root root 4096 Jan 13 13:13 qtree2
drwxr-xr-x 2 nfs4 daemon 4096 Jan 11 14:30 testdir
```

The `nfsidmap -l` output shows the user `pcuser` in the display but not `netapp-user`; this is the anonymous user in our export-policy rule (65534).

```
# nfsidmap -l
6 .id_resolver keys found:
gid:pcuser@CVSDEMO.LOCAL
uid:pcuser@CVSDEMO.LOCAL
gid:daemon@CVSDEMO.LOCAL
uid:nfs4@CVSDEMO.LOCAL
gid:root@CVSDEMO.LOCAL
uid:root@CVSDEMO.LOCAL
```

[Next: SMB.](#)

## SMB

[Previous: NFS.](#)

**SMB** is a network file sharing protocol developed by Microsoft that provides centralized user/group authentication, permissions, locking, and file sharing to multiple SMB clients over an Ethernet network. Files and folders are presented to clients by way of shares, which can be configured with a variety of share properties and offers access control through share-level permissions. SMB can be presented to any client that offers support for the protocol, including Windows, Apple, and Linux clients.

Cloud Volumes Service provides support for the SMB 2.1 and 3.x versions of the protocol.

## Access control/SMB shares

- When a Windows username requests access to the Cloud Volumes Service volume, Cloud Volumes Service looks for a UNIX username using the methods configured by Cloud Volumes Service administrators.
- If an external UNIX identity provider (LDAP) is configured and Windows/UNIX usernames are identical, then Windows usernames will map 1:1 to UNIX usernames without any additional configuration needed.

When LDAP is enabled, Active Directory is used to host those UNIX attributes for user and group objects.

- If Windows names and UNIX names do not match identically, then LDAP must be configured to allow Cloud Volumes Service to use the LDAP name mapping configuration (see the section “[Using LDAP for asymmetric name mapping](#)”).
- If LDAP is not in use, then Windows SMB users map to a default local UNIX user named `pcuser` in Cloud Volumes Service. This means files written in Windows by users that map to the `pcuser` show UNIX ownership as `pcuser` in multiprotocol NAS environments. `pcuser` here is effectively the `nobody` user in Linux environments (UID 65534).

In deployments with SMB only, the `pcuser` mapping still occurs, but it won’t matter, because Windows user and group ownership is correctly displayed and NFS access to the SMB-only volume is not allowed. In addition, SMB-only volumes do not support conversion to NFS or dual-protocol volumes after they are created.

Windows leverages Kerberos for username authentication with the Active Directory domain controllers, which requires a username/password exchange with the AD DCs, which is external to the Cloud Volumes Service instance. Kerberos authentication is used when the `\\\$ERVERNAME` UNC path is used by the SMB clients and the following is true:

- DNS A/AAAA entry exists for SERVERNAME
- A valid SPN for SMB/CIFS access exists for SERVERNAME

When a Cloud Volumes Service SMB volume is created, the machine account name is created as defined in the section “[How Cloud Volumes Service shows up in Active Directory](#).” That machine account name also becomes the SMB share access path because Cloud Volumes Service leverages Dynamic DNS (DDNS) to create the necessary A/AAAA and PTR entries in DNS and the necessary SPN entries on the machine account principal.



For PTR entries to be created, the reverse lookup zone for the Cloud Volumes Service instance IP address must exist on the DNS server.

For example, this Cloud Volumes Service volume uses the following UNC share path: `\\\cvs-east-433d.cvsdemo.local`.

In Active Directory, these are the Cloud Volumes Service-generated SPN entries:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
HOST/cvs-east-433d.cvsdemo.local
HOST/CSV-EAST-433D
```

This is the DNS forward/reverse lookup result:

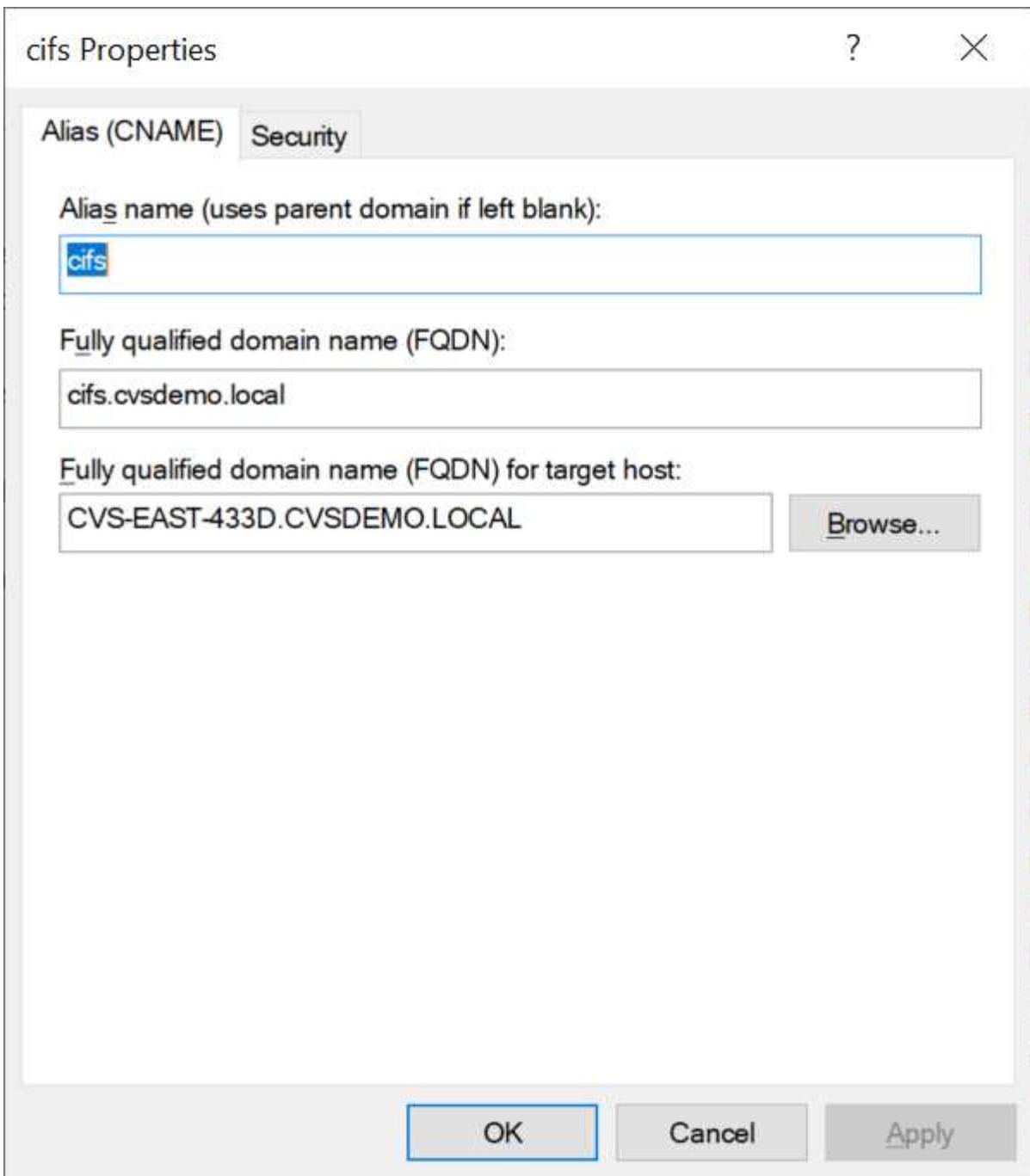
```
PS C:\> nslookup CVS-EAST-433D
Server: activedirectory. region. lab. internal
Address: 10. xx.0. xx
Name: CVS-EAST-433D.cvsdemo.local
Address: 10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server: activedirectory.region.lab.internal
Address: 10.xx.0.xx
Name: CVS-EAST-433D.CVSDEMO.LOCAL
Address: 10. xxx.0. x
```

Optionally, more access control can be applied by enabling/requiring SMB encryption for SMB shares in Cloud Volumes Service. If SMB encryption isn't supported by one of the endpoints, then access is not allowed.

### Using SMB name aliases

In some cases, it might be a security concern for end users to know the machine account name in use for Cloud Volumes Service. In other cases, you might simply want to provide a simpler access path to your end users. In those cases, you can create SMB aliases.

If you want to create aliases for the SMB share path, you can leverage what is known as a CNAME record in DNS. For example, if you want to use the name \\CIFS to access shares instead of \\cvs-east-433d.cvsdemo.local, but you still want to use Kerberos authentication, a CNAME in DNS that points to the existing A/AAAA record and an additional SPN added to the existing machine account provides Kerberos access.



This is the resulting DNS forward lookup result after adding a CNAME:

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address: 10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address: 10. xxx.0. x
Aliases: cifs.cvsdemo.local
```

This is the resulting SPN query after adding new SPNs:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
  cifs/cifs.cvsdemo.local
  cifs/cifs
  HOST/cvs-east-433d.cvsdemo.local
  HOST/CVS-EAST-433D
```

In a packet capture, we can see the Session Setup Request using the SPN tied to the CNAME.

431 4.156722	SMB2	308 Negotiate Protocol Response
432 4.156785	SMB2	232 Negotiate Protocol Request
434 4.158108	SMB2	374 Negotiate Protocol Response
435 4.160977	SMB2	1978 Session Setup Request
437 4.166224	SMB2	322 Session Setup Response
438 4.166891	SMB2	152 Tree Connect Request Tree: \\cifs\IPC\$
439 4.168063	SMB2	138 Tree Connect Response

realm: CVSDEMO.LOCAL
▼ sname
name-type: kRB5-NT-SRV-INST (2)
▼ sname-string: 2 items
SNameString: cifs
SNameString: cifs
▼ enc-part
etype: eTYPE-ARCFOUR-HMAC-MD5 (23)

## SMB authentication dialects

Cloud Volumes Service supports the following [dialects](#) for SMB authentication:

- LM
- NTLM
- NTLMv2
- Kerberos

Kerberos authentication for SMB share access is the most secure level of authentication you can use. With AES and SMB encryption enabled, the security level is further increased.

Cloud Volumes Service also supports backward compatibility for LM and NTLM authentication. When Kerberos is misconfigured (such as when creating SMB aliases), share access falls back to weaker authentication methods (such as NTLMv2). Because these mechanisms are less secure, they are disabled in some Active Directory environments. If weaker authentication methods are disabled and Kerberos is not configured properly, share access fails because there is no valid authentication method to fall back to.

For information about configuring/viewing your supported authentication levels in Active Directory, see [Network security: LAN Manager authentication level](#).

## Permission models

### NTFS/File permissions

NTFS permissions are the permissions applied to files and folders in file systems adhering to NTFS logic. You can apply NTFS permissions in Basic or Advanced and can be set to Allow or Deny for access control.

Basic permissions include the following:

- Full Control
- Modify
- Read & Execute
- Read
- Write

When you set permissions for a user or group, referred to as an ACE, it resides in an ACL. NTFS permissions use the same read/write/execute basics as UNIX mode bits, but they can also extend to more granular and extended access controls (also known as Special Permissions), such as Take Ownership, Create Folders/Append Data, Write Attributes, and more.

Standard UNIX mode bits do not provide the same level of granularity as NTFS permissions (such as being able to set permissions for individual user and group objects in an ACL or setting extended attributes). However, NFSv4.1 ACLs do provide the same functionality as NTFS ACLs.

NTFS permissions are more specific than share permissions and can be used in conjunction with share permissions. With NTFS permission structures, the most restrictive applies. As such, explicit denials to a user or group overrides even Full Control when defining access rights.

NTFS permissions are controlled from Windows SMB clients.

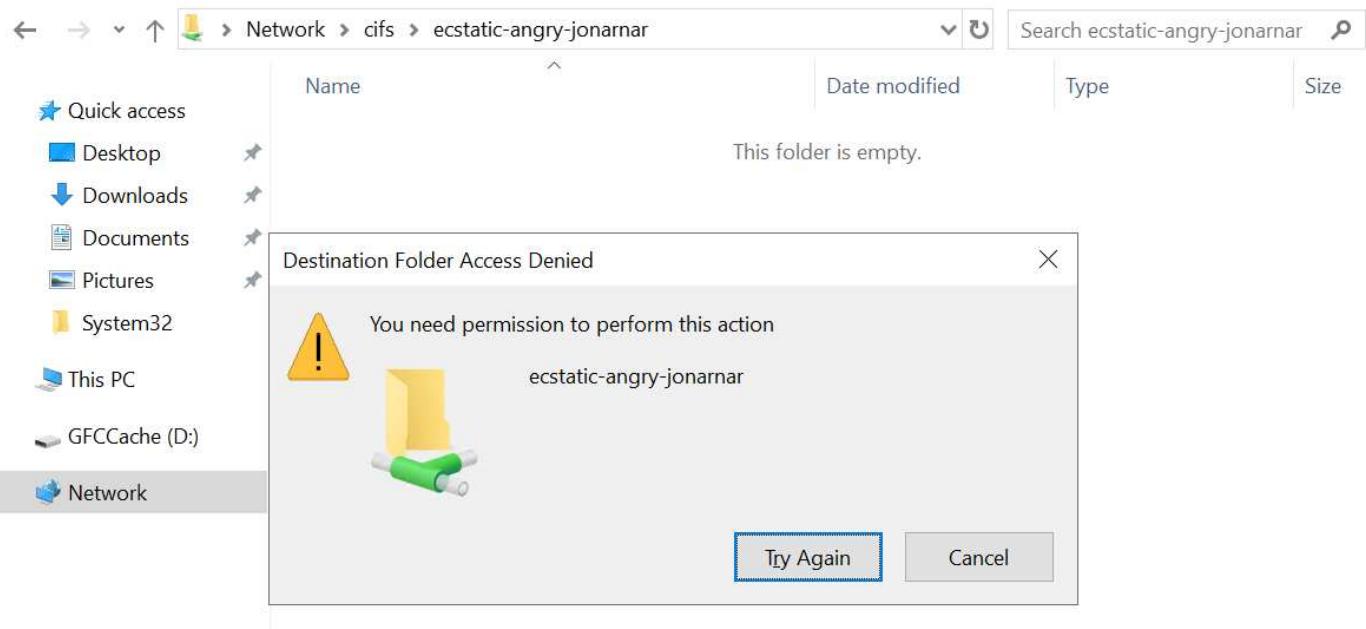
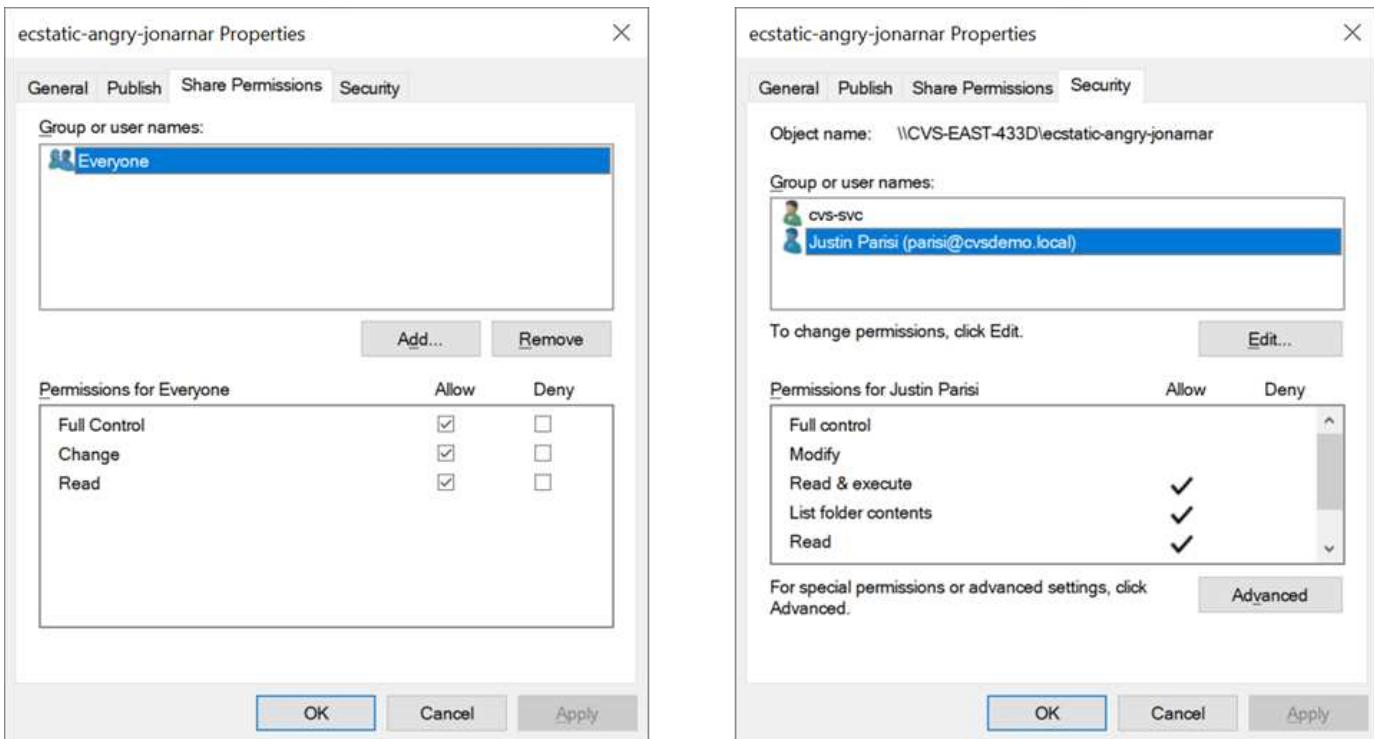
## Share permissions

Share permissions are more general than NTFS permissions (Read/Change/Full Control only) and control the initial entry into an SMB share—similar to how NFS export policy rules work.

Although NFS export policy rules control access through host-based information such as IP addresses or host names, SMB share permissions can control access by using user and group ACEs in a share ACL. You can set share ACLs either from the Windows client or from the Cloud Volumes Service management UI.

By default, share ACLs and initial volume ACLs include Everyone with Full Control. The file ACLs should be changed but share permissions are overruled by the file permissions on objects in the share.

For instance, if a user is only allowed Read access to the Cloud Volumes Service volume file ACL, they are denied access to create files and folders even though the share ACL is set to Everyone with Full Control, as shown in the following figure.



For best security results, do the following:

- Remove Everyone from the share and file ACLs and instead set share access for users or groups.
- Use groups for access control instead of individual users for ease of management and faster removal/addition of users to share ACLs through group management.
- Allow less restrictive, more general share access to the ACEs on the share permissions and lock down access to users and groups with file permissions for more granular access control.
- Avoid general use of explicit deny ACLs, because they override allow ACLs. Limit use of explicit deny ACLs for users or groups that need to be restricted from access to a file system quickly.
- Make sure that you pay attention to the [ACL inheritance](#) settings when modifying permissions; setting the inheritance flag at the top level of a directory or volume with high file counts means that each file below that

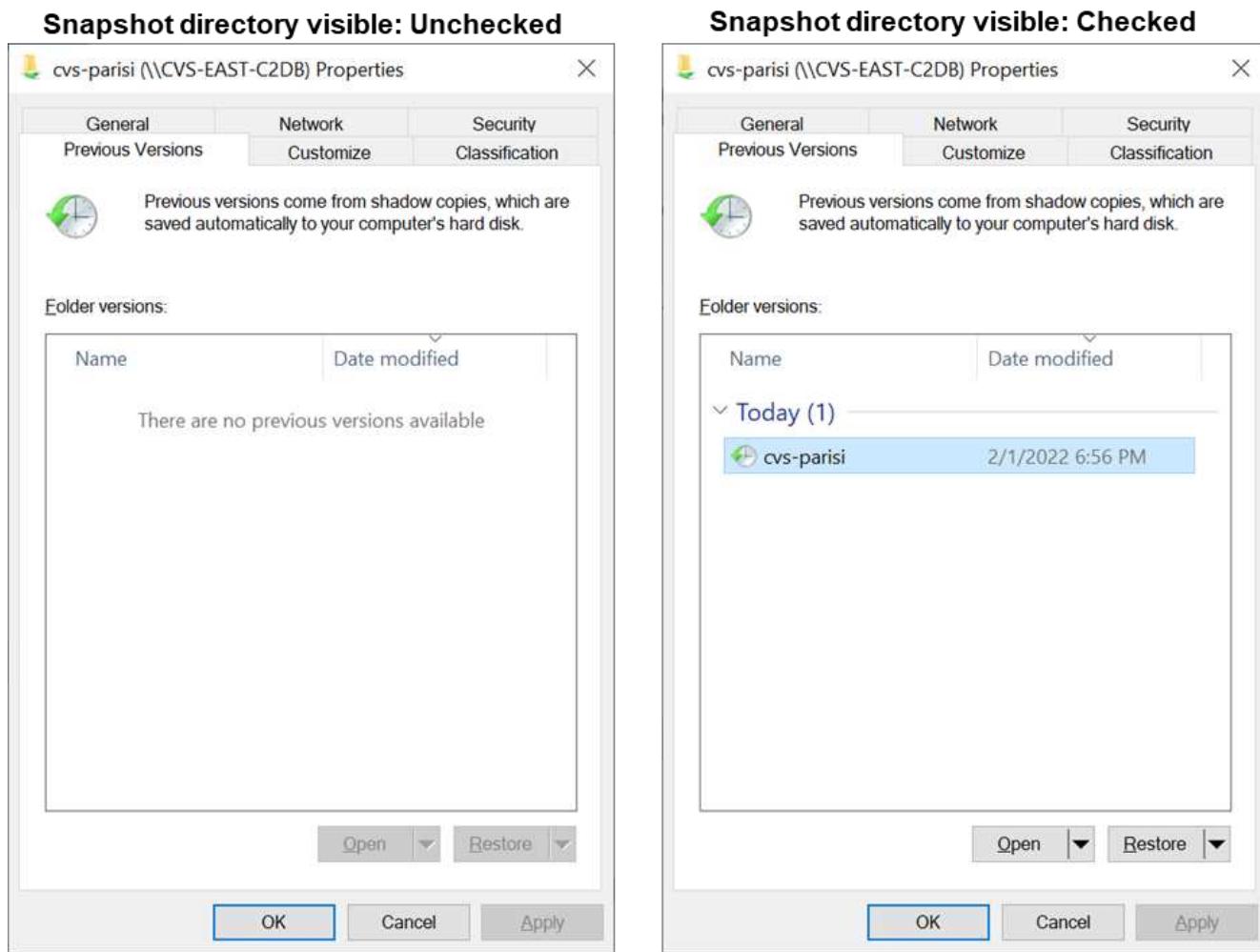
directory or volume has inherited permissions added to it, which can create unwanted behavior such as unintended access/denial and long churn of permission modification as each file is adjusted.

## SMB share security features

When you first create a volume with SMB access in Cloud Volumes Service, you are presented with a series of choices for securing that volume.

Some of these choices depend on the Cloud Volumes Service level (Performance or Software) and choices include:

- **Make snapshot directory visible (available for both CVS-Performance and CVS-SW).** This option controls whether or not SMB clients can access the Snapshot directory in an SMB share (\server\share\~snapshot and/or Previous Versions tab). The default setting is Not Checked, which means that the volume defaults to hiding and disallowing access to the ~snapshot directory, and no Snapshot copies appear in the Previous Versions tab for the volume.



Hiding Snapshot copies from end users might be desired for security reasons, performance reasons (hiding these folders from AV scans) or preference. Cloud Volumes Service Snapshots are read-only, so even if these Snapshots are visible, end users cannot delete or modify files in the Snapshot directory. File permissions on the files or folders at the time the Snapshot copy was taken apply. If a file or folder's permissions change between Snapshot copies, then the changes also apply to the files or folders in the Snapshot directory. Users and groups can gain access to these files or folders based on permissions. While deletes or modifications of files in the Snapshot directory are not possible, it is possible to copy files or folders out of the Snapshot

directory.

- **Enable SMB encryption (available for both CVS-Performance and CVS-SW).** SMB encryption is disabled on the SMB share by default (unchecked). Checking the box enables SMB encryption, which means traffic between the SMB client and server is encrypted in-flight with the highest supported encryption levels negotiated. Cloud Volumes Service supports up to AES-256 encryption for SMB. Enabling SMB encryption does carry a performance penalty that might or might not be noticeable to your SMB clients—roughly in the 10-20% range. NetApp strongly encourages testing to see if that performance penalty is acceptable.
- **Hide SMB share (available for both CVS-Performance and CVS-SW).** Setting this option hides the SMB share path from normal browsing. This means that clients that do not know the share path cannot see the shares when accessing the default UNC path (such as \\CVS-SMB). When the checkbox is selected, only clients that explicitly know the SMB share path or have the share path defined by a Group Policy Object can access it (security through obfuscation).
- **Enable access-based enumeration (ABE) (CVS-SW only).** This is similar to hiding the SMB share, except the shares or files are only hidden from users or groups that do not have permissions to access the objects. For instance, if Windows user joe is not allowed at least Read access through the permissions, then the Windows user joe cannot see the SMB share or files at all. This is disabled by default, and you can enable it by selecting the checkbox. For more information on ABE, see the NetApp Knowledge Base article [How does Access Based Enumeration \(ABE\) work?](#)
- **Enable Continuously Available (CA) share support (CVS-Performance only).** [Continuously Available SMB shares](#) provide a way to minimize application disruptions during failover events by replicating lock states across nodes in the Cloud Volumes Service backend system. This is not a security feature, but it does offer better overall resiliency. Currently, only SQL Server and FSLogix applications are supported for this functionality.

## Default hidden shares

When an SMB server is created in Cloud Volumes Service, there are [hidden administrative shares](#) (using the \$ naming convention) that are created in addition to the data volume SMB share. These include C\$ (namespace access) and IPC\$ (sharing named pipes for communication between programs, such as the remote procedure calls (RPC) used for Microsoft Management Console (MMC) access).

The IPC\$ share contains no share ACLs and cannot be modified—it is strictly used for RPC calls and [Windows disallows anonymous access to these shares by default](#).

The C\$ share allows BUILTIN/Administrators access by default, but Cloud Volumes Service automation removes the share ACL and does not allow access to anyone because access to the C\$ share allows visibility into all mounted volumes in the Cloud Volumes Service file systems. As a result, attempts to navigate to \\SERVER\C\$ fail.

## Accounts with local/BUILTIN administrator/backup rights

Cloud Volumes Service SMB servers maintain similar functionality to regular Windows SMB servers in that there are local groups (such as BUILTIN\Administrators) that apply access rights to select domain users and groups.

When you specify a user to be added to Backup Users, the user is added to the BUILTIN\Backup Operators group in the Cloud Volumes Service instance that uses that Active Directory connection, which then gets the [SeBackupPrivilege](#) and [SeRestorePrivilege](#).

When you add a user to Security Privilege Users, the user is given the SeSecurityPrivilege, which is useful in some application use cases, such as [SQL Server on SMB shares](#).

## Backup Users

Provide a comma separated list of domain users or a domain group name that require elevated privileges to access volumes created by Cloud Volumes Service.

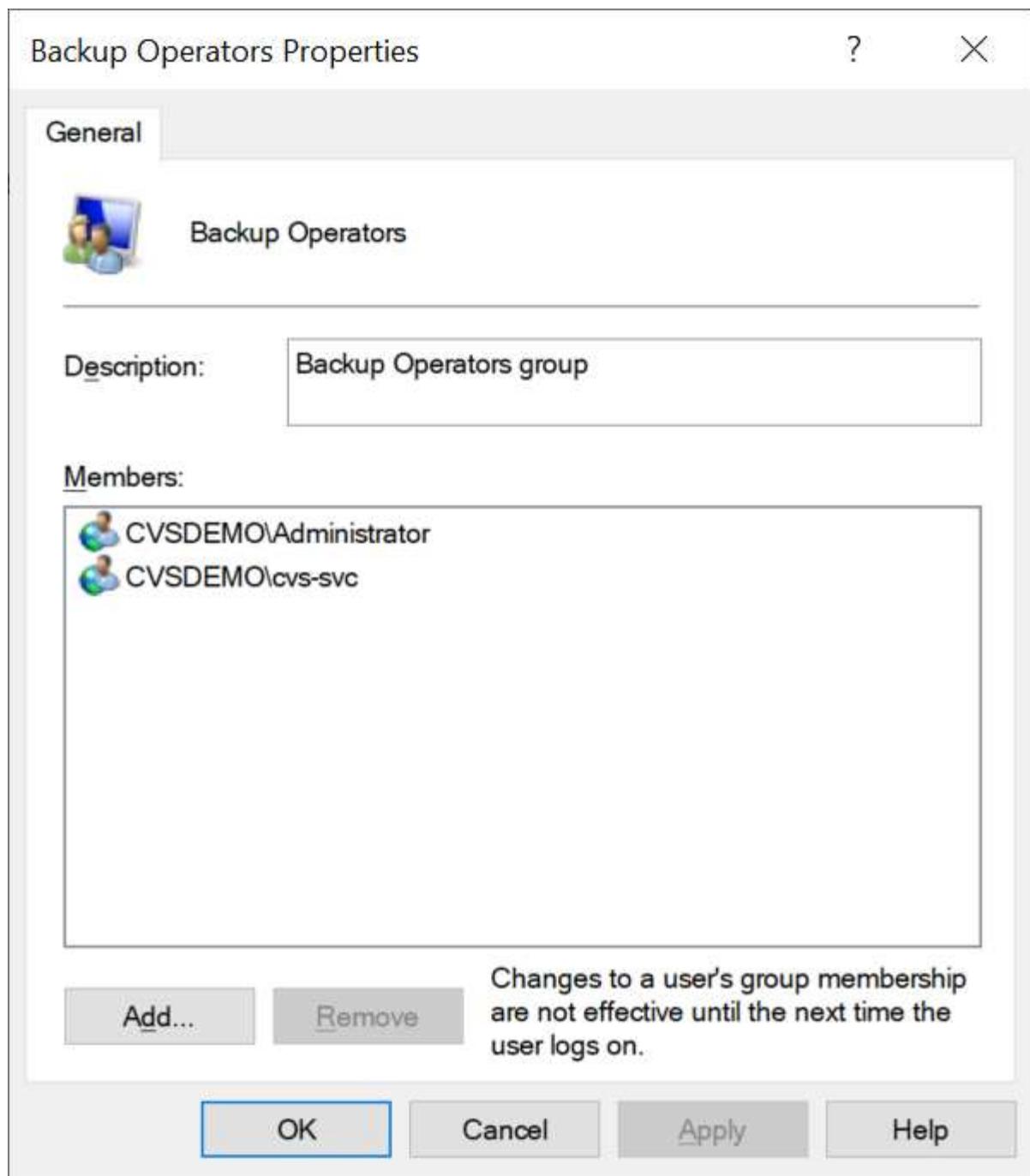
Accountnames —  
administrator,cvs-svc

## Security Privilege Users

Provide a list of comma separated domain user accounts that require elevated privileges to manage security log for the Active Directory associated with Cloud Volumes Service.

Accountnames —  
administrator,cvs-svc

You can view Cloud Volumes Service local group memberships through the MMC with the proper privileges. The following figure shows users that have been added by using the Cloud Volumes Service console.



The following table shows the list of default BUILTIN groups and what users/groups are added by default.

Local/BUILTIN group	Default members
BUILTIN\Administrators*	DOMAIN\Domain Admins
BUILTIN\Backup Operators*	None
BUILTIN\Guests	DOMAIN\Domain Guests
BUILTIN\Power Users	None
BUILTIN\Domain Users	DOMAIN\Domain Users

\*Group membership controlled in Cloud Volumes Service Active Directory connection configuration.

You can view local users and groups (and group memberships) in the MMC window, but you cannot add or delete objects or change group memberships from this console. By default, only the Domain Admins group and Administrator are added to the BUILTIN\Administrators group in Cloud Volumes Service. Currently, you cannot modify this.

Computer Management (CVS-EAST-C2DB)	Name	Full Name	Description
System Tools Task Scheduler Event Viewer Shared Folders Shares Sessions Open Files Local Users and Groups Users Groups	Administrator		Built-in administrator account

Computer Management (CVS-EAST-C2DB)	Name	Description
System Tools Task Scheduler Event Viewer Shared Folders Shares Sessions Open Files Local Users and Groups Users Groups	Administrators	Built-in Administrators group
	Users	All users
	Guests	Built-in Guests Group
	Power Users	Restricted administrative privileges
	Backup Operators	Backup Operators group

Administrators Properties

General

Administrators

Description: Built-in Administrators group

Members:

Administrator  
CVSDEMO\Domain Admins

Add... Remove

Changes to a user's group membership are not effective until the next time the user logs on.

OK Cancel Apply Help

## MMC/Computer Management access

SMB access in Cloud Volumes Service provides connectivity to the Computer Management MMC, which allows you to view shares, manage share ACLs, and view/manage SMB sessions and open files.

To use the MMC to view SMB shares and sessions in Cloud Volumes Service, the user logged in currently must be a domain administrator. Other users are allowed access to view or manage the SMB server from MMC and receive a You Do Not Have Permissions dialog box when attempting to view shares or sessions on the Cloud Volumes Service SMB instance.

To connect to the SMB server, open Computer Management, right click Computer Management and then select Connect To Another Computer. This opens the Select Computer dialog box where you can enter the SMB server name (found in the Cloud Volumes Service volume information).

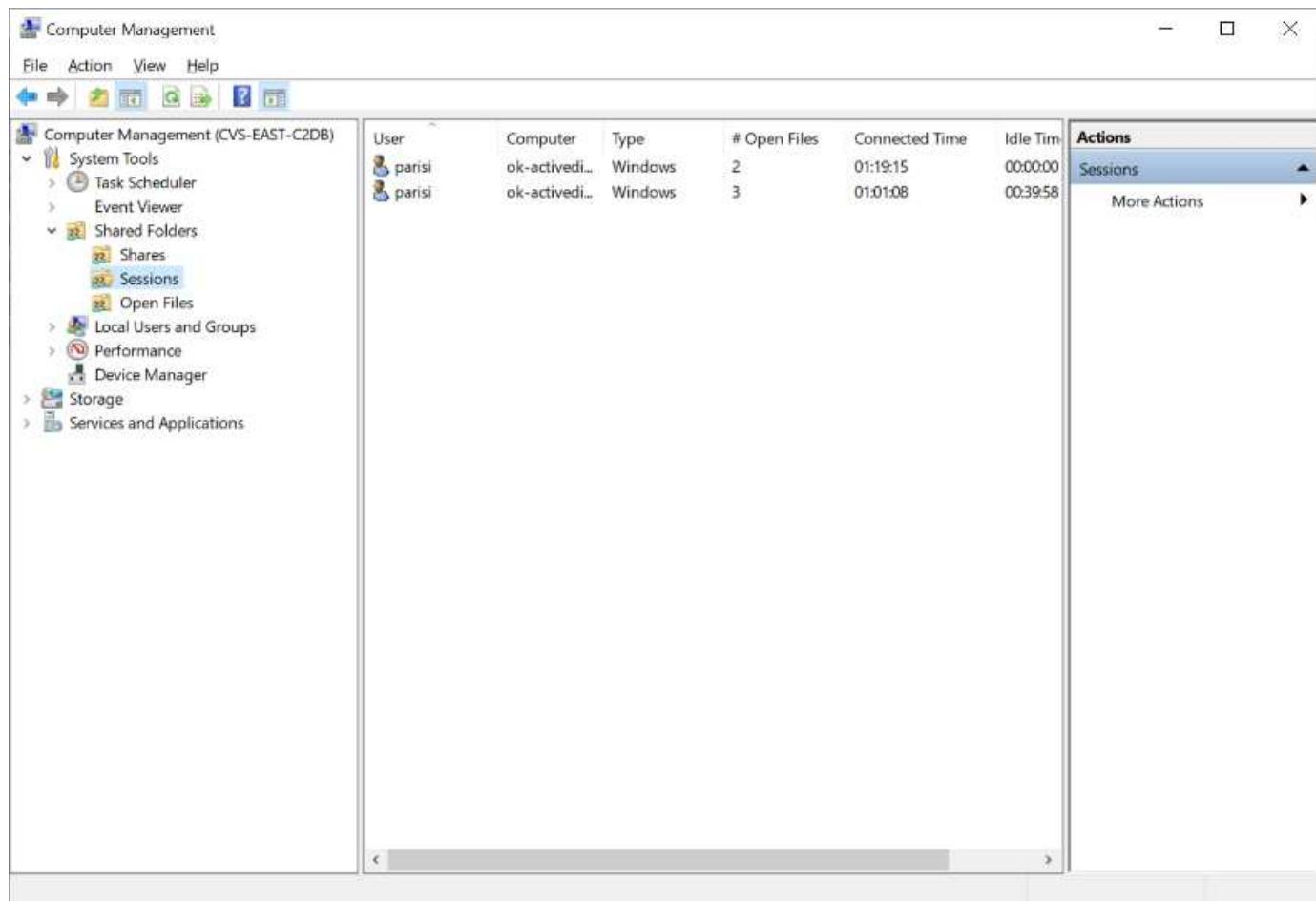
When you view SMB shares with the proper permissions, you see all available shares in the Cloud Volumes Service instance that share the Active Directory connection. To control this behavior, set the Hide SMB Shares option on the Cloud Volumes Service volume instance.

Remember, only one Active Directory connection is allowed per region.

The screenshot shows the Windows Computer Management console window. The left pane displays a tree view of management tools, with 'Shared Folders' expanded to show 'Shares'. The right pane is a table listing SMB shares:

Share Name	Folder Path	Type	# Client Connections	Description
c\$	C:\	Windows	0	
cvs-parisi	C\cvs-parisi	Windows	1	
dgeyer-sm...	C\dgeyer-smb-test	Windows	0	
ipc\$		Windows	2	

The 'Shares' item in the Actions column is highlighted. A 'More Actions' button is visible at the bottom of the Actions column.



The following table shows a list of supported/unsupported functionality for the MMC.

Supported functions	Unsupported functions
<ul style="list-style-type: none"> <li>View shares</li> <li>View active SMB sessions</li> <li>View open files</li> <li>View local users and groups</li> <li>View local group memberships</li> <li>Enumerate the list of sessions, files, and tree connections in the system</li> <li>Close open files in the system</li> <li>Close open sessions</li> <li>Create/manage shares</li> </ul>	<ul style="list-style-type: none"> <li>Creating new local users/groups</li> <li>Managing/viewing existing local user/groups</li> <li>View events or performance logs</li> <li>Managing storage</li> <li>Managing services and applications</li> </ul>

## SMB server security information

The SMB server in Cloud Volumes Service uses a series of options that define security policies for SMB connections, including things such as Kerberos clock skew, ticket age, encryption, and more.

The following table contains a list of those options, what they do, the default configurations, and if they can be modified with Cloud Volumes Service. Some options do not apply to Cloud Volumes Service.

Security option	What it does	Default value	Can change?
Maximum Kerberos Clock Skew (minutes)	Maximum time skew between Cloud Volumes Service and domain controllers. If the time skew exceeds 5 minutes, Kerberos authentication fails. This is set to the Active Directory default value.	5	No
Kerberos Ticket Lifetime (hours)	Maximum time a Kerberos ticket remains valid before requiring a renewal. If no renewal occurs before the 10 hours, you must obtain a new ticket. Cloud Volumes Service performs these renewals automatically. 10 hours is the Active Directory default value.	10	No
Maximum Kerberos Ticket Renewal (days)	Maximum number of days that a Kerberos ticket can be renewed before a new authorization request is needed. Cloud Volumes Service automatically renews tickets for SMB connections. Seven days is the Active Directory default value.	7	No
Kerberos KDC Connection Timeout (secs)	The number of seconds before a KDC connection times out.	3	No
Require Signing for Incoming SMB Traffic	Setting to require signing for SMB traffic. If set to true, clients that do not support signing fail connectivity.	False	
Require Password Complexity for Local User Accounts	Used for passwords on local SMB users. Cloud Volumes Service does not support local user creation, so this option does not apply to Cloud Volumes Service.	True	No

Security option	What it does	Default value	Can change?
Use start_tls for Active Directory LDAP Connections	Used to enable start TLS connections for Active Directory LDAP. Cloud Volumes Service does not currently support enabling this.	False	No
Is AES-128 and AES-256 Encryption for Kerberos Enabled	This controls whether AES encryption is used for Active Directory connections and is controlled with the Enable AES Encryption for Active Directory Authentication option when creating/modifying the Active Directory connection.	False	Yes
LM Compatibility Level	Level of supported authentication dialects for Active Directory connections. See the section “ <a href="#">SMB authentication dialects</a> ” for more information.	ntlmv2-krb	No
Require SMB Encryption for Incoming CIFS Traffic	Requires SMB encryption for all shares. This is not used by Cloud Volumes Service; instead, set encryption on a per-volume basis (see the section “ <a href="#">SMB share security features</a> ”).	False	No
Client Session Security	Sets signing and/or sealing for LDAP communication. This is not currently set in Cloud Volumes Service but might be needed in future releases to address . Remediation for LDAP authentication issues due to the Windows patch is covered in the section “ <a href="#">LDAP channel binding</a> .”.	None	No
SMB2 enable for DC connections	Uses SMB2 for DC connections. Enabled by default.	System-default	No

Security option	What it does	Default value	Can change?
LDAP Referral Chasing	When using multiple LDAP servers, referral chasing allows the client to refer to other LDAP servers in the list when an entry is not found in the first server. This is currently not supported by Cloud Volumes Service.	False	No
Use LDAPS for Secure Active Directory Connections	Enables the use of LDAP over SSL. Currently not supported by Cloud Volumes Service.	False	No
Encryption is required for DC Connection	Requires encryption for successful DC connections. Disabled by default in Cloud Volumes Service.	False	No

[Next: Dual-protocol/multiprotocol.](#)

[Dual-protocol/multiprotocol](#)

[Previous: SMB.](#)

Cloud Volumes Service offers the ability to share the same datasets to both SMB and NFS clients while maintaining proper access permissions ([dual-protocol](#)). This is done by coordinating identity mapping between protocols and using a centralized backend LDAP server to provide the UNIX identities to Cloud Volumes Service. You can use Windows Active Directory to provide both Windows and UNIX users for ease of use.

## Access control

- **Share access controls.** Determine which clients and/or user and groups can access a NAS share. For NFS, export policies and rules control client access to exports. NFS exports are managed from the Cloud Volumes Service instance. SMB makes use of CIFS/SMB shares and share ACLs to provide more granular control at the user and group level. You can only configure share-level ACLs from SMB clients by using [MMC/Computer Management](#) with an account that has administrator rights on the Cloud Volumes Service instance (see the section “[Accounts with local/BUILTIN administrator/backup rights.](#)”).
- **File access controls.** Control permissions at a file or folder level and are always managed from the NAS client. NFS clients can make use of traditional mode bits (rwx) or NFSv4 ACLs. SMB clients leverage NTFS permissions.

The access control for volumes that serve data to both NFS and SMB depends on the protocol in use. For information on permissions with dual protocol, see the section “[Permission model](#).”

## User mapping

When a client accesses a volume, Cloud Volumes Service attempts to map the incoming user to a valid user in the opposite direction. This is necessary for proper access to be determined across protocols and to ensure that the user requesting access is indeed who they claim to be.

For example, if a Windows user named `joe` attempts access to a volume with UNIX permissions through SMB, then Cloud Volumes Service performs a search to find a corresponding UNIX user named `joe`. If one exists, then files that are written to an SMB share as Windows user `joe` appears as UNIX user `joe` from NFS clients.

Alternately, if a UNIX user named `joe` attempts access to a Cloud Volumes Service volume with Windows permissions, then the UNIX user must be able to map to a valid Windows user. Otherwise, access to the volume is denied.

Currently, only Active Directory is supported for external UNIX identity management with LDAP. For more information about configuring access to this service, see [Creating an AD connection](#).

## Permission model

When using dual-protocol setups, Cloud Volumes Service makes use of security styles for volumes to determine the type of ACL. These security styles are set based on which NAS protocol is specified, or in the case of dual protocol, is a choice made at the time of Cloud Volumes Service volume creation.

- If you are only using NFS, Cloud Volumes Service volumes use UNIX permissions.
- If you are only using SMB, Cloud Volumes Service volumes use NTFS permissions.

If you are creating a dual-protocol volume, you can choose the ACL style at volume creation. This decision should be made based on the desired permissions management. If your users manage permissions from Windows/SMB clients, select NTFS. If your users prefer using NFS clients and chmod/chown, use UNIX security styles.

[Next: Considerations for creating Active Directory connections.](#)

## Considerations for creating Active Directory connections

[Previous: Dual-protocol/multiprotocol.](#)

Cloud Volumes Service provides the ability to connect your Cloud Volumes Service instance to an external Active Directory server for identity management for both SMB and UNIX users. Creating an Active Directory connection is required to use SMB in Cloud Volumes Service.

The configuration for this provides several options that require some consideration for security. The external Active Directory server can be an on-premises instance or cloud native. If you are using an on-premises Active Directory server, don't expose the domain to the external network (such as with a DMZ or an external IP address). Instead, use secure private tunnels or VPNs, one-way forest trusts, or dedicated network connections to the on-premises networks with [Private Google Access](#). See the Google Cloud documentation for more information about [best practices using Active Directory in Google Cloud](#).

 CVS-SW requires Active Directory servers to be located in the same region. If a DC connection is attempted in CVS-SW to another region, the attempt fails. When using CVS-SW, be sure to create Active Directory sites that include the Active Directory DCs and then specify sites in Cloud Volumes Service to avoid cross-region DC connection attempts.

## Active Directory credentials

When SMB or LDAP for NFS is enabled, Cloud Volumes Service interacts with the Active Directory controllers to create a machine account object to use for authentication. This is no different from how a Windows SMB client joins a domain and requires the same access rights to Organizational Units (OUs) in Active Directory.

In many cases, security groups do not allow the use of a Windows administrator account on external servers

such as Cloud Volumes Service. In some cases, the Windows Administrator user is disabled entirely as a security best practice.

## Permissions needed to create SMB machine accounts

To add Cloud Volumes Service machine objects to an Active Directory, an account that either has administrative rights to the domain or has [delegated permissions to create and modify machine account objects](#) to a specified OU is required. You can do this with the Delegation of Control Wizard in Active Directory by creating a custom task that provides a user access to creation/deletion of computer objects with the following access permissions provided:

- Read/Write
- Create/Delete All Child Objects
- Read/Write All Properties
- Change/Reset Password

Doing this automatically adds a security ACL for the defined user to the OU in Active Directory and minimizes the access to the Active Directory environment. After a user has been delegated, that username and password can be provided as Active Directory Credentials in this window.



The username and password that is passed to the Active Directory domain leverages Kerberos encryption during the machine account object query and creation for added security.

## Active Directory connection details

The [Active Directory Connection Details](#) provide fields for administrators to give specific Active Directory schema information for machine account placement, such as the following:

- **Active Directory Connection Type.** Used to specify whether the Active Directory connection in a region is used for volumes of either Cloud Volumes Service or CVS-Performance service type. If this is set incorrectly on an existing connection, it might not work properly when used or edited.
- **Domain.** The Active Directory domain name.
- **Site.** Limits Active Directory servers to a specific site for security and performance [considerations](#). This is necessary when multiple Active Directory servers span regions because Cloud Volumes Service does not currently support allowing Active Directory authentication requests to Active Directory servers in a different region than the Cloud Volumes Service instance. (For instance, the Active Directory domain controller is in a region that only CVS-Performance supports but you want an SMB share in a CVS-SW instance.)
- **DNS servers.** DNS servers to use in name lookups.
- **NetBIOS name (optional).** If desired, the NetBIOS name for the server. This what is used when new machine accounts are created using the Active Directory connection. For instance, if the NetBIOS name is set to CVS-EAST then the machine account names will be CVS-EAST-{1234}. See the section "[How Cloud Volumes Service shows up in Active Directory](#)" for more information.
- **Organizational Unit (OU).** The specific OU to create the computer account. This is useful if you're delegating control to a user for machine accounts to a specific OU.
- **AES Encryption.** You can also check or uncheck the Enable AES Encryption for AD Authentication checkbox. Enabling AES encryption for Active Directory authentication provides extra security for Cloud Volumes Service to Active Directory communication during user and group lookups. Before enabling this option, check with your domain administrator to confirm that the Active Directory domain controllers support AES authentication.



By default, most Windows servers do not disable weaker ciphers (such as DES or RC4-HMAC), but if you choose to disable weaker ciphers, confirm Cloud Volumes Service Active Directory connection has been configured to enable AES. Otherwise, authentication failures occur. Enabling AES encryption doesn't disable weaker ciphers but instead adds support for AES ciphers to the Cloud Volumes Service SMB machine account.

## Kerberos realm details

This option does not apply to SMB servers. Rather, it is used when configuring NFS Kerberos for the Cloud Volumes Service system. When these details are populated, the NFS Kerberos realm is configured (similar to a krb5.conf file on Linux) and is used when NFS Kerberos is specified on the Cloud Volumes Service volume creation, as the Active Directory connection acts as the NFS Kerberos Distribution Center (KDC).



Non-Windows KDCs are currently unsupported for use with Cloud Volumes Service.

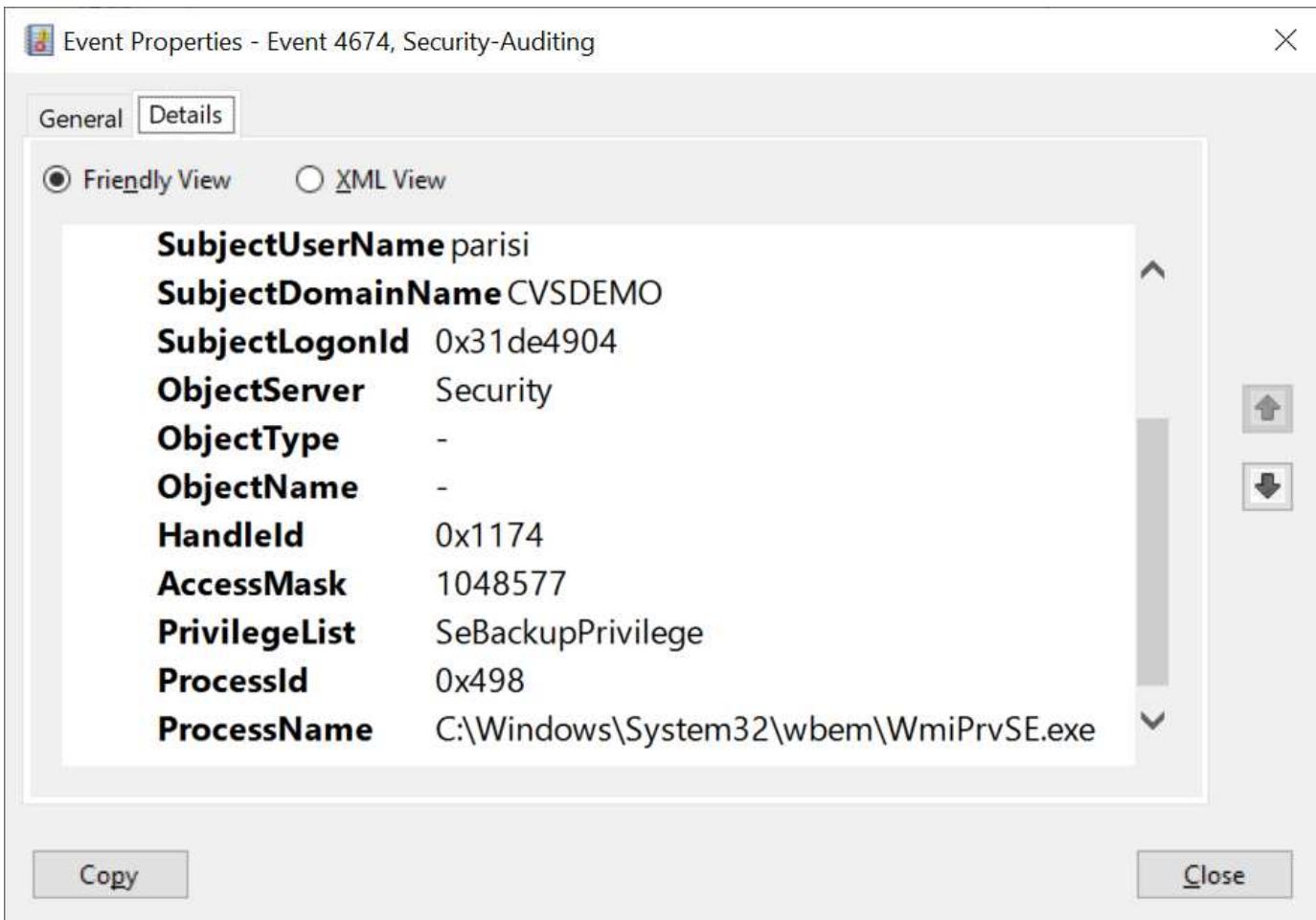
## Region

A region enables you to specify the location where the Active Directory connection resides. This region must be the same region as the Cloud Volumes Service volume.

- **Local NFS Users with LDAP.** In this section, there is also an option to Allow Local NFS Users with LDAP. This option must be left unselected if you want to extend your UNIX user group membership support beyond the 16-group limitation of NFS (extended groups). However, using extended groups requires a configured LDAP server for UNIX identities. If you don't have an LDAP server, leave this option unselected. If you have an LDAP server and want to also use local UNIX users (such as root), select this option.

## Backup users

This option enables you to specify Windows users that have backup permissions to the Cloud Volumes Service volume. Backup privileges (SeBackupPrivilege) are necessary for some applications to properly backup and restore data in NAS volumes. This user has a high level of access to data in the volume, so you should consider [enabling auditing of that user access](#). After it is enabled, audit events display in Event Viewer > Windows Logs > Security.



