



NetApp Verified Architecture

NetApp HCI with Anthos

NVA Design/Deployment

Alan Cowles, NetApp

November 2019 | NVA-1141 | Version 1.0

Abstract

NetApp HCI with Anthos is a verified, best-practice hybrid cloud architecture for the deployment of an on-premises Google Kubernetes Engine environment in a reliable and dependable manner. This architecture reference document provides design and deployment validation of the Anthos solution on NetApp HCI and a use-case validation of the deployment.

In partnership with



TABLE OF CONTENTS

1	Program Summary.....	4
1.1	NetApp Verified Architecture.....	4
1.2	NetApp HCI Design	4
2	Solution Overview	5
2.1	NetApp HCI.....	5
2.1.1	NetApp Element Software.....	6
2.2	Anthos.....	8
3	Networking Requirements	10
3.1	Port Identification	10
3.2	Network Design.....	11
3.3	VLAN Requirements	12
3.4	Network Infrastructure Support Resources	13
4	Anthos for NetApp HCI Requirements	13
4.1	Hardware Requirements	13
4.2	Software Requirements	13
5	Deployment Procedures	14
5.1	Configure Management Switches	14
5.2	Configure Data Switches	16
5.3	Deploy NetApp HCI with the NetApp Deployment Engine	19
5.4	Configure the vCenter Server	29
5.5	Deploy and Configure the F5 Big-IP Virtual Edition Appliance.....	35
5.6	Complete Anthos Prerequisites.....	45
5.7	Deploy the Anthos Admin Workstation.....	48
5.8	Deploy the Admin and the First User Cluster	53
5.9	Deploy Additional User Clusters	60
5.10	Enable Access to the Cluster with the GKE Console	63
5.11	Install and Configure NetApp Trident Storage Provisioner.....	65
6	Best Practices	68
6.1	Install a Second F5 Big-IP Virtual Edition Appliance	68
6.2	Enable VMware vSphere DRS and Configure Anti-Affinity Rules	68
6.3	Leverage SnapMirror to Copy Data Remotely for Disaster Recovery	68
7	Conclusion	68

Where to Find Additional Information	69
Version History	69

LIST OF TABLES

Table 1) VLANs required.	12
Table 2) Hardware requirements.	13
Table 3) Software requirements.	13
Table 4) Google Cloud Service Accounts.	47

LIST OF FIGURES

Figure 1) NetApp HCI minimum configuration.	5
Figure 2) Anthos Architecture.	9
Figure 3) NetApp HCI network ports (compute node).	11
Figure 4) Network cabling reference diagram.	12
Figure 5) Non-whitelisted view.	63
Figure 6) View of clusters.	63

1 Program Summary

1.1 NetApp Verified Architecture

NetApp HCI with Anthos 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 architecture reference document serves as both a design guide and a deployment validation of the Anthos solution on NetApp HCI. The architecture described in this document has been validated by subject matter experts at NetApp and Google to provide the advantage of running Anthos on NetApp HCI within your own enterprise data-center environment.

NetApp HCI, is the industry's first and leading disaggregated hybrid cloud infrastructure, providing the widely recognized benefits of hyperconverged solutions. Benefits include lower TCO and ease of acquisition, deployment, and management for virtualized workloads, while also allowing enterprise customers to independently scale compute and storage resources as needed. NetApp HCI with Anthos provides an on-premises, cloud-like experience for the deployment of containerized workloads managed by Anthos GKE on-premises. This solution provides simplified management, detailed metrics, and a range of additional functionalities that enable the easy movement of workloads deployed both on-site and in the cloud.

1.2 NetApp HCI Design

By providing an agile turnkey infrastructure platform, NetApp HCI enables you to run enterprise-class virtualized and containerized workloads in an accelerated manner. At its core, NetApp HCI is designed to provide predictable performance, linear scalability of both compute and storage resources, and a simple deployment and management experience.

Predictable

One of the biggest challenges in a multitenant environment is delivering consistent, predictable performance for all your workloads. Running multiple enterprise-grade workloads can result in resource contention, in which one workload might interfere with the performance of another. NetApp HCI alleviates this concern with storage quality-of-service (QoS) limits that are available natively with NetApp Element[®] software. Element enables the granular control of every application and volume, helps to eliminate noisy neighbors, and satisfies enterprise performance SLAs. NetApp HCI multitenancy capabilities can help eliminate many traditional performance-related problems.

Flexible

Previous generations of hyperconverged infrastructures often required fixed resource ratios, limiting deployments to four-node and eight-node configurations. NetApp HCI is a disaggregated hyperconverged infrastructure that can scale compute and storage resources independently. Independent scaling prevents costly and inefficient overprovisioning, eliminates the 10% to 30% HCI tax from controller VM overhead, and simplifies capacity and performance planning. NetApp HCI is available in mix-and-match small, medium, and large storage and compute configurations.

The architectural design choices offered enable you to confidently scale on your terms, making HCI viable for core Tier 1 data center applications and platforms. NetApp HCI is architected in building blocks at either the chassis or the node level. Each chassis can hold four nodes in a mixed configuration of storage or compute nodes.

Simple

A driving imperative within the IT community is to simplify deployment and automate routine tasks, eliminating the risk of user error while freeing up resources to focus on more interesting, higher-value projects. NetApp HCI can help your IT department become more agile and responsive by both simplifying

deployment and ongoing management. The NetApp Deployment Engine (NDE) tool eases the configuration and deployment of physical infrastructure, including the installation of the VMware vSphere environment and the integration of the NetApp Element Plug-in for vCenter Server. With NDE, future scaling operations can be performed without difficulty.

2 Solution Overview

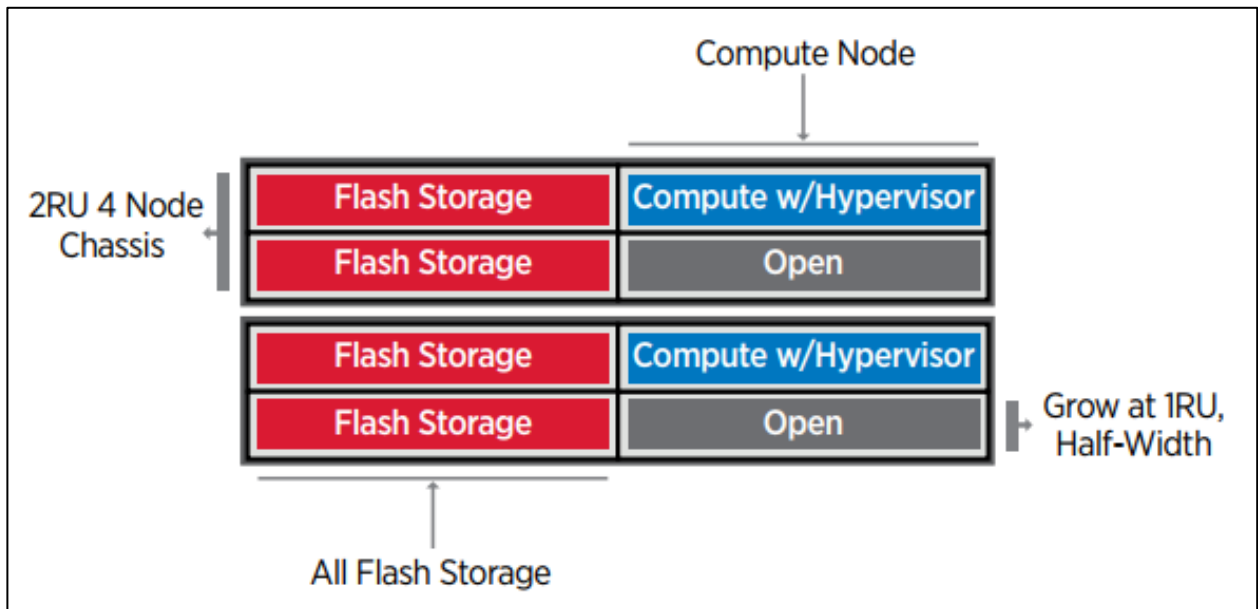
With NetApp HCI for Anthos, you can deploy a fully integrated, production-grade Anthos GKE environment in your on-premises data center, which allows you to take advantage of the following features:

- NetApp HCI compute and storage nodes
 - Enterprise-grade hyperconverged infrastructure designed for hybrid cloud workloads
 - NetApp Element storage software
 - Intel-based server compute nodes, including options for Nvidia GPUs
- VMware vSphere 6.5
 - Enterprise hypervisor solution for deployment and management of virtual infrastructures
- Anthos GKE in Google Cloud and On-Prem
 - Deploy Anthos GKE instances in Google Cloud or on NetApp HCI

2.1 NetApp HCI

NetApp HCI is an enterprise-scale disaggregated hybrid cloud infrastructure (HCI) solution that delivers compute and storage resources in an agile, scalable, and easy-to-manage two-rack unit (2RU) four-node building block. It can also be configured with 1RU compute and server nodes. The minimum deployment depicted in Figure 1 consists of four NetApp HCI storage nodes and two NetApp HCI compute nodes. The compute nodes are installed as VMware ESXi hypervisors in an HA cluster without the enforcement of VMware DRS anti-affinity rules. This minimum deployment can be easily scaled to fit customer enterprise workload demands by adding additional NetApp HCI storage or compute nodes to expand available storage.

Figure 1) NetApp HCI minimum configuration.



The design for NetApp HCI for Anthos consists of the following components in a minimum starting configuration:

- NetApp H-Series all-flash storage nodes running NetApp Element software
- NetApp H-Series compute nodes running VMware vSphere 6.5U2

For more information about compute and storage nodes in NetApp HCI, see the [NetApp HCI Datasheet](#).

2.1.1 NetApp Element Software

NetApp Element software provides modular, scalable performance, with each storage node delivering guaranteed capacity and throughput to the environment. You can also specify per-volume storage QoS policies to support dedicated performance levels for even the most demanding workloads.

iSCSI Login Redirection and Self-Healing Capabilities

NetApp Element software uses the iSCSI storage protocol, a standard way to encapsulate SCSI commands on a traditional TCP/IP network. When SCSI standards change or when Ethernet network performance 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 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 specific 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.
- **VPN routing/forwarding (VFR)-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 service provider environments where scale and preservation of IP-space 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 Element 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.

Note: Element was designed for automation. All the storage features mentioned above can be managed with APIs. These APIs are the only method that the UI uses to control the system whether actions are performed directly through Element or through the vSphere plug-in for Element.

VMware vSphere

VMware vSphere is the industry leading virtualization solution built on VMware ESXi hypervisors and managed by vCenter Server, which provides advanced functionality often required for enterprise datacenters. When using the NDE with NetApp HCI, a VMware vSphere environment is configured and installed. The following features are available after the environment is deployed:

- **Centralized Management.** Through vSphere, individual hypervisors can be grouped into data centers and combined into clusters, allowing for advanced organization to ease the overall management of resources.

- **VMware HA.** This feature allows virtual guests to restart automatically if their host becomes unavailable. By enabling this feature, virtual guests become fault tolerant, and virtual infrastructures experience minimal disruption when there are physical failures in the environment.
- **VMware Distributed Resource Scheduler (DRS).** VMware vMotion allows for the movement of guests between hosts nondisruptively when certain user-defined thresholds are met. This capability makes the virtual guests in an environment highly available.
- **vSphere Distributed Switch (vDS).** A virtual switch is controlled by the vCenter server, enabling centralized configuration and management of connectivity for each host by creating port groups that map to the physical interfaces on each host.

2.2 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.

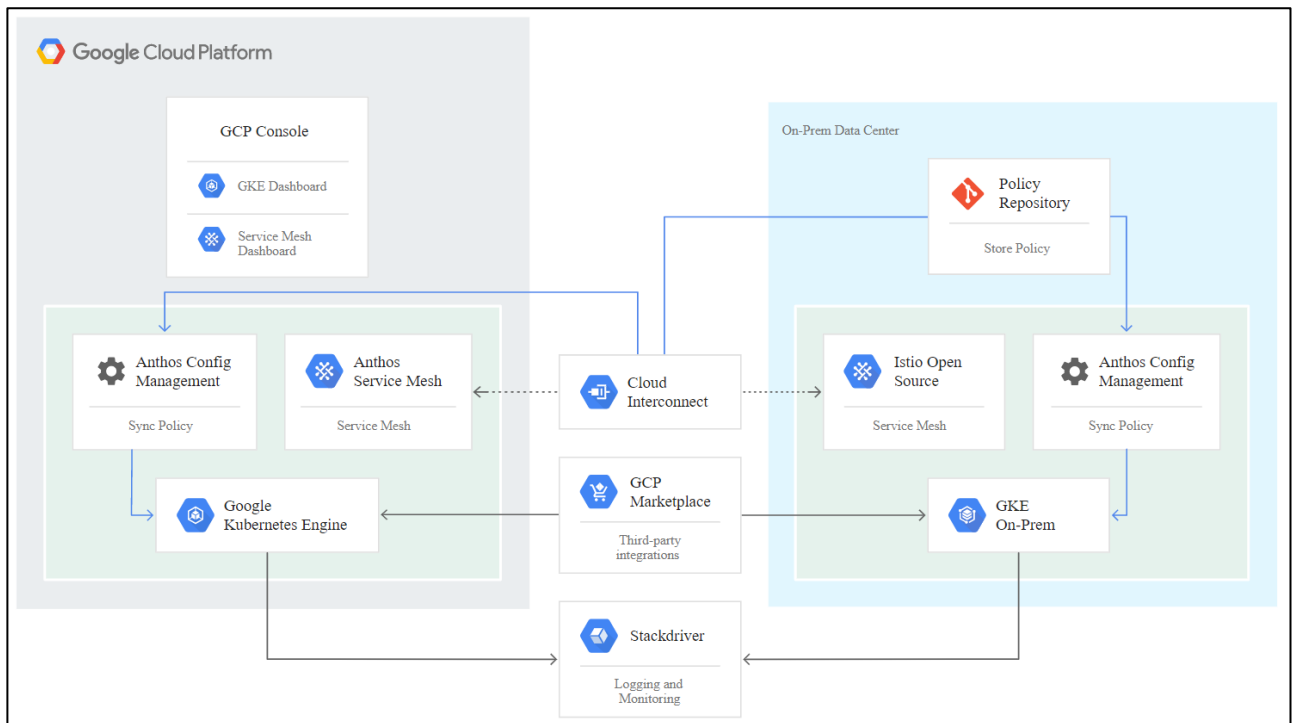
Adopting containers, service mesh, and other transformational technologies enables organizations to experience consistent application development cycles and production-ready workloads in local and cloud-based environments. Figure 2 depicts the Anthos solution and how a deployment in an on-premises data 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.

Figure 2) Anthos Architecture.



Containers and Kubernetes Orchestration

Container technology has been available to developers for a long time. However, it has only recently become a core concept in data center architecture and design as more enterprises have adopted application-specific workload requirements.

A traditional development environment requires a dedicated development host deployed on either a bare-metal or virtual server. Such environments require each application to have its own dedicated machine, complete with operating system (OS) and networking connectivity. These machines often must be managed by the enterprise system administration team, who must account for the application versions installed as well as host OS patches. In contrast, containers by design require less overhead to deploy. All that is needed is the packaging of application code and supporting libraries together, because all other services depend on the host OS. Rather than managing a complete virtual machine (VM) environment, developers can instead focus on the application development process.

As container technology began to find appeal in the enterprise landscape, many enterprise features, such as fault tolerance and application scaling, were both requested and expected. In response, Google partnered with the Linux Foundation to form the Cloud Native Computing Foundation (CNCF). Together, they introduced Kubernetes (K8s), an open-source platform for orchestrating and managing containers. Kubernetes was designed by Google to be a successor to both the Omega and Borg container management platforms that had been used in their data centers in the previous decade.

Anthos GKE

Anthos GKE is a certified distribution of Kubernetes in the Google Cloud. It allows end users to easily deploy managed, production-ready Kubernetes clusters, enabling developers to focus primarily on application development rather than on the management of their environment. Deploying Kubernetes clusters in Anthos GKE offers the following benefits:

- **Simplifying Deployment of Applications.** Anthos GKE allows for rapid development, deployment, and updates of applications and services. By providing simple descriptions of the expected system resources (compute, memory, and storage) required by the application containers, the Kubernetes Engine automatically provisions and manages the lifecycle of the cluster environment.
- **Ensuring Availability of Clusters.** The environment is made extremely accessible and easy to manage by using the dashboard built into the Google Cloud console. Anthos GKE clusters are continually monitored by Google Site Reliability Engineers (SREs) to make sure that clusters behave as expected by collecting regular metrics and observing the use of assigned system resources. A user can also leverage available health checks to make sure that their deployed applications are highly available and that they can recover easily should something go awry.
- **Securing Clusters in Google Cloud.** An end user can ensure that clusters are secure and accessible by customizing network policies available from Google Cloud's Global Virtual Private Cloud. Public services can be placed behind a single global IP address for load balancing purposes. A single IP can help provide high availability for applications and protect against Distributed Denial of Service (DDOS) and other forms of attacks that might hinder service performance.
- **Easily Scaling to Meet Requirements.** An end user can enable auto-scaling on their cluster to easily counter both planned and unexpected increases in application demands. Auto-scaling helps make sure that system resources are always available by increasing capacity during high-demand windows. It also allows the cluster to return to its previous state and size after peak demand wanes.

Anthos on VMware

Anthos 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 on VMware offers the following benefits:

- **Cost Savings.** End users can realize significant cost savings by utilizing their own physical resources for their application deployments instead of provisioning resources in their Google Cloud environment.
- **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.

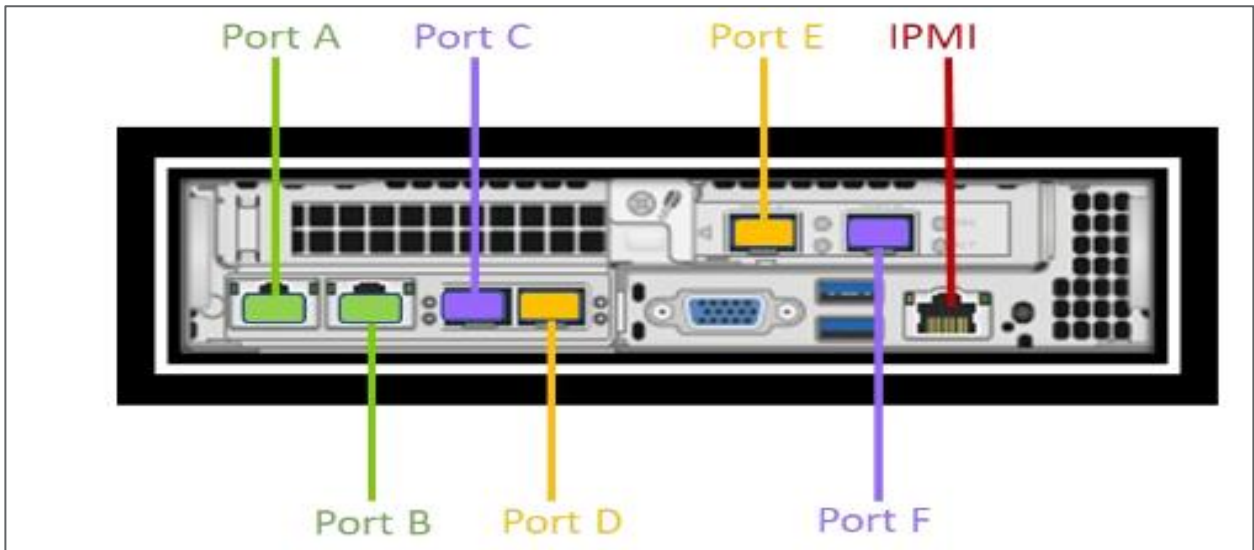
3 Networking Requirements

This section describes the networking requirements for the deployment of Anthos on NetApp HCI as a validated solution. It provides physical diagrams of the network ports on both the NetApp HCI compute nodes and the switches deployed in the solution. This section also describes the arrangement and purpose of each virtual network segment used in the solution.

