NetApp Verified Architecture

NetApp HCI - NIST Security Controls for FISMA with HyTrust for Multitenant Infrastructure

NVA Design and Deployment

Arvind Ramakrishnan, Abhinav Singh, NetApp

January 2020 | NVA-1143 | Version 1.0

Abstract

This document describes how NetApp® HCI can be designed and deployed to meet National Institute of Standards and Technology (NIST) SP 800-53 Revision 4 Security and Privacy controls, which are crucial for private cloud infrastructures and multitenant deployments.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Executive Summary

Organizations must deal with massive quantities of sensitive, mission-critical data that can be accessed by people from across the globe. Although it is highly beneficial for employees and customers of a business to access their data whenever and wherever they want, it also exposes the business to external and internal security threats and attacks.

An organization is vulnerable to threats at various levels of the IT infrastructure. The key to mitigate these risks is to make sure that there is a focused effort on securing the IT infrastructure, its applications, and its users with the right technologies.

Securing a business does not stop at securing data. An organization must also implement and follow effective processes, best-practices, standards and compliance. These elements must be implemented in every layer of the organization's IT infrastructure and continually monitored for violations and corrections.

Building a private cloud IT infrastructure with all the required security measures is a highly complex and time-consuming task. It requires specialists focused on data storage, IT network design, compute infrastructure, IT applications, and other areas, including the identification of security measures and the methods to implement them.

This NetApp Verified Architecture (NVA) describes how NetApp HCI expedites and simplifies the design, deployment, and management of a private cloud IT infrastructure so that the environment adheres to the key Federal Information Security Management Act (FISMA) security measures described in NIST SP 800-53 Revision 4.

2 Program Summary

2.1 NetApp Verified Architecture

The NVA program offers customers a verified, referenceable architecture for NetApp solutions. With an NVA solution, you get a NetApp solution architecture that provides the following advantages:

- Thoroughly tested
- Prescriptive in nature
- Minimized deployment risks
- Accelerated time to market

2.2 NetApp HCI Design Principles

NetApp HCI is designed to provide predictable performance, linear scalability, and a simple deployment and management experience.

Predictable Performance

The NetApp HCI infrastructure is an ideal platform to host a multitenant environment. The tenants can be different workloads or functional units of an organization or an entire organization with its own users and data. The challenge in a such an environment is to provide consistent and predictable performance for all the tenants. The system must also meet the requirements of tenants that have high resource requirements without affecting the performance of other tenants.

NetApp HCI alleviates this concern with quality of service (QoS) limits that are available natively with NetApp Element® software. NetApp Element allows granular control of every application and volume, eliminates noisy neighbors, and satisfies performance SLAs.

© 2020 NetApp, Inc. All rights reserved.

Flexible and Scalable

Unlike a traditional HCI platform, NetApp HCI allows you to scale compute and storage nodes independently of each other. This capability makes sure that the system is the right size to meet your workload requirements and, it also prevents overprovisioning of resources. Multiple combinations of compute and storage nodes are available with varying specifications to suit a wide range of workloads.

NetApp HCI is architected in building blocks at either the chassis or the node level. Each chassis can hold four nodes made up of storage nodes, compute nodes, or both. At the time of publication, the minimum configuration is two chassis with six nodes (four storage nodes and two compute nodes).

Simple

The NetApp HCI architecture is based on a modular design, and the NetApp Deployment Engine (NDE) simplifies day-zero deployment by reducing the number of manual steps from over 400 to fewer than 30. It enables the quick deployment of NetApp HCI, including a NetApp Element software cluster and VMware virtualized infrastructure. NDE optimally configures data and management networks; configures the cluster; and sets up VMware ESXi, vCenter, and other required configurations. The virtualized environment becomes operational in a risk-free process. With NDE, additional compute and storage nodes can be added to the HCI system with minimal effort.

3 Solution Overview

This NetApp HCI solution gives customers a fully validated multitenant solution that integrates with HyTrust CloudControl (HTCC) and DataControl to meet the key security measures for FISMA as defined in NIST SP 800-53 Revision 4.

Some of the key highlights offered by this solution are as follows:

- NetApp HCI as a FISMA-ready private cloud infrastructure
- Notional workload based on VMware Private Cloud
- Integration with HTCC for fine-grained control over physical and logical infrastructure components
- Integration with HyTrust DataControl (HTDC) for encryption and decryption at the VM level with onboard key management
- VMware NSX for network virtualization and security in a software-defined datacenter

3.1 Target Audience

The target audience for this solution includes the following groups:

- Federal agencies
- Private sector companies that have a contractual relationship with the government
- Enterprise IT cloud administrators
- Service providers

3.2 Solution Technology

The key technologies in this design include the following elements:

NetApp HCI

NetApp HCI provides a flexible platform that allows data center resizing and expansion at multiple tiers and levels of the infrastructure, including CPU, memory, storage capacity, and storage IOPS requirements.

© 2020 NetApp, Inc. All rights reserved.

With NetApp HCI, storage and compute nodes with the desired specifications (capacity, CPU, RAM, and so on) can be added and repurposed to expand or contract the compute or storage parameters based on datacenter requirements.

The NDE manages the scaling of the HCI system, its configuration, and its deployment. Using NDE, compute and storage nodes can be added or removed from an HCI system with ease. Compute nodes are added to the vCenter data center and its compute clusters. Storage nodes are added to the NetApp HCI cluster in a way that is transparent to vCenter and the ESXi hosts.

VMware management tools are used to add compute nodes to available data centers and compute clusters, and compute resources can be dynamically applied using VMware Distributed Resource Scheduling (DRS).

The NetApp SolidFire Plug-in for VMware vCenter Server can be used to perform configuration and management operations on the underlying Element OS storage cluster from the vCenter GUI. This simplifies configuration and management by allowing the use of integrated plug-ins to add and manage clusters, datastores, and QoS policies; enable virtual volumes; and monitor events throughout the deployed cluster.

NIST SP 800-53 Revision 4

NIST Special Publication 800-53, Revision 4 provides a catalog of privacy and security controls for organizations and federal information systems. It also provides a process for selecting controls to protect an organization’s operations, assets, and individuals from a diverse set of threats.

These controls can be customized and implemented as part of an organization-wide process that manages information security and privacy risk. These controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure. They are derived from legislation, executive orders, policies, directives, regulations, standards, and mission and business needs.

This catalog of security controls addresses security functions, their strength, and the mechanisms provided. This catalog also assurance issues, or the measure of confidence in the implemented security capability.

In this solution, security controls necessary for the protection of a NetApp HCI system were selected and tested in the lab. It is important to note that security controls can be implemented in many ways and there is no single correct method. The approach to implement a security control can vary based on datacenter design, logistics, cost, adherence to existing organizational processes, preferred technology, and so on.

HyTrust CloudControl

HTCC provides a unified framework for security and compliance and therefore lowers both risk and operational overhead. HTCC was designed to address the security and compliance gaps that exist in a typical virtual environment. It provides a standard for policy-based access controls, enforcement, and automated compliance for the virtual environment and software-defined data center (SDDC).

HTCC provides a robust set of capabilities, including the following:

- Granular role-based access controls (RBAC)
- Object-based access controls (OBAC)
- Secondary approval
- Audit quality logging
- Root password vaulting (RPV)
- Hypervisor configuration hardening
- Two-factor authentication (2FA)

© 2020 NetApp, Inc. All rights reserved.

HTCC also includes visually appealing, user-friendly, and detailed management dashboards that can help organizations understand how privileged users' actions were performed throughout the entire lifecycle of a virtual object.

HyTrust DataControl

HTDC provides encryption and key management for virtual machines (VMs) located in data centers or private, public, or hybrid clouds.

DataControl consists of two main components:

- **HyTrust KeyControl.** KeyControl stores encryption keys, policies, and configuration for any number of VMs with the HTDC Policy Agent installed.
- **HTDC Policy Agent.** This software module runs inside Windows and most Linux operating systems to provide encryption of virtual disks, file systems, and individual files.

4 Technology Requirements

This section lists the hardware and software models or versions used during solution validation.

4.1 Hardware Requirements

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

Note: Specific switch infrastructure is not included in the required hardware because there are various deployment options available. See the section "Network and Switch Requirements."

Table 1) Hardware requirements.

Hardware	Quantity
Compute node: NetApp H410C	6*
Storage node: NetApp H410S	4

*In this solution, the configuration of the vSphere virtual infrastructure was similar to a VMware Validated Design. The virtual infrastructure had three clusters: a management cluster, an edge cluster, and an additional cluster to host the workload, with each cluster containing two ESXi hosts.

4.2 Software Requirements

Table 2 lists the software components that were used to build the base solution.

Note: To meet the requirements specified in the security controls, additional software can be used.

Table 2) Software requirements.

Product Family	Product Name	Product Version
VMware vSphere Enterprise Plus	ESXi	6.7.0
	vCenter Server Appliance	6.7.0.20000
VMware NSX for vSphere Enterprise	NSX for vSphere	6.4.5
NetApp	Element	11.3.1.5

Product Family	Product Name	Product Version
	NDE	1.6 P1
	vSphere Plug-in for SolidFire	4.3.0
HyTrust	CloudControl	5.6.0.56288
	DataControl	5.0

5 Solution Design

5.1 Architectural Overview

The architecture of the NetApp HCI system used in this solution is similar to a VMware Validated Design for a standard SDDC.

Figure 1) NetApp HCI architecture for NIST.

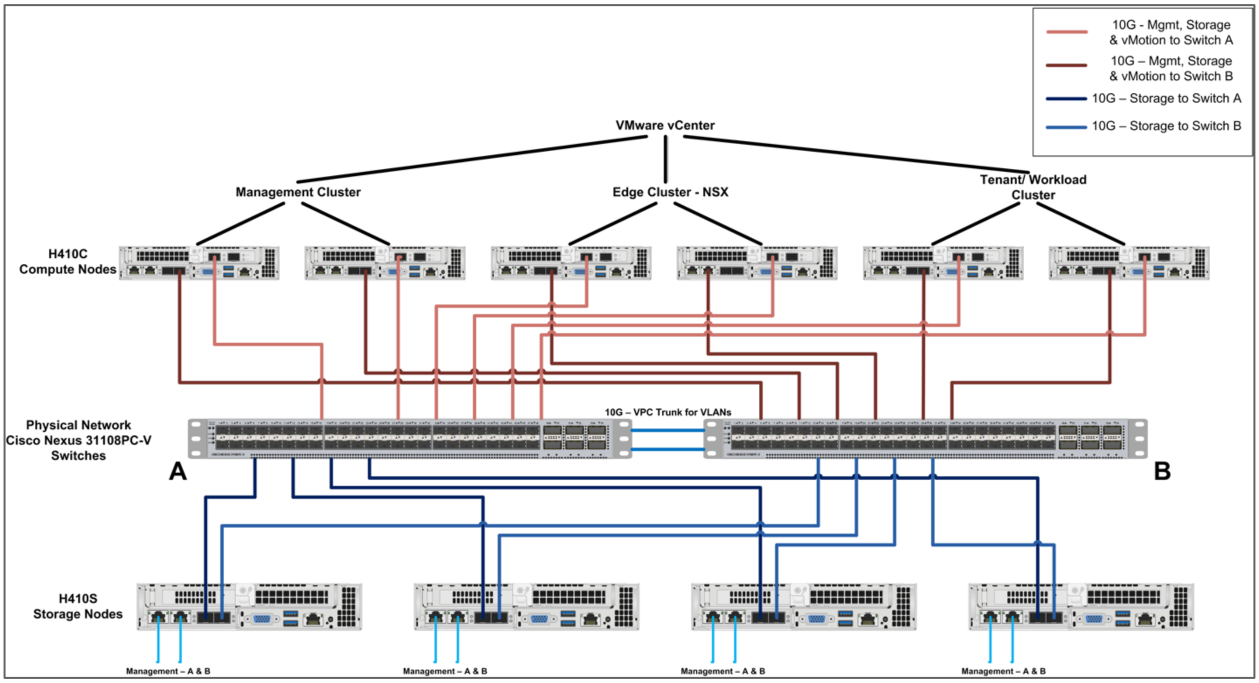

10G - Mgmt, Storage & vMotion to Switch A
10G – Mgmt, Storage & vMotion to Switch B
10G – Storage to Switch A
10G – Storage to Switch B
VMware vCenter
Management Cluster
Edge Cluster - NSX
Tenant/ Workload Cluster
H410C Compute Nodes
Physical Network Cisco Nexus 31108PC-V Switches
10G – VPC Trunk for VLANs
A
B
H410S Storage Nodes
Management – A & B
Management – A & B
Management – A & B
Management – A & B

Figure 1 represents the physical architecture of the NetApp HCI system that was designed for this solution. Three clusters were created within VMware vCenter: management, edge, and tenant-workload. The management cluster hosts the VMs and applications like vCenter, NetApp mNode, NSX Manager, Log Insight, and HTCC. The edge cluster hosted the NSX controllers, the NSX DLR Control VM, and the perimeter firewall. A third tenant-workload cluster was reserved for hosting the tenant's workloads and applications. It also hosted the HTDC instance. HTDC was installed in the tenant cluster and its control was handled by the tenant administrator so that the tenant has exclusive access to the key management of its encrypted VMs.

Four storage nodes (minimum configuration) were configured as an Element cluster by the NetApp Deployment Engine. NDE automatically created two volumes and configured them as datastores in vCenter and mounted them on all the ESXi hosts. This configuration of NDE was later modified to meet the design needs of this solution, as discussed in the section "Storage Design."

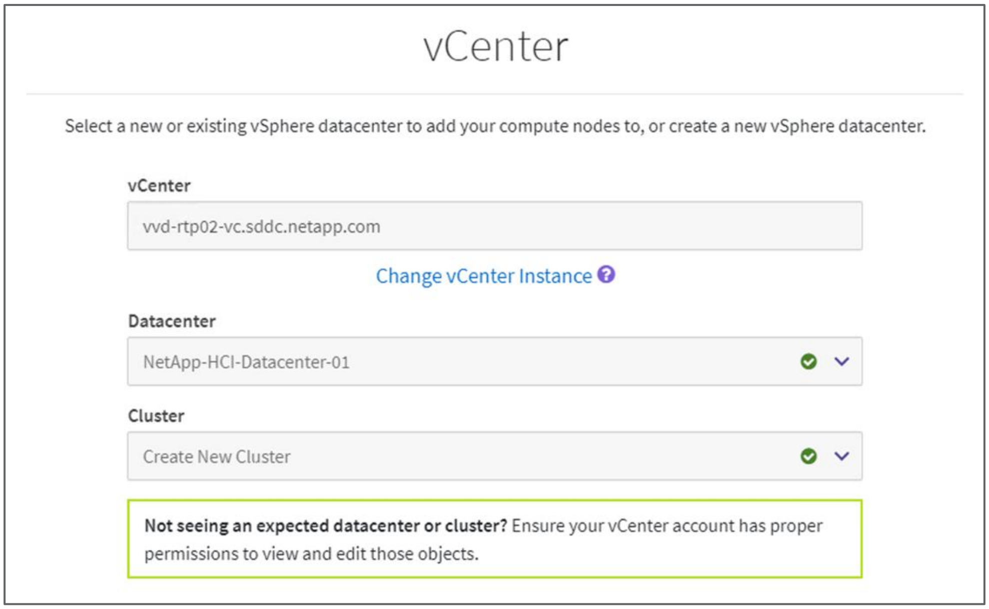
The NetApp HCI system only contains the compute and storage nodes. The network switches can be a standard top-of-rack switch that provide a specific set of capabilities described in the section “Network Design.” NetApp does not provide a specific list of switch vendors, so customers can use the switch vendor of their choice.