## Security privilege users

This option enables you to specify Windows users that have security modification permissions to the Cloud Volumes Service volume. Security privileges (SeSecurityPrivilege) are necessary for some applications ([such as SQL Server](#)) to properly set permissions during installation. This privilege is needed to manage the security log. Although this privilege is not as powerful as SeBackupPrivilege, NetApp recommends [auditing user access of users](#) with this privilege level if needed.

For more information, see [Special privileges assigned to new logon](#).

## How Cloud Volumes Service shows up in Active Directory

Cloud Volumes Service shows up in Active Directory as a normal machine account object. The naming conventions are as follows.

- CIFS/SMB and NFS Kerberos create separate machine account objects.
- NFS with LDAP enabled creates a machine account in Active Directory for Kerberos LDAP binds.
- Dual protocol volumes with LDAP share the CIFS/SMB machine account for LDAP and SMB.
- CIFS/SMB machine accounts use a naming convention of NAME-1234 (random four digit ID with hyphen appended to <10 character name) for the machine account. You can define NAME by the NetBIOS name setting on the Active Directory connection (see the section "[Active Directory connection details](#)").
- NFS Kerberos uses NFS-NAME-1234 as the naming convention (up to 15 characters). If more than 15 characters are used, the name is NFS-TRUNCATED-NAME-1234.

- NFS-only CVS-Performance instances with LDAP enabled create an SMB machine account for binding to the LDAP server with the same naming convention as CIFS/SMB instances.
- When an SMB machine account is created, default hidden admin shares (see the section “[Default hidden shares](#)”) are also created (c\$, admin\$, ipc\$), but those shares have no ACLs assigned and are inaccessible.
- The machine account objects are placed in CN=Computers by default, but you can specify a different OU when necessary. See the section “[Permissions needed to create SMB machine accounts](#)” for information about what access rights are needed to add/remove machine account objects for Cloud Volumes Service.

When Cloud Volumes Service adds the SMB machine account to Active Directory, the following fields are populated:

- cn (with the specified SMB server name)
- dNSHostName (with SMBserver.domain.com)
- msDS-SupportedEncryptionTypes (Allows DES\_CBC\_MD5, RC4\_HMAC\_MD5 if AES encryption is not enabled; if AES encryption is enabled, DES\_CBC\_MD5, RC4\_HMAC\_MD5, AES128\_CTS\_HMAC\_SHA1\_96, AES256\_CTS\_HMAC\_SHA1\_96 are allowed for Kerberos ticket exchange with the machine account for SMB)
- name (with the SMB server name)
- sAMAccountName (with SMBserver\$)
- servicePrincipalName (with host/smbserver.domain.com and host/smbserver SPNs for Kerberos)

If you want to disable weaker Kerberos encryption types ( enctype) on the machine account, you can change the msDS-SupportedEncryptionTypes value on the machine account to one of the values in the following table to allow AES only.

<b>msDS-SupportedEncryptionTypes value</b>	<b>Enctype enabled</b>
2	DES_CBC_MD5
4	RC4_HMAC
8	AES128_CTS_HMAC_SHA1_96 only
16	AES256_CTS_HMAC_SHA1_96 only
24	AES128_CTS_HMAC_SHA1_96 and AES256_CTS_HMAC_SHA1_96
30	DES_CBC_MD5, RC4_HMAC, AES128_CTS_HMAC_SHA1_96 and AES256_CTS_HMAC_SHA1_96

To enable AES encryption for SMB machine accounts, click Enable AES Encryption for AD Authentication when creating the Active Directory connection.

To enable AES encryption for NFS Kerberos, [see the Cloud Volumes Service documentation](#).

[Next: Other NAS Infrastructure service dependencies \(KDC, LDAP, DNS\).](#)

[Other NAS Infrastructure service dependencies \(KDC, LDAP, and DNS\)](#)

[Previous: Considerations for creating Active Directory connections.](#)

When using Cloud Volumes Service for NAS shares, there might be external dependencies required for proper functionality. These dependencies are in play under specific circumstances. The following table shows various configuration options and what, if any, dependencies are required.

Configuration	Dependencies required
NFSv3 only	None
NFSv3 Kerberos only	Windows Active Directory: * KDC * DNS * LDAP
NFSv4.1 only	Client ID mapping configuration (/etc/idmap.conf)
NFSv4.1 Kerberos only	<ul style="list-style-type: none"> <li>• Client ID mapping configuration (/etc/idmap.conf)</li> <li>• Windows Active Directory: KDC DNS LDAP</li> </ul>
SMB only	Active Directory: * KDC * DNS
Multiprotocol NAS (NFS and SMB)	<ul style="list-style-type: none"> <li>• Client ID mapping configuration (NFSv4.1 only; /etc/idmap.conf)</li> <li>• Windows Active Directory: KDC DNS LDAP</li> </ul>

### Kerberos keytab rotation/password resets for machine account objects

With SMB machine accounts, Cloud Volumes Service schedules periodic password resets for the SMB machine account. These password resets occur using Kerberos encryption and operate on a schedule of every fourth Sunday at a random time between 11PM and 1AM. These password resets change the Kerberos key versions, rotate the keytabs stored on the Cloud Volumes Service system, and help maintain a greater level of security for SMB servers running in Cloud Volumes Service. Machine account passwords are randomized and are not known to administrators.

For NFS Kerberos machine accounts, password resets take place only when a new keytab is created/exchanged with the KDC. Currently, this is not possible to do in Cloud Volumes Service.

### Network ports for use with LDAP and Kerberos

When using LDAP and Kerberos, you should determine the network ports in use by these services. You can find a complete list of ports in use by Cloud Volumes Service in the [Cloud Volumes Service documentation on security considerations](#).

### LDAP

Cloud Volumes Service acts as an LDAP client and uses standard LDAP search queries for user and group lookups for UNIX identities. LDAP is necessary if you intend to use users and groups outside the standard

default users provided by Cloud Volumes Service. LDAP is also necessary if you plan on using NFS Kerberos with user principals (such as [user1@domain.com](mailto:user1@domain.com)). Currently, only LDAP using Microsoft Active Directory is supported.

To use Active Directory as a UNIX LDAP server, you must populate the necessary UNIX attributes on users and groups you intend to use for UNIX identities. Cloud Volumes Service uses a default LDAP schema template that queries attributes based on [RFC-2307-bis](#). As a result, the following table shows the bare minimum necessary Active Directory attributes to populate for users and groups and what each attribute is used for.

For more information about setting LDAP attributes in Active Directory, see [Managing dual-protocol access](#).

Attribute	What it does
uid*	Specifies the UNIX user name
uidNumber*	Specifies the UNIX user's numeric ID
gidNumber*	Specifies the UNIX user's primary group numeric ID
objectClass*	Specifies what type of object is being used; Cloud Volumes Service requires "user" to be included in the list of object classes (is included in most Active Directory deployments by default).
name	General information about the account (real name, phone number, and so on—also known as gecos)
unixUserPassword	No need to set this; not used in UNIX identity lookups for NAS authentication. Setting this puts the configured unixUserPassword value in plaintext.
unixHomeDirectory	Defines path to UNIX home directories when a user authenticates against LDAP from a Linux client. Set this if you want to use LDAP for UNIX home directory functionality.
loginShell	Defines path to the bash/profile shell for Linux clients when a user authenticates against LDAP.

\*Denotes attribute is required for proper functionality with Cloud Volumes Service. Remaining attributes are for client-side use only.

Attribute	What it does
cn*	Specifies the UNIX group name. When using Active Directory for LDAP, this is set when the object is first created, but it can be changed later. This name cannot be the same as other objects. For instance, if your UNIX user named user1 belongs to a group named user1 on your Linux client, Windows doesn't allow two objects with the same cn attribute. To work around this, rename the Windows user to a unique name (such as user1-UNIX); LDAP in Cloud Volumes Service uses the uid attribute for UNIX user names.
gidNumber*	Specifies the UNIX group numeric ID.

Attribute	What it does
objectClass*	Specifies what type of object is being used; Cloud Volumes Service requires group to be included in the list of object classes (this attribute is included in most Active Directory deployments by default).
memberUid	Specifies which UNIX users are members of the UNIX group. With Active Directory LDAP in Cloud Volumes Service, this field is not necessary. The Cloud Volumes Service LDAP schema uses the Member field for group memberships.
Member*	Required for group memberships/secondary UNIX groups. This field is populated by adding Windows users to Windows groups. However, if the Windows groups don't have UNIX attributes populated, they are not included in the UNIX user's group membership lists. Any groups that need to be available in NFS must populate the required UNIX group attributes listed in this table.

\*Denotes attribute is required for proper functionality with Cloud Volumes Service. Remaining attributes are for client-side use only.

## LDAP bind information

To query users in LDAP, Cloud Volumes Service must bind (login) to the LDAP service. This login has read-only permissions and is used to query LDAP UNIX attributes for directory lookups. Currently, LDAP binds are possible only by using an SMB machine account.

You can only enable LDAP for CVS-Performance instances and use it for NFSv3, NFSv4.1, or dual-protocol volumes. An Active Directory connection must be established in the same region as the Cloud Volumes Service volume for successful deployment of the LDAP-enabled volume.

When LDAP is enabled, the following occurs in specific scenarios.

- If only NFSv3 or NFSv4.1 is used for the Cloud Volumes Service project, then a new machine account is created in the Active Directory domain controller, and the LDAP client in Cloud Volumes Service binds to Active Directory by using the machine account credentials. No SMB shares are created for the NFS volume and default hidden administrative shares (see the section “[Default hidden shares](#)”) have share ACLs removed.
- If dual-protocol volumes are used for the Cloud Volumes Service project, then only the single machine account created for SMB access is used to bind the LDAP client in Cloud Volumes Service to Active Directory. No additional machine accounts are created.
- If dedicated SMB volumes are created separately (either before or after NFS volumes with LDAP are enabled), then the machine account for LDAP binds is shared with the SMB machine account.
- If NFS Kerberos is also enabled, two machine accounts are created—one for SMB shares and/or LDAP binds and one for NFS Kerberos authentication.

## LDAP queries

Although LDAP binds are encrypted, LDAP queries are passed over the wire in plaintext by using the common LDAP port 389. This well-known port cannot currently be changed in Cloud Volumes Service. As a result,

someone with access to packet sniffing in the network can see user and group names, numeric IDs, and group memberships.

However, Google Cloud VMs cannot sniff other VM's unicast traffic. Only VMs actively participating in LDAP traffic (that is, being able to bind) can see traffic from the LDAP server. For more information about packet sniffing in Cloud Volumes Service, see the section "[Packet sniffing/trace considerations](#)".

## LDAP client configuration defaults

When LDAP is enabled in a Cloud Volumes Service instance, an LDAP client configuration is created with specific configuration details by default. In some cases, options either do not apply to Cloud Volumes Service (not supported) or are not configurable.

LDAP client option	What it does	Default value	Can change?
LDAP Server List	Sets LDAP server names or IP addresses to use for queries. This is not used for Cloud Volumes Service. Instead, Active Directory Domain is used to define LDAP servers.	Not set	No
Active Directory Domain	Sets the Active Directory Domain to use for LDAP queries. Cloud Volumes Service leverages SRV records for LDAP in DNS to find LDAP servers in the domain.	Set to the Active Directory domain specified in the Active Directory connection.	No
Preferred Active Directory Servers	Sets the preferred Active Directory servers to use for LDAP. Not supported by Cloud Volumes Service. Instead, use Active Directory sites to control LDAP server selection.	Not set.	No
Bind using SMB Server Credentials	Binds to LDAP by using the SMB machine account. Currently, the only supported LDAP bind method in Cloud Volumes Service.	True	No
Schema Template	The schema template used for LDAP queries.	MS-AD-BIS	No
LDAP Server Port	The port number used for LDAP queries. Cloud Volumes Service currently uses only the standard LDAP port 389. LDAPS/port 636 is not currently supported.	389	No

LDAP client option	What it does	Default value	Can change?
Is LDAPS Enabled	Controls whether LDAP over Secure Sockets Layer (SSL) is used for queries and binds. Currently not supported by Cloud Volumes Service.	False	No
Query Timeout (sec)	Timeout for queries. If queries take longer than the specified value, queries fail.	3	No
Minimum Bind Authentication Level	The minimum supported bind level. Because Cloud Volumes Service uses machine accounts for LDAP binds and Active Directory does not support anonymous binds by default, this option does not come into play for security.	Anonymous	No
Bind DN	The user/distinguished name (DN) used for binds when simple bind is used. Cloud Volumes Service uses machine accounts for LDAP binds and does not currently support simple bind authentication.	Not set	No
Base DN	The base DN used for LDAP searches.	The Windows domain used for the Active Directory connection, in DN format (that is, DC=domain, DC=local).	No
Base search scope	The search scope for base DN searches. Values can include base, onelevel, or subtree. Cloud Volumes Service only supports subtree searches.	Subtree	No
User DN	Defines the DN where user searches start for LDAP queries. Currently not supported for Cloud Volumes Service, so all user searches start at the base DN.	Not set	No

LDAP client option	What it does	Default value	Can change?
User search scope	The search scope for user DN searches. Values can include base, onlevel, or subtree. Cloud Volumes Service does not support setting the user search scope.	Subtree	No
Group DN	Defines the DN where group searches start for LDAP queries. Currently not supported for Cloud Volumes Service, so all group searches start at the base DN.	Not set	No
Group search scope	The search scope for group DN searches. Values can include base, onlevel, or subtree. Cloud Volumes Service does not support setting the group search scope.	Subtree	No
Netgroup DN	Defines the DN where netgroup searches start for LDAP queries. Currently not supported for Cloud Volumes Service, so all netgroup searches start at the base DN.	Not set	No
Netgroup search scope	The search scope for netgroup DN searches. Values can include base, onlevel, or subtree. Cloud Volumes Service does not support setting the netgroup search scope.	Subtree	No
Use start_tls over LDAP	Leverages Start TLS for certificate based LDAP connections over port 389. Currently not supported by Cloud Volumes Service.	False	No
Enable netgroup-by-host lookup	Enables netgroup lookups by hostname rather than expanding netgroups to list all members. Currently not supported by Cloud Volumes Service.	False	No

LDAP client option	What it does	Default value	Can change?
Netgroup-by-host DN	Defines the DN where netgroup-by-host searches start for LDAP queries. Netgroup-by-host is currently not supported for Cloud Volumes Service.	Not set	No
Netgroup-by-host search scope	The search scope for netgroup-by-host DN searches. Values can include base, onlevel or subtree. Netgroup-by-host is currently not supported for Cloud Volumes Service.	Subtree	No
Client session security	Defines what level of session security is used by LDAP (sign, seal, or none). LDAP signing is supported by Cloud Volumes Service, but sealing is not currently supported.	None	No
LDAP referral chasing	When using multiple LDAP servers, referral chasing allows the client to refer to other LDAP servers in the list when an entry is not found in the first server. This is currently not supported by Cloud Volumes Service.	False	No
Group membership filter	Provides a custom LDAP search filter to be used when looking up group membership from an LDAP server. Not currently supported with Cloud Volumes Service.	Not set	No

## Using LDAP for asymmetric name mapping

Cloud Volumes Service, by default, maps Windows users and UNIX users with identical usernames bidirectionally without special configuration. As long as Cloud Volumes Service can find a valid UNIX user (with LDAP), then 1:1 name mapping occurs. For instance, if Windows user `johndoe` is used, then, if Cloud Volumes Service can find a UNIX user named `johndoe` in LDAP, name mapping succeeds for that user, all files/folders created by `johndoe` show the correct user ownership, and all ACLs affecting `johndoe` are honored regardless of the NAS protocol in use. This is known as symmetric name mapping.

Asymmetric name mapping is when the Windows user and UNIX user identity don't match. For instance, if

Windows user `johnsmith` has a UNIX identity of `jsmith`, Cloud Volumes Service needs a way to be told about the variation. Because Cloud Volumes Service currently doesn't support creation of static name mapping rules, LDAP must be used to look up the identity of the users for both Windows and UNIX identities to ensure proper ownership of files and folders and expected permissions.

By default, Cloud Volumes Service includes LDAP in the ns-switch of the instance for the name map database, so that to provide name mapping functionality by using LDAP for asymmetric names, you only need to modify some of the user/group attributes to reflect what Cloud Volumes Service looks for.

The following table shows what attributes must be populated in LDAP for asymmetric name mapping functionality. In most cases, Active Directory is already configured to do this.

Cloud Volumes Service attribute	What it does	Value used by Cloud Volumes Service for name mapping
Windows to UNIX objectClass	Specifies the type of object being used. (That is, user, group, posixAccount, and so on)	Must include user (can contain multiple other values, if desired.)
Windows to UNIX attribute	that defines the Windows username at creation. Cloud Volumes Service uses this for Windows to UNIX lookups.	No change needed here; sAMAccountName is the same as the Windows login name.
UID	Defines the UNIX username.	Desired UNIX username.

Cloud Volumes Service currently does not use domain prefixes in LDAP lookups, so multiple domain LDAP environments do not function properly with LDAP namemap lookups.

The following example shows a user with the Windows name `asymmetric`, the UNIX name `unix-user`, and the behavior it follows when writing files from both SMB and NFS.

The following figure shows how LDAP attributes look from the Windows server.

## asymmetric Properties

?

X

Published Certificates		Member Of		Password Replication		Dial-in	Object									
Security		Environment		Sessions		Remote control										
General	Address	Account	Profile	Telephones	Organization											
Remote Desktop Services Profile			COM+		Attribute Editor											
Attributes:																
Attribute	Value															
name	asymmetric															
objectCategory	CN=Person,CN=Schema,CN=Configuration,															
objectClass	top; person; organizationalPerson; user															
objectGUID	de489556-dd7b-43a3-98fa-2722f79d67ed															
objectSid	S-1-5-21-3552729481-4032800560-2279794															
primaryGroupID	513 = ( GROUP_RID_USERS )															
pwdLastSet	1/19/2017 1:56:34 PM Eastern Standard Time															
replPropertyMetaData	AttID	Ver	Loc.USN	Org.DSA												
sAMAccountName	asymmetric															
sAMAccountType	805306368 = ( NORMAL_USER_ACCOUNT )															
uid	unix-user															
uidNumber	1207															

From an NFS client, you can query the UNIX name but not the Windows name:

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

When a file is written from NFS as unix-user, the following is the result from the NFS client:

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx----- 1 unix-user sharedgroup      0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

From a Windows client, you can see that the owner of the file is set to the proper Windows user:

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner  
Owner  
----  
NTAP\asymmetric
```

Conversely, files created by the Windows user `asymmetric` from an SMB client show the proper UNIX owner, as shown in the following text.

SMB:

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS:

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt  
-rwx----- 1 unix-user sharedgroup 14 Feb 28 12:43 asymmetric-  
user-smb.txt  
sh-4.2$ cat asymmetric-user-smb.txt  
TEXT
```

## LDAP channel binding

Because of a vulnerability with Windows Active Directory domain controllers, [Microsoft Security Advisory ADV190023](#) changes how DCs allow LDAP binds.

The impact for Cloud Volumes Service is the same as for any LDAP client. Cloud Volumes Service does not currently support channel binding. Because Cloud Volumes Service supports LDAP signing by default through negotiation, LDAP channel binding should not be an issue. If you do have issues binding to LDAP with channel binding enabled, follow the remediation steps in ADV190023 to allow LDAP binds from Cloud Volumes Service to succeed.

## DNS

Active Directory and Kerberos both have dependencies on DNS for host name to IP/IP to host name resolution. DNS requires port 53 to be open. Cloud Volumes Service does not make any modifications to DNS records, nor does it currently support the use of [dynamic DNS](#) on network interfaces.

You can configure Active Directory DNS to restrict which servers can update DNS records. For more information, see [Secure Windows DNS](#).

Note that resources within a Google project default to using Google Cloud DNS, which isn't connected with Active Directory DNS. Clients using Cloud DNS cannot resolve UNC paths returned by Cloud Volumes Service. Windows clients joined to the Active Directory domain are configured to use Active Directory DNS and can resolve such UNC paths.

To join a client to Active Directory, you must configure its DNS configuration to use Active Directory DNS.

Optionally, you can configure Cloud DNS to forward requests to Active Directory DNS. See [Why can't my client resolve the SMB NetBIOS name?](#) for more information.



Cloud Volumes Service does not currently support DNSSEC and DNS queries are performed in plaintext.

## File access auditing

Currently not supported for Cloud Volumes Service.

## Antivirus protection

You must perform antivirus scanning in Cloud Volumes Service at the client to a NAS share. There is currently no native antivirus integration with Cloud Volumes Service.

[Next: Service operation.](#)

## Service operation

[Previous: Other NAS Infrastructure service dependencies \(KDC, LDAP, DNS\).](#)

The Cloud Volumes Service team manages the backend services in Google Cloud and uses multiple strategies to secure the platform and prevent unwanted access.

Each customer gets their own unique subnet that has access fenced off from other customers by default, and every tenant in Cloud Volumes Service gets their own namespace and VLAN for total data isolation. After a user is authenticated, the Service Delivery Engine (SDE) can only read configuration data specific to that tenant.

## Physical security

With proper preapproval, only onsite engineers and NetApp-badged Field Support Engineers (FSEs) have access to the cage and racks for physical work. Storage and network management is not permitted. Only these onsite resources are able to perform hardware maintenance tasks.

For onsite engineers, a ticket is raised for the statement of work (SOW) that includes the rack ID and device location (RU) and all other details are included in the ticket. For NetApp FSEs, a site visitation ticket must be raised with the COLO and the ticket includes the visitor's details, date, and time for auditing purposes. The SOW for the FSE is communicated internally to NetApp.

## Operations team

The operations team for Cloud Volumes Service consists of Production Engineering and a Site Reliability Engineer (SRE) for Cloud Volume Services and NetApp Field Support Engineers and Partners for hardware. All operations team members are accredited for work in Google Cloud and detailed records of work are maintained for every ticket raised. In addition, there is a stringent change control and approval process in place to ensure each decision is appropriately scrutinized.

The SRE team manages the control plane and how the data is routed from UI requests to backend hardware and software in Cloud Volumes Service. The SRE team also manages system resources, such as volume and inode maximums. SREs are not allowed to interact with or have access to customer data. SREs also provide coordination with Return Material Authorizations (RMAs), such as new disk or memory replacement requests for the backend hardware.

## **Customer responsibilities**

Customers of Cloud Volumes Service manage their organization's Active Directory and user role management as well as the volume and data operations. Customers can have administrative roles and can delegate permissions to other end users within the same Google Cloud project using the two predefined roles that NetApp and Google Cloud provide (Administrator and Viewer).

The administrator can peer any VPC within the customer project to Cloud Volumes Service that the customer determines to be appropriate. It is the responsibility of the customer to manage access to their Google Cloud marketplace subscription and to manage the VPCs that have access to the data plane.

## **Malicious SRE protection**

One concern that could arise is how does Cloud Volumes Service protect against scenarios in which there is a malicious SRE or when SRE credentials have been compromised?

Access to the production environment is with a limited number of SRE individuals only. Administrative privileges are further restricted to a handful of experienced administrators. All actions performed by anyone in the Cloud Volumes Service production environment are logged and any anomalies to the baseline or suspicious activities are detected by our security information and event management (SIEM) threat intelligence platform. As a result, malicious actions can be tracked and mitigated before too much damage is done to the Cloud Volumes Service backend.

## **Volume life cycle**

Cloud Volumes Service manages only the objects within the service—not the data within the volumes. Only clients accessing the volumes can manage the data, the ACLs, file owners, and so on. The data in these volumes is encrypted at rest and access is limited to tenants of the Cloud Volumes Service instance.

The volume lifecycle for Cloud Volumes Service is create-update-delete. Volumes retain Snapshot copies of volumes until the volumes are deleted, and only validated Cloud Volumes Service administrators can delete volumes in Cloud Volumes Service. When a volume deletion is requested by an administrator, an additional step of entering the volume name is required to verify the deletion. After a volume is deleted, the volume is gone and cannot be recovered.

In cases where a Cloud Volumes Service contract is terminated, NetApp marks volumes for deletion after a specific time period. Before that time period expires, you can recover volumes at the customer's request.

## **Certifications**

Cloud Volumes Services for Google Cloud is currently certified to ISO/IEC 27001:2013 and ISO/IEC 27018:2019 standards. The service also recently received its SOC2 Type I attestation report. For information about the NetApp commitment to data security and privacy, see [Compliance: Data security and data privacy](#).

## **GDPR**

Our commitments to privacy and compliance with GDPR are available in a number of our [customer contracts](#), such as our [Customer Data Processing Addendum](#), which includes the [Standard Contractual Clauses](#) provided by the European Commission. We also make these commitments in our Privacy Policy, backed by the core values set out in our corporate Code of Conduct.

[Next: Additional information, version history, and contact information.](#)

## **Additional information, version history, and contact information**

[Previous: Service operation.](#)

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

- Google Cloud documentation for Cloud Volumes Service

<https://cloud.google.com/architecture/partners/netapp-cloud-volumes/>

- Google private service access

[https://cloud.google.com/vpc/docs/private-services-access?hl=en\\_US](https://cloud.google.com/vpc/docs/private-services-access?hl=en_US)

- NetApp product documentation

<https://www.netapp.com/support-and-training/documentation/>

- Cryptographic Validation Module Program—NetApp CryptoMod

<https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144>

- The NetApp Solution for Ransomware

<https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745>

- TR-4616: NFS Kerberos in ONTAP

<https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf>

## **Version history**

<b>Version</b>	<b>Date</b>	<b>Document version history</b>
Version 1.0	May 2022	Initial release.

## **Contact us**

Let us know how we can improve this technical report.

Contact us at [doccomments@netapp.com](mailto:doccomments@netapp.com). Include TECHNICAL REPORT 4918 in the subject line.

# NetApp Solutions for Virtualization

## Get Started With NetApp & VMware

VMware on NetApp: Your journey starts here!

If you're ready to start transforming your VMware environment, browse the latest solution overview, review our latest technical solutions and product demonstrations. If you're ready for the next step, engage NetApp and VMware community of experts to help plan and execute your data center modernization, hybrid cloud or containerized application initiatives.

Not sure where to start? [Contact](#) a member of the VMware Experts at NetApp.

**NetApp and VMware: Better Together**



The content presented on this page is also available for download in [PDF format](#).

## Learn about NetApp and VMware Solutions

- [NetApp & VMware: Better Together](#)
- [ONTAP 9.8 Latest Features for VMware Overview](#)
- [Leveraging SnapCenter Plugin for VMware vSphere](#)
- [Redefining VMware Performance with NetApp and NVMe](#)
- [A Low-Cost Performant World for VMware Cloud on AWS](#)
- [Introducing VMware Tanzu with NetApp](#)
- [Virtual Desktop Infrastructure \(VDI\): Delivering Employee Workstations on Demand](#)
- [VMware on AWS: Architecture and Service Options](#)
- [Programming with NetApp Cloud Volumes Service APIs To Optimize AWS Experience](#)
- [Kubernetes: Running K8s on vSphere and Tanzu](#)

## Build Your Virtualized Data Fabric

### Review our latest NetApp Solutions for VMware

- [VMware vSphere with ONTAP : NetApp Solutions](#)
- [VMware vSphere Virtual Volumes with ONTAP](#)
- [SnapCenter Plug-in for VMware vSphere](#)
- [NetApp Modern NVMeoF VMware vSphere Workload Design & Validation](#)
- [NetApp Modern NVMeoF Cloud-Connected Flash Solution for VMware & SQL Server](#)
- [Accelerate Your Kubernetes Journey with VMware Tanzu & ONTAP](#)
- [Lower The Cost of Running VMware Cloud on AWS](#)

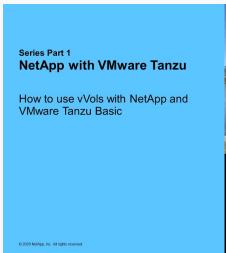
### Explore video demonstrations of the latest VMware solutions

- Best Practices for VMware vSphere and NetApp ONTAP
- Your VMware Environment - Let's Run it on NVMe-oF with ONTAP
- vVols Disaster Recovery with ONTAP Tools and VMware SRM
- VMware Backup and Recovery for the Data Fabric

## Deploy flexible hybrid-cloud & modernized applications infrastructure for VMware

### Videos

- Architecting VMware Datastores on NetApp All Flash FAS
- A Low-Cost Performant World for VMware Cloud on AWS
- Migrate Your VMware VMs to Google Cloud

 <p><b>Series Part 1 NetApp with VMware Tanzu</b> How to use vVols with NetApp and VMware Tanzu Basic</p> <p><b>NetApp</b></p>	 <p><b>Using vVols with NetApp &amp; VMware Tanzu Basic</b> Part 2</p> <p><b>NetApp</b></p>	 <p><b>Using vVols with NetApp &amp; VMware Tanzu Basic</b> Part 3</p> <p><b>NetApp</b></p>
<p><b>Deploying Dynamic Persistent NetApp Storage for VMware Tanzu, part 1</b></p> <p><b>Deploying Dynamic Persistent NetApp Storage for VMware Tanzu, part 2</b></p> <p><b>Deploying Dynamic Persistent NetApp Storage for VMware Tanzu, part 3</b></p>		

### Blogs

- VMware Cloud on AWS: How Fujitsu Saves Millions using CVO

## Engage NetApp & VMware Experts

- Join The VMware Solutions Discussion Forum
- Contact The NetApp Global Services Team To Get Started

## VMware Virtualization for ONTAP

### NetApp ONTAP Benefits for VMware vSphere Administrators

#### Introduction to ONTAP for vSphere Administrators

##### Why ONTAP for vSphere?

NetApp ONTAP simplifies storage and data management operations and distinctly complements VMware environments, whether deploying on-premises or to the cloud. NetApp best-in-class data protection, storage efficiency innovations, and outstanding performance in both SAN- and NAS-based VMware architectures are among the reasons why tens of thousands of customers have selected ONTAP as their storage solution for vSphere deployments.

NetApp provides numerous VMware plug-ins, validations, and qualifications of various VMware products to support customers facing the unique challenges of administering a virtualization environment. NetApp does for storage and data management what VMware does for virtualization, allowing customers to focus on their core competencies rather than managing physical storage. This nearly 20-year partnership between VMware and NetApp continues to evolve and add customer value as new technologies, such as VMware Cloud Foundation and Tanzu, emerge, while continuing to support the foundation of vSphere.

Key factors customers value include:

- **Unified storage**
- **Storage efficiency**
- **Virtual volumes and storage policy-based management**
- **Hybrid cloud**

For more information regarding supported NetApp and VMware solutions, see the following resources:

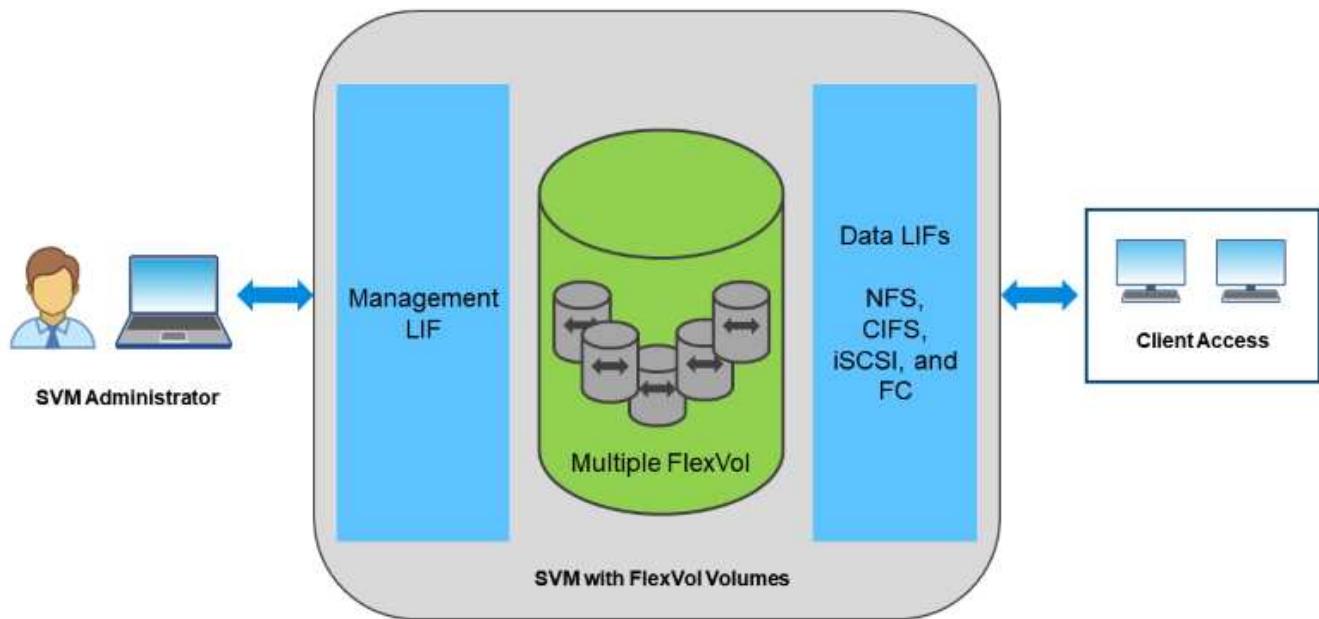
- [The NetApp Interoperability Matrix Tool](#) (IMT). The IMT defines the qualified components and versions you can use to build FC/FCoE, iSCSI, NFS and CIFS configurations.
- [The VMware Compatibility Guide](#). The VMware Compatibility guide lists System, I/O, Storage/SAN and Backup compatibility with VMware Infrastructure and software products
- [NetApp ONTAP Tools for VMware](#). ONTAP tools for VMware vSphere is a single vCenter Server plug-in that includes the VSC, VASA Provider, and Storage Replication Adapter (SRA) extensions.

## ONTAP Unified Storage

### About Unified Storage

Systems running ONTAP software are unified in several significant ways. Originally this approach referred to supporting both NAS and SAN protocols on one storage system, and ONTAP continues to be a leading platform for SAN along with its original strength in NAS.

A storage virtual machine (SVM) is a logical construct allowing client access to systems running ONTAP software. SVMs can serve data concurrently through multiple data access protocols via logical interfaces (LIFs). SVMs provide file-level data access through NAS protocols, such as CIFS and NFS, and block-level data access through SAN protocols, such as iSCSI, FC/FCoE, and NVMe. SVMs can serve data to SAN and NAS clients independently at the same time.



In the vSphere world, this approach could also mean a unified system for virtual desktop infrastructure (VDI) together with virtual server infrastructure (VSI). Systems running ONTAP software are typically less expensive for VSI than traditional enterprise arrays and yet have advanced storage efficiency capabilities to handle VDI in the same system. ONTAP also unifies a variety of storage media, from SSDs to SATA, and can extend that easily into the cloud. There's no need to buy one flash array for performance, a SATA array for archives, and separate systems for the cloud. ONTAP ties them all together.



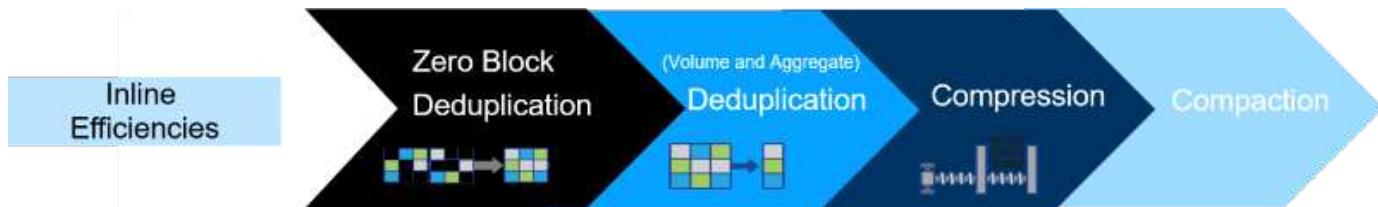
For more information on SVMs, unified storage and client access, see [Storage Virtualization](#) in the ONTAP 9 Documentation center.

## ONTAP storage efficiencies

### About storage efficiencies

Although NetApp was the first to deliver deduplication for production workloads, this innovation wasn't the first or last one in this area. It started with ONTAP Snapshot copies, a space-efficient data protection mechanism with no performance effect, along with FlexClone technology to instantly make read/write copies of VMs for production and backup use. NetApp went on to deliver inline capabilities, including deduplication, compression, and zero-block deduplication, to squeeze out the most storage from expensive SSDs. Most recently, ONTAP added compaction to strengthen our storage efficiencies.

- **Inline zero-block deduplication.** Eliminates space wasted by all-zero blocks.
- **Inline compression.** Compresses data blocks to reduce the amount of physical storage required.
- **Inline deduplication.** Eliminates incoming blocks with existing blocks on disk.
- **Inline data compaction.** Packs smaller I/O operations and files into each physical block.



You can run deduplication, data compression, and data compaction together or independently to achieve optimal space savings on a FlexVol volume. The combination of these capabilities has resulted in customers seeing savings of up to 5:1 for VSI and up to 30:1 for VDI.



For more information on ONTAP storage efficiencies, see [Using deduplication, data compression, and data compaction to increase storage efficiency](#) in the ONTAP 9 Documentation center.

## **Virtual Volumes (vVols) and Storage Policy Based Management (SPBM)**

### **About vVols and SPBM**

NetApp was an early design partner with VMware in the development of vSphere Virtual Volumes (vVols), providing architectural input and early support for vVols and VMware vSphere APIs for Storage Awareness (VASA). Not only did this approach bring VM granular storage management to VMFS, it also supported automation of storage provisioning through Storage Policy-Based Management (SPBM).

SPBM provides a framework that serves as an abstraction layer between the storage services available to your virtualization environment and the provisioned storage elements via policies. This approach allows storage architects to design storage pools with different capabilities that can be easily consumed by VM administrators. Administrators can then match virtual machine workload requirements against the provisioned storage pools, allowing for granular control of various settings on a per-VM or virtual disk level.

ONTAP leads the storage industry in vVols scale, supporting hundreds of thousands of vVols in a single cluster, whereas enterprise array and smaller flash array vendors support as few as several thousand vVols per array. NetApp is also driving the evolution of VM granular management with upcoming capabilities in support of vVols 3.0.



For more information on VMware vSphere Virtual Volumes, SPBM, and ONTAP, see [TR-4400: VMware vSphere Virtual Volumes with ONTAP](#).

## **Hybrid Cloud with ONTAP and vSphere**

### **About Hybrid Cloud**

Whether used for an on-premises private cloud, public-cloud infrastructure, or a hybrid cloud that combines the best of both, ONTAP solutions help you build your data fabric to streamline and optimize data management. Start with high-performance, all-flash systems, then couple them with either disk or cloud storage systems for data protection and cloud compute.

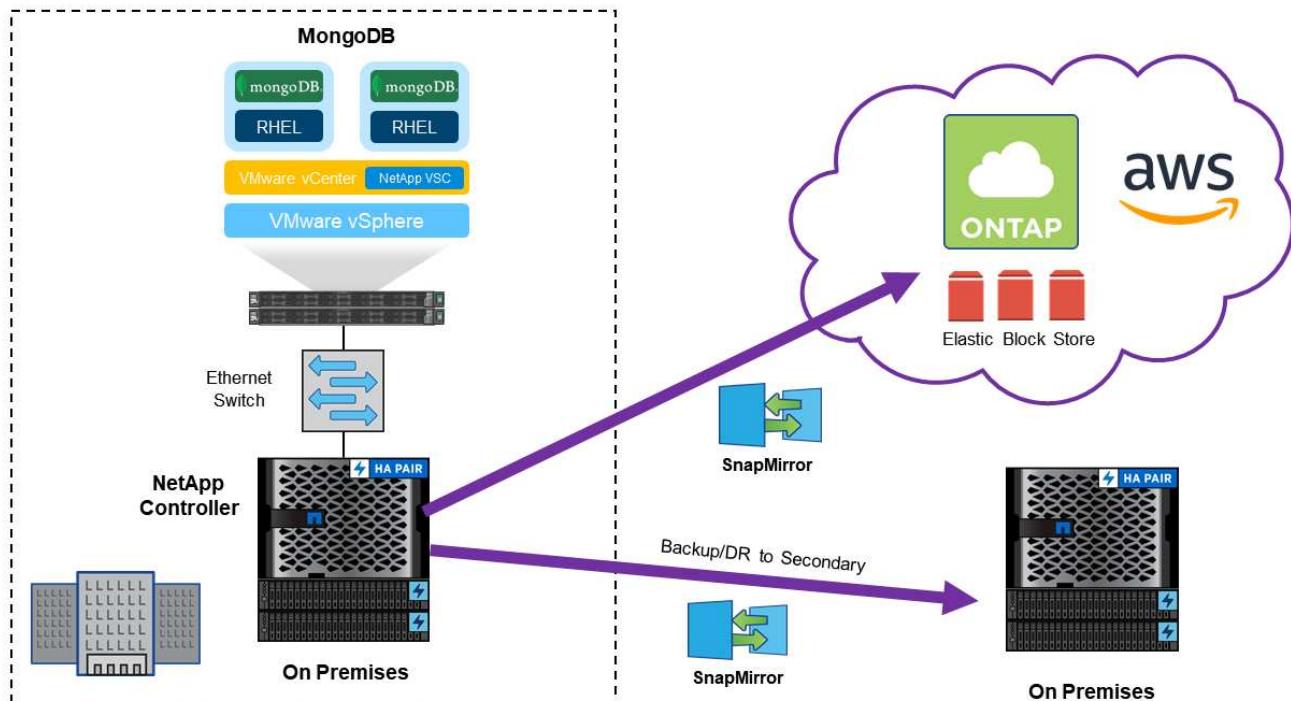
Choose from Azure, AWS, IBM, or Google clouds to optimize costs and avoid lock-in. Leverage advanced support for OpenStack and container technologies as needed.

Data protection is often the first thing customers try when they begin their cloud journey. Protection can be as simple as asynchronous replication of key data or as complex as a complete hot-backup site. Data protection is based primarily on NetApp SnapMirror technology.

Some customers choose to move entire workloads to the cloud. This can be more complicated than just using the cloud for data protection, but ONTAP makes moving easier because you do not have to rewrite your applications to use cloud-based storage. ONTAP in the cloud works just like on-premises ONTAP does. Your on-premises ONTAP system offers data efficiency features that enable you to store more data in less physical space and to tier rarely used data to lower cost storage. Whether you use a hybrid cloud configuration or move an entire workload to the cloud, ONTAP maximizes storage performance and efficiency.

NetApp also offers cloud-based backup (SnapMirror Cloud, Cloud Backup Service, and Cloud Sync) and storage tiering and archiving tools (FabricPool) for ONTAP to help reduce operating expenses and leverage the broad reach of the cloud.

The following figure provides a sample hybrid cloud use case.



**i** For more information on ONTAP and hybrid clouds, see [ONTAP and the Cloud](#) in the ONTAP 9 Documentation Center.

## TR-4597: VMware vSphere for ONTAP

Karl Konnerth, NetApp

NetApp ONTAP software has been a leading storage solution for VMware vSphere environments for almost two decades and continues to add innovative capabilities to simplify management while reducing costs. This document introduces the ONTAP solution for vSphere, including the latest product information and best practices, to streamline deployment, reduce risk, and simplify management.

Best practices supplement other documents such as guides and compatibility lists. They are developed based on lab testing and extensive field experience by NetApp engineers and customers. They might not be the only supported practices that work in every environment, but they are generally the simplest solutions that meet the needs of most customers.

This document is focused on capabilities in recent releases of ONTAP (9.x) running on vSphere 6.0 or later. See the section [ONTAP and vSphere release-specific information](#) for details related to specific releases.

## Why ONTAP for vSphere?

There are many reasons why tens of thousands of customers have selected ONTAP as their storage solution for vSphere, such as a unified storage system supporting both SAN and NAS protocols, robust data protection capabilities using space-efficient NetApp Snapshot copies, and a wealth of tools to help you manage application data. Using a storage system separate from the hypervisor allows you to offload many functions and maximize your investment in vSphere host systems. This approach not only makes sure your host resources are focused on application workloads, but it also avoids random performance effects on applications from storage operations.

Using ONTAP together with vSphere is a great combination that lets you reduce host hardware and VMware software expenses. You can also protect your data at lower cost with consistent high performance. Because virtualized workloads are mobile, you can explore different approaches using Storage vMotion to move VMs across VMFS, NFS, or vVols datastores, all on the same storage system.

Here are key factors customers value today:

- **Unified storage.** Systems running ONTAP software are unified in several significant ways. Originally this approach referred to both NAS and SAN protocols, and ONTAP continues to be a leading platform for SAN along with its original strength in NAS. In the vSphere world, this approach could also mean a unified system for virtual desktop infrastructure (VDI) together with virtual server infrastructure (VSI). Systems running ONTAP software are typically less expensive for VSI than traditional enterprise arrays and yet have advanced storage efficiency capabilities to handle VDI in the same system. ONTAP also unifies a variety of storage media, from SSDs to SATA, and can extend that easily into the cloud. There's no need to buy one flash array for performance, a SATA array for archives, and separate systems for the cloud. ONTAP ties them all together.
- **Virtual volumes and storage policy-based management.** NetApp was an early design partner with VMware in the development of vSphere Virtual Volumes (vVols), providing architectural input and early support for vVols and VMware vSphere APIs for Storage Awareness (VASA). Not only did this approach bring granular VM storage management to VMFS, it also supported automation of storage provisioning through storage policy-based management. This approach allows storage architects to design storage pools with different capabilities that can be easily consumed by VM administrators. ONTAP leads the storage industry in vVol scale, supporting hundreds of thousands of vVols in a single cluster, whereas enterprise array and smaller flash array vendors support as few as several thousand vVols per array. NetApp is also driving the evolution of granular VM management with upcoming capabilities in support of vVols 3.0.
- **Storage efficiency.** Although NetApp was the first to deliver deduplication for production workloads, this innovation wasn't the first or last one in this area. It started with ONTAP Snapshot copies, a space-efficient data protection mechanism with no performance effect, along with FlexClone technology to instantly make read/write copies of VMs for production and backup use. NetApp went on to deliver inline capabilities, including deduplication, compression, and zero-block deduplication, to squeeze out the most storage from expensive SSDs. Most recently, ONTAP added the ability to pack smaller I/O operations and files into a disk block using compaction. The combination of these capabilities has resulted in customers seeing savings of up to 5:1 for VSI and up to 30:1 for VDI.
- **Hybrid cloud.** Whether used for on-premises private cloud, public cloud infrastructure, or a hybrid cloud that combines the best of both, ONTAP solutions help you build your data fabric to streamline and optimize data management. Start with high-performance all-flash systems, then couple them with either disk or cloud storage systems for data protection and cloud compute. Choose from Azure, AWS, IBM, or Google clouds to optimize costs and avoid lock-in. Leverage advanced support for OpenStack and container technologies as needed. NetApp also offers cloud-based backup (SnapMirror Cloud, Cloud Backup

Service, and Cloud Sync) and storage tiering and archiving tools (FabricPool) for ONTAP to help reduce operating expenses and leverage the broad reach of the cloud.

- **And more.** Take advantage of the extreme performance of NetApp AFF A-Series arrays to accelerate your virtualized infrastructure while managing costs. Enjoy completely nondisruptive operations, from maintenance to upgrades to complete replacement of your storage system, using scale-out ONTAP clusters. Protect data at rest with NetApp encryption capabilities at no additional cost. Make sure performance meets business service levels through fine-grained quality of service capabilities. They are all part of the broad range of capabilities that come with ONTAP, the industry's leading enterprise data management software.

## ONTAP capabilities for vSphere

### Protocols

ONTAP supports all major storage protocols used for virtualization, such as iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), or Non-Volatile Memory Express over Fibre Channel (NVMe/FC) for SAN environments, as well as NFS (v3 and v4.1), and SMB or S3 for guest connections. Customers are free to pick what works best for their environment and can combine protocols as needed on a single system (for example, augmenting general use of NFS datastores with a few iSCSI LUNs or guest shares).

### Features

There are many ONTAP features that are useful for managing virtualized workloads. Some that require additional product licenses are described in the next section. Others packaged as standalone tools, some for ONTAP and others for the entire NetApp portfolio, are described after that.

Here are further details about base ONTAP features:

- **NetApp Snapshot copies.** ONTAP offers instant Snapshot copies of a VM or datastore with zero performance effect when you create or use a Snapshot copy. They can be used to create a restoration point for a VM prior to patching or for simple data protection. Note that these are different from VMware (consistency) snapshots. The easiest way to make an ONTAP Snapshot copy is to use the SnapCenter Plug-In for VMware vSphere to back up VMs and datastores.
- **Storage efficiency.** ONTAP supports inline and background deduplication and compression, zero-block deduplication, and data compaction.
- **Volume and LUN move.** Allows nondisruptive movement of volumes and LUNs supporting vSphere datastores and vVols within the ONTAP cluster to balance performance and capacity or support nondisruptive maintenance and upgrades.
- **QoS.** QoS allows for managing performance on an individual LUN, volume, or file. This function can be used to limit an unknown or busy VM or to make sure an important VM gets sufficient performance resources.
- **NetApp Volume Encryption, NetApp Aggregate Encryption.** NetApp encryption options offer easy software-based encryption to protect data at rest.
- **FabricPool.** This feature tiers colder data automatically at the block level to a separate object store, freeing up expensive flash storage.
- **REST, Ansible.** Use [ONTAP REST APIs](#) to automate storage and data management, and [Ansible modules](#) for configuration management of your ONTAP systems. Note that some ONTAP features are not well-suited for vSphere workloads. For example, FlexGroup prior to ONTAP 9.8 did not have full cloning support and was not tested with vSphere (see the FlexGroup section for the latest on using it with vSphere). FlexCache is also not optimal for vSphere as it is designed for read-mostly workloads. Writes can be problematic when the cache is disconnected from the origin, resulting in NFS datastore errors on both sides.

## ONTAP licensing

Some ONTAP features that are valuable for managing virtualized workloads require an additional license, whether available at no additional cost, in a license bundle, or a la carte. For many customers, the most cost-effective approach is with a license bundle. Here are the key licenses relevant to vSphere and how they are used:

- **FlexClone.** FlexClone enables instant, space-efficient clones of ONTAP volumes and files. This cloning is used when operations are offloaded to the storage system by VMware vSphere Storage APIs – Array Integration (VAAI), for backup verification and recovery (SnapCenter software), and for vVols cloning and Snapshot copies. Here is how they are used:
  - VAAI is supported with ONTAP for offloaded copy in support of vSphere clone and migration (Storage vMotion) operations. The FlexClone license allows for fast clones within a NetApp FlexVol volume, but, if not licensed, it still allows clones using slower block copies.
  - A FlexClone license is required for vVols functionality. It enables cloning of vVols within a single datastore or between datastores, and it enables vSphere-managed Snapshot copies of vVols, which are offloaded to the storage system.
- The storage replication adapter (SRA) is used with VMware Site Recovery Manager, and a FlexClone license is required to test recovery in both NAS and SAN environments. SRA may be used without FlexClone for discovery, recovery, and reprottection workflows.
- **SnapRestore.** SnapRestore technology enables instant recovery of a volume in place without copying data. It is required by NetApp backup and recovery tools such as SnapCenter where it is used to mount the datastore for verification and restore operations.
- **SnapMirror.** SnapMirror technology allows for simple, fast replication of data between ONTAP systems on-premises and in the cloud. SnapMirror supports the version flexibility of logical replication with the performance of block replication, sending only changed data to the secondary system. Data can be protected with mirror and/or vault policies, allowing for disaster recovery as well as long-term data retention for backup. SnapMirror supports asynchronous as well as synchronous relationships, and ONTAP 9.8 introduces transparent application failover with SnapMirror Business Continuity.

SnapMirror is required for SRA replication with Site Recovery Manager. It is also required for SnapCenter to enable replication of Snapshot copies to a secondary storage system.

- **SnapCenter.** SnapCenter software provides a unified, scalable platform and plug-in suite for application-consistent data protection and clone management. A SnapCenter license is included with the data protection license bundles for AFF and FAS systems. SnapCenter Plug-in for VMware vSphere is a free product if you are using the following storage systems: FAS, AFF, Cloud Volumes ONTAP, or ONTAP Select. However, SnapRestore and FlexClone licenses are required.
- **MetroCluster.** NetApp MetroCluster is a synchronous replication solution combining high availability and disaster recovery in a campus or metropolitan area to protect against both site disasters and hardware outages. It provides solutions with transparent recovery from failure, with zero data loss (0 RPO) and fast recovery (RTO within minutes). It is used in vSphere environments as part of a vSphere Metro Storage Cluster configuration.

## Virtualization tools for ONTAP

NetApp offers several standalone software tools that can be used together with ONTAP and vSphere to manage your virtualized environment. The following tools are included with the ONTAP license at no additional cost. See Figure 1 for a depiction of how these tools work together in your vSphere environment.

## **ONTAP tools for VMware vSphere**

ONTAP tools for VMware vSphere is a set of tools for using ONTAP storage together with vSphere. The vCenter plug-in, formerly known as the Virtual Storage Console (VSC), simplifies storage management and efficiency features, enhances availability, and reduces storage costs and operational overhead, whether you are using SAN or NAS. It uses best practices for provisioning datastores and optimizes ESXi host settings for NFS and block storage environments. For all these benefits, NetApp recommends using these ONTAP tools as a best practice when using vSphere with systems running ONTAP software. It includes both a server appliance and user interface extensions for vCenter.