3.1 Port Identification

NetApp HCI consists of NetApp H-Series nodes dedicated to either compute or storage. Both node configurations are available with two 1GbE ports (ports A and B) and two 10/25 GbE ports (ports C and D) on board. The compute nodes have additional 10/25GbE ports (ports E and F) available in the first mezzanine slot. Each node also has an additional out-of-band management port that supports Intelligent Platform Management Interface (IPMI) functionality. Figure 3 identifies each of these ports on the rear of an H410C node.

Figure 3) NetApp HCI network ports (compute node).



3.2 Network Design

The NetApp HCI with Anthos 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.

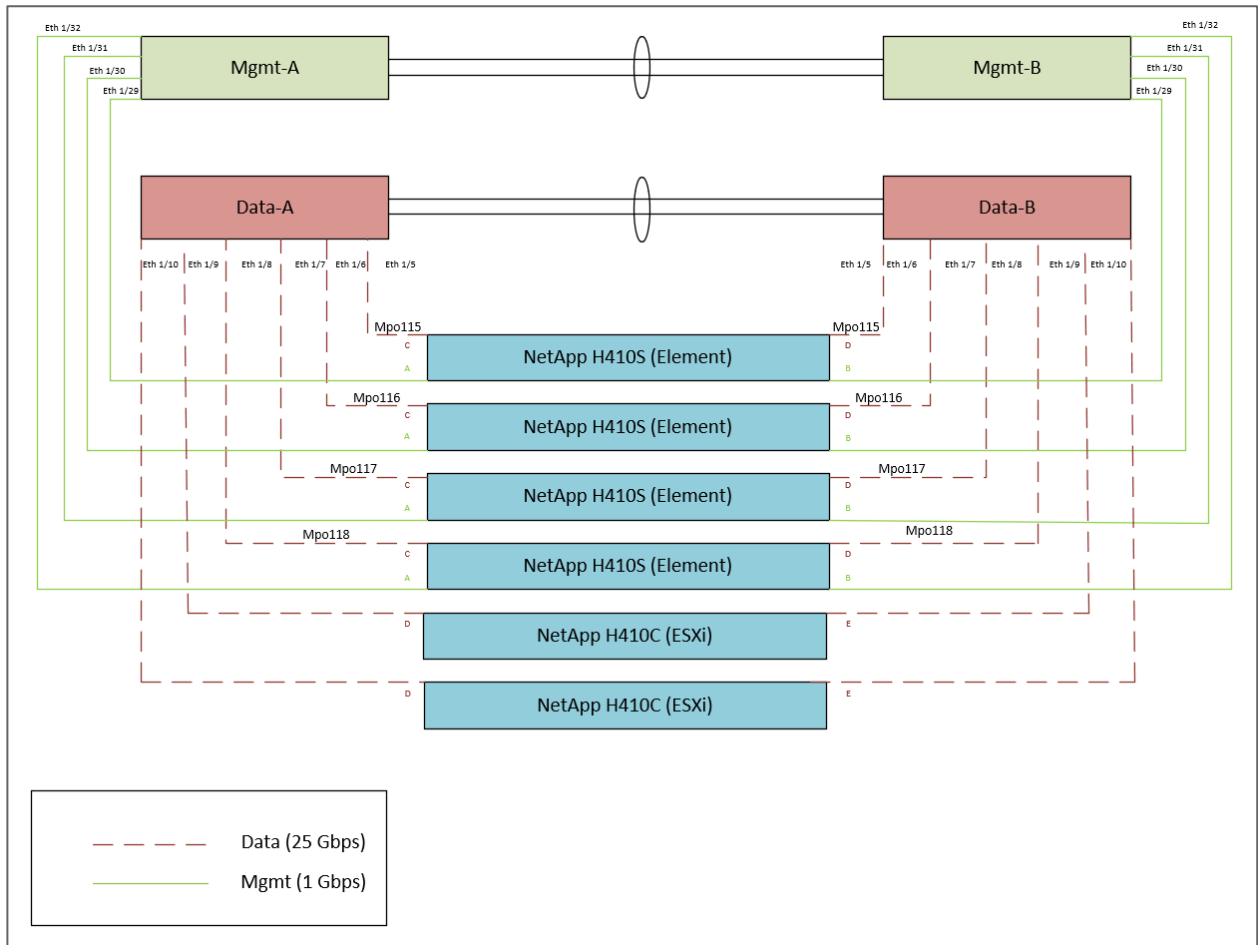
Cabling Storage Nodes

The management ports A and B must be active on each storage node to run NDE, configure the NetApp HCI cluster, and provide management accessibility to Element after the solution is deployed. The two 25Gbps ports (C and D) should be connected, one to each data switch, to provide physical fault tolerance. The switch ports should be configured for multi-chassis link aggregation (MLAG) and the data ports on the node should be configured for LACP with jumbo-frames support enabled. The IPMI ports on each node can be used to remotely manage the node after it is installed in a data center. With IPMI, the node can be accessed with a web-browser-based console to run the initial installation, run diagnostics, and reboot or shut down the node if necessary.

Cabling Compute Nodes

The 25Gbps ports on the compute nodes are cabled with one onboard port (C) cabled to one data switch, and an additional port from the PCI slot (E) cabled to the second switch to provide physical fault tolerance. These ports should be configured to support jumbo frames. Connectivity for the node is managed by the vDS after VMware vSphere is deployed in the environment. The IPMI ports can also be used to remotely manage the node after it is installed in a data center. With IPMI, the node can be accessed via a web-browser-based console to run diagnostics and to be rebooted or shut down if necessary.

Figure 4) Network cabling reference diagram.



3.3 VLAN Requirements

The solution is designed to logically separate network traffic for different purposes by using Virtual Local Area Networks (VLANs). NetApp HCI requires a minimum of three network segments. However, this configuration can be scaled to meet customer demands or to provide further isolation for specific network services. Table 2 lists the VLANs that are required to implement the solution, as well as the specific VLAN IDs that are used later in the validated architecture deployment.

Table 1) VLANs required.

VLANs	Purpose	VLAN Used
Out-of-band management	Management for HCI nodes	16
In-band management	Management for HCI nodes and infrastructure virtual guests.	3480
Storage network	Storage network for NetApp Element.	3481
vMotion network	Network for VMware vMotion.	3482
VM network	Network for virtual guests	1172

3.4 Network Infrastructure Support Resources

The following infrastructure should be in place prior to the deployment of the Anthos on NetApp HCI solution:

- A DHCP server providing addresses for both the in-band management network and the VM network. The DHCP pool must be large enough to support at least 10 VMs for an initial deployment and should be scaled as necessary.
- 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.
- Outbound internet connectivity for both the in-band management network and the VM network.

4 Anthos for NetApp HCI Requirements

4.1 Hardware Requirements

Table 2 lists the minimum number of hardware components that are required to implement the solution. The hardware components that are used in specific implementations of the solution might vary based on customer requirements.

Table 2) Hardware requirements.

Hardware	Model	Quantity
NetApp HCI compute nodes	NetApp H410C	2
NetApp HCI storage nodes	NetApp H410S	4
Data switches	Cisco Nexus 3048	2
Management switches	Mellanox SN2010	2

4.2 Software Requirements

Table 3 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.

Table 3) Software requirements.

Software	Purpose	Version
NetApp HCI	Infrastructure (compute/storage)	1.6P1
VMware vSphere	Virtualization	6.5U2
Anthos on VMware	Container orchestration	1.1
F5 Big-IP Virtual Edition	Load balancing	15.0.1
HashiCorp Terraform	Automation and provisioning	0.12.12
NetApp Trident	Storage management	19.10

5 Deployment Procedures

Deploying Anthos for NetApp HCI involves the following tasks:

1. Configure Management Switches
2. Configure Data Switches
3. Deploy NetApp HCI with the NetApp Deployment Engine
4. Configure the vCenter Server
5. Deploy and Configure the F5 Big-IP Virtual Edition Appliance
6. Complete Anthos Prerequisites
7. Deploy the Anthos Admin Workstation
8. Deploy the Admin and the First User Cluster
9. Deploy Additional User Clusters
10. Enable Access to the Cluster with the GKE Console
11. Install and Configure NetApp Trident Storage Provisioner

5.1 Configure Management Switches

Cisco Nexus 3048 switches are used in this deployment procedure to provide 1Gbps connectivity for in and out-of-band management of the compute and storage nodes. These steps begin after the switches have been racked, powered, and put through the initial setup process. To configure the switches to provide management connectivity to the infrastructure, complete the following steps:

Enable Advanced Features for Cisco Nexus

Run the following commands on each Cisco Nexus 3048 switch to configure advanced features:

1. Enter configuration mode.

```
Switch-01# configure terminal
```

2. Enable VLAN functionality.

```
Switch-01(config)# feature interface-vlan
```

3. Enable LACP.

```
Switch-01(config)# feature lacp
```

4. Enable virtual port channels (vPCs).

```
Switch-01(config)# feature vpc
```

5. Set the global port-channel load-balancing configuration.

```
Switch-01(config)# port-channel load-balance src-dst ip-l4port
```

6. Perform the global spanning-tree configuration.

```
Switch-01(config)# spanning-tree port type network default  
Switch-01(config)# spanning-tree port type edge bpduguard default
```

Configure Ports on the Switch for In-Band Management

1. Run the following commands to create VLANs for management purposes.

```
Switch-01(config)# vlan 2  
Switch-01(config-vlan)# Name Native_VLAN  
Switch-01(config-vlan)# vlan 16  
Switch-01(config-vlan)# Name OOB_Network  
Switch-01(config-vlan)# vlan 3480
```

```
Switch-01(config-vlan)# Name MGMT_Network
Switch-01(config-vlan)# exit
```

2. Configure the ports ETH1/29-32 as VLAN trunk ports that connect to management interfaces on each HCI storage node.

```
Switch-01(config)# int eth 1/29
Switch-01(config-if)# description HCI-STG-01 PortA
Switch-01(config-if)# switchport mode trunk
Switch-01(config-if)# switchport trunk native vlan 2
Switch-01(config-if)# switchport trunk allowed vlan 3480
Switch-01(config-if)# spanning tree port type edge trunk
Switch-01(config-if)# int eth 1/30
Switch-01(config-if)# description HCI-STG-02 PortA
Switch-01(config-if)# switchport mode trunk
Switch-01(config-if)# switchport trunk native vlan 2
Switch-01(config-if)# switchport trunk allowed vlan 3480
Switch-01(config-if)# spanning tree port type edge trunk
Switch-01(config-if)# int eth 1/31
Switch-01(config-if)# description HCI-STG-03 PortA
Switch-01(config-if)# switchport mode trunk
Switch-01(config-if)# switchport trunk native vlan 2
Switch-01(config-if)# switchport trunk allowed vlan 3480
Switch-01(config-if)# spanning tree port type edge trunk
Switch-01(config-if)# int eth 1/32
Switch-01(config-if)# description HCI-STG-04 PortA
Switch-01(config-if)# switchport mode trunk
Switch-01(config-if)# switchport trunk native vlan 2
Switch-01(config-if)# switchport trunk allowed vlan 3480
Switch-01(config-if)# spanning tree port type edge trunk
Switch-01(config-if)# exit
```

Configure Ports on the Switch for Out-of-Band Management

Run the following commands to configure the ports for cabling the IPMI interfaces on each HCI node.

```
Switch-01(config)# int eth 1/13
Switch-01(config-if)# description HCI-CMP-01 IPMI
Switch-01(config-if)# switchport mode access
Switch-01(config-if)# switchport access vlan 16
Switch-01(config-if)# spanning-tree port type edge
Switch-01(config-if)# int eth 1/14
Switch-01(config-if)# description HCI-STG-01 IPMI
Switch-01(config-if)# switchport mode access
Switch-01(config-if)# switchport access vlan 16
Switch-01(config-if)# spanning-tree port type edge
Switch-01(config-if)# int eth 1/15
Switch-01(config-if)# description HCI-STG-03 IPMI
Switch-01(config-if)# switchport mode access
Switch-01(config-if)# switchport access vlan 16
Switch-01(config-if)# spanning-tree port type edge
Switch-01(config-if)# exit
```

Note: In the validated configuration, we cabled odd-node IPMI interfaces to Switch-01, and even-node IPMI interfaces to Switch-02.

Create a vPC Domain to Ensure Fault Tolerance

1. Activate the ports used for the vPC peer-link between the two switches.

```
Switch-01(config)# int eth 1/1
Switch-01(config-if)# description vPC peer-link Switch-02 1/1
Switch-01(config-if)# int eth 1/2
Switch-01(config-if)# description vPC peer-link Switch-02 1/2
Switch-01(config-if)# exit
```

2. Perform the vPC global configuration.

```
Switch-01(config)# vpc domain 1
```

```
Switch-01(config-vpc-domain)# role priority 10
Switch-01(config-vpc-domain)# peer-keepalive destination <switch-02_mgmt_address> source <switch-01_mgmt_address> vrf management
Switch-01(config-vpc-domain)# peer-gateway
Switch-01(config-vpc-domain)# auto recovery
Switch-01(config-vpc-domain)# ip arp synchronize
Switch-01(config-vpc-domain)# int eth 1/1-2
Switch-01(config-vpc-domain)# channel-group 10 mode active
Switch-01(config-vpc-domain)# int Po10
Switch-01(config-if)# description vPC peer-link
Switch-01(config-if)# switchport mode trunk
Switch-01(config-if)# switchport trunk native vlan 2
Switch-01(config-if)# switchport trunk allowed vlan 16,3480
Switch-01(config-if)# spanning-tree port type network
Switch-01(config-if)# vpc peer-link
Switch-01(config-if)# exit
```

5.2 Configure Data Switches

Mellanox SN2010 switches are used in this deployment procedure to provide 25Gbps connectivity for the data plane of the compute and storage nodes. These steps begin after the switches have been racked, cabled, and put through the initial setup process. To configure the switches to provide data connectivity to the infrastructure, complete the following steps:

Create MLAG Cluster to Ensure Fault Tolerance

1. Run the following commands on each Mellanox SN210 switch for general configuration:

- a. Enter configuration mode.

```
Switch-01 enable
Switch-01 configure terminal
```

- b. Enable the LACP required for the Inter-Peer Link (IPL).

```
Switch-01 (config) # lacp
```

- c. Enable the Link Layer Discovery Protocol (LLDP).

```
Switch-01 (config) # lldp
```

- d. Enable IP routing.

```
Switch-01 (config) # ip routing
```

- e. Enable the MLAG protocol.

```
Switch-01 (config) # protocol mlag
```

- f. Enable global QoS.

```
Switch-01 (config) # dcb priority-flow-control enable force
```

2. For MLAG to function, the switches must be made peers to each other through an IPL. This should consist of two or more physical links for redundancy. The MTU for the IPL is set for jumbo frames (9216), and all VLANs are enabled by default. Run the following commands on each switch in the domain:

- a. Create port channel 10 for the IPL.

```
Switch-01 (config) # interface port-channel 10
Switch-01 (config interface port-channel 10) # description IPL
Switch-01 (config interface port-channel 10) # exit
```

- b. Add interfaces ETH 1/20 and 1/22 to the port channel.

```
Switch-01 (config) # interface ethernet 1/20 channel-group 10 mode active
Switch-01 (config) # interface ethernet 1/20 description ISL-SWB_01
Switch-01 (config) # interface ethernet 1/22 channel-group 10 mode active
```



```
Switch-01 (config) # interface ethernet 1/22 description ISL-SWB_02
```

- c. Create a VLAN outside of the standard range dedicated to IPL traffic.

```
Switch-01 (config) # vlan 4000
Switch-01 (config vlan 4000) # name IPL VLAN
Switch-01 (config vlan 4000) # exit
```

- d. Define the port channel as the IPL.

```
Switch-01 (config) # interface port-channel 10 ipl 1
Switch-01 (config) # interface port-channel 10 dcb priority-flow-control mode on force
```

- e. Set an IP for each IPL member (non-routable; it is not advertised outside of the switch).

```
Switch-01 (config) # interface vlan 4000
Switch-01 (config vlan 4000) # ip address 10.0.0.1 255.255.255.0
Switch-01 (config vlan 4000) # ipl 1 peer-address 10.0.0.2
Switch-01 (config vlan 4000) # exit
```

3. Create a unique MLAG domain name for the two switches and assign a MLAG virtual IP (VIP). This IP is used for keep-alive heartbeat messages between the two switches. Run these commands on each switch in the domain:

- a. Create the MLAG domain and set the IP address and subnet.

```
Switch-01 (config) # mlag-vip MLAG-VIP-DOM ip a.b.c.d /24 force
```

- b. Create a virtual MAC address for the system MLAG.

```
Switch-01 (config) # mlag system-mac AA:BB:CC:DD:EE:FF
```

- c. Configure the MLAG domain so that it is active globally.

```
Switch-01 (config) # no mlag shutdown
```

Note: The IP used for the MLAG VIP must be in the same subnet as the switch management network (mgmt0).

Note: The MAC address used can be any unicast MAC address and must be set to the same value on both switches in the MLAG domain.

Configure Ports to Connect to Storage and Compute Hosts

1. Create each of the VLANs needed to support the services for NetApp HCI. Run these commands on each switch in the domain:

- a. Create the VLANs identified in Table 1.

```
Switch-01 (config) # vlan 1172
Switch-01 (config vlan 1172) exit
Switch-01 (config) # vlan 3480-3482
Switch-01 (config vlan 3480-3482) exit
```

- b. Create names for each VLAN for easier accounting.

```
Switch-01 (config) # vlan 1172 name "VM_Network"
Switch-01 (config) # vlan 3480 name "MGMT_Network"
Switch-01 (config) # vlan 3481 name "Storage_Network"
Switch-01 (config) # vlan 3482 name "vMotion_Network"
```

2. Create Hybrid VLAN ports on ports ETH1/9-10 so that you can tag the appropriate VLANs for the NetApp HCI compute nodes.