5.2 Compute Design

The minimum number of compute nodes required to build a NetApp HCI system is two. However, in this solution, six compute nodes were used.

These six compute nodes were added to the virtual infrastructure in a phased approach.

The management cluster was configured first as part of the initial configuration with NDE. After the management services were running, NDE was invoked again to expand the compute node footprint by adding ESXi servers to a new cluster in the virtual infrastructure.



vCenter

Select a new or existing vSphere datacenter to add your compute nodes to, or create a new vSphere datacenter.

vCenter: vvd-rtp02-vc.sddc.netapp.com

Change vCenter Instance

Datacenter: NetApp-HCI-Datacenter-01

Cluster: Create New Cluster

Not seeing an expected datacenter or cluster? Ensure your vCenter account has proper permissions to view and edit those objects.

An alternative approach to adding the compute nodes to the virtual infrastructure is to select all the nodes during the initial NDE configuration phase. With this approach, all nodes become part of a single cluster after NDE completes its operations. Post-NDE, two additional clusters must be created, and the four ESXi hosts must to be moved to the two new clusters.

5.3 Network Design

As specified earlier, customers can choose a network switch vendor to connect the compute and storage nodes. However, to ensure a successful deployment, the switches must possess the following capabilities:

- All switch ports connected to NetApp HCI nodes must be configured to allow the Spanning Tree Protocol (STP) to immediately enter the forwarding state. On Cisco switches, this functionality is known as PortFast. Ports connected to NetApp HCI nodes should not receive STP Bridge Protocol Data Units (BPDUs).
- The switches handling storage, VM, and vMotion traffic must support speeds of at least 10GbE per port (up to 25GbE per port is supported).
- The switches handling management traffic must support speeds of at least 1GbE per port.

- The MTU size on the switches handling storage traffic must be 9216 bytes end-to-end for a successful installation. MTU size is configured automatically on the storage node interfaces.
- Cisco Virtual PortChannel (vPC), Multi-Chassis Link Aggregation (MLAG), or the equivalent switch stacking technology must be configured on the switches handling the storage network for NetApp HCI. Switch stacking technology eases configuration of the Link Aggregation Control Protocol (LACP) and port channels. It provides a loop-free topology between switches and the 10/25GbE ports on the storage nodes.
- The switch ports connected to the 10/25GbE interfaces on NetApp HCI storage nodes must be configured as an LACP port channel.
- The LACP timers on the switches handling storage traffic must be set to `fast mode (1s)` for optimal failover detection time. During deployment, the Bond1G interface on all NetApp HCI storage nodes are automatically configured for active-passive mode.
- Round-trip network latency between all storage and compute nodes should not exceed 2ms.

You should implement the following best practices to prepare the network for NetApp HCI deployment:

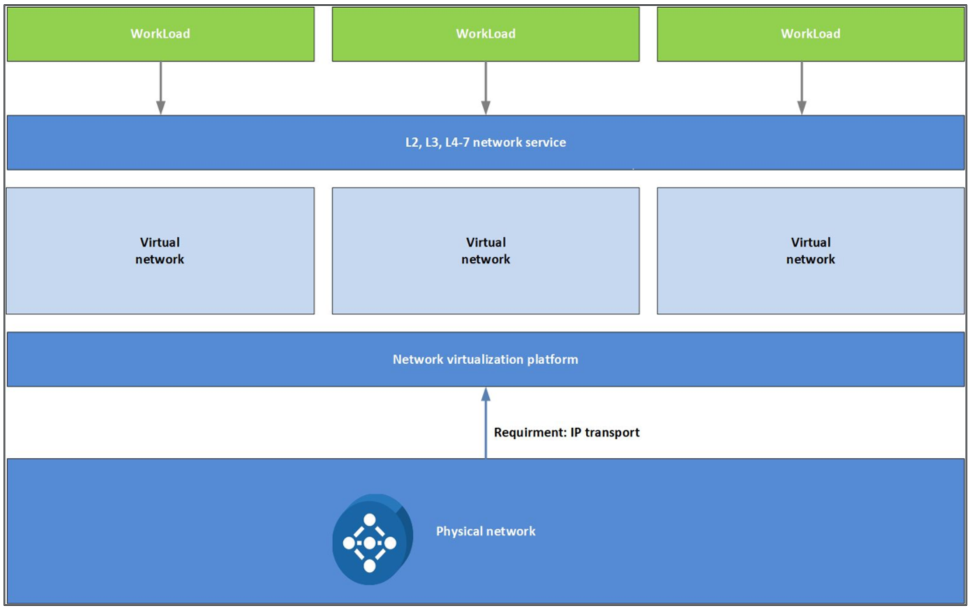
- Install as many switches as needed to meet high-availability requirements.
- Balance 1/10GbE port traffic between at least two 1/10GbE-capable management switches.
- Balance 10/25GbE port traffic between two 10GbE-capable switches.

5.3.1 VMware NSX

VMware NSX Data Center delivers a new operational model for software-defined networking. Data center operators can now achieve levels of agility, security, and economics that were previously unattainable when the data center network was tied to physical hardware components. Network virtualization works as an overlay above any physical network hardware and works with any server hypervisor platform. The only requirement from a physical network is that it provides IP transport 1. There is no dependency on the underlying hardware or hypervisor.

Figure 1 is a representation of network virtualization. The functional equivalent of a network hypervisor reproduces the complete set of Layer 2 through Layer 7 networking services (for example, switching, routing, access control, firewall and load balancing).

Figure 1) NSX-V for vSphere.



Network isolation among different workloads can be achieved by using the VXLAN encapsulation protocol. This encapsulation allows two VMs on the same network to talk to each other, even if the path between the VMs must be routed. All VM-to-VM traffic is encapsulated in VXLAN and transmitted over a routed network to the destination host. Each hypervisor has a virtual tunnel end point (VTEP) that is responsible for encapsulating VM traffic inside of a VXLAN header and routing the packet to a destination VTEP for further processing. Traffic can be routed to another VTEP on a different host or to the VMware NSX Edge Gateway to access the physical network.

The VMware implementation of VXLAN in NSX comes in the form of logical switches. The logical switches use VXLAN to create a virtual wire network between ESXi hosts. The logical switch uses the segment ID pool, which is the way VMware presents the Virtual Network Identifiers (VNI) for consumption to logically separate out one logical switch from another. The Distributed Logical Router (DLR) and the Edge Service Gateway (ESG) are Layer-3 components that perform routing for the VMs. DLR is responsible for handling routing for VM-to-VM (east-west) traffic, and ESG acts as a transit between the outer physical network and inner virtual network. It is responsible for north-south traffic. Both DLR and ESG have built-in firewall capabilities that provide a level of granular control over security policies that is not possible with traditional firewalls.

In this design, NSX manager was deployed in the management cluster, the controllers and edge VMs were deployed in the edge cluster to provide compute-level isolation. DLR and ESG can be peered using a static or dynamic routing protocol (Open Shortest Path First [OSPF] or Border Gateway Protocol [BGP]). In this design, OSPF was used to peer DLR and ESG. In the same way, ESG can be peered to the TOR switch using a static or dynamic routing protocol (OSPF/BGP). Static routing is configured in this design between ESG and TOR for virtual to physical communication.

The production and development VMs for the web servers, applications, and databases were deployed and attached to their respective logical switches. All the logical switches were connected to the DLR, which is responsible for forwarding layer-3 traffic between the VMs from different segments (VNIs). Micro segmentation was used to create traffic separation between the production VMs and the development VMs.

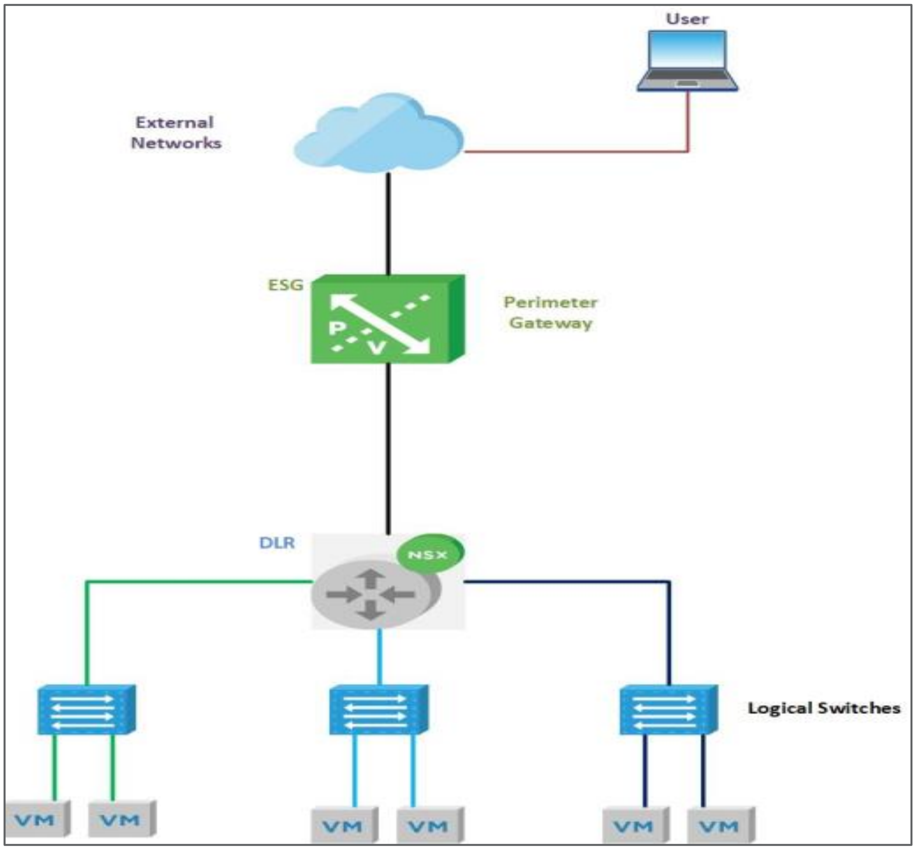
The HyTrust Key Control primary and secondary VMs were deployed in the tenant-workload cluster. We used this configuration to provide absolute control of key management to the tenant administrators. The HyTrust Key Control VMs were attached to a separate logical switch. The benefit of using this approach was that traffic between the VMs in the tenant-workload cluster and their key management server was restricted to the cluster.

For shared service workloads like DNS, Active Directory, the Network Time Protocol (NTP), and Syslog, a dedicated logical switch was used in this design. All workload VMs could communicate with shared-service VMs. Any other VMs from other clusters were not able to communicate with shared-service VMs.

The external client access to the workloads was controlled by a perimeter firewall. A default rule for the ESG was configured to deny traffic from all sources, and a separate rule was created to allow access for a specific source.

Figure 2 depicts NSX logical connectivity for switching and routing of the VMs that were deployed on NetApp HCI.

Figure 2) NetApp HCI with NSX.



5.4 Storage Design

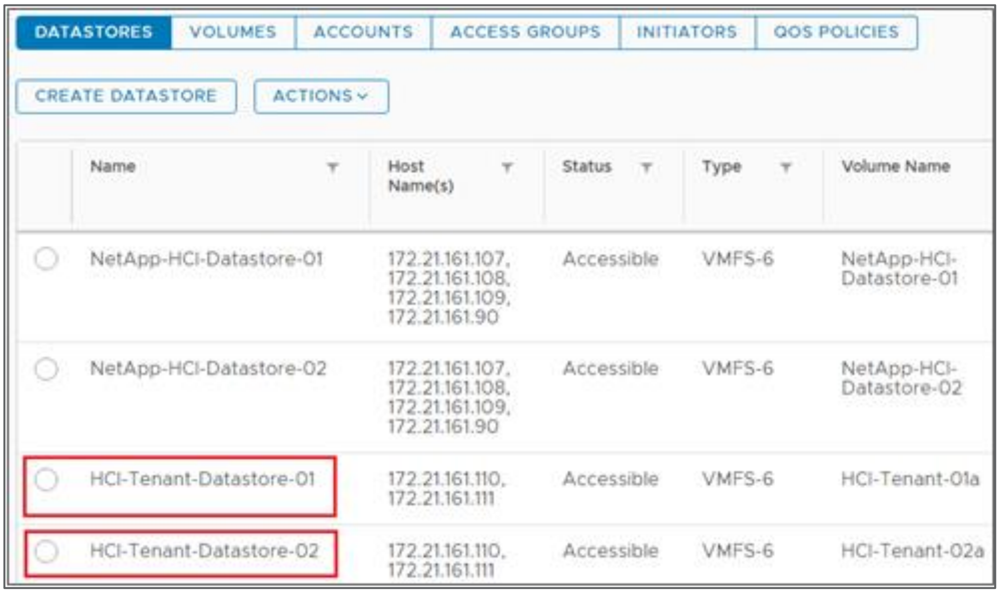
The minimum number of storage nodes required to build a NetApp HCI system is four. We configured all four storage nodes in an Element cluster with the NDE. NDE automatically created two volumes and configured them as VMFS datastores in vCenter and mounted them on the ESXi hosts in the management cluster deployed by NDE during its initial run. This Element configuration was later extended to meet the design needs of this solution.

After the configuration of the management cluster, we expanded the virtual infrastructure by adding an edge cluster with two ESXi hosts. The datastores that were mounted to the ESXi hosts in the management cluster were also mounted to these new ESXi hosts.

After the edge cluster was configured, we added a tenant-workload cluster to the infrastructure. For this cluster, we created a separate account with an associated access group. We created two volumes in this account and provisioned them as datastores to the ESXi hosts in the tenant-workload cluster. These new datastores, `HCI-Tenant-Datastore01` and `HCI-Tenant-Datastore02`, were made visible to the ESXi hosts of the tenant-workload cluster. This provided secure separation between the tenant and workload data and the management and edge data.

© 2020 NetApp, Inc. All rights reserved.

Figure 2) HCI-Tenant-Datastore01 and HCI-Tenant-Datastore02.



	Name	Host Name(s)	Status	Type	Volume Name
○	NetApp-HCI-Datastore-01	172.21.161.107, 172.21.161.108, 172.21.161.109, 172.21.161.90	Accessible	VMFS-6	NetApp-HCI-Datastore-01
○	NetApp-HCI-Datastore-02	172.21.161.107, 172.21.161.108, 172.21.161.109, 172.21.161.90	Accessible	VMFS-6	NetApp-HCI-Datastore-02
○	HCI-Tenant-Datastore-01	172.21.161.110, 172.21.161.111	Accessible	VMFS-6	HCI-Tenant-01a
○	HCI-Tenant-Datastore-02	172.21.161.110, 172.21.161.111	Accessible	VMFS-6	HCI-Tenant-02a

5.5 HyTrust CloudControl

The HTCC appliance is a secure, hardened operating system built on the CentOS platform. HTCC serves as a proxy to the VMware vCenter management platform and enhances the platform with forensic-grade logging and advanced administrative control. With HTCC’s granular RBAC, administrative functions can be easily set to control permissions on a virtual-object level. HTCC applies smart labels to enable further segregation of virtual objects by constraining object access based on certain labels. HTCC offers two-person integrity for destructive actions on VMs through the secondary approval function.