## **NFS Plug-In for VMware VAAI**

The NetApp NFS Plug-In for VMware is a plug-in for ESXi hosts that allows them to use VAAI features with NFS datastores on ONTAP. It supports copy offload for clone operations, space reservation for thick virtual disk files, and Snapshot copy offload. Offloading copy operations to storage is not necessarily faster to complete, but it does offload host resources such as CPU cycles, buffers, and queues. You can use ONTAP tools for VMware vSphere to install the plug-in on ESXi hosts.

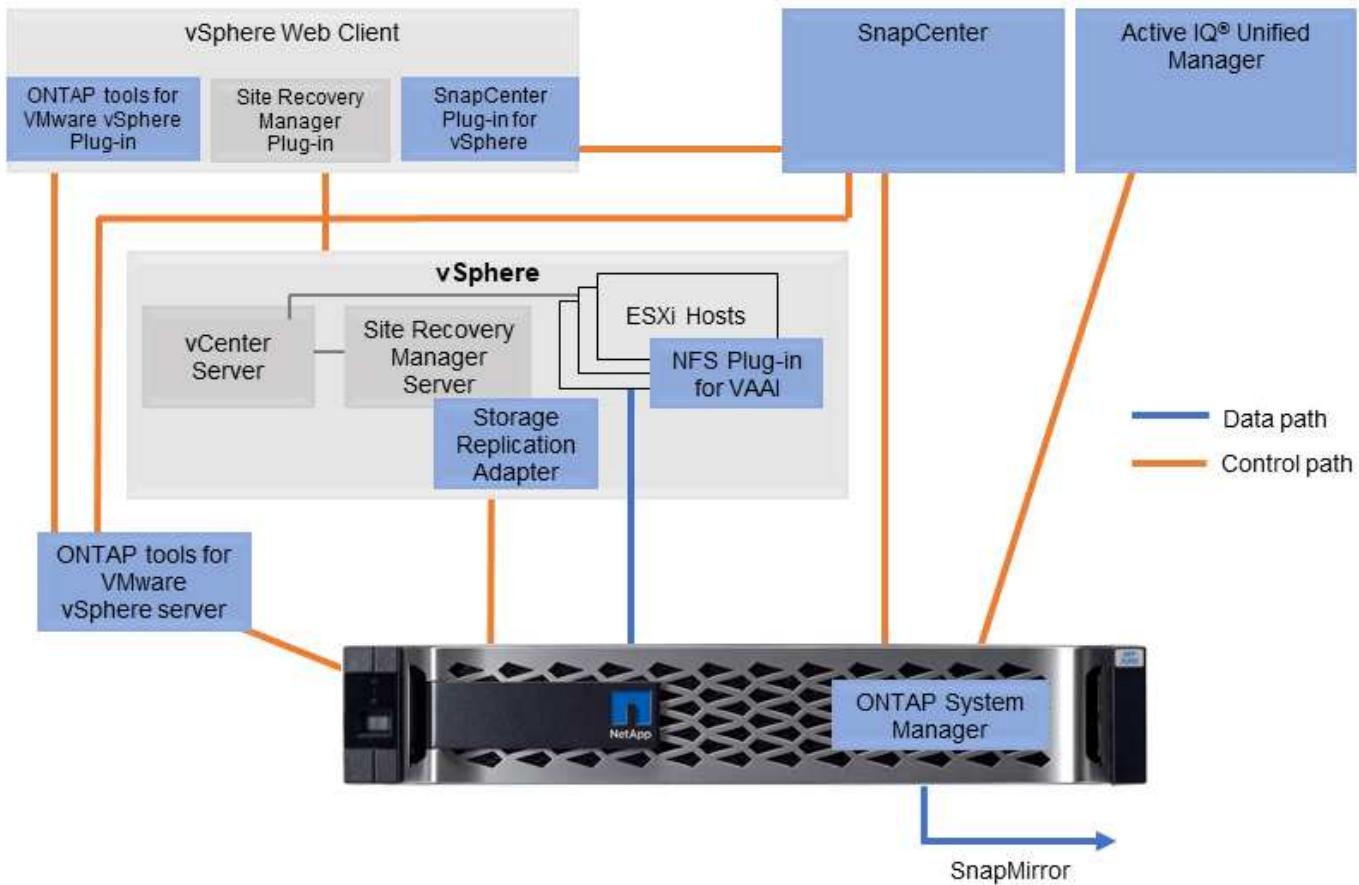
## **VASA Provider for ONTAP**

The VASA Provider for ONTAP supports the VMware vStorage APIs for Storage Awareness (VASA) framework. It is supplied as part of ONTAP tools for VMware vSphere as a single virtual appliance for ease of deployment. VASA Provider connects vCenter Server with ONTAP to aid in provisioning and monitoring VM storage. It enables VMware Virtual Volumes (vVols) support, management of storage capability profiles and individual VM vVols performance, and alarms for monitoring capacity and compliance with the profiles.

## **Storage Replication Adapter**

The SRA is used together with VMware Site Recovery Manager (SRM) to manage data replication between production and disaster recovery sites and test the DR replicas nondisruptively. It helps automate the tasks of discovery, recovery, and reprottection. It includes both an SRA server appliance and SRA adapters for the Windows SRM server and SRM appliance. The SRA is supplied as part of ONTAP tools for VMware vSphere.

The following figure depicts ONTAP tools for vSphere.



## Best practices

### vSphere datastore and protocol features

Five protocols are used to connect VMware vSphere to datastores on a system running ONTAP software:

- FC
- FCoE
- NVMe/FC
- iSCSI
- NFS

FC, FCoE, NVMe/FC, and iSCSI are block protocols that use the vSphere Virtual Machine File System (VMFS) to store VMs inside ONTAP LUNs or namespaces that are contained in an ONTAP volume. Note that, starting from vSphere 7.0, VMware no longer supports software FCoE in production environments. NFS is a file protocol that places VMs into datastores (which are simply ONTAP volumes) without the need for VMFS. SMB, iSCSI, or NFS can also be used directly from a guest OS to ONTAP.

The following tables presents vSphere supported traditional datastore features with ONTAP. This information does not apply to vVols datastores, but it does generally applies to vSphere 6.x and 7.x releases using supported ONTAP releases. You can also consult [VMware Configuration Maximums](#) for specific vSphere releases to confirm specific limits.

Capability/Feature	FC/FCoE	iSCSI	NFS
Format	VMFS or raw device mapping (RDM)	VMFS or RDM	N/A
Maximum number of datastores or LUNs	256 targets/HBA	256 targets	256 mounts Default NFS. MaxVolumes is 8. Use ONTAP tools for VMware vSphere to increase to 256.
Maximum datastore size	64TB	64TB	100TB FlexVol volume or greater with FlexGroup volume
Maximum datastore file size (for VMDKs using vSphere version 5.5 and VMFS 5 or later)	62TB	62TB	16TB 62TB is the maximum size supported by vSphere.
Optimal queue depth per LUN or file system	64	64	N/A

The following table lists supported VMware storage-related functionalities.

Capacity/Feature	FC/FCoE	iSCSI	NFS
vMotion	Yes	Yes	Yes
Storage vMotion	Yes	Yes	Yes
VMware HA	Yes	Yes	Yes
Storage Distributed Resource Scheduler (SDRS)	Yes	Yes	Yes
VMware vStorage APIs for Data Protection (VADP)—enabled backup software	Yes	Yes	Yes
Microsoft Cluster Service (MSCS) or failover clustering within a VM	Yes	Yes*	Not supported
Fault Tolerance	Yes	Yes	Yes
Site Recovery Manager	Yes	Yes	Yes
Thin-provisioned VMs (virtual disks)	Yes	Yes	Yes This setting is the default for all VMs on NFS when not using VAAI.
VMware native multipathing	Yes	Yes	N/A

\*NetApp recommends using in-guest iSCSI for Microsoft clusters rather than multi-writer enabled VMDKs in a

VMFS datastore. This approach is fully supported by Microsoft and VMware, offers great flexibility with ONTAP (SnapMirror to ONTAP systems on-premises or in the cloud), is easy to configure and automate, and can be protected with SnapCenter. vSphere 7 adds a new clustered VMDK option. This is different from multi-writer enabled VMDKs but requires a datastore presented via the FC protocol, which has clustered VMDK support enabled. Other restrictions apply. See VMware's [Setup for Windows Server Failover Clustering](#) documentation for configuration guidelines.

The following table lists supported ONTAP storage management features.

Capability/Feature	FC/FCoE	iSCSI	NFS
Data deduplication	Savings in the array	Savings in the array	Savings in the datastore
Thin provisioning	Datastore or RDM	Datastore or RDM	Datastore
Resize datastore	Grow only	Grow only	Grow, autogrow, and shrink
SnapCenter plug-ins for Windows, Linux applications (in guest)	Yes	Yes	Yes
Monitoring and host configuration using ONTAP tools for VMware vSphere	Yes	Yes	Yes
Provisioning using ONTAP tools for VMware vSphere	Yes	Yes	Yes

The following table lists supported backup features.

Capability/Feature	FC/FCoE	iSCSI	NFS
ONTAP Snapshot copies	Yes	Yes	Yes
SRM supported by replicated backups	Yes	Yes	Yes
Volume SnapMirror	Yes	Yes	Yes
VMDK image access	VADP-enabled backup software	VADP-enabled backup software	VADP-enabled backup software, vSphere Client, and vSphere Web Client datastore browser
VMDK file-level access	VADP-enabled backup software, Windows only	VADP-enabled backup software, Windows only	VADP-enabled backup software and third-party applications
NDMP granularity	Datastore	Datastore	Datastore or VM

#### Selecting a storage protocol

Systems running ONTAP software support all major storage protocols, so customers can choose what is best for their environment, depending on existing and planned networking infrastructure and staff skills. NetApp testing has generally shown little difference between protocols running at similar line speeds, so it is best to focus on your network infrastructure and staff capabilities over raw protocol performance.

The following factors might be useful in considering a choice of protocol:

- **Current customer environment.** Although IT teams are generally skilled at managing Ethernet IP infrastructure, not all are skilled at managing an FC SAN fabric. However, using a general-purpose IP network that's not designed for storage traffic might not work well. Consider the networking infrastructure you have in place, any planned improvements, and the skills and availability of staff to manage them.
- **Ease of setup.** Beyond initial configuration of the FC fabric (additional switches and cabling, zoning, and the interoperability verification of HBA and firmware), block protocols also require creation and mapping of LUNs and discovery and formatting by the guest OS. After the NFS volumes are created and exported, they are mounted by the ESXi host and ready to use. NFS has no special hardware qualification or firmware to manage.
- **Ease of management.** With SAN protocols, if more space is needed, several steps are necessary, including growing a LUN, rescanning to discover the new size, and then growing the file system). Although growing a LUN is possible, reducing the size of a LUN is not, and recovering unused space can require additional effort. NFS allows easy sizing up or down, and this resizing can be automated by the storage system. SAN offers space reclamation through guest OS TRIM/UNMAP commands, allowing space from deleted files to be returned to the array. This type of space reclamation is more difficult with NFS datastores.
- **Storage space transparency.** Storage utilization is typically easier to see in NFS environments because thin provisioning returns savings immediately. Likewise, deduplication and cloning savings are immediately available for other VMs in the same datastore or for other storage system volumes. VM density is also typically greater in an NFS datastore, which can improve deduplication savings as well as reduce management costs by having fewer datastores to manage.

## Datastore layout

ONTAP storage systems offer great flexibility in creating datastores for VMs and virtual disks. Although many ONTAP best practices are applied when using the VSC to provision datastores for vSphere (listed in the section [Recommended ESXi host and other ONTAP settings](#)), here are some additional guidelines to consider:

- Deploying vSphere with ONTAP NFS datastores results in a high-performing, easy-to-manage implementation that provides VM-to-datastore ratios that cannot be obtained with block-based storage protocols. This architecture can result in a tenfold increase in datastore density with a correlating reduction in the number of datastores. Although a larger datastore can benefit storage efficiency and provide operational benefits, consider using at least four datastores (FlexVol volumes) to store your VMs on a single ONTAP controller to get maximum performance from the hardware resources. This approach also allows you to establish datastores with different recovery policies. Some can be backed up or replicated more frequently than others, based on business needs. Multiple datastores are not required with FlexGroup volumes for performance as it scales by design.
- NetApp recommends the use of FlexVol volumes and, starting with ONTAP 9.8 FlexGroup volumes, NFS datastores. Other ONTAP storage containers such as qtrees are not generally recommended because these are not currently supported by ONTAP tools for VMware vSphere. Deploying datastores as multiple qtrees in a single volume might be useful for highly automated environments that can benefit from datastore-level quotas or VM file clones.
- A good size for a FlexVol volume datastore is around 4TB to 8TB. This size is a good balance point for performance, ease of management, and data protection. Start small (say, 4TB) and grow the datastore as needed (up to the maximum 100TB). Smaller datastores are faster to recover from backup or after a disaster and can be moved quickly across the cluster. Consider the use of ONTAP autosize to automatically grow and shrink the volume as used space changes. The ONTAP tools for VMware vSphere Datastore Provisioning Wizard use autosize by default for new datastores. Additional customization of the grow and shrink thresholds and maximum and minimum size can be done with System Manager or the command line.

- Alternately, VMFS datastores can be configured with LUNs that are accessed by FC, iSCSI, or FCoE. VMFS allows traditional LUNs to be accessed simultaneously by every ESX server in a cluster. VMFS datastores can be up to 64TB in size and consist of up to 32 2TB LUNs (VMFS 3) or a single 64TB LUN (VMFS 5). The ONTAP maximum LUN size is 16TB on most systems, and 128TB on All SAN Array systems. Therefore, a maximum size VMFS 5 datastore on most ONTAP systems can be created by using four 16TB LUNs. While there can be performance benefit for high-I/O workloads with multiple LUNs (with high-end FAS or AFF systems), this benefit is offset by added management complexity to create, manage, and protect the datastore LUNs and increased availability risk. NetApp generally recommends using a single, large LUN for each datastore and only span if there is a special need to go beyond a 16TB datastore. As with NFS, consider using multiple datastores (volumes) to maximize performance on a single ONTAP controller.
- Older guest operating systems (OSs) needed alignment with the storage system for best performance and storage efficiency. However, modern vendor-supported OSs from Microsoft and Linux distributors such as Red Hat no longer require adjustments to align the file system partition with the blocks of the underlying storage system in a virtual environment. If you are using an old OS that might require alignment, search the NetApp Support Knowledgebase for articles using “VM alignment” or request a copy of TR-3747 from a NetApp sales or partner contact.
- Avoid the use of defragmentation utilities within the guest OS, as this offers no performance benefit and affects storage efficiency and Snapshot copy space usage. Also consider turning off search indexing in the guest OS for virtual desktops.
- ONTAP has led the industry with innovative storage efficiency features, allowing you to get the most out of your usable disk space. AFF systems take this efficiency further with default inline deduplication and compression. Data is deduplicated across all volumes in an aggregate, so you no longer need to group similar operating systems and similar applications within a single datastore to maximize savings.
- In some cases, you might not even need a datastore. For the best performance and manageability, avoid using a datastore for high-I/O applications such as databases and some applications. Instead, consider guest-owned file systems such as NFS or iSCSI file systems managed by the guest or with RDMS. For specific application guidance, see NetApp technical reports for your application. For example, [TR-3633: Oracle Databases on Data ONTAP](#) has a section about virtualization with helpful details.
- First Class Disks (or Improved Virtual Disks) allow for vCenter-managed disks independent of a VM with vSphere 6.5 and later. While primarily managed by API, they can be useful with vVols, especially when managed by OpenStack or Kubernetes tools. They are supported by ONTAP as well as ONTAP tools for VMware vSphere.

### Datastore and VM migration

When migrating VMs from an existing datastore on another storage system to ONTAP, here are some practices to keep in mind:

- Use Storage vMotion to move the bulk of your virtual machines to ONTAP. Not only is this approach nondisruptive to running VMs, it also allows ONTAP storage efficiency features such as inline deduplication and compression to process the data as it migrates. Consider using vCenter capabilities to select multiple VMs from the inventory list and then schedule the migration (use Ctrl key while clicking Actions) at an appropriate time.
- While you could carefully plan a migration to appropriate destination datastores, it is often simpler to migrate in bulk and then organize later as needed. If you have specific data protection needs, such as different Snapshot schedules, you might want to use this approach to guide your migration to different datastores.
- Most VMs and their storage may be migrated while running (hot), but migrating attached (not in datastore) storage such as ISOs, LUNs, or NFS volumes from another storage system might require cold migration.
- Virtual machines that need more careful migration include databases and applications that use attached

storage. In general, consider the use of the application's tools to manage migration. For Oracle, consider using Oracle tools such as RMAN or ASM to migrate the database files. See [TR-4534](#) for more information. Likewise, for SQL Server, consider using either SQL Server Management Studio or NetApp tools such as SnapManager for SQL Server or SnapCenter.

### ONTAP tools for VMware vSphere

The most important best practice when using vSphere with systems running ONTAP software is to install and use the ONTAP tools for VMware vSphere plug-in (formerly known as Virtual Storage Console). This vCenter plug-in simplifies storage management, enhances availability, and reduces storage costs and operational overhead, whether using SAN or NAS. It uses best practices for provisioning datastores and optimizes ESXi host settings for multipath and HBA timeouts (these are described in Appendix B). Because it's a vCenter plug-in, it's available to all vSphere web clients that connect to the vCenter server.

The plug-in also helps you use other ONTAP tools in vSphere environments. It allows you to install the NFS Plug-In for VMware VAAI, which enables copy offload to ONTAP for VM cloning operations, space reservation for thick virtual disk files, and ONTAP Snapshot copy offload.

The plug-in is also the management interface for many functions of the VASA Provider for ONTAP, supporting storage policy-based management with vVols. After ONTAP tools for VMware vSphere is registered, use it to create storage capability profiles, map them to storage, and make sure of datastore compliance with the profiles over time. The VASA Provider also provides an interface to create and manage vVol datastores.

In general, NetApp recommends using the ONTAP tools for VMware vSphere interface within vCenter to provision traditional and vVols datastores to make sure best practices are followed.

### General Networking

Configuring network settings when using vSphere with systems running ONTAP software is straightforward and similar to other network configuration. Here are some things to consider:

- Separate storage network traffic from other networks. A separate network can be achieved by using a dedicated VLAN or separate switches for storage. If the storage network shares physical paths such as uplinks, you might need QoS or additional uplink ports to make sure of sufficient bandwidth. Don't connect hosts directly to storage; use switches to have redundant paths and allow VMware HA to work without intervention.
- Jumbo frames can be used if desired and supported by your network, especially when using iSCSI. If they are used, make sure they are configured identically on all network devices, VLANs, and so on in the path between storage and the ESXi host. Otherwise, you might see performance or connection problems. The MTU must also be set identically on the ESXi virtual switch, the VMkernel port, and also on the physical ports or interface groups of each ONTAP node.
- NetApp only recommends disabling network flow control on the cluster network ports within an ONTAP cluster. NetApp makes no other recommendations for best practices for the remaining network ports used for data traffic. You should enable or disable as necessary. See [TR-4182](#) for more background on flow control.
- When ESXi and ONTAP storage arrays are connected to Ethernet storage networks, NetApp recommends configuring the Ethernet ports to which these systems connect as Rapid Spanning Tree Protocol (RSTP) edge ports or by using the Cisco PortFast feature. NetApp recommends enabling the Spanning-Tree PortFast trunk feature in environments that use the Cisco PortFast feature and that have 802.1Q VLAN trunking enabled to either the ESXi server or the ONTAP storage arrays.
- NetApp recommends the following best practices for link aggregation:
  - Use switches that support link aggregation of ports on two separate switch chassis, using a multichassis link aggregation group approach such as Cisco's Virtual PortChannel (vPC).

- Disable LACP for switch ports connected to ESXi unless using dvSwitches 5.1 or later with LACP configured.
- Use LACP to create link aggregates for ONTAP storage systems, with dynamic multimode interface groups with IP hash.
- Use IP hash teaming policy on ESXi.

The following table provides a summary of network configuration items and indicates where the settings are applied.

Item	ESXi	Switch	Node	SVM
IP address	VMkernel	No**	No**	Yes
Link aggregation	Virtual switch	Yes	Yes	No*
VLAN	VMkernel and VM port groups	Yes	Yes	No*
Flow control	NIC	Yes	Yes	No*
Spanning tree	No	Yes	No	No
MTU (for jumbo frames)	Virtual switch and VMkernel port (9000)	Yes (set to max)	Yes (9000)	No*
Failover groups	No	No	Yes (create)	Yes (select)

\*SVM LIFs connect to ports, interface groups, or VLAN interfaces that have VLAN, MTU, and other settings, but the settings are not managed at the SVM level.

\*\*These devices have IP addresses of their own for management, but these addresses are not used in the context of ESXi storage networking.

#### **SAN (FC, FCoE, NVMe/FC, iSCSI), RDM**

In vSphere, there are three ways to use block storage LUNs:

- With VMFS datastores
- With raw device mapping (RDM)
- As a LUN accessed and controlled by a software initiator from a VM guest OS

VMFS is a high-performance clustered file system that provides datastores that are shared storage pools. VMFS datastores can be configured with LUNs that are accessed using FC, iSCSI, FCoE, or NVMe namespaces accessed by the NVMe/FC protocol. VMFS allows traditional LUNs to be accessed simultaneously by every ESX server in a cluster. The ONTAP maximum LUN size is generally 16TB; therefore, a maximum-size VMFS 5 datastore of 64TB (see the first table in this section) is created by using four 16TB LUNs (All SAN Array systems support the maximum VMFS LUN size of 64TB). Because the ONTAP LUN architecture does not have small individual queue depths, VMFS datastores in ONTAP can scale to a greater degree than with traditional array architectures in a relatively simple manner.

vSphere includes built-in support for multiple paths to storage devices, referred to as native multipathing (NMP). NMP can detect the type of storage for supported storage systems and automatically configures the NMP stack to support the capabilities of the storage system in use.

Both NMP and NetApp ONTAP support Asymmetric Logical Unit Access (ALUA) to negotiate optimized and nonoptimized paths. In ONTAP, an ALUA-optimized path follows a direct data path, using a target port on the node that hosts the LUN being accessed. ALUA is turned on by default in both vSphere and ONTAP. The NMP recognizes the ONTAP cluster as ALUA, and it uses the ALUA storage array type plug-in (`VMW_SATP_ALUA`) and selects the round robin path selection plug-in (`VMW_PSP_RR`).

ESXi 6 supports up to 256 LUNs and up to 1,024 total paths to LUNs. Any LUNs or paths beyond these limits are not seen by ESXi. Assuming the maximum number of LUNs, the path limit allows four paths per LUN. In a larger ONTAP cluster, it is possible to reach the path limit before the LUN limit. To address this limitation, ONTAP supports selective LUN map (SLM) in release 8.3 and later.

SLM limits the nodes that advertise paths to a given LUN. It is a NetApp best practice to have at least one LIF per node per SVM and to use SLM to limit the paths advertised to the node hosting the LUN and its HA partner. Although other paths exist, they aren't advertised by default. It is possible to modify the paths advertised with the add and remove reporting node arguments within SLM. Note that LUNs created in releases prior to 8.3 advertise all paths and need to be modified to only advertise the paths to the hosting HA pair. For more information about SLM, review section 5.9 of [TR-4080](#). The previous method of portsets can also be used to further reduce the available paths for a LUN. Portsets help by reducing the number of visible paths through which initiators in an igroup can see LUNs.

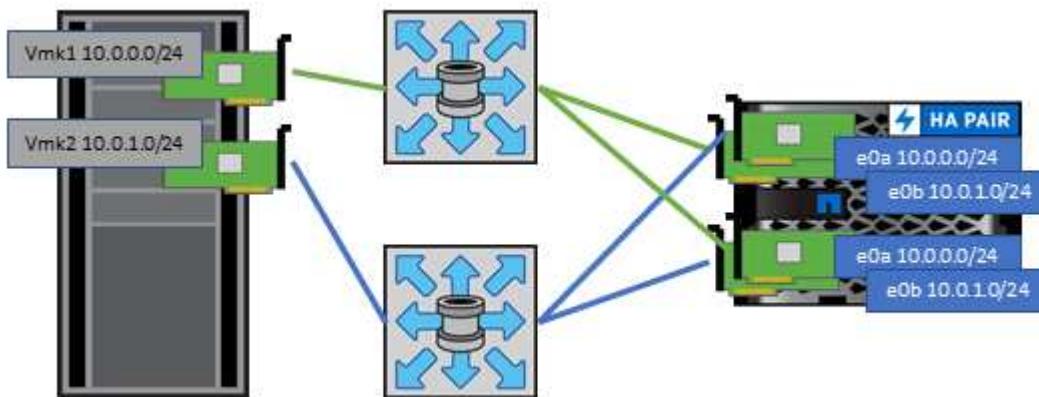
- SLM is enabled by default. Unless you are using portsets, no additional configuration is required.
- For LUNs created prior to Data ONTAP 8.3, manually apply SLM by running the `lun mapping remove-reporting-nodes` command to remove the LUN reporting nodes and restrict LUN access to the LUN-owning node and its HA partner.

Block protocols (iSCSI, FC, and FCoE) access LUNs by using LUN IDs and serial numbers, along with unique names. FC and FCoE use worldwide names (WWNNs and WWPNs), and iSCSI uses iSCSI qualified names (IQNs). The path to LUNs inside the storage is meaningless to the block protocols and is not presented anywhere in the protocol. Therefore, a volume that contains only LUNs does not need to be internally mounted at all, and a junction path is not needed for volumes that contain LUNs used in datastores. The NVMe subsystem in ONTAP works similarly.

Other best practices to consider:

- Make sure that a logical interface (LIF) is created for each SVM on each node in the ONTAP cluster for maximum availability and mobility. ONTAP SAN best practice is to use two physical ports and LIFs per node, one for each fabric. ALUA is used to parse paths and identify active optimized (direct) paths versus active nonoptimized paths. ALUA is used for FC, FCoE, and iSCSI.
- For iSCSI networks, use multiple VMkernel network interfaces on different network subnets with NIC teaming when multiple virtual switches are present. You can also use multiple physical NICs connected to multiple physical switches to provide HA and increased throughput. The following figure provides an example of multipath connectivity. In ONTAP, configure either a single-mode interface group for failover with two or more links that are connected to two or more switches, or use LACP or other link-aggregation technology with multimode interface groups to provide HA and the benefits of link aggregation.
- If the Challenge-Handshake Authentication Protocol (CHAP) is used in ESXi for target authentication, it must also be configured in ONTAP using the CLI (`vserver iscsi security create`) or with System Manager (edit Initiator Security under Storage > SVMs > SVM Settings > Protocols > iSCSI).
- Use ONTAP tools for VMware vSphere to create and manage LUNs and igroups. The plug-in automatically determines the WWPNs of servers and creates appropriate igroups. It also configures LUNs according to best practices and maps them to the correct igroups.
- Use RDMS with care because they can be more difficult to manage, and they also use paths, which are limited as described earlier. ONTAP LUNs support both [physical and virtual compatibility mode RDMS](#).

- For more on using NVMe/FC with vSphere 7.0, see this [ONTAP NVMe/FC Host Configuration guide](#) and [TR-4684](#). The following figure depicts multipath connectivity from a vSphere host to an ONTAP LUN.



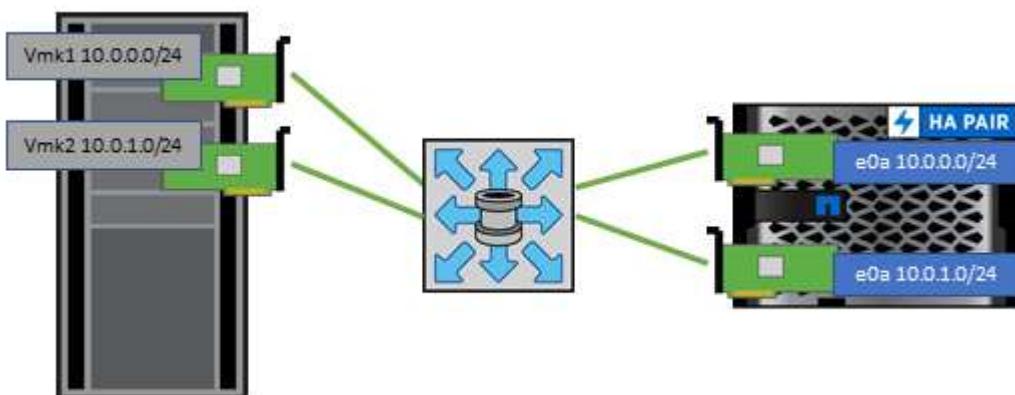
## NFS

vSphere allows customers to use enterprise-class NFS arrays to provide concurrent access to datastores to all the nodes in an ESXi cluster. As mentioned in the datastore section, there are some ease of use and storage efficiency visibility benefits when using NFS with vSphere.

The following best practices are recommended when using ONTAP NFS with vSphere:

- Use a single logical interface (LIF) for each SVM on each node in the ONTAP cluster. Past recommendations of a LIF per datastore are no longer necessary. While direct access (LIF and datastore on same node) is best, don't worry about indirect access because the performance effect is generally minimal (microseconds).
- VMware has supported NFSv3 since VMware Infrastructure 3. vSphere 6.0 added support for NFSv4.1, which enables some advanced capabilities such as Kerberos security. Where NFSv3 uses client-side locking, NFSv4.1 uses server-side locking. Although an ONTAP volume can be exported through both protocols, ESXi can only mount through one protocol. This single protocol mount does not preclude other ESXi hosts from mounting the same datastore through a different version. Make sure to specify the protocol version to use when mounting so that all hosts use the same version and, therefore, the same locking style. Do not mix NFS versions across hosts. If possible, use host profiles to check compliancy.
  - Because there is no automatic datastore conversion between NFSv3 and NFSv4.1, create a new NFSv4.1 datastore and use Storage vMotion to migrate VMs to the new datastore.
  - Please refer to the NFS v4.1 Interoperability table notes in the [NetApp Interoperability Matrix tool](#) for specific ESXi patch levels required for support.
- NFS export policies are used to control access by vSphere hosts. You can use one policy with multiple volumes (datastores). With NFSv3, ESXi uses the sys (UNIX) security style and requires the root mount option to execute VMs. In ONTAP, this option is referred to as superuser, and when the superuser option is used, it is not necessary to specify the anonymous user ID. Note that export policy rules with different values for -anon and -allow-suid can cause SVM discovery problems with the ONTAP tools. Here's a sample policy:
  - Access Protocol: nfs3
  - Client Match Spec: 192.168.42.21
  - RO Access Rule: sys
  - RW Access Rule: sys

- Anonymous UID:
- Superuser: sys
- If the NetApp NFS Plug-In for VMware VAAI is used, the protocol should be set as nfs when the export policy rule is created or modified. The NFSv4 protocol is required for VAAI copy offload to work, and specifying the protocol as nfs automatically includes both the NFSv3 and the NFSv4 versions.
- NFS datastore volumes are junctioned from the root volume of the SVM; therefore, ESXi must also have access to the root volume to navigate and mount datastore volumes. The export policy for the root volume, and for any other volumes in which the datastore volume's junction is nested, must include a rule or rules for the ESXi servers granting them read-only access. Here's a sample policy for the root volume, also using the VAAI plug-in:
  - Access Protocol. nfs (which includes both nfs3 and nfs4)
  - Client Match Spec. 192.168.42.21
  - RO Access Rule. sys
  - RW Access Rule. never (best security for root volume)
  - Anonymous UID.
  - Superuser. sys (also required for root volume with VAAI)
- Use ONTAP tools for VMware vSphere (the most important best practice):
  - Use ONTAP tools for VMware vSphere to provision datastores because it simplifies management of export policies automatically.
  - When creating datastores for VMware clusters with the plug-in, select the cluster rather than a single ESX server. This choice triggers it to automatically mount the datastore to all hosts in the cluster.
  - Use the plug-in mount function to apply existing datastores to new servers.
  - When not using ONTAP tools for VMware vSphere, use a single export policy for all servers or for each cluster of servers where additional access control is needed.
- Although ONTAP offers a flexible volume namespace structure to arrange volumes in a tree using junctions, this approach has no value for vSphere. It creates a directory for each VM at the root of the datastore, regardless of the namespace hierarchy of the storage. Thus, the best practice is to simply mount the junction path for volumes for vSphere at the root volume of the SVM, which is how ONTAP tools for VMware vSphere provisions datastores. Not having nested junction paths also means that no volume is dependent on any volume other than the root volume and that taking a volume offline or destroying it, even intentionally, does not affect the path to other volumes.
- A block size of 4K is fine for NTFS partitions on NFS datastores. The following figure depicts connectivity from a vSphere host to an ONTAP NFS datastore.



The following table lists NFS versions and supported features.

vSphere Features	NFSv3	NFSv4.1
vMotion and Storage vMotion	Yes	Yes
High availability	Yes	Yes
Fault tolerance	Yes	Yes
DRS	Yes	Yes
Host profiles	Yes	Yes
Storage DRS	Yes	No
Storage I/O control	Yes	No
SRM	Yes	No
Virtual volumes	Yes	No
Hardware acceleration (VAAI)	Yes	Yes (vSphere 6.5 and later, NetApp VAAI Plug-in 1.1.2)
Kerberos authentication	No	Yes (enhanced with vSphere 6.5 and later to support AES, krb5i)
Multipathing support	No	No (ESXi 6.5 and later supports through session trunking; ONTAP supports through pNFS)

### FlexGroup

ONTAP 9.8 adds support for FlexGroup datastores in vSphere, along with the ONTAP tools for VMware vSphere 9.8 release. FlexGroup simplifies the creation of large datastores and automatically creates a number of constituent volumes to get maximum performance from an ONTAP system. Use FlexGroup with vSphere for a single, scalable vSphere datastore with the power of a full ONTAP cluster.

In addition to extensive system testing with vSphere workloads, ONTAP 9.8 also adds a new copy offload mechanism for FlexGroup datastores. This uses an improved copy engine to copy files between constituents in the background while allowing access on both source and destination. Multiple copies use instantly available, space-efficient file clones within a constituent when needed based on scale.

ONTAP 9.8 also adds new file-based performance metrics (IOPS, throughput, and latency) for FlexGroup files, and these metrics can be viewed in the ONTAP tools for VMware vSphere dashboard and VM reports. The ONTAP tools for VMware vSphere plug-in also allows you to set Quality of Service (QoS) rules using a combination of maximum and/or minimum IOPS. These can be set across all VMs in a datastore or individually for specific VMs.

Here are some additional best practices that NetApp has developed:

- Use FlexGroup provisioning defaults. While ONTAP tools for VMware vSphere is recommended because it creates and mounts the FlexGroup within vSphere, ONTAP System Manager or the command line might be used for special needs. Even then, use the defaults such as the number of constituent members per node because this is what has been tested with vSphere.
- When sizing a FlexGroup datastore, keep in mind that the FlexGroup consists of multiple smaller FlexVol volumes that create a larger namespace. As such, size the datastore to be at least 8x the size of your largest virtual machine. For example, if you have a 6TB VM in your environment, size the FlexGroup

datastore no smaller than 48TB.

- Allow FlexGroup to manage datastore space. Autosize and Elastic Sizing have been tested with vSphere datastores. Should the datastore get close to full capacity, use ONTAP tools for VMware vSphere or another tool to resize the FlexGroup volume. FlexGroup keeps capacity and inodes balanced across constituents, prioritizing files within a folder (VM) to the same constituent if capacity allows.
- VMware and NetApp do not currently support a common multipath networking approach. For NFSv4.1, NetApp supports pNFS, whereas VMware supports session trunking. NFSv3 does not support multiple physical paths to a volume. For FlexGroup with ONTAP 9.8, our recommended best practice is to let ONTAP tools for VMware vSphere make the single mount, because the effect of indirect access is typically minimal (microseconds). It's possible to use round-robin DNS to distribute ESXi hosts across LIFs on different nodes in the FlexGroup, but this would require the FlexGroup to be created and mounted without ONTAP tools for VMware vSphere. Then the performance management features would not be available.
- FlexGroup vSphere datastore support has been tested up to 1500 VMs with the 9.8 release.
- Use the NFS Plug-In for VMware VAAI for copy offload. Note that while cloning is enhanced within a FlexGroup datastore, ONTAP does not provide significant performance advantages versus ESXi host copy when copying VMs between FlexVol and/or FlexGroup volumes.
- Use ONTAP tools for VMware vSphere 9.8 to monitor performance of FlexGroup VMs using ONTAP metrics (dashboard and VM reports), and to manage QoS on individual VMs. These metrics are not currently available through ONTAP commands or APIs.
- QoS (max/min IOPS) can be set on individual VMs or on all VMs in a datastore at that time. Setting QoS on all VMs replaces any separate per-VM settings. Settings do not extend to new or migrated VMs in the future; either set QoS on the new VMs or re-apply QoS to all VMs in the datastore.
- SnapCenter Plug-In for VMware vSphere release 4.4 supports backup and recovery of VMs in a FlexGroup datastore on the primary storage system. While SnapMirror may be used manually to replicate a FlexGroup to a secondary system, SCV 4.4 does not manage the secondary copies.

## Other capabilities for vSphere

### Data protection

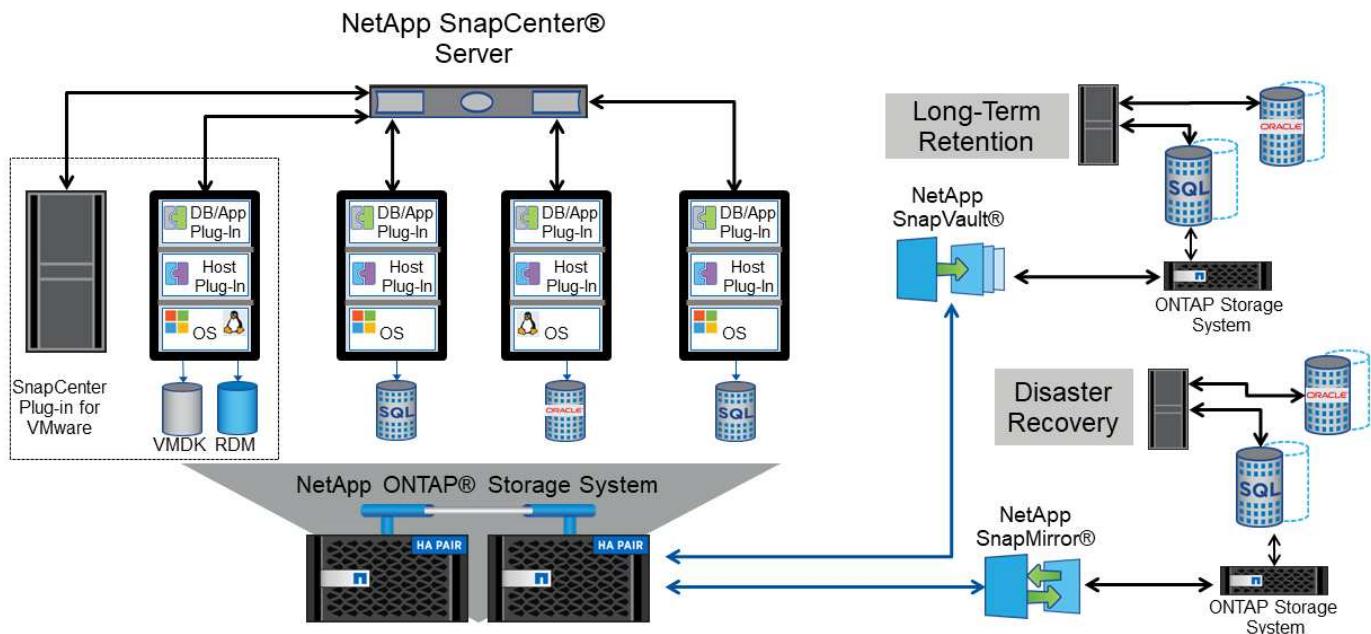
Backing up your VMs and quickly recovering them are among the great strengths of ONTAP for vSphere, and it is easy to manage this ability inside vCenter with the SnapCenter Plug-In for VMware vSphere. Use Snapshot copies to make quick copies of your VM or datastore without affecting performance, and then send them to a secondary system using SnapMirror for longer-term off-site data protection. This approach minimizes storage space and network bandwidth by only storing changed information.

SnapCenter allows you to create backup policies that can be applied to multiple jobs. These policies can define schedule, retention, replication, and other capabilities. They continue to allow optional selection of VM-consistent snapshots, which leverages the hypervisor's ability to quiesce I/O before taking a VMware snapshot. However, due to the performance effect of VMware snapshots, they are generally not recommended unless you need the guest file system to be quiesced. Instead, use ONTAP Snapshot copies for general protection, and use application tools such as SnapCenter plug-ins to protect transactional data such as SQL Server or Oracle. These Snapshot copies are different from VMware (consistency) snapshots and are suitable for longer term protection. VMware snapshots are only [recommended](#) for short term use due to performance and other effects.

These plug-ins offer extended capabilities to protect the databases in both physical and virtual environments. With vSphere, you can use them to protect SQL Server or Oracle databases where data is stored on RDM LUNs, iSCSI LUNs directly connected to the guest OS, or VMDK files on either VMFS or NFS datastores. The plug-ins allow specification of different types of database backups, supporting online or offline backup, and protecting database files along with log files. In addition to backup and recovery, the plug-ins also support

cloning of databases for development or test purposes.

The following figure depicts an example of SnapCenter deployment.



For enhanced disaster recovery capabilities, consider using the NetApp SRA for ONTAP with VMware Site Recovery Manager. In addition to support for the replication of datastores to a DR site, it also enables nondisruptive testing in the DR environment by cloning the replicated datastores. Recovery from a disaster and reprotecting production after the outage has been resolved are also made easy by automation built into SRA.

Finally, for the highest level of data protection, consider a VMware vSphere Metro Storage Cluster (vMSC) configuration using NetApp MetroCluster. vMSC is a VMware-certified solution that combines synchronous replication with array-based clustering, giving the same benefits of a high-availability cluster but distributed across separate sites to protect against site disaster. NetApp MetroCluster offers cost-effective configurations for synchronous replication with transparent recovery from any single storage component failure as well as single-command recovery in the event of a site disaster. vMSC is described in greater detail in [TR-4128](#).

#### Space reclamation

Space can be reclaimed for other uses when VMs are deleted from a datastore. When using NFS datastores, space is reclaimed immediately when a VM is deleted (of course, this approach only makes sense when the volume is thin provisioned, that is, the volume guarantee is set to none). However, when files are deleted within the VM guest OS, space is not automatically reclaimed with an NFS datastore. For LUN-based VMFS datastores, ESXi as well as the guest OS can issue VAAI UNMAP primitives to the storage (again, when using thin provisioning) to reclaim space. Depending on the release, this support is either manual or automatic.

In vSphere 5.5 and later, the `vmkfstools -y` command is replaced by the `esxcli storage vmfs unmap` command, which specifies the number of free blocks (see VMware KB [2057513](#) for more info). In vSphere 6.5 and later when using VMFS 6, space should be automatically reclaimed asynchronously (see [Storage Space Reclamation](#) in the vSphere documentation), but can also be run manually if needed. This automatic UNMAP is supported by ONTAP, and ONTAP tools for VMware vSphere sets it to low priority.

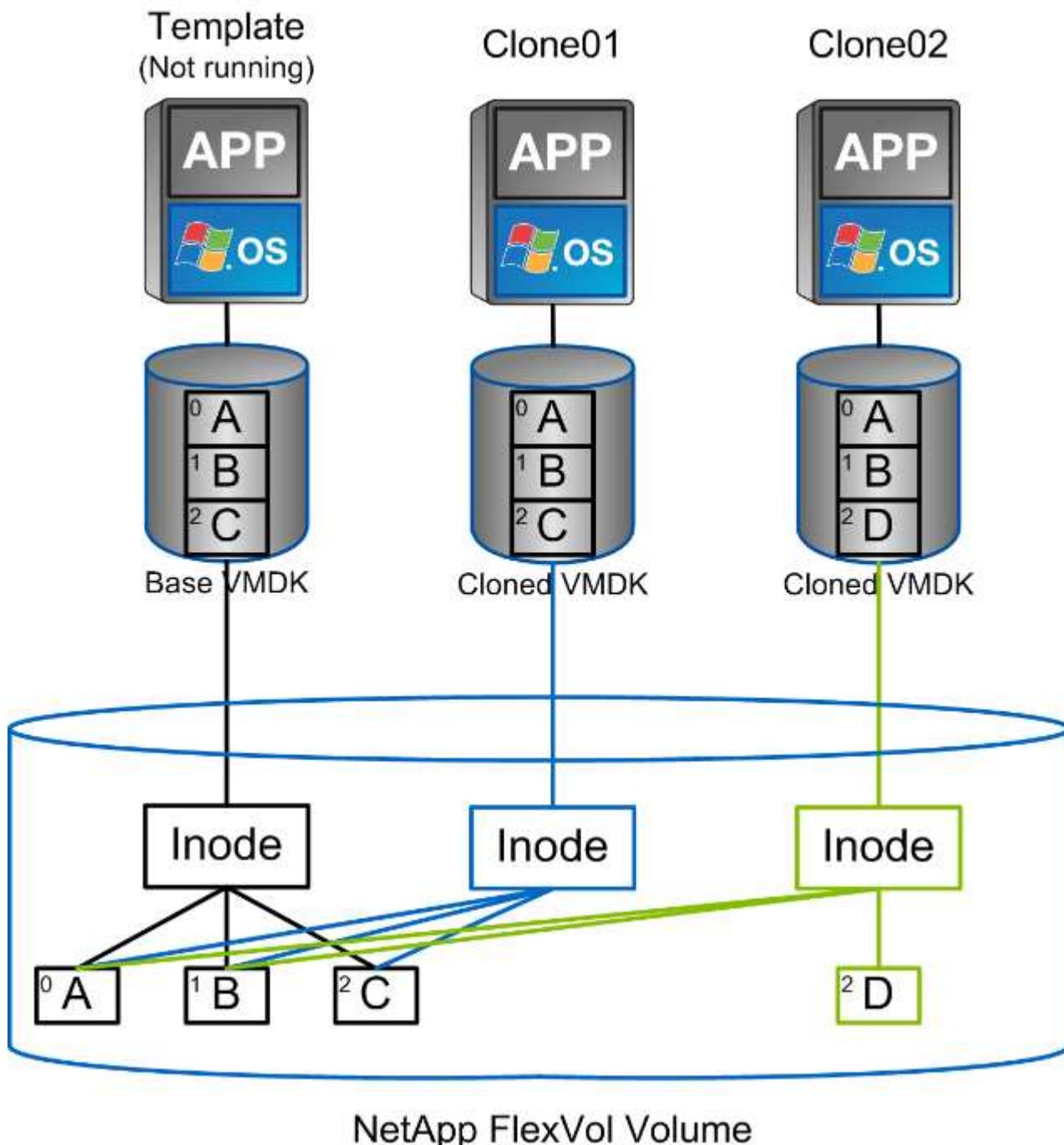
#### VM and datastore cloning

Cloning a storage object allows you to quickly create copies for further use, such as provisioning additional

VMs, backup/recovery operations, and so on. In vSphere, you can clone a VM, virtual disk, vVol, or datastore. After being cloned, the object can be further customized, often through an automated process. vSphere supports both full copy clones, as well as linked clones, where it tracks changes separately from the original object.

Linked clones are great for saving space, but they increase the amount of I/O that vSphere handles for the VM, affecting performance of that VM and perhaps the host overall. That's why NetApp customers often use storage system-based clones to get the best of both worlds: efficient use of storage and increased performance.

The following figure depicts ONTAP cloning.



Cloning can be offloaded to systems running ONTAP software through several mechanisms, typically at the

VM, vVol, or datastore level. These include the following:

- vVols using the NetApp vSphere APIs for Storage Awareness (VASA) Provider. ONTAP clones are used to support vVol Snapshot copies managed by vCenter that are space-efficient with minimal I/O effect to create and delete them. VMs can also be cloned using vCenter, and these are also offloaded to ONTAP, whether within a single datastore/volume or between datastores/volumes.
- vSphere cloning and migration using vSphere APIs – Array Integration (VAAI). VM cloning operations can be offloaded to ONTAP in both SAN and NAS environments (NetApp supplies an ESXi plug-in to enable VAAI for NFS). vSphere only offloads operations on cold (powered off) VMs in a NAS datastore, whereas operations on hot VMs (cloning and storage vMotion) are also offloaded for SAN. ONTAP uses the most efficient approach based on source, destination, and installed product licenses. This capability is also used by VMware Horizon View.
- SRA (used with VMware Site Recovery Manager). Here, clones are used to test recovery of the DR replica nondisruptively.
- Backup and recovery using NetApp tools such as SnapCenter. VM clones are used to verify backup operations as well as to mount a VM backup so that individual files can be copied.

ONTAP offloaded cloning can be invoked by VMware, NetApp, and third-party tools. Clones that are offloaded to ONTAP have several advantages. They are space-efficient in most cases, needing storage only for changes to the object; there is no additional performance effect to read and write them, and in some cases performance is improved by sharing blocks in high-speed caches. They also offload CPU cycles and network I/O from the ESXi server. Copy offload within a traditional datastore using a FlexVol volume can be fast and efficient with FlexClone licensed, but copies between FlexVol volumes might be slower. If you maintain VM templates as a source of clones, consider placing them within the datastore volume (use folders or content libraries to organize them) for fast, space efficient clones.

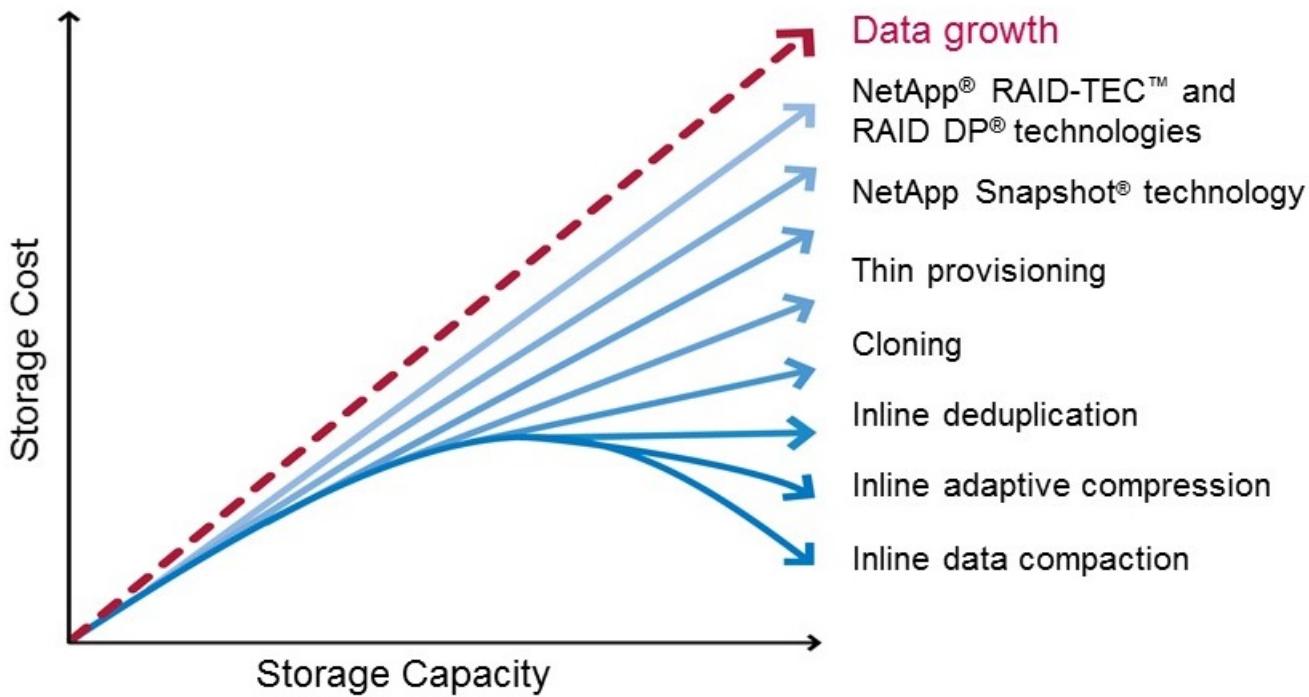
You can also clone a volume or LUN directly within ONTAP to clone a datastore. With NFS datastores, FlexClone technology can clone an entire volume, and the clone can be exported from ONTAP and mounted by ESXi as another datastore. For VMFS datastores, ONTAP can clone a LUN within a volume or a whole volume, including one or more LUNs within it. A LUN containing a VMFS must be mapped to an ESXi initiator group (igroup) and then resignatured by ESXi to be mounted and used as a regular datastore. For some temporary use cases, a cloned VMFS can be mounted without resignaturing. After a datastore is cloned, VMs inside it can be registered, reconfigured, and customized as if they were individually cloned VMs.

In some cases, additional licensed features can be used to enhance cloning, such as SnapRestore for backup or FlexClone. These licenses are often included in license bundles at no additional cost. A FlexClone license is required for vVol cloning operations as well as to support managed Snapshot copies of a vVol (which are offloaded from the hypervisor to ONTAP). A FlexClone license can also improve certain VAAI-based clones when used within a datastore/volume (creates instant, space-efficient copies instead of block copies). It is also used by the SRA when testing recovery of a DR replica, and SnapCenter for clone operations and to browse backup copies to restore individual files.

### **Storage efficiency and thin provisioning**

NetApp has led the industry with storage-efficiency innovation such as the first deduplication for primary workloads, and inline data compaction, which enhances compression and stores small files and I/O efficiently. ONTAP supports both inline and background deduplication, as well as inline and background compression.