- a. Select the ports you want to work with.

```
Switch-01 (config) # interface ethernet 1/9-1/10
```

- b. Set the MTU for each port.

```
Switch-01 (config interface ethernet 1/9-1/10) # mtu 9216 force
```

c. Modify spanning-tree settings for each port.

```
Switch-01 (config interface ethernet 1/9-1/10) # spanning-tree bpdupfilter enable
Switch-01 (config interface ethernet 1/9-1/10) # spanning-tree port type edge
Switch-01 (config interface ethernet 1/9-1/10) # spanning-tree bpduguard enable
```

d. Set the switchport mode to hybrid.

```
Switch-01 (config interface ethernet 1/9-1/10 ) # switchport mode hybrid
Switch-01 (config interface ethernet 1/9-1/10 ) # exit
```

e. Create descriptions for each port being modified.

```
Switch-01 (config) # interface ethernet 1/9 description HCI-CMP-01 PortD
Switch-01 (config) # interface ethernet 1/10 description HCI-CMP-02 PortD
```

f. Tag the appropriate VLANs for the NetApp HCI environment.

```
Switch-01 (config) # interface ethernet 1/9 switchport hybrid allowed-vlan add 1172
Switch-01 (config) # interface ethernet 1/9 switchport hybrid allowed-vlan add 3480-3482
Switch-01 (config) # interface ethernet 1/10 switchport hybrid allowed-vlan add 1172
Switch-01 (config) # interface ethernet 1/10 switchport hybrid allowed-vlan add 3480-3482
```

3. Create MLAG interfaces and hybrid VLAN ports on ports ETH1/5-8 so that you can distribute connectivity between the switches and tag the appropriate VLANs for the NetApp HCI storage nodes.

a. Select the ports that you want to work with.

```
Switch-01 (config) # interface ethernet 1/5-1/8
```

b. Set the MTU for each port.

```
Switch-01 (config interface ethernet 1/5-1/8) # mtu 9216 force
```

c. Modify spanning tree settings for each port.

```
Switch-01 (config interface ethernet 1/5-1/8) # spanning-tree bpdupfilter enable
Switch-01 (config interface ethernet 1/5-1/8) # spanning-tree port type edge
Switch-01 (config interface ethernet 1/5-1/8) # spanning-tree bpduguard enable
```

d. Set the switchport mode to hybrid.

```
Switch-01 (config interface ethernet 1/5-1/8 ) # switchport mode hybrid
Switch-01 (config interface ethernet 1/5-1/8 ) # exit
```

e. Create descriptions for each port being modified.

```
Switch-01 (config) # interface ethernet 1/5 description HCI-STG-01 PortD
Switch-01 (config) # interface ethernet 1/6 description HCI-STG-02 PortD
Switch-01 (config) # interface ethernet 1/7 description HCI-STG-03 PortD
Switch-01 (config) # interface ethernet 1/8 description HCI-STG-04 PortD
```

f. Create and configure the MLAG port channels.

```
Switch-01 (config) # interface mlag-port-channel 115-118
Switch-01 (config interface mlag-port-channel 115-118) # exit
Switch-01 (config) # interface mlag-port-channel 115-118 no shutdown
Switch-01 (config) # interface mlag-port-channel 115-118 mtu 9216 force
Switch-01 (config) # interface mlag-port-channel 115-118 lacp-individual enable force
Switch-01 (config) # interface ethernet 1/5-1/8 lacp port-priority 10
Switch-01 (config) # interface ethernet 1/5-1/8 lacp rate fast
Switch-01 (config) # interface ethernet 1/5 mlag-channel-group 115 mode active
Switch-01 (config) # interface ethernet 1/6 mlag-channel-group 116 mode active
Switch-01 (config) # interface ethernet 1/7 mlag-channel-group 117 mode active
Switch-01 (config) # interface ethernet 1/8 mlag-channel-group 118 mode active
```

g. Tag the appropriate VLANs for the storage environment.

```
Switch-01 (config) # interface mlag-port-channel 115-118 switchport mode hybrid
Switch-01 (config) # interface mlag-port-channel 115 switchport hybrid allowed-vlan add 1172
Switch-01 (config) # interface mlag-port-channel 116 switchport hybrid allowed-vlan add 1172
Switch-01 (config) # interface mlag-port-channel 117 switchport hybrid allowed-vlan add 1172
Switch-01 (config) # interface mlag-port-channel 118 switchport hybrid allowed-vlan add 1172
```

```
Switch-01 (config) # interface mlag-port-channel 115 switchport hybrid allowed-vlan add 3481
Switch-01 (config) # interface mlag-port-channel 116 switchport hybrid allowed-vlan add 3481
Switch-01 (config) # interface mlag-port-channel 117 switchport hybrid allowed-vlan add 3481
Switch-01 (config) # interface mlag-port-channel 118 switchport hybrid allowed-vlan add 3481
```

Note: The configurations in this section must also be run on the second switch in the MLAG domain. NetApp recommends that the descriptions for each port are updated to reflect the device ports that are being cabled and configured on the other switch.

Create Uplink Ports for the Switches

1. Create an MLAG interface to provide uplinks to both Mellanox SN2010 switches from the core network.

```
Switch-01 (config) # interface mlag port-channel 101
Switch-01 (config interface mlag port-channel) # description Uplink CORE-SWITCH port PORT
Switch-01 (config interface mlag port-channel) # exit
```

2. Configure the MLAG members.

```
Switch-01 (config) # interface ethernet 1/18 description Uplink to CORE-SWITCH port PORT
Switch-01 (config) # interface ethernet 1/18 speed 10000 force
Switch-01 (config) # interface mlag-port-channel 101 mtu 9216 force
Switch-01 (config) # interface ethernet 1/18 mlag-channel-group 101 mode active
```

3. Set the switchport mode to hybrid and allow all VLANs from the core uplink switches.

```
Switch-01 (config) # interface mlag-port-channel switchport mode hybrid
Switch-01 (config) # interface mlag-port-channel switchport hybrid allowed-vlan all
```

4. Verify that the MLAG interface is up.

```
Switch-01 (config) # interface mlag-port-channel 101 no shutdown
Switch-01 (config) # exit
```

5.3 Deploy NetApp HCI with the NetApp Deployment Engine

NDE delivers a simple and streamlined deployment experience for the NetApp HCI solution. These steps begin after the nodes have been racked, and cabled, and the IPMI port has been configured on each node using the console. A detailed guide to using NDE 1.6 to deploy your NetApp HCI system can be found [here](#).

To Deploy the NetApp HCI solution using NDE, complete the following steps:

1. Access the out-of-band management console for one of the storage nodes in the cluster and log in with the default credentials ADMIN/ADMIN.



2. Click the Remote Console Preview image in the center of the screen to download a JNLP file launched by Java Web Start, which launches an interactive console to the system.
3. With the virtual console launched, a user can log in to the HCI Storage node, using the ADMIN/ADMIN username and password combination.
4. The Bond1G interface must have an IP, a netmask, and a gateway set statically; its VLAN set to 3480; and DNS servers defined for the environment.

```

Bond1G

Method          : static

Link Speed      : 1000

IPv4 Address     : 172.21.224.153

IPv4 Subnet Mask : 255.255.255.0
--->

IPv4 Gateway Address : 172.21.224.254
--->

IPv6 Address     :
--->

IPv6 Gateway Address :
--->

MTU              : 1500
--->

DNS Servers      : 10.61.184.251, 10.61.184.252
--->

Search Domains   :
--->

Bond Mode        : ActivePassive [ActivePassive, ALB, LACP]
--->

Status           : UpAndRunning [Down, Up, UpAndRunning]
--->

Virtual Network Tag : 3480
--->

Routes           : Number of routes: 0.
--->

```

Note: Select an IP that is within the subnet you intend to use for in-band management, but not an IP you would like to use in production. NDE reconfigures the node with a production IP after initial access.

Note: This task must only be performed on the first storage node. Afterward, the other nodes in the infrastructure are discovered by the Automatic Private IP Address (APIPA) addresses assigned to each storage interface when left unconfigured.

5. The Bond 10G interface must have its MTU setting changed to enable jumbo frames and its bond mode changed to LACP.

```

Bond10G

Method          : static

Link Speed      : 50000

IPv4 Address     :

IPv4 Subnet Mask :
---->

IPv4 Gateway Address :
---->

MTU             : 9000
---->

Bond Mode       : LACP [ActivePassive, ALB, LACP]
---->

LACP Rate       : Fast [Fast, Slow]
---->

Status          : UpAndRunning [Down, Up, UpAndRunning]
---->

Virtual Network Tag :
---->

Routes          : Number of routes: 0.
---->

```

Note: Configure each of the four storage nodes in the NetApp HCI solution this way. The NDE process is then able to discover all the nodes in the solution and configure them. You do not need to modify the Bond10g interfaces on the two compute nodes.

6. After completion, open a web browser and visit the IP address you configured for the management port to start the NetApp HCI configuration with NDE.
7. On the Welcome to NetApp HCI page, click the Get Started button.
8. Check each associated box on the Prerequisites page and click Continue.
9. The next page presents End User Licenses for NetApp HCI and VMware vSphere. If you accept the terms, click I Accept at the end of each agreement and then click Continue.
10. Click Configure a New vSphere Deployment, select vSphere 6.5U2, and enter the Fully Qualified Domain Name (FQDN) of your vCenter Server. Then click Continue.

vSphere Configuration

You may elect to configure a new vSphere deployment or to join an existing vSphere deployment.

- ☒ Configure a new vSphere deployment
 - ☐ Configure Using vSphere Version 6.7 Update 1
 - ☒ Configure Using vSphere Version 6.5 Update 2
- ☐ Join and extend an existing vSphere deployment

If you have set up a DNS record for your new vCenter server, then configure your server using its fully qualified domain name and DNS server IP address:

- ☒ Configure Using a Fully Qualified Domain Name  *Best Practice!*

vCenter Server Fully Qualified Domain Name

anthos-vc.cie.netapp.com



Note: The domain name must resolve to an unused IP address.

DNS Server IP Address

10.61.184.251



If you have not set up a DNS record for your new vCenter server, you may configure using an IP address that we define:

- ☐ Configure Using an IP Address ?

Note: Once defined, the IP address cannot be changed.

Back

Continue

11. NDE asks for the credentials to be used in the environment. This is used for VMware vSphere, the NetApp Element storage cluster, and the NetApp Mnode, which provides management functionality for the cluster. When you are finished, click Continue.

Credentials

Define the user name and password that will be used for the storage cluster, vCenter, and the management node.

User Name

admin



Password



Password must contain:

- ✓ At least 8 characters
- ✓ No more than 20 characters
- ✓ 1 uppercase letter that is not the first character ?
- ✓ 1 lowercase letter
- ✓ 1 of the following special characters: !@\$
- ✓ Allowed characters: A-Z a-z 0-9 !@\$
- ✓ 1 number that is not the last character ?

Re-enter Password



Back

Continue

12. NDE then prompts for the network topology used to cable the NetApp HCI environment. The validated solution in this document has been deployed using the 2 Cable Option for the compute nodes, and the 4 Cable Option for the storage nodes. Click Continue.

Network Topology

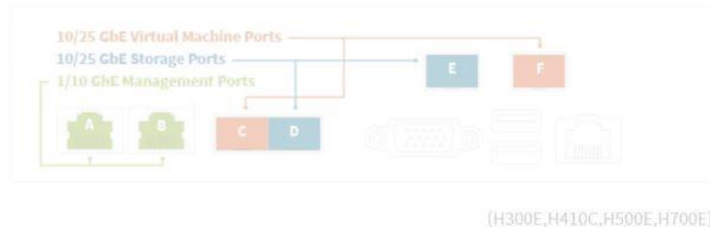
Select a compute node topology and a storage node topology appropriate for your hardware installation.

Compute Node Topology

☐ 6 Cable Option

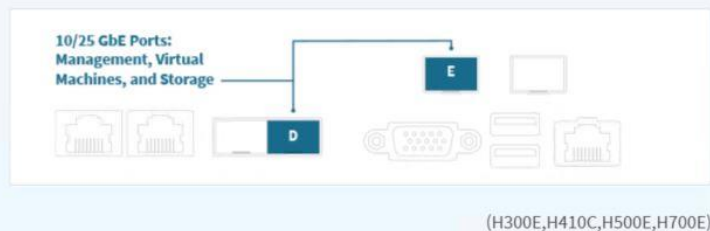
The 6 cable option provides dedicated ports for management (2 x 1/10 GbE), virtual machines (2 x 10/25 GbE) and storage (2 x 10/25 GbE).

☐ Use vSphere Distributed Switch? [?](#)



☒ 2 Cable Option

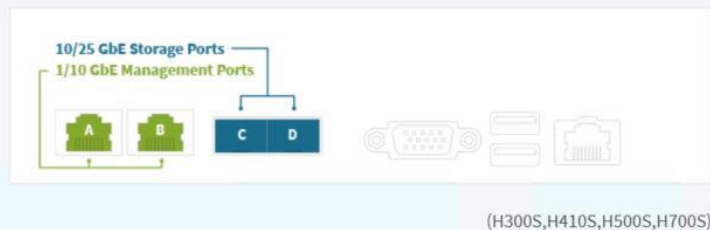
The 2 cable option provides shared management with ports for virtual machines and storage (2 x 10/25 GbE). The 2 cable option uses vSphere Distributed Switch. [?](#)



Storage Node Topology

☒ 4 Cable Option

The 4 cable option provides dedicated ports for management (2 x 1/10 GbE) and storage (2 x 10/25 GbE).



[Back](#)

[Continue](#)

13. The next page presented by NDE is the inventory of the environment as discovered by the APIPA addressed on the storage network. The storage node that is currently running NDE is already selected with a green check mark. Select the corresponding boxes to add additional nodes to the NetApp HCI environment. Click Continue.

Inventory

Verify the available nodes and select **at least 2 compute nodes and 4 storage nodes** to include in your installation.

[Refresh Inventory](#)

Compute Nodes

<input checked="" type="checkbox"/>	Serial Number ↕	Chassis Serial Number / Slot ↕	Node Type ↕	Software Version ↕	Physical CPU Cores ↕	Memory ↕	1 GbE Ports ↕	10 GbE Ports ↕
<input checked="" type="checkbox"/>	HM17CS002729	002170990158 / B	H410C	1.6	8	384 GB	0 of 2 detected	2 of 4 detected
<input checked="" type="checkbox"/>	HM181S002024	002170990158 / A	H410C	1.6	8	384 GB	0 of 2 detected	2 of 4 detected

1 - 2 of 2 results 20 ▾

2 compute nodes selected

Storage Nodes

<input checked="" type="checkbox"/>	Serial Number ↕	Chassis Serial Number / Slot ↕	Node Type ↕	Raw Capacity ↕	Element Version ↕	Drive Count ↕	1 GbE Ports ↕	10 GbE Ports ↕
<input checked="" type="checkbox"/>	221814003506	221814003436 / C	H500S	5.76 TB	11.3.1.5	6 of 6 detected	2 of 2 detected	2 of 2 detected
<input checked="" type="checkbox"/>	221818004613	221814003436 / D	H500S	5.76 TB	11.3.1.5	6 of 6 detected	2 of 2 detected	2 of 2 detected
<input checked="" type="checkbox"/> ?	221826005865	002170990158 / C	H500S	5.76 TB	11.3.1.5	6 of 6 detected	2 of 2 detected	2 of 2 detected
<input checked="" type="checkbox"/>	221826005866	002170990158 / D	H500S	5.76 TB	11.3.1.5	6 of 6 detected	2 of 2 detected	2 of 2 detected

1 - 4 of 4 results 20 ▾

4 storage nodes selected

[Back](#)
[Continue](#)

Note: If there are any nodes missing from the inventory screen, wait a few minutes and click Refresh Inventory. If the node still fails to appear, additional investigation of environment networking may be required.

14. You must next configure the permanent network settings for the NetApp HCI deployment. The first page configures infrastructure services (DNS and NTP), vCenter networking, and Mnode networking.

Network Settings

Provide the network settings that will be used for your installation.

Live network validation is: On ?

Infrastructure Services

DNS Server IP Address 1

 ✓

DNS Server IP Address 2 (Optional)

 ✓

NTP Server Address 1 ?

 ✓

NTP Server Address 2 (Optional)

 ✓

To save time, launch the easy form to enter fewer network settings. > ?

vCenter Networking

VLAN ID	Subnet ?	Default Gateway	FQDN	IP Address
<input type="text" value="3480"/> ✓	<input type="text" value="172.21.224.0/24"/> ✓	<input type="text" value="172.21.224.1"/> ✓	anthos-vc.cie.netapp.com	<input type="text" value="172.21.224.10"/> ✓

Management Node Networking ?

Management Network

VLAN ID: ✓

Subnet ? : ✓

Default Gateway: ✓

iSCSI Network

VLAN ID: ✓

Subnet ? : ✓

Hostname	Management IP Address	Storage (iSCSI) IP Address
<input type="text" value="anthos-mnode"/> ✓	<input type="text" value="172.21.224.50"/> ✓	<input type="text" value="172.21.225.50"/> ✓

- The next page allows you to configure each node in the environment. For the compute nodes, it allows you to configure the host name, management network, vMotion network, and storage network. For the storage nodes, name the storage cluster and configure the management and storage networks being used for each node. Click Continue.

Compute Node Networking

Management Network	vMotion Network	iSCSI A Network	iSCSI B Network
VLAN ID 3480 ✓	VLAN ID 3482 ✓	VLAN ID 3481 ✓	VLAN ID 3481 ✓
Subnet ? 172.21.224.0/24 ✓	Subnet ? 172.21.226.0/24 ✓	Subnet ? 172.21.225.0/24 ✓	Subnet ? 172.21.225.0/24 ✓
Default Gateway 172.21.224.1 ✓	Default Gateway (Optional)	Default Gateway (Optional)	Default Gateway (Optional)

Serial Number	Hostname	Management IP Address	vMotion IP Address	iSCSI A - IP Address	iSCSI B - IP Address
HM17CS002729	Anthos-ESXi-01 ✓	172.21.224.11 ✓	172.21.226.11 ✓	172.21.225.11 ✓	172.21.225.111 ✓
HM181S002024	Anthos-ESXi-02 ✓	172.21.224.12 ✓	172.21.226.12 ✓	172.21.225.12 ✓	172.21.225.112 ✓

Storage Node Networking

Storage Cluster Name
Anthos-Store ✓

Note: The storage cluster name cannot be changed after deployment.