HTCC offers automated compliance validation and implementation for VMware ESXi hosts. Variables can be set and then applied to each host so that the host security posture complies with the required baseline standards. HTCC can use Intel Trusted Execution Technology (TXT) to enable trusted compute pools by labeling hosts and configuring VMs to run only on a host that has the correct label.

HTCC is deployed in the mapped mode and as a cluster configuration. In the mapped mode, all the hosts that need to be protected by HTCC are configured with a published IP (PIP). This PIP is used by users and clients to access the hosts.

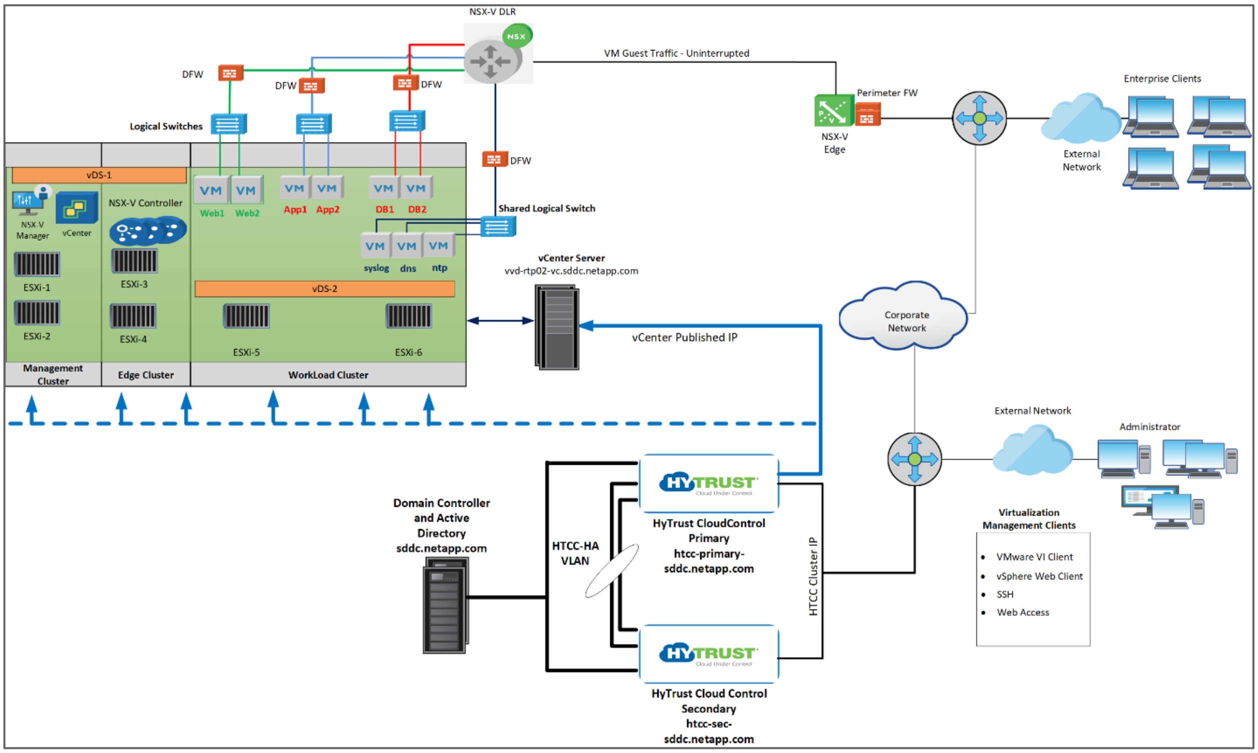
HTCC is deployed as a transparent proxy that sits between the users and all management interfaces to the protected hosts. From this central vantage point, HTCC intercepts and logs all administrative requests coming through the PIP and enforces role-based and resource-based policies that protect workloads from unauthorized access.

A private cluster network is set up on a dedicated VLAN for the HTCC cluster nodes to communicate with each other.

HTCC is integrated with an Active Directory domain instance to apply the user identities and privileges extended to each user. Also, HTCC provides a set of access controls to users that can be configured to have specific privileges in the virtual infrastructure space.

Figure 3 depicts HTCC integrated with the VMware virtual infrastructure deployed on NetApp HCI.

Figure 3) NetApp HCI with HyTrust CloudControl.



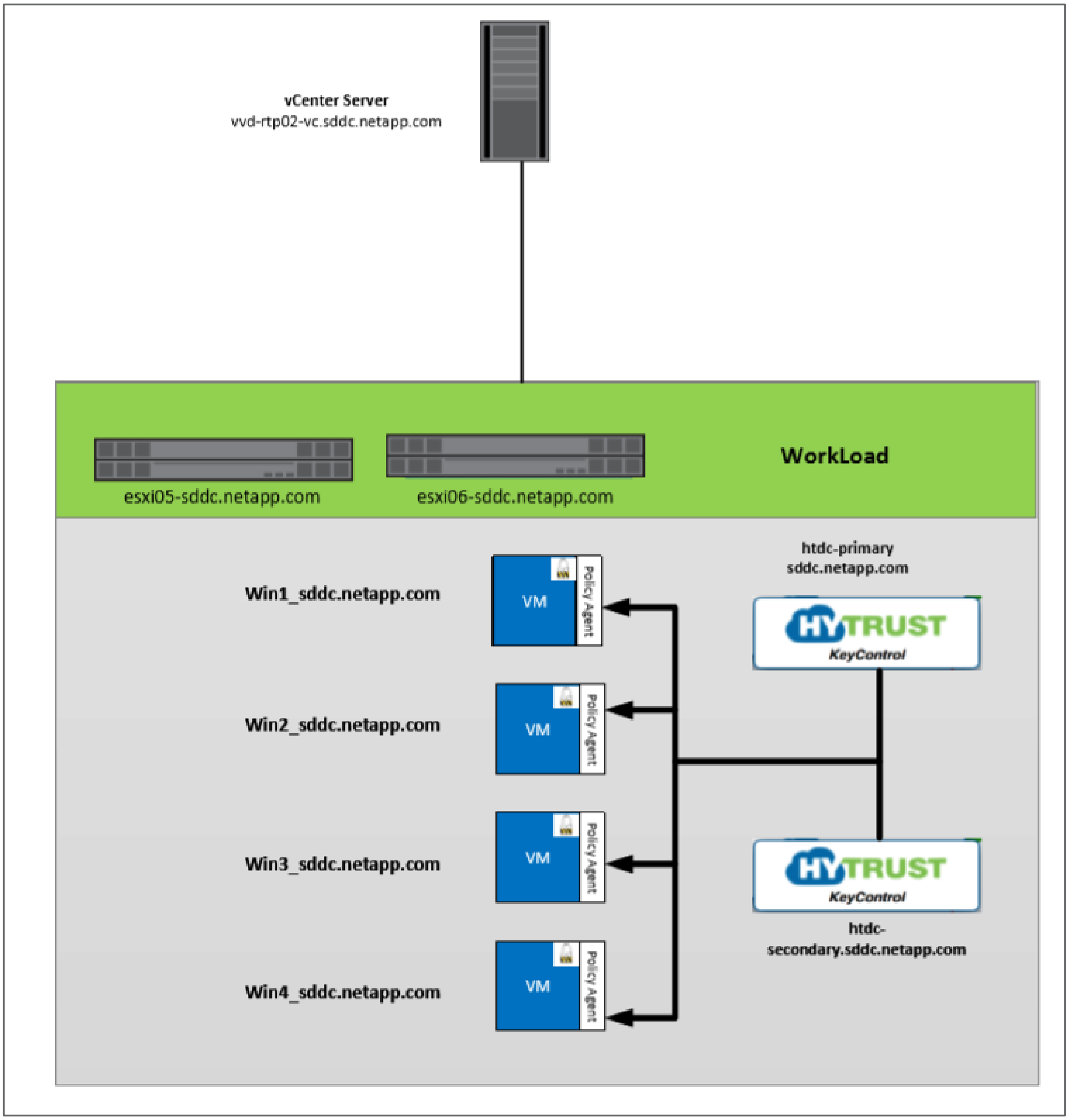
5.6 HyTrust DataControl

HTDC provides encryption of VM data while it is in motion and at rest. HTDC is deployed as a virtual appliance in a high-availability configuration. The solution includes three critical components: Key Control, Policy Engine, and Policy Agent.

Administrators can configure or modify encryption policies through the Policy Engine; the Policy Engine then collects the rules for the Key Controller. The Key Controller in turn makes sure that the Policy Agent (which resides in the VM or workload) executes on these policies by managing encryption key creation, renewals, and destruction.

Figure 4 illustrates how HTDC protects the data of the VMs running on various tenants within the NetApp HCI environment.

Figure 4) NetApp HCI with HyTrust DataControl.



6 Deployment Procedures

This section describes the steps required to deploy a NetApp HCI solution based on VMware Private Cloud. This deployment includes key management of VMs with HTDC, fine-grained access control of the virtual infrastructure using HTCC, and software-defined networking (SDN) with VMware NSX-V. These steps include a review of prerequisites, deployment of the physical infrastructure, configuration of the NetApp HCI system with VMware vCenter 6.7u1 and VMware NSX-V, and deployment of HTCC and HTDC.

6.1 Virtual Infrastructure Implementation with NetApp Deployment Engine

NDE Deployment Prerequisites

Consult the NetApp HCI Prerequisites Checklist to see the requirements and recommendations for NetApp HCI before you begin deployment.

The following are high-level requirements for NDE:

- Network and switch requirements and configuration
- Required VLAN ID preparation
- Network requirements for NSX
- Switch configuration
- IP address requirements for NetApp HCI, VMware, and HyTrust
- DNS and time-keeping requirements
- Final preparations

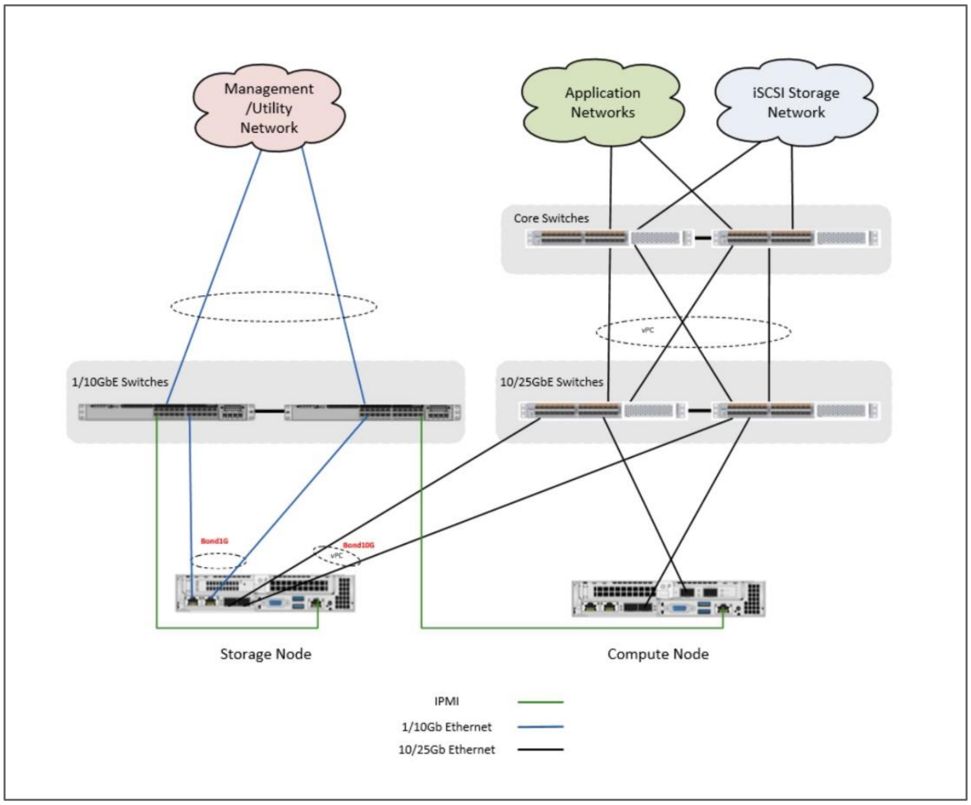
Network and Switch Requirements

The switches used to transfer NetApp HCI traffic require a specific configuration for successful deployment.

Consult the NetApp HCI Network Setup Guide for the physical cabling and switch details. This NVA uses a two-cable design for compute nodes. Optionally, compute nodes can be configured in a six-node cable design affording options for the deployment of compute nodes.

Figure 5 depicts the network topology of this NetApp HCI with VMware Private Cloud architecture with a two-cable design for compute nodes.

Figure 5) NetApp HCI with VMware Private Cloud network topology.



© 2020 NetApp, Inc. All rights reserved.

Prepare Required VLAN IDs

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

- Management
- VMware network
- vMotion
- Storage
- HTCC high availability (HA)

Table 3 lists the necessary VLANs for deployment, as outlined in this validation. NetApp recommends configuring these VLANs on the network switches prior to executing NDE.

Table 3) Required VLANs.

Network Segment	Details	VLAN ID
Out-of-band management network	Network for HCI terminal user interface (TUI)	16
In-band management network	Network for accessing management interfaces of nodes, hosts, and guests	3417
VMware vMotion	Network for live migration of VMs	3425
SAN storage	Network for iSCSI storage traffic	3426
Tenant VM network	Network for VM traffic	186
NSX VLAN for VTEPs	Network for VXLAN VTEPs	3421
HTCC HA	Private network for HTCC HA traffic	3418

Network Requirements for VMware NSX

VMware NSX requires multiple IP addresses (Table 4). Unless otherwise indicated, addresses are assigned automatically by the NDE.

Table 4) NSX Required IP addresses.

IP Address Quantity	Details	VLAN ID/VNI
X1 per interface	External tenant connectivity	202
X2 per host	NSX VXLAN VTEPs	3421
X1 per interface	VXLAN (DLR-ESG)	5001
X1 per App VM	VXLAN (app)	5002
X1 per DB VM	VXLAN (db)	5003
X1 per Web VM	VXLAN (web)	5005
X1 per HTDC VM	VXLAN (secure)	5006
X1 per VM	VXLAN (shared services). For example, DNS, NTP, Sylog, and so on.	5000

Switch Configuration

NetApp HCI has specific physical and network requirements for an enterprise-grade data center deployment. As a part of prerequisites to run NDE, the switches must be deployed and possess the relevant configuration for the compute and storage ports.

This solution uses Cisco Nexus OS-based switches because they provided all the necessary requirements specified in section “Network Design”. The complete switch configuration is beyond the scope of this document.

This procedure assumes that the switches have been installed, cabled, and the initial configuration, such as NTP, default gateway, management IP, port descriptions and other relevant global configurations, are complete. Features defined in the section “Network Design” should be enabled on the switches.