The following figure depicts the combined effect of ONTAP storage efficiency features.



Here are recommendations on using ONTAP storage efficiency in a vSphere environment:

- The amount of data deduplication savings realized is based on the commonality of the data. With ONTAP 9.1 and earlier, data deduplication operated at the volume level, but with aggregate deduplication in ONTAP 9.2 and later, data is deduplicated across all volumes in an aggregate on AFF systems. You no longer need to group similar operating systems and similar applications within a single datastore to maximize savings.
- To realize the benefits of deduplication in a block environment, the LUNs must be thin provisioned. Although the LUN is still seen by the VM administrator as taking the provisioned capacity, the deduplication savings are returned to the volume to be used for other needs. NetApp recommends deploying these LUNs in FlexVol volumes that are also thin provisioned (ONTAP tools for VMware vSphere size the volume about 5% larger than the LUN).
- Thin provisioning is also recommended (and is the default) for NFS FlexVol volumes. In an NFS environment, deduplication savings are immediately visible to both storage and VM administrators with thin-provisioned volumes.
- Thin provisioning applies to the VMs as well, where NetApp generally recommends thin-provisioned VMDKs rather than thick. When using thin provisioning, make sure you monitor available space with ONTAP tools for VMware vSphere, ONTAP, or other available tools to avoid out-of-space problems.
- Note that there is no performance penalty when using thin provisioning with ONTAP systems; data is written to available space so that write performance and read performance are maximized. Despite this fact, some products such as Microsoft failover clustering or other low-latency applications might require guaranteed or fixed provisioning, and it is wise to follow these requirements to avoid support problems.
- For maximum deduplication savings, consider scheduling background deduplication on hard disk-based systems or automatic background deduplication on AFF systems. However, the scheduled processes use system resources when running, so ideally they should be scheduled during less active times (such as weekends) or run more frequently to reduce the amount of changed data to be processed. Automatic background deduplication on AFF systems has much less effect on foreground activities. Background compression (for hard disk-based systems) also consumes resources, so it should only be considered for secondary workloads with limited performance requirements.

- NetApp AFF systems primarily use inline storage efficiency capabilities. When data is moved to them using NetApp tools that use block replication such as the 7-Mode Transition Tool, SnapMirror, or Volume Move, it can be useful to run compression and compaction scanners to maximize efficiency savings. Review this NetApp Support [KB article](#) for additional details.
- Snapshot copies might lock blocks that could be reduced by compression or deduplication. When using scheduled background efficiency or one-time scanners, make sure that they run and complete before the next Snapshot copy is taken. Review your Snapshot copies and retention to make sure you only retain needed Snapshot copies, especially before a background or scanner job is run.

The following table provide storage efficiency guidelines for virtualized workloads on different types of ONTAP storage:

<b>Workload</b>	<b>Storage efficiency guidelines</b>		
	AFF	Flash Pool	Hard Disk Drives
VDI and SVI	<p>For primary and secondary workloads, use:</p> <ul style="list-style-type: none"> <li>Adaptive inline compression</li> <li>Inline deduplication</li> <li>Background deduplication</li> <li>Inline data compaction</li> </ul>	<p>For primary and secondary workloads, use:</p> <ul style="list-style-type: none"> <li>Adaptive inline compression</li> <li>Inline deduplication</li> <li>Background deduplication</li> <li>Inline data compaction</li> </ul>	<p>For primary workloads, use:</p> <ul style="list-style-type: none"> <li>Background deduplication</li> </ul> <p>For secondary workloads, use:</p> <ul style="list-style-type: none"> <li>Adaptive inline compression</li> <li>Adaptive background compression</li> <li>Inline deduplication</li> <li>Background deduplication</li> <li>Inline data compaction</li> </ul>

#### **Quality of service (QoS)**

Systems running ONTAP software can use the ONTAP storage QoS feature to limit throughput in MBps and/or I/Os per second (IOPS) for different storage objects such as files, LUNs, volumes, or entire SVMs.

Throughput limits are useful in controlling unknown or test workloads before deployment to make sure they don't affect other workloads. They can also be used to constrain a bully workload after it is identified. Minimum levels of service based on IOPS are also supported to provide consistent performance for SAN objects in ONTAP 9.2 and for NAS objects in ONTAP 9.3.

With an NFS datastore, a QoS policy can be applied to the entire FlexVol volume or individual VMDK files within it. With VMFS datastores using ONTAP LUNs, the QoS policies can be applied to the FlexVol volume that contains the LUNs or individual LUNs, but not individual VMDK files because ONTAP has no awareness of the VMFS file system. When using vVols, minimum and/or maximum QoS can be set on individual VMs using the storage capability profile and VM storage policy.

The QoS maximum throughput limit on an object can be set in MBps and/or IOPS. If both are used, the first limit reached is enforced by ONTAP. A workload can contain multiple objects, and a QoS policy can be applied to one or more workloads. When a policy is applied to multiple workloads, the workloads share the total limit of the policy. Nested objects are not supported (for example, files within a volume cannot each have their own policy). QoS minimums can only be set in IOPS.

The following tools are currently available for managing ONTAP QoS policies and applying them to objects:

- ONTAP CLI
- ONTAP System Manager
- OnCommand Workflow Automation
- Active IQ Unified Manager
- NetApp PowerShell Toolkit for ONTAP
- ONTAP tools for VMware vSphere VASA Provider

To assign a QoS policy to a VMDK on NFS, note the following guidelines:

- The policy must be applied to the `vmname-flat.vmdk` that contains the actual virtual disk image, not the `vmname.vmdk` (virtual disk descriptor file) or `vmname.vmx` (VM descriptor file).
- Do not apply policies to other VM files such as virtual swap files (`vmname.vswp`).
- When using the vSphere web client to find file paths (Datastore > Files), be aware that it combines the information of the `-flat.vmdk` and `.vmdk` and simply shows one file with the name of the `.vmdk` but the size of the `-flat.vmdk`. Add `-flat` into the file name to get the correct path.

To assign a QoS policy to a LUN, including VMFS and RDM, the ONTAP SVM (displayed as Vserver), LUN path, and serial number can be obtained from the Storage Systems menu on the ONTAP tools for VMware vSphere home page. Select the storage system (SVM), and then Related Objects > SAN. Use this approach when specifying QoS using one of the ONTAP tools.

Maximum and minimum QoS can be easily assigned to a vVol-based VM with ONTAP tools for VMware vSphere or Virtual Storage Console 7.1 and later. When creating the storage capability profile for the vVol container, specify a max and/or min IOPS value under the performance capability and then reference this SCP with the VM's storage policy. Use this policy when creating the VM or apply the policy to an existing VM.

FlexGroup datastores offer enhanced QoS capabilities when using ONTAP tools for VMware vSphere 9.8 and later. You can easily set QoS on all VMs in a datastore or on specific VMs. See the FlexGroup section of this report for more information.

## ONTAP QoS and VMware SIOC

ONTAP QoS and VMware vSphere Storage I/O Control (SIOC) are complementary technologies that vSphere and storage administrators can use together to manage performance of vSphere VMs hosted on systems running ONTAP software. Each tool has its own strengths, as shown in the following table. Because of the different scopes of VMware vCenter and ONTAP, some objects can be seen and managed by one system and not the other.

Property	ONTAP QoS	VMware SIOC
When active	Policy is always active	Active when contention exists (datastore latency over threshold)
Type of units	IOPS, MBps	IOPS, shares
vCenter or application scope	Multiple vCenter environments, other hypervisors and applications	Single vCenter server
Set QoS on VM?	VMDK on NFS only	VMDK on NFS or VMFS
Set QoS on LUN (RDM)?	Yes	No

Property	ONTAP QoS	VMware SIOC
Set QoS on LUN (VMFS)?	Yes	No
Set QoS on volume (NFS datastore)?	Yes	No
Set QoS on SVM (tenant)?	Yes	No
Policy-based approach?	Yes; can be shared by all workloads in the policy or applied in full to each workload in the policy.	Yes, with vSphere 6.5 and later.
License required	Included with ONTAP	Enterprise Plus

### VMware Storage Distributed Resource Scheduler

VMware Storage Distributed Resource Scheduler (SDRS) is a vSphere feature that places VMs on storage based on the current I/O latency and space usage. It then moves the VM or VMDKs nondisruptively between the datastores in a datastore cluster (also referred to as a pod), selecting the best datastore in which to place the VM or VMDKs in the datastore cluster. A datastore cluster is a collection of similar datastores that are aggregated into a single unit of consumption from the vSphere administrator's perspective.

When using SDRS with the NetApp ONTAP tools for VMware vSphere, you must first create a datastore with the plug-in, use vCenter to create the datastore cluster, and then add the datastore to it. After the datastore cluster is created, additional datastores can be added to the datastore cluster directly from the provisioning wizard on the Details page.

Other ONTAP best practices for SDRS include the following:

- All datastores in the cluster should use the same type of storage (such as SAS, SATA, or SSD), be either all VMFS or NFS datastores, and have the same replication and protection settings.
- Consider using SDRS in default (manual) mode. This approach allows you to review the recommendations and decide whether to apply them or not. Be aware of these effects of VMDK migrations:
  - When SDRS moves VMDKs between datastores, any space savings from ONTAP cloning or deduplication are lost. You can rerun deduplication to regain these savings.
  - After SDRS moves VMDKs, NetApp recommends recreating the Snapshot copies at the source datastore because space is otherwise locked by the VM that was moved.
  - Moving VMDKs between datastores on the same aggregate has little benefit, and SDRS does not have visibility into other workloads that might share the aggregate.

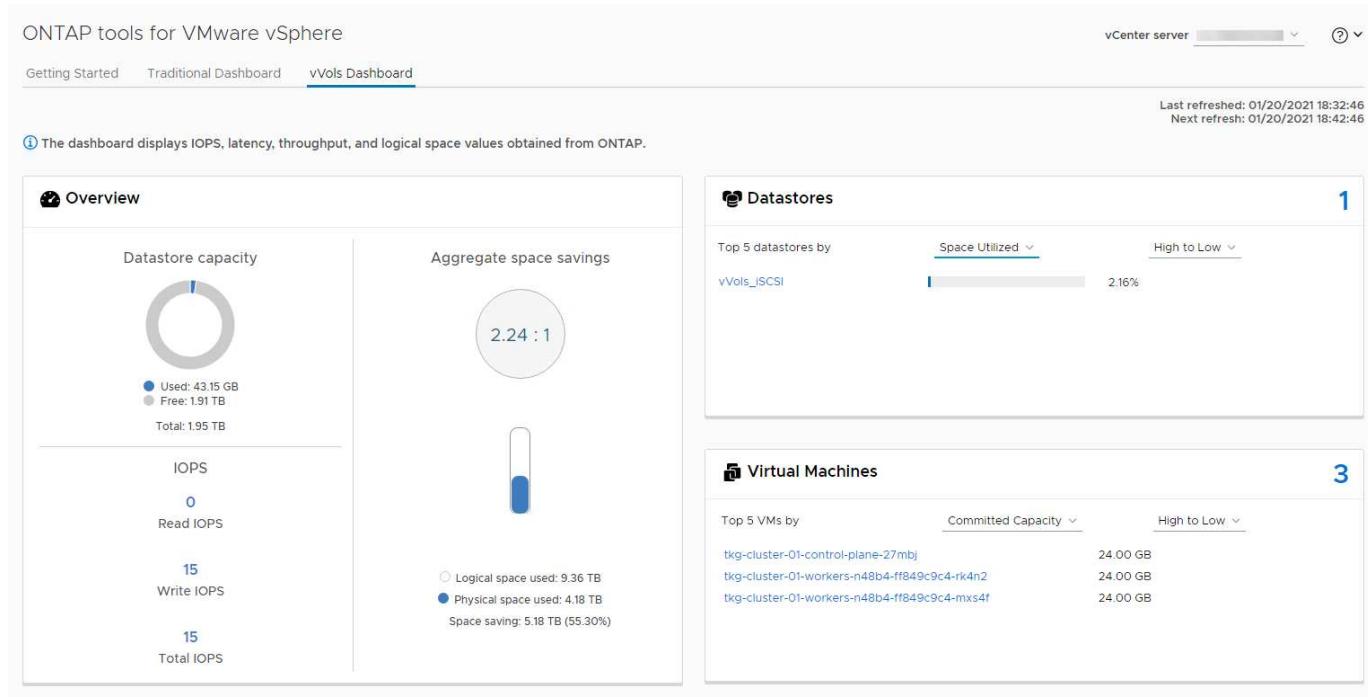
### Storage policy-based management and vVols

VMware vSphere APIs for Storage Awareness (VASA) make it easy for a storage administrator to configure datastores with well-defined capabilities and let the VM administrator use those whenever needed to provision VMs without having to interact with each other. It's worth taking a look at this approach to see how it can streamline your virtualization storage operations and avoid a lot of trivial work.

Prior to VASA, VM administrators could define VM storage policies, but they had to work with the storage administrator to identify appropriate datastores, often by using documentation or naming conventions. With VASA, the storage administrator can define a range of storage capabilities, including performance, tiering, encryption, and replication. A set of capabilities for a volume or a set of volumes is called a storage capability profile (SCP).

The SCP supports minimum and/or maximum QoS for a VM's data vVols. Minimum QoS is supported only on AFF systems. ONTAP tools for VMware vSphere includes a dashboard that displays VM granular performance and logical capacity for vVols on ONTAP systems.

The following figure depicts ONTAP tools for VMware vSphere 9.8 vVols dashboard.



After the storage capability profile is defined, it can be used to provision VMs using the storage policy that identifies its requirements. The mapping between the VM storage policy and the datastore storage capability profile allows vCenter to display a list of compatible datastores for selection. This approach is known as storage policy-based management.

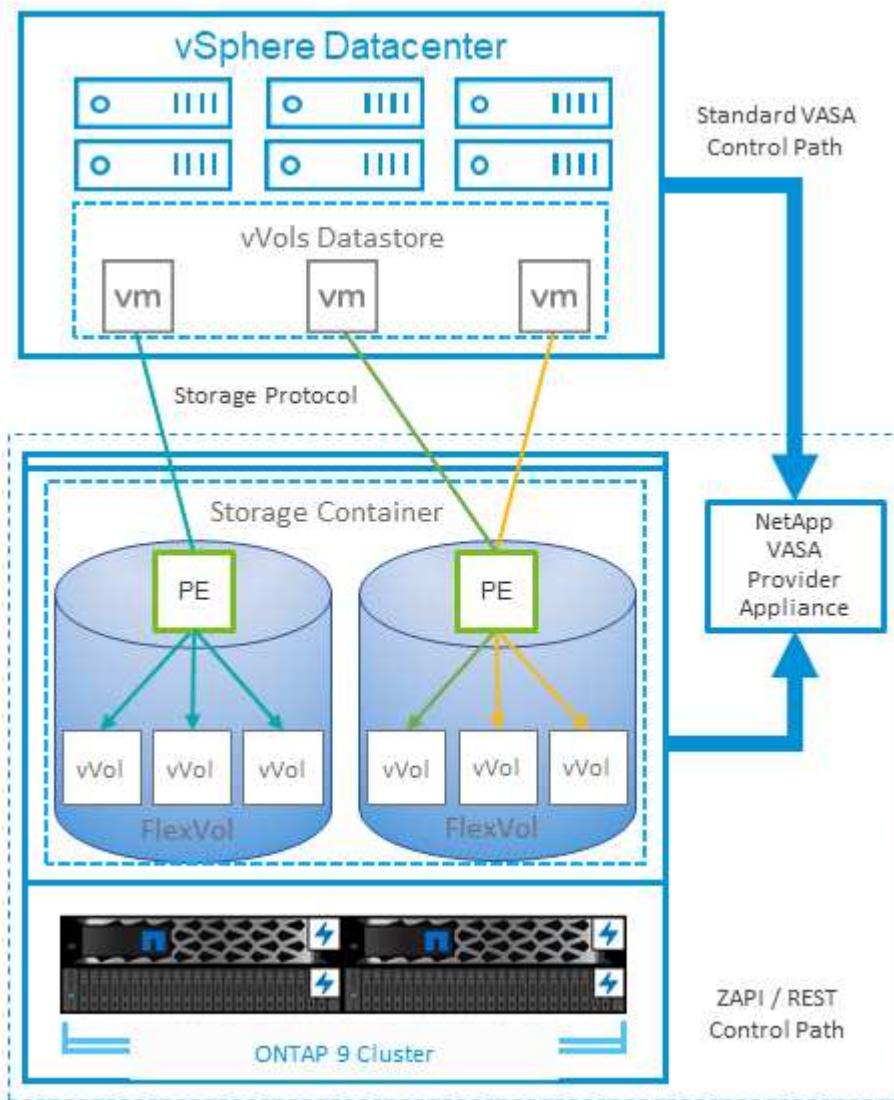
VASA provides the technology to query storage and return a set of storage capabilities to vCenter. VASA vendor providers supply the translation between the storage system APIs and constructs and the VMware APIs that are understood by vCenter. NetApp's VASA Provider for ONTAP is offered as part of the ONTAP tools for VMware vSphere appliance VM, and the vCenter plug-in provides the interface to provision and manage vVol datastores, as well as the ability to define storage capability profiles (SCPs).

ONTAP supports both VMFS and NFS vVol datastores. Using vVols with SAN datastores brings some of the benefits of NFS such as VM-level granularity. Here are some best practices to consider, and you can find additional information in [TR-4400](#):

- A vVol datastore can consist of multiple FlexVol volumes on multiple cluster nodes. The simplest approach is a single datastore, even when the volumes have different capabilities. SPBM makes sure that a compatible volume is used for the VM. However, the volumes must all be part of a single ONTAP SVM and accessed using a single protocol. One LIF per node for each protocol is sufficient. Avoid using multiple ONTAP releases within a single vVol datastore because the storage capabilities might vary across releases.
- Use the ONTAP tools for VMware vSphere plug-in to create and manage vVol datastores. In addition to managing the datastore and its profile, it automatically creates a protocol endpoint to access the vVols if needed. If LUNs are used, note that LUN PEs are mapped using LUN IDs 300 and higher. Verify that the ESXi host advanced system setting `Disk.MaxLUN` allows a LUN ID number that is higher than 300 (the default is 1,024). Do this step by selecting the ESXi host in vCenter, then the Configure tab, and find `Disk.MaxLUN` in the list of Advanced System Settings.

- Do not install or migrate VASA Provider, vCenter Server (appliance or Windows based), or ONTAP tools for VMware vSphere itself onto a vVols datastore, because they are then mutually dependent, limiting your ability to manage them in the event of a power outage or other data center disruption.
- Back up the VASA Provider VM regularly. At a minimum, create hourly Snapshot copies of the traditional datastore that contains VASA Provider. For more about protecting and recovering the VASA Provider, see this [KB article](#).

The following figure shows vVols components.



#### Cloud migration and backup

Another ONTAP strength is broad support for the hybrid cloud, merging systems in your on-premises private cloud with public cloud capabilities. Here are some NetApp cloud solutions that can be used in conjunction with vSphere:

- **Cloud Volumes.** NetApp Cloud Volumes Service for AWS or GCP and Azure NetApp Files for ANF provide high-performance, multi-protocol managed storage services in the leading public cloud environments. They can be used directly by VMware Cloud VM guests.
- **Cloud Volumes ONTAP.** NetApp Cloud Volumes ONTAP data management software delivers control, protection, flexibility, and efficiency to your data on your choice of cloud. Cloud Volumes ONTAP is cloud-

native data management software built on NetApp ONTAP storage software. Use together with Cloud Manager to deploy and manage Cloud Volumes ONTAP instances together with your on-premises ONTAP systems. Take advantage of advanced NAS and iSCSI SAN capabilities together with unified data management, including snapshot copies and SnapMirror replication.

- **Cloud Services.** Use Cloud Backup Service or SnapMirror Cloud to protect data from on-premises systems using public cloud storage. Cloud Sync helps migrate and keep your data in sync across NAS, object stores, and Cloud Volumes Service storage.
- **FabricPool.** FabricPool offers quick and easy tiering for ONTAP data. Cold blocks in Snapshot copies can be migrated to an object store in either public clouds or a private StorageGRID object store and are automatically recalled when the ONTAP data is accessed again. Or use the object tier as a third level of protection for data that is already managed by SnapVault. This approach can allow you to [store more Snapshot copies of your VMs](#) on primary and/or secondary ONTAP storage systems.
- **ONTAP Select.** Use NetApp software-defined storage to extend your private cloud across the Internet to remote facilities and offices, where you can use ONTAP Select to support block and file services as well as the same vSphere data management capabilities you have in your enterprise data center.

When designing your VM-based applications, consider future cloud mobility. For example, rather than placing application and data files together use a separate LUN or NFS export for the data. This allows you to migrate the VM and data separately to cloud services.

#### Encryption for vSphere data

Today, there are increasing demands to protect data at rest through encryption. Although the initial focus was on financial and healthcare information, there is growing interest in protecting all information, whether it's stored in files, databases, or other data types.

Systems running ONTAP software make it easy to protect any data with at-rest encryption. NetApp Storage Encryption (NSE) uses self-encrypting disk drives with ONTAP to protect SAN and NAS data. NetApp also offers NetApp Volume Encryption and NetApp Aggregate Encryption as a simple, software-based approach to encrypt volumes on any disk drives. This software encryption doesn't require special disk drives or external key managers and is available to ONTAP customers at no additional cost. You can upgrade and start using it without any disruption to your clients or applications, and they are validated to the FIPS 140-2 level 1 standard, including the onboard key manager.

There are several approaches for protecting the data of virtualized applications running on VMware vSphere. One approach is to protect the data with software inside the VM at the guest OS level. Newer hypervisors such as vSphere 6.5 now support encryption at the VM level as another alternative. However, NetApp software encryption is simple and easy and has these benefits:

- **No effect on the virtual server CPU.** Some virtual server environments need every available CPU cycle for their applications, yet tests have shown up to 5x CPU resources are needed with hypervisor-level encryption. Even if the encryption software supports Intel's AES-NI instruction set to offload encryption workload (as NetApp software encryption does), this approach might not be feasible due to the requirement for new CPUs that are not compatible with older servers.
- **Onboard key manager included.** NetApp software encryption includes an onboard key manager at no additional cost, which makes it easy to get started without high-availability key management servers that are complex to purchase and use.
- **No effect on storage efficiency.** Storage efficiency techniques such as deduplication and compression are widely used today and are key to using flash disk media cost-effectively. However, encrypted data cannot typically be deduplicated or compressed. NetApp hardware and storage encryption operate at a lower level and allow full use of industry-leading NetApp storage efficiency features, unlike other approaches.

- **Easy datastore granular encryption.** With NetApp Volume Encryption, each volume gets its own AES 256-bit key. If you need to change it, you can do so with a single command. This approach is great if you have multiple tenants or need to prove independent encryption for different departments or apps. This encryption is managed at the datastore level, which is a lot easier than managing individual VMs.

It's simple to get started with software encryption. After the license is installed, simply configure the onboard key manager by specifying a passphrase and then either create a new volume or do a storage-side volume move to enable encryption. NetApp is working to add more integrated support for encryption capabilities in future releases of its VMware tools.

## Active IQ Unified Manager

Active IQ Unified Manager provides visibility into the VMs in your virtual infrastructure and enables monitoring and troubleshooting storage and performance issues in your virtual environment.

A typical virtual infrastructure deployment on ONTAP has various components that are spread across compute, network, and storage layers. Any performance lag in a VM application might occur due to a combination of latencies faced by the various components at the respective layers.

The following screenshot shows the Active IQ Unified Manager Virtual Machines view.

Name	Status	Power State	Protocol	Capacity (Used   Allocated)	IOPS	VM Latency (ms)	Host IOPS	Host Latency (ms)	Network Latency (ms)	Datastore IOPS	Datastore Latency (ms)
vCenter7	ON	NFS		160 GB   712 GB	183	0	243	0	0	831	0.3
POWER	ON										
VCENTER-SERVER											
vcenter7.stl.netapp.com											
TOPOLOGY VIEW											
Compute											
VDISK (16)											
Worst Latency/VDisk											
VM											
vCenter7											
HOST											
esxi02.stl.netapp.com											
NETWORK											
LATENCY											
Storage											
DATASTORE INFRASTRUCTURE											
VMDK (16)											
IOPS											
LATENCY											
Expand Topology											
AD	ON	NFS		8.05 GB   100 GB	167	0	306	0	0	831	0.3
BluePaddle-01	ON	NFS		398 GB   2.26 TB	44	0	149	0	0	831	0.3
AIQUM	ON	NFS		92 GB   400 GB	41	0	149	0	0	831	0.3
DirtWolf-02	ON	NFS		138 GB   2.26 TB	39	0	306	0	0	831	0.3
BluePaddle-02	ON	NFS		398 GB   2.26 TB	38	0	149	0	0	831	0.3

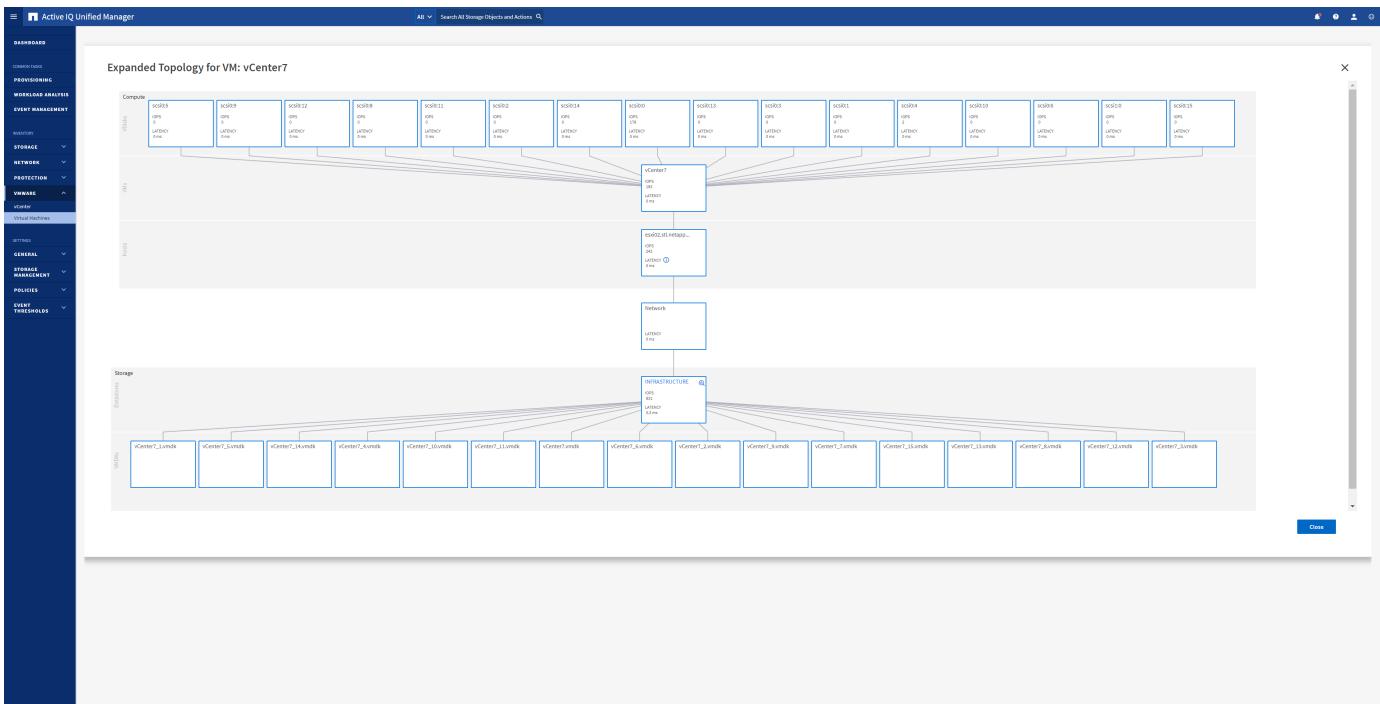
Last updated: Jan 29, 2021, 9:30 AM

Show / Hide

Showing all 44 Virtual Machines

Unified Manager presents the underlying sub-system of a virtual environment in a topological view for determining whether a latency issue has occurred in the compute node, network, or storage. The view also highlights the specific object that causes the performance lag for taking remedial steps and addressing the underlying issue.

The following screenshot shows the AIQUM expanded topology.



## ONTAP and vSphere release-specific information

This section provides guidance on capabilities supported by specific releases of ONTAP and vSphere. NetApp recommends confirming a specific combination of releases with the [NetApp Interoperability Matrix](#).

### ONTAP releases

At the time of publication, NetApp provides full support for these release families:

- ONTAP 9.5
- ONTAP 9.6
- ONTAP 9.7
- ONTAP 9.8

### vSphere and ESXi support

NetApp ONTAP has broad support for vSphere ESXi hosts. The four major release families just described (9.5, 9.6, 9.7, and 9.8) are fully supported as data storage platforms for recent vSphere releases, including 6.0, 6.5, and 7.0 (including updates for these releases). NFS v3 interoperability is broadly defined, and NetApp supports any client, including hypervisors, that is compliant with the NFS v3 standard. NFSv4.1 support is limited to vSphere 6.0 through 7.0.

For SAN environments, NetApp conducts extensive testing of SAN components. In general, NetApp supports standard X86-64 rack servers and Cisco UCS servers together with standard Ethernet adapters for iSCSI connections. FC, FCoE, and NVMe/FC environments have more specifically defined support due to the HBA firmware and drivers needed.

Always check the [NetApp Interoperability Matrix](#) to confirm support for a specific hardware and software configuration.

## NFS Plug-In for VMware VAAI

This plug-in for ESXi hosts helps by offloading operations to ONTAP using VAAI. The latest release, 1.1.2, includes support for NFSv4.1 datastores, including Kerberos (krb5 and krb5i) support. It is supported with ESXi 6.0, 6.5, and 7.0 together with ONTAP 9.5-9.8.

## VASA Provider

NetApp's VASA Provider supports vVol provisioning and management (see section 3.7). Recent VASA Provider releases support ESXi 6.0, 6.5, and 7.0 together with ONTAP 9.5-9.8.

## ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere is key for managing ONTAP storage together with vSphere (using it is a best practice). The latest release, 9.8, is supported with vSphere 6.5 and 7.0 together with ONTAP 9.5-9.8.

## Recommended ESXi host and other ONTAP settings

NetApp has developed a set of ESXi host multipathing and HBA timeout settings for proper behavior with ONTAP based on NetApp testing. These are easily set using ONTAP tools for VMware vSphere. From the Summary dashboard, click Edit Settings in the Host Systems portlet or right-click the host in vCenter, then navigate to ONTAP tools > Set Recommended Values. Here are the currently recommended host settings with the 9.8 release.

Host setting	NetApp recommended value
<b>ESXi advanced configuration</b>	
VMFS3.HardwareAcceleratedLocking	Leave as set (VMware default is 1).
VMFS3.EnableBlockDelete	Leave as set (VMware default is 0, but this is not needed for VMFS6). For more information, see VMware KB article <a href="#">2007427</a> .
<b>NFS Settings</b>	
Net.TcpipHeapSize	vSphere 6.0 or later, set to 32. All other NFS configurations, set to 30.
Net.TcpipHeapMax	Set to 1536 for vSphere 6.0 and later.
NFS.MaxVolumes	vSphere 6.0 or later, set to 256. All other NFS configurations, set to 64.
NFS41.MaxVolumes	vSphere 6.0 or later, set to 256.
NFS.MaxQueueDepth	vSphere 6.0 or later, set to 128.
NFS.HeartbeatMaxFailures	Set to 10 for all NFS configurations.
NFS.HeartbeatFrequency	Set to 12 for all NFS configurations.
NFS.HeartbeatTimeout	Set to 5 for all NFS configurations.
SunRPC.MaxConnPerIP	vSphere 7.0 or later, set to 128.
<b>FC/FCoE Settings</b>	

Path selection policy	Set to RR (round robin) when FC paths with ALUA are used. Set to FIXED for all other configurations. Setting this value to RR helps provide load balancing across all active/optimized paths. The value FIXED is for older, non-ALUA configurations and helps prevent proxy I/O. In other words, it helps keep I/O from going to the other node of a high-availability (HA) pair in an environment that has Data ONTAP operating in 7-Mode.
Disk.QFullSampleSize	Set to 32 for all configurations. Setting this value helps prevent I/O errors.
Disk.QFullThreshold	Set to 8 for all configurations. Setting this value helps prevent I/O errors.
Emulex FC HBA timeouts	Use the default value.
QLogic FC HBA timeouts	Use the default value.
<b>iSCSI Settings</b>	
Path selection policy	Set to RR (round robin) for all iSCSI paths. Setting this value to RR helps provide load balancing across all active/optimized paths.
Disk.QFullSampleSize	Set to 32 for all configurations. Setting this value helps prevent I/O errors.
Disk.QFullThreshold	Set to 8 for all configurations. Setting this value helps prevent I/O errors.

ONTAP tools also specify certain default settings when creating ONTAP FlexVol volumes and LUNs:

ONTAP tool	Default setting
Snapshot reserve (-percent-snapshot-space)	0
Fractional reserve (-fractional-reserve)	0
Access time update (-atime-update)	False
Minimum readahead (-min-readahead)	False
Scheduled Snapshot copies	None
Storage efficiency	Enabled
Volume guarantee	None (thin provisioned)
Volume Autosize	grow_shrink
LUN space reservation	Disabled
LUN space allocation	Enabled

#### Other host multipath configuration considerations

While not currently configured by available ONTAP tools, NetApp suggests considering these configuration options:

- In high-performance environments or when testing performance with a single LUN datastore, consider changing the load balance setting of the round-robin (VMW\_PSP\_RR) path selection policy (PSP) from the default IOPS setting of 1000 to a value of 1. See VMware KB [2069356](#) for more info.
- In vSphere 6.7 Update 1, VMware introduced a new latency load balance mechanism for the Round Robin PSP. The new option considers I/O bandwidth and path latency when selecting the optimal path for I/O. You might benefit from using it in environments with non-equivalent path connectivity, such as cases where there are more network hops on one path than another, or when using a NetApp All SAN Array system. See [Path Selection Plug-Ins and Policies](#) for more information.

## Where to find additional information

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

- VMware Product Documentation  
<https://www.vmware.com/support/pubs/>
- NetApp Product Documentation  
<https://docs.netapp.com>

## Contact us

Do you have comments about this technical report?

Send them to us at [doccomments@netapp.com](mailto:doccomments@netapp.com) and include TR-4597 in the subject line.

## TR-4900: VMware Site Recovery Manager with NetApp ONTAP 9

Chance Bingen, NetApp

### ONTAP for vSphere

NetApp ONTAP has been a leading storage solution for VMware vSphere environments since its introduction into the modern datacenter in 2002, and it continues to add innovative capabilities to simplify management while reducing costs. This document introduces the ONTAP solution for VMware Site Recovery Manager (SRM), VMware's industry leading disaster recovery (DR) software, including the latest product information and best practices to streamline deployment, reduce risk, and simplify ongoing management.

Best practices supplement other documents such as guides and compatibility tools. They are developed based on lab testing and extensive field experience by NetApp engineers and customers. In some cases, recommended best practices might not be the right fit for your environment; however, they are generally the simplest solutions that meet the needs of the most customers.

This document is focused on capabilities in recent releases of ONTAP 9 when used in conjunction with supported versions of ONTAP tools for VMware vSphere (which includes the NetApp Storage Replication Adapter [SRA] and VASA Provider [VP]), as well as VMware Site Recovery Manager 8.4.

### Why use ONTAP with SRM?

NetApp data management platforms powered by ONTAP software are some of the most widely adopted storage solutions for SRM. The reasons are plentiful: A secure, high performance, unified protocol (NAS and SAN together) data management platform that provides industry defining storage efficiency, multitenancy, quality of service controls, data protection with space-efficient Snapshot copies and replication with SnapMirror. All leveraging native hybrid multi-cloud integration for the protection of VMware workloads and a plethora of

automation and orchestration tools at your fingertips.

When you use SnapMirror for array-based replication, you take advantage of one of ONTAP's most proven and mature technologies. SnapMirror gives you the advantage of secure and highly efficient data transfers, copying only changed file system blocks, not entire VMs or datastores. Even those blocks take advantage of space savings, such as deduplication, compression, and compaction. Modern ONTAP systems now use version-independent SnapMirror, allowing you flexibility in selecting your source and destination clusters. SnapMirror has truly become one of the most powerful tools available for disaster recovery.

Whether you are using traditional NFS, iSCSI, or Fibre Channel- attached datastores (now with support for vVols datastores), SRM provides a robust first party offering that leverages the best of ONTAP capabilities for disaster recovery or datacenter migration planning and orchestration.

## How SRM leverages ONTAP 9

SRM leverages the advanced data management technologies of ONTAP systems by integrating with ONTAP tools for VMware vSphere, a virtual appliance that includes three primary components:

- The vCenter plug-in, formerly known as Virtual Storage Console (VSC), simplifies storage management and efficiency features, enhances availability, and reduces storage costs and operational overhead, whether you are using SAN or NAS. It uses best practices for provisioning datastores and optimizes ESXi host settings for NFS and block storage environments. For all these benefits, NetApp recommends this plug-in when using vSphere with systems running ONTAP software.
- The VASA Provider for ONTAP supports the VMware vStorage APIs for Storage Awareness (VASA) framework. VASA Provider connects vCenter Server with ONTAP to aid in provisioning and monitoring VM storage. It enables VMware Virtual Volumes (vVols) support and the management of storage capability profiles (including vVols replication capabilities) and individual VM vVols performance. It also provides alarms for monitoring capacity and compliance with the profiles. When used in conjunction with SRM, the VASA Provider for ONTAP enables support for vVols- based virtual machines without requiring the installation of an SRA adapter on the SRM server.
- The SRA is used together with SRM to manage the replication of VM data between production and disaster recovery sites for traditional VMFS and NFS datastores and also for the nondisruptive testing of DR replicas. It helps automate the tasks of discovery, recovery, and reprottection. It includes both an SRA server appliance and SRA adapters for the Windows SRM server and the SRM appliance.

After you have installed and configured the SRA adapters on the SRM server for protecting non-vVols datastores and/or enabled vVols replication in the VASA Provider settings, you can begin the task of configuring your vSphere environment for disaster recovery.

The SRA and VASA Provider deliver a command-and-control interface for the SRM server to manage the ONTAP FlexVols that contain your VMware Virtual Machines (VMs), as well as the SnapMirror replication protecting them.

Starting with SRM 8.3, a new SRM vVols Provider control path was introduced into the SRM server, allowing it to communicate with the vCenter server and, through it, to the VASA Provider without needing an SRA. This enabled the SRM server to leverage much deeper control over the ONTAP cluster than was possible before, because VASA provides a complete API for closely coupled integration.

SRM can test your DR plan nondisruptively using NetApp's proprietary FlexClone technology to make nearly instantaneous clones of your protected datastores at your DR site. SRM creates a sandbox to safely test so that your organization, and your customers, are protected in the event of a true disaster, giving you confidence in your organizations ability to execute a failover during a disaster.

In the event of a true disaster or even a planned migration, SRM allows you to send any last-minute changes

to the dataset via a final SnapMirror update (if you choose to do so). It then breaks the mirror and mounts the datastore to your DR hosts. At that point, your VMs can be automatically powered up in any order according to your pre-planned strategy.

## SRM with ONTAP and other use cases: hybrid cloud and migration

Integrating your SRM deployment with ONTAP advanced data management capabilities allows for vastly improved scale and performance when compared with local storage options. But more than that, it brings the flexibility of the hybrid cloud. The hybrid cloud enables you to save money by tiering unused data blocks from your high-performance array to your preferred hyperscaler using FabricPool, which could be an on-premises S3 store such as NetApp StorageGRID. You can also use SnapMirror for edge-based systems with software-defined ONTAP Select or cloud-based DR using Cloud Volumes ONTAP (CVO) or [NetApp Private Storage in Equinix](#) for Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) to create a fully integrated storage, networking, and compute- services stack in the cloud.

You could then perform test failover inside a cloud service provider's datacenter with near-zero storage footprint thanks to FlexClone. Protecting your organization can now cost less than ever before.

SRM can also be used to execute planned migrations by leveraging SnapMirror to efficiently transfer your VMs from one datacenter to another or even within the same datacenter, whether your own, or via any number of NetApp partner service providers.

## New features with SRM and ONTAP Tools

With the transition from the legacy virtual appliance, ONTAP tools brings a wealth of new features, higher limits, and new vVols support.

### Latest versions of vSphere and Site Recovery Manager

With the release of SRM 8.3 and later and the 9.7.1 and later releases of ONTAP tools, you are now able to protect VMs running on VMware vSphere 7.

NetApp has shared a deep partnership with VMware for nearly two decades and strives to provide support for the latest releases as soon as possible. Always check the NetApp Interoperability Matrix Tool (IMT) for the latest qualified combinations of software.

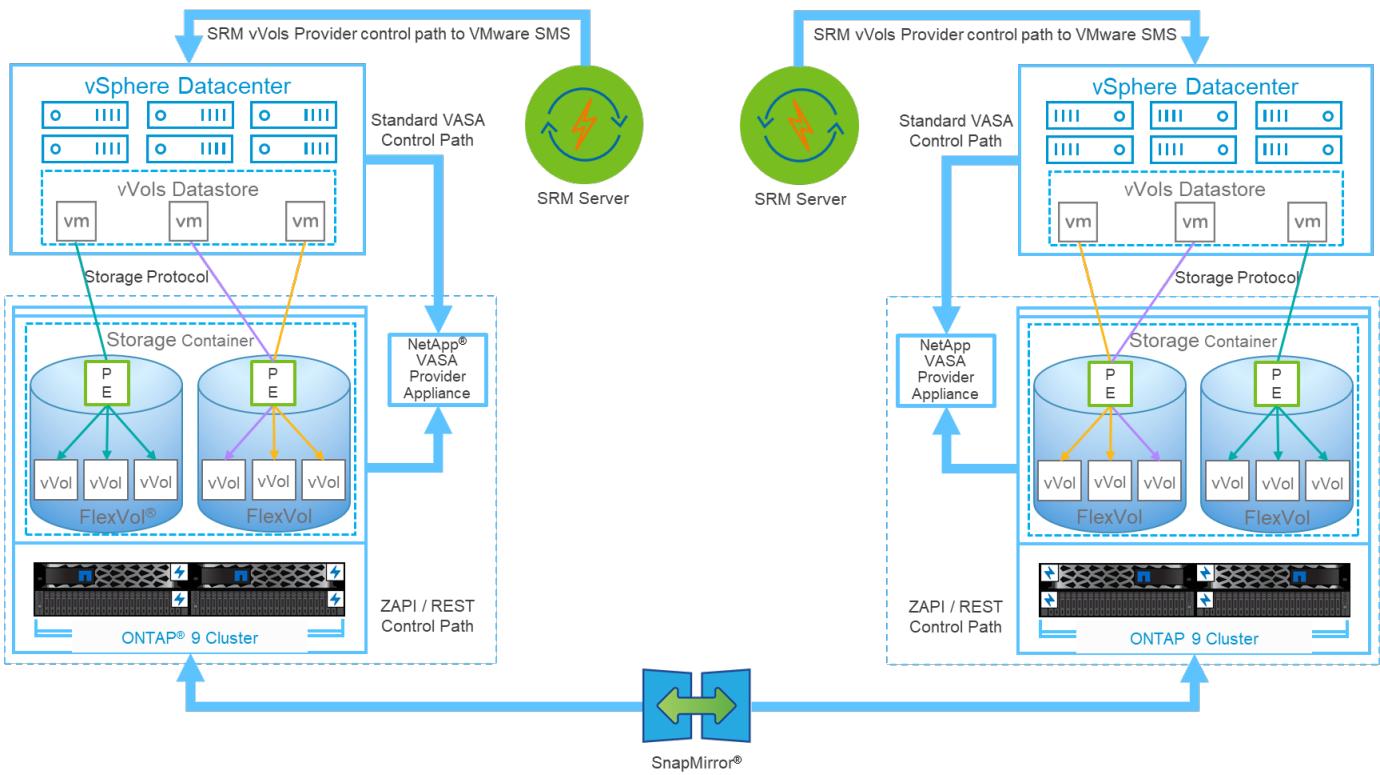
The NetApp IMT can be found [here](#).

### vVols support (and why SPBM matters, even with SRM)

Starting with the 8.3 release, SRM now supports storage policy-based management (SPBM) of replication leveraging vVols and array-based replication. To accomplish this, the SRM server was updated to include a new SRM vVols provider service, which communicates to the vCenter server's SMS service for VASA related tasks.

One advantage to this architecture is that an SRA is no longer needed since everything is handled using VASA.

SPBM is a powerful tool in the vSphere toolbox, allow simplified, predictable, and consistent storage services for consumption by automation frameworks in private and hybrid cloud environments. Fundamentally, SPBM allows you to define classes of service that meet the needs of your diverse customer base. SRM now allows you to expose replication capabilities to your customers for critical workloads requiring robust industry-standard disaster- recovery orchestration and automation.



### vVols Architecture 2.3 Support for appliance-based SRM servers

Photon OS-based SRM servers are now supported, in addition to legacy Windows-based platforms.

You can now install SRA adapters regardless of your preferred SRM server type.

### Support for IPv6

IPv6 is now supported with the following limitations:

- vCenter 6.7 or later
- Not supported with SRM 8.2 (8.1, 8.3, and 8.4 are supported)
- Check the [Interoperability Matrix Tool](#) for the latest qualified versions.

### Improved performance

Operational performance is a key requirement for SRM task execution. To meet the requirements of modern RTOs and RPOs, the SRA with ONTAP tools has added two new improvements.

- **Support for concurrent reprotect operations.** First introduced in SRA 9.7.1, enabling this feature allows you to run reprotect on two or more recovery plans concurrently, thus reducing the time required to reprotect datastores after a failover or migration and remain within your RTO and RPO parameters.
- **ONTAP Tools 9.8 adds a new NAS- only optimized mode.** When you use SVM- scoped accounts and connections to ONTAP clusters with only NFS based datastores, you can enable NAS-only optimized mode for peak performance in supported environments.

### Greater scale

The ONTAP tools SRA can now support up to 500 protection groups (PGs) when used with SRM 8.3 and later.

## Synchronous replication

A long awaited and much anticipated new feature is SnapMirror Synchronous (SM-S) with ONTAP 9.5 and later which delivers a volume granular zero RPO data replication solution for your mission-critical applications. SM-S requires ONTAP tools 9.8 or later.

## REST API support

SRA server configuration can now be managed by REST APIs. A Swagger UI has been added to assist in building your automation workflows and can be found on your ONTAP tools appliance at <https://<appliance>:8143/api/rest/swagger-ui.html#/>.

## Deployment best practices

### SVM layout and segmentation for SMT

With ONTAP, the concept of the storage virtual machine (SVM) provides strict segmentation in secure multitenant environments. SVM users on one SVM cannot access or manage resources from another. In this way, you can leverage ONTAP technology by creating separate SVMs for different business units who manage their own SRM workflows on the same cluster for greater overall storage efficiency.

Consider managing ONTAP using SVM-scoped accounts and SVM management LIFs to not only improve security controls, but also improve performance. Performance is inherently greater when using SVM-scoped connections because the SRA is not required to process all the resources in an entire cluster, including physical resources. Instead, it only needs to understand the logical assets that are abstracted to the particular SVM.

When using NAS protocols only (no SAN access), you can even leverage the new NAS optimized mode by setting the following parameter (note that the name is such because SRA and VASA use the same backend services in the appliance):

1. Log into the control panel at `https://<IP address>:9083` and click Web based CLI interface.
2. Run the command `vp updateconfig -key=enable.qtree.discovery -value=true`.
3. Run the command `vp updateconfig -key=enable.optimised.sra -value=true`.
4. Run the command `vp reloadconfig`.

### Deploy ONTAP tools and considerations for vVols

If you intend to use SRM with vVols, you must manage the storage using cluster- scoped credentials and a cluster management LIF. This is because the VASA Provider must understand the underlying physical architecture to satisfy the policy requires for VM storage policies. For example, if you have a policy that requires all- flash storage, the VASA Provider must be able to see which systems are all flash.

Another deployment best practice is to never store your ONTAP tools appliance on a vVols datastore that it is managing. This could lead to a situation whereby you cannot power on the VASA Provider because you cannot create the swap vVol for the appliance because the appliance is offline.

### Best practices for managing ONTAP 9 systems

As previously mentioned, you can manage ONTAP clusters using either cluster or SVM scoped credentials and management LIFs. For optimum performance, you may want to consider using SVM- scoped credentials whenever you aren't using vVols. However, in doing so, you should be aware of some requirements, and that you do lose some functionality.

- The default vsadmin SVM account does not have the required access level to perform ONTAP tools tasks. Therefore, you need to create a new SVM account.
- If you are using ONTAP 9.8 or later, NetApp recommends creating an RBAC least privileged user account using ONTAP System Manager's users menu together with the JSON file available on your ONTAP tools appliance at <https://<IP address>:9083/vsc/config/>. Use your administrator password to download the JSON file. This can be used for SVM or cluster scoped accounts.

If you are using ONTAP 9.6 or earlier, you should use the RBAC User Creator (RUC) tool available in the [NetApp Support Site Toolchest](#).

- Because the vCenter UI plugin, VASA Provider, and SRA server are all fully integrated services, you must add storage to the SRA adapter in SRM the same way you add storage in the vCenter UI for ONTAP tools. Otherwise, the SRA server might not recognize the requests being sent from SRM via the SRA adapter.
- NFS path checking is not performed when using SVM-scoped credentials. This is because the physical location is logically abstracted from the SVM. This is not a cause for concern though, as modern ONTAP systems no longer suffer any noticeable performance decline when using indirect paths.
- Aggregate space savings due to storage efficiency might not be reported.
- Where supported, load-sharing mirrors cannot be updated.
- EMS logging might not be performed on ONTAP systems managed with SVM scoped credentials.

## **Operational best practices**

### **Datastores and protocols**

If possible, always use ONTAP tools to provision datastores and volumes. This makes sure that volumes, junction paths, LUNs, igroups, export policies, and other settings are configured in a compatible manner.

SRM supports iSCSI, Fibre Channel, and NFS version 3 with ONTAP 9 when using array-based replication through SRA. SRM does not support array-based replication for NFS version 4.1 with either traditional or vVols datastores.

To confirm connectivity, always verify that you can mount and unmount a new test datastore at the DR site from the destination ONTAP cluster. Test each protocol you intend to use for datastore connectivity. A best practice is to use ONTAP tools to create your test datastore, since it is doing all the datastore automation as directed by SRM.

SAN protocols should be homogeneous for each site. You can mix NFS and SAN, but the SAN protocols should not be mixed within a site. For example, you can use FCP in site A, and iSCSI in site B. You should not use both FCP and iSCSI at site A. The reason for this is that the SRA does not create mixed igroups at the recovery site and SRM does not filter the initiator list given to the SRA.

Previous guides advised to create LIF to data locality. That is to say, always mount a datastore using a LIF located on the node that physically owns the volume. That is no longer a requirement in modern versions of ONTAP 9. Whenever possible, and if given cluster scoped credentials, ONTAP tools will still choose to load balance across LIFs local to the data, but it is not a requirement for high availability or performance.

NetApp ONTAP 9 can be configured to automatically remove Snapshot copies to preserve uptime in the event of an out-of-space condition when autosize is not able to supply sufficient emergency capacity. The default setting for this capability does not automatically delete the Snapshot copies that are created by SnapMirror. If SnapMirror Snapshot copies are deleted, then the NetApp SRA cannot reverse and resynchronize replication for the affected volume. To prevent ONTAP from deleting SnapMirror Snapshot copies, configure the Snapshot autodelete capability to try.

```
snap autodelete modify -volume -commitment try
```

Volume autosize should be set to grow for volumes containing SAN datastores and grow\_shrink for NFS datastores. Refer to the [ONTAP 9 Documentation Center](#) for specific syntax.

## SPBM and vVols

Starting with SRM 8.3, protection of VMs using vVols datastores is supported. SnapMirror schedules are exposed to VM storage policies by the VASA Provider when vVols replication is enabled in the ONTAP tools settings menu, as shown in the following screenshots.

The following example show the enablement of vVols replication.

## Manage Capabilities

### Enable VASA Provider

vStorage APIs for Storage Awareness (VASA) is a set of application program interfaces (APIs) that enables vSphere vCenter to recognize the capabilities of storage arrays.

### Enable vVols replication

Enables replication of vVols when used with VMware Site Recovery Manager 8.3 or later.

### Enable Storage Replication Adapter (SRA)

Storage Replication Adapter (SRA) allows VMware Site Recovery Manager (SRM) to integrate with third party storage array technology.

Enter authentication details for VASA Provider and SRA server:

IP address or hostname: 192.168.64.7

Username: Administrator

Password: \_\_\_\_\_

CANCEL

APPLY

The following screenshot provides an example of SnapMirror schedules displayed in the Create VM Storage Policy wizard.

Create VM Storage Policy

NetApp.clustered.Data.ONTAP.VP.vvol rules

Placement Replication Tags

Disabled  
 Custom

Provider: NetApp.clustered.Data.ONTAP.VP.vvolReplication

Replication: Asynchronous

Replication Schedule: [Select Value]  
[Select Value]  
hourly

CANCEL BACK NEXT

The ONTAP VASA Provider supports failover to dissimilar storage. For example, the system can fail over from ONTAP Select at an edge location to an AFF system in the core datacenter. Regardless of storage similarity, you must always configure storage policy mappings and reverse mappings for replication-enabled VM storage policies to make sure that services provided at the recovery site meet expectations and requirements. The following screenshot highlights a sample policy mapping.