Management Network	iSCSI Network
VLAN ID 3480 ✓	VLAN ID 3481 ✓
Subnet ? 172.21.224.0/24 ✓	Subnet ? 172.21.225.0/24 ✓
Default Gateway 172.21.224.1 ✓	Default Gateway (Optional)
Management Virtual IP (MVIP) ? 172.21.224.20 ✓	Storage Virtual IP (SVIP) ? 172.21.225.20 ✓

Serial Number	Hostname	Management IP Address	Storage (iSCSI) IP Address
221814003506	Anthos-Store-01 ✓	172.21.224.21 ✓	172.21.225.21 ✓
221818004613	Anthos-Store-02 ✓	172.21.224.22 ✓	172.21.225.22 ✓
221826005865	Anthos-Store-03 ✓	172.21.224.23 ✓	172.21.225.23 ✓
221826005866	Anthos-Store-04 ✓	172.21.224.24 ✓	172.21.225.24 ✓

Back

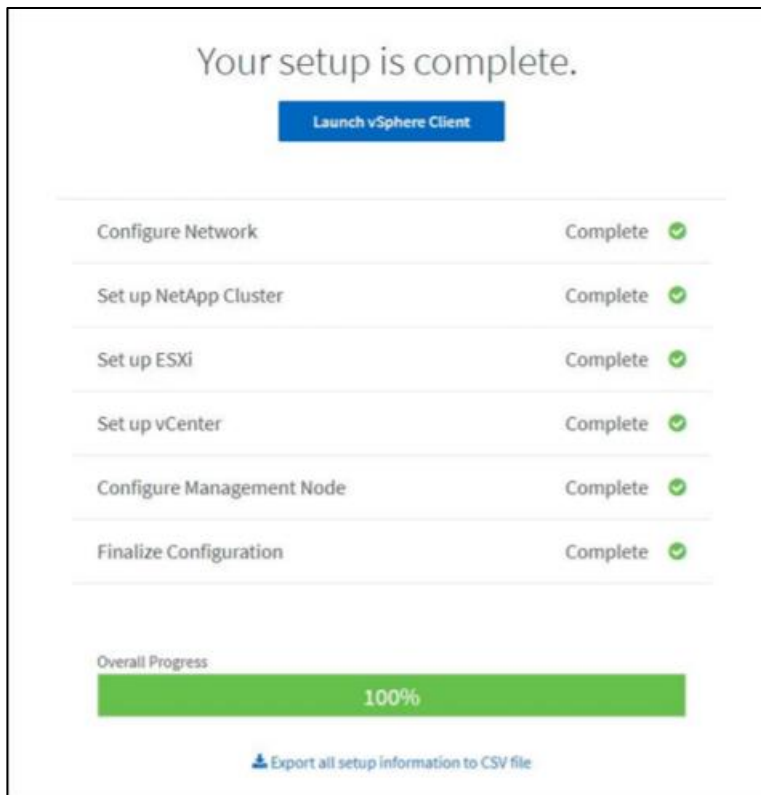
Live network validation is:
On ?

Continue

16. On the next page, review all the settings that have been defined for the environment by expanding each section, and, if necessary, click Edit to make corrections. There is also a check box on this page that enables or disables the Mnode from sending real-time health and diagnostics information to NetApp Active IQ®. If all the information is correct, click Start Deployment.

Note: If you want to enable Active IQ, verify that your management network can reach the internet. If NDE is unable to reach Active IQ, the deployment can fail.

17. A summary page appears along with a progress bar for each component of the NetApp HCI solution, as well as the overall solution. When complete, you are presented with an option to launch the vSphere client and begin working with your environment.

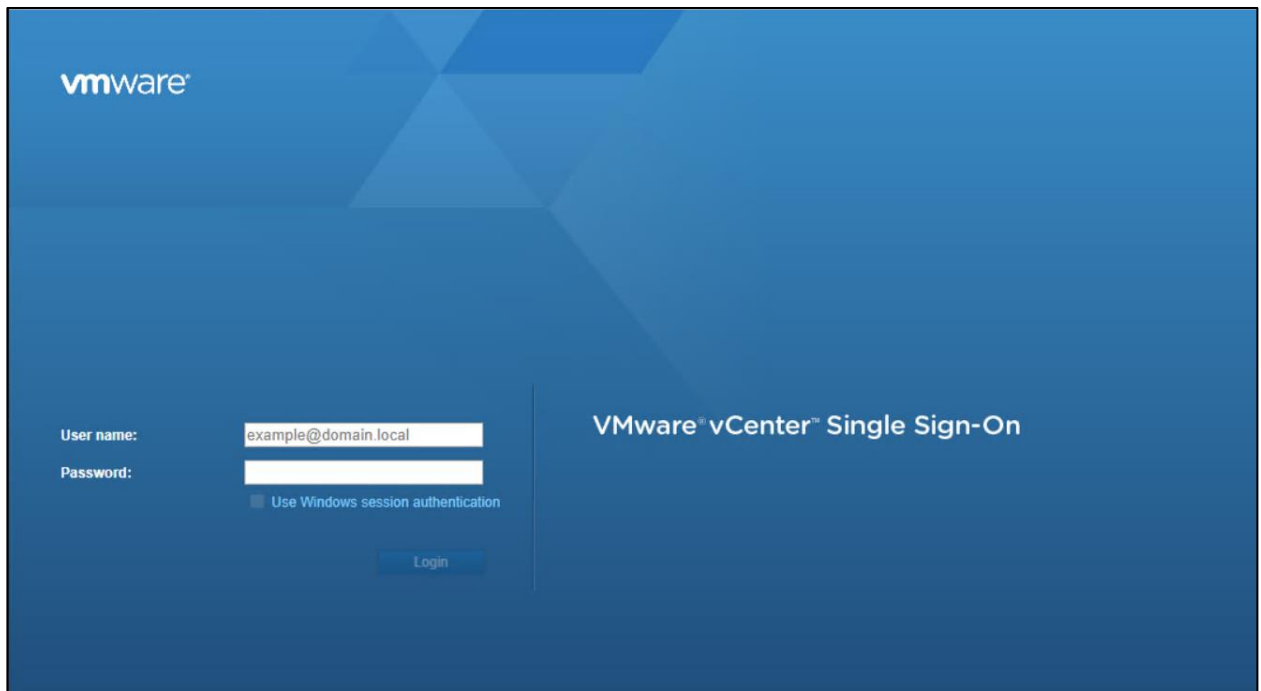


5.4 Configure the vCenter Server

NDE deploys the solution with vCenter server and integrates the solution with the Element cluster by provisioning the Mnode VM and installing the NetApp Element Plug-in for vCenter. After deployment, a few modifications must be made to the environment, including the creation of additional vDS portgroups, datastores, and resource groups for the deployment of the Anthos on VMware solution.

Complete the following steps to configure your vCenter Server for use:

1. Log into the VMware vCenter server using the Administrator@vsphere.local[mailto:](mailto:Administrator@vsphere.local) account and the password chosen for the admin user during NDE configuration.



2. Right-click `NetApp-HCI-Cluster-01` created by NDE and select the option to create a new resource pool. Name this pool `Infrastructure-Resource-Pool` and accept the defaults by clicking OK. This resource pool is used in a later configuration step.

New Resource Pool
NetApp-HCI-Cluster-01

Name	Infrastructure Resource		
CPU			
Shares	Normal	4000	
Reservation	0		MHz
Max reservation: 54,128 MHz			
Reservation Type	<input checked="" type="checkbox"/> Expandable		
Limit	Unlimited		MHz
Max limit: 58,128 MHz			
Memory			
Shares	Normal	163840	
Reservation	0		MB
Max reservation: 751,064 MB			
Reservation Type	<input checked="" type="checkbox"/> Expandable		
Limit	Unlimited		MB
Max limit: 756,820 MB			

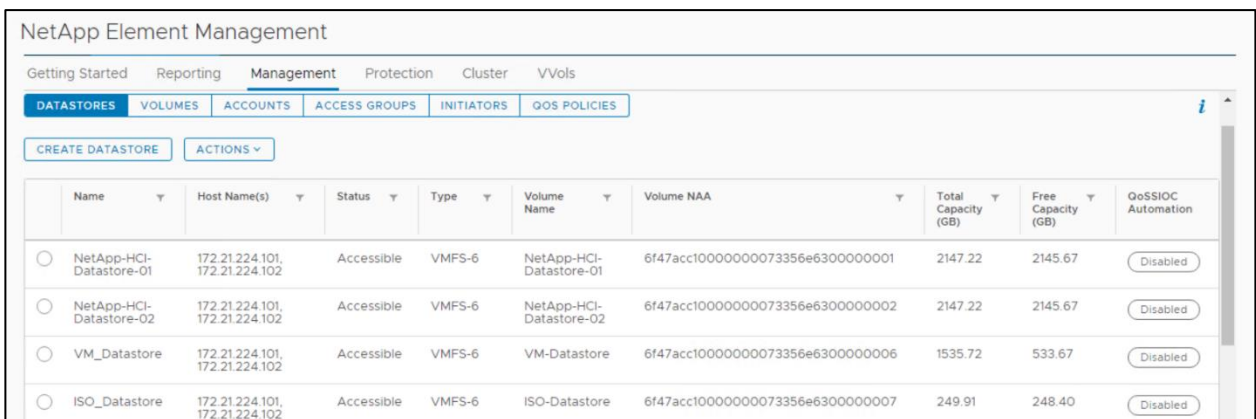
CANCEL
OK

- Note:** The reservations in this resource pool can be modified based on the resources available in the environment. NetApp HCI is deployed as an all-in-one solution. Therefore, NetApp recommends reserving the resources necessary to provide availability for the infrastructure services by placing them into this resource pool and adjusting the resources appropriately. Infrastructure services include vCenter Server, NetApp Mnode, and F5 Big-IP Load Balancer.
- Repeat this step to create another resource pool for VMs deployed by Anthos. Name this pool `Anthos-Resource-Pool` and click the OK button to accept the default values. Adjust the resource availability based on the specific environment in which you are deploying the solution. This resource pool is used in a later deployment step.

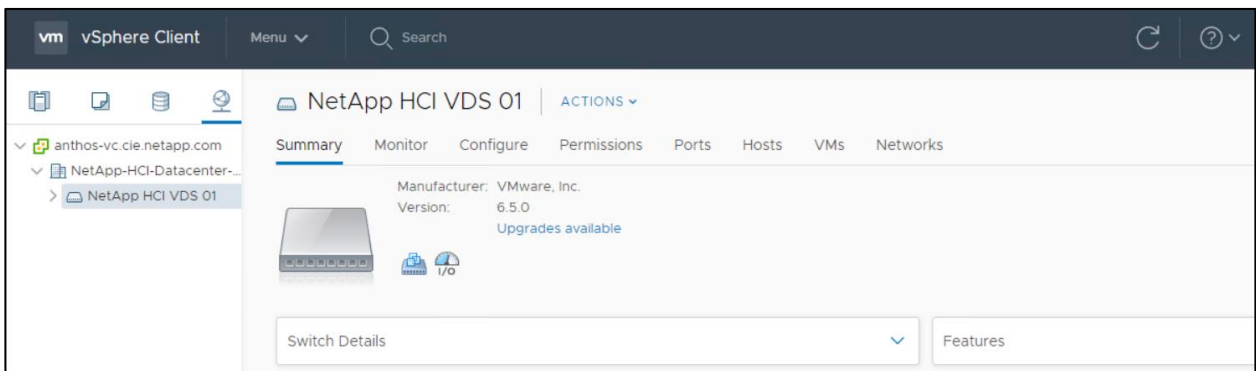
- To configure Element volumes to be used as vSphere datastores, click the dropdown menu and select NetApp Element Management from the list.
- A Getting Started screen appears with details about your Element cluster.



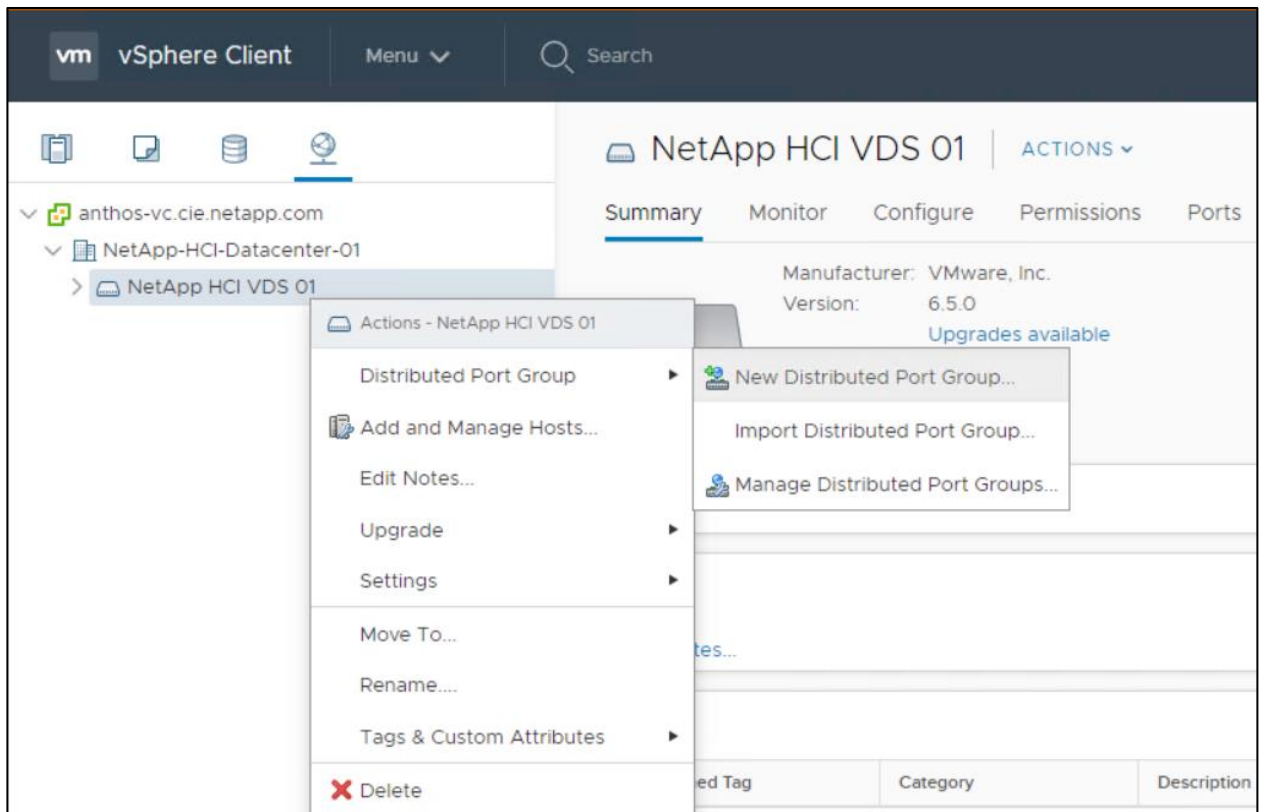
- Click Management, and the vSphere client presents a list of datastores. Click Create Datastore to create one datastore to host VMs and another to host ISOs for future guest installs.



- Next click the Network menu item in the left panel. This displays a screen with information about the vDS deployed by NDE.



- Several virtual port groups are defined by the initial configuration. NetApp recommends leaving these alone to support the infrastructure, and additional port groups should be created for user-deployed virtual guests. Right-click the NetApp HCI VDS 01 vDS in the left panel, and then select Distributed Port Group followed by the New Distributed Port Group option from the expanded menu.




9. Create a new distributed port group called `Management_Network`. Then click Next.

New Distributed Port Group

1 Select name and location
2 Configure settings
3 Ready to complete

Select name and location

Select port group name and distributed switch where to locate it.

Name	<u>Management_Network</u>
Location	 NetApp HCI VDS 01

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

10. On the next screen, select the VLAN type as VLAN, and set the VLAN ID to 3480 for management purposes. Click Next, and, after reviewing the options on the summary page, click Next again to complete the creation of the distributed port group.

New Distributed Port Group

1 Select name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding

Static binding

Port allocation

Elastic

Number of ports

8

Network resource pool

(default)

VLAN

VLAN type

VLAN

VLAN ID

3480

Advanced

☐ Customize default policies configuration

CANCEL

BACK

NEXT

- Repeat these steps to create distributed port groups for the `VM_Network` (VLAN 1172), as well as any other networks that might be used in the NetApp HCI environment.

Note: Additional networks can be defined to segment any additional deployed VMs. Examples of this use could be for a dedicated HA network for additional F5 Big-IP appliances if provisioned. Such configurations are in addition to the environment deployed in this validated solution and are considered out of scope for this NVA document.

5.5 Deploy and Configure the F5 Big-IP Virtual Edition Appliance

Anthos enables native integration with F5 Big-IP load balancers to expose services from each pod to the world. This solution makes use of the virtual appliance deployed in VMware vSphere as deployed by NDE. 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](#).

To deploy the F5 Big-IP Virtual Edition appliance, complete the following steps:

- Download the virtual application Open Virtual Appliance (OVA) file from F5 [here](#).

Note: 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.

- 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

Choose Files

BIGIP-15.0.1-0.....ALL-vmware.ova

CANCEL

BACK

NEXT

- 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.
- 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.

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

✓ 3 Select a compute resource

✓ 4 Review details

✓ 5 License agreements

✓ 6 Configuration

✓ 7 Select storage

8 Select networks

9 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
Internal	BIG-IP-Internal
External	VM_Network
HA	BIG-IP-HA
Management	Management_Network

4 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL

BACK

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.

BIGIP-15.0.1-0.0.11-vmware-B | ACTIONS ▾

Summary | Monitor | Configure | Permissions | Datastores | Networks

Guest OS: CentOS 4/5 or later (64-bit)
 Compatibility: ESXi 5.5 and later (VM version 10)
 VMware Tools: Running, version:10245 (Guest Managed)
[More info](#)

DNS Name: localhost.localdomain
 IP Addresses: 127.20.0.254
[View all 6 IP addresses](#)

Host: 172.21.224.101

Powered On

[Launch Web Console](#)
[Launch Remote Console](#)

BIGIP-15.0.1-0.0.11-vmwa... (X)

IP Addresses:
 127.20.0.254
 127.1.1.254
 172.21.224.20

- 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.

f5 BIG-IP Configuration Utility
 F5 Networks, Inc.

Hostname
bigip1

IP Address
172.21.224.20

Username
admin

Password

Log in

Welcome to the BIG-IP Configuration Utility.
 Log in with your username and password using the fields on the left.

(c) Copyright 1996-2019, F5 Networks, Inc., Seattle, Washington. All rights reserved.
[F5 Networks, Inc. Legal Notices](#)

- The first screen prompts the user to complete the Setup Utility. Begin the utility by clicking Next.

Welcome

Setup Utility

To begin configuring this BIG-IP® system, please complete the Setup Utility. To begin, click the "Next" button.

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.

General Properties

Base Registration Key: BFXBY-PVROQ-QIHCH-NZGSZ-AZCFDPX [Revert]

Add-On Registration Key List:

Add-On Key: [] [Add]

[Edit] [Delete]

Activation Method: ☒ Automatic (requires outbound connectivity) ☐ Manual

Outbound Interface: mgmt ▼

License Comparison: ☐ Enable License Comparison

Next...

- Note:** 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.

BIG-IP system configuration has changed

Tue Nov 05 2019 18:10:20

The configuration for this device has been updated. Consequently, the features and functionality previously available on the BIG-IP system might have changed.