IP Address Requirements for NetApp HCI, VMware vCenter, and HyTrust

The deployment of NetApp HCI, VMware, and HyTrust requires the allocation of multiple IP addresses. Table 5 lists the required IP addresses. Unless otherwise indicated, addresses are assigned automatically with NDE.

Table 5) Required IP addresses.

IP Address Qty	Details	VLAN ID
1 per storage and compute node*	HCI terminal user interface (TUI) addresses	16
1 per vCenter Server (VM)	vCenter Server management address	3417
1 per management node (VM)	Management node IP address	
1 per ESXi host	ESXi compute management addresses	
1 per storage node	NetApp HCI storage node management addresses	
1 per storage cluster	Storage cluster management address	
1 per ESXi host**	NSX VXLAN VTEPs	3421
1 per ESXi host	VMware vMotion address	3425
2 per ESXi host	ESXi host initiator address for iSCSI storage traffic	3426
2 per storage node	Storage node target address for iSCSI storage traffic	
1 per storage cluster	Storage cluster target address for iSCSI storage traffic	
The following IPs are assigned manually when the respective components are configured		
1+ per guest VM**	IP address for the tenant VM network; assigned based on use case	186
1 per HTCC HA setup**	HTCC virtual management IP	3417
1 per HTCC VM**	HTCC node IP	3417
1 for vCenter added to HTCC**	Global ESXi PIP	3417

1 for vCenter added to HTCC**	vCenter PIP	3417
1 for NSX added to HTCC**	NSX PIP	3417
1 per HTTC VM**	HTCC HA IP	3418
1 per HTDC VM**	HTDC node IP	5006 (via NSX VNI)

*This validation requires the initial setup of the first storage node TUI address. NDE automatically assigns the TUI address for subsequent nodes.

**Addresses are assigned after the NDE completes.

DNS and Timekeeping Requirement

Depending on your deployment, you might need to prepare DNS records for your NetApp HCI system. NetApp HCI requires a valid NTP server for timekeeping. You can use a publicly available time server if you do not have one in your environment.

This validation involves deploying NetApp HCI with a new VMware vCenter Server instance using a fully qualified domain name (FQDN). Before deployment, you must have one pointer (PTR) record and one address (A) record created on the DNS server.

Final Preparations

For instructions on deploying NetApp HCI H-Series system, see the Installation and Setup Instructions guide. This document covers the following subjects:

- Preparation for installation. Gathering all relevant information about your network, current or planned VMware infrastructure, and planned user credentials.
- Preparation of hardware. Installation, cabling, and powering on the NetApp HCI system.
- Configuration of NetApp HCI using the NDE.

For more information about the rack setup of your NetApp HCI system, see the NetApp HCI Rail Kit Installation Flyer.

For detailed deployment steps for the HCI system, see the NetApp HCI Deployment Guide Version 1.6.

The following steps should be completed before executing the NDE:

- Review the installation and setup instructions guide
- Review HCI Rail kit installation flyer
- Install HCI system
- Cable HCI system
- Prepare to execute the NDE

NDE Execution

Before you execute the NDE, you must complete the rack and stack of all components, configuration of the network switches, and verification of all prerequisites. You can execute the NDE by connecting to the management address of a single storage node if you plan to allow NDE to automatically configure all addresses.

NDE performs the following tasks to bring an HCI system online:

1. Installs the storage node (NetApp Element software) on a minimum of four storage nodes.
2. Installs the VMware hypervisor on a minimum of two compute nodes.
3. Installs VMware vCenter to manage the entire NetApp HCI stack.

4. Installs and configures the NetApp storage management node (mNode) and NetApp Monitoring Agent.
5. Installs and configures management access for an ONTAP Select appliance.

Note: This validation uses NDE to automatically configure all addresses. You can also set up DHCP in your environment or manually assign IP addresses for each storage node and compute node. These steps are not covered in this guide.

Note: As mentioned previously, this validation uses a two-cable configuration for compute nodes.

Note: Detailed steps for the NDE are not covered in this document.

Launch NDE

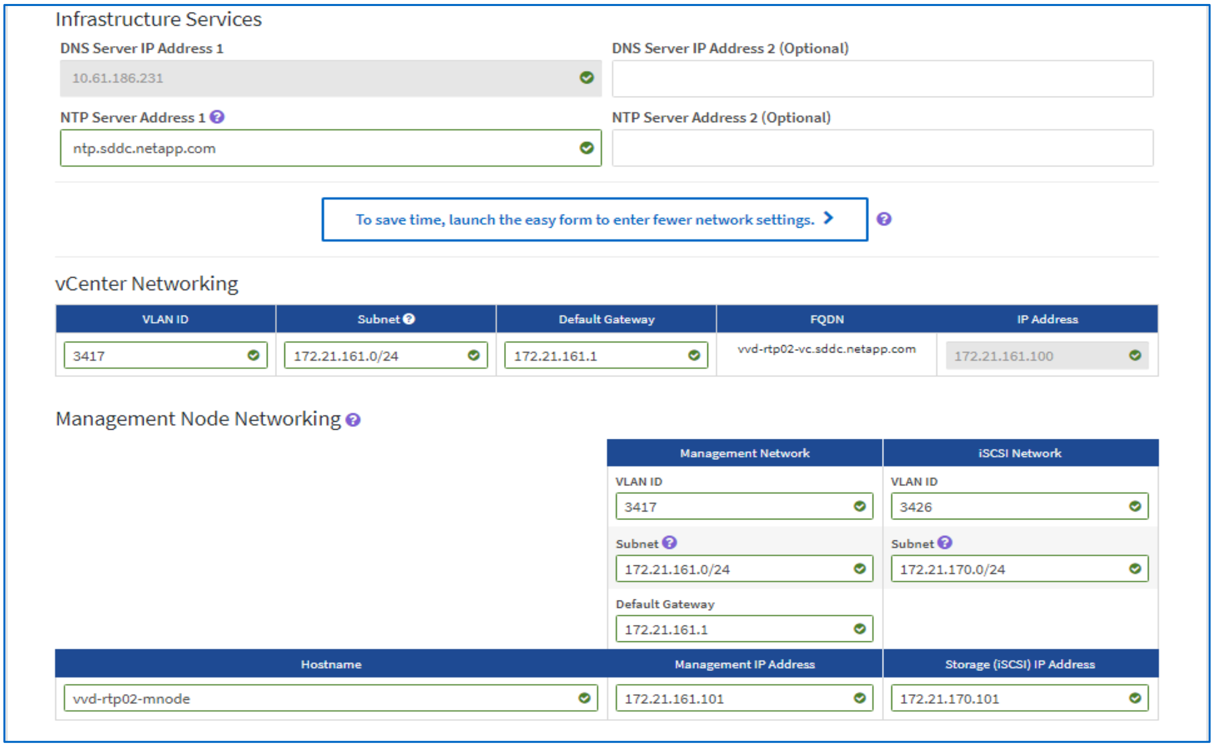
To execute NDE, complete the following steps:

1. Navigate to the management address of the first storage node http://storage_node_mgmt_ip:442/nde:

   Note: Be sure to use `http` rather than `https`.

2. Log in with the default credentials: ADMIN and ADMIN.
3. Click Get Started.
4. Select the three prerequisites checkboxes.
5. Accept the NetApp EULA and VMware EULA. Click Continue.
6. Click Configure a New vSphere Deployment, select vSphere 6.7 U1, and enter the FQDN of your vCenter server. Click continue.
7. 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.
8. NDE then prompts for the network topology used to cable the NetApp HCI environment. The validated solution in this document was deployed using the 2 Cable Option for the compute nodes and the 4 Cable Option for the storage nodes. Click Continue.
9. The Inventory page presents the compute and storage nodes. The storage node that is currently running NDE is already checked with a green mark. Select the corresponding boxes to add the additional nodes.
10. Then configure the permanent network settings for the NetApp HCI deployment. The first page configures infrastructure services (DNS and NTP), vCenter networking, and mNode networking. Click the easy form to enter fewer network settings.

© 2020 NetApp, Inc. All rights reserved.



Infrastructure Services

DNS Server IP Address 1	DNS Server IP Address 2 (Optional)
10.61.186.231 ✓	
NTP Server Address 1	NTP Server Address 2 (Optional)
ntp.sddc.netapp.com ✓	

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

vCenter Networking

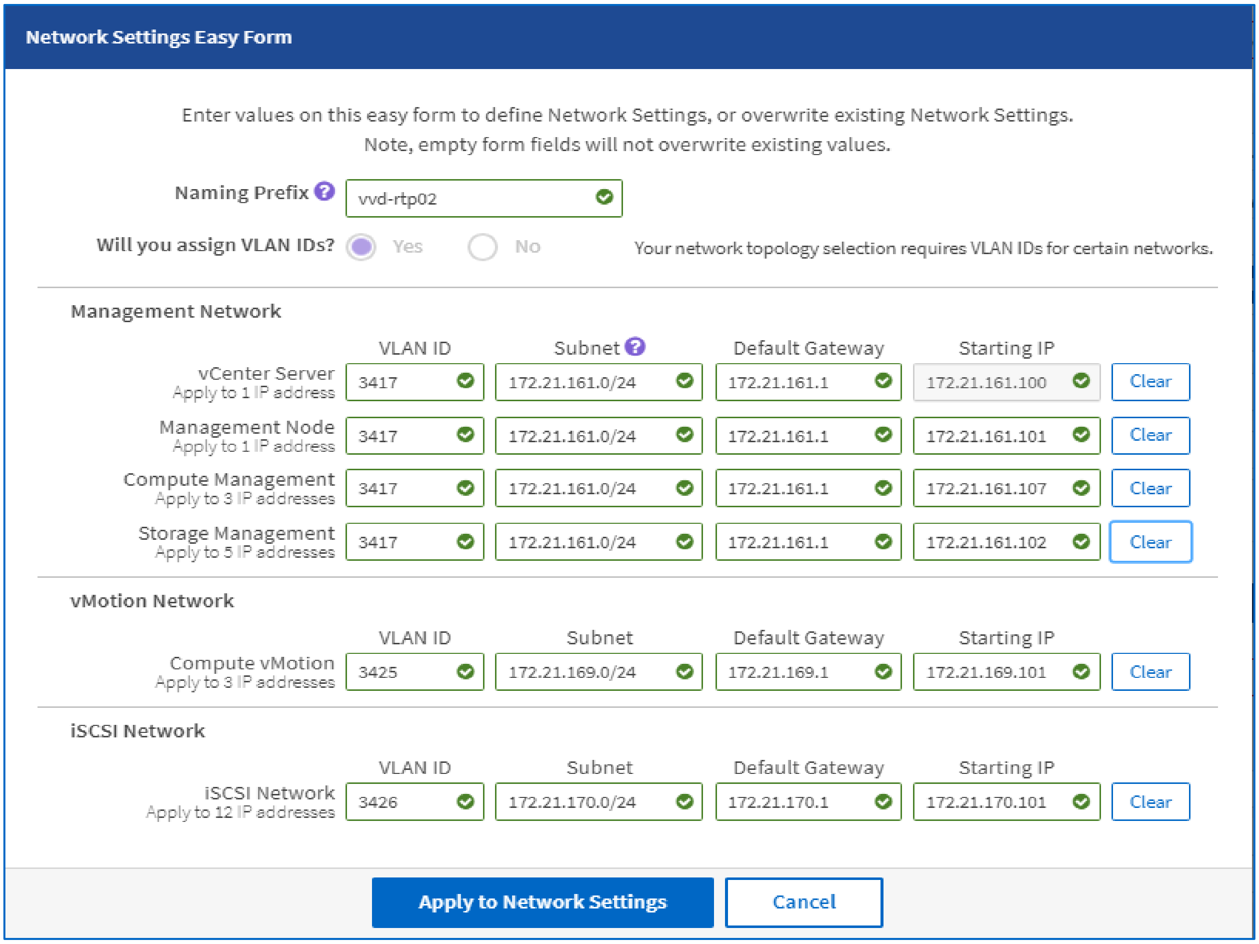
VLAN ID	Subnet	Default Gateway	FQDN	IP Address
3417 ✓	172.21.161.0/24 ✓	172.21.161.1 ✓	vvd-rtp02-vc.sddc.netapp.com	172.21.161.100 ✓

Management Node Networking

Management Network	iSCSI Network
VLAN ID: 3417 ✓	VLAN ID: 3426 ✓
Subnet: 172.21.161.0/24 ✓	Subnet: 172.21.170.0/24 ✓
Default Gateway: 172.21.161.1 ✓	

Hostname	Management IP Address	Storage (iSCSI) IP Address
vvd-rtp02-mnode ✓	172.21.161.101 ✓	172.21.170.101 ✓

11. Fill in the details like the naming prefix and the VLAN ID and IP addresses from management, vMotion, and the iSCSI network. Review your input, click Apply to Network Settings, and click Yes to continue.



Network Settings Easy Form

Enter values on this easy form to define Network Settings, or overwrite existing Network Settings.
Note, empty form fields will not overwrite existing values.

Naming Prefix: vvd-rtp02

Will you assign VLAN IDs? ● Yes ○ No — Your network topology selection requires VLAN IDs for certain networks.