New Storage Policy Mappings

Recovery storage policies

Configure recovery storage policy mappings for one or more storage policies.

vc1.demo.netapp.com	vc2.demo.netapp.com
<input type="radio"/> vc1.demo.netapp.com	<input type="radio"/> vc2.demo.netapp.com
<input type="radio"/> Host-local PMem Default Storage Policy	<input type="radio"/> Host-local PMem Default Storage Policy
<input type="radio"/> VC1 Storage Policy *	<input type="radio"/> VC2 Storage Policy
<input type="radio"/> VM Encryption Policy	<input type="radio"/> VM Encryption Policy
<input type="radio"/> vSAN Default Storage Policy	<input type="radio"/> vSAN Default Storage Policy
<input type="radio"/> VVol No Requirements Policy	<input type="radio"/> VVol No Requirements Policy

vc1.demo.netapp.com vc2.demo.netapp.com

VOLUME MAPPINGS

vc1.demo.netapp.com vc2.demo.netapp.com

VC1 Storage Policy VC2 Storage Policy

1 mapping(s)

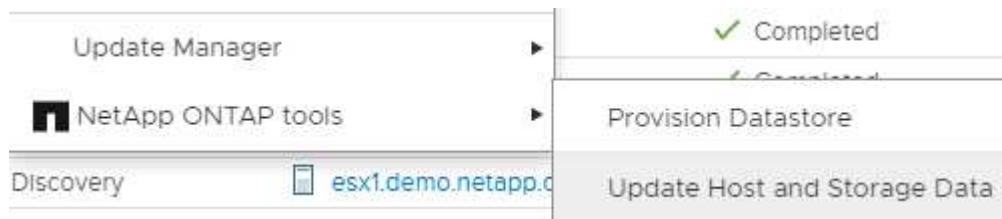
CANCEL BACK NEXT

### Create replicated volumes for vVols datastores

Unlike previous vVols datastores, replicated vVols datastores must be created from the start with replication enabled, and they must use volumes that were pre-created on the ONTAP systems with SnapMirror

relationships. This requires pre-configuring things like cluster peering and SVM peering. These activities should be performed by your ONTAP administrator, because this facilitates a strict separation of responsibilities between those who manage the ONTAP systems across multiple sites and those who are primarily responsible for vSphere operations.

This does come with a new requirement on behalf of the vSphere administrator. Because volumes are being created outside the scope of ONTAP tools, it is unaware of the changes your ONTAP administrator has made until the regularly scheduled rediscovery period. For that reason, it is a best practice to always run rediscovery whenever you create a volume or SnapMirror relationship to be used with vVols. Simply right click on the host or cluster and select NetApp ONTAP tools > Update Host and Storage Data, as shown in the following screenshot.



One caution should be taken when it comes to vVols and SRM. Never mix protected and unprotected VMs in the same vVols datastore. The reason for this is that when you use SRM to failover to your DR site, only those VMs that are part of the protection group are brought online in DR. Therefore, when you reprotect (reverse the SnapMirror from DR back to production again), you may overwrite the VMs that were not failed over and could contain valuable data.

#### About array pairs

An array manager is created for each array pair. With SRM and ONTAP tools, each array pairing is done with the scope of an SVM, even if you are using cluster credentials. This allows you to segment DR workflows between tenants based on which SVMs they have been assigned to manage. You can create multiple array managers for a given cluster, and they can be asymmetric in nature. You can fan out or fan in between different ONTAP 9 clusters. For example, you can have SVM-A and SVM-B on Cluster-1 replicating to SVM-C on Cluster-2, SVM-D on Cluster-3, or vice-versa.

When configuring array pairs in SRM, you should always add them in SRM the same way as you added them to ONTAP Tools, meaning, they must use the same username, password, and management LIF. This requirement ensures that SRA communicates properly with the array. The following screenshot illustrates how a cluster might appear in ONTAP Tools and how it might be added to an array manager.

The screenshot shows the vSphere Client interface with the 'Storage Systems' tab selected. The left sidebar has 'Storage Systems' highlighted. The main pane displays a table with one row: 'cluster2' under 'Name', 'Cluster' under 'Type', and 'cluster2.demo.netapp.com' under 'IP Address'. A red arrow points from the 'cluster2 demo.netapp.com' entry in the table to the corresponding input field in the 'Edit Local Array Manager' dialog.

## Edit Local Array Manager

Enter a name for the array manager on "vc2.demo.netapp.com":

vc2\_array\_manager

Storage Array Parameters

Storage Management IP Address or Hostname

cluster2 demo.netapp.com

Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.

## About replication groups

Replication groups contain logical collections of virtual machines that are recovered together. The ONTAP tools VASA Provider automatically creates replication groups for you. Because ONTAP SnapMirror replication occurs at the volume level, all VMs in a volume are in the same replication group.

There are several factors to consider with replication groups and how you distribute VMs across FlexVol volumes. Grouping similar VMs in the same volume can increase storage efficiency with older ONTAP systems that lack aggregate-level deduplication, but grouping increases the size of the volume and reduces volume I/O concurrency. The best balance of performance and storage efficiency can be achieved in modern ONTAP systems by distributing VMs across FlexVol volumes in the same aggregate, thereby leveraging aggregate level deduplication and gaining greater I/O parallelization across multiple volumes. You can recover VMs in the volumes together because a protection group (discussed below) can contain multiple replication groups. The downside to this layout is that blocks might be transmitted over the wire multiple times because volume SnapMirror doesn't take aggregate deduplication into account.

One final consideration for replication groups is that each one is by its nature a logical consistency group (not to be confused with SRM consistency groups). This is because all VMs in the volume are transferred together using the same snapshot. So if you have VMs that must be consistent with each other, consider storing them in the same FlexVol.

## About protection groups

Protection groups define VMs and datastores in groups that are recovered together from the protected site. The protected site is where the VMs that are configured in a protection group exist during normal steady-state operations. It is important to note that even though SRM might display multiple array managers for a protection group, a protection group cannot span multiple array managers. For this reason, you should not span VM files across datastores on different SVMs.

## About recovery plans

Recovery plans define which protection groups are recovered in the same process. Multiple protection groups can be configured in the same recovery plan. Also, to enable more options for the execution of recovery plans,

a single protection group can be included in multiple recovery plans.

Recovery plans allow SRM administrators to define recovery workflows by assigning VMs to a priority group from 1 (highest) to 5 (lowest), with 3 (medium) being the default. Within a priority group, VMs can be configured for dependencies.

For example, your company could have a tier-1 business critical application that relies on a Microsoft SQL server for its database. So, you decide to place your VMs in priority group 1. Within priority group 1, you begin planning the order to bring up services. You probably want your Microsoft Windows domain controller to boot up before your Microsoft SQL server, which would need to be online before your application server, and so on. You would add all these VMs to the priority group and then set the dependencies, because dependencies only apply within a given priority group.

NetApp strongly recommends working with your application teams to understand the order of operations required in a failover scenario and to construct your recovery plans accordingly.

### Test failover

As a best practice, always perform a test failover whenever a change is made to the configuration of a protected VM storage. This ensures that, in the event of a disaster, you can trust that Site Recovery Manager is able to restore services within the expected RTO target.

NetApp also recommends confirming in-guest application functionality occasionally, especially after reconfiguring VM storage.

When a test recovery operation is performed, a private test bubble network is created on the ESXi host for the VMs. However, this network is not automatically connected to any physical network adapters and therefore does not provide connectivity between the ESXi hosts. To allow communication among VMs that are running on different ESXi hosts during DR testing, a physical private network is created between the ESXi hosts at the DR site. To verify that the test network is private, the test bubble network can be separated physically or by using VLANs or VLAN tagging. This network must be segregated from the production network because as the VMs are recovered, they cannot be placed on the production network with IP addresses that could conflict with actual production systems. When a recovery plan is created in SRM, the test network that was created can be selected as the private network to connect the VMs to during the test.

After the test has been validated and is no longer required, perform a cleanup operation. Running cleanup returns the protected VMs to their initial state and resets the recovery plan to the Ready state.

### Failover considerations

There are several other considerations when it comes to failing over a site in addition to the order of operations mentioned in this guide.

One issue you might have to contend with is networking differences between sites. Some environments might be able to use the same network IP addresses at both the primary site and the DR site. This ability is referred to as a stretched virtual LAN (VLAN) or stretched network setup. Other environments might have a requirement to use different network IP addresses (for example, in different VLANs) at the primary site relative to the DR site.

VMware offers several ways to solve this problem. For one, network virtualization technologies like VMware NSX-T Data Center abstract the entire networking stack from layers 2 through 7 from the operating environment, allowing for more portable solutions. You can read more about NSX-T options with SRM [here](#).

SRM also gives you the ability to change the network configuration of a VM as it is recovered. This reconfiguration includes settings such as IP addresses, gateway address, and DNS server settings. Different

network settings, which are applied to individual VMs as they are recovered, can be specified in the property's settings of a VM in the recovery plan.

To configure SRM to apply different network settings to multiple VMs without having to edit the properties of each one in the recovery plan, VMware provides a tool called the dr-ip-customizer. For information on how to use this utility, refer to VMware's documentation [here](#).

### **Reprotect**

After a recovery, the recovery site becomes the new production site. Because the recovery operation broke the SnapMirror replication, the new production site is not protected from any future disaster. A best practice is to protect the new production site to another site immediately after a recovery. If the original production site is operational, the VMware administrator can use the original production site as a new recovery site to protect the new production site, effectively reversing the direction of protection. Reprotection is available only in non-catastrophic failures. Therefore, the original vCenter Servers, ESXi servers, SRM servers, and corresponding databases must be eventually recoverable. If they are not available, a new protection group and a new recovery plan must be created.

### **Failback**

A failback operation is fundamentally a failover in a different direction than before. As a best practice, you verify that the original site is back to acceptable levels of functionality before attempting to failback, or, in other words, failover to the original site. If the original site is still compromised, you should delay failback until the failure is sufficiently remediated.

Another failback best practice is to always perform a test failover after completing reprotect and before doing your final failback. This verifies that the systems in place at the original site can complete the operation.

#### **Reprotecting the original site**

After failback, you should confirm with all stakeholders that their services have been returned to normal before running reprotect again.

Running reprotect after failback essentially puts the environment back in the state it was in at the beginning, with SnapMirror replication again running from the production site to the recovery site.

### **Replication topologies**

In ONTAP 9, the physical components of a cluster are visible to cluster administrators, but they are not directly visible to the applications and hosts that use the cluster. The physical components provide a pool of shared resources from which the logical cluster resources are constructed. Applications and hosts access data only through SVMs that contain volumes and LIFs.

Each NetApp SVM is treated as an array in VMware vCenter Site Recovery Manager. SRM supports certain array-to-array (or SVM-to-SVM) replication layouts.

A single VM cannot own data—Virtual Machine Disk (VMDK) or RDM—on more than one SRM array for the following reasons:

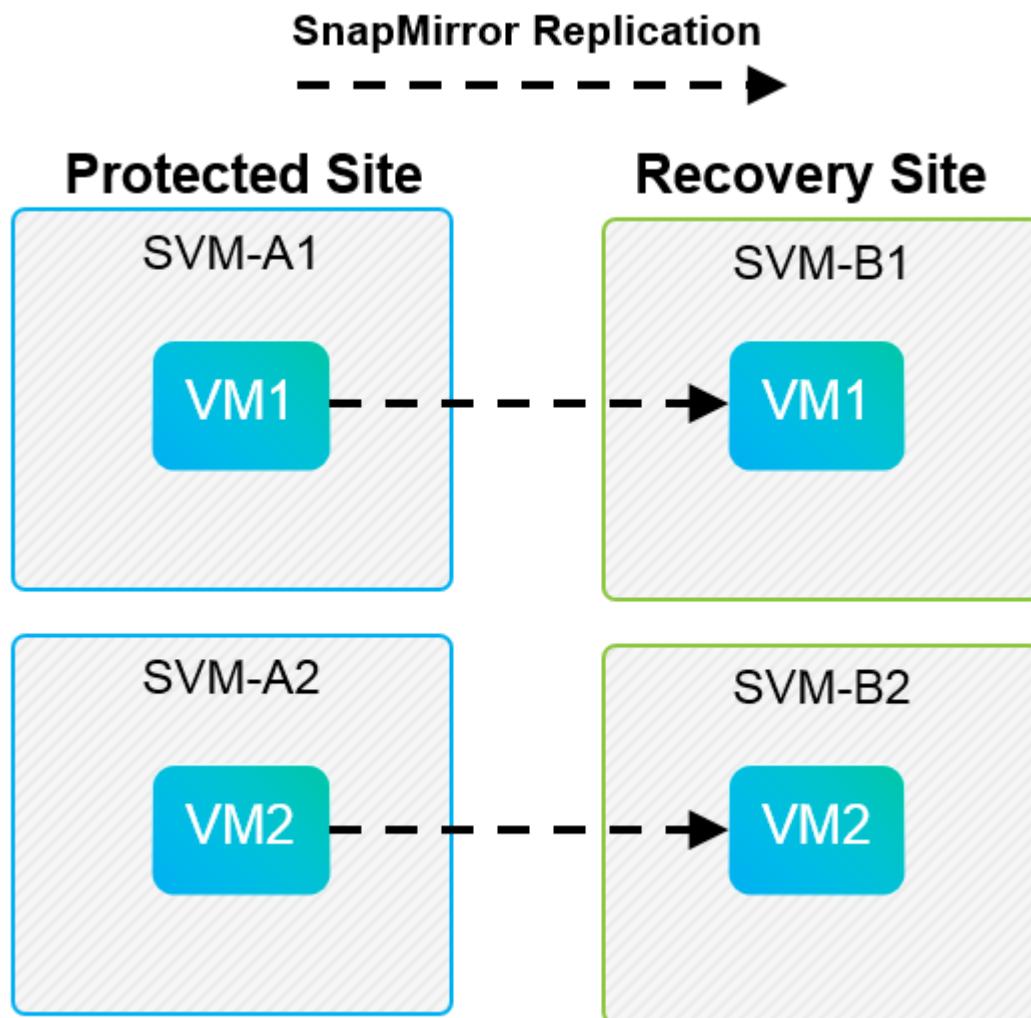
- SRM sees only the SVM, not an individual physical controller.
- An SVM can control LUNs and volumes that span multiple nodes in a cluster.

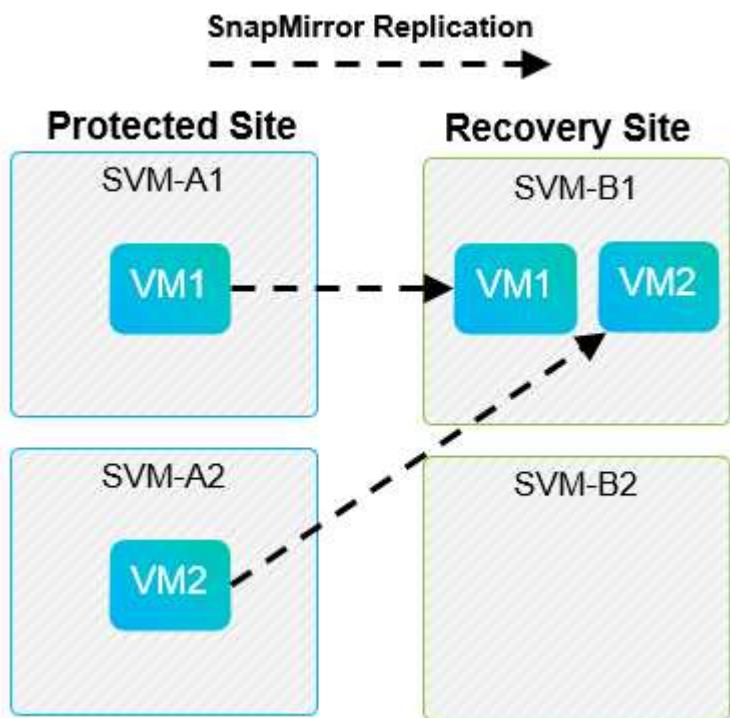
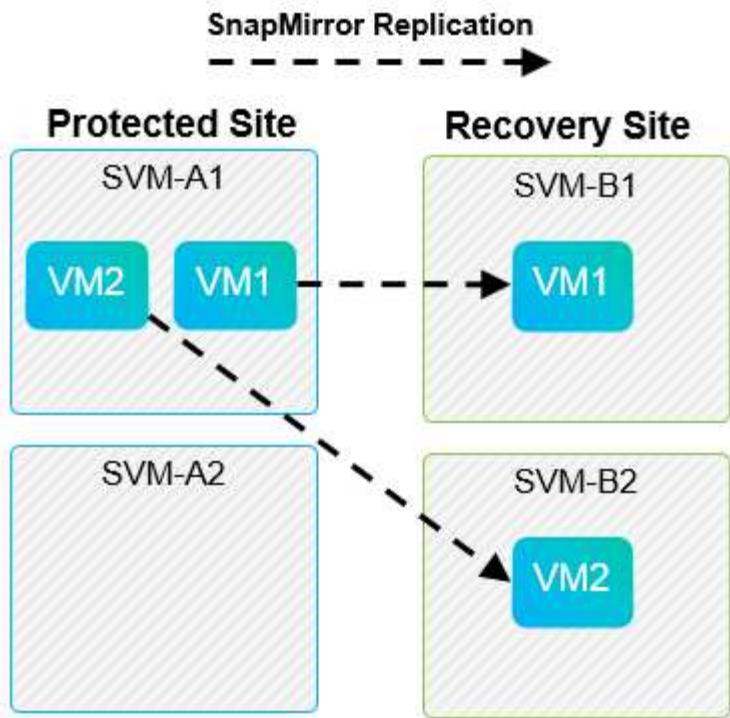
## Best Practice

To determine supportability, keep this rule in mind: to protect a VM by using SRM and the NetApp SRA, all parts of the VM must exist on only one SVM. This rule applies at both the protected site and the recovery site.

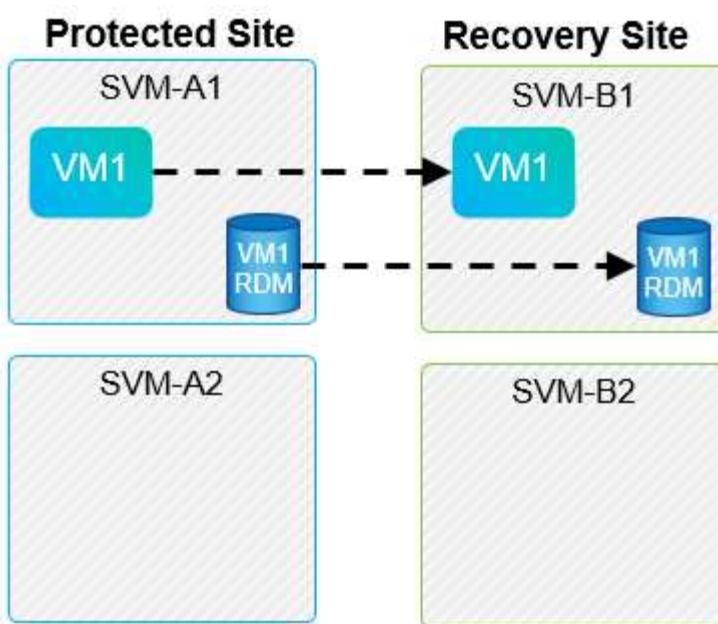
### Supported SnapMirror layouts

The following figures show the SnapMirror relationship layout scenarios that SRM and SRA support. Each VM in the replicated volumes owns data on only one SRM array (SVM) at each site.





## SnapMirror Replication



### Supported Array Manager layouts

When you use array-based replication (ABR) in SRM, protection groups are isolated to a single array pair, as shown in the following screenshot. In this scenario, SVM1 and SVM2 are peered with SVM3 and SVM4 at the recovery site. However, you can select only one of the two array pairs when you create a protection group.

New Protection Group

1 Name and direction

2 Type

3 Datastore groups

4 Recovery plan

5 Ready to complete

Type

Select the type of protection group you want to create:

Datastore groups (array-based replication)  
Protect all virtual machines which are on specific datastores.

Individual VMs (vSphere Replication)  
Protect specific virtual machines, regardless of the datastores.

Virtual Volumes (vVol replication)  
Protect virtual machines which are on replicated vVol storage.

Storage policies (array-based replication)  
Protect virtual machines with specific storage policies.

Select array pair

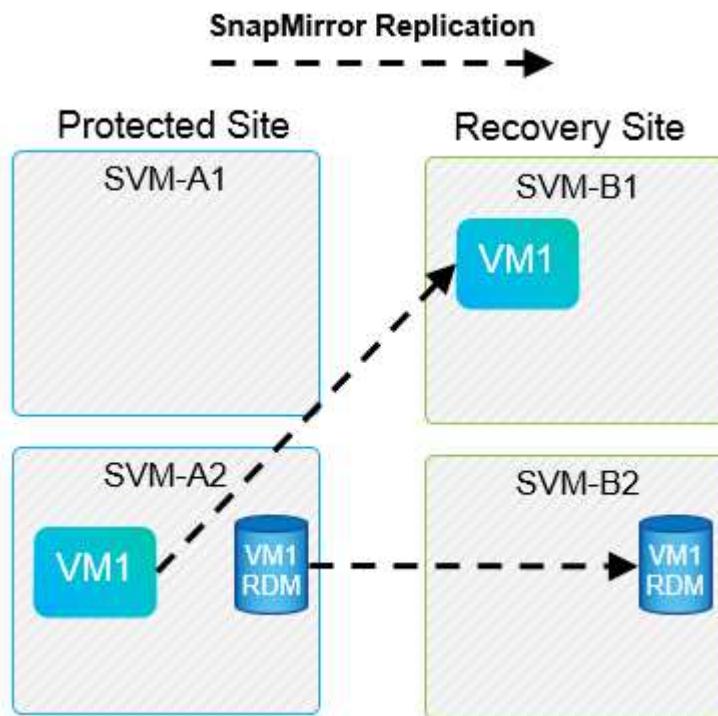
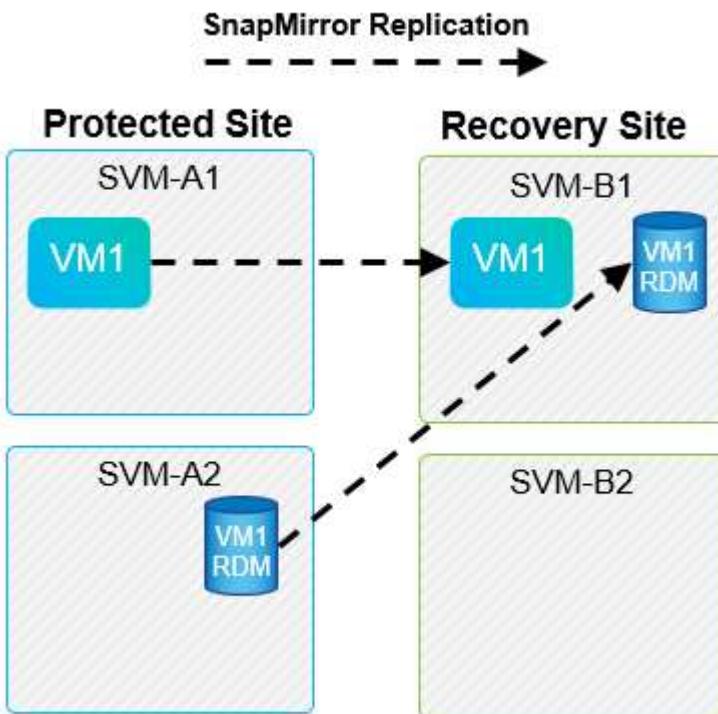
Array Pair	Array Manager Pair
<input type="radio"/> ✓ cluster1:svm1 ↔ cluster2:svm2	vc1 array manager ↔ vc2 array manager
<input type="radio"/> ✓ cluster1:svm3 ↔ cluster2:svm4	vc1 trad datastores ↔ vc2 trad datastores

CANCEL BACK NEXT

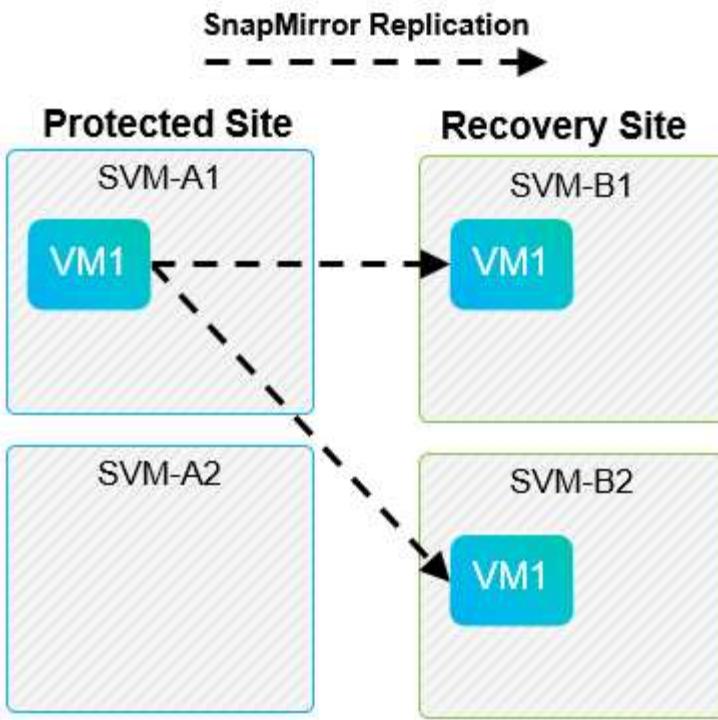
### Unsupported layouts

Unsupported configurations have data (VMDK or RDM) on multiple SVMs that is owned by an individual VM. In

In the examples shown in the following figures, VM1 cannot be configured for protection with SRM because VM1 has data on two SVMs.

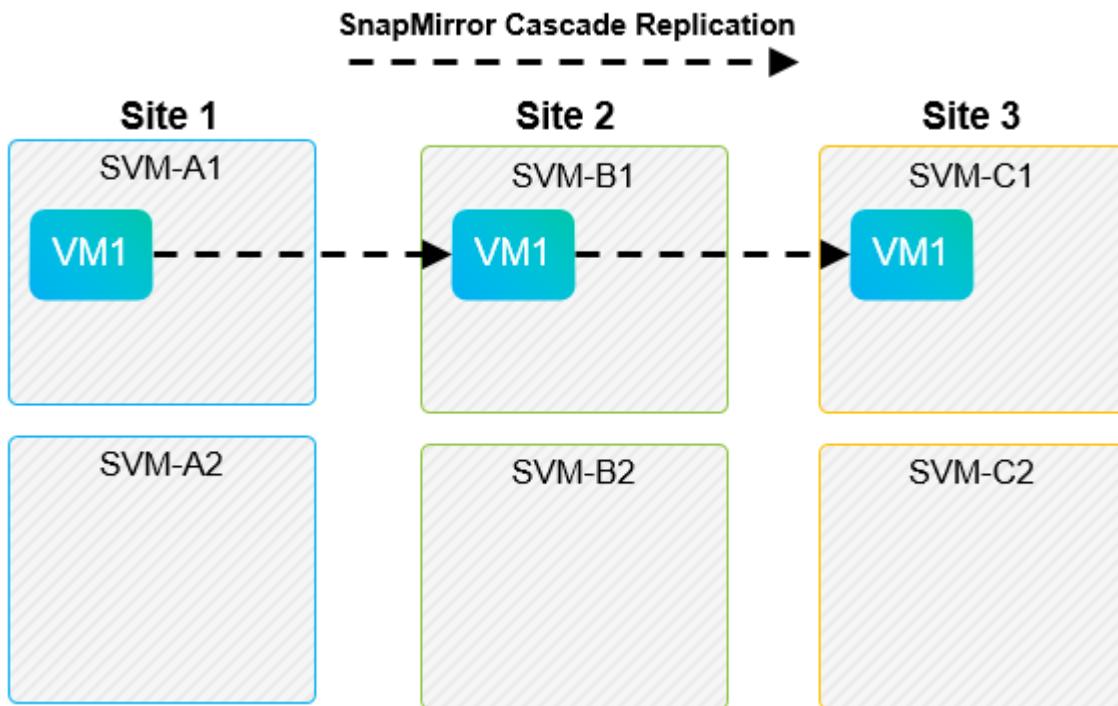


Any replication relationship in which an individual NetApp volume is replicated from one source SVM to multiple destinations in the same SVM or in different SVMs is referred to as SnapMirror fan-out. Fan-out is not supported with SRM. In the example shown in the following figure, VM1 cannot be configured for protection in SRM because it is replicated with SnapMirror to two different locations.



#### SnapMirror cascade

SRM does not support cascading of SnapMirror relationships, in which a source volume is replicated to a destination volume and that destination volume is also replicated with SnapMirror to another destination volume. In the scenario shown in the following figure, SRM cannot be used for failover between any sites.



#### SnapMirror and SnapVault

NetApp SnapVault software enables disk-based backup of enterprise data between NetApp storage systems. SnapVault and SnapMirror can coexist in the same environment; however, SRM supports the failover of only

the SnapMirror relationships.



The NetApp SRA supports the `mirror-vault` policy type.

SnapVault was rebuilt from the ground up for ONTAP 8.2. Although former Data ONTAP 7-Mode users should find similarities, major enhancements have been made in this version of SnapVault. One major advance is the ability to preserve storage efficiencies on primary data during SnapVault transfers.

An important architectural change is that SnapVault in ONTAP 9 replicates at the volume level as opposed to at the qtree level, as is the case in 7-Mode SnapVault. This setup means that the source of a SnapVault relationship must be a volume, and that volume must replicate to its own volume on the SnapVault secondary system.

In an environment in which SnapVault is used, specifically named Snapshot copies are created on the primary storage system. Depending on the configuration implemented, the named Snapshot copies can be created on the primary system by a SnapVault schedule or by an application such as NetApp Active IQ Unified Manager. The named Snapshot copies that are created on the primary system are then replicated to the SnapMirror destination, and from there they are vaulted to the SnapVault destination.

A source volume can be created in a cascade configuration in which a volume is replicated to a SnapMirror destination in the DR site, and from there it is vaulted to a SnapVault destination. A source volume can also be created in a fan-out relationship in which one destination is a SnapMirror destination and the other destination is a SnapVault destination. However, SRA does not automatically reconfigure the SnapVault relationship to use the SnapMirror destination volume as the source for the vault when SRM failover or replication reversal occurs.

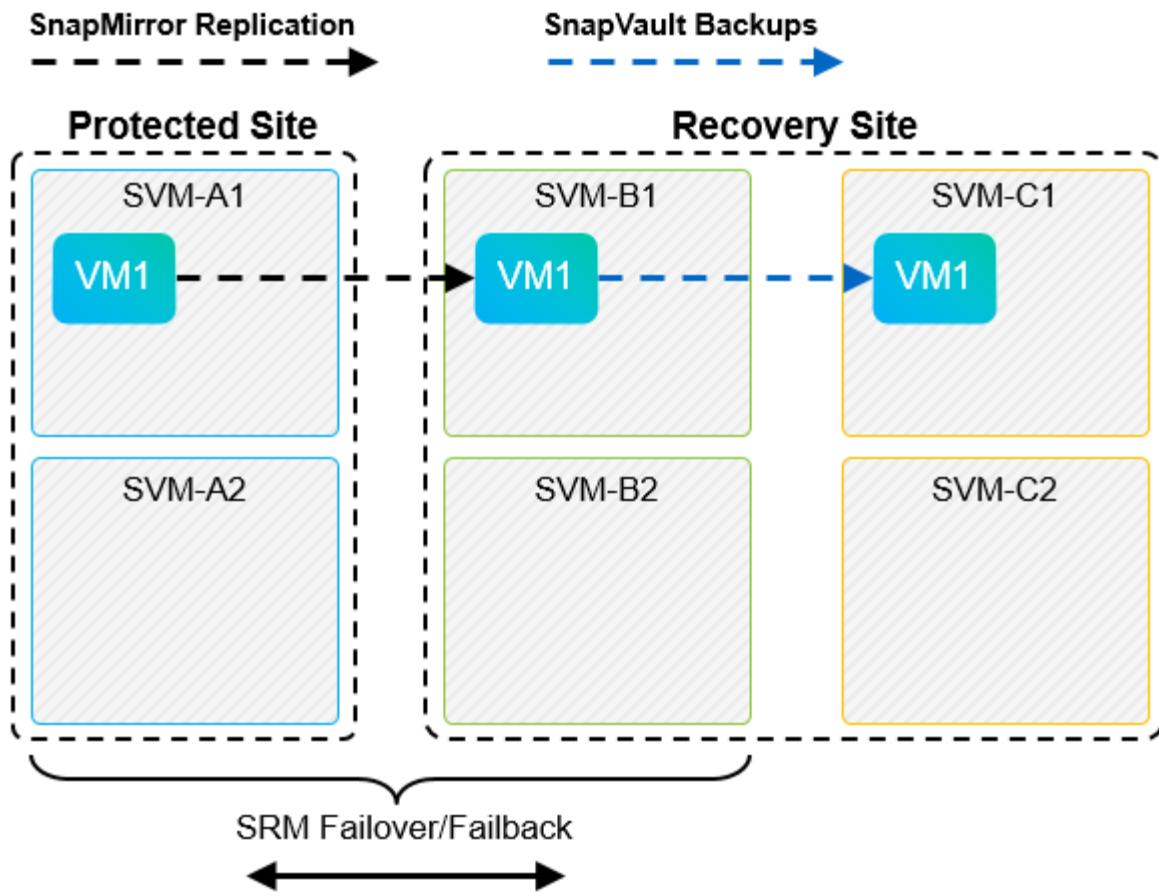
For the latest information about SnapMirror and SnapVault for ONTAP 9, see [TR-4015 SnapMirror Configuration Best Practice Guide for ONTAP 9](#).

### Best Practice

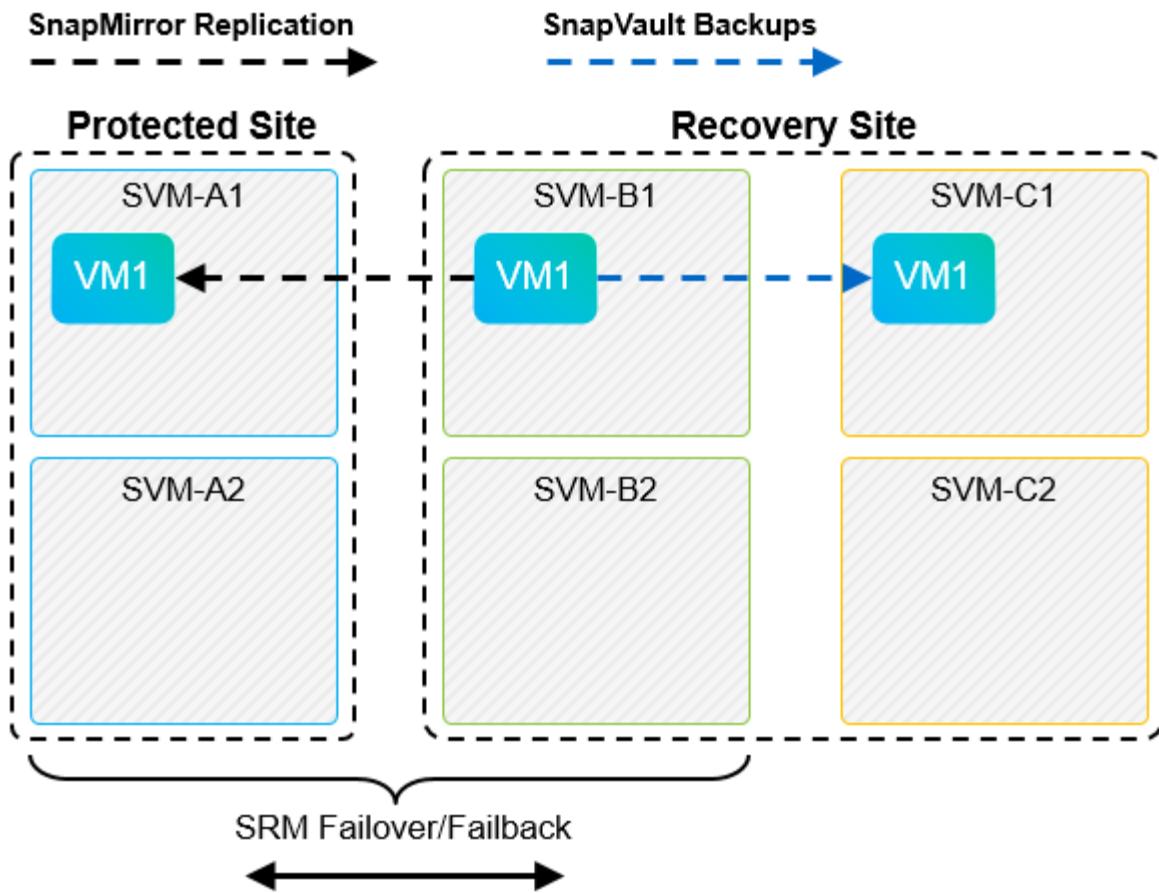
If SnapVault and SRM are used in the same environment, NetApp recommends using a SnapMirror to SnapVault cascade configuration in which SnapVault backups are normally performed from the SnapMirror destination at the DR site. In the event of a disaster, this configuration makes the primary site inaccessible. Keeping the SnapVault destination at the recovery site allows SnapVault backups to be reconfigured after failover so that SnapVault backups can continue while operating at the recovery site.

In a VMware environment, each datastore has a universal unique identifier (UUID), and each VM has a unique managed object ID (MOID). These IDs are not maintained by SRM during failover or failback. Because datastore UUIDs and VM MOIDs are not maintained during failover by SRM, any applications that depend on these IDs must be reconfigured after SRM failover. An example application is NetApp Active IQ Unified Manager, which coordinates SnapVault replication with the vSphere environment.

The following figure depicts a SnapMirror to SnapVault cascade configuration. If the SnapVault destination is at the DR site or at a tertiary site that is not affected by an outage at the primary site, the environment can be reconfigured to allow backups to continue after failover.



The following figure depicts the configuration after SRM has been used to reverse SnapMirror replication back to the primary site. The environment has also been reconfigured such that SnapVault backups are occurring from what is now the SnapMirror source. This setup is a SnapMirror SnapVault fan-out configuration.



After SRM performs failover and a second reversal of the SnapMirror relationships, the production data is back at the primary site. This data is now protected in the same way that it was before the failover to the DR site—through SnapMirror and SnapVault backups.

#### Use of Qtrees in Site Recovery Manager environments

Qtrees are special directories that allow the application of file system quotas for NAS. ONTAP 9 allows the creation of qtrees, and qtrees can exist in volumes that are replicated with SnapMirror. However, SnapMirror does not allow replication of individual qtrees or qtree-level replication. All SnapMirror replication is at the volume level only. For this reason, NetApp does not recommend the use of qtrees with SRM.

#### Mixed FC and iSCSI environments

With the supported SAN protocols (FC, FCoE, and iSCSI), ONTAP 9 provides LUN services—that is, the ability to create and map LUNs to attached hosts. Because the cluster consists of multiple controllers, there are multiple logical paths that are managed by multipath I/O to any individual LUN. Asymmetric logical unit access (ALUA) is used on the hosts so that the optimized path to a LUN is selected and is made active for data transfer. If the optimized path to any LUN changes (for example, because the containing volume is moved), ONTAP 9 automatically recognizes and nondisruptively adjusts for this change. If the optimized path becomes unavailable, ONTAP can nondisruptively switch to any other available path.

VMware SRM and NetApp SRA support the use of the FC protocol at one site and the iSCSI protocol at the other site. It does not support having a mix of FC-attached datastores and iSCSI-attached datastores in the same ESXi host or in different hosts in the same cluster, however. This configuration is not supported with SRM because, during the SRM failover or test failover, SRM includes all FC and iSCSI initiators in the ESXi hosts in the request.

## **Best Practice**

SRM and SRA support mixed FC and iSCSI protocols between the protected and recovery sites. However, each site should be configured with only one protocol, either FC or iSCSI, not both protocols at the same site. If a requirement exists to have both FC and iSCSI protocols configured at the same site, NetApp recommends that some hosts use iSCSI and other hosts use FC. NetApp also recommends in this case that SRM resource mappings be set up so that the VMs are configured to fail over into one group of hosts or the other.

## **Troubleshooting SRM when using vVols replication**

The workflow within SRM is significantly different when using vVols replication from what is used with SRA and traditional datastores. For example, there is no array manager concept. As such, `discoverarrays` and `discoverdevices` commands are never seen.

When troubleshooting, it is beneficial to understand the new workflows, which are listed below:

1. `queryReplicationPeer`: Discovers the replication agreements between two fault domains.
2. `queryFaultDomain`: Discovers fault domain hierarchy.
3. `queryReplicationGroup`: Discovers the replication groups present in the source or target domains.
4. `syncReplicationGroup`: Synchronizes the data between source and target.
5. `queryPointInTimeReplica`: Discovers the point in time replicas on a target.
6. `testFailoverReplicationGroupStart`: Begins test failover.
7. `testFailoverReplicationGroupStop`: Ends test failover.
8. `promoteReplicationGroup`: Promotes a group currently in test to production.
9. `prepareFailoverReplicationGroup`: Prepares for a disaster recovery.
10. `failoverReplicationGroup`: Executes disaster recovery.
11. `reverseReplicateGroup`: Initiates reverse replication.
12. `queryMatchingContainer`: Finds containers (along with Hosts or Replication Groups) that might satisfy a provisioning request with a given policy.
13. `queryResourceMetadata`: Discovers the metadata of all resources from the VASA provider, the resource utilization can be returned as an answer to the `queryMatchingContainer` function.

The most common error seen when configuring vVols replication is a failure to discover the SnapMirror relationships. This occurs because the volumes and SnapMirror relationships are created outside of the purview of ONTAP Tools. Therefore, it is a best practice to always make sure your SnapMirror relationship is fully initialized and that you have run a rediscovery in ONTAP Tools at both sites before attempting to create a replicated vVols datastore.

## **Conclusion**

VMware vCenter Site Recovery Manager is a disaster recovery offering that provides automated orchestration and nondisruptive testing of centralized recovery plans to simplify disaster recovery management for all virtualized applications.

By deploying Site Recovery Manager on NetApp ONTAP systems, you can dramatically lower the cost and complexity of disaster recovery. With high-performance, easy-to-manage, and scalable storage appliances and robust software offerings, NetApp offers flexible storage and data management solutions to support vSphere environments.

The best practices and recommendations that are provided in this guide are not a one-size-fits-all solution. This document contains a collection of best practices and recommendations that provide guidelines to plan, deploy, and manage SRM DR plans. Consult with a local NetApp VMware expert when you plan and deploy VMware vCenter Site Recovery environments onto NetApp storage. NetApp VMware experts can quickly identify the needs and demands of any vSphere environment and can adjust the storage solution accordingly.

## Additional Information

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

- TR-4597: VMware vSphere for ONTAP  
[https://docs.netapp.com/us-en/netapp-solutions/virtualization/vsphere\\_ontap\\_ontap\\_for\\_vsphere.html](https://docs.netapp.com/us-en/netapp-solutions/virtualization/vsphere_ontap_ontap_for_vsphere.html)
- TR-4400: VMware vSphere Virtual Volumes with ONTAP  
<https://www.netapp.com/pdf.html?item=/media/13555-tr4400.pdf>
- TR-4015 SnapMirror Configuration Best Practice Guide for ONTAP 9  
<https://www.netapp.com/media/17229-tr4015.pdf?v=127202175503P>
- RBAC User Creator for ONTAP  
<https://mysupport.netapp.com/site/tools/tool-eula/rbac>
- ONTAP tools for VMware vSphere Resources  
<https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab>
- VMware Site Recovery Manager Documentation  
<https://docs.vmware.com/en/Site-Recovery-Manager/index.html>

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.

## WP-7353: ONTAP tools for VMware vSphere - Product Security

Chance Bingen, Dan Tulleedge, Jenn Schrie, NetApp

### Secure development activities

Software engineering with NetApp ONTAP Tools for VMware vSphere employs the following secure development activities:

- **Threat modeling.** The purpose of threat modelling is to discover security flaws in a feature, component, or product early in the software development life cycle. A threat model is a structured representation of all the information that affects the security of an application. In essence, it is a view of the application and its environment through the lens of security.
- **Dynamic Application Security Testing (DAST).** This technology is designed to detect vulnerable conditions on applications in their running state. DAST tests the exposed HTTP and HTML interfaces of web-enable applications.
- **Third-party code currency.** As part of software development with open-source software (OSS), you must address security vulnerabilities that might be associated with any OSS incorporated into your product. This is a continuing effort because a new OSS version might have a newly discovered vulnerability reported at any time.

- **Vulnerability scanning.** The purpose of vulnerability scanning is to detect common and known security vulnerabilities in NetApp products before they are released to customers.
- **Penetration testing.** Penetration testing is the process of evaluating a system, web application, or network to find security vulnerabilities that could be exploited by an attacker. Penetration tests (pen tests) at NetApp are conducted by a group of approved and trusted third-party companies. Their testing scope includes the launching of attacks against an application or software similar to hostile intruders or hackers using sophisticated exploitation methods or tools.

## Product security features

NetApp ONTAP tools for VMware vSphere includes the following security features in each release.

- **Login banner.** SSH is disabled by default and only allows one-time logins if enabled from the VM console. The following login banner is shown after the user enters a username in the login prompt:

**WARNING:** Unauthorized access to this system is forbidden and will be prosecuted by law. By accessing this system, you agree that your actions may be monitored if unauthorized usage is suspected.

After the user completes login through the SSH channel, the following text is displayed:

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **Role-based access control (RBAC).** Two kinds of RBAC controls are associated with ONTAP tools:
  - Native vCenter Server privileges
  - vCenter plug-in specific privileges. For details, see [this link](#).
- **Encrypted communications channels.** All external communication happens over HTTPS using version 1.2 of TLS.
- **Minimal port exposure.** Only the necessary ports are open on the firewall.

The following table describes the open port details.

TCP v4/v6 port #	Direction	Function
8143	inbound	HTTPS connections for REST API
8043	inbound	HTTPS connections
9060	inbound	HTTPS connections Used for SOAP over https connections This port must be opened to allow a client to connect to the ONTAP tools API server.
22	inbound	SSH (Disabled by default)

TCP v4/v6 port #	Direction	Function
9080	inbound	HTTPS connections - VP and SRA - Internal connections from loopback only
9083	inbound	HTTPS connections - VP and SRA Used for SOAP over https connections
1162	inbound	VP SNMP trap packets
1527	internal only	Derby database port, only between this computer and itself, external connections not accepted — Internal connections only
443	bi-directional	Used for connections to ONTAP clusters

- **Support for certificate authority (CA) signed certificates.** ONTAP tools for VMware vSphere supports CA signed certificates. See this [kb article](#) for more information.
- **Audit logging.** Support bundles can be downloaded and are extremely detailed. ONTAP tools logs all user login and logout activity in a separate log file. VASA API calls are logged in a dedicated VASA audit log (local cxf.log).
- **Password policies.** The following password policies are followed:
  - Passwords are not logged in any log files.
  - Passwords are not communicated in plain text.
  - Passwords are configured during the installation process itself.
  - Password history is a configurable parameter.
  - Minimum password age is set to 24 hours.
  - Auto complete for the password fields are disabled.
  - ONTAP tools encrypts all stored credential information using SHA256 hashing.

## Version history

Version	Date	Document version history
Version 1.0	November 2021	Initial release

## Introduction to automation for ONTAP and vSphere

### VMware automation

Automation has been an integral part of managing VMware environments since the first days of VMware ESX. The ability to deploy infrastructure as code and extend practices to private cloud operations helps to alleviate concerns surrounding scale, flexibility, self-provisioning, and efficiency.

Automation can be organized into the following categories:

- **Virtual infrastructure deployment**
- **Guest machine operations**
- **Cloud operations**

There are many options available to administrators with respect to automating their infrastructure. Whether through using native vSphere features such as Host Profiles or Customization Specifications for virtual machines to available APIs on the VMware software components, operating systems, and NetApp storage systems; there is significant documentation and guidance available.

Data ONTAP 8.0.1 and later supports certain VMware vSphere APIs for Array Integration (VAAI) features when the ESX host is running ESX 4.1 or later. VAAI is a set of APIs that enable communication between VMware vSphere ESXi hosts and storage devices. These features help offload operations from the ESX host to the storage system and increase network throughput. The ESX host enables the features automatically in the correct environment. You can determine the extent to which your system is using VAAI features by checking the statistics contained in the VAAI counters.

The most common starting point for automating the deployment of a VMware environment is provisioning block or file-based datastores. It is important to map out the requirements of the actual tasks prior to developing the corresponding automation.

For more information concerning the automation of VMware environments, see the following resources:

- [The NetApp Pub](#). NetApp configuration management and automation.
- [The Ansible Galaxy Community for VMware](#). A collection of Ansible resources for VMware.
- [VMware {code} Resources](#). Resources needed to design solutions for the software-defined data center, including forums, design standards, sample code, and developer tools.

## vSphere traditional block storage provisioning with ONTAP

VMware vSphere supports the following VMFS datastore options with ONTAP SAN protocol support indicated.

VMFS datastore options	ONTAP SAN protocol support
Fibre Channel (FC)	yes
Fibre Channel over Ethernet (FCoE)	yes
iSCSI	yes
iSCSI Extensions for RDMA (iSER)	no
NVMe over Fabric with FC (NVMe/FC)	yes
NVMe over Fabric with RDMA over Converged Ethernet (NVMe/RoCE)	no



If iSER or NVMe/RoCE VMFS is required, check SANtricity-based storage systems.

## vSphere VMFS datastore - Fibre Channel storage backend with ONTAP

### About this task

This section covers the creation of a VMFS datastore with ONTAP Fibre Channel (FC) storage.

For automated provisioning, use one of these scripts: [\[PowerShell\]](#), [Ansible Playbook](#), or [\[Terraform\]](#).

## What you need

- The basic skills necessary to manage a vSphere environment and ONTAP
- An ONTAP storage system (FAS/AFF/CVO/ONTAP Select/ASA) running ONTAP 9.8 or later
- ONTAP credentials (SVM name, userID, and password)
- ONTAP WWPN of host, target, and SVM and LUN information
- [The completed FC configuration worksheet](#)
- vCenter Server credentials
- vSphere host(s) information
  - vSphere 7.0 or later
- Fabric switch(es)
  - With connected ONTAP FC data ports and vSphere hosts
  - With the N\_port ID virtualization (NPIV) feature enabled
  - Create a single initiator single target zone.
    - Create one zone for each initiator (single initiator zone).
    - For each zone, include a target that is the ONTAP FC logical interface (WWPN) for the SVMs. There should be at least two logical interfaces per node per SVM. Do not use the WWPN of the physical ports.
- An ONTAP Tool for VMware vSphere deployed, configured, and ready to consume.

## Provisioning a VMFS datastore

To provision a VMFS datastore, complete the following steps:

1. Check compatibility with the [Interoperability Matrix Tool \(IMT\)](#)
2. Verify that the [FCP Configuration is supported](#).

## ONTAP tasks

1. [Verify that you have an ONTAP license for FCP.](#)
  - a. Use the `system license show` command to check that FCP is listed.
  - b. Use `license add -license-code <license code>` to add the license.
2. Make sure that the FCP protocol is enabled on the SVM.
  - a. [Verify the FCP on an existing SVM.](#)
  - b. [Configure the FCP on an existing SVM.](#)
  - c. [Create a new SVM with the FCP.](#)
3. Make sure that FCP logical interfaces are available on an SVM.
  - a. Use `Network Interface show` to verify the FCP adapter.
  - b. When an SVM is created with the GUI, logical interfaces are a part of that process.
  - c. To rename network interfaces, use `Network Interface modify`.

4. [Create and Map a LUN](#). Skip this step if you are using ONTAP tools for VMware vSphere.

## VMware vSphere tasks

1. Verify that HBA drivers are installed. VMware supported HBAs have drivers deployed out of the box and should be visible in the [Storage Adapter Information](#).
2. [Provision a VMFS datastore with ONTAP Tools](#).

### vSphere VMFS Datastore - Fibre Channel over Ethernet storage protocol with ONTAP

#### About this task

This section covers the creation of a VMFS datastore with the Fibre Channel over Ethernet (FCoE) transport protocol to ONTAP storage.

For automated provisioning, use one of these scripts: [\[PowerShell\]](#), [Ansible Playbook](#), or [\[Terraform\]](#).

#### What you need

- The basic skills necessary to manage a vSphere environment and ONTAP
- An ONTAP storage system (FAS/AFF/CVO/ONTAP Select) running ONTAP 9.8 or later
- ONTAP credentials (SVM name, userID, and password)
- [A supported FCoE combination](#)
- [A completed configuration worksheet](#)
- vCenter Server credentials
- vSphere host(s) information
  - vSphere 7.0 or later
- Fabric switch(es)
  - With either ONTAP FC data ports or vSphere hosts connected
  - With the N\_port ID virtualization (NPIV) feature enabled
  - Create a single initiator single target zone.
  - [FC/FCoE zoning configured](#)
- Network switch(es)
  - FCoE support
  - DCB support
  - [Jumbo frames for FCoE](#)
- ONTAP Tool for VMware vSphere deployed, configured, and ready to consume

#### Provision a VMFS datastore

- Check compatibility with the [Interoperability Matrix Tool \(IMT\)](#).
- [Verify that the FCoE configuration is supported](#).