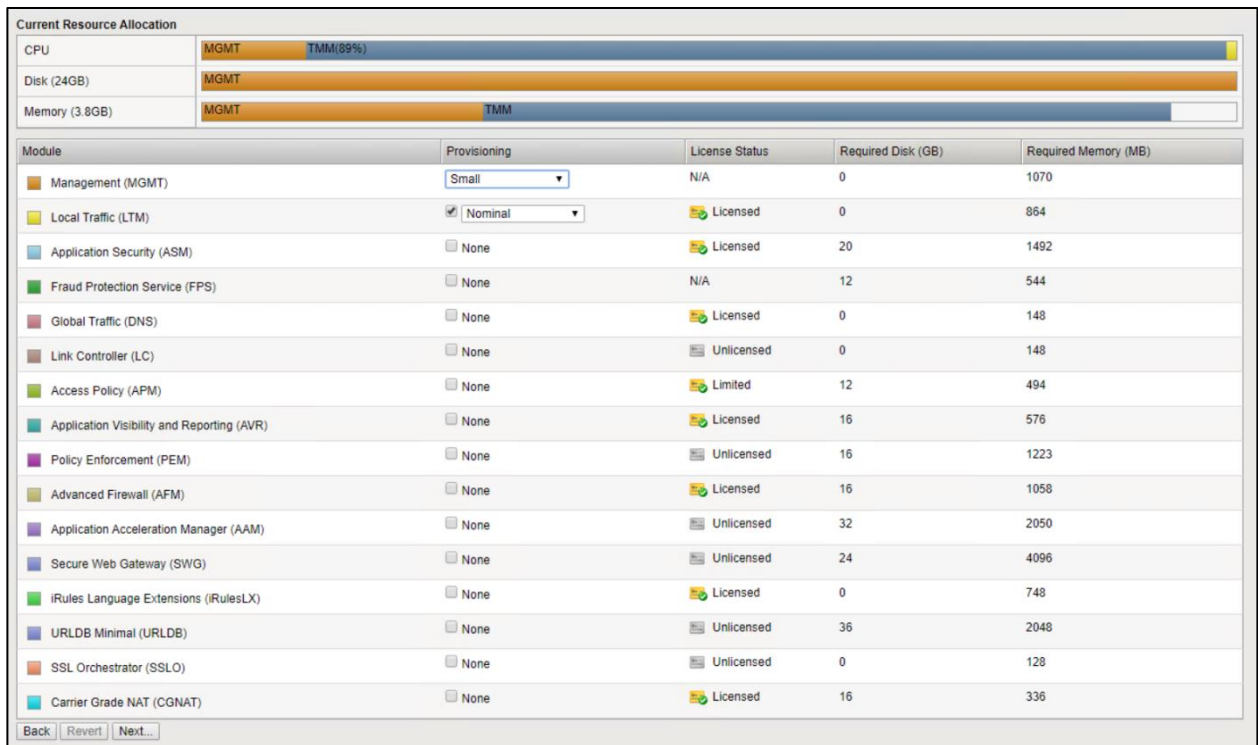
Elapsed Time: 49 seconds

✓ Please wait while the configuration changes are verified...
The BIG-IP Configuration utility will be updated momentarily.

✓ Configuration changes have been verified
You may now continue using the BIG-IP Configuration utility.

Continue

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.



- 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.

General Properties

Management Config IPV4	<input checked="" type="radio"/> Automatic (DHCP) <input type="radio"/> Manual
Management Config IPV6	<input checked="" type="radio"/> Automatic (DHCP) <input type="radio"/> Manual
Host Name	Anthos-F5-Big-IP
Host IP Address	Use Management Port IP Address
Time Zone	America/New York

User Administration

Root Account	<input type="checkbox"/> Disable login Password: <input type="password"/> Confirm: <input type="password"/>
SSH Access	<input checked="" type="checkbox"/> Enabled
SSH IP Allow	* All Addresses

Back Next...

- Next click the Network menu, which enables you to configure standard networking features. Click Next to begin the Standard Network Configuration wizard.

Standard Network Configuration

Create a standard network configuration by configuring these features:

- Redundancy
- VLANs
- NTP
- DNS
- Config Sync
- Failover
- Mirroring
- Peer Device Discovery (for Redundant Configurations)

Next...

Advanced Network Configuration

Create advanced device configurations by clicking **Finished** and navigating to the Main tab of the Configuration Utility.

Finished

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.

Internal Network Configuration

Self IP	Address: 192.168.1.11
	Netmask: 255.255.255.0
	Port Lockdown: Allow Default
Floating IP	Address: 192.168.1.10
	Port Lockdown: Allow Default

Internal VLAN Configuration

VLAN Name	Internal
VLAN Tag ID	auto
	VLAN Interfaces: 1.1
	Tagging: Select...
	Add
Interfaces	
	Edit Delete

Cancel Next...

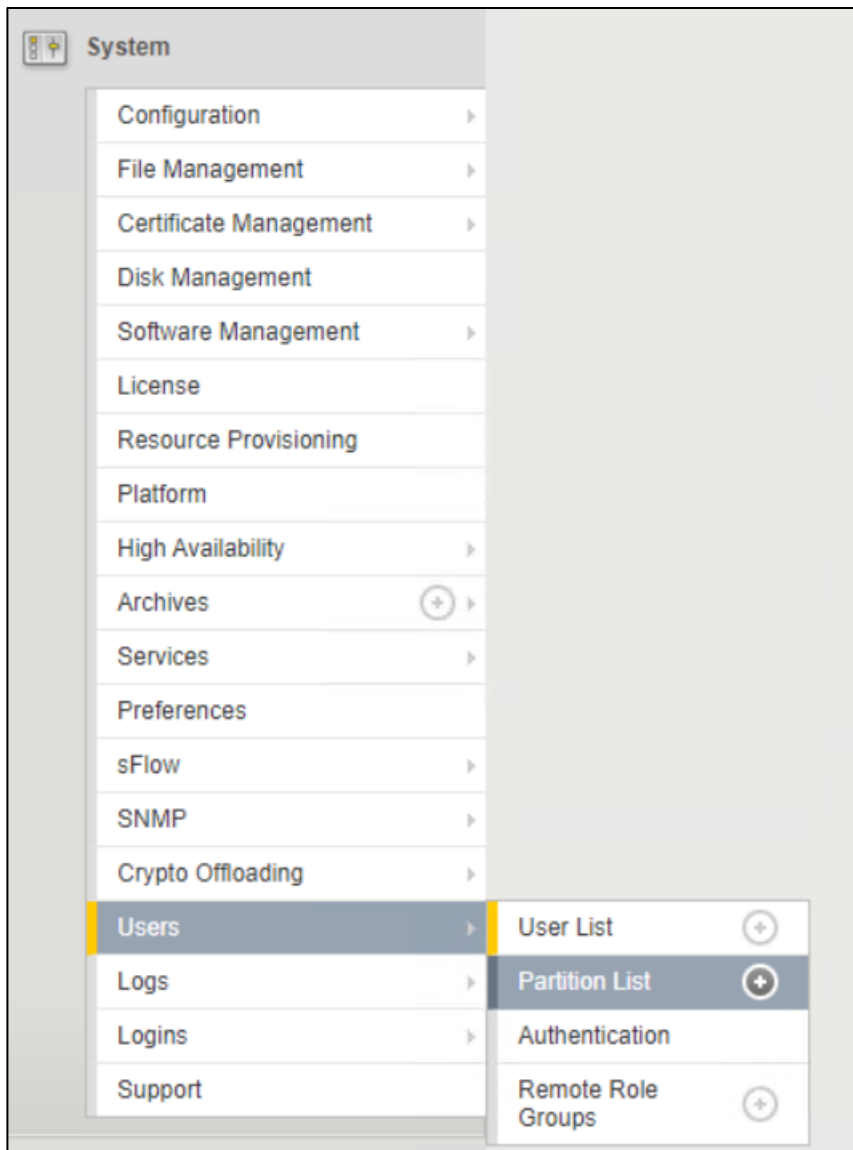
- Note:** The spaces in this page for Self IP Address, Netmask, and Floating IP address can be filled with a non-routable IP for use as a placeholder. They can also be filled with an internal network that has been configured as a distributed port group for virtual guests if you are deploying the three-armed 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.

External Network Configuration	
External VLAN	<input checked="" type="radio"/> Create VLAN external <input type="radio"/> Select existing VLAN
Self IP	Address: <input type="text" value="10.63.172.101"/> Netmask: <input type="text" value="255.255.255.0"/> Port Lockdown: <input type="text" value="Allow None"/>
Default Gateway	<input type="text" value="10.63.172.1"/>
Floating IP	Address: <input type="text" value="10.63.172.100"/> Port Lockdown: <input type="text" value="Allow None"/>
External VLAN Configuration	
VLAN Name	external
VLAN Tag ID	auto
Interfaces	VLAN Interfaces: <input type="text" value="1.2"/> Tagging: <input type="text" value="Select..."/> <input type="button" value="Add"/> <div style="border: 1px solid #ccc; height: 40px; margin-top: 5px;"></div> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="button" value="Cancel"/> <input type="button" value="Next..."/>	

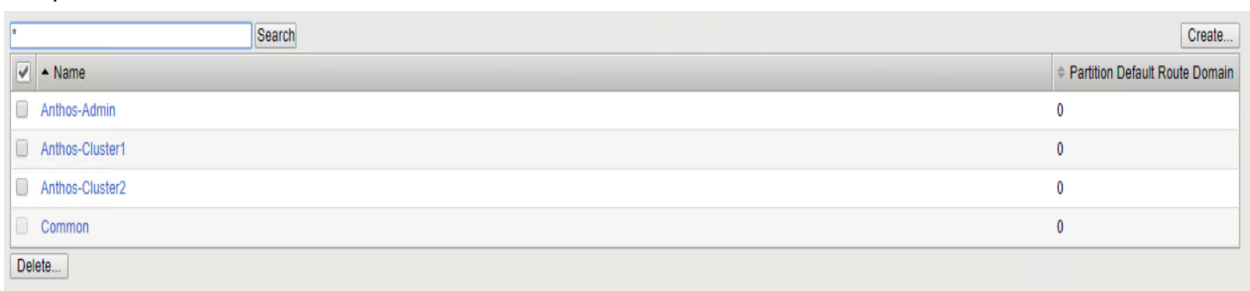
17. On the next page, you can configure an internal-HA network if you are deploying multiple virtual appliances in the environment. To proceed, you must fill the Self-IP Address and the Netmask fields, and you must select interface 1.3 as the VLAN Interface, which maps to the HA network defined by the OVF template wizard.

High Availability Network Configuration	
High Availability VLAN	<input checked="" type="radio"/> Create VLAN HA <input type="radio"/> Select existing VLAN
Self IP	Address: <input type="text" value="192.168.2.11"/> Netmask: <input type="text" value="255.255.255.0"/>
High Availability VLAN Configuration	
VLAN Name	HA
VLAN Tag ID	auto
Interfaces	VLAN Interfaces: <input type="text" value="1.3"/> Tagging: <input type="text" value="Select..."/> <input type="button" value="Add"/> <div style="border: 1px solid #ccc; height: 40px; margin-top: 5px;"></div> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="button" value="Cancel"/> <input type="button" value="Next..."/>	

18. The next page enables you to configure of 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 show the current common partition. Click Create on the right to create the first additional partition, and name it `Anthos-Admin`. Then click Repeat, and name the partition `Anthos-Cluster1`, and click the Repeat button again to name the next partition `Anthos-Cluster2`. Finally click Finished to complete the wizard. The Partition list screen returns with all the partitions now listed.



5.6 Complete Anthos Prerequisites

Now that the physical environment is set up, you can begin Anthos deployment. This starts with several prerequisites that you must meet to deploy the solution and access it afterward. Each of these steps are discussed in depth in the Anthos [GKE On-Prem Guide](#). To prepare your environment for the deployment of Anthos on VMware, complete the following steps:

1. Create a Google Cloud project following the instructions available [here](#).

Note: Your organization might already have a project in place intended for this purpose. Check with your cloud administration team to see if a project exists and is already configured for access to Anthos on VMware. All projects intended for use with Anthos must be whitelisted by Google. This includes the primary user account, additional team members, and the access service account created in a later step.

2. Create a deployment workstation from which to manage the installation of Anthos on VMware. The deployment workstation can be Linux, MacOS, or Windows. For the purposes of this validated deployment, Red Hat Enterprise Linux 7 was used.

Note: This workstation can be hosted either internal or external to the NetApp HCI deployment. The only requirement is that it must be able to successfully communicate with the deployed VMware vCenter Server and the internet to function correctly.

3. Install [Google Cloud SDK](#) for interactions with Google Cloud. It can be downloaded as an archive of binaries for manual install or installed by either the apt-get (Ubuntu/Debian) or yum (RHEL) package managers.

```
[user@rhel7 ~]$ sudo yum install google-cloud-sdk
Failed to set locale, defaulting to C
Loaded plugins: langpacks, product-id, search-disabled-repos, subscription-manager
Resolving Dependencies
--> Running transaction check
---> Package google-cloud-sdk.noarch 0:270.0.0-1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                               Arch      Version      Repository      Size
=====
Installing:
google-cloud-sdk                      noarch    270.0.0-1    google-cloud-sdk 36 M

Transaction Summary
=====
Install 1 Package

Total download size: 36 M
Installed size: 174 M
Is this ok [y/d/N]: y
Downloading packages:
6d81c821884ae40244c746f6044fcbcd801143a0d9c8da06767036b8d090a24-google-cloud-sdk-270.0.0-1.noar
| 36 MB 00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : google-cloud-sdk-270.0.0-1.noarch 1/1
  Verifying  : google-cloud-sdk-270.0.0-1.noarch 1/1

Installed:
google-cloud-sdk.noarch 0:270.0.0-1

Complete!
```

Note: The gcloud binary must be at least version 265.0.0. You can update a manual install with a gcloud components update. However, if SDK was installed by a package manager, future updates must also be performed using that same package manager.

4. Install [govc](#), the CLI for VMware vSphere. Installing govc allows you to interact directly with the management of VMware vCenter. Govc is available as a pre-packaged binary available in a gzip format for download. For installation, a user must download the gzip archive, unzip, and copy the resulting binary to a local path directory such as /usr/local/bin.

```
[user@rhel7 ~]$ wget
https://github.com/vmware/govcmomi/releases/download/v0.20.0/govc_linux_amd64.gz
--2019-11-06 09:06:10--
https://github.com/vmware/govcmomi/releases/download/v0.20.0/govc_linux_amd64.gz
Resolving github.com (github.com)... 13.250.177.223
Connecting to github.com (github.com)|13.250.177.223|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7650188 (7.3M) [application/octet-stream]
Saving to: 'govc_linux_amd64.gz.1'

100%[=====] 7,650,188 --.-K/s in 0.1s

2019-11-06 09:06:12 (76.4 MB/s) - 'govc_linux_amd64.gz' saved [7650188/7650188]

[user@rhel7 ~]$ gunzip govc_linux_amd64.gz
[user@rhel7 ~]$ sudo cp govc_linux_amd64 /usr/local/bin/govc
[user@rhel7 ~]$ which govc
/usr/local/bin/govc
```

5. Install [Hashicorp Terraform](#). Terraform enables the automated deployment of VMs in a VMware vSphere environment and is used to deploy the Anthos admin workstation in a later step. Like the govc install, Terraform can be downloaded as a zip archive and unzipped, and the resulting binary can be copied to a directory in the local user's path.

```
[user@rhel7 ~]$ wget
https://releases.hashicorp.com/terraform/0.12.13/terraform_0.12.13_linux_amd64.zip
--2019-11-06 09:13:40--
https://releases.hashicorp.com/terraform/0.12.13/terraform_0.12.13_linux_amd64.zip
Resolving releases.hashicorp.com (releases.hashicorp.com)... 151.101.193.183, 151.101.1.183,
151.101.65.183, ...
Connecting to releases.hashicorp.com (releases.hashicorp.com)|151.101.193.183|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16341595 (16M) [application/zip]
Saving to: 'terraform_0.12.13_linux_amd64.zip.1'

100%[=====] 16,341,595 --.-K/s in 0.1s

2019-11-06 09:13:40 (141 MB/s) - 'terraform_0.12.13_linux_amd64.zip.1' saved [16341595/16341595]

[user@rhel7 ~]$ unzip terraform_0.12.13_linux_amd64.zip
Archive:  terraform_0.12.13_linux_amd64.zip
  inflating: terraform
[user@rhel7 ~]$ cp terraform /usr/local/bin
[user@rhel7 ~]$ which terraform
/usr/local/bin/terraform
```

6. With the workstation configured, log in to Google Cloud with your credentials. To do so, enter the login command from the deployment workstation and retrieve a link that can be copied and pasted into a browser to allow interactive sign-in to Google services. After you have logged in, the web page presents a code that you can copy and paste back into the deployment workstation when prompted.

```
[user@rhel7 ~]$ gcloud auth login
Go to the following link in your browser:

https://accounts.google.com/o/oauth2/auth?code_challenge=
7oPNSySHr_Sd2ZZ4K83koIeGTLVcdBjc8omr6zCbAI&prompt=select_account&code_challenge_method=S256&access_type=offline&redirect_uri=urn%3Aietf%3Aawg%3Aoauth%3A2.0%3Aaob&response_type=code&client_id=3265
```

```
5940559.apps.googleusercontent.com&scope=https%3A%3F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcloud-platform+https%3A%6F%2Fwww.googleapis.com%2Fauth%2Fappengine.admin+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcompute+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth
```

```
Enter verification code: 6/swGAh52VVgB-TRS5LVrSvP79ZdDlb9V6ObyUGqoY67a3zp9NPciIKsM
You are now logged in as [user@netapp.com].
Your current project is [anthos-dev]. You can change this setting by running:
$ gcloud config set project PROJECT_ID
```

7. Before you can install Anthos on VMware, you must create four service accounts, each with a specific purpose in interacting with Google Cloud. Table 4 lists the accounts and their purposes.

Table 4) Google Cloud Service Accounts.

Account Name	Purpose
access-service-account	Used to download the Anthos binaries from Cloud Storage.
register-service-account	Used to register Anthos clusters to the Google Cloud console.
connect-service-account	Used to maintain the connection between user clusters and the Google Cloud.
stackdriver-service-account	Used to write logging and monitoring data to Stackdriver.