Management Network

	VLAN ID	Subnet	Default Gateway	Starting IP
vCenter Server Apply to 1 IP address	3417	172.21.161.0/24	172.21.161.1	172.21.161.100
Management Node Apply to 1 IP address	3417	172.21.161.0/24	172.21.161.1	172.21.161.101
Compute Management Apply to 3 IP addresses	3417	172.21.161.0/24	172.21.161.1	172.21.161.107
Storage Management Apply to 5 IP addresses	3417	172.21.161.0/24	172.21.161.1	172.21.161.102

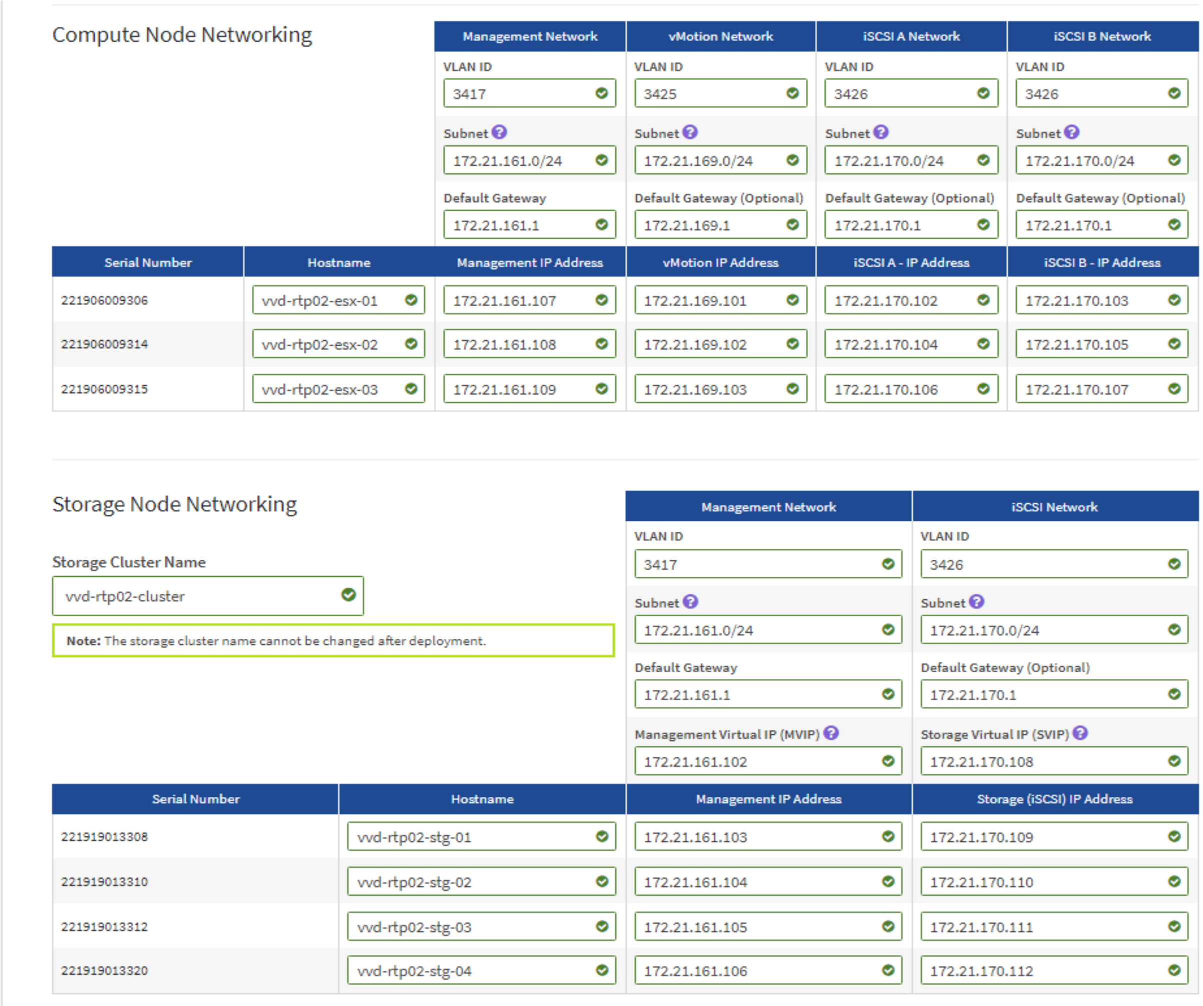
vMotion Network

	VLAN ID	Subnet	Default Gateway	Starting IP
Compute vMotion Apply to 3 IP addresses	3425	172.21.169.0/24	172.21.169.1	172.21.169.101

iSCSI Network

	VLAN ID	Subnet	Default Gateway	Starting IP
iSCSI Network Apply to 12 IP addresses	3426	172.21.170.0/24	172.21.170.1	172.21.170.101

12. The NDE automatically populates the IP addresses based on the ranges that you supplied. Live network validation is turned on by default. It takes a few minutes for the NDE to verify the availability of all IP addresses.



Compute Node Networking

	Management Network	vMotion Network	iSCSI A Network	iSCSI B Network
VLAN ID	3417	3425	3426	3426
Subnet	172.21.161.0/24	172.21.169.0/24	172.21.170.0/24	172.21.170.0/24
Default Gateway	172.21.161.1			
Default Gateway (Optional)		172.21.169.1	172.21.170.1	172.21.170.1

Serial Number	Hostname	Management IP Address	vMotion IP Address	iSCSI A - IP Address	iSCSI B - IP Address
221906009306	vvd-rtp02-esx-01	172.21.161.107	172.21.169.101	172.21.170.102	172.21.170.103
221906009314	vvd-rtp02-esx-02	172.21.161.108	172.21.169.102	172.21.170.104	172.21.170.105
221906009315	vvd-rtp02-esx-03	172.21.161.109	172.21.169.103	172.21.170.106	172.21.170.107

Storage Node Networking

Storage Cluster Name

vvd-rtp02-cluster

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

	Management Network	iSCSI Network
VLAN ID	3417	3426
Subnet	172.21.161.0/24	172.21.170.0/24
Default Gateway	172.21.161.1	
Default Gateway (Optional)		172.21.170.1
Management Virtual IP (MVIP)	172.21.161.102	
Storage Virtual IP (SVIP)		172.21.170.108

Serial Number	Hostname	Management IP Address	Storage (iSCSI) IP Address
221919013308	vvd-rtp02-stg-01	172.21.161.103	172.21.170.109
221919013310	vvd-rtp02-stg-02	172.21.161.104	172.21.170.110
221919013312	vvd-rtp02-stg-03	172.21.161.105	172.21.170.111
221919013320	vvd-rtp02-stg-04	172.21.161.106	172.21.170.112

13. Review the information and start the 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.

14. 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.
15. On the Your Setup is Complete page, click Export all Setup information to CSV file. The setup information about the installation downloads in the CSV format.

Post NDE Configuration

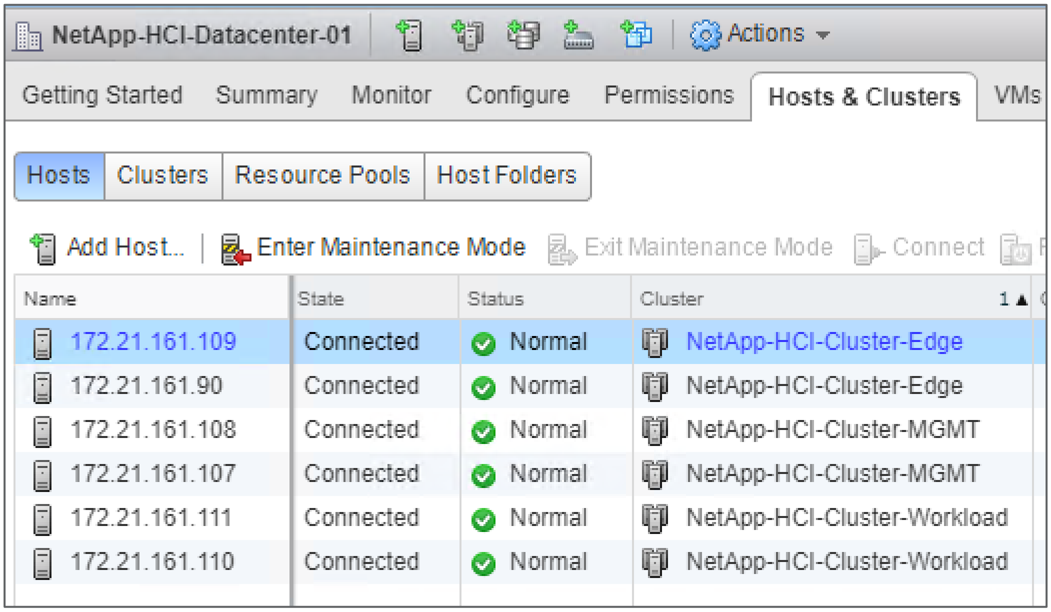
After the successful deployment of NetApp HCI using NDE, there are a few additional activities that you must perform to complete the solution deployment:

1. Addition of compute nodes to the HCI system to deploy additional clusters
2. Expansion of the Element OS configuration to meet the needs of additional clusters
3. Deployment of VMware NSX-V

Add Compute Nodes (for More Clusters)

Post installation, two more clusters (edge and tenant-workload) were created. Two ESXi hosts were added to each newly created cluster. This was done by accessing the NDE URL (https://<storage_node_mgmt_IP:442/scale/login) and completing the following steps:

1. In the first screen, accept VMware EULA and click Continue.
2. Provide the existing vCenter details along with the user name and password of the vCenter.
3. Select your datacenter from the dropdown menu, and, under Cluster, select Create New Cluster. Click Continue.
4. On the ESXi Credentials page, provide the password for the ESXi host.
5. In the Available Inventory screen, select the detected compute nodes and click Continue.
6. Provide the IP address for the management, vMotion, and iSCSI networks for your new compute nodes.
7. Click Continue.
8. Review the information populated on the screen and click Add Nodes.
9. Monitor the progress of the NDE.
10. When the NDE finishes, verify the expansion by checking vCenter for the presence of the new nodes.



Name	State	Status	Cluster 1 ▲
172.21.161.109	Connected	✓ Normal	NetApp-HCI-Cluster-Edge
172.21.161.90	Connected	✓ Normal	NetApp-HCI-Cluster-Edge
172.21.161.108	Connected	✓ Normal	NetApp-HCI-Cluster-MGMT
172.21.161.107	Connected	✓ Normal	NetApp-HCI-Cluster-MGMT
172.21.161.111	Connected	✓ Normal	NetApp-HCI-Cluster-Workload
172.21.161.110	Connected	✓ Normal	NetApp-HCI-Cluster-Workload

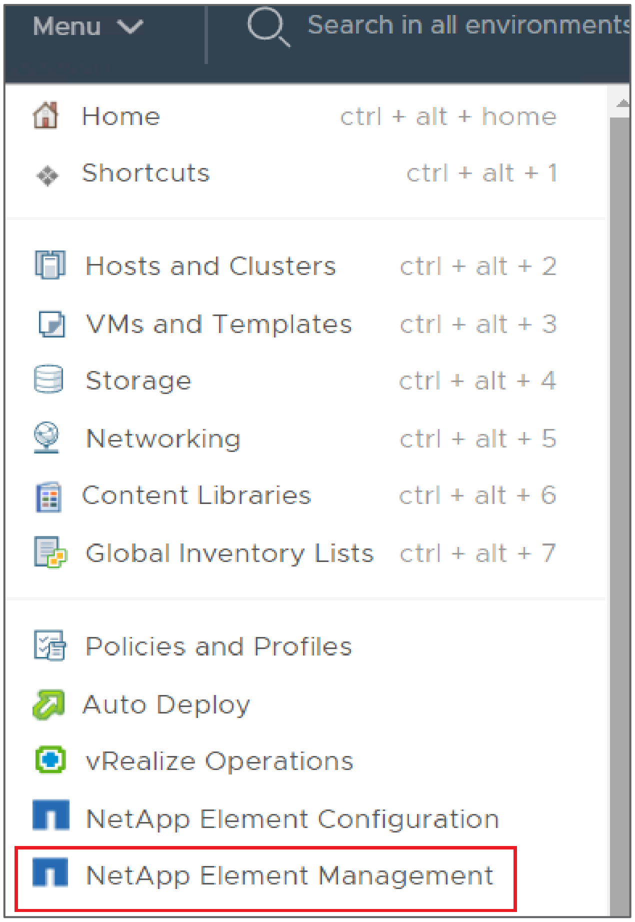
Customization of NetApp Element Configuration

After NDE configuration of Element, the storage configuration was further extended to provide securely separated data access for the tenant-workload cluster. This was done by completing the following two steps:

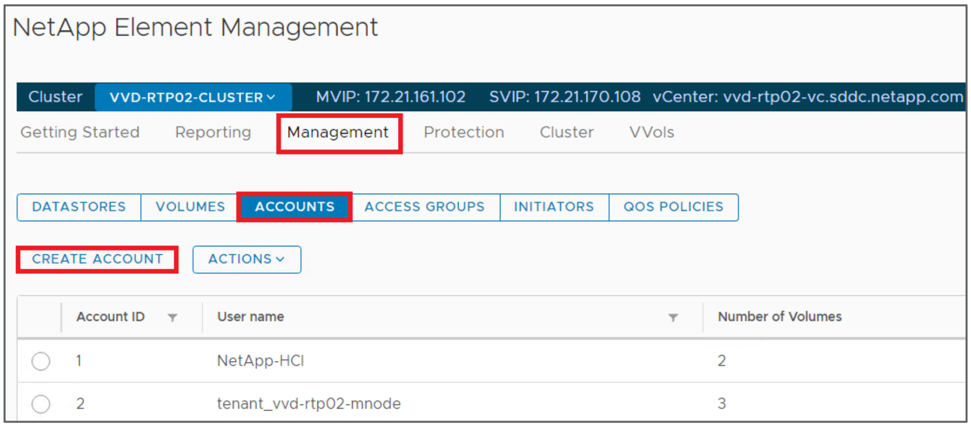
- Create a new account and an associated access group.
- Create two volumes within the newly created account and mount it as a datastore.

1. Login to the vCenter and click the Menu drop-down and select NetApp Element Management

© 2020 NetApp, Inc. All rights reserved.


Menu
Search in all environments
Home ctrl + alt + home
Shortcuts ctrl + alt + 1
Hosts and Clusters ctrl + alt + 2
VMs and Templates ctrl + alt + 3
Storage ctrl + alt + 4
Networking ctrl + alt + 5
Content Libraries ctrl + alt + 6
Global Inventory Lists ctrl + alt + 7
Policies and Profiles
Auto Deploy
vRealize Operations
NetApp Element Configuration
NetApp Element Management

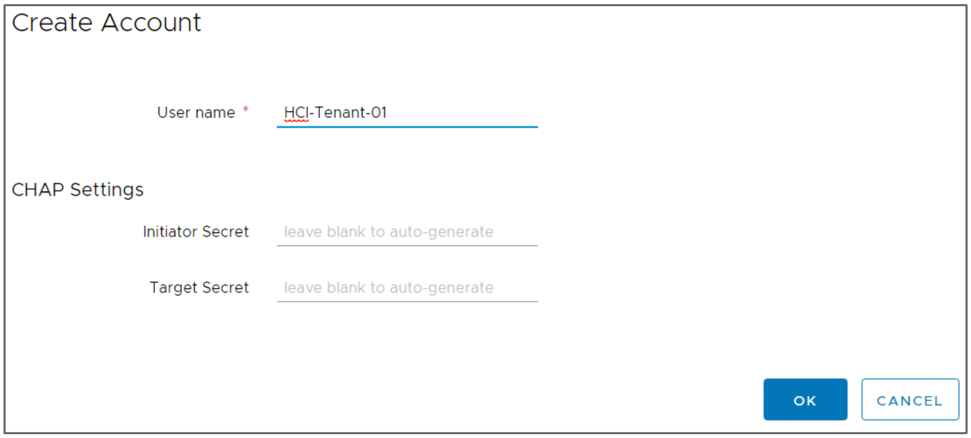
2. On the NetApp Element Management page, click Management >Accounts > Create Account.



	Account ID	User name	Number of Volumes
○	1	NetApp-HCI	2
○	2	tenant_vvd-rtp02-mnode	3

3. Enter the account name and leave the CHAP settings blank.

© 2020 NetApp, Inc. All rights reserved.