## ONTAP tasks

1. [Verify the ONTAP license for FCP.](#)
  - a. Use the system license show command to verify that the FCP is listed.
  - b. Use license add -license-code <license code> to add a license.
2. Verify that the FCP protocol is enabled on the SVM.
  - a. [Verify the FCP on an existing SVM.](#)
  - b. [Configure the FCP on an existing SVM.](#)
  - c. [Create a new SVM with the FCP.](#)
3. Verify that FCP logical interfaces are available on the SVM.
  - a. Use Network Interface show to verify the FCP adapter.
  - b. When the SVM is created with the GUI, logical interfaces are a part of that process.
  - c. To rename the network interface, use Network Interface modify.
4. [Create and map a LUN](#); skip this step if you are using ONTAP tools for VMware vSphere.

## VMware vSphere tasks

1. Verify that HBA drivers are installed. VMware-supported HBAs have drivers deployed out of the box and should be visible in the [storage adapter information](#).
2. [Provision a VMFS datastore with ONTAP Tools](#).

### vSphere VMFS Datastore - iSCSI Storage backend with ONTAP

#### About this task

This section covers the creation of a VMFS datastore with ONTAP iSCSI storage.

For automated provisioning, use one of these scripts: [\[PowerShell\]](#), [Ansible Playbook](#), or [\[Terraform\]](#).

#### What you need

- The basic skills necessary to manage a vSphere environment and ONTAP.
- An ONTAP storage system (FAS/AFF/CVO/ONTAP Select/ASA) running ONTAP 9.8 or later
- ONTAP credentials (SVM name, userID, and password)
- ONTAP network port, SVM, and LUN information for iSCSI
- [A completed iSCSI configuration worksheet](#)
- vCenter Server credentials
- vSphere host(s) information
  - vSphere 7.0 or later
- iSCSI VMKernel adapter IP information
- Network switch(es)
  - With ONTAP system network data ports and connected vSphere hosts
  - VLAN(s) configured for iSCSI

- (Optional) link aggregation configured for ONTAP network data ports
- ONTAP Tool for VMware vSphere deployed, configured, and ready to consume

## Steps

1. Check compatibility with the [Interoperability Matrix Tool \(IMT\)](#).
2. [Verify that the iSCSI configuration is supported](#).
3. Complete the following ONTAP and vSphere tasks.

## ONTAP tasks

1. [Verify the ONTAP license for iSCSI](#).
  - a. Use the `system license show` command to check if iSCSI is listed.
  - b. Use `license add -license-code <license code>` to add the license.
2. [Verify that the iSCSI protocol is enabled on the SVM](#).
3. Verify that iSCSI network logical interfaces are available on the SVM.

 When an SVM is created using the GUI, iSCSI network interfaces are also created.
4. Use the `Network interface` command to view or make changes to the network interface.

 Two iSCSI network interfaces per node are recommended.
5. [Create an iSCSI network interface](#). You can use the `default-data-blocks service policy`.
6. [Verify that the data-iscsi service is included in the service policy](#). You can use `network interface service-policy show` to verify.
7. [Verify that jumbo frames are enabled](#).
8. [Create and map the LUN](#). Skip this step if you are using ONTAP tools for VMware vSphere. Repeat this step for each LUN.

## VMware vSphere tasks

1. Verify that at least one NIC is available for the iSCSI VLAN. Two NICs are preferred for better performance and fault tolerance.
2. [Identify the number of physical NICs available on the vSphere host](#).
3. [Configure the iSCSI initiator](#). A typical use case is a software iSCSI initiator.
4. [Verify that the TCPIP stack for iSCSI is available](#).
5. [Verify that iSCSI portgroups are available](#).
  - We typically use a single virtual switch with multiple uplink ports.
  - Use 1:1 adapter mapping.
6. Verify that iSCSI VMKernel adapters are enabled to match the number of NICs and that IPs are assigned.
7. [Bind the iSCSI software adapter to the iSCSI VMKernel adapter\(s\)](#).
8. [Provision the VMFS datastore with ONTAP Tools](#). Repeat this step for all datastores.

## 9. Verify hardware acceleration support.

### What's next?

After these the tasks are completed, the VMFS datastore is ready to consume for provisioning virtual machines.

### Ansible Playbook

```
## Disclaimer: Sample script for reference purpose only.

- hosts: '{{ vsphere_host }}'
  name: Play for vSphere iSCSI Configuration
  connection: local
  gather_facts: false
  tasks:
    # Generate Session ID for vCenter
    - name: Generate a Session ID for vCenter
      uri:
        url: "https://{{ vcenter_hostname }}/rest/com/vmware/cis/session"
        validate_certs: false
        method: POST
        user: "{{ vcenter_username }}"
        password: "{{ vcenter_password }}"
        force_basic_auth: yes
        return_content: yes
      register: vclogin

    # Generate Session ID for ONTAP tools with vCenter
    - name: Generate a Session ID for ONTAP tools with vCenter
      uri:
        url: "https://{{ ontap_tools_ip }}:8143/api/rest/2.0/security/user/login"
        validate_certs: false
        method: POST
        return_content: yes
        body_format: json
        body:
          vccenterUserName: "{{ vcenter_username }}"
          vccenterPassword: "{{ vcenter_password }}"
      register: login

    # Get existing registered ONTAP Cluster info with ONTAP tools
    - name: Get ONTAP Cluster info from ONTAP tools
      uri:
        url: "https://{{ ontap_tools_ip }}:8143/api/rest/2.0/storage/clusters"
        validate_certs: false
```

```

method: Get
return_content: yes
headers:
    vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
register: clusterinfo

- name: Get ONTAP Cluster ID
  set_fact:
    ontap_cluster_id: "{{ clusterinfo.json | json_query(clusteridquery) }}"
  vars:
    clusteridquery: "records[?ipAddress == '{{ netapp_hostname }}' && type=='Cluster'].id | [0]"

- name: Get ONTAP SVM ID
  set_fact:
    ontap_svm_id: "{{ clusterinfo.json | json_query(svmidquery) }}"
  vars:
    svmidquery: "records[?ipAddress == '{{ netapp_hostname }}' && type=='SVM' && name == '{{ svm_name }}'].id | [0]"

- name: Get Aggregate detail
  uri:
    url: "https://{{ ontap_tools_ip }}:8143/api/rest/2.0/storage/clusters/{{ ontap_svm_id }}/aggregates"
    validate_certs: false
    method: GET
    return_content: yes
  headers:
    vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
    cluster-id: "{{ ontap_svm_id }}"
  when: ontap_svm_id != ''
  register: aggrinfo

- name: Select Aggregate with max free capacity
  set_fact:
    aggr_name: "{{ aggrinfo.json | json_query(aggrquery) }}"
  vars:
    aggrquery: "max_by(records, &freeCapacity).name"

- name: Convert datastore size in MB
  set_fact:
    datastoreSizeInMB: "{{ iscsi_datastore_size | human_to_bytes/1024/1024 | int }}"
  register: datastore_size_mb

- name: Get vSphere Cluster Info

```

```

uri:
  url: "https://{{ vcenter_hostname }}/api/vcenter/cluster?names={{ vsphere_cluster }}"
  validate_certs: false
  method: GET
  return_content: yes
  body_format: json
  headers:
    vmware-api-session-id: "{{ vclogin.json.value }}"
when: vsphere_cluster != ''
register: vcenterclusterid

- name: Create iSCSI VMFS-6 Datastore with ONTAP tools
  uri:
    url: "https://{{ ontap_tools_ip }}:8143/api/rest/3.0/admin/datastore"
    validate_certs: false
    method: POST
    return_content: yes
    status_code: [200]
    body_format: json
    body:
      traditionalDatastoreRequest:
        name: "{{ iscsi_datastore_name }}"
        datastoreType: VMFS
        protocol: ISCSI
        spaceReserve: Thin
        clusterID: "{{ ontap_cluster_id }}"
        svmID: "{{ ontap_svm_id }}"
        targetMoref: ClusterComputeResource:{{ vcenterclusterid.json[0].cluster }}
        datastoreSizeInMB: "{{ datastoreSizeInMB | int }}"
        vmfsFileSystem: VMFS6
        aggrName: "{{ aggr_name }}"
        existingFlexVolName: ""
        volumeStyle: FLEXVOL
        datastoreClusterMoref: ""
    headers:
      vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
when: ontap_cluster_id != '' and ontap_svm_id != '' and aggr_name != ''
register: result
changed_when: result.status == 200

```

## vSphere VMFS Datastore - NVMe/FC with ONTAP

### About this task

This section covers the creation of a VMFS datastore with ONTAP storage using NVMe/FC.

For automated provisioning, use one of these scripts: [\[PowerShell\]](#), [Ansible Playbook](#), or [\[Terraform\]](#).

### What you need

- Basic skills needed to manage a vSphere environment and ONTAP.
- [Basic understanding of NVMe/FC](#).
- An ONTAP Storage System (FAS/AFF/CVO/ONTAP Select/ASA) running ONTAP 9.8 or later
- ONTAP credentials (SVM name, userID, and password)
- ONTAP WWPN for host, target, and SVMs and LUN information
- [A completed FC configuration worksheet](#)
- vCenter Server
- vSphere host(s) information (vSphere 7.0 or later)
- Fabric switch(es)
  - With ONTAP FC data ports and vSphere hosts connected.
  - With the N\_port ID virtualization (NPIV) feature enabled.
  - Create a single initiator target zone.
  - Create one zone for each initiator (single initiator zone).
  - For each zone, include a target that is the ONTAP FC logical interface (WWPN) for the SVMs. There should be at least two logical interfaces per node per SVM. DO not use the WWPN of physical ports.

### Provision VMFS datastore

1. Check compatibility with the [Interoperability Matrix Tool \(IMT\)](#).
2. [Verify that the NVMe/FC configuration is supported](#).

### ONTAP tasks

1. [Verify the ONTAP license for FCP](#).  
Use the system license show command and check if NVMe\_oF is listed.  
Use license add -license-code <license code> to add a license.
2. Verify that NVMe protocol is enabled on the SVM.
  - a. [Configure SVMs for NVMe](#).
3. Verify that NVMe/FC Logical Interfaces are available on the SVMs.
  - a. Use Network Interface show to verify the FCP adapter.
  - b. When an SVM is created with the GUI, logical interfaces are as part of that process.
  - c. To rename the network interface, use the command Network Interface modify.
4. [Create NVMe namespace and subsystem](#)

## VMware vSphere Tasks

1. Verify that HBA drivers are installed. VMware supported HBAs have the drivers deployed out of the box and should be visible at [Storage Adapter Information](#)
2. Perform vSphere Host NVMe driver installation and validation tasks
3. Create VMFS Datastore

## vSphere traditional file storage provisioning with ONTAP

VMware vSphere supports following NFS protocols, both of which support ONTAP.

- [NFS Version 3](#)
- [NFS Version 4.1](#)

If you need help selecting the correct NFS version for vSphere, check [this comparison of NFS client versions](#).

### Reference

[vSphere datastore and protocol features: NFS](#)

### vSphere NFS datastore - Version 3 with ONTAP

#### About this task

Creation of NFS version 3 datastore with ONTAP NAS storage.

For automated provisioning, use one of these scripts: [\[PowerShell\]](#), [Ansible Playbook](#), or [\[Terraform\]](#).

#### What you need

- The basic skill necessary to manage a vSphere environment and ONTAP.
- An ONTAP storage system (FAS/AFF/CVO/ONTAP Select/Cloud Volume Service/Azure NetApp Files) running ONTAP 9.8 or later
- ONTAP credentials (SVM name, userID, password)
- ONTAP network port, SVM, and LUN information for NFS
  - [A completed NFS configuration worksheet](#)
- vCenter Server credentials
- vSphere host(s) information for vSphere 7.0 or later
- NFS VMKernel adapter IP information
- Network switch(es)
  - with ONTAP system network data ports and connected vSphere hosts
  - VLAN(s) configured for NFS
  - (Optional) link aggregation configured for ONTAP network data ports
- ONTAP Tool for VMware vSphere deployed, configured, and ready to consume

#### Steps

- Check compatibility with the [Interoperability Matrix Tool \(IMT\)](#)

- Verify that the NFS configuration is supported.
- Complete the following ONTAP and vSphere tasks.

## ONTAP tasks

1. [Verify the ONTAP license for NFS.](#)
  - a. Use the system license show command and check that NFS is listed.
  - b. Use license add -license-code <license code> to add a license.
2. [Follow the NFS configuration workflow.](#)

## VMware vSphere Tasks

Follow the workflow for NFS client configuration for vSphere.

## Reference

[vSphere datastore and protocol features: NFS](#)

## What's next?

After these tasks are completed, the NFS datastore is ready to consume for provisioning virtual machines.

[vSphere NFS Datastore - Version 4.1 with ONTAP](#)

## About this task

This section describes the creation of an NFS version 4.1 datastore with ONTAP NAS storage.

For automated provisioning, use one of these scripts: [\[PowerShell\]](#), [Ansible Playbook](#), or [\[Terraform\]](#).

## What you need

- The basic skills necessary to manage a vSphere environment and ONTAP
- ONTAP Storage System (FAS/AFF/CVO/ONTAP Select/Cloud Volume Service/Azure NetApp Files) running ONTAP 9.8 or later
- ONTAP credentials (SVM name, userID, password)
- ONTAP network port, SVM, and LUN information for NFS
- [A completed NFS configuration worksheet](#)
- vCenter Server credentials
- vSphere host(s) information vSphere 7.0 or later
- NFS VMKernel adapter IP information
- Network switch(es)
  - with ONTAP system network data ports, vSphere hosts, and connected
  - VLAN(s) configured for NFS
  - (Optional) link aggregation configured for ONTAP network data ports

- ONTAP Tools for VMware vSphere deployed, configured, and ready to consume

## Steps

- Check compatibility with the [Interoperability Matrix Tool \(IMT\)](#).
  - Verify that the NFS configuration is supported.
- Complete the ONTAP and vSphere Tasks provided below.

## ONTAP tasks

### 1. [Verify ONTAP license for NFS](#)

- a. Use the system license show command to check whether NFS is listed.
- b. Use license add -license-code <license code> to add a license.

### 2. [Follow the NFS configuration workflow](#)

## VMware vSphere tasks

[Follow the NFS Client Configuration for vSphere workflow.](#)

## What's next?

After these tasks are completed, the NFS datastore is ready to consume for provisioning virtual machines.

# NetApp Hybrid Multi-Cloud Solutions

## VMware Hybrid Cloud Use Cases

### Use Cases for NetApp Hybrid Multi-Cloud with VMware

An overview of the use cases of importance to IT organization when planning hybrid-cloud or cloud-first deployments.

#### Popular Use Cases

Use cases include:

- Disaster recovery,
- Hosting workloads during data center maintenance, \* quick burst in which additional resources are required beyond what's provisioned in the local data center,
- VMware site expansion,
- Fast migration to the cloud,
- Dev/test, and
- Modernization of apps leveraging cloud native technologies.

Throughout this documentation, cloud workload references will be detailed using the VMware use-cases. These use-cases are:

- Protect (includes both Disaster Recovery and Backup / Restore)
- Migrate
- Extend

### Inside the IT Journey

Most organizations are on a journey to transformation and modernization. As part of this process, companies are trying to use their existing VMware investments while leveraging cloud benefits and exploring ways to make the migration process as seamless as possible. This approach would make their modernization efforts very easy because the data is already in the cloud.

The easiest answer to this scenario is VMware offerings in each hyperscaler. Like NetApp® Cloud Volumes, VMware provides a way to move or extend on-premises VMware environments to any cloud, allowing you to retain existing on-premises assets, skills, and tools while running workloads natively in the cloud. This reduces risk because there will be no service breaks or a need for IP changes and provides the IT team the ability to operate the way they do on-premises using existing skills and tools. This can lead to accelerated cloud migrations and a much smoother transition to a hybrid multi-cloud architecture.

### Understanding the Importance of Native Storage Options

While VMware in any cloud delivers unique hybrid capabilities to every customer, limited native storage options have restricted its usefulness for organizations with storage-heavy workloads. Because storage is directly tied to hosts, the only way to scale storage is to add more hosts—and that can increase costs by 35–40 percent or more for storage intensive workloads. These workloads just need additional storage, not additional horsepower. But that means paying for additional hosts.

Let's consider this scenario:

A customer requires just five hosts for CPU and memory, but has a lot of storage needs, and needs 12 hosts to meet the storage requirement. This requirement ends up really tipping the financial scale by having to buy the additional horsepower, when they only need to increment the storage.

When you're planning cloud adoption and migrations, it's always important to evaluate the best approach and take the easiest path that reduces total investments. The most common and easiest approach for any application migration is rehosting (also known as lift and shift) where there is no virtual machine (VM) or data conversion. Using NetApp Cloud Volumes with VMware software-defined data center (SDDC), while complementing vSAN, provides an easy lift-and-shift option.

## Virtual Desktops

### Virtual Desktop Services (VDS)

#### TR-4861: Hybrid Cloud VDI with Virtual Desktop Service

Suresh Thoppay, NetApp

The NetApp Virtual Desktop Service (VDS) orchestrates Remote Desktop Services (RDS) in major public clouds as well as on private clouds. VDS supports Windows Virtual Desktop (WVD) on Microsoft Azure. VDS automates many tasks that must be performed after deployment of WVD or RDS, including setting up SMB file shares (for user profiles, shared data, and the user home drive), enabling Windows features, application and agent installation, firewall, and policies, and so on.

Users consume VDS for dedicated desktops, shared desktops, and remote applications. VDS provides

scripted events for automating application management for desktops and reduces the number of images to manage.

VDS provides a single management portal for handling deployments across public and private cloud environments.

#### **Customer Value**

The remote workforce explosion of 2020 has changed requirements for business continuity. IT departments are faced with new challenges to rapidly provision virtual desktops and thus require provisioning agility, remote management, and the TCO advantages of a hybrid cloud that makes it easy to provision on-premises and cloud resources. They need a hybrid-cloud solution that:

- Addresses the post-COVID workspace reality to enable flexible work models with global dynamics
- Enables shift work by simplifying and accelerating the deployment of work environments for all employees, from task workers to power users
- Mobilizes your workforce by providing rich, secure VDI resources regardless of the physical location
- Simplifies hybrid-cloud deployment
- Automates and simplifies risk reduction management

[Next: Use Cases](#)

#### **Use Cases**

Hybrid VDI with NetApp VDS allows service providers and enterprise virtual desktop administrators to easily expand resources to other cloud environment without affecting their users. Having on-premises resources provides better control of resources and offers wide selection of choices (compute, GPU, storage, and network) to meet demand.

This solution applies to the following use cases:

- Bursting into the cloud for surges in demand for remote desktops and applications
- Reducing TCO for long running remote desktops and applications by hosting them on-premises with flash storage and GPU resources
- Ease of management of remote desktops and applications across cloud environments
- Experience remote desktops and applications by using a software-as-a-service model with on-premises resources

#### **Target Audience**

The target audience for the solution includes the following groups:

- EUC/VDI architects who wants to understand the requirements for a hybrid VDS
- NetApp partners who would like to assist customers with their remote desktop and application needs
- Existing NetApp HCI customers who want to address remote desktop and application demands

[Next: NetApp Virtual Desktop Service Overview](#)

#### **NetApp Virtual Desktop Service Overview**

NetApp offers many cloud services, including the rapid provisioning of virtual desktop with WVD or remote

applications and rapid integration with Azure NetApp Files.

Traditionally, it takes weeks to provision and deliver remote desktop services to customers. Apart from provisioning, it can be difficult to manage applications, user profiles, shared data, and group policy objects to enforce policies. Firewall rules can increase complexity and require a separate skillset and tools.

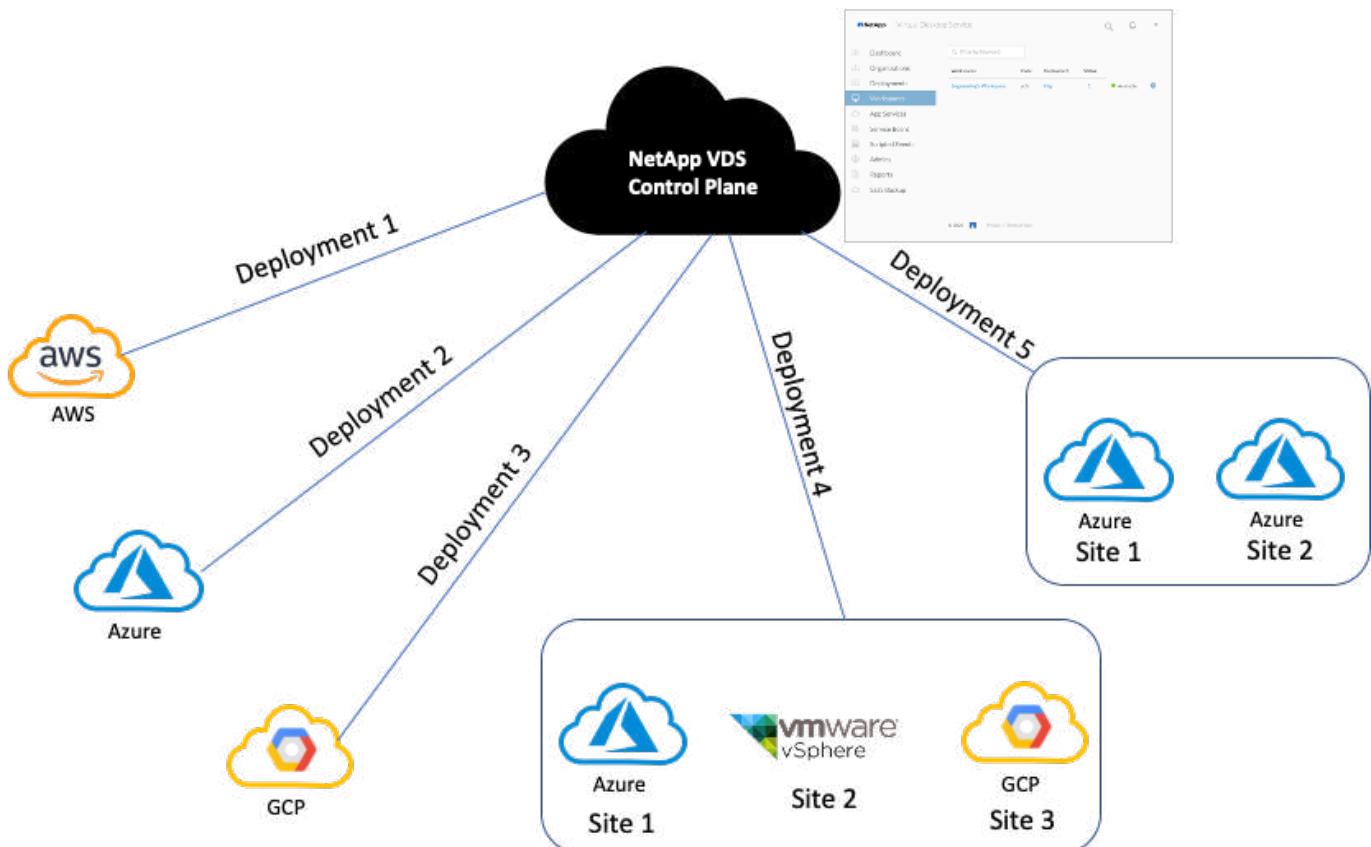
With Microsoft Azure Windows Virtual Desktop service, Microsoft takes care of maintenance for Remote Desktop Services components, allowing customers to focus on provisioning workspaces in the cloud. Customers must provision and manage the complete stack which requires special skills to manage VDI environments.

With NetApp VDS, customers can rapidly deploy virtual desktops without worrying about where to install the architecture components like brokers, gateways, agents, and so on. Customers who require complete control of their environment can work with a professional services team to achieve their goals. Customers consume VDS as a service and thus can focus on their key business challenges.

NetApp VDS is a software-as-a-service offering for centrally managing multiple deployments across AWS, Azure, GCP, or private cloud environments. Microsoft Windows Virtual Desktop is available only on Microsoft Azure. NetApp VDS orchestrates Microsoft Remote Desktop Services in other environments.

Microsoft offers multisession on Windows 10 exclusively for Windows Virtual Desktop environments on Azure. Authentication and identity are handled by the virtual desktop technology; WVD requires Azure Active Directory synced (with AD Connect) to Active Directory and session VMs joined to Active Directory. RDS requires Active Directory for user identity and authentication and VM domain join and management.

A sample deployment topology is shown in the following figure.

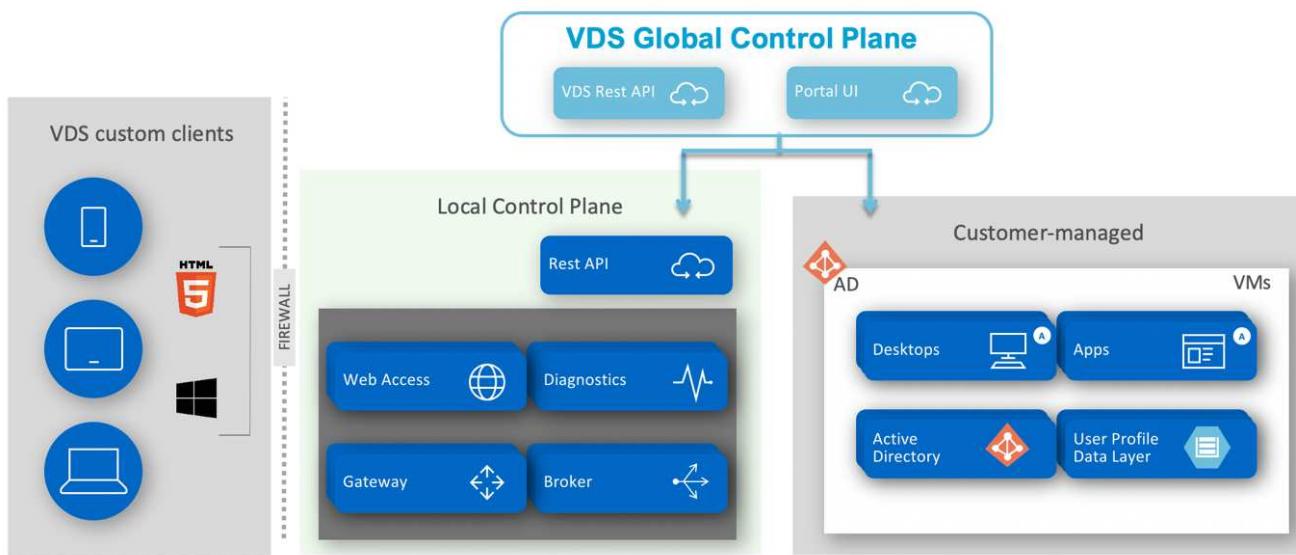


Each deployment is associated with an active directory domain and provides clients with an access entry point

for workspaces and applications. A service provider or enterprise that has multiple active directory domains typically has more deployments. A single Active Directory domain that spans multiple regions typically has a single deployment with multiple sites.

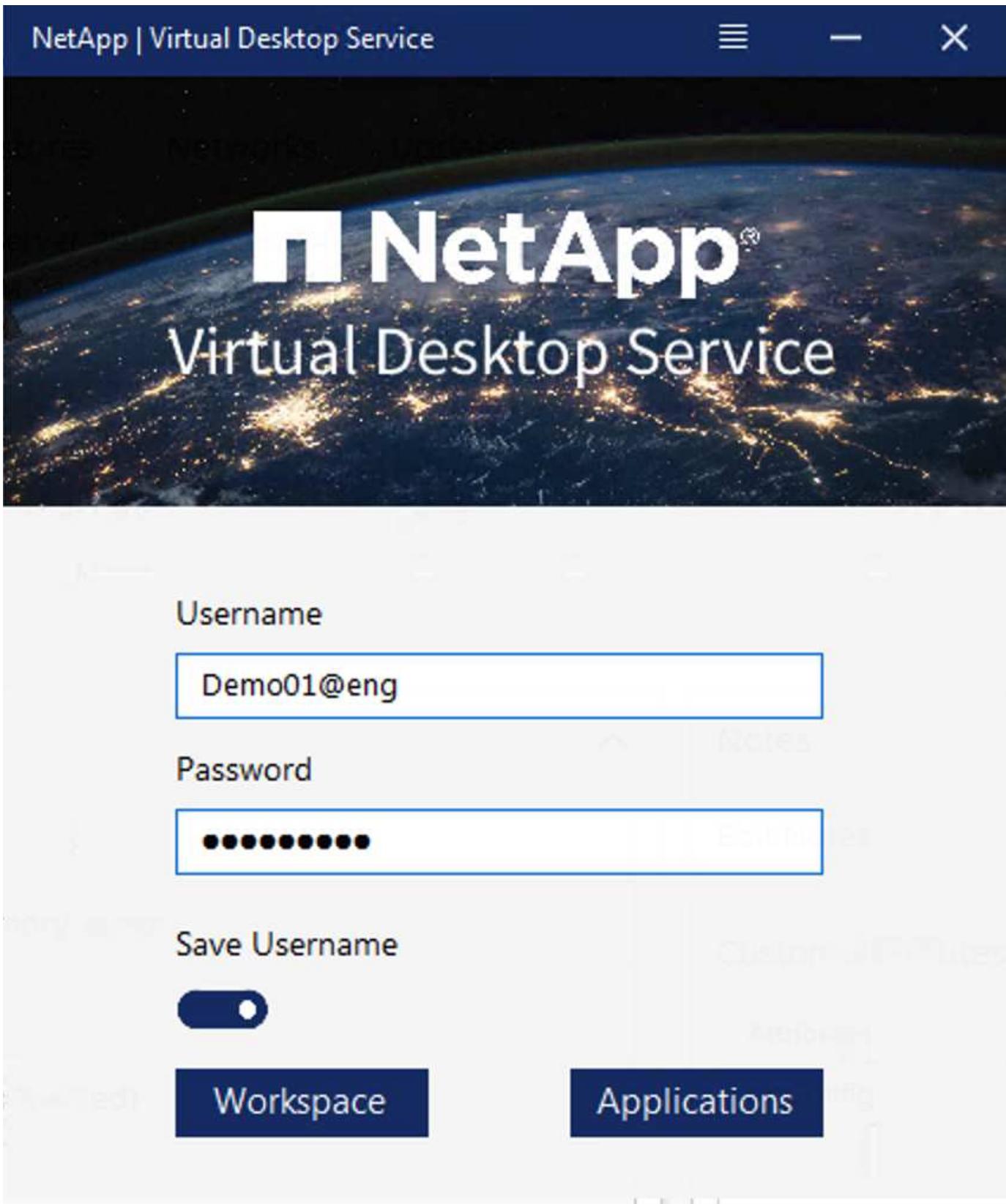
For WVD in Azure, Microsoft provides a platform-as-a-service that is consumed by NetApp VDS. For other environments, NetApp VDS orchestrates the deployment and configuration of Microsoft Remote Desktop Services. NetApp VDS supports both WVD Classic and WVD ARM and can also be used to upgrade existing versions.

Each deployment has its own platform services, which consists of Cloud Workspace Manager (REST API endpoint), an HTML 5 Gateway (connect to VMs from a VDS management portal), RDS Gateways (Access point for clients), and a Domain Controller. The following figure depicts the VDS Control Plane architecture for RDS implementation.



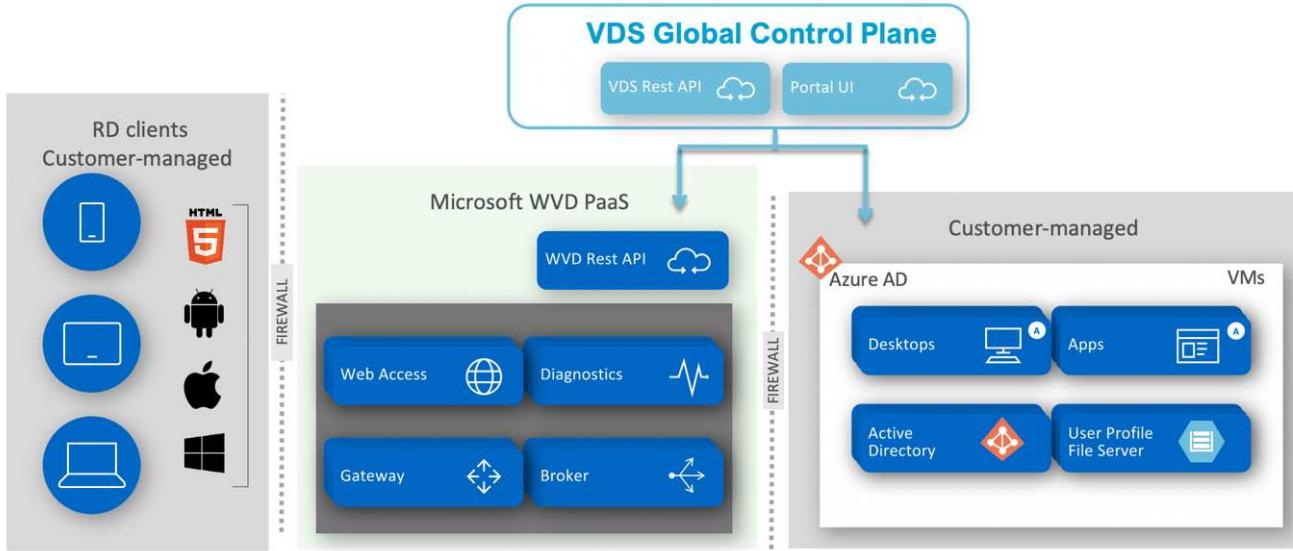
For RDS implementations, NetApp VDS can be readily accessed from Windows and browsers using client software that can be customized to include customer logo and images. Based on user credentials, it provides user access to approved workspaces and applications. There is no need to configure the gateway details.

The following figure shows the NetApp VDS client.



In the Azure WVD implementation, Microsoft handles the access entry point for the clients and can be consumed by a Microsoft WVD client available natively for various OSs. It can also be accessed from a web-based portal. The configuration of client software must be handled by the Group Policy Object (GPO) or in other ways preferred by customers.

The following figure depicts the VDS Control Plane architecture for Azure WVD implementations.



In addition to the deployment and configuration of required components, NetApp VDS also handles user management, application management, resource scaling, and optimization.

NetApp VDS can create users or grant existing user accounts access to cloud workspace or application services. The portal can also be used for password resets and the delegation of administrating a subset of components. Helpdesk administrators or Level-3 technicians can shadow user sessions for troubleshooting or connect to servers from within the portal.

NetApp VDS can use image templates that you create, or it can use existing ones from the marketplace for cloud-based provisioning. To reduce the number of images to manage, you can use a base image, and any additional applications that you require can be provisioned using the provided framework to include any command-line tools like Chocolatey, MSIX app attach, PowerShell, and so on. Even custom scripts can be used as part of machine lifecycle events.

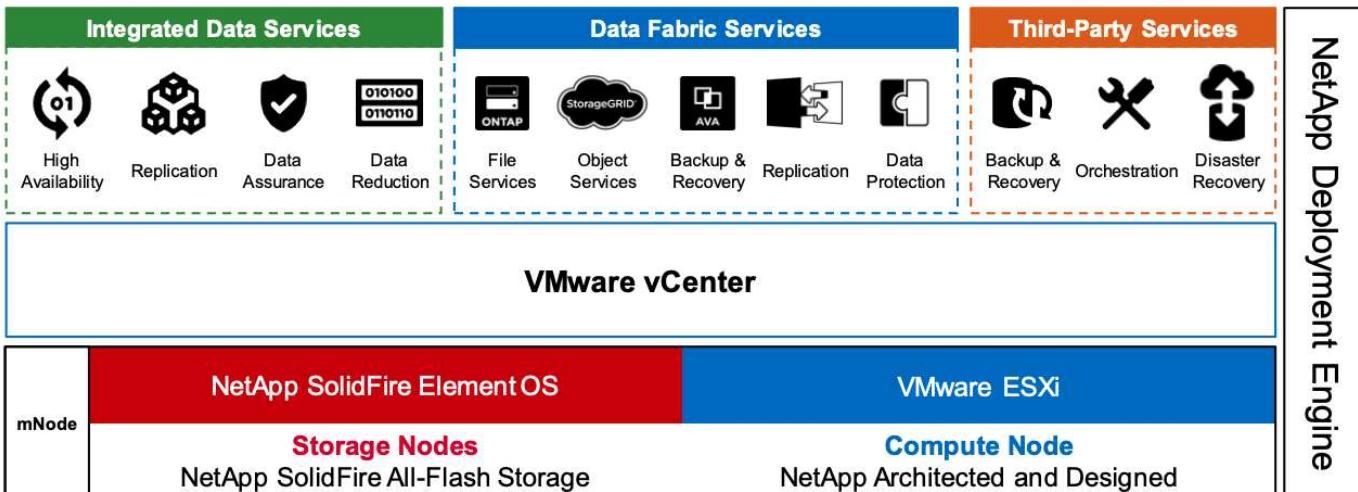
[Next: NetApp HCI Overview](#)

### NetApp HCI Overview

NetApp HCI is a hybrid cloud infrastructure that consists of a mix of storage nodes and compute nodes. It is available as either a two-rack unit or single-rack unit, depending on the model. The installation and configuration required to deploy VMs are automated with the NetApp Deployment Engine (NDE). Compute clusters are managed with VMware vCenter, and storage clusters are managed with the vCenter Plug-in deployed with NDE. A management VM called the mNode is deployed as part of the NDE.

NetApp HCI handles the following functions:

- Version upgrades
- Pushing events to vCenter
- vCenter Plug-In management
- A VPN tunnel for support
- The NetApp Active IQ collector
- The extension of NetApp Cloud Services to on the premises, enabling a hybrid cloud infrastructure. The following figure depicts HCI components.



## Storage Nodes

Storage nodes are available as either a half-width or full-width rack unit. A minimum of four storage nodes is required at first, and a cluster can expand to up to 40 nodes. A storage cluster can be shared across multiple compute clusters. All the storage nodes contain a cache controller to improve write performance. A single node provides either 50K or 100K IOPS at a 4K block size.

NetApp HCI storage nodes run NetApp Element software, which provides minimum, maximum, and burst QoS limits. The storage cluster supports a mix of storage nodes, although one storage node cannot exceed one-third of total capacity.

## Compute Nodes



NetApp supports its storage connected to any compute servers listed in the [VMware Compatability Guide](#).

Compute nodes are available in half-width, full-width, and two rack-unit sizes. The NetApp HCI H410C and H610C are based on scalable Intel Skylake processors. The H615C is based on second-generation scalable Intel Cascade Lake processors. There are two compute models that contain GPUs: the H610C contains two NVIDIA M10 cards and the H615C contains three NVIDIA T4 cards.



The NVIDIA T4 has 40 RT cores that provide the computation power needed to deliver real-time ray tracing. The same server model used by designers and engineers can now also be used by artists to create photorealistic imagery that features light bouncing off surfaces just as it would in real life. This RTX-capable GPU produces real-time ray tracing performance of up to five Giga Rays per second. The NVIDIA T4, when combined with Quadro Virtual Data Center Workstation (Quadro vDWS) software, enables artists to create photorealistic designs with accurate shadows, reflections, and refractions on any device from any location.

Tensor cores enable you to run deep learning inferencing workloads. When running these workloads, an NVIDIA T4 powered with Quadro vDWS can perform up to 25 times faster than a VM driven by a CPU-only server. A NetApp H615C with three NVIDIA T4 cards in one rack unit is an ideal solution for graphics and compute-intensive workloads.

The following figure lists NVIDIA GPU cards and compares their features.

## NVIDIA GPUs Recommended for Virtualization

	V100S	RTX 8000	RTX 6000	T4	M10	P6
						
<b>GPU</b>	1 NVIDIA Volta	1 NVIDIA Turing	1 NVIDIA Turing	1 NVIDIA Turing	4 NVIDIA Maxwell	1 NVIDIA Pascal
<b>CUDA Cores</b>	5,120	4,608	4,608	2,560	2,560 (640 per GPU)	2,048
<b>Tensor Cores</b>	640	576	576	320	—	—
<b>RT Cores</b>	—	72	72	40	—	—
<b>Guaranteed QoS [GPU Scheduler]</b>	✓	✓	✓	✓	—	✓
<b>Live Migration</b>	✓	✓	✓	✓	✓	✓
<b>Multi-vGPU</b>	✓	✓	✓	✓	✓	✓
<b>Memory Size</b>	32/16 GB HBM2	48 GB GDDR6	24 GB GDDR6	16 GB GDDR6	32 GB GDDR5 (8 GB per GPU)	16 GB GDDR5
<b>vGPU Profiles</b>	1 GB, 2 GB, 4 GB, 8 GB, 16 GB, 32 GB	1 GB, 2 GB, 3 GB, 4 GB, 6 GB, 8 GB, 12 GB, 16 GB, 24 GB, 48 GB	1 GB, 2 GB, 3 GB, 4 GB, 6 GB, 8 GB, 12 GB, 24 GB	1 GB, 2 GB, 4 GB, 8 GB, 16 GB	0.5 GB, 1 GB, 2 GB, 4 GB, 8 GB	1 GB, 2 GB, 4 GB, 8 GB, 16 GB
<b>Form Factor</b>	PCIe 3.0 dual slot and SXM2	PCIe 3.0 dual slot	PCIe 3.0 dual slot	PCIe 3.0 single slot	PCIe 3.0 dual slot	MXM (blade servers)
<b>Power</b>	250 W/300 W (SXM2)	250 W	250 W	70 W	225 W	90 W
<b>Thermal</b>	passive	passive	passive	passive	passive	bare board
<b>vGPU Software Support</b>	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer
<b>Use Case</b>	Ultra-high-end rendering, simulation, 3D design with Quadro vDWS; ideal upgrade path for V100	High-end rendering, 3D design and creative workflows with Quadro vDWS	Mid-range to high-end rendering, 3D design and creative workflows with Quadro vDWS	Entry-level to high-end 3D design and engineering workflows with Quadro vDWS. High-density, low power GPU acceleration for knowledge workers with NVIDIA GRID software.	Knowledge workers using modern productivity apps and Windows 10 requiring best density and total cost of ownership (TCO), multi-monitor support with NVIDIA GRID vPC/vApps	For customers requiring GPUs in a blade server form factor; ideal upgrade path for M6

The M10 GPU remains the best TCO solution for knowledge-worker use cases. However, the T4 makes a great alternative when IT wants to standardize on a GPU that can be used across multiple use cases, such as virtual workstations, graphics performance, real-time interactive rendering, and inferencing. With the T4, IT can take advantage of the same GPU resources to run mixed workloads—for example, running VDI during the day and repurposing the resources to run compute workloads at night.

The H610C compute node is two rack units in size; the H615C is one rack unit in size and consumes less power. The H615C supports H.264 and H.265 (High Efficiency Video Coding [HEVC]) 4:4:4 encoding and decoding. It also supports the increasingly mainstream VP9 decoder; even the WebM container package served by YouTube uses the VP9 codec for video.

The number of nodes in a compute cluster is dictated by VMware; currently, it is 96 with VMware vSphere 7.0 Update 1. Mixing different models of compute nodes in a cluster is supported when Enhanced vMotion Compatibility (EVC) is enabled.

## Next: NVIDIA Licensing

### NVIDIA Licensing

When using an H610C or H615C, the license for the GPU must be procured from NVIDIA partners that are authorized to resell the licenses. You can find NVIDIA partners with the [partner locator](#). Search for competencies such as virtual GPU (vGPU) or Tesla.

NVIDIA vGPU software is available in four editions:

- NVIDIA GRID Virtual PC (GRID vPC)
- NVIDIA GRID Virtual Applications (GRID vApps)
- NVIDIA Quadro Virtual Data Center Workstation (Quadro vDWS)
- NVIDIA Virtual ComputeServer (vComputeServer)

## **GRID Virtual PC**

This product is ideal for users who want a virtual desktop that provides a great user experience for Microsoft Windows applications, browsers, high-definition video, and multi-monitor support. The NVIDIA GRID Virtual PC delivers a native experience in a virtual environment, allowing you to run all your PC applications at full performance.

## **GRID Virtual Applications**

GRID vApps are for organizations deploying a Remote Desktop Session Host (RDSH) or other app-streaming or session-based solutions. Designed to deliver Microsoft Windows applications at full performance, Windows Server-hosted RDSH desktops are also supported by GRID vApps.

## **Quadro Virtual Data Center Workstation**

This edition is ideal for mainstream and high-end designers who use powerful 3D content creation applications like Dassault CATIA, SOLIDWORKS, 3Dexcite, Siemens NX, PTC Creo, Schlumberger Petrel, or Autodesk Maya. NVIDIA Quadro vDWS allows users to access their professional graphics applications with full features and performance anywhere on any device.

## **NVIDIA Virtual ComputeServer**

Many organizations run compute-intensive server workloads such as artificial intelligence (AI), deep learning (DL), and data science. For these use cases, NVIDIA vComputeServer software virtualizes the NVIDIA GPU, which accelerates compute-intensive server workloads with features such as error correction code, page retirement, peer-to-peer over NVLink, and multi-vGPU.



A Quadro vDWS license enables you to use GRID vPC and NVIDIA vComputeServer.

## [Next: Deployment](#)

### **Deployment**

NetApp VDS can be deployed to Microsoft Azure using a setup app available based on the required codebase. The current release is available [here](#) and the preview release of the upcoming product is available [here](#).

See [this video](#) for deployment instructions.



# NetApp Virtual Desktop Service

## Deployment & AD Connect

Toby vanRoojen  
Product Marketing Manager  
June, 2020

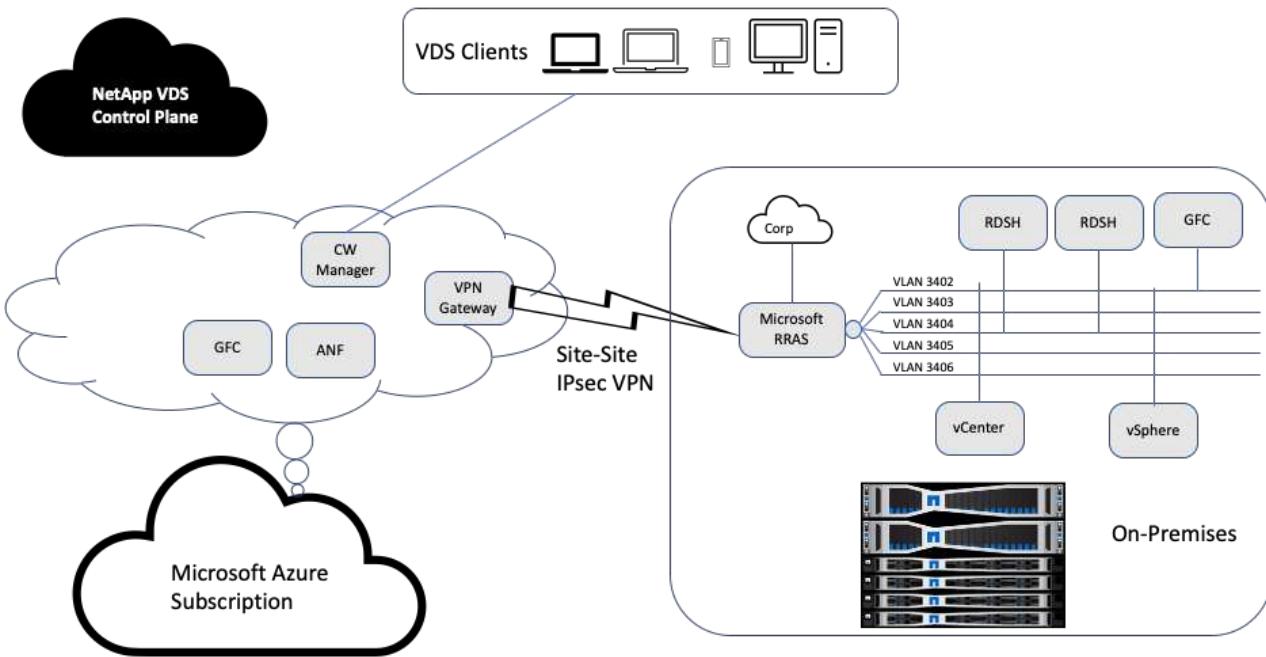


[Next: Hybrid Cloud Environment](#)

### Hybrid Cloud Environment

NetApp Virtual Desktop Service can be extended to on-premises when connectivity exists between on-premises resources and cloud resources. Enterprises can establish the link to Microsoft Azure using Express Route or a site-to-site IPsec VPN connection. You can also create links to other clouds in a similar way either using a dedicated link or with an IPsec VPN tunnel.

For the solution validation, we used the environment depicted in the following figure.



On-premises, we had multiple VLANs for management, remote-desktop-session hosts, and so on. They were on the 172.21.146-150.0/24 subnet and routed to the corporate network using the Microsoft Remote Routing Access Service. We also performed the following tasks:

1. We noted the public IP of the Microsoft Routing and Remote Access Server (RRAS; identified with IPchicken.com).
2. We created a Virtual Network Gateway resource (route-based VPN) on Azure Subscription.
3. We created the connection providing the local network gateway address for the public IP of the Microsoft RRAS server.
4. We completed VPN configuration on RRAS to create a virtual interface using pre-shared authentication that was provided while creating the VPN gateway. If configured correctly, the VPN should be in the connected state. Instead of Microsoft RRAS, you can also use pfSense or other relevant tools to create the site-to-site IPsec VPN tunnel. Since it is route-based, the tunnel redirects traffic based on the specific subnets configured.

Microsoft Azure Active Directory provides identity authentication based on OAuth. Enterprise client authentications typically require NTLM or Kerberos-based authentication. Microsoft Azure Active Directory Domain Services perform password hash sync between Azure Active Directory and on-prem domain controllers using ADConnect.

For this Hybrid VDS solution validation, we initially deployed to Microsoft Azure and added an additional site with vSphere. The advantage with this approach is that platform services were deployed to Microsoft Azure and were then readily backed up using the portal. Services can then be easily accessed from anywhere, even if the site-site VPN link is down.

To add another site, we used a tool called DCConfig. The shortcut to that application is available on the desktop of the cloud workspace manager (CWMgr) VM. After this application is launched, navigate to the DataCenter Sites tab, add the new datacenter site, and fill in the required info as shown below. The URL points to the vCenter IP. Make sure that the CWMgr VM can communicate with vCenter before adding the

configuration.



Make sure that vSphere PowerCLI 5.1 on CloudWorkspace manager is installed to enable communication with VMware vSphere environment.

The following figure depicts on-premises datacenter site configuration.

The screenshot shows the 'DataCenter' tab selected in the navigation bar. A table lists two sites: 'Site 1' (AzureRM) and 'Site 2' (vSphere). The 'Site 2' row has an 'Edit' button highlighted. The main panel displays the 'DataCenter Site' configuration for 'Site 2'. It includes fields for 'DataCenter Site' (Site 2), 'Hypervisor' (vSphere), and buttons for 'Cancel Edit', 'Save', 'Load Hypervisor', and 'Test'. Under 'General Settings', there are sections for 'Local VM Account' (Username: Administrator, Password: \*\*\*\*\*) and 'Hypervisor Account' (Username: Administrator@vsphere, Password: \*\*\*\*\*). The 'URL' is set to <https://172.21.146.150/sdk/>. Configuration options include 'Vm Name Prefix' (empty), 'Max Concurrent Create Server' (20), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (172.21.148.250), 'Is Primary Hypervisor?' (radio button for Yes selected), and 'Must Set IpAddress Of VM?' (radio button for No selected). The 'DNS' section shows 'Primary DNS' (10.67.78.11) and 'Secondary DNS' (empty). A radio button for 'Set DNS Address' is set to 'Yes'. The 'VSphere' section contains dropdowns for 'Data Center' (NetApp-HCI-Datacenter), 'Cluster' (empty), 'Resource Pool' (empty), 'Host Name' (empty), and 'VM Folder' (VDS). It also includes fields for 'Max VMs In Datastore' (-1), 'Min HD Free Space In Datastore GB' (-1), and 'Min Ram Free GB' (-1). At the bottom are buttons for 'Exclude VSphere DataStore' and 'Exclude VSphere ResourcePools'.

Note that there are filtering options available for compute resource based on the specific cluster, host name, or free RAM space. Filtering options for storage resource includes the minimum free space on datastores or the maximum VMs per datastore. Datastores can be excluded using regular expressions. Click Save button to save the configuration.

To validate the configuration, click the Test button or click Load Hypervisor and check any dropdown under the vSphere section. It should be populated with appropriate values. It is a best practice to keep the primary hypervisor set to yes for the default provisioning site.

The VM templates created on VMware vSphere are consumed as provisioning collections on VDS. Provisioning collections come in two forms: shared and VDI. The shared provisioning collection type is used for remote desktop services for which a single resource policy is applied to all servers. The VDI type is used for WVD instances for which the resource policy is individually assigned. The servers in a provisioning collection can be assigned one of the following three roles:

- **TSDATA.** Combination of Terminal Services and Data server role.
- **TS.** Terminal Services (Session Host).
- **DATA.** File Server or Database Server. When you define the server role, you must pick the VM template and storage (datastore). The datastore chosen can be restricted to a specific datastore or you can use the least-used option in which the datastore is chosen based on data usage.

Each deployment has VM resource defaults for the cloud resource allocation based on Active Users, Fixed, Server Load, or User Count.

## [Next: Single Server Load Test with Login VSI](#)

### Single server load test with Login VSI

The NetApp Virtual Desktop Service uses the Microsoft Remote Desktop Protocol to access virtual desktop sessions and applications, and the Login VSI tool determines the maximum number of users that can be hosted on a specific server model. Login VSI simulates user login at specific intervals and performs user operations like opening documents, reading and composing mails, working with Excel and PowerPoint, printing documents, compressing files, and taking random breaks. It then measures response times. User response time is low when server utilization is low and increases when more user sessions are added. Login VSI determines the baseline based on initial user login sessions and it reports the maximum user session when the user response exceeds 2 seconds from the baseline.