Note: Each account is assigned an email address that references your approved Google Cloud project name. The examples below all list the project Anthos-Dev which was used during the NetApp validation. Make sure to substitute your appropriate project name in syntax examples where necessary.

```
[user@rhel7 ~]$ gcloud iam service-accounts create access-service-account
[user@rhel7 ~]$ gcloud iam service-accounts create register-service-account
[user@rhel7 ~]$ gcloud iam service-accounts create connect-service-account
[user@rhel7 ~]$ gcloud iam service-accounts create stackdriver-service-account
[user@rhel7 ~]$ gcloud iam service-accounts list
NAME                                EMAIL                                DISABLED
stackdriver-service-account@anthos-dev.iam.gserviceaccount.com    False
register-service-account@anthos-dev.iam.gserviceaccount.com       False
access-service-account@anthos-dev.iam.gserviceaccount.com         False
connect-service-account@anthos-dev.iam.gserviceaccount.com        False
```

8. Enable several APIs so that your environment can communicate with Google Cloud. The pods deployed in your clusters must be able to access <https://www.googleapis.com> and <https://gkeconnect.googleapis.com> to function as expected. Therefore, the VM_Network that the worker nodes are attached to must have internet access. To enable the necessary APIs, run the following command from the deployment workstation:

```
[user@rhel7 ~]$ gcloud services enable \
cloudresourcemanager.googleapis.com \
container.googleapis.com \
gkeconnect.googleapis.com \
gkehub.googleapis.com \
serviceusage.googleapis.com \
stackdriver.googleapis.com \
monitoring.googleapis.com \
logging.googleapis.com
```

9. The final step needed to prepare your environment to deploy Anthos is to limit certain privileges to your service accounts. You need the associated email address for each service account listed in Step 7.

- a. Using the register service account, assign the roles for `gkehub.admin` and `serviceusage.serviceUsageViewer`.

```
[user@rhel7 ~]$ gcloud projects add-iam-policy-binding anthos-dev \
--member "serviceAccount: register-service-account@anthos-dev.iam.gserviceaccount.com"
```

```
--role "roles/gkehub.admin"

[user@rhel7 ~]$ gcloud projects add-iam-policy-binding anthos-dev \
--member "serviceAccount: register-service-account@anthos-dev.iam.gserviceaccount.com" \
--role "roles/serviceusage.serviceUsageViewer"
```

- b. Using the connect service account, assign the roles for `gkehub.connect`.

```
[user@rhel7 ~]$ gcloud projects add-iam-policy-binding anthos-dev \
--member "serviceAccount: connect-service-account@anthos-dev.iam.gserviceaccount.com" \
--role "roles/gkehub.connect"
```

- c. With the stackdriver service account, assign the roles for `stackdriver.resourceMetadata.writer`, `logging.logWriter`, and `monitoring.metricWriter`.

```
[user@rhel7 ~]$ gcloud projects add-iam-policy-binding anthos-dev \
--member "serviceAccount: stackdriver-service-account@anthos-dev.iam.gserviceaccount.com" \
--role "roles/stackdriver.resourceMetadata.writer"

[user@rhel7 ~]$ gcloud projects add-iam-policy-binding anthos-dev \
--member "serviceAccount: stackdriver-service-account@anthos-dev.iam.gserviceaccount.com" \
--role "roles/logging.logWriter"

[user@rhel7 ~]$ gcloud projects add-iam-policy-binding anthos-dev \
--member "serviceAccount: stackdriver-service-account@anthos-dev.iam.gserviceaccount.com" \
--role "roles/monitoring.metricWriter"
```

5.7 Deploy the Anthos Admin Workstation

The admin workstation is a vSphere VM deployed within your NetApp HCI environment that is preinstalled with all the tools necessary to administer the Anthos on VMware solution. Follow the instructions in this section to download, deploy, and configure the Anthos admin workstation.

Note: The admin workstation image is packaged as an OVA file and is only available for download to those users with whitelisted access service accounts. If you are unable to download the OVA from cloud storage, contact your project administrator or open a support ticket with Google Cloud support.

To deploy the Anthos admin workstation, complete the following steps:

1. Download the latest version of the virtual appliance here. You must first set your account to the whitelisted access service account that has permission to download the OVA.

```
[user@rhel7 ~]$ gcloud config set account 'access-service-account@anthos-dev.iam.gserviceaccount.com'
Updated property [core/account].
[user@rhel7 ~]$ gsutil cp gs://gke-on-prem-release/admin-appliance/1.1.1-gke.2/gke-on-prem-admin-appliance-vsphere-1.1.1-gke.2.{ova,ova.sig} ~/
Copying gs://gke-on-prem-release/admin-appliance/1.1.1-gke.2/gke-on-prem-admin-appliance-vsphere-1.1.1-gke.2.ova...
==> NOTE: You are downloading one or more large file(s), which would
run significantly faster if you enabled sliced object downloads. This
feature is enabled by default but requires that compiled crcmod be
installed (see "gsutil help crcmod").

- [0 files][ 40.2 MiB/ 5.1 GiB]
```

2. When the OVA file is downloaded, use `govc` to load it into your vCenter. You need to set several environment variables for your current user that provide specific information about your VMware vSphere environment deployed on NetApp HCI.

```
[user@rhel7 ~]$ export GOVC_URL=https://anthos-vc.cie.netapp.com/sdk
[user@rhel7 ~]$ export GOVC_USERNAME=administrator@vsphere.local
[user@rhel7 ~]$ export GOVC_PASSWORD=vcpasssword
[user@rhel7 ~]$ export GOVC_DATASTORE=VM_Datastore
[user@rhel7 ~]$ export GOVC_DATACENTER=NetApp-HCI-Datacenter-01
[user@rhel7 ~]$ export GOVC_RESOURCE_POOL= Anthos-Resource-Pool
```



```
[user@rhel7 ~]$ export GOVC_INSECURE=true
```



3. Because the NetApp HCI deployment uses a vDS, you need to create a custom options file that you pass as an additional argument to govc. Create a file called `options_specs`, and commit the following information to the file:

```
cat > options_spec <<EOF
{
  "DiskProvisioning": "thin",
  "MarkAsTemplate": true,
  "NetworkMapping": [
    {
      "Name": "VM Network",
      "Network": "VM_Network"
    }
  ]
}
EOF
```

4. To import the OVA file as template in VMware vSphere, enter the following command referencing the downloaded virtual appliance file, as well as the options file that you just created. The console reports upload progress, and you can also verify the upload by browsing to the Recent Tasks window in VMware vSphere.

```
[user@rhel7 ~]$ govc import.ova -options options_spec .\gke-on-prem-admin-appliance-vsphere-1.1.1-gke.2.ova
[06-11-19 10:56:39] Uploading gke-on-prem-admin-appliance-vsphere-1.1.1-gke.2.vmdk... (23%, 26.8MiB/s)
```

Recent TasksAlarms

Task Name	Target	Status	Initiator
Deploy OVF template	 gke-on-prem-admin-a...	<div><div></div></div> 51%	VSPHERE.LOCAL\Adminis...
Check new notifications	 anthos-vc.cie.netapp...	✓ Completed	VMware vSphere Update ...

All

5. With the template uploaded, we can now use Terraform to deploy the Anthos admin workstation VM. Google provides a Terraform template and variable files for environments using DHCP as well those using static IP addresses. Create a directory for these Terraform files, and copy and paste the text for both the TF and TFVARS files available here into files created with a text editor.

```
[user@rhel7 ~]$ mkdir terraform
[user@rhel7 ~]$ cd terraform
[user@rhel7 ~]$ vi terraform.tfvars
```

6. See the following `terraform.tfvars` file contents.

```
# vCenter Server username
vcenter_user = "administrator@vsphere.local"

# vCenter Server password
vcenter_password = "vcpassword"

# vCenter Server IP or hostname
vcenter_server = "https://anthos-vc.cie.netapp.com"

# Path in which the admin workstation's VM's public key should be saved
ssh_public_key_path = "~/ssh/vsphere_workstation.pub"

# Hostname for the VM
vm_name = "admin-workstation"
```

```
# vSphere datastore to use for storage
datastore = "VM_Datastore"

# vSphere datacenter in which to create the VM
datacenter = "NetApp-HCI-Datacenter-01"

# vSphere cluster in which to create the VM
cluster = "NetApp-HCI-Cluster-01"

# vSphere resource pool in which to create VM, if you are using a non-default resource pool
# If you are using the default resource pool, provide a value like "CLUSTER-NAME/Resources"
resource_pool = "Anthos-Resource-Pool"

# vSphere network to use for the VM
network = "VM_Network"

# Number of CPUs for this VM. Recommended minimum 4.
num_cpus = 4

# Memory in MB for this VM. Recommended minimum 8192.
memory = 8192

# The VM template (OVA) to clone. Change the version if you imported a different version of the
OVA.
vm_template = "gke-on-prem-admin-appliance-vsphere-1.1.1-gke.2"

[user@rhel7 ~]$ vi terraform.tf
```

7. See the following terraform.tf file contents.

```
#####
##### VARIABLES #####
#####

# The following variables are declared in the accompanying TFVARS file

# vCenter Server username
variable "vcenter_user" { }

# vCenter Server password
variable "vcenter_password" { }

# vCenter Server address
variable "vcenter_server" { }

# Path in which the VM's public key should be saved
variable "ssh_public_key_path" { default = "~/.ssh/vsphere_workstation.pub" }

# vSphere network to use for the VM
variable "network" { default = "VM Network" }

# Hostname for the VM
variable "vm_name" { default = "vsphere-workstation" }

# vSphere datacenter in which to create the admin workstation VM
variable "datacenter" { }

# vSphere datastore to use for storage
variable "datastore" { }

# vSphere cluster in which to create the VM
variable "cluster" { }

# vSphere resource pool in which to create the VM
variable "resource_pool" { }

# Number of CPUs for this VM. Recommended minimum 4.
variable "num_cpus" { default = 4 }
```

```

# Memory in MB for this VM. Recommended minimum 8192.
variable "memory" { default = 8192 }

# The VM template (OVA) to clone
variable "vm_template" { }

#####
#####

provider "vsphere" {
  version      = "~> 1.5"
  user         = "${var.vcenter_user}"
  password     = "${var.vcenter_password}"
  vcenter_server = "${var.vcenter_server}"

  # if you have a self-signed cert
  allow_unverified_ssl = true
}

### vSphere Data ###

data "vsphere_datastore" "datastore" {
  name           = "${var.datastore}"
  datacenter_id = "${data.vsphere_datacenter.dc.id}"
}

data "vsphere_datacenter" "dc" {
  name = "${var.datacenter}"
}

data "vsphere_compute_cluster" "cluster" {
  name           = "${var.cluster}"
  datacenter_id = "${data.vsphere_datacenter.dc.id}"
}

data "vsphere_resource_pool" "pool" {
  name           = "${var.resource_pool}"
  datacenter_id = "${data.vsphere_datacenter.dc.id}"
}

data "vsphere_network" "network" {
  name           = "${var.network}"
  datacenter_id = "${data.vsphere_datacenter.dc.id}"
}

data "vsphere_virtual_machine" "template_from_ovf" {
  name           = "${var.vm_template}"
  datacenter_id = "${data.vsphere_datacenter.dc.id}"
}

data "template_file" "dhcp_ip_config" {
  template = <<EOF
network:
  version: 2
  ethernet:
    ens192:
      dhcp4: true
EOF
}

data "template_file" "user_data" {
  template = <<EOF
#cloud-config
apt:
  primary:
    - arches: [default]
      uri: http://us-west1.gce.archive.ubuntu.com/ubuntu/
write_files:
  - path: /etc/netplan/99-dhcp.yaml
    permissions: '0644'

```

```

        encoding: base64
        content: |
            ${dhcp_ip_config}
    runcmd:
    - netplan apply
    - /var/lib/gke/guest-startup.sh
EOF
vars = {
    dhcp_ip_config = "${base64encode(data.template_file.dhcp_ip_config.rendered)}"
}
}

### vSphere Resources ###

resource "vsphere_virtual_machine" "vm" {
    name = "${var.vm_name}"
    resource_pool_id = "${data.vsphere_resource_pool.pool.id}"
    datastore_id = "${data.vsphere_datastore.datastore.id}"
    num_cpus = "${var.num_cpus}"
    memory = "${var.memory}"
    guest_id = "${data.vsphere_virtual_machine.template_from_ovf.guest_id}"
    enable_disk_uuid = "true"
    scsi_type = "${data.vsphere_virtual_machine.template_from_ovf.scsi_type}"
    network_interface {
        network_id = "${data.vsphere_network.network.id}"
        adapter_type = "${data.vsphere_virtual_machine.template_from_ovf.network_interface_types[0]}"
    }

    wait_for_guest_net_timeout = 15

    nested_hv_enabled = false
    cpu_performance_counters_enabled = false

    disk {
        label = "disk0"
        size = "${max(50, data.vsphere_virtual_machine.template_from_ovf.disks.0.size)}"
        eagerly_scrub = "${data.vsphere_virtual_machine.template_from_ovf.disks.0.eagerly_scrub}"
        thin_provisioned =
        "${data.vsphere_virtual_machine.template_from_ovf.disks.0.thin_provisioned}"
    }

    cdrom {
        client_device = true
    }

    vapp {
        properties = {
            hostname = "${var.vm_name}"
            public-keys = "${file(var.ssh_public_key_path)}"
            user-data = "${base64encode(data.template_file.user_data.rendered)}"
        }
    }

    clone {
        template_uuid = "${data.vsphere_virtual_machine.template_from_ovf.id}"
    }
}

output "ip_address" {
    value = "${vsphere_virtual_machine.vm.default_ip_address}"
}

```

Note: Values specific to the deployed environment have been added to the `terraform.tfvars` file. However, you should not modify the `terraform.tf` file in any manner.

8. Create an SSH public/private keypair used to log in to the admin workstation after it is deployed. Name the public key so that it matches the variable that was assigned in the `terraform.tfvars` file.

```
[user@rhel7 ~]$ ssh-keygen -t rsa -f ~/.ssh/vsphere_workstation -N ""
Generating public/private rsa key pair.
Your identification has been saved in /home/user/.ssh/vsphere_workstation2.
Your public key has been saved in /home/user/.ssh/vsphere_workstation2.pub.
The key fingerprint is:
SHA256:qEk8G13LhwiKqf85ekHHZkIZduX2MkZUxGNEHvFT2vw user@rhel7
The key's randomart image is:
+---[RSA 2048]-----+
|  oo.o+*B. . . |
|  .o. o .+o = |
|  ... B.o.+ o |
| o ooo=B * . . |
|o ..==+ S . E|
|. ..* . |
|. +. |
|. o. |
| o+o. |
+----[SHA256]-----+
```

9. Navigate to the directory created to host the TF and TFVARS files. Within this directory, initialize Terraform and use it to launch the deployment of the admin workstation VM.

```
[user@rhel7 ~]$ cd terraform
[user@rhel7 terraform]$ ls
terraform.tf  terraform.tfvars
[user@rhel7 terraform]$ terraform init && terraform apply -auto-approve -input=false
Initializing the backend...
Initializing provider plugins...
The following providers do not have any version constraints in configuration,
so the latest version was installed.
To prevent automatic upgrades to new major versions that may contain breaking
changes, it is recommended to add version = "..." constraints to the
corresponding provider blocks in configuration, with the constraint strings
suggested below.
* provider.template: version = "~> 2.1"
Terraform has been successfully initialized!

data.template_file.dhcp_ip_config: Refreshing state...
data.template_file.user_data: Refreshing state...
data.vsphere_datacenter.dc: Refreshing state...
data.vsphere_resource_pool.pool: Refreshing state...
data.vsphere_datastore.datastore: Refreshing state...
data.vsphere_virtual_machine.template_from_ovf: Refreshing state...
data.vsphere_network.network: Refreshing state...
data.vsphere_compute_cluster.cluster: Refreshing state...
vsphere_virtual_machine.vm: Creating...
vsphere_virtual_machine.vm: Still creating... [10s elapsed]
vsphere_virtual_machine.vm: Still creating... [20s elapsed]
vsphere_virtual_machine.vm: Still creating... [30s elapsed]
vsphere_virtual_machine.vm: Still creating... [40s elapsed]
vsphere_virtual_machine.vm: Creation complete after 49s [id=42118cfa-d464-b815-f7b1-37cd85b2943a]

Warning: "vcenter_server": [DEPRECATED] This field has been renamed to vsphere_server.

Apply complete! Resources: 1 added, 0 changed, 0 destroyed.

Outputs:

ip_address = 10.63.172.21
```

5.8 Deploy the Admin and the First User Cluster

All Kubernetes clusters deployed as a part of the Anthos solution are deployed from the Anthos admin workstation that you just created. A user logs into the admin workstation using SSH, the public key created in a previous step, and the IP address provided at the end of the VM deployment. They can then begin creating their first clusters.

Note: There are specific procedures for deploying clusters that use static IP addresses [here](#), and procedures for environments with DHCP can be found [here](#). In this guide, we use the second set of instructions.

To deploy the initial admin and first user cluster, complete the following steps:

1. Login to the admin workstation using the SSH public key and the IP address output at the end of Terraform deployment.

```
[user@rhel7 ~]$ ssh -i ~/.ssh/vsphere_workstation ubuntu@10.63.172.21
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

36 packages can be updated.
23 updates are security updates.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@admin-workstation:~$
```

2. Log in with the `gcloud auth` command as you did before from your deployment workstation by copying the URL into a web browser, signing into your Google account, and pasting the verification code back into the workstation.

```
ubuntu@admin-workstation:~$ gcloud auth login
Go to the following link in your browser:

https://accounts.google.com/o/oauth2/auth?code_challenge=Q1F7H-
CMUMuArasQD6AzHA0avKolGfDqUyUgjFxf9ZI&prompt=select_account&code_challenge_method=S256&access_typ
e=offline&redirect_uri=urn%3Aietf%3Aawg%3Aoauth%3A2.0%3Aaob&response_type=code&client_id=325559405
59.apps.googleusercontent.com&scope=https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+http
s%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcloud-
platform+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fappengine.admin+https%3A%2F%2Fwww.googleapis.c
om%2Fauth%2Fcompute+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth

Enter verification code: 6/swFG_ZKZyd0eblfuXsgtnBgYrIt1XwFQeB5ASrEQaaDfa09aio0bnNg

WARNING: `gcloud auth login` no longer writes application default credentials.
If you need to use ADC, see:
  gcloud auth application-default --help

You are now logged in as [user@netapp.com].
Your current project is [None]. You can change this setting by running:
  $ gcloud config set project PROJECT_ID
```

3. Set the project that you intend to deploy your clusters in for Anthos on VMware, because the project is not set by default when you log in.

```
ubuntu@admin-workstation:~$ gcloud config set project anthos-dev
Updated property [core/project].
```

4. Register `gcloud` as a Docker credential helper, which enables it to manage the credentials for Docker registries used for deployment. This way, the default credential store is not used for operations involving the credentials of the specified registries.

```
ubuntu@admin-workstation:~$ gcloud auth configure-docker
The following settings will be added to your Docker config file
located at [/home/ubuntu/.docker/config.json]:
{
  "credHelpers": {
```

```

    "gcr.io": "gcloud",
    "us.gcr.io": "gcloud",
    "eu.gcr.io": "gcloud",
    "asia.gcr.io": "gcloud",
    "staging-k8s.gcr.io": "gcloud",
    "marketplace.gcr.io": "gcloud"
  }
}

```

Do you want to continue (Y/n)? y

Docker configuration file updated.

Note: By default, Anthos on VMware uses a pre-existing, Google-owned container image registry that requires no additional setup. If you choose to use a private Docker registry for deployment, then you must configure that registry separately based on instructions found [here](#). This step is beyond the scope of this deployment guide.