Create Account

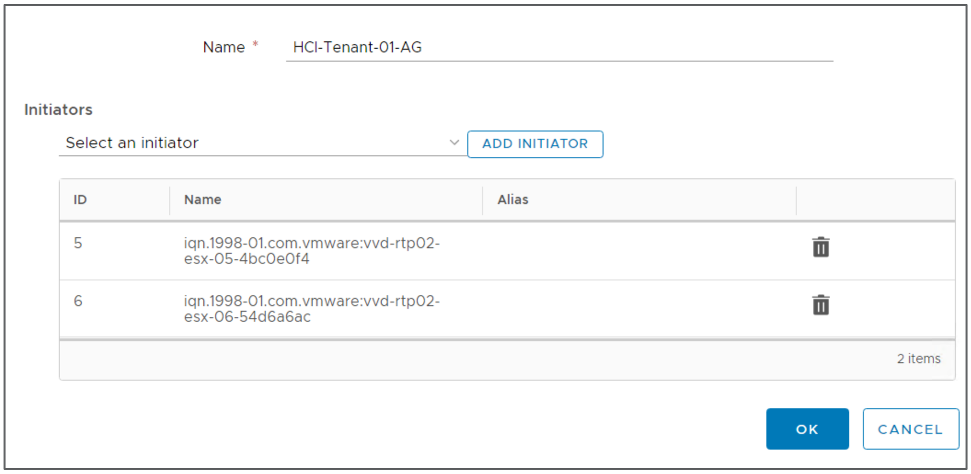
User name * HCI-Tenant-01

CHAP Settings

Initiator Secret leave blank to auto-generate

Target Secret leave blank to auto-generate

4. Go to the Access Group tab and create an Access Group. Then select the ESXi hosts from the tenant-workload cluster.



Name * HCI-Tenant-01-AG

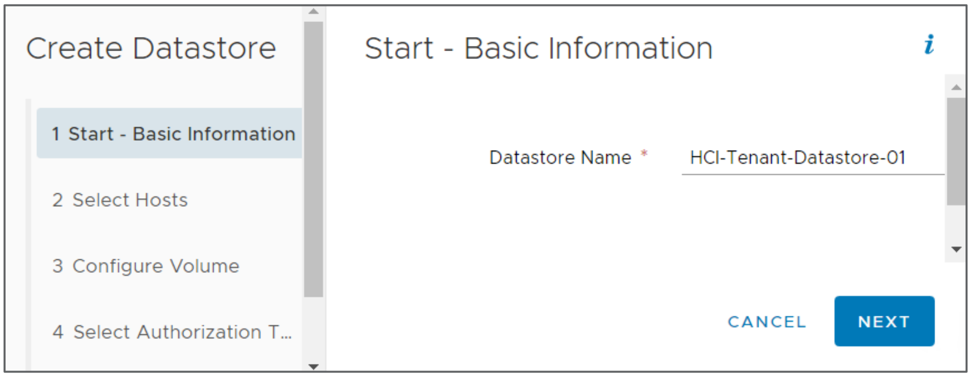
Initiators

Select an initiator

ID	Name	Alias
5	iqn.1998-01.com.vmware:vvd-rtp02-esx-05-4bc0e0f4	
6	iqn.1998-01.com.vmware:vvd-rtp02-esx-06-54d6a6ac	

2 items

5. Go to the Datastore tab and Create a new datastore. Enter the name of the datastore and click Next.



Create Datastore

1 Start - Basic Information

2 Select Hosts

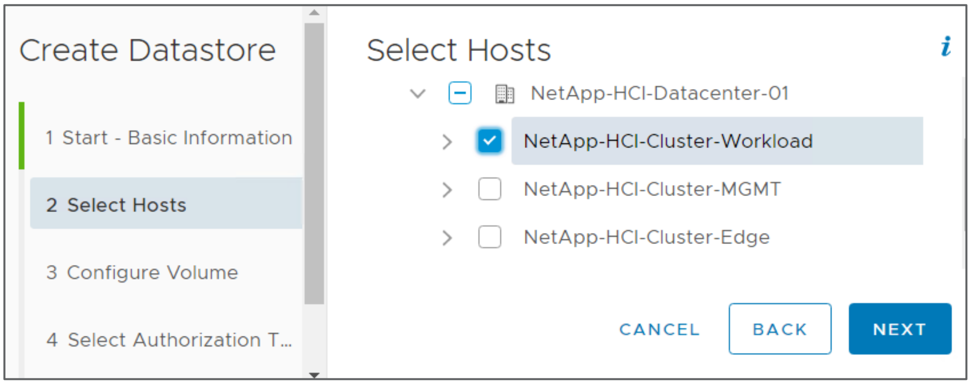
3 Configure Volume

4 Select Authorization T...

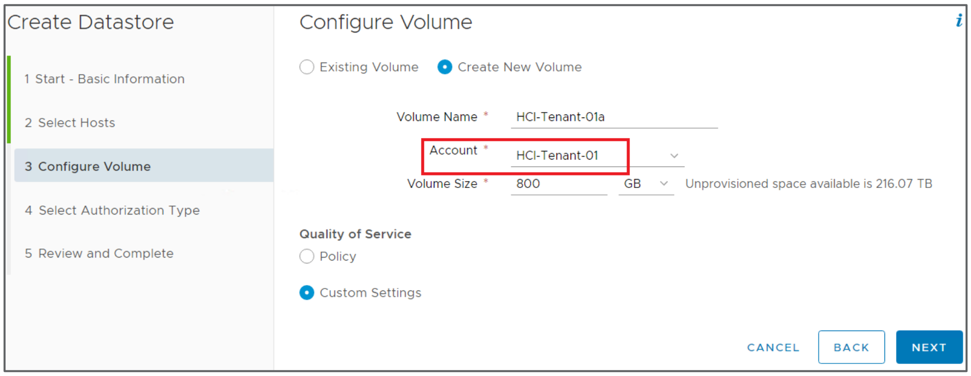
Start - Basic Information

Datastore Name * HCI-Tenant-Datastore-01

6. Select the ESXi hosts from the Workload cluster and click next.


Create Datastore
1 Start - Basic Information
2 Select Hosts
3 Configure Volume
4 Select Authorization T...
Select Hosts
NetApp-HCI-Datacenter-01
☑ NetApp-HCI-Cluster-Workload
□ NetApp-HCI-Cluster-MGMT
□ NetApp-HCI-Cluster-Edge
CANCEL
BACK
NEXT

7. Create a new volume and select Custom Settings under Quality of Service. Make sure to select the correct account to access this volume, and then click next.



○ Existing Volume ● Create New Volume

Volume Name * HCI-Tenant-01a

Account * HCI-Tenant-01

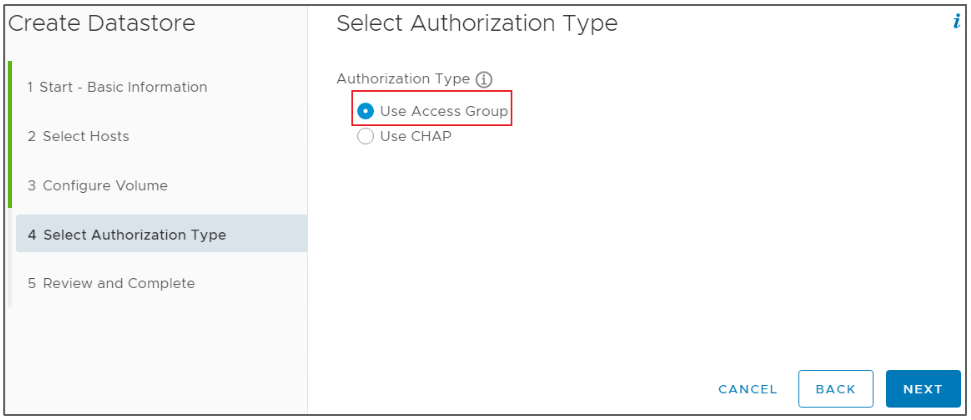
Volume Size * 800 GB Unprovisioned space available is 216.07 TB

Quality of Service

○ Policy

● Custom Settings

8. Under Select Authorization Type, select Use Access Group. Click Next.

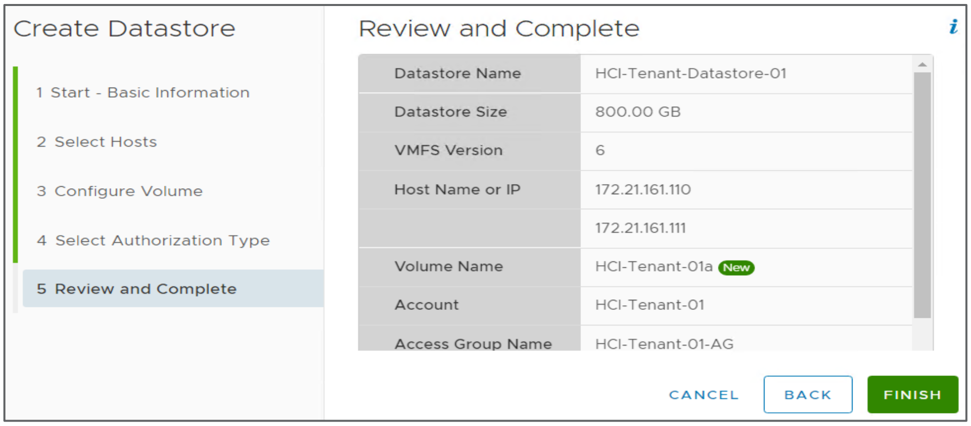


Authorization Type

● Use Access Group

○ Use CHAP

9. Review the details and click Finish.



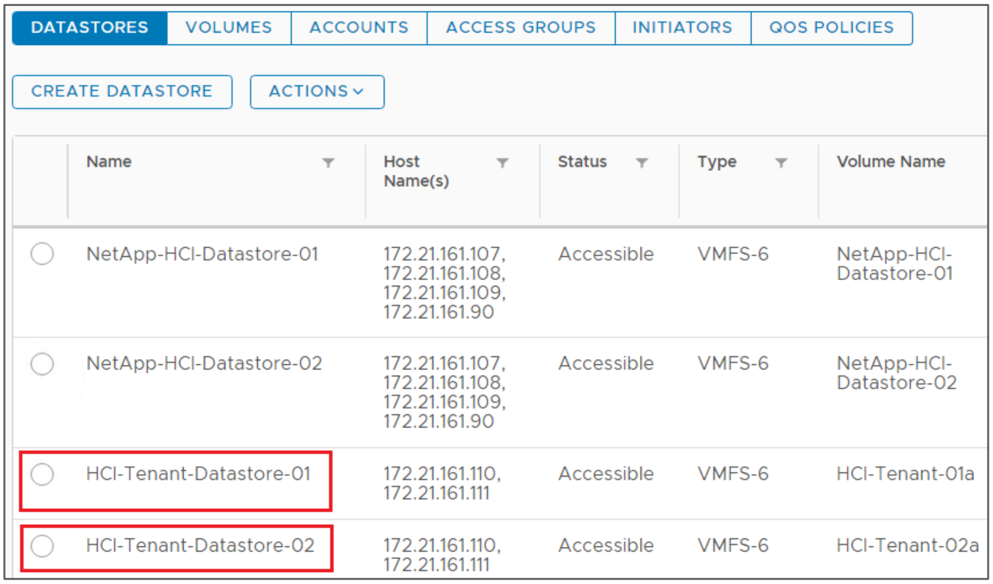
Create Datastore

1 Start - Basic Information
2 Select Hosts
3 Configure Volume
4 Select Authorization Type
5 Review and Complete

Review and Complete

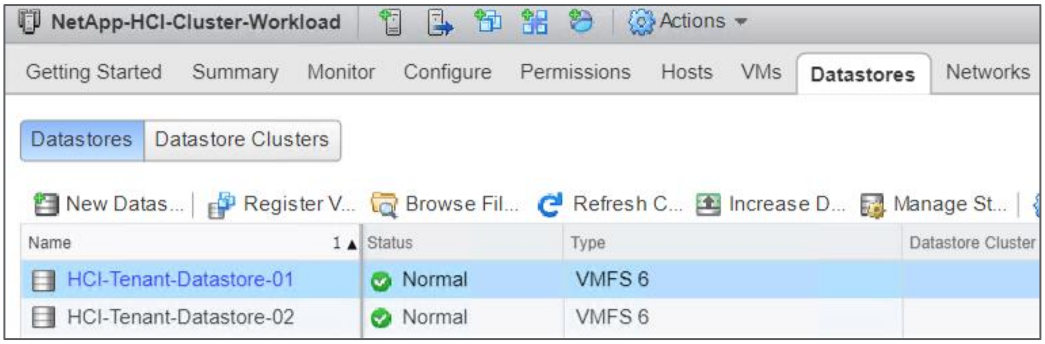
Datastore Name	HCI-Tenant-Datastore-01
Datastore Size	800.00 GB
VMFS Version	6
Host Name or IP	172.21.161.110
	172.21.161.111
Volume Name	HCI-Tenant-01a New
Account	HCI-Tenant-01
Access Group Name	HCI-Tenant-01-AG

10. Create one more datastore following the steps listed as above.
11. Two datastores should be visible under the datastore tab.



	Name	Host Name(s)	Status	Type	Volume Name
○	NetApp-HCI-Datastore-01	172.21.161.107, 172.21.161.108, 172.21.161.109, 172.21.161.90	Accessible	VMFS-6	NetApp-HCI-Datastore-01
○	NetApp-HCI-Datastore-02	172.21.161.107, 172.21.161.108, 172.21.161.109, 172.21.161.90	Accessible	VMFS-6	NetApp-HCI-Datastore-02
○	HCI-Tenant-Datastore-01	172.21.161.110, 172.21.161.111	Accessible	VMFS-6	HCI-Tenant-01a
○	HCI-Tenant-Datastore-02	172.21.161.110, 172.21.161.111	Accessible	VMFS-6	HCI-Tenant-02a

12. Both datastores are automatically mounted to the ESXi hosts of the tenant-workload cluster.



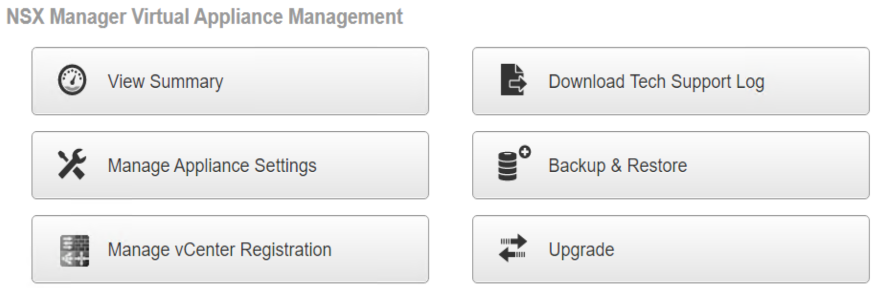
Name 1 ▲	Status	Type	Datastore Cluster
HCI-Tenant-Datastore-01	Normal	VMFS 6	
HCI-Tenant-Datastore-02	Normal	VMFS 6	

VMware NSX Deployment

The following steps deploy and configure NSX:

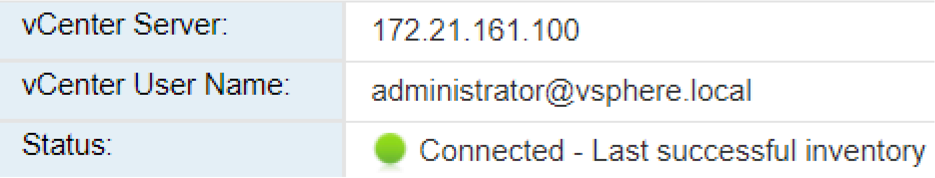
© 2020 NetApp, Inc. All rights reserved.