NetApp Virtual Desktop Service utilizes Microsoft Remote Desktop Protocol to access the Virtual Desktop session and Applications. To determine the maximum number of users that can be hosted on a specific server model, we used the Login VSI tool. Login VSI simulates user login at specific intervals and performs user operations like opening documents, reading and composing mails, working with Excel and PowerPoint, printing documents, compressing files, taking random breaks, and so on. It also measures response times. User response time is low when server utilization is low and increases when more user sessions are added. Login VSI determines the baseline based on the initial user login sessions and it reports maximum user sessions when the user response exceeds 2sec from the baseline.

The following table contains the hardware used for this validation.

Model	Count	Description
NetApp HCI H610C	4	Three in a cluster for launchers, AD, DHCP, and so on. One server for load testing.
NetApp HCI H615C	1	2x24C Intel Xeon Gold 6282 @2.1GHz. 1.5TB RAM.

The following table contains the software used for this validation.

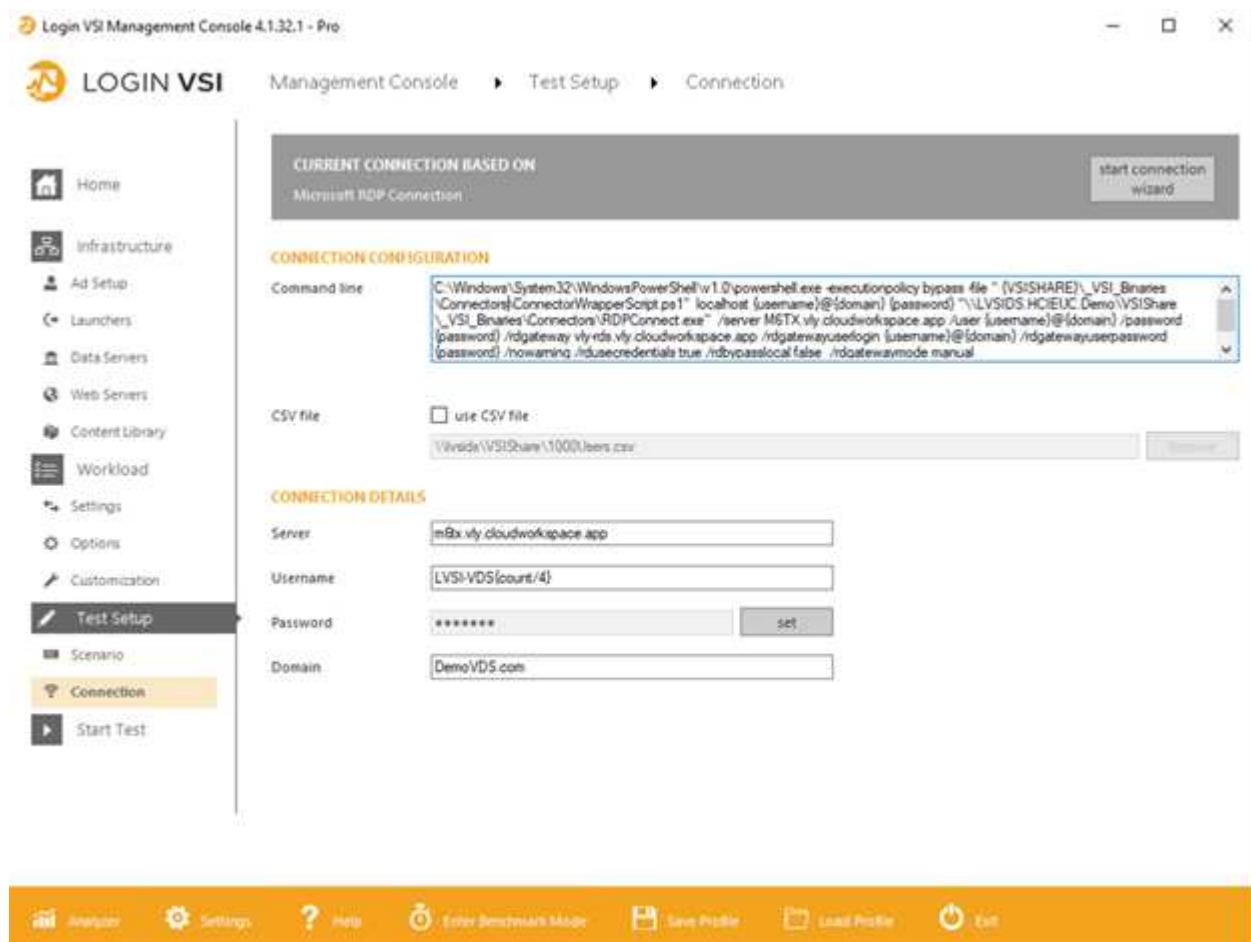
product	Description
NetApp VDS 5.4	Orchestration
VM Template Windows 2019 1809	Server OS for RDSH
Login VSI	4.1.32.1
VMware vSphere 6.7 Update 3	Hypervisor
VMware vCenter 6.7 Update 3f	VMware management tool

The Login VSI test results are as follows:

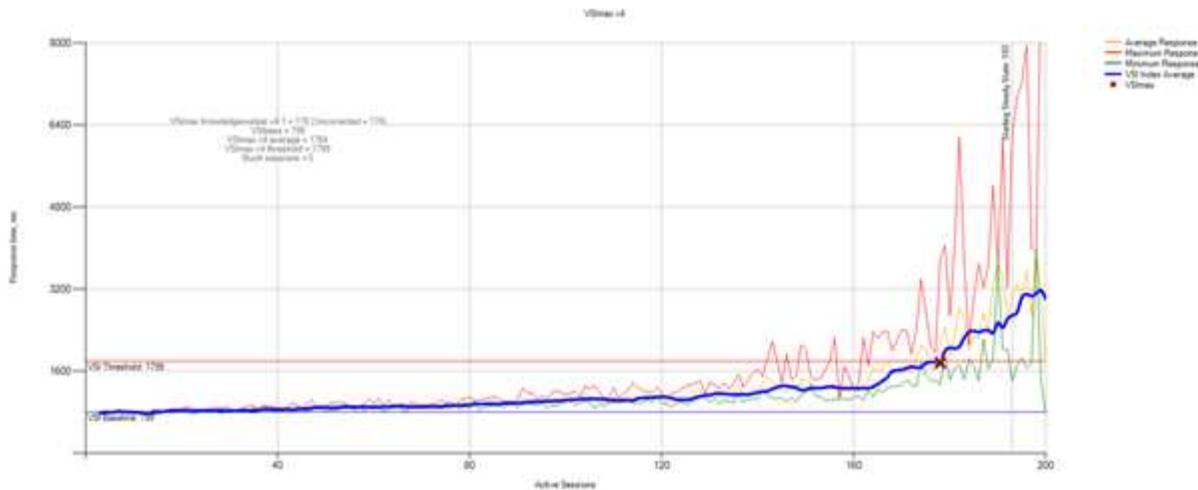
Model	VM configuration	Login VSI baseline	Login VSI Max
H610C	8 vCPU, 48GB RAM, 75GB disk, 8Q vGPU profile	799	178
H615C	12 vCPU, 128GB RAM, 75GB disk	763	272

Considering sub-NUMA boundaries and hyperthreading, the eight VMs chosen for VM testing and configuration depended on the cores available on the host.

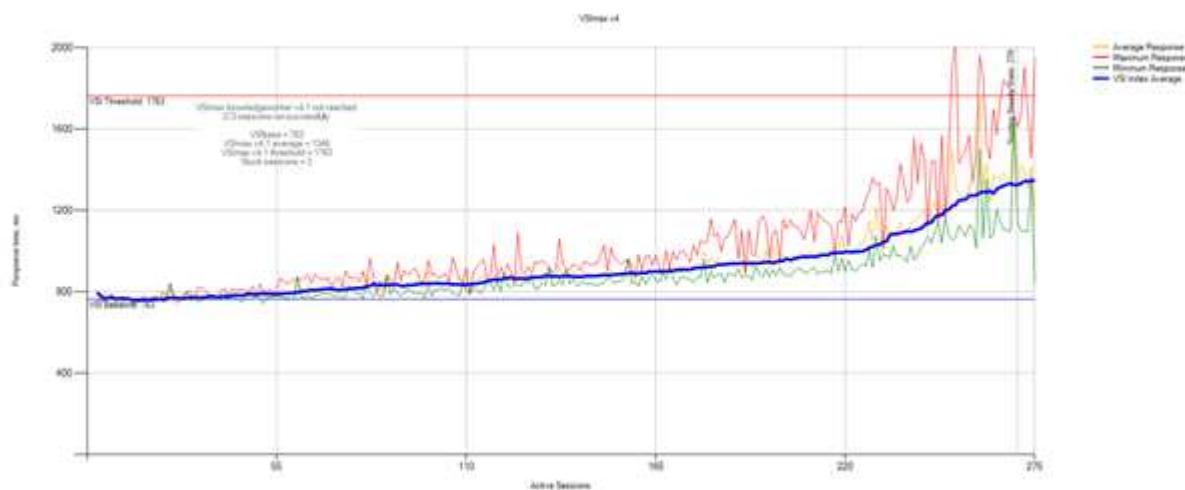
We used 10 launcher VMs on the H610C, which used the RDP protocol to connect to the user session. The following figure depicts the Login VSI connection information.



The following figure displays the Login VSI response time versus the active sessions for the H610C.



The following figure displays the Login VSI response time versus active sessions for the H615C.



The performance metrics from Cloud Insights during H615C Login VSI testing for the vSphere host and VMs are shown in the following figure.



## Next: Management Portal

### Management Portal

NetApp VDS Cloud Workspace Management Suite portal is available [here](#) and the upcoming version is available [here](#).

The portal allows centralized management for various VDS deployments including one that has sites defined for on-premises, administrative users, the application catalog, and scripted events. The portal is also used by administrative users for the manual provisioning of applications if required and to connect to any machines for troubleshooting.

Service providers can use this portal to add their own channel partners and allow them to manage their own clients.

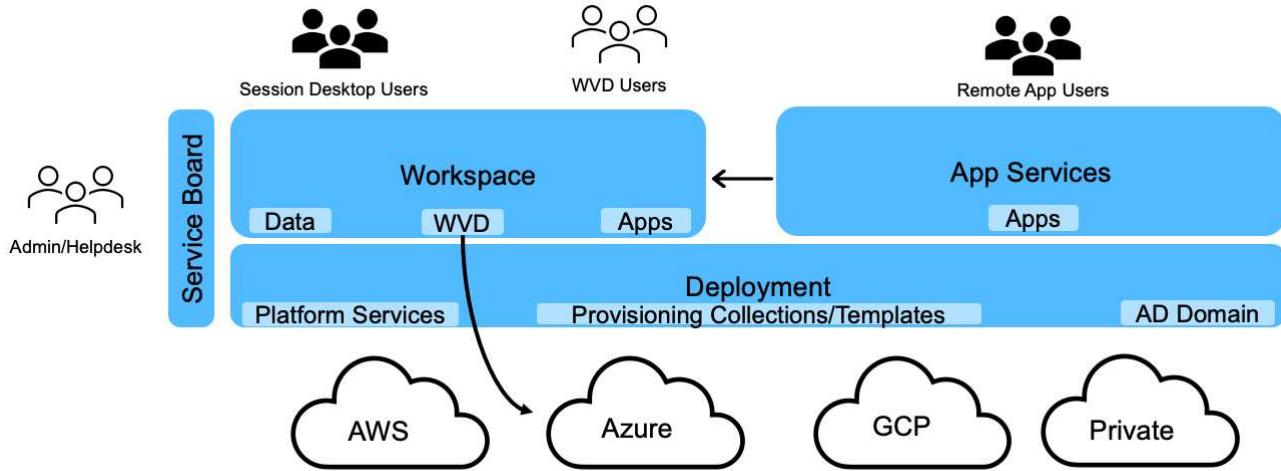
## Next: User Management

### User Management

NetApp VDS uses Azure Active Directory for identity authentication and Azure Active Directory Domain Services for NTLM/Kerberos authentication. The ADConnect tool can be used to sync an on-prem Active Directory domain with Azure Active Directory.

New users can be added from the portal, or you can enable cloud workspace for existing users. Permissions for workspaces and application services can be controlled by individual users or by groups. From the management portal, administrative users can be defined to control permissions for the portal, workspaces, and so on.

The following figure depicts user management in NetApp VDS.



Each workspace resides in its own Active Directory organization unit (OU) under the Cloud Workspace OU as shown in the following figure.

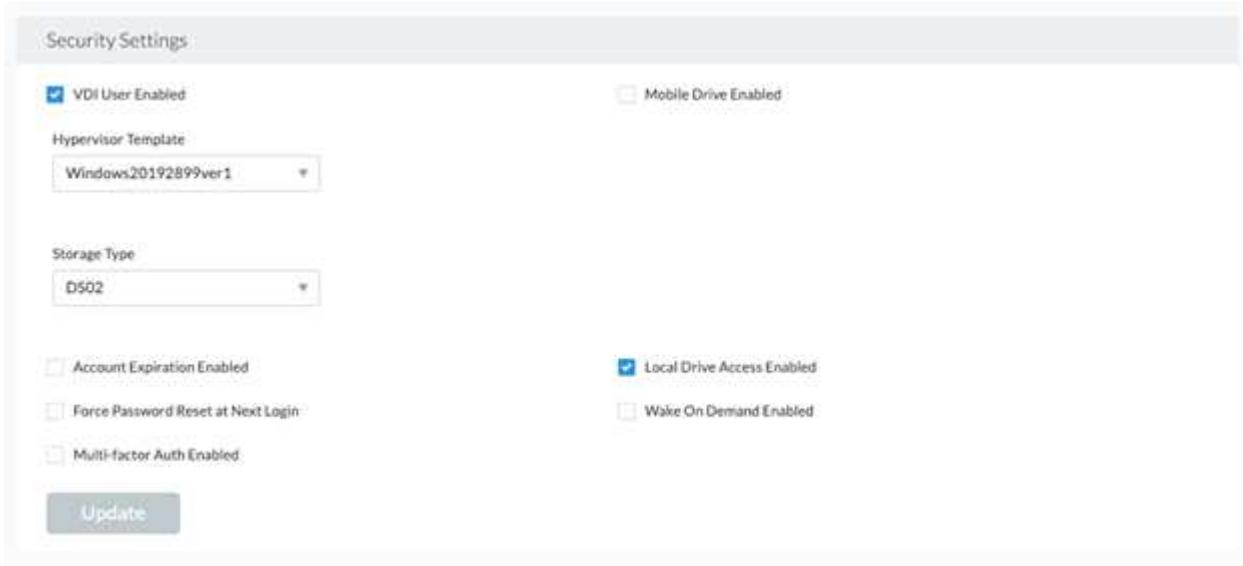
The screenshot shows the Active Directory Users and Computers interface. The left pane displays the navigation tree, which includes the root Active Directory Users and Computers [cwmgr1.vds], a Saved Queries folder, and several organizational units (OUs) under vds.demo. The most prominent OUs are vds.demo\Cloud Workspace\Cloud Workspace Companies\hpyh and vds.demo\Cloud Workspace\Cloud Workspace Companies\ych. The right pane lists the objects within these OUs, showing columns for Name, Type, and Description. The objects listed are:

Name	Type	Description
87499	Security Group...	Microsoft Access
87500	Security Group...	Microsoft Excel
87501	Security Group...	Google Chrome
87502	Security Group...	Microsoft PowerPoint
87503	Security Group...	Microsoft Word
87517	Security Group...	PuTTY
ych-all users	Security Group...	Company All Users

For more info, see [this video](#) on user permissions and user management in NetApp VDS.

When an Active Directory group is defined as a CRAUserGroup using an API call for the datacenter, all the users in that group are imported into the CloudWorkspace for management using the UI. As the cloud workspace is enabled for the user, VDS creates user home folders, settings permissions, user properties updates, and so on.

If VDI User Enabled is checked, VDS creates a single-session RDS machine dedicated to that user. It prompts for the template and the datastore to provision.



[Next: Workspace Management](#)

### Workspace Management

A workspace consists of a desktop environment; this can be shared remote desktop sessions hosted on-premises or on any supported cloud environment. With Microsoft Azure, the desktop environment can be persistent with Windows Virtual Desktops. Each workspace is associated with a specific organization or client. Options available when creating a new workspace can be seen in the following figure.

## New Workspace

Client & Settings      Choose Applications      Add Users      Review & Provision

---

Select a Client [Add](#)

No Clients Added.

**Workspace Settings**

Company Name

**Application Settings**

- Enable Remote App
- Enable App Locker
- Enable Application Usage Tracking

**Primary Notification Email**

**Device Settings**

- Disable Printing Access
- Enable Workspace User Data Storage

**Security Settings**

- Require Complex User Password
- Enable MFA for All Users
- Permit Access To Task Manager

[Cancel](#) [Continue](#)



Each workspace is associated with specific deployment.

Workspaces contain associated apps and app services, shared data folders, servers, and a WVD instance. Each workspace can control security options like enforcing password complexity, multifactor authentication, file audits, and so on.

Workspaces can control the workload schedule to power on extra servers, limit the number of users per server, or set the schedule for the resources available for given period (always on/off). Resources can also be configured to wake up on demand.

The workspace can override the deployment VM resource defaults if required. For WVD, WVD host pools (which contains session hosts and app groups) and WVD workspaces can also be managed from the cloud workspace management suite portal. For more info on the WVD host pool, see this [video](#).

[Next: Application Management](#)

### Application Management

Task workers can quickly launch an application from the list of applications made available to them. App services publish applications from the Remote Desktop Services session hosts. With WVD, App Groups provide similar functionality from multi-session Windows 10 host pools.

For office workers to power users, the applications that they require can be provisioned manually using a service board, or they can be auto-provisioned using the scripted events feature in NetApp VDS.

For more information, see the [NetApp Application Entitlement page](#).

Next: [ONTAP features for Virtual Desktop Service](#)

## ONTAP features for Virtual Desktop Service

The following ONTAP features make it attractive choice for use with a virtual desktop service.

- **Scale-out filesystem.** ONTAP FlexGroup volumes can grow to more than 20PB in size and can contain more than 400 billion files within a single namespace. The cluster can contain up to 24 storage nodes, each with a flexible the number of network interface cards depending on the model used.

User's virtual desktops, home folders, user profile containers, shared data, and so on can grow based on demand with no concern for filesystem limitations.

- **File system analytics.** You can use the XCP tool to gain insights into shared data. With ONTAP 9.8+ and ActiveIQ Unified Manager, you can easily query and retrieve file metadata information and identify cold data.
- **Cloud tiering.** You can migrate cold data to an object store in the cloud or to any S3-compatible storage in your datacenter.
- **File versions.** Users can recover files protected by NetApp ONTAP Snapshot copies. ONTAP Snapshot copies are very space efficient because they only record changed blocks.
- **Global namespace.** ONTAP FlexCache technology allows remote caching of file storage making it easier to manage shared data across locations containing ONTAP storage systems.
- **Secure multi-tenancy support.** A single physical storage cluster can be presented as multiple virtual storage arrays each with its own volumes, storage protocols, logical network interfaces, identity and authentication domain, management users, and so on. Therefore, you can share the storage array across multiple business units or environments, such as test, development, and production.

To guarantee performance, you can use adaptive QoS to set performance levels based on used or allocated space, and you can control storage capacity by using quotas.

- **VMware integration.** ONTAP tools for VMware vSphere provides a vCenter plug-in to provision datastores, implement vSphere host best practices, and monitor ONTAP resources.

ONTAP supports vStorage APIs for Array Integration (VAAI) for offloading SCSI/file operations to the storage array. ONTAP also supports vStorage APIs for Storage Awareness (VASA) and Virtual Volumes support for both block and file protocols.

The Snapcenter Plug-in for VMware vSphere provides an easy way to back up and restore virtual machines using the Snapshot feature on a storage array.

ActiveIQ Unified Manager provides end-to-end storage network visibility in a vSphere environment. Administrators can easily identify any latency issues that might occur on virtual desktop environments hosted on ONTAP.

- **Security compliance.** With ActiveIQ Unified Manager, you can monitor multiple ONTAP systems with alerts for any policy violations.
- **Multi-protocol support.** ONTAP supports block (iSCSI, FC, FCoE, and NVMe/FC), file (NFSv3, NFSv4.1, SMB2.x, and SMB3.x), and object (S3) storage protocols.
- **Automation support.** ONTAP provides REST API, Ansible, and PowerShell modules to automate tasks with the VDS Management Portal.

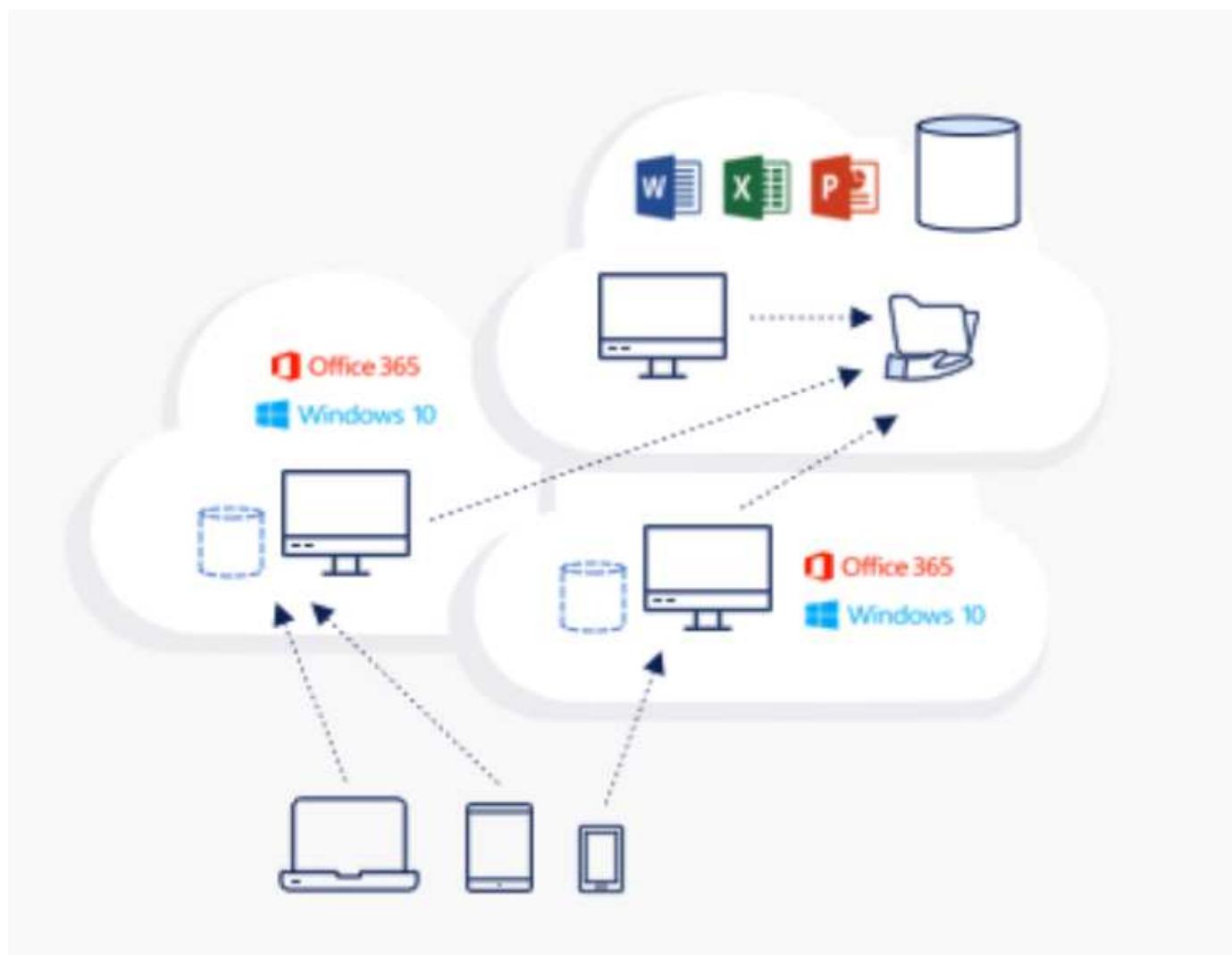
Next: Data Management

## Data Management

As a part of deployment, you can choose the file-services method to host the user profile, shared data, and the home drive folder. The available options are File Server, Azure Files, or Azure NetApp Files. However, after deployment, you can modify this choice with the Command Center tool to point to any SMB share. There are various advantages to hosting with NetApp ONTAP. To learn how to change the SMB share, see [Change Data Layer](#).

## Global File Cache

When users are spread across multiple sites within a global namespace, Global File Cache can help reduce latency for frequently accessed data. Global File Cache deployment can be automated using a provisioning collection and scripted events. Global File Cache handles the read and write caches locally and maintains file locks across locations. Global File Cache can work with any SMB file servers, including Azure NetApp Files.



Global File Cache requires the following:

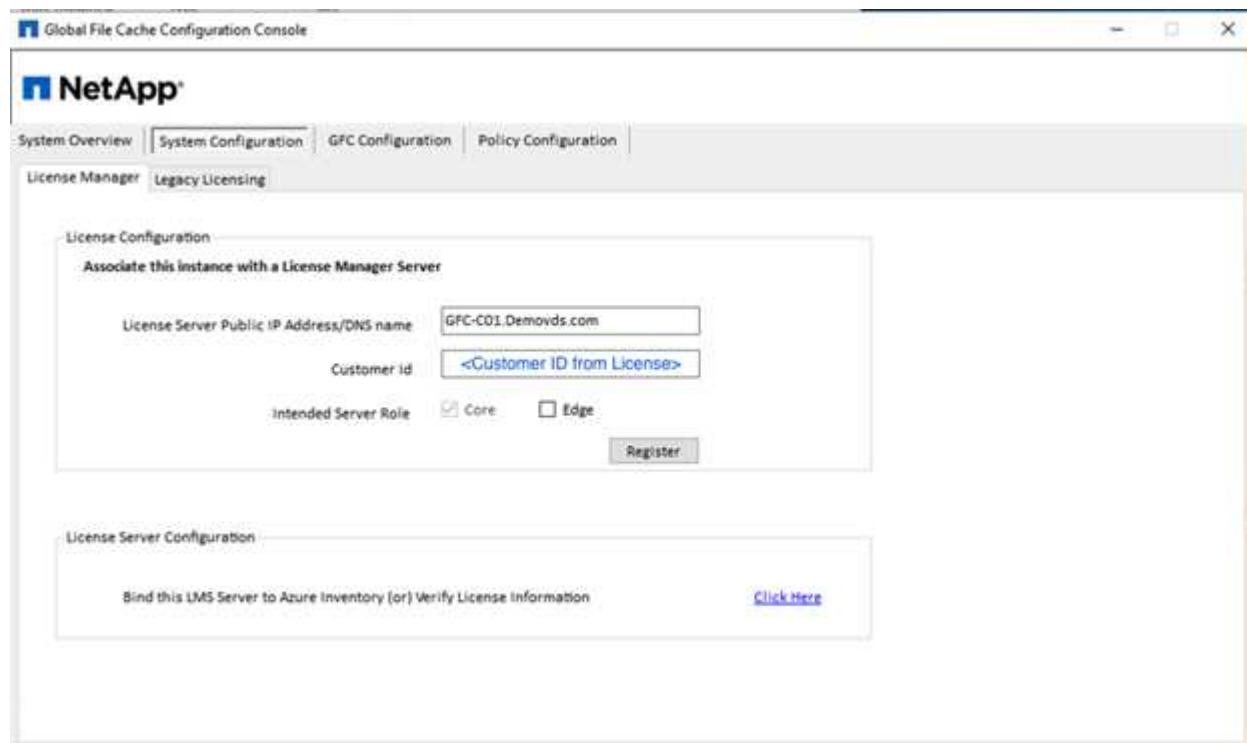
- Management server (License Management Server)
- Core

- Edge with enough disk capacity to cache the data

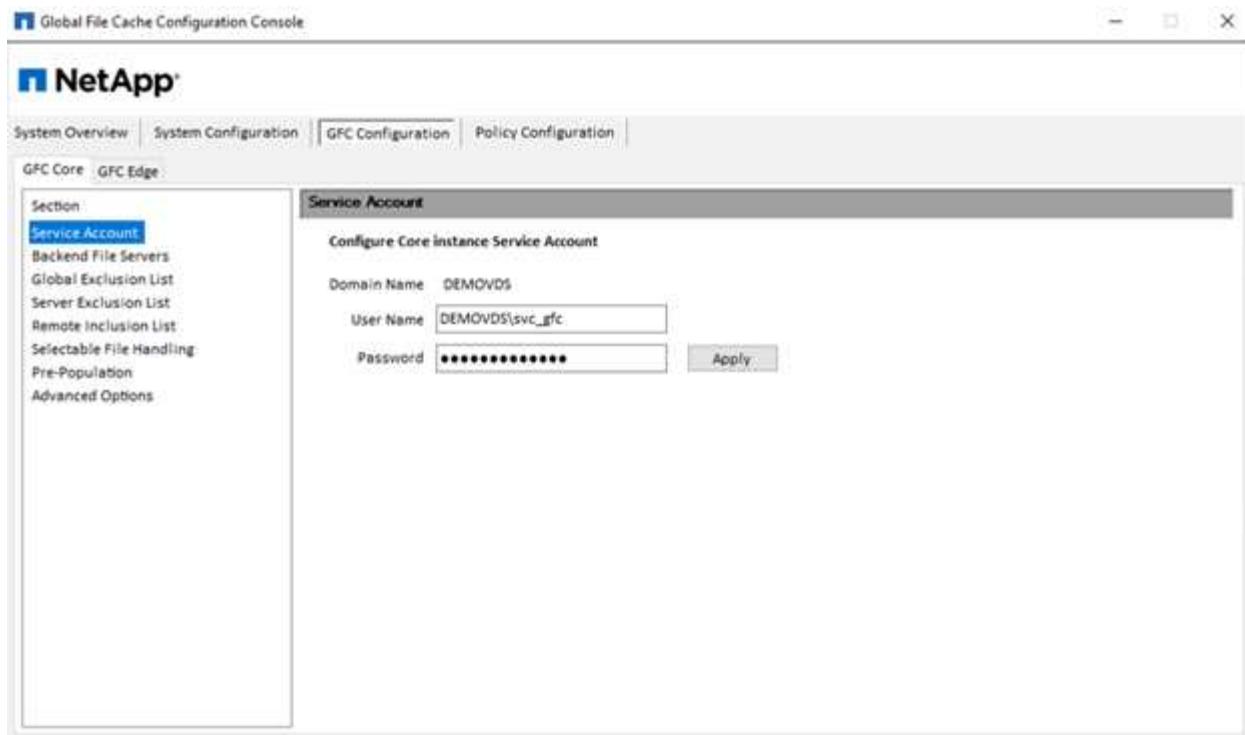
To download the software and to calculate the disk cache capacity for Edge, see the [GFC documentation](#).

For our validation, we deployed the core and management resources on the same VM at Azure and edge resources on NetApp HCI. Please note that the core is where high-volume data access is required and the edge is a subset of the core. After the software is installed, you must activate the license activated before use. To do so, complete the following steps:

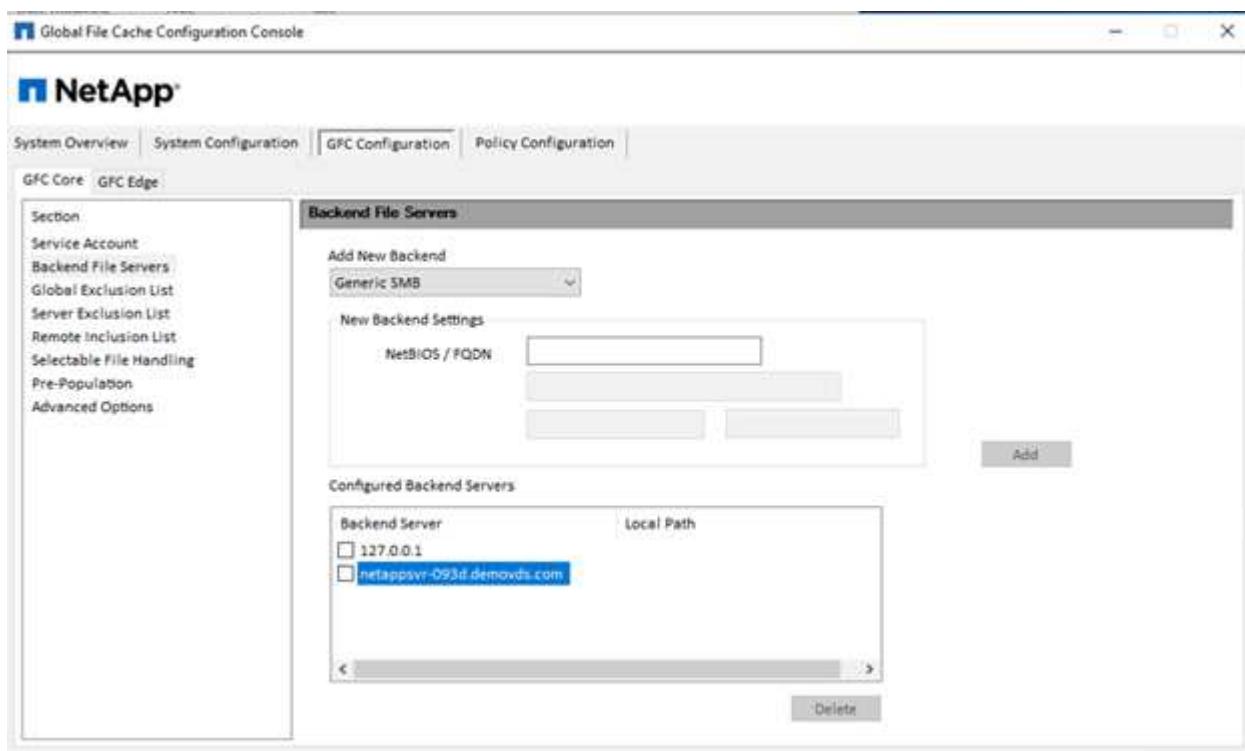
1. Under the License Configuration section, use the link Click Here to complete the license activation. Then register the core.



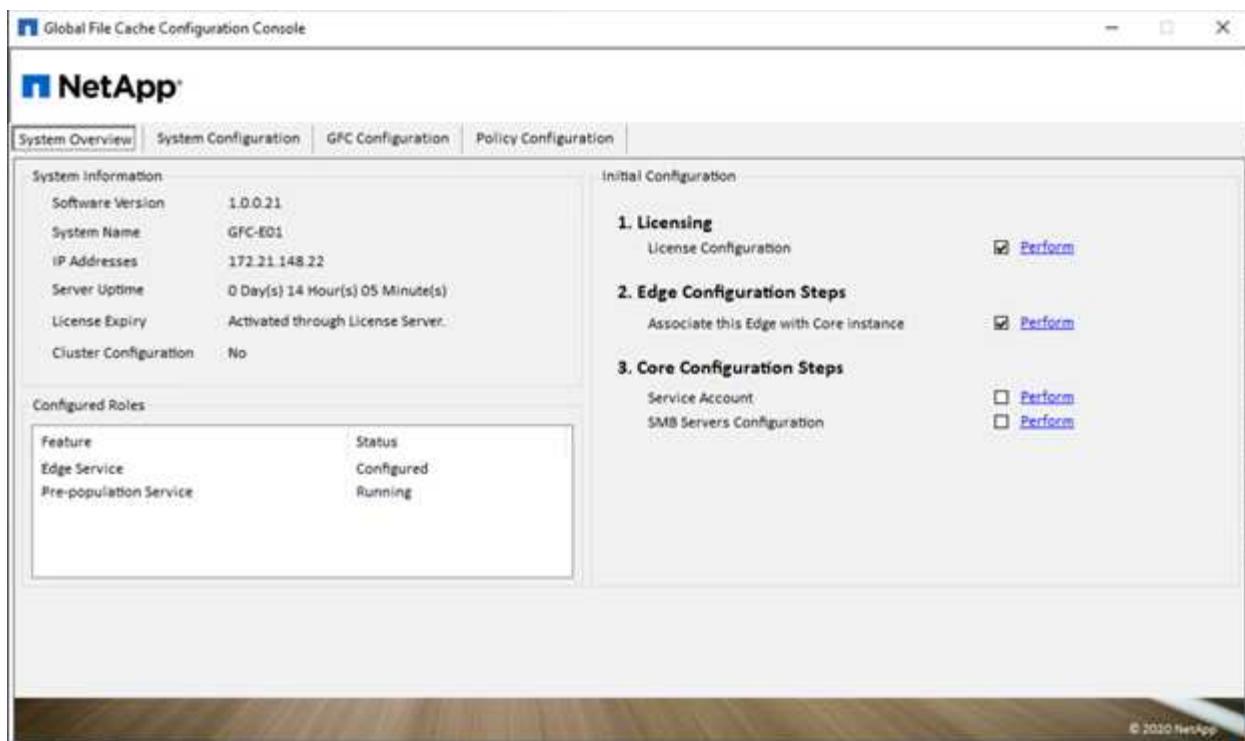
2. Provide the service account to be used for the Global File Cache. For the required permissions for this account, see the [GFC documentation](#).



3. Add a new backend file server and provide the file server name or IP.



4. On the edge, the cache drive must have the drive letter D. If it does not, use diskpart.exe to select the volume and change drive letter. Register with the license server as edge.



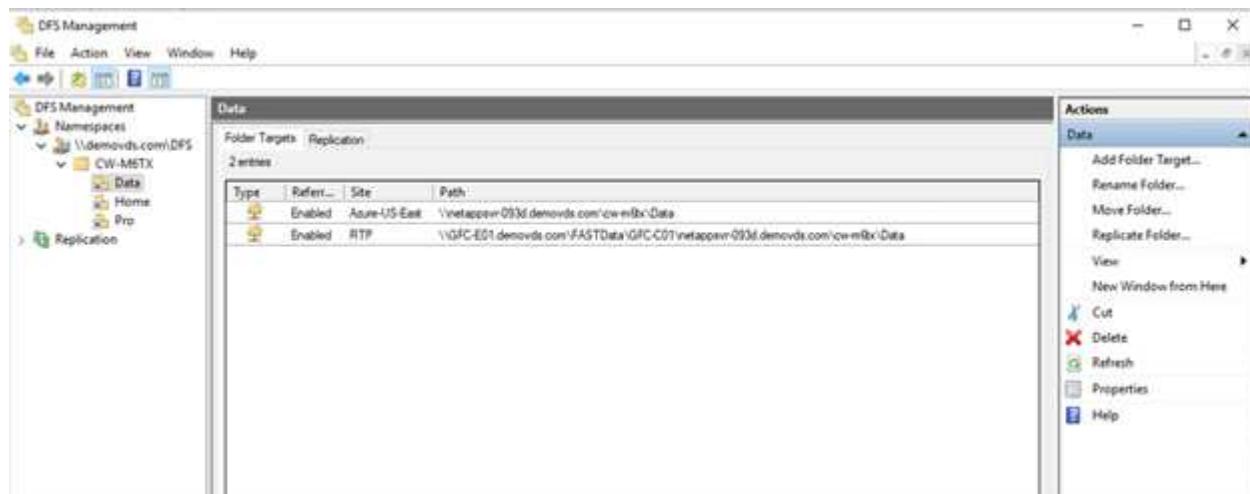
If core auto-configuration is enabled, core information is retrieved from the license management server automatically.

This screenshot shows the 'GFC Configuration' tab with 'GFC Core: GFC Edge' selected. On the left, a sidebar has 'Core Instances' selected. The main area is titled 'Core Instances' and contains fields for 'Core Auto Configuration' (checked, with a note '(Requires License Manager Server)'), 'Associate this Edge instance with a Core', and input fields for 'Cloud Fabric ID', 'FQDN / IP Address', 'Enabled SSL' (unchecked), 'User Name' (with '(Optional)' note), and 'Password' (with '(Optional)' note and an 'Add' button). Below these is a table showing existing associations: Cloud Fabric ID (GFC-C01), FQDN/IP Address (10.67.64.10), and SSL Enabled (0). A 'Delete' button is at the bottom right of the table.

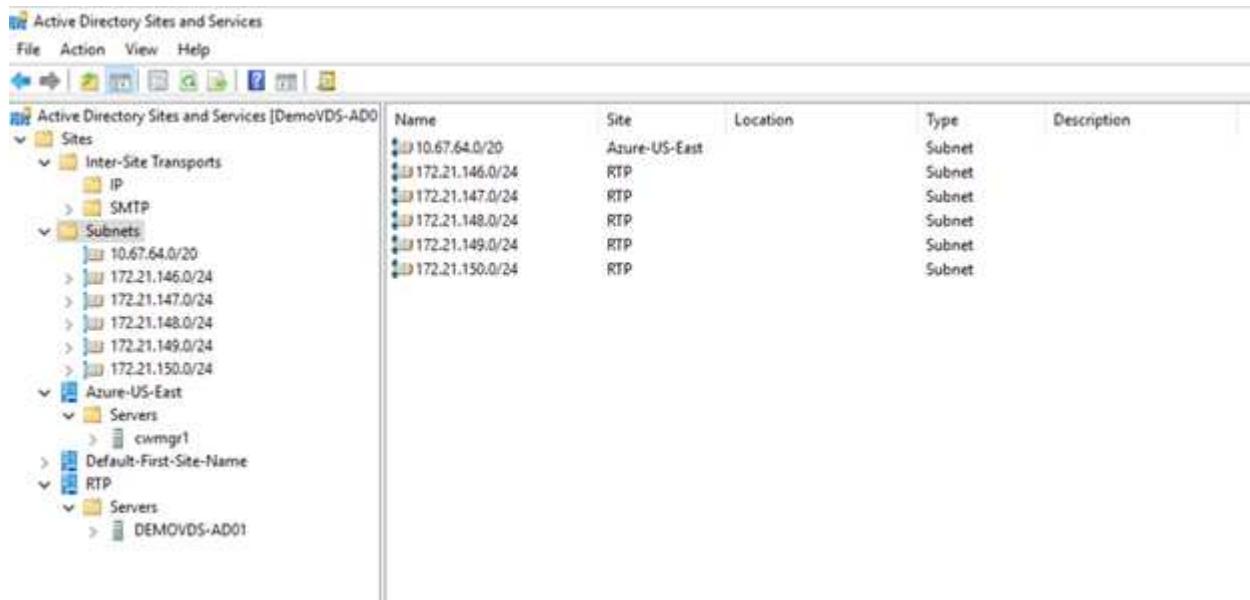
From any client machine, the administrators that used to access the share on the file server can access it with GFC edge using UNC Path \\<edge server name>\FASTDATA\<core server name>\<backend file server name>\<share name>. Administrators can include this path in user logonscript or GPO for users drive mapping at the edge location.

To provide transparent access for users across the globe, an administrator can setup the Microsoft Distributed

Filesystem (DFS) with links pointing to file server shares and to edge locations.



When users log in with Active Directory credentials based on the subnets associated with the site, the appropriate link is utilized by the DFS client to access the data.

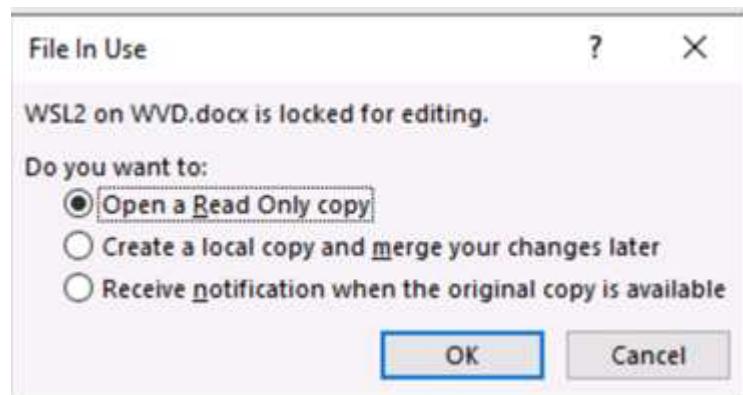


File icons change depending on whether a file is cached; files that are not cached have a grey X on the lower left corner of the icon. After a user in an edge location accesses a file, that file is cached, and the icon changes.

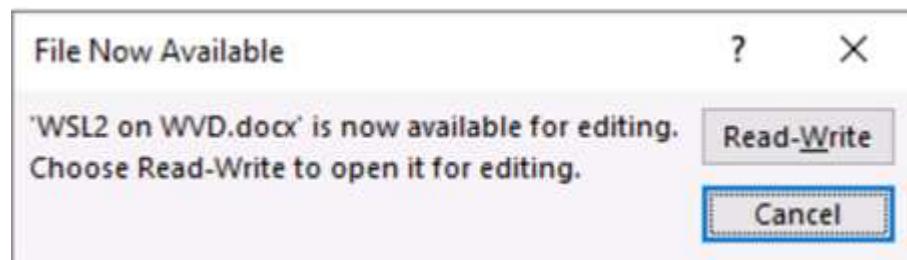
A screenshot of a Windows File Explorer window. The left sidebar shows 'Quick access', 'This PC', and 'Network'. The main area shows a list of files and folders in a folder named 'Data'. The columns are 'Name', 'Date modified', 'Type', and 'Size'. The list includes 'Department' (File folder), 'Outlook' (File folder), 'Outlook Files' (File folder), 'Output' (File folder), 'WindowsPowerShell' (File folder), 'FSLogix' (Registration Entries), 'GFC-1-0-0-21-Release' (Application, 26,869 KB), 'PDF1.pdf' (PDF File, 1,101 KB), 'PDF2.pdf' (PDF File, 1,066 KB), 'Spreadsheet.xlsx' (XLSX File, 298 KB), 'UserEdit.doc' (DOC File, 1,061 KB), 'UserEdit1.doc' (DOC File, 1,061 KB), 'UserEdit2.doc' (DOC File, 1,063 KB), 'UserMindmap.mm' (MM File, 86 KB), and 'UserPresentation.ppt' (PPT File, 3,071 KB). The file 'GFC-1-0-0-21-Release' is highlighted.

Name	Date modified	Type	Size
Department	10/1/2020 5:28 PM	File folder	
Outlook	10/12/2020 3:05 PM	File folder	
Outlook Files	10/12/2020 6:07 PM	File folder	
Output	10/12/2020 3:12 PM	File folder	
WindowsPowerShell	10/11/2020 6:24 PM	File folder	
FSLogix	10/11/2020 9:11 PM	Registration Entries	2 KB
GFC-1-0-0-21-Release	10/11/2020 10:05 ...	Application	26,869 KB
PDF1.pdf	6/22/2016 9:31 PM	PDF File	1,101 KB
PDF2.pdf	6/22/2016 9:31 PM	PDF File	1,066 KB
Spreadsheet.xlsx	6/22/2016 9:31 PM	XLSX File	298 KB
UserEdit.doc	6/22/2016 9:31 PM	DOC File	1,061 KB
UserEdit1.doc	10/12/2020 3:13 PM	DOC File	1,061 KB
UserEdit2.doc	10/12/2020 3:01 PM	DOC File	1,063 KB
UserMindmap.mm	6/22/2016 9:31 PM	MM File	86 KB
UserPresentation.ppt	6/22/2016 9:31 PM	PPT File	3,071 KB

When a file is open and another user is trying to open the same file from an edge location, the user is prompted with the following selection:



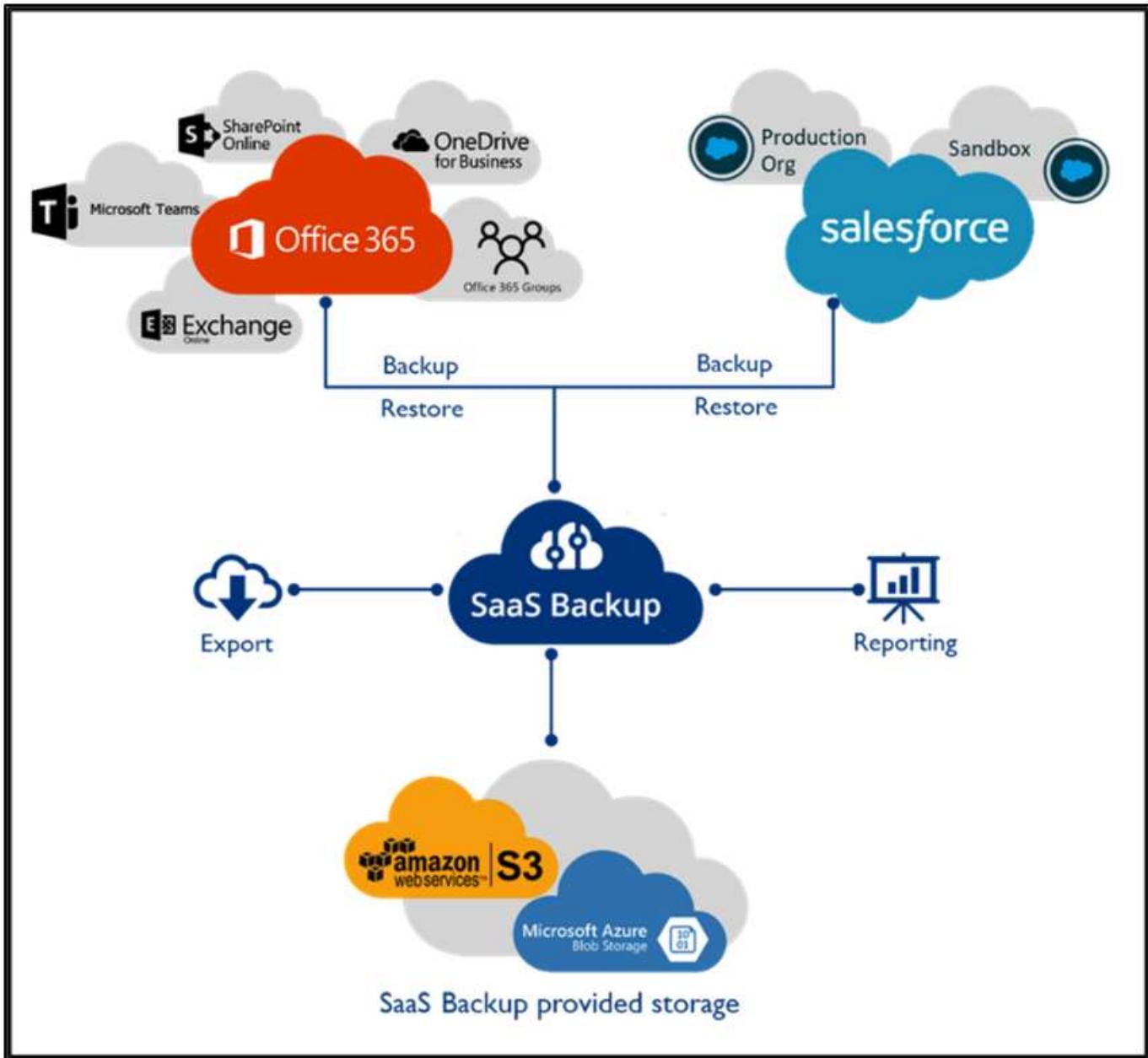
If the user selects the option to receive a notification when the original copy is available, the user is notified as follows:



For more information, see this [video on Talon and Azure NetApp Files Deployment](#).

## SaaS Backup

NetApp VDS provides data protection for Salesforce and Microsoft Office 365, including Exchange, SharePoint, and Microsoft OneDrive. The following figure shows how NetApp VDS provides SaaS Backup for these data services.



For a demonstration of Microsoft Office 365 data protection, see [this video](#).

For a demonstration of Salesforce data protection, see [this video](#).

**Next: Operation Management**

#### Operation management

With NetApp VDS, administrators can delegate tasks to others. They can connect to deployed servers to troubleshoot, view logs, and run audit reports. While assisting customers, helpdesk or level-3 technicians can shadow user sessions, view process lists, and kill processes if required.

For information on VDS logfiles, see the [Troubleshooting Failed VDA Actions page](#).

For more information on the required minimum permissions, see the [VDA Components and Permissions page](#).

If you would like to manually clone a server, see the [Cloning Virtual Machines page](#).

To automatically increase the VM disk size, see the [Auto-Increase Disk Space Feature page](#).