5. In the next step to deploy an admin cluster, create a private key file in the JSON format for each of the service accounts created in the prerequisites section.

```

ubuntu@admin-workstation:~$ gcloud iam service-accounts list
NAME                                EMAIL                                DISABLED
stackdriver-service-account@anthos-dev.iam.gserviceaccount.com  False
register-service-account@anthos-dev.iam.gserviceaccount.com     False
access-service-account@anthos-dev.iam.gserviceaccount.com        False
connect-service-account@anthos-dev.iam.gserviceaccount.com       False

ubuntu@admin-workstation:~$ gcloud iam service-accounts keys create access-key.json --iam-account
access-service-account@anthos-dev.iam.gserviceaccount.com
created key [8d5f8ce039dd98766e18a3c5ee6794912fb8d095] of type [json] as [access-key.json] for
[access-service-account@anthos-dev.iam.gserviceaccount.com]
ubuntu@admin-workstation:~$ gcloud iam service-accounts keys create register-key.json --iam-
account register-service-account@anthos-dev.iam.gserviceaccount.com
created key [f08b494c665321f83bcb8c8526ba21185b456a11] of type [json] as [register-key.json] for
[register-service-account@anthos-dev.iam.gserviceaccount.com]
ubuntu@admin-workstation:~$ gcloud iam service-accounts keys create connect-key.json --iam-
account connect-service-account@anthos-dev.iam.gserviceaccount.com
created key [c9640021ff6157d3df2a15db49f5c85b7b1495c2] of type [json] as [connect-key.json] for
[connect-service-account@anthos-dev.iam.gserviceaccount.com]
ubuntu@admin-workstation:~$ gcloud iam service-accounts keys create stackdriver-key.json --iam-
account stackdriver-service-account@anthos-dev.iam.gserviceaccount.com
created key [3c9427dfdef161d139ff998be896565c1df0b122] of type [json] as [stackdriver-key.json]
for [stackdriver-service-account@anthos-dev.iam.gserviceaccount.com]

```

6. For the next step, you must use the access service key created in the previous step to activate the associated service account.

```

ubuntu@admin-workstation:~$ gcloud auth activate-service-account --key-file=access-key.json
Activated service account credentials for: [access-service-account@anthos-
dev.iam.gserviceaccount.com]

```

7. The deployment of the first clusters is performed using inputs from a config file generated by GKE. A generic config file can be created with no additional input, or an existing config file can be referenced to create additional clusters.

```

ubuntu@admin-workstation:~$ gkectl create-config
ubuntu@admin-workstation:~$ ls
access-key.json  config.yaml  connect-key.json  register-key.json  stackdriver-key.json

```

8. The config.yaml file created by running the previous command has several variables that must be customized for the current environment.
 - a. First, you must determine the full path location and the name of the current GKE bundle that is deployed into the environment. The file exists in the /var/lib/gke/bundles directory on the admin workstation.

```

ubuntu@admin-workstation:~$ ls /var/lib/gke/bundles
gke-onprem-vsphere-1.1.1-gke.2-full.tgz  gke-onprem-vsphere-1.1.1-gke.2.tgz

```

- b. Next, you must get the fully recognized host name or IP address of our vCenter Server as displayed in its default SSL certificate. Connect to vSphere and dump the certificate contents into a file called `vcenter.pem`. Examining this file gives you the information that you need for the value of Subject: CN (common name).

```
ubuntu@admin-workstation:~$ true | openssl s_client -connect anthos-vc.cie.netapp.com:443 -
showcerts 2>/dev/null | sed -ne '/-BEGIN/,/-END/p' > vcenter.pem
ubuntu@admin-workstation:~$ openssl x509 -in vcenter.pem -text -noout | grep Subject:\ CN
Subject: CN = anthos-vc.cie.netapp.com, C = US
```

Note: If the value added to the `config.yaml` file does not match that of the CN found in the certificate, communication with the vCenter server fails.

9. With the information from those two commands and the generated `vcenter.pem` file, we can now edit the `config.yaml` file to prepare for deployment. Editing this file is very similar to the edits that you performed to the `terraform.tfvars` file to provide specifics regarding the VMware vCenter instance deployed in NetApp HCI.

Note: When deploying the cluster, determine which IP addresses to use for the control plane and ingress VIPs for both the admin and user cluster. Also determine the compute and memory resources that must be reserved for each node deployed, because it is not possible to edit a cluster after it has been deployed.

```
# Absolute path to a GKE bundle on disk
bundlepath: "/var/lib/gke/bundles/gke-onprem-vsphere-1.1.1-gke.2-full.tgz"
# Specify which vCenter resources to use for deployment
vcenter:
  # The credentials and address GKE should use to connect to vCenter
  credentials:
    address: "anthos-vc.cie.netapp.com"
    username: "administrator@vsphere.local"
    password: "vcpass"
  datacenter: "NetApp-HCI-Datacenter-01"
  datastore: "VM_Datastore"
  cluster: "NetApp-HCI-Cluster-01"
  network: "VM_Network"
  resourcepool: "Anthos Resource Pool"
  # Provide the name for the persistent disk to be used by the deployment (ending
  # in .vmdk). Any directory in the supplied path must be created before deployment.
  # Not required when adding additional user clusters
  datadisk: "anthos-admin-data-disk.vmdk"
  # Provide the path to vCenter CA certificate pub key for SSL verification
  cacertpath: "/home/ubuntu/vcenter.pem"
# Specify the proxy configuration.
proxy:
  # The URL of the proxy
  url: ""
  # The domains and IP addresses excluded from proxying
  noproxy: ""
# Specify admin cluster settings for a fresh GKE On-Prem deployment. Omit this section
# and use the --adminconfig flag when adding a new user cluster to an existing deployment
admincluster:
  # In-Cluster vCenter configuration
  vcenter:
    # If specified it overwrites the network field in global vcenter configuration
    network: ""
    # # The absolute or relative path to the yaml file to use for static IP allocation.
    # # Do not include if using DHCP
    # ipblockfilepath: ""
    # # Specify pre-defined nodeports if using "manual" load balancer mode
    # manullbspec:
    #   ingresshttpnodeport: 32527
    #   ingresshttpsnodeport: 30139
    #   controlplanenodeport: 30968
    #   addonsnodeport: 31405
  # Specify the already-existing partition and credentials to use with F5
  bigip:
    # To re-use credentials across clusters we recommend using YAML node anchors.
```



```

# See https://yaml.org/spec/1.2/spec.html#id2785586
credentials:
  address: "172.21.224.22"
  username: "admin"
  password: "lbpass"
  partition: "Anthos-Admin-Part"
# # Optionally specify a pool name if using SNAT
# # snatpoolname: ""
# The VIPs to use for load balancing
vips:
  # Used to connect to the Kubernetes API
  controlplanevip: "10.63.172.98"
  # Shared by all services for ingress traffic
  ingressvip: "10.63.172.99"
  # # Used for admin cluster addons (needed for multi cluster features). Must be the same
  # # across clusters
  # addonsvip: ""
# The Kubernetes service CIDR range for the cluster. Must not overlap with the pod
# CIDR range
serviceiprange: 10.96.232.0/24
# The Kubernetes pod CIDR range for the cluster. Must not overlap with the service
# CIDR range
podiprange: 192.168.0.0/16
# Specify settings when deploying a new user cluster. Used both with a fresh deployment
# or when adding a new cluster to an existing deployment.
usercluster:
  antiaffinitygroups:
    enabled: false
  # In-Cluster vCenter configuration
  vcenter:
    # If specified it overwrites the network field in global vcenter configuration
    network: ""
  # # The absolute or relative path to the yaml file to use for static IP allocation.
  # # Do not include if using DHCP
  # ipblockfilepath: ""
  # # Specify pre-defined nodeports if using "manual" load balancer mode
  # manullbspec:
  #   ingresshttpnodeport: 30243
  #   ingresshttpsnodeport: 30879
  #   controlplanenodeport: 30562
  #   addonsnodeport: 0
  # Specify the already-existing partition and credentials to use with F5
bigip:
  # To re-use credentials across clusters we recommend using YAML node anchors.
  # See https://yaml.org/spec/1.2/spec.html#id2785586
  credentials:
    address: "172.21.224.22"
    username: "admin"
    password: "lbpass"
    partition: "Anthos-Cluster01-Part"
  # # Optionally specify a pool name if using SNAT
  # # snatpoolname: ""
# The VIPs to use for load balancing
vips:
  # Used to connect to the Kubernetes API
  controlplanevip: "10.63.172.105"
  # Shared by all services for ingress traffic
  ingressvip: "10.63.172.106"
  # # Used for admin cluster addons (needed for multi cluster features). Must be the same
  # # across clusters
  # addonsvip: ""
# A unique name for this cluster
clustername: "anthos-cluster01"
# User cluster master nodes must have either 1 or 3 replicas
masternode:
  cpus: 4
  memorymb: 8192
  # How many machines of this type to deploy
  replicas: 1
# The number of worker nodes to deploy and their size. Min. 2 replicas
workernode:

```

```

cpus: 4
memorymb: 8192
# How many machines of this type to deploy
replicas: 3
# The Kubernetes service CIDR range for the cluster
serviceiprange: 10.96.0.0/12
# The Kubernetes pod CIDR range for the cluster
podiprange: 192.168.0.0/16
# # Uncomment this section to use OIDC authentication
# oidc:
#   issuerurl: ""
#   kubectlredirecturl: ""
#   clientid: ""
#   clientsecret: ""
#   username: ""
#   usernameprefix: ""
#   group: ""
#   groupprefix: ""
#   scopes: ""
#   extraparams: ""
#   # Set value to string "true" or "false"
#   usehttpproxy: ""
#   # # The absolute or relative path to the CA file (optional)
#   # capath: ""
#   # Optionally provide an additional serving certificate for the API server
#   sni:
#   certpath: ""
#   keypath: ""
# Which load balancer mode to use "Manual" or "Integrated"
lbmode: Integrated
# Specify which GCP project to connect your GKE clusters to
gkeconnect:
  projectid: "anthos-dev"
  # The absolute or relative path to the key file for a GCP service account used to
  # register the cluster
  registerserviceaccountkeypath: "/home/ubuntu/register-key.json"
  # The absolute or relative path to the key file for a GCP service account used by
  # the GKE connect agent
  agentserviceaccountkeypath: "/home/ubuntu/connect-key.json"
# Specify which GCP project to connect your logs and metrics to
stackdriver:
  projectid: "anthos-dev"
  # A GCP region where you would like to store logs and metrics for this cluster.
  clusterlocation: "us-east1"
  enablevpc: false
  # The absolute or relative path to the key file for a GCP service account used to
  # send logs and metrics from the cluster
  serviceaccountkeypath: "/home/ubuntu/stackdriver-key.json"
# # Optionally use a private Docker registry to host GKE images
# privateregistryconfig:
#   # Do not include the scheme with your registry address
#   credentials:
#     address: ""
#     username: ""
#     password: ""
#   # The absolute or relative path to the CA certificate for this registry
#   cacertpath: ""
# The absolute or relative path to the GCP service account key that will be used to
# pull GKE images
gcrkeypath: "/home/ubuntu/access-key.json"
# Configure kubernetes apiserver audit logging
cloudauditlogging:
  projectid: ""
  # A GCP region where you would like to store audit logs for this cluster.
  clusterlocation: ""
  # The absolute or relative path to the key file for a GCP service account used to
  # send audit logs from the cluster
  serviceaccountkeypath: ""

```

10. Because spacing in YAML files can be very important, you can check the syntax of the config file by running the following command. If the command outputs any failures, be sure to examine the file and make any needed corrections.

```
ubuntu@admin-workstation:~$ gkectl check-config --config config.yaml
- Validation Category: Config Check
  - [SUCCESS] Config

- Validation Category: Docker Registry
  - [SUCCESS] gcr.io/gke-on-prem-release access

- Validation Category: vCenter
  - [SUCCESS] Credentials
  - [SUCCESS] Datacenter
  - [SUCCESS] Datastore
  - [SUCCESS] Data Disk
  - [SUCCESS] Resource Pool
  - [SUCCESS] Network

- Validation Category: F5 BIG-IP
  - [SUCCESS] Credentials
  - [SUCCESS] Partition

- Validation Category: Network Configuration
  - [SUCCESS] CIDR, VIP and static IP (availability and overlapping)

- Validation Category: VIPs
  - [SUCCESS] ping (availability)

- Validation Category: Node IPs
  - [SKIPPED] ping (availability): All specified clusters use DHCP.

Some validations FAILED or SKIPPED. Check report above.
```

Note: Using DHCP skips the step to validate node IP availability. This is an expected behavior and deployment can continue.

11. Preparing the cluster for deployment and deploying the cluster are performed with two commands:

- a. The `gkectl prepare` command initializes the vSphere environment by uploading the node OS image, marking it as a template, and validating the build attestations for all container images.

```
ubuntu@admin-workstation:~$ gkectl prepare --config config.yaml
- Validation Category: Config Check
  - [SUCCESS] Config

- Validation Category: Docker Registry
  - [SUCCESS] gcr.io/gke-on-prem-release access

- Validation Category: vCenter
  - [SUCCESS] Credentials
  - [SUCCESS] Datacenter
  - [SUCCESS] Datastore
  - [SUCCESS] Data Disk
  - [SUCCESS] Resource Pool
  - [SUCCESS] Network

All validations SUCCEEDED.
Downloading OS image gke-on-prem-osimage-1.13.7-gke.20-20190816-8138298d96.ova...  DONE

Setting up OS image as a VM template in vSphere...  DONE
```

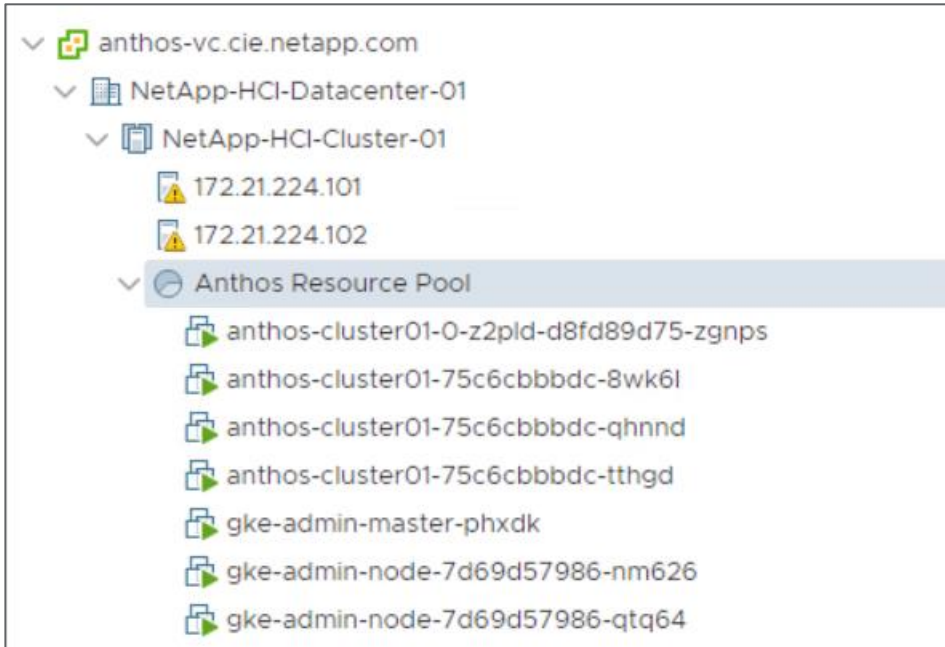
- b. The `gkectl create cluster` command deploys the cluster as depicted in the `config.yaml` file.

```
ubuntu@admin-workstation:~$ gkectl create cluster --config config.yaml
```

- c. The process runs for several minutes and can be monitored on screen and in vCenter by watching the resource pool as the VMs populate. When complete, you should be able to see the gke-admin cluster (three nodes) and the first user cluster (four nodes).

Note: During the deployment process, the standard out might display several messages about the current node not being available or not being ready. This is normal and happens when the control plane checks for machines that have not yet completed deployment or received DHCP addresses.

Note: When using DHCP, if a deployment fails because nodes cannot be reached, there might not be enough available addresses in the pool. Leases for previously failed deployments might need to be cleared manually to allow for additional deployment attempts.



- d. You can access and execute commands against the user cluster that has been deployed using the kubectl command line tool and the kubeconfig file generated by the process (stored in the working directory).

```
ubuntu@Anthos-Admin-Workstation:~$ kubectl get nodes --kubeconfig anthos-cluster01-kubeconfig
NAME                                STATUS    ROLES    AGE    VERSION
anthos-cluster01-75c6cbbddc-8wk6l  Ready    <none>    149m   v1.13.7-gke.20
anthos-cluster01-75c6cbbddc-qhnnd  Ready    <none>    149m   v1.13.7-gke.20
anthos-cluster01-75c6cbbddc-tthgd  Ready    <none>    149m   v1.13.7-gke.20
```

5.9 Deploy Additional User Clusters

With Anthos, organizations can scale their environments to incorporate multiple user clusters and segregate workloads between teams. A single admin cluster can support up to five user clusters, and each user cluster can support up to twenty-five nodes.

1. To add an additional cluster to your deployment, copy the `config.yaml` file to a new file named `anthos-cluster02-config.yaml`.

```
ubuntu@Anthos-Admin-Workstation:~$ cp config.yaml anthos-cluster02-config.yaml
```

2. Make the following edits to the newly created file:
 - a. Comment out the sections that refer to the existing admin cluster with (#).
 - b. When you get to the `usercluster` section, update the following fields:

- i) Update the partition name under the bigip section.
- ii) Update the controlplanevip and ingressvip values under the vip section.
- iii) Update the clustername value.

```

usercluster:
# In-Cluster vCenter configuration
vcenter:
# If specified it overwrites the network field in global vcenter configuration
network: ""
# The absolute or relative path to the yaml file to use for static IP allocation.
# Do not include if using DHCP
# ipblockfilepath: ""
# Specify pre-defined nodeports if using "manual" load balancer mode
# manullbspec:
#   ingresshttpnodeport: 30243
#   ingresshttpsnodeport: 30879
#   controlplanenodeport: 30562
#   addonsnodeport: 0
# Specify the already-existing partition and credentials to use with F5
bigip:
# To re-use credentials across clusters we recommend using YAML node anchors.
# See https://yaml.org/spec/1.2/spec.html#id2785586
credentials:
  address: "172.21.224.22"
  username: "admin"
  password: "NetApp!23"
partition: "Anthos-Cluster02-Part"
# Optionally specify a pool name if using SNAT
# snatpoolname: ""
# The VIPs to use for load balancing
vips:
# Used to connect to the Kubernetes API
controlplanevip: "10.63.172.108"
# Shared by all services for ingress traffic
ingressvip: "10.63.172.109"
# Used for admin cluster addons (needed for multi cluster features). Must be the same
# across clusters
# addonsvip: ""
# A unique name for this cluster
clustername: "anthos-cluster02"
# User cluster master nodes must have either 1 or 3 replicas
masternode:
  cpus: 4
  memorymb: 8192
# How many machines of this type to deploy
  replicas: 1
# The number of worker nodes to deploy and their size. Min. 2 replicas
workernode:
  cpus: 4
  memorymb: 8192
# How many machines of this type to deploy
  replicas: 3
# The Kubernetes service CIDR range for the cluster
serviceiprange: 10.96.0.0/12
# The Kubernetes pod CIDR range for the cluster
podiprange: 192.168.0.0/16

```

3. Run the following command to check the config file again to verify that there are no syntax errors. Because you have removed the admin section, you must reference the kubeconfig file for the admin cluster named kubeconfig (found in the working directory).

```

ubuntu@Anthos-Admin-Workstation:~$ gkectl check-config --config anthos-cluster02-config.yaml --
kubeconfig kubeconfig
- Validation Category: Config Check
  - [SUCCESS] Config
- Validation Category: Docker Registry
  - [SUCCESS] gcr.io/gke-on-prem-release access

```

```

- Validation Category: vCenter
  - [SUCCESS] Credentials
  - [SUCCESS] Datacenter
  - [SUCCESS] Datastore
  - [FAILURE] Data Disk: vCenter data disk already exists
  - [SUCCESS] Resource Pool
  - [SUCCESS] Network

- Validation Category: F5 BIG-IP
  - [SUCCESS] Credentials
  - [SUCCESS] Partition

- Validation Category: Network Configuration
  - [SUCCESS] CIDR, VIP and static IP (availability and overlapping)

- Validation Category: VIPs
  - [SUCCESS] ping (availability)

- Validation Category: Node IPs
  - [SUCCESS] ping (availability)

Some validations FAILED or SKIPPED. Check report above.