1. Open a web browser.
2. Enter the IP address for the vCenter previously configured with the NDE.
3. Enter credentials for the admin account entered during NDE.
4. Right-click vCenter in the Navigator pane.
5. Select Deploy OVF Template.
6. In the Select template dialog, select the location where you have your NSX Manager OVA file. Click Next.
7. In the Select Name and Location dialog, enter the name of the new VM and select the datacenter to deploy into. Click Next.
8. In the Select a Resource dialog, select the Management cluster and click Next.
9. In the Review Details dialog, review the details of the new template, and click Next.
10. In the Accept License Agreements dialog, review and click Accept. Click Next.
11. In the Select Storage dialog, select the disk format, leave the VM storage policy as none, and select NetApp-HCI-Datastore-01. Click Next.
12. In the Select Networks dialog, select the Management Network. Click Next.
13. In the Customize Template dialog, complete the following steps:
    a. Enter the DNS server list information.
    a. Enter the domain search list information.
    b. Enter the network properties, including the gateway, hostname, network 1 IP address, and network 1 netmask.
    c. Do not select the check box to enable SSH and enter the NTP server information.
    d. Enter the CLI admin user password and the CLI privilege mode password.
    e. Select whether to join the VMware Customer Experience Improvement Program.
14. Click Next.
15. In the Ready to Complete dialog, review the settings, and click Finish.
16. Review the Recent Tasks pane, and confirm task completion.
17. Right-click the newly created NSX Manager VM.
18. Expand Power and select Power On.
19. Open a web browser and Navigate to https://<ip_address_NSX_Manager.
20. Enter the admin credentials.
21. Click Manage vCenter Registration.


NSX Manager Virtual Appliance Management
View Summary
Download Tech Support Log
Manage Appliance Settings
Backup & Restore
Manage vCenter Registration
Upgrade

22. Click Manage.
23. Select NSX Management Service.
24. Click Edit under vCenter Server.

25. Enter the IP address or FQDN of the vCenter server.
26. Enter the vCenter username and password and Click OK.
27. Click Yes to trust the certificate. vCenter Status should be connected.



vCenter Server:	172.21.161.100
vCenter User Name:	administrator@vsphere.local
Status:	● Connected - Last successful inventory

28. Return to your vCenter web client.
29. Click Home.
30. Click Licensing.
31. In the Licenses pane, click the + icon to add a new license.
32. In the Enter License Key dialog, enter your licenses in the text box.
33. Click Next.
34. In the Edit License Names dialog, optionally modify the license name.
35. Click Next.
36. In the Ready to Complete dialog, review the licenses to be added.
37. Click Finish.
38. Under the Licenses tab, review the licenses that have been added.
39. Navigate to the Assets tab.
40. Select Solutions under the Assets tab.
41. Select Assign License.
42. In the Assign License wizard, select the NSX for vSphere – Enterprise license.
43. Click Ok.
44. Select Home > Networking & Security.
45. Select Installation and Upgrade.
46. Select the NSX Controller Node tab.
47. Click the + ADD icon.
48. Select the NSX Manager.
49. In the Password Settings dialog, enter the credentials for the NSX Manager.
50. Click Next.
51. In the Deployment & Connectivity dialog, complete the following steps:

    f. Select the first NSX controller.

    a. Select NetApp-HCI-Datacenter-01.

    b. Select NetApp-HCI-Cluster-Edge.

    c. Select NetApp-HCI-Datastore-01.

    d. Select a host.

    e. Select the Management Network of VDS.

    f. Select the IP pool and, in the wizard, create a new IP pool.

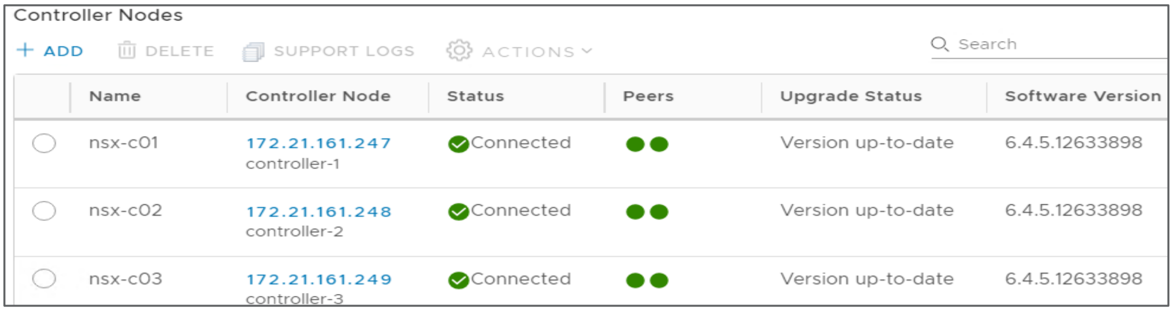
    g. Enter the name of the IP pool.

    h. Enter the gateway.

   i. Enter the prefix length.
   j. Enter the primary DNS.
   k. Enter the secondary DNS.
   l. Enter the DNS suffix.
   m. Click the + ADD icon to add an IP address range.
   n. Enter the IP address range.
   o. Click ADD.
   p. Select the newly created IP pool.
   q. Click OK.

52. Click Finish.
53. Review the Status column of hci-nsx-controller-1 and wait until ✓ Connected is shown.

Note: Repeat step 28 (including sub steps) through step 30 for the remaining two controller nodes.



Controller Nodes

	Name	Controller Node	Status	Peers	Upgrade Status	Software Version
○	nsx-c01	172.21.161.247 controller-1	✓ Connected	●●	Version up-to-date	6.4.5.12633898
○	nsx-c02	172.21.161.248 controller-2	✓ Connected	●●	Version up-to-date	6.4.5.12633898
○	nsx-c03	172.21.161.249 controller-3	✓ Connected	●●	Version up-to-date	6.4.5.12633898

54. Select the Host Preparation tab.
55. Select the Management cluster.
56. Click the Install NSX Icon.
57. Click Yes.
58. Click the Configure VXLAN icon.
59. Select the HCI Compute switch.
60. Enter the VLAN ID for the VM network.
61. Keep the default for the MTU.
62. Select the IP Pool radial.
63. Select the IP Pool icon and in the wizard create a new IP Pool.
   a. Enter the name of the IP pool.
   b. Enter the gateway.
   c. Enter the prefix length.
   d. Enter the primary DNS
   e. Enter the secondary DNS
   f. Enter the DNS suffix.
   g. Click the + ADD icon to add an IP address range.
   h. Enter the IP address range.
   i. Click ADD.
64. Set vmkNIC Teaming Policy to Load Balance – SRCID.

65. Click Save.
66. Select NetApp-HCI-Cluster-Edge.
67. Click the Install NSX icon.
68. Click Yes.
69. Click the Configure VXLAN icon.
70. Select the HCI Compute switch.
71. Enter the VLAN ID for the VM Network.
72. Keep the default for the MTU.
73. Select the IP Pool radial.
74. Set the vmkNIC Teaming Policy to Load Balance – SRCID.
75. Click Save
76. Select the Logical Network Settings.
77. Under the VXLAN settings, Click Edit under Segment IDs.
78. Specify the range of available IDs in the ID pool.
79. Click Save.
80. Select the Transport Zone icon.
81. Click the + ADD icon.
82. Enter the name VXLAN-Global-Transport.
83. Select Unicast as the Replication Mode.
84. Select all clusters.
85. Click Add.
86. Select Logical Switches on the Navigator pane.
87. Click the + icon to add a New Logical Switch.
88. Enter the name of the new logical switch.
89. Enter the description of the new logical switch.
90. Enter the VXLAN-Global-Transport zone.
91. Select Unicast as the Replication Mode.
92. Click OK.

Note: Repeat these steps as needed for additional VXLANs.

Automated Installation of VMware NSX-V

NetApp provides a sample Python script at GitHub for automating the deployment of NSX. The operations that this NSX deployment script perform are as follows:

1. Deploys NSX Manager.
2. Registers NSX Manager with vCenter.
3. Deploys the NSX controllers.
4. Prepares the hosts and the cluster for NSX.
5. Prepares and configures logical networking.

The automated installation of NSX is split into of four phases:

1. Preparation of the environment to run the sample script.
2. Deployment of the NSX Manager.

3. Configuration of the NSX Manager.
4. Confirmation of the successful deployment of NSX.

Preparation of the Environment

To prepare the environment to execute the sample script, complete the following steps.

1. Install Python 3.6.6 on a system with access to the management network of the HCI environment.
2. Install the required packages.

```
pip3 install --upgrade pyvim requests vcrpy pyvmomi suds-jurko lxml ipaddress
```

3. Install Git with the Windows or Linux installer. Add the Git binary location to PATH (if not completed by the installer).
4. Download the pyVmomi community samples from GitHub.

```
git clone https://github.com/vmware/pyvmomi-community-samples.git
```

5. Install the pyVmomi community samples from the directory.

```
setup.py install
```

6. Clone the pyNSXdeploy scripts from the NetApp GitHub site to a local directory.

```
git clone https://github.com/solidfire/pyNSXdeploy/blob/master/deploy_nsx_manager.py
```

7. Copy the `tools` directory to the `pyNSXdeploy` directory under `pyvmomi-community-samples/samples/tools`.

Deployment of NSX Manager

After the environment has been prepared to run the script, complete the following step to deploy NSX Manager.

1. Modify and execute the sample script to deploy NSX Manager.

```
python ./deploy_nsx_manager.py -s vvd-rtp02-vc.sddc.netapp.com -u administrator@vsphere.local -p
NetApp!23 -S -ds NetApp-HCI-Datastore-02 --ova-path "E:\Software\VMware\NSX\VMware-NSX-Manager-
6.4.5-13282012.ova" -vsm_cli_passwd_0 NetApp!23NetApp!23 -vsm_cli_en_passwd_0 NetApp!23NetApp!23
-vsm_hostname vvd-rtp02-nsx-01 -vsm_ip_0 172.21.161.140 -vsm_netmask_0 255.255.255.0 -
vsm_gateway_0 172.21.161.1 -vsm_ntp_0 10.61.185.177 -vsm_dns1_0 10.61.186.231 -
map_eth0_to_network "Management Network" -cluster Management
```

Note: Wait for 5-10 minutes before configuring NSX Manager.

Configuration of NSX Manager

After deploying NSX Manager, complete the following step to configure NSX Manager.

1. Modify and execute the sample script to configure NSX Manager.

```
Python ./configure_nsx_manager.py -nsx_manager_address nsxmanager1.vvd.local -
nsx_manager_username admin -nsx_manager_password NetApp123!NetApp123! -s vvd-vcsa1.vvd.local -u
administrator@vsphere.local -p NetApp123! -S -VTEP_IP_Range 172.21.165.20-172.21.165.30 -
VTEP_Mask /24 -VTEP_Gateway 172.21.165.1 -VTEP_DNS 10.61.186.231 -VTEP_domain vvd.local -
lookup_service_address vvd-vcsa1.vvd.local -VTEP_VLAN_ID 20 -Controller_IP_Range 172.21.161.247-
172.21.161.251 -Controller_Mask /24 -Controller_Gateway 172.21.161.1 -Controller_Cluster
Management -Controller_DNS 10.61.186.231 -Controller_domain vvd.local -Controller_Datastores
Management_Cluster_Datastore_1,Management_Cluster_Datastore_2,Management_Cluster_Datastore_3 -
Controller_Network Management_VMs -Controller_Password NetApp123!NetApp123! -DVS Compute_DVS -
cluster_prep_list Compute -key <insert NSX license key>
```

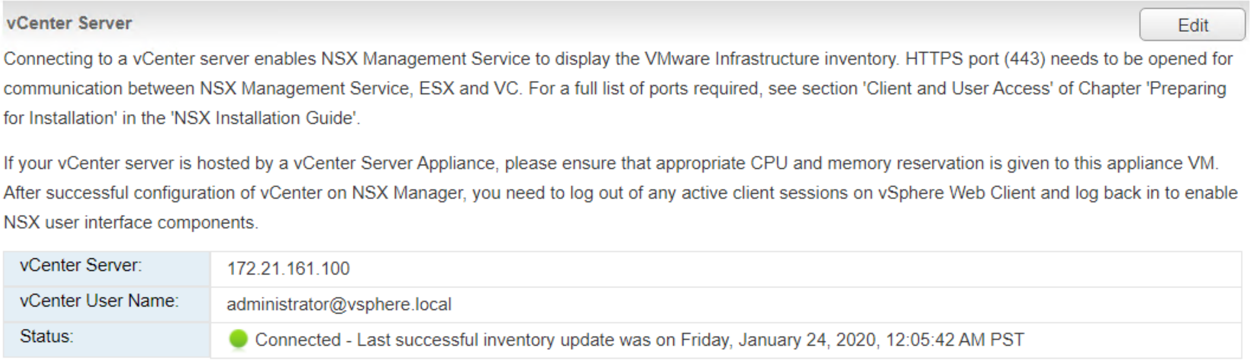
Note: Insert the NSX license key for `Compute -key`.

© 2020 NetApp, Inc. All rights reserved.

Confirm the Successful Deployment of NSX

To confirm the NSX deployment, complete the following steps:

1. Navigate to `https://<ip_address_NSX_Manager`.
2. Enter the admin credentials.
3. Click Manage.
4. Click NSX Management Service and verify vCenter connectivity.



Connecting to a vCenter server enables NSX Management Service to display the VMware Infrastructure inventory. HTTPS port (443) needs to be opened for communication between NSX Management Service, ESX and VC. For a full list of ports required, see section 'Client and User Access' of Chapter 'Preparing for Installation' in the 'NSX Installation Guide'.

If your vCenter server is hosted by a vCenter Server Appliance, please ensure that appropriate CPU and memory reservation is given to this appliance VM. After successful configuration of vCenter on NSX Manager, you need to log out of any active client sessions on vSphere Web Client and log back in to enable NSX user interface components.

vCenter Server:	172.21.161.100
vCenter User Name:	administrator@vsphere.local
Status:	● Connected - Last successful inventory update was on Friday, January 24, 2020, 12:05:42 AM PST

Deploy ESG

1. Select NSX Edges in the Navigator pane. Click the + icon.
2. In the Name and Description dialog, complete the following steps:
   a. Select Edge Services Gateway as the Install Type.
   b. Enter the name of the gateway.
   c. Optionally, enter a hostname.
   d. Optionally, enter a description and tenant.
   e. Leave the Deploy NSX Edge checkbox selected and Click Next.
   f. Enter and confirm the admin password and Click Next.
3. In the Configure deployment dialog complete the following steps:
   a. Select the HCI datacenter.
   b. Select the appropriate appliance size and click the + icon.
   c. Select NetApp-HCI-Cluster-Edge.
   d. Select HCI Datastore 02. Click OK and Next.
4. In the Configure Interfaces dialog complete the following steps:
   a. Click the + icon.
   b. Enter the name of the NSX Edge interface.
   c. Select Type: Uplink.
   d. Click select to connect the NSX Edge to a network.
   e. Select the appropriate logical switch for this connection. Click OK.
   f. Click the + icon.
   g. Enter the primary IP address.
   h. Enter the Subnet Prefix Length, Click OK.
   i. Click Next.
5. In the Default gateway settings dialog, complete the following steps:

© 2020 NetApp, Inc. All rights reserved.

    a. Leave the Configure Default Gateway checkbox selected.
    b. Select the appropriate vNIC.
    c. Enter the Gateway IP.
    d. Click Next.
6. In the Firewall and HA dialog, accept the defaults, click Next, review the setting, and click Finish.