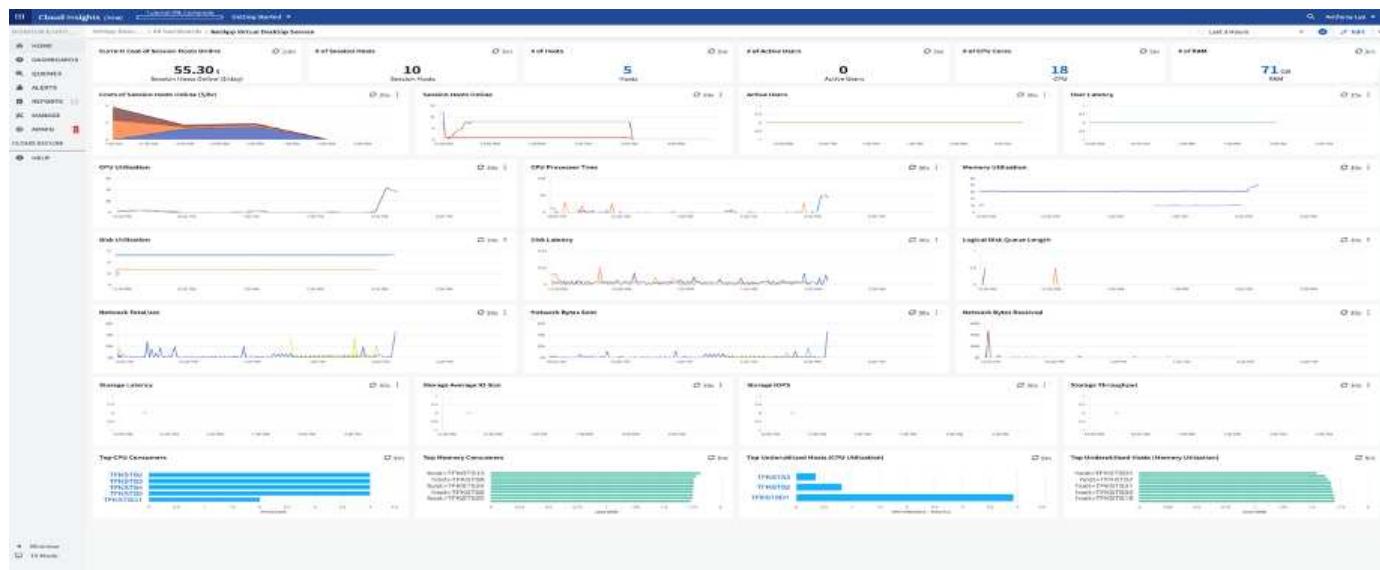
To identify the gateway address to manually configure the client, see the [End User Requirements page](#).

## Cloud Insights

NetApp Cloud Insights is a web-based monitoring tool that gives you complete visibility into infrastructure and applications running on NetApp and other third-party infrastructure components. Cloud Insights supports both private cloud and public clouds for monitoring, troubleshooting, and optimizing resources.

Only the acquisition unit VM (can be Windows or Linux) must be installed on a private cloud to collect metrics from data collectors without the need for agents. Agent-based data collectors allow you to pull custom metrics from Windows Performance Monitor or any input agents that Telegraf supports.

The following figure depicts the Cloud Insights VDS dashboard.



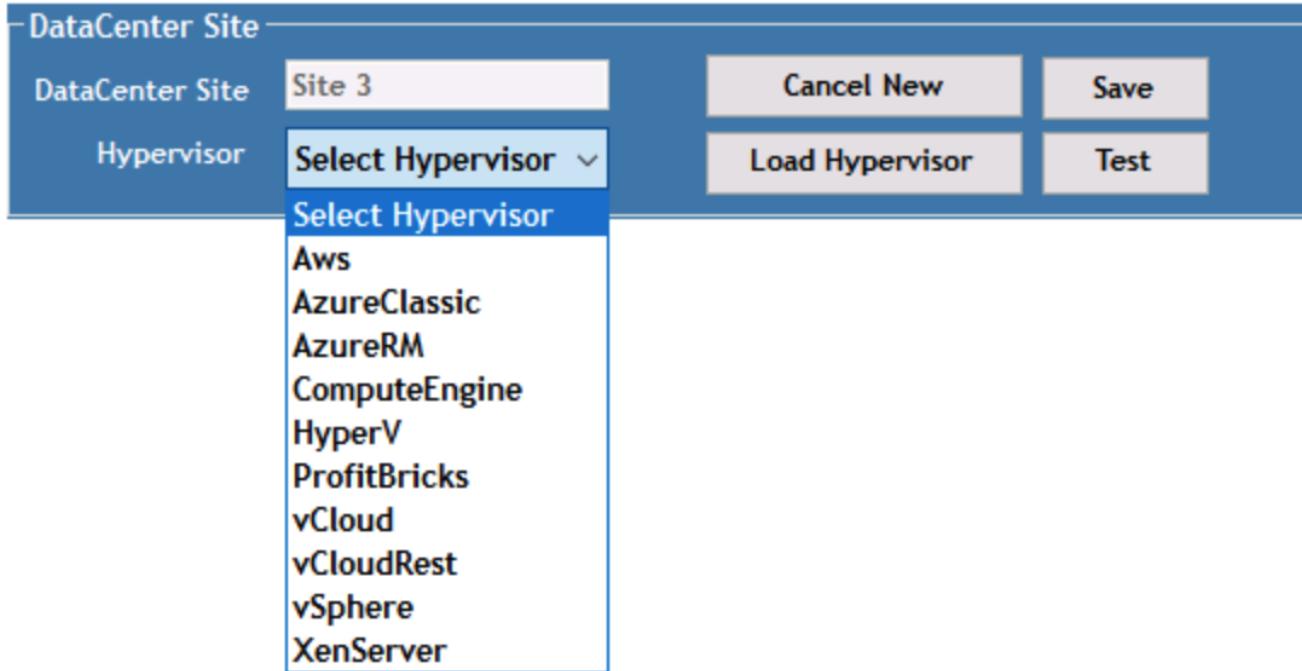
For more info on NetApp Cloud Insights, see [this video](#).

Next: [Tools and logs](#)

## Tools and Logs

### DCCConfig Tool

The DCCconfig tool supports the following hypervisor options for adding a site:



The screenshot shows the 'Configuration' interface with a tab bar including 'DataCenter', 'Accounts', 'Email', 'DatabaseConnection', 'Exclude', 'DataCenter Sites', 'Product Keys', 'Static IpAddress', and 'Drive Mapping'. The 'Drive Mapping' tab is active. A table lists shared data mappings:

Description	DriveLetter
Shared Data	P
FTP	F
User Home	H

A large gray area below the table is likely a placeholder for additional content or a form.

Workspace-specific drive-letter mapping for shared data can be handled using GPO. Professional Services or the support team can use the advanced tab to customize settings like Active Directory OU names, the option to enable or disable deployment of FSLogix, various timeout values, and so on.

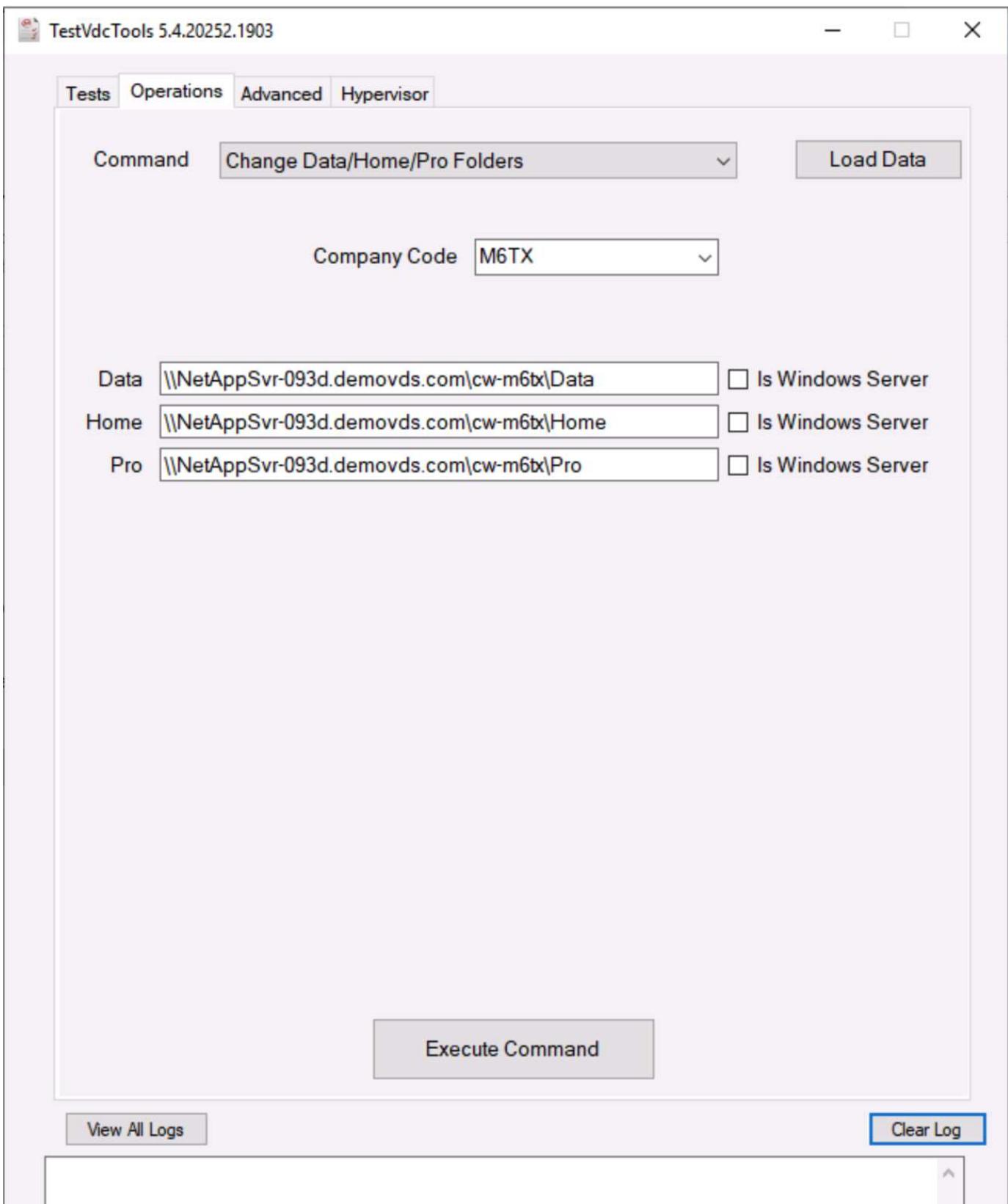
PropertyName	FriendlyName	Value
Server Creation	UpdateVMNameWhenRemovedFromCache	<input type="checkbox"/>
Server Creation	UpdateFirewallRules	<input checked="" type="checkbox"/>
Server Creation	WaitAfterRebootMin	6
Server Creation	WaitAfterHypervisorCreateMin	1
Server Creation	WaitAfterSysPrepMin	10
Server Creation	WaitAfterSysPrepOr2008ServersMin	30
Server Creation	GFI Agent Path	
Server Creation	Automated Cloning Enabled	<input checked="" type="checkbox"/>
Server Creation	CompaniesOU	Cloud Workspace Companies
Server Creation	Install ThinPrint v11	<input checked="" type="checkbox"/>
Server Creation	ServersOU	Cloud Workspace Servers
Server Creation	Install FSLogix	<input checked="" type="checkbox"/>
Server Creation	Use Default OUs	<input checked="" type="checkbox"/>
Server Creation	Max Threads	50
Server Creation	Wait for DNS to Update Minutes	15
Check Vdc Tools Version	Run Every X Minutes	5
Daily Actions	Enabled	<input checked="" type="checkbox"/>
Daily Actions	Run at Startup	<input checked="" type="checkbox"/>
Generate Reports	Time Of Day	06:00
Daily Maintenance	Enabled	<input checked="" type="checkbox"/>
Daily Maintenance	Time Of Day	08:01
Weekly Maintenance	Enabled	<input checked="" type="checkbox"/>
Weekly Maintenance	Time Of Day	08:01
Automatic Resource Allocation	Day	Sunday
Resource Allocation	Enabled	<input checked="" type="checkbox"/>
Email Reports	Use Data Center Defaults	<input checked="" type="checkbox"/>
Email Reports	IncludeEmailAttachment	<input type="checkbox"/>
Server Heartbeat	Interval Minutes	15

## Command Center (Previously known as TestVdc Tools)

To launch Command Center and the required role, see the [Command Center Overview](#).

You can perform the following operations:

- Change the SMB Path for a workspace.



- Change the site for provisioning collection.

TestVdcTools 5.4.20252.1903

Tests Operations Advanced Hypervisor

Command Edit Provisioning Collection

Provisioning Collection Windows2019

Description On vSphere Site 2

Share Drive P

Minimum Cache Level 1

Operating System Windows Server 2019

Collection Type Shared

	Data Center Site	Role	Template	Storage
▶	Site 2	TSData	Windows2019	DS01
*				

< >

Execute Command

### Log Files

Name	Date modified	Type	Size
CwAgent	9/19/2020 12:35 PM	File folder	
CWAutomationService	9/19/2020 12:34 PM	File folder	
CWManagerX	9/19/2020 12:53 PM	File folder	
CwVmAutomationService	9/19/2020 12:34 PM	File folder	
TestVdcTools	9/22/2020 8:20 PM	File folder	
report	9/19/2020 12:18 PM	Executable Jar File	705 KB

Check [automation logs](#) for more info.

Next: Conclusion

#### GPU considerations

GPUs are typically used for graphic visualization (rendering) by performing repetitive arithmetic calculations. This repetitive compute capability is often used for AI and deep learning use cases.

For graphic intensive applications, Microsoft Azure offers the NV series based on the NVIDIA Tesla M60 card with one to four GPUs per VM. Each NVIDIA Tesla M60 card includes two Maxwell-based GPUs, each with 8GB of GDDR5 memory for a total of 16GB.



An NVIDIA license is included with the NV series.

Graphics Card

Sensors

Advanced

Validation

Name NVIDIA Tesla M60 Lookup

GPU GM204 Revision FF

Technology 28 nm Die Size 398 mm<sup>2</sup>

Release Date Aug 30, 2015 Transistors 5200M

**NVIDIA**BIOS Version 84.04.85.00.03 ↻  UEFI

Subvendor NVIDIA Device ID 10DE 13F2 - 10DE 115E

ROPs/TMUs 64 / 128 Bus Interface PCI ?

Shaders 2048 Unified DirectX Support 12 (12\_1)

Pixel Fillrate 75.4 GPixel/s Texture Fillrate 150.8 GTexel/s

Memory Type GDDR5 (Hynix) Bus Width 256 bit

Memory Size 8192 MB Bandwidth 160.4 GB/s

Driver Version 27.21.14.5257 (NVIDIA 452.57) / 2016

Driver Date Oct 22, 2020 Digital Signature WHQL

GPU Clock 557 MHz Memory 1253 MHz Boost 1178 MHz

Default Clock 557 MHz Memory 1253 MHz Boost 1178 MHz

NVIDIA SLI Disabled

Computing  OpenCL  CUDA  DirectCompute  DirectMLTechnologies  Vulkan  Ray Tracing  PhysX  OpenGL 4.6

NVIDIA Tesla M60

Close

With NetApp HCI, the H615C GPU contains three NVIDIA Tesla T4 cards. Each NVIDIA Tesla T4 card has a Touring-based GPU with 16GB of GDDR6 memory. When used in a VMware vSphere environment, virtual machines are able to share the GPU, with each VM having dedicated frame buffer memory. Ray tracing is available with the GPUs on the NetApp HCI H615C to produce realistic images including light reflections. Please note that you need to have an NVIDIA license server with a license for GPU features.

Graphics Card

Sensors

Advanced

Validation



Name

NVIDIA GRID T4-8Q

Lookup

GPU

TU104

Revision

A1



Technology

12 nm

Die Size

545 mm<sup>2</sup>

Release Date

Sep 13, 2018

Transistors

13600M

BIOS Version

0.00.00.00.00



UEFI

Subvendor

NVIDIA

Device ID

10DE 1EB8 - 10DE 130F

ROPs/TMUs

8 / 160

Bus Interface

PCI

?

Shaders

2560 Unified

DirectX Support

12 (12\_2)

Pixel Fillrate

4.7 GPixel/s

Texture Fillrate

93.6 GTexel/s

Memory Type

GDDR6

Bus Width

256 bit

Memory Size

8192 MB

Bandwidth

Unknown

Driver Version

27.21.14.5257 (NVIDIA 452.57) / 2016

Driver Date

Oct 22, 2020

Digital Signature

WHQL

GPU Clock

585 MHz

Memory

0 MHz

Shader

N/A

Default Clock

585 MHz

Memory

0 MHz

Shader

N/A

NVIDIA SLI

Disabled

Computing

 OpenCL CUDA DirectCompute DirectML

Technologies

 Vulkan Ray Tracing PhysX OpenGL 4.6

NVIDIA GRID T4-8Q

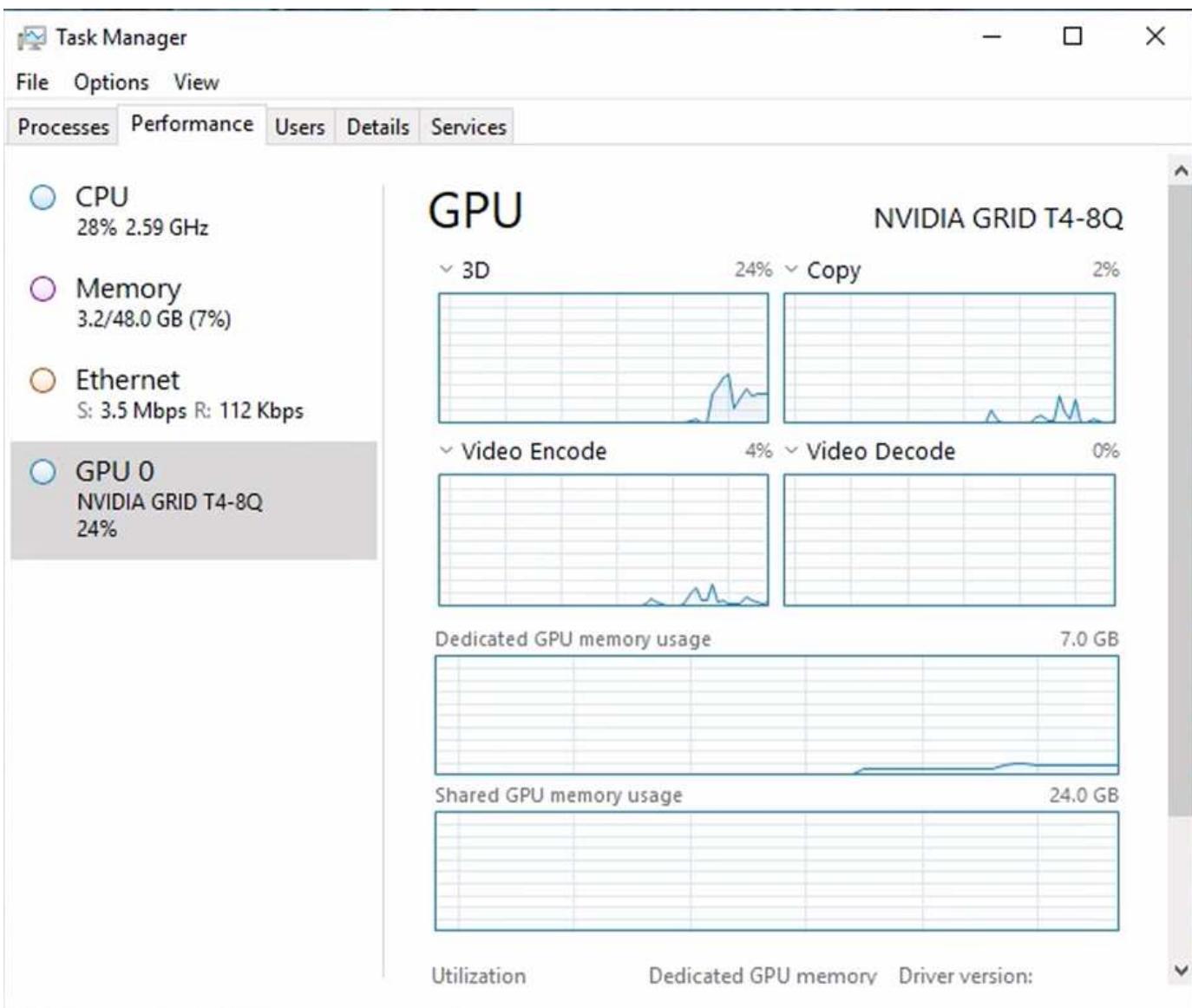
Close

To use the GPU, you must install the appropriate driver, which can be downloaded from the NVIDIA license portal. In an Azure environment, the NVIDIA driver is available as GPU driver extension. Next, the group policies in the following screenshot must be updated to use GPU hardware for remote desktop service sessions. You should prioritize H.264 graphics mode and enable encoder functionality.

The screenshot shows the Local Group Policy Editor window. The left pane displays a tree view of policy settings under 'Microsoft account' and 'Remote Desktop Services'. The right pane lists specific settings with their current state and comments. The 'Remote Desktop Services' section is expanded, showing various options like 'Limit maximum color depth', 'Enforce Removal of Remote Desktop Wallpaper', and 'Prioritize H.264/AVC 444 graphics mode for Remote Desktop Connections'. Most of these settings are currently set to 'Not configured' or 'Enabled' with a comment of 'No'.

Setting	State	Comment
RemoteFX for Windows Server 2008 R2:	Not configured	No
Limit maximum color depth	Not configured	No
Enforce Removal of Remote Desktop Wallpaper	Enabled	No
Use hardware graphics adapters for all Remote Desktop Services sessions	Not configured	No
Limit maximum display resolution	Not configured	No
Limit number of monitors	Not configured	No
Remove "Disconnect" option from Shut Down dialog	Not configured	No
Remove Windows Security item from Start menu	Not configured	No
Use advanced RemoteFX graphics for RemoteApp	Not configured	No
Prioritize H.264/AVC 444 graphics mode for Remote Desktop Connections	Enabled	No
Configure H.264/AVC hardware encoding for Remote Desktop Connections	Enabled	No
Configure compression for RemoteFX data	Not configured	No
Configure image quality for RemoteFX Adaptive Graphics	Not configured	No
Enable RemoteFX encoding for RemoteFX clients designed for Windows Server 2008 R2 SP1	Not configured	No
Configure RemoteFX Adaptive Graphics	Not configured	No
Start a program on connection	Not configured	No
Always show desktop on connection	Not configured	No
Allow desktop composition for remote desktop sessions	Not configured	No
Do not allow font smoothing	Not configured	No

Validate GPU performance monitoring with Task Manager or by using the nvidia-smi CLI when running WebGL samples. Make sure that GPU, memory, and encoder resources are being consumed.



To make sure that the virtual machine is deployed to the NetApp HCI H615C with Virtual Desktop Service, define a site with the vCenter cluster resource that has H615C hosts. The VM template must have the required vGPU profile attached.

For shared multi-session environments, consider allocating multiple homogenous vGPU profiles. However, for high end professional graphics application, it is better to have each VM dedicated to a user to keep VMs isolated.

The GPU processor can be controlled by a QoS policy, and each vGPU profile can have dedicated frame buffers. However, the encoder and decoder are shared for each card. The placement of a vGPU profile on a GPU card is controlled by the vSphere host GPU assignment policy, which can emphasize performance (spread VMs) or consolidation (group VMs).

[Next: Solutions for industry.](#)

### Solutions for Industry

Graphics workstations are typically used in industries such as manufacturing, healthcare, energy, media and entertainment, education, architecture, and so on. Mobility is often limited for graphics-intensive applications.

To address the issue of mobility, Virtual Desktop Services provide a desktop environment for all types of workers, from task workers to expert users, using hardware resources in the cloud or with NetApp HCI, including options for flexible GPU configurations. VDS enables users to access their work environment from anywhere with laptops, tablets, and other mobile devices.

To run manufacturing workloads with software like ANSYS Fluent, ANSYS Mechanical, Autodesk AutoCAD, Autodesk Inventor, Autodesk 3ds Max, Dassault Systèmes SOLIDWORKS, Dassault Systèmes CATIA, PTC Creo, Siemens PLM NX, and so on, the GPUs available on various clouds (as of Jan 2021) are listed in the following table.

GPU Model	Microsoft Azure	Google Compute (GCP)	Amazon Web Services (AWS)	On-Premises (NetApp HCI)
NVIDIA M60	Yes	Yes	Yes	No
NVIDIA T4	No	Yes	Yes	Yes
NVIDIA P100	No	Yes	No	No
NVIDIA P4	No	Yes	No	No

Shared desktop sessions with other users and dedicated personal desktops are also available. Virtual desktops can have one to four GPUs or can utilize partial GPUs with NetApp HCI. The NVIDIA T4 is a versatile GPU card that can address the demands of a wide spectrum of user workloads.

Each GPU card on NetApp HCI H615C has 16GB of frame buffer memory and three cards per server. The number of users that can be hosted on single H615C server depends on the user workload.

Users/Server	Light (4GB)	Medium (8GB)	Heavy (16GB)
H615C	12	6	3

To determine the user type, run the GPU profiler tool while users are working with applications performing typical tasks. The GPU profiler captures memory demands, the number of displays, and the resolution that users require. You can then pick the vGPU profile that satisfies your requirements.

Virtual desktops with GPUs can support a display resolution of up to 8K, and the utility nView can split a single monitor into regions to work with different datasets.

With ONTAP file storage, you can realize the following benefits:

- A single namespace that can grow up to 20PB of storage with 400 billion of files, without much administrative input
- A namespace that can span the globe with a Global File Cache
- Secure multitenancy with managed NetApp storage
- The migration of cold data to object stores using NetApp FabricPool
- Quick file statistics with file system analytics
- Scaling a storage cluster up to 24 nodes increasing capacity and performance
- The ability to control storage space using quotas and guaranteed performance with QoS limits
- Securing data with encryption
- Meeting broad requirements for data protection and compliance
- Delivering flexible business continuity options

[Next: Conclusion](#)

## Conclusion

The NetApp Virtual Desktop Service provides an easy-to-consume virtual desktop and application environment with a sharp focus on business challenges. By extending VDS with the on-premises ONTAP environment, you can use powerful NetApp features in a VDS environment, including rapid clone, in-line deduplication, compaction, thin provisioning, and compression. These features save storage costs and improve performance with all-flash storage. With VMware vSphere hypervisor, which minimizes server-provisioning time by using Virtual Volumes and vSphere API for Array integration. Using the hybrid cloud, customers can pick the right environment for their demanding workloads and save money. The desktop session running on-premises can access cloud resources based on policy.

[Next: Where to Find Additional Information](#)

## Where to Find Additional Information

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

- [NetApp Cloud](#)
- [NetApp VDS Product Documentation](#)
- [Connect your on-premises network to Azure with VPN Gateway](#)
- [Azure Portal](#)
- [Microsoft Windows Virtual Desktop](#)
- [Azure NetApp Files Registration](#)

## VMware Horizon

## Demos and Tutorials

### Hybrid Cloud, Virtualization and Containers Videos and Demos

See the following videos and demos highlighting specific features of the hybrid cloud, virtualization, and container solutions.

## NetApp ONTAP Tools for VMware vSphere

### ONTAP Tools for VMware - Overview

- ▶ [https://docs.netapp.com/us-en/netapp-solutions/media/otv\\_overview.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/otv_overview.mp4) (video)

### VMware iSCSI Datastore Provisioning with ONTAP

- ▶ [https://docs.netapp.com/us-en/netapp-solutions/media/otv\\_iscsi\\_provision.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/otv_iscsi_provision.mp4) (video)

### VMware NFS Datastore Provisioning with ONTAP

- ▶ [https://docs.netapp.com/us-en/netapp-solutions/media/otv\\_nfs\\_provision.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/otv_nfs_provision.mp4) (video)

## VMware Cloud on AWS with AWS FSx for NetApp ONTAP

### Windows Guest Connected Storage with FSx ONTAP using iSCSI

- ▶ [https://docs.netapp.com/us-en/netapp-solutions/media/vmc\\_windows\\_vm\\_iscsi.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/vmc_windows_vm_iscsi.mp4) (video)

### Linux Guest Connected Storage with FSx ONTAP using NFS

- ▶ [https://docs.netapp.com/us-en/netapp-solutions/media/vmc\\_linux\\_vm\\_nfs.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/vmc_linux_vm_nfs.mp4) (video)

## SnapCenter Plug-in for VMware vSphere

NetApp SnapCenter software is an easy-to-use enterprise platform to securely coordinate and manage data protection across applications, databases, and file systems.

The SnapCenter Plug-in for VMware vSphere allows you to perform backup, restore, and attach operations for VMs and backup and mount operations for datastores that are registered with SnapCenter directly within VMware vCenter.

For more information about NetApp SnapCenter Plug-in for VMware vSphere, see the [NetApp SnapCenter Plug-in for VMware vSphere Overview](#).

### SnapCenter Plug-in for VMware vSphere - Solution Pre-Requisites

- ▶ [https://docs.netapp.com/us-en/netapp-solutions/media/scv\\_prereq\\_overview.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/scv_prereq_overview.mp4) (video)

### SnapCenter Plug-in for VMware vSphere - Deployment

- ▶ [https://docs.netapp.com/us-en/netapp-solutions/media/scv\\_deployment.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/scv_deployment.mp4) (video)

### SnapCenter Plug-in for VMware vSphere - Backup Workflow

- ▶ [https://docs.netapp.com/us-en/netapp-solutions/media/scv\\_backup\\_workflow.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/scv_backup_workflow.mp4) (video)

### SnapCenter Plug-in for VMware vSphere - Restore Workflow

- ▶ [https://docs.netapp.com/us-en/netapp-solutions/media/scv\\_restore\\_workflow.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/scv_restore_workflow.mp4) (video)

### SnapCenter - SQL Restore Workflow

- ▶ [https://docs.netapp.com/us-en/netapp-solutions/media/scv\\_sql\\_restore.mp4](https://docs.netapp.com/us-en/netapp-solutions/media/scv_sql_restore.mp4) (video)

## NetApp with VMware Tanzu

VMware Tanzu enables customers to deploy, administer, and manage their Kubernetes environment through vSphere or the VMware Cloud Foundation. This portfolio of products from VMware allows customer to manage all their relevant Kubernetes clusters from a single control plane by choosing the VMware Tanzu edition that best suits their needs.

For more information about VMware Tanzu, see the [VMware Tanzu Overview](#). This review covers use cases, available additions, and more about VMware Tanzu.

- [How to use vVols with NetApp and VMware Tanzu Basic, part 1](#)
- [How to use vVols with NetApp and VMware Tanzu Basic, part 2](#)
- [How to use vVols with NetApp and VMware Tanzu Basic, part 3](#)

## NetApp with Red Hat OpenShift

Red Hat OpenShift, an enterprise Kubernetes platform, enables you to run container-based applications with an open hybrid-cloud strategy. Available as a cloud service on leading public clouds or as self-managed software, Red Hat OpenShift provides customers with the flexibility they need when designing their container-based solution.

For more information regarding Red Hat OpenShift, see this [Red Hat OpenShift Overview](#). You can also review the product documentation and deployment options to learn more about Red Hat OpenShift.

- [Workload Migration - Red Hat OpenShift with NetApp](#)
- [Red Hat OpenShift Deployment on RHV: Red Hat OpenShift with NetApp](#)

## Blogs

### NetApp and VMware Cloud Foundation (VCF)

# Solution Automation

## NetApp Solution Automation

### Introduction

In providing solutions to meet today's business challenges, NetApp delivers solutions with the following goals:

- Providing validated deployment and configuration steps,
- Providing solutions that are easily consumable,
- Providing solution deployment that has a predictable outcome, is easily repeated, and scalable across a customer's enterprise.

In order to achieve these goals, it is paramount that the deployment and configuration of infrastructure and/or applications delivered through our solutions is simplified through automation. NetApp is committed to simplifying solution consumption through automation.

Utilizing open-source automation tools such as Red Hat Ansible, HashiCorp Terraform, or Microsoft Powershell, NetApp solutions have the ability to automate application deployment, cloud provisioning, configuration management, and many other common IT tasks. NetApp's solutions take advantage of publicly available automation artifacts - as well as providing NetApp authored automation - to simplify the overall deployment of a solution.

Where automation capabilities are available, the solution collateral will guide the user through the process for automating the solution or solution steps via the specific automation tool(s).

### Setup the Ansible control node (For CLI based deployments)

## NetApp Solution Automation

### AWS Authentication Requirements for CVO and Connector Using NetApp Cloud Manager

To configure automated Deployments of CVO and Connectors using Ansible playbooks via AWX/Ansible Tower, the following information is needed:

#### Acquiring Access/Secret Keys from AWS

1. To deploy CVO and Connector in Cloud Manager, we need AWS Access/Secret Key. Acquire the keys in AWS console by launching IAM-->Users-->your username-->security credentials-->Create Access key.
2. Copy access keys and keep them secured to use in Connector and CVO deployment.



If you lose your key, you can create another access key and delete the one you lost

## Access keys

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can also use them with third-party tools.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. Learn more.

[Create access key](#)

Access key ID	Created	Last used
---------------	---------	-----------

## Acquiring Refresh Token from NetApp Cloud Central

1. Login into your cloud central account using your account credentials at <https://services.cloud.netapp.com/refresh-token>
2. Generate a refresh Token and save it for deployments.

### Refresh Token Generator

You can use this refresh token to obtain an access tokens for users. Store this refresh token securely. If necessary, you can revoke the token at a later time by navigating to the [Refresh Token Generator](#).

Note that this token is displayed on this page only—it is not stored on our servers. The token will no longer be displayed if you refresh or leave this page.

REFRESH TOKEN: [Copy to clipboard](#)  
EAafPTMCuu4QJI9hR2PTRT75Lswr0fHp4BheEjT2XFsHt

## Acquiring Client ID

1. Access the API page to copy Client ID at <https://services.cloud.netapp.com/developer-hub>.
2. Click on "learn How to Authenticate", in the top right corner.
3. From the Authentication window that pops up, copy the Client ID from Regular Access if you require a username/password to login. Federated users with SSO should copy the client ID from the "Refresh Token Tab".

## Authentication Information

X

NetApp Cloud Central Services use OAuth 2.0, an industry-standard protocol, for authorization.

Communicating with an authenticated endpoint is a two step-process.

1. Acquire a JWT access token from the OAuth token endpoint.
2. Call an API endpoint with the JWT access token.

Non-federated users can use regular access or refresh token access, federated users must use refresh token access.

[Regular Access](#)    [Refresh Token Access \(Required for federated users\)](#)

### How to Acquire a JWT Access Token via regular token access

1. Make an HTTP POST request to the endpoint

<https://netapp-cloud-account.auth0.com/oauth/token>

Include the header Content-Type: application/json

Include the body:

[Copy to clipboard](#)

```
{  
  "grant_type": "password",  
  "username": "YOUR_EMAIL_ADDRESS",  
  "password": "YOUR_PASSWORD",  
  "audience": "https://api.cloud.netapp.com",  
  "client_id": "  
}
```

## Acquiring Key Pair from AWS

1. In AWS console, search for “Key Pair” and create a key pair with “pem”. Remember the name of you key\_pair, we will use it to deploy the connector.

EC2 > Key pairs > Create key pair

### Create key pair

**Key pair**  
A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name:  The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

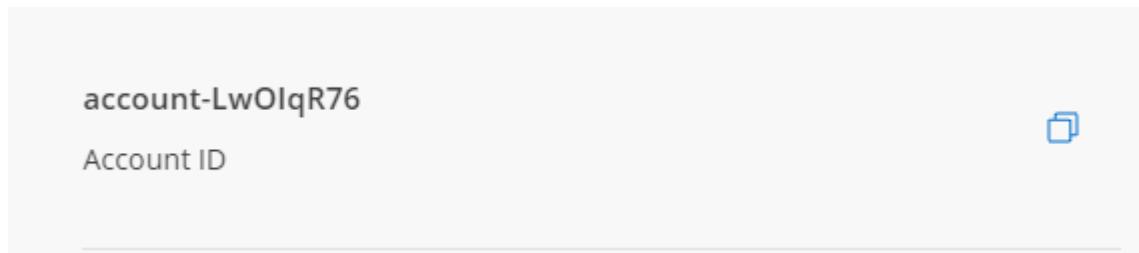
Private key file format:  pem For use with OpenSSH  
 ppk For use with PuTTY

Tags (Optional)  
No tags associated with the resource.  
[Add tag](#)  
You can add 50 more tags.

[Cancel](#) [Create key pair](#)

## Acquiring Account ID

1. In Cloud Manager, click on Account → Manage Accounts and then copy the account id for use in variables for AWX.



## Cloud Volumes Automation via Terraform

This solution documents the automated deployments of Cloud Volumes on AWS (CVO Single Node, CVO HA and FSX ONTAP) and Azure (CVO Single Node, CVO HA and ANF) using Terraform modules. The code can be found at [https://github.com/NetApp-Automation/na\\_cloud\\_volumes\\_automation](https://github.com/NetApp-Automation/na_cloud_volumes_automation)

### Pre-requisites

1. Terraform >= 0.13
2. Cloud Manager Account
3. Cloud Provider Account – AWS, Azure
4. Host machine (any OS supported by Terraform)

### Provider documentation

The documentation of Terraform provider for Cloud Manager is available at: <https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/latest/docs>

### Controlling the provider version

Note that you can also control the provider version. This is controlled by a required\_providers block in your Terraform configuration.

The syntax is as follows:

```
terraform {  
    required_providers {  
        netapp-cloudmanager = {  
            source = "NetApp/netapp-cloudmanager"  
            version = "20.10.0"  
        }  
    }  
}
```

Read more on provider version control.

## Running Specific Modules

### AWS

Unresolved directive in automation/cloud\_volumes\_terraform.adoc -  
include::automation/cloud\_volumes\_aws.adoc[]

### Azure

Unresolved directive in automation/cloud\_volumes\_terraform.adoc -  
include::automation/cloud\_volumes\_azure.adoc[]

### GCP

Unresolved directive in automation/cloud\_volumes\_terraform.adoc -  
include::automation/cloud\_volumes\_gcp.adoc[]

# **NetApp Solutions Change Log**

Recent changes to the NetApp Solutions collateral. The most recent changes are listed first.

## All Changes

Date	Solution Area	Description of change
06/07/20 22	Hybrid Cloud	Updated AVS region support to match public preview announcement / support
06/07/20 22	Data Analytics	Added link to NetApp EF600 with Splunk Enterprise solution
06/02/20 22	Hybrid Cloud	Added list of region availability for NFS datastores for NetApp Hybrid Multi-Cloud with VMware
05/20/20 22	AI	New BeeGFS Design and Deployment guides for SuperPOD
04/01/20 22	Hybrid Cloud	Organized content of Enterprise Hybrid Cloud solutions: landing pages for each hyperscaler and inclusion of available solution (use case) content
03/29/20 22	Containers	Added a new TR: DevOps with NetApp Astra
03/08/20 22	Containers	Added a new video demo: Accelerate Software Development with Astra Control and NetApp FlexClone Technology
03/01/20 22	Containers	Added new sections to NVA-1160: Installation of Astra Control Center via OperatorHub and Ansible
02/02/20 22	General	Created landing pages to better organize content for AI and Modern Data Analytics
01/22/20 22	AI	Added TR: Data movement with E-Series and BeeGFS for AI and analytics workflows
12/21/20 21	General	Created landing pages to better organize content for Virtualization and Enterprise Hybrid Cloud
12/21/20 21	Containers	Added a new video demo: Leverage NetApp Astra Control to Perform Post-mortem Analysis and Restore Your Application to NVA-1160
12/06/20 21	Hybrid Cloud	Creation of Enterprise Hybrid Cloud (EHC) content for virtualization environment and guest connected storage options
11/15/20 21	Containers	Added a new video demo: Data Protection in CI/CD pipeline with Astra Control to NVA-1160
11/15/20 21	Modern Data Analytics	New content: Best Practices for Confluent Kafka
11/02/20 21	Automation	AWS Authentication Requirements for CVO and Connector Using NetApp Cloud Manager
10/29/20 21	Modern Data Analytics	New content: TR-4657 - NetApp hybrid cloud data solutions: Spark and Hadoop
10/29/20 21	Enterprise Database	Automated Data Protection for Oracle Databases
10/26/20 21	Enterprise Database	Added blog section for enterprise applications and database to NetApp solutions tile. Added two blogs to enterprise database blogs.

10/18/20 21	Enterprise Database	TR-4908 - Hybrid Cloud Database Solutions with SnapCenter
10/14/20 21	Virtualization	Added parts 1-4 of NetApp with VMware VCF blog series
10/04/20 21	Containers	Added a new video demo: Workload Migration using Astra Control Center to NVA-1160
09/23/20 21	Data Migration	New content: NetApp Best Practices for NetApp XCP
09/21/20 21	Virtualization	New content on ONTAP for VMware vSphere Administrators, VMware vSphere automation
09/09/20 21	Containers	Added F5 BIG-IP load balancer integration with OpenShift to NVA-1160
08/05/20 21	Containers	Added a new technology integration to NVA-1160 - NetApp Astra Control Center on Red Hat OpenShift
07/21/20 21	Enterprise Database	Automated Deployment of Oracle19c for ONTAP on NFS
07/02/20 21	Enterprise Database	TR-4897 - SQL Server on Azure NetApp Files: Real Deployment View
06/16/20 21	Containers	Added a new video demo, Installing OpenShift Virtualization: Red Hat OpenShift with NetApp
06/16/20 21	Containers	Added a new video demo, Deploying a Virtual Machine with OpenShift Virtualization: Red Hat OpenShift with NetApp
06/14/20 21	Enterprise Database	Added solution: Microsoft SQL Server on Azure NetApp Files
06/11/20 21	Containers	Added a new video demo: Workload Migration using Astra Trident and SnapMirror to NVA-1160
06/09/20 21	Containers	Added a new use-case to NVA-1160 - Advanced Cluster Management for Kubernetes on Red Hat OpenShift with NetApp
05/28/20 21	Containers	Added a new use-case to NVA-1160 - OpenShift Virtualization with NetApp ONTAP
05/27/20 21	Containers	Added a new use-case to NVA-1160- Multitenancy on OpenShift with NetApp ONTAP
05/26/20 21	Containers	Added NVA-1160 - Red Hat OpenShift with NetApp
05/25/20 21	Containers	Added blog: Installing NetApp Trident on Red Hat OpenShift – How to solve the Docker ‘toomanyrequests’ issue!
05/19/20 21	General	Added link to FlexPod solutions
05/19/20 21	AI	Converted AI Control Plane solution from PDF to HTML
05/17/20 21	General	Added Solution Feedback tile to main page

05/11/20 21	Enterprise Database	Added automated deployment of Oracle 19c for ONTAP on NFS
05/10/20 21	Virtualization	New video: How to use vVols with NetApp and VMware Tanzu Basic, part 3
05/06/20 21	Oracle Database	Added link to Oracle 19c RAC Databases on FlexPod DataCenter with Cisco UCS and NetApp AFF A800 over FC
05/05/20 21	Oracle Database	Added FlexPod Oracle NVA (1155) and Automation video
05/03/20 21	Desktop Virtualization	Added link to FlexPod Desktop Virtualization solutions
04/30/20 21	Virtualization	Video: How to use vVols with NetApp and VMware Tanzu Basic, part 2
04/26/20 21	Containers	Added blog: Using VMware Tanzu with ONTAP to accelerate your Kubernetes journey
04/06/20 21	General	Added "About this Repository"
03/31/20 21	AI	Added TR-4886 - AI Inferencing at the Edge: NetApp ONTAP with Lenovo ThinkSystem Solution Design
03/29/20 21	Modern Data Analytics	Added NVA-1157 - Apache Spark Workload with NetApp Storage Solution
03/23/20 21	Virtualization	Video: How to use vVols with NetApp and VMware Tanzu Basic, part 1
03/09/20 21	General	Added E-Series content; categorized AI content
03/04/20 21	Automation	New content: getting started with NetApp solution automation
02/18/20 21	Virtualization	Added TR-4597 - VMware vSphere for ONTAP
02/16/20 21	AI	Added automated deployment steps for AI Edge Inferencing
02/03/20 21	SAP	Added landing page for all SAP and SAP HANA content
02/01/20 21	Desktop Virtualization	VDI with NetApp VDS, Added content for GPU nodes
01/06/20 21	AI	New solution: NetApp ONTAP AI with NVIDIA DGX A100 Systems and Mellanox Spectrum Ethernet Switches (Design and Deployment)
12/22/20 20	General	Initial release of NetApp Solutions repository

## AI / Data Analytics

Date	Solution Area	Description of change
------	---------------	-----------------------

06/07/20 22	Data Analytics	Added link to NetApp EF600 with Splunk Enterprise solution
05/20/20 22	AI	New BeeGFS Design and Deployment guides for SuperPOD
02/02/20 22	General	Created landing pages to better organize content for AI and Modern Data Analytics
01/22/20 22	AI	Added TR: Data movement with E-Series and BeeGFS for AI and analytics workflows
11/15/20 21	Modern Data Analytics	New content: Best Practices for Confluent Kafka
10/29/20 21	Modern Data Analytics	New content: TR-4657 - NetApp hybrid cloud data solutions: Spark and Hadoop
05/19/20 21	AI	Converted AI Control Plane solution from PDF to HTML
03/31/20 21	AI	Added TR-4886 - AI Inferencing at the Edge: NetApp ONTAP with Lenovo ThinkSystem Solution Design
03/29/20 21	Modern Data Analytics	Added NVA-1157 - Apache Spark Workload with NetApp Storage Solution
02/16/20 21	AI	Added automated deployment steps for AI Edge Inferencing
01/06/20 21	AI	New solution: NetApp ONTAP AI with NVIDIA DGX A100 Systems and Mellanox Spectrum Ethernet Switches (Design and Deployment)

#### Hybrid Multi-Cloud

Date	Solution Area	Description of change
06/07/20 22	Hybrid Cloud	Updated AVS region support to match public preview announcement / support
06/02/20 22	Hybrid Cloud	Added list of region availability for NFS datastores for NetApp Hybrid Multi-Cloud with VMware
04/01/20 22	Hybrid Cloud	Organized content of Enterprise Hybrid Cloud solutions: landing pages for each hyperscaler and inclusion of available solution (use case) content
12/21/20 21	General	Created landing pages to better organize content for Virtualization and Enterprise Hybrid Cloud
12/06/20 21	Hybrid Cloud	Creation of Enterprise Hybrid Cloud (EHC) content for virtualization environment and guest connected storage options

#### Virtualization

Date	Solution Area	Description of change
04/01/20 22	Hybrid Cloud	Organized content of Enterprise Hybrid Cloud solutions: landing pages for each hyperscaler and inclusion of available solution (use case) content

12/21/20 21	General	Created landing pages to better organize content for Virtualization and Enterprise Hybrid Cloud
10/14/20 21	Virtualization	Added parts 1-4 of NetApp with VMware VCF blog series
09/21/20 21	Virtualization	New content on ONTAP for VMware vSphere Administrators, VMware vSphere automation
05/10/20 21	Virtualization	New video: How to use vVols with NetApp and VMware Tanzu Basic, part 3
05/03/20 21	Desktop Virtualization	Added link to FlexPod Desktop Virtualization solutions
04/30/20 21	Virtualization	Video: How to use vVols with NetApp and VMware Tanzu Basic, part 2
04/26/20 21	Containers	Added blog: Using VMware Tanzu with ONTAP to accelerate your Kubernetes journey
03/23/20 21	Virtualization	Video: How to use vVols with NetApp and VMware Tanzu Basic, part 1
02/18/20 21	Virtualization	Added TR-4597 - VMware vSphere for ONTAP
02/01/20 21	Desktop Virtualization	VDI with NetApp VDS, Added content for GPU nodes

## Containers

Date	Solution Area	Description of change
03/29/20 22	Containers	Added a new TR: DevOps with NetApp Astra
03/08/20 22	Containers	Added a new video demo: Accelerate Software Development with Astra Control and NetApp FlexClone Technology
03/01/20 22	Containers	Added new sections to NVA-1160: Installation of Astra Control Center via OperatorHub and Ansible
12/21/20 21	Containers	Added a new video demo: Leverage NetApp Astra Control to Perform Post-mortem Analysis and Restore Your Application to NVA-1160
11/15/20 21	Containers	Added a new video demo: Data Protection in CI/CD pipeline with Astra Control to NVA-1160
10/04/20 21	Containers	Added a new video demo: Workload Migration using Astra Control Center to NVA-1160
09/09/20 21	Containers	Added F5 BIG-IP load balancer integration with OpenShift to NVA-1160
08/05/20 21	Containers	Added a new technology integration to NVA-1160 - NetApp Astra Control Center on Red Hat OpenShift
06/16/20 21	Containers	Added a new video demo, Installing OpenShift Virtualization: Red Hat OpenShift with NetApp

06/16/20 21	Containers	Added a new video demo, Deploying a Virtual Machine with OpenShift Virtualization: Red Hat OpenShift with NetApp
06/11/20 21	Containers	Added a new video demo: Workload Migration using Astra Trident and SnapMirror to NVA-1160
06/09/20 21	Containers	Added a new use-case to NVA-1160 - Advanced Cluster Management for Kubernetes on Red Hat OpenShift with NetApp
05/28/20 21	Containers	Added a new use-case to NVA-1160 - OpenShift Virtualization with NetApp ONTAP
05/27/20 21	Containers	Added a new use-case to NVA-1160- Multitenancy on OpenShift with NetApp ONTAP
05/26/20 21	Containers	Added NVA-1160 - Red Hat OpenShift with NetApp
05/25/20 21	Containers	Added blog: Installing NetApp Trident on Red Hat OpenShift – How to solve the Docker ‘toomanyrequests’ issue!
05/10/20 21	Virtualization	New video: How to use vVols with NetApp and VMware Tanzu Basic, part 3
04/30/20 21	Virtualization	Video: How to use vVols with NetApp and VMware Tanzu Basic, part 2
04/26/20 21	Containers	Added blog: Using VMware Tanzu with ONTAP to accelerate your Kubernetes journey
03/23/20 21	Virtualization	Video: How to use vVols with NetApp and VMware Tanzu Basic, part 1

## Enterprise Apps and DB

Date	Solution Area	Description of change
10/29/20 21	Enterprise Database	Automated Data Protection for Oracle Databases
10/26/20 21	Enterprise Database	Added blog section for enterprise applications and database to NetApp solutions tile. Added two blogs to enterprise database blogs.
10/18/20 21	Enterprise Database	TR-4908 - Hybrid Cloud Database Solutions with SnapCenter
07/21/20 21	Enterprise Database	Automated Deployment of Oracle19c for ONTAP on NFS
07/02/20 21	Enterprise Database	TR-4897 - SQL Server on Azure NetApp Files: Real Deployment View
06/14/20 21	Enterprise Database	Added solution: Microsoft SQL Server on Azure NetApp Files
05/11/20 21	Enterprise Database	Added automated deployment of Oracle 19c for ONTAP on NFS
05/06/20 21	Oracle Database	Added link to Oracle 19c RAC Databases on FlexPod DataCenter with Cisco UCS and NetApp AFF A800 over FC

05/05/20 21	Oracle Database	Added FlexPod Oracle NVA (1155) and Automation video
02/03/20 21	SAP	Added landing page for all SAP and SAP HANA content



For more information on SAP and SAP HANA updates, refer to the "Update History" content present for each of the solutions in the [SAP Solutions Repository](#).

#### Data Protection and Data Migration

Date	Solution Area	Description of change
10/29/2021	Enterprise Database	Automated Data Protection for Oracle Databases
09/23/2021	Data Migration	New content: NetApp Best Practices for NetApp XCP

#### Solution Automation

Date	Solution Area	Description of change
11/02/20 21	Automation	AWS Authentication Requirements for CVO and Connector Using NetApp Cloud Manager
10/29/20 21	Enterprise Database	Automated Data Protection for Oracle Databases
07/21/20 21	Enterprise Database	Automated Deployment of Oracle19c for ONTAP on NFS
05/11/20 21	Enterprise Database	Added automated deployment of Oracle 19c for ONTAP on NFS
03/04/20 21	Automation	New content: getting started with NetApp solution automation

# About this Repository

Brief introduction of the NetApp Solutions repository - where to find specific solutions and how to use this repository.

## Navigation of the Repository

Navigation of the repository is managed by the main sidebar which is presented on the left side of the page. Solutions are categorized into higher level technical areas defined as the "technology towers" for NetApp Solutions.

### Overview of Technology Towers

Section	Description	Content Landing Page
Artificial Intelligence	Collection of AI based solutions. The AI landing page offers popular content presented in content specific "tiles".	<a href="#">AI content</a>
Modern Data Analytics	Collection of Modern Data Analytics solutions (e.g. Splunk SmartStore, Apache Spark, etc.). The Modern Data Analytics landing page offers popular content presented in content specific "tiles".	<a href="#">Modern Data Analytics content</a>
Hybrid Multi-Cloud with VMware	Defines NetApp in a hybrid multi-cloud model - including VMware in the Public Cloud and NetApp Storage options in each of the hyperscalers. The hybrid multi-cloud landing page offers popular content presented in content specific "tiles".	<a href="#">Hybrid Multi-Cloud with VMware content</a>
Virtualization	Collection of virtualization core solutions, including desktop virtualization. The Virtualization landing page offers popular content presented in content specific "tiles".	<a href="#">Virtualization content</a>
Containers	Collection of container based solutions. The Virtualization landing page offers popular content presented in content specific "tiles".	<a href="#">Containers content</a>
Business Applications and Databases	Collection of business applications and database solutions. The SAP and SAP HANA landing page offers popular content presented in content specific "tiles". Oracle and SQL Server database solutions are also covered in this section.	<a href="#">SAP and SAP HANA content</a>
Data Migration and Data Protection	Collection of data migration, data protection and data security solutions.	
Solution Automation	Overview of getting started with solution automation using Red Hat Ansible.	

## Change Log

All major changes to the repository (new solutions, major updates, new videos / demos, etc.) are tracked in the [change log](#).

# **Feedback**

Please use [this link](#) to request changes to content or provide feedback on the content. Please be as specific as possible to ensure that your feedback is addressed appropriately.

# **Legal notices**

Legal notices provide access to copyright statements, trademarks, patents, and more.

## **Copyright**

<http://www.netapp.com/us/legal/copyright.aspx>

## **Trademarks**

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## **Patents**

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/us/media/patents-page.pdf>

## **Privacy policy**

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## **Open source**

Notice files provide information about third-party copyright and licenses used in NetApp software.

## **Copyright Information**

Copyright © 2022 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## **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.