```

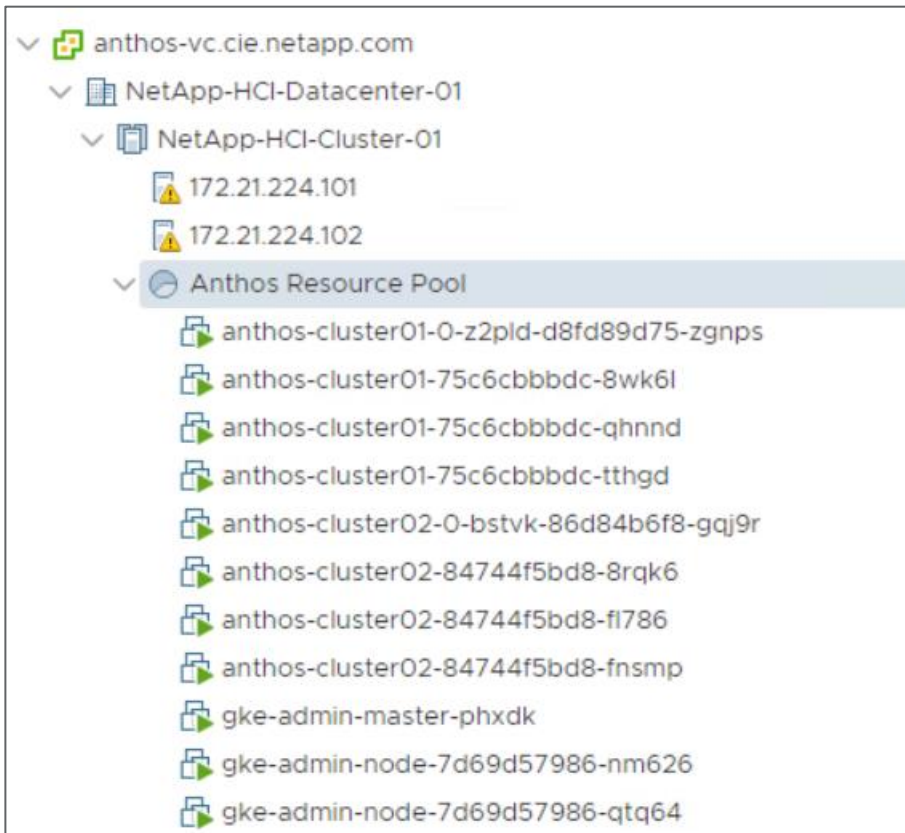
4. If all the checks succeed as expected, you can deploy this new user cluster in a manner very similar to the first cluster creation, referencing the `kubeconfig` file from the admin cluster.

```

ubuntu@Anthos-Admin-Workstation:~$ gkectl create cluster --config anthos-cluster02-config.yaml --
kubeconfig kubeconfig

```

5. As with the previous deployment, the process runs for several minutes and can be monitored on screen and in vCenter by watching the resource pool as the VMs populate. When complete, you should be able to see the new user cluster (four nodes).



6. You can access and execute commands against the deployed user cluster using the `kubectl` command line tool and the `kubeconfig` file generated by the process (stored in the working directory).

```
ubuntu@Anthos-Admin-Workstation:~$ kubectl get nodes --kubeconfig anthos-cluster02-kubeconfig
NAME                                STATUS    ROLES    AGE      VERSION
anthos-cluster02-84744f5bd8-8rqk6  Ready    <none>   9m16s    v1.13.7-gke.20
anthos-cluster02-84744f5bd8-f1786  Ready    <none>   9m28s    v1.13.7-gke.20
anthos-cluster02-84744f5bd8-fnsmp  Ready    <none>   9m21s    v1.13.7-gke.20
```

5.10 Enable Access to the Cluster with the GKE Console

After clusters are deployed and registered with Google Cloud, they must be logged into with the Google Cloud console to be managed and to receive additional cluster details. The official procedure to gain access to Anthos user clusters after they are deployed is detailed [here](#).

Note: The project and the specific user must be whitelisted to access on-premises clusters in the Google Cloud console and use Anthos on VMware services. If you are unable to see the clusters after they are deployed, you might need to open a support ticket with Google.

Figure 5) Non-whitelisted view.

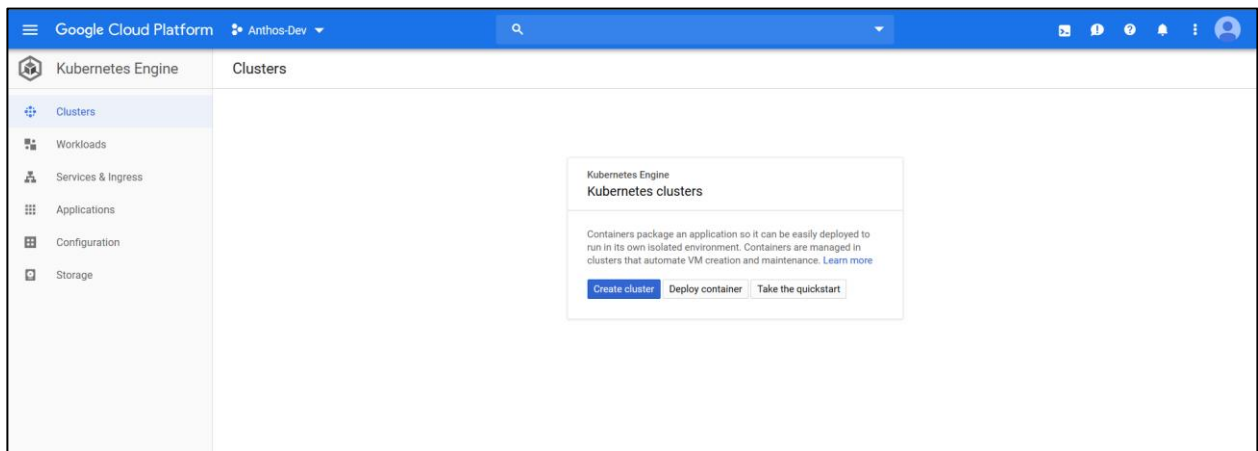


Figure 6) View of clusters.

Kubernetes clusters								
+ CREATE CLUSTER + DEPLOY REGISTER CLUSTER REFRESH DELETE								
Filter by label or name								
<input type="checkbox"/> Name ^	Location	Cluster type	Cluster size	Total cores	Total memory	Notifications	Labels	
<input type="checkbox"/> anthos-cluster01	registered	Anthos	-	-	-	Log in to cluster	provider: gke_on_prem	Login
<input type="checkbox"/> anthos-cluster02	registered	Anthos	-	-	-	Log in to cluster	provider: gke_on_prem	Login

To enable access to your user clusters using the GKE console, complete the following steps:

1. Create a `node-reader.yaml` file that gives you the ability to access the cluster.

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: node-reader
rules:
- apiGroups: [""]
  resources: ["nodes"]
  verbs: ["get", "list", "watch"]
```


Log in to cluster

Choose the method you want to use for authentication to the cluster

☒ Token

Jxc9By6LgOW0nyaH4__gexy4ula61fNLKV2SKe4_gAN41ffOCKe4Tq8sa6zM0-8g

☐ Basic authentication

☐ Authenticate with Identity Provider configured for the cluster

CLOSE
LOGIN

- After login is complete, you see a green check mark next to the cluster name, and information is displayed about the physical environment. Clicking the cluster name displays more verbose information.

Kubernetes cluster details
REFRESH
DELETE
DEPLOY
LOGOUT

Details
Storage
Nodes

Name	anthos-cluster01
Endpoint	kubernetes.default.svc.cluster.local
Master version	v1.13.7-gke.20
Total number of nodes	3
Total cores	12 CPU
Total memory	25.09 GB

Login information

Status	✔ Authenticated Logout
Authentication method	Bearer token

Labels

provider : gke_on_prem

5.11 Install and Configure NetApp Trident Storage Provisioner

Trident is a storage orchestrator for containers. With Trident, microservices and containerized applications can take advantage of enterprise-class storage services provided by the full NetApp portfolio of storage systems for persistent storage mounts. Depending on an application’s requirements, Trident dynamically provisions storage for ONTAP-based products such as NetApp AFF and FAS systems and Element storage systems like NetApp SolidFire® and NetApp HCI.

To install Trident on the deployed user cluster and provision a persistent volume, complete the following steps:

- Download the installation archive to the admin workstation and extract the contents. The current version of Trident is 19.10, which can be downloaded [here](#).

```

ubuntu@Anthos-Admin-Workstation:~$ wget
https://github.com/NetApp/trident/releases/download/v19.10.0/trident-installer-19.10.0.tar.gz
--2019-11-07 16:45:33-- https://github.com/NetApp/trident/releases/download/v19.10.0/trident-
installer-19.10.0.tar.gz
Resolving github.com (github.com)... 140.82.118.4
Connecting to github.com (github.com)|140.82.118.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github-production-release-asset-2e65be.s3.amazonaws.com/77179634/4d3b5900-
Resolving github-production-release-asset-2e65be.s3.amazonaws.com (github-production-release-
asset-2e65be.s3.amazonaws.com)... 52.216.81.8
Connecting to github-production-release-asset-2e65be.s3.amazonaws.com (github-production-release-
asset-2e65be.s3.amazonaws.com)|52.216.81.8|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68903585 (66M) [application/octet-stream]
Saving to: 'trident-installer-19.10.0.tar.gz.1'

trident-installer-19.10.0.tar 100%[=====>] 65.71M
53.8MB/s in 1.2s

2019-11-07 16:45:35 (53.8 MB/s) - 'trident-installer-19.10.0.tar.gz.1' saved [68903585/68903585]

ubuntu@Anthos-Admin-Workstation:~$ tar -xf trident-installer-19.10.0.tar.gz

```

2. 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@Anthos-Admin-Workstation:~$ export KUBECONFIG=~/.anthos-cluster01-kubeconfig

```

3. Navigate to the Trident directory and execute the tridentctl tool to install trident to your cluster. NetApp recommends installing Trident into its own namespace within the cluster. You can then verify that the install finished correctly.

```

ubuntu@Anthos-Admin-Workstation:~$ cd trident-installer --csi
ubuntu@Anthos-Admin-Workstation:~/trident-installer$ ./tridentctl install -n trident
INFO Starting Trident installation.                namespace=trident
INFO Created namespace.                            namespace=trident
INFO Created service account.
INFO Created cluster role.
INFO Created cluster role binding.
INFO Created custom resource definitions.           namespace=trident
INFO Added finalizers to custom resource definitions.
INFO Created Trident deployment.
INFO Waiting for Trident pod to start.
INFO Trident pod started.                          namespace=trident pod=trident-79c76ff764-77sgl
INFO Waiting for Trident REST interface.
INFO Trident REST interface is up.                  version=19.10.0
INFO Trident installation succeeded.
ubuntu@Anthos-Admin-Workstation:~/trident-installer$ ./tridentctl version -n trident
+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 19.10.0        | 19.10.0        |
+-----+-----+

```

4. The next step in enabling Trident integration with the NetApp HCI solution and Anthos is to create a backend that enables communication with the storage system. There are sample backend files available in the downloaded installation archive in the sample-input folder. Copy the backend-solidfire.json to your working directory and edit it to provide information detailing the storage system environment.

```

ubuntu@Anthos-Admin-Workstation:~/trident-installer$ cp sample-input/backend-solidfire.json ./
ubuntu@Anthos-Admin-Workstation:~/trident-installer$ vi backend-solidfire.json

```

5. Edit the user, password, and MVIP value on the EndPoint line.
6. Edit the SVIP value.

```

{
  "version": 1,

```

```

"storageDriverName": "solidfire-san",
"Endpoint": "https://trident:password@172.21.224.150/json-rpc/8.0",
"SVIP": "10.63.172.100:3260",
"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}}]
}

```

7. With this back-end file in place, run the following command to create your first backend.

```

ubuntu@Anthos-Admin-Workstation:~/trident-installer$ ./tridentctl -n trident create backend -f
backend.json
+-----+-----+-----+-----+-----+-----+
| NAME           | STORAGE DRIVER | UUID                               | STATE | VOLUMES |
+-----+-----+-----+-----+-----+-----+
| solidfire-backend | solidfire-san  | a5f9e159-c8f4-4340-a13a-c615fef0f433 | online | 0       |
+-----+-----+-----+-----+-----+-----+

```

8. 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@Anthos-Admin-Workstation:~/trident-installer$ cp sample-input/storage-class-csi.yaml.templ
./storage-class-basic.yaml
ubuntu@Anthos-Admin-Workstation:~/trident-installer$ vi storage-class-basic.yaml

```

9. 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"

```

10. Run the `kubectl` command to create the storage class.

```

ubuntu@Anthos-Admin-Workstation:~/trident-installer$ kubectl create -f sample-input/storage-
class-basic.yaml

```

11. 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. The only edit that must be made to this file is ensuring that the `storageClassName` field matches the one just created.

```

ubuntu@Anthos-Admin-Workstation:~/trident-installer$ vi sample-input/pvc-basic.yaml
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi

```

12. 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@Anthos-Admin-Workstation:~/trident-installer$ kubectl create -f sample-input/pvc-
basic.yaml

ubuntu@Anthos-Admin-Workstation:~/trident-installer$ kubectl get pvc --watch

```

NAME	STATUS	VOLUME	CAPACITY	ACCESS	MODES
STORAGECLASS	AGE				
basic	Pending				basic
1s					
basic	Pending	pvc-2azg0d2c-b13e-12e6-8d5f-5342040d22bf	0		basic
5s					
basic	Bound	pvc-2azg0d2c-b13e-12e6-8d5f-5342040d22bf	1Gi	RWO	basic
7s					

6 Best Practices

This section lists several best practices that an organization should consider before deploying this solution into production.

6.1 Install a Second F5 Big-IP Virtual Edition Appliance

In a production environment, it is a best practice to avoid single points of failure in your environment. For this validation, a single F5 BIG-IP Virtual Edition Load Balancer appliance was used to validate connectivity to the control plane and the ingress VIP addresses for the Anthos on VMware clusters. While this works fine for a simple validation, loss of communication with the control plane VIP for a cluster can make a cluster inaccessible or unable to be managed from the admin workstation or the Google Cloud console. F5 BIG-IP Virtual Edition supports application-based HA to make sure disruptions do not happen. Although this issue is mentioned briefly, setup procedures for this functionality are not described in detail in this document. However, NetApp recommends investigating this feature further before deploying the NetApp HCI for Anthos solution into production.

6.2 Enable VMware vSphere DRS and Configure Anti-Affinity Rules

VMware vSphere provides a feature that makes sure that no single node in the cluster runs low on physical resources available to virtual guests. The Distributed Resource Scheduler (DRS) can be configured on vSphere clusters consisting of at least three ESXi nodes. The NetApp HCI minimum configuration described in this deployment guide consists of two compute nodes and is unable to make use of this feature. As a result of this limitation, we were also forced to disable anti-affinity rules for the Anthos on VMware clusters that we deployed.

Anti-affinity rules ensure all masters or all workers for a specific user cluster run on different nodes, so that a single node failure cannot disable an entire user cluster or the pods that it is hosting. As the NetApp HCI system is both easily and rapidly scalable, and considering the minimum deployment described in this validation has two open chassis slots for immediate expansion of HCI 410C nodes, NetApp suggests adding additional compute nodes into the empty chassis slots prior to deploying the solution into production, and enabling DRS with Anti-Affinity rules.

6.3 Leverage SnapMirror to Copy Data Remotely for Disaster Recovery

NetApp Element storage systems can use NetApp SnapMirror® technology to replicate storage volumes to systems running the NetApp ONTAP system, including AFF, FAS, and Cloud Volumes ONTAP. You can set up regularly scheduled SnapMirror operations to back up the VMware datastores and restore from a remote site in the event of a disaster. It is also possible to use SnapMirror to back up or migrate the persistent volumes provisioned by Trident and reattach them to Kubernetes clusters deployed in other environments and in the cloud.

7 Conclusion

With NetApp HCI with Anthos, organizations can adopt and use DevOps methodologies to run their day-to-day operations in an agile manner. NetApp HCI with Anthos is an enterprise-level hybrid cloud solution that uses best-in-the-field features of the NetApp Element storage system, VMware vSphere for

virtualization, and Anthos for VMware for the deployment of Kubernetes clusters. By using the NetApp HCI platform as the host for Anthos on VMware, organizations have access to a simple, high-performing, and scalable architecture to build their hybrid cloud operations, without any of the additional difficulties associated with deploying and managing Kubernetes clusters manually.

Where to Find Additional Information

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

- Anthos Documentation
<https://cloud.google.com/anthos/docs/>
- NetApp HCI Documentation
<https://www.netapp.com/us/documentation/hci.aspx>
- NetApp NDE 1.6 Deployment Guide
https://library.netapp.com/ecm/ecm_download_file/ECMLP2856899
- NetApp Trident Documentation
<https://netapp-trident.readthedocs.io/en/stable-v19.10/>
- VMware vSphere 6.5 Documentation
<https://docs.vmware.com/en/VMware-vSphere/index.html>
- F5 BIG-IP Documentation
<https://www.f5.com/services/resources>

Version History

Version	Date	Document Version History
Version 1.0	November 2019	Initial release of document.

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

Copyright Information

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

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

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

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

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

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

Trademark Information

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