Deploy DLR

1. Select NSX Edges in the Navigator pane. Click the + icon.
2. In the Name and Description dialog, complete the following steps:
    a. Select Logical Router as the Install Type.
    b. Enter the name of the logical router.
    c. Optionally, enter a host name.
    d. Optionally, enter a description and a tenant.
    e. Leave the Deploy NSX Edge checkbox selected and Click Next.
    f. Enter and confirm the admin password and Click Next.
3. In the Configuration deployment dialog, complete the following steps:
    a. Select the HCI datacenter.
    b. Select the appropriate appliance size. Click the + icon.
    c. Select NetApp-HCI-Cluster-Edge.
    d. Select HCI Datastore 02. Click OK and Next.
4. In the Configure Interfaces dialog complete the following steps:
    a. Click the + icon.
    b. Enter the name of the NSX Edge interface.
    c. Select Type: Uplink.
    d. Click select to connect the NSX Edge to a logical switch that provides mapping with the ESG instance.
    e. Select the appropriate logical switch for this connection. Click OK.
    f. Click the + icon.
    g. Enter the primary IP address.
    h. Enter the Subnet Prefix Length. Click OK and click Next.
5. In the Name and Description settings dialog, complete the following steps:
    a. Uncheck the Configure Default Gateway checkbox.
    b. Select the appropriate vNIC.
    c. Click Next.
    d. Review the details and Click Finish.

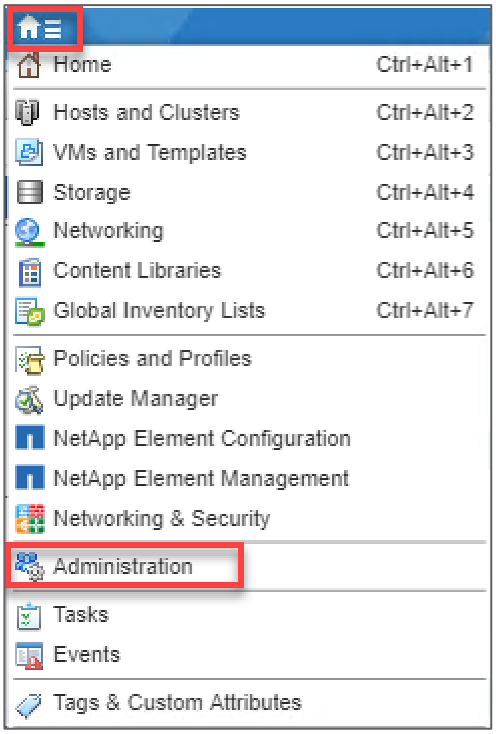
Active Directory Considerations

Organizations that use Windows Active Directory should add the vCenter instance to their environment. This simplifies user management and improves auditing. The steps in this section detail how to join the vCenter instance to Active Directory and add Active Directory authentication in vCenter.

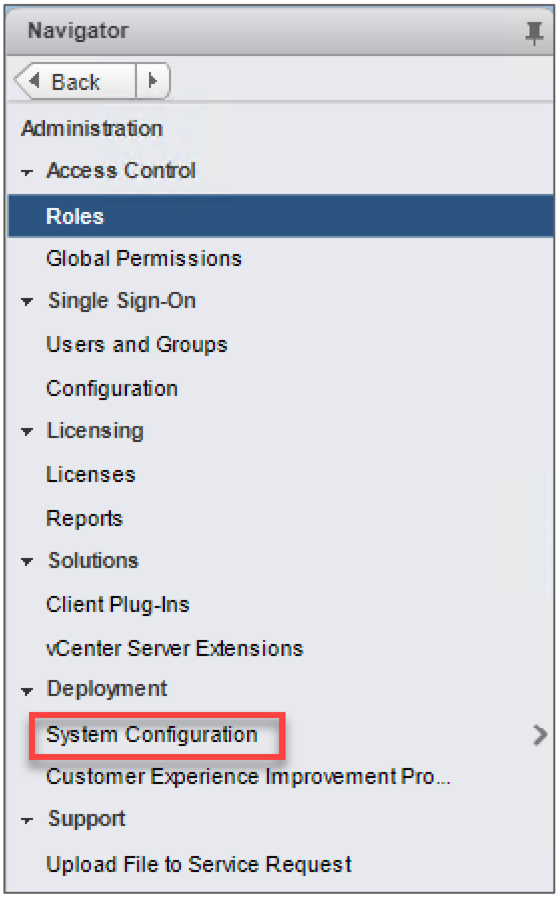
Join vCenter Instance to Active Directory

To join the vCenter instance to Active Directory, complete the following steps:

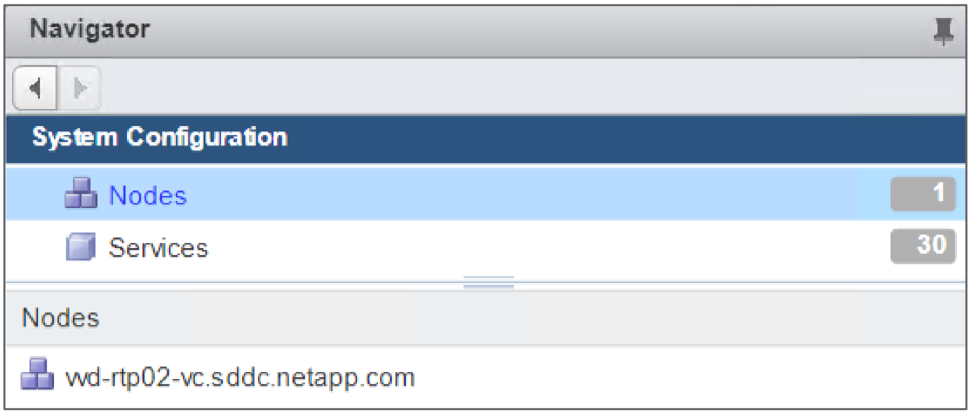
1. Log in to the vSphere Web Client.
2. Navigate to Home > Administration.


Home Ctrl+Alt+1
Hosts and Clusters Ctrl+Alt+2
VMs and Templates Ctrl+Alt+3
Storage Ctrl+Alt+4
Networking Ctrl+Alt+5
Content Libraries Ctrl+Alt+6
Global Inventory Lists Ctrl+Alt+7
Policies and Profiles
Update Manager
NetApp Element Configuration
NetApp Element Management
Networking & Security
Administration
Tasks
Events
Tags & Custom Attributes

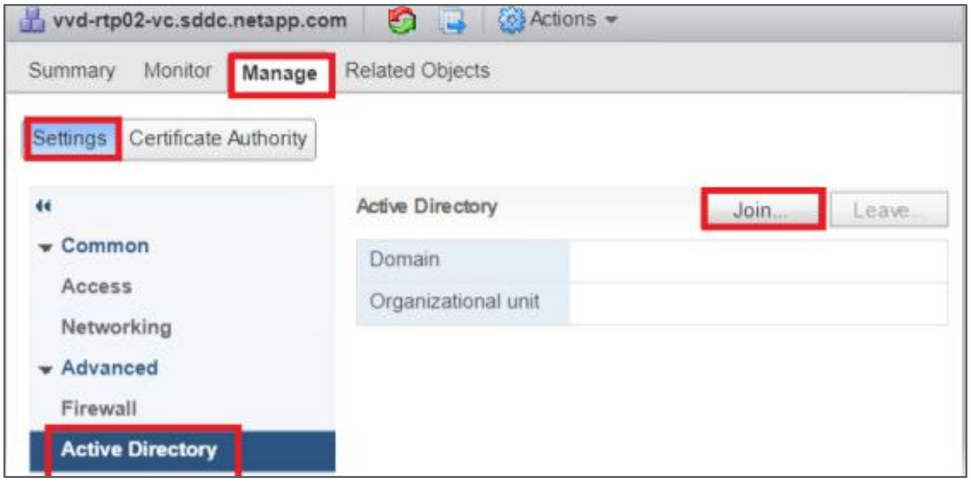
3. Under Deployment, select System Configuration.



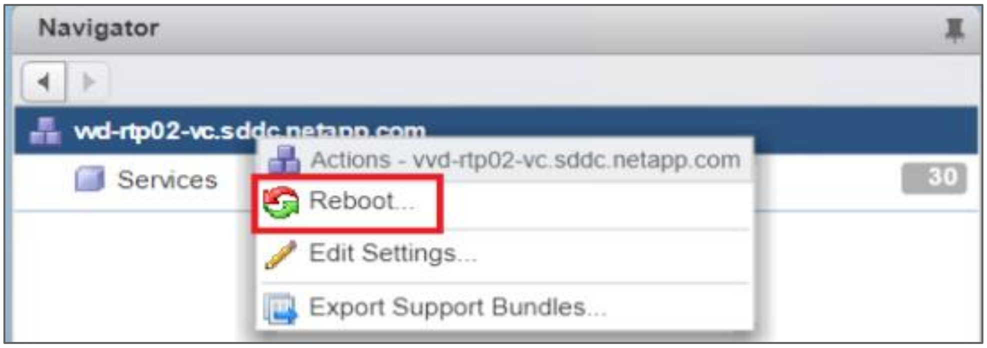
4. Navigate to Nodes and select the vCenter FQDN.



5. Go to Manage > Settings > Advanced > Active Directory and click Join.



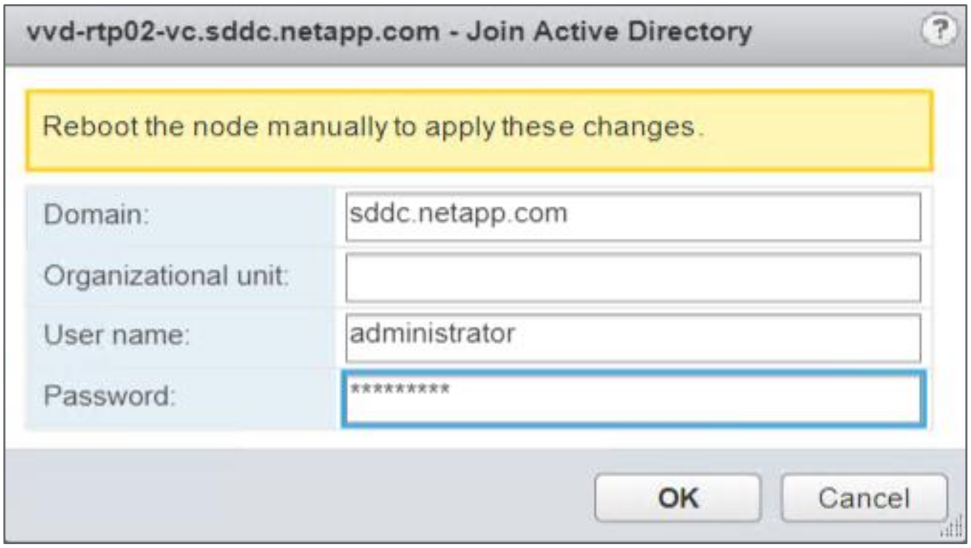
6. Enter the domain, organization unit, user name, and password. Click OK.
7. Reboot vCenter by selecting Nodes, right-clicking vCenter FQDN, and then selecting Reboot.


Navigator
vvd-rtp02-vc.sddc.netapp.com
Services
30
Actions - vvd-rtp02-vc.sddc.netapp.com
Reboot...
Edit Settings...
Export Support Bundles...

Add Active Directory Authentication in vCenter

To add Active Directory Authentication in vCenter, complete the following steps:

1. Log in to the vSphere Web Client as a single sign-on administrator.


vvd-rtp02-vc.sddc.netapp.com - Join Active Directory

Reboot the node manually to apply these changes.

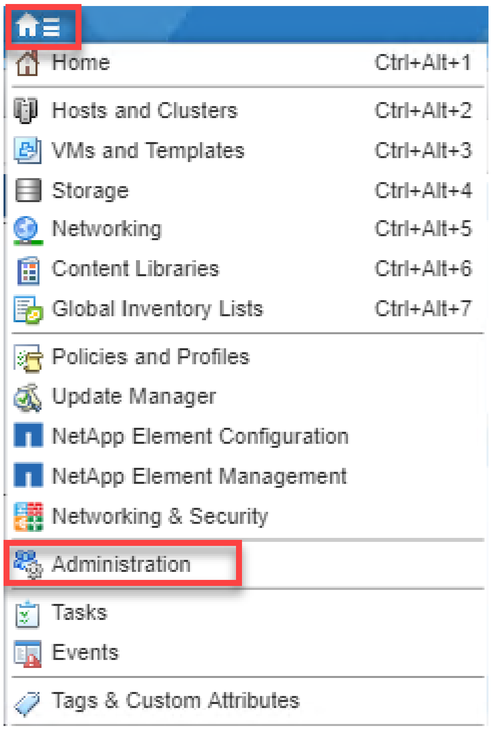
Domain: sddc.netapp.com

Organizational unit:

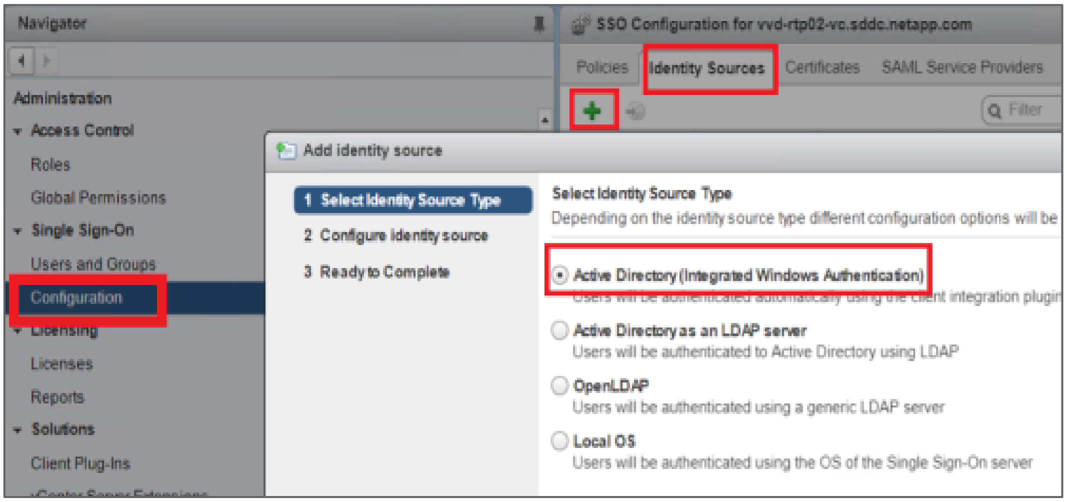
User name: administrator

Password: *********

2. Navigate to Home > Administration.


Home Ctrl+Alt+1
Hosts and Clusters Ctrl+Alt+2
VMs and Templates Ctrl+Alt+3
Storage Ctrl+Alt+4
Networking Ctrl+Alt+5
Content Libraries Ctrl+Alt+6
Global Inventory Lists Ctrl+Alt+7
Policies and Profiles
Update Manager
NetApp Element Configuration
NetApp Element Management
Networking & Security
Administration
Tasks
Events
Tags & Custom Attributes

3. Under Single Sign-On, select Configuration > Identity Sources > Add.



Select Identity Source Type

Depending on the identity source type different configuration options will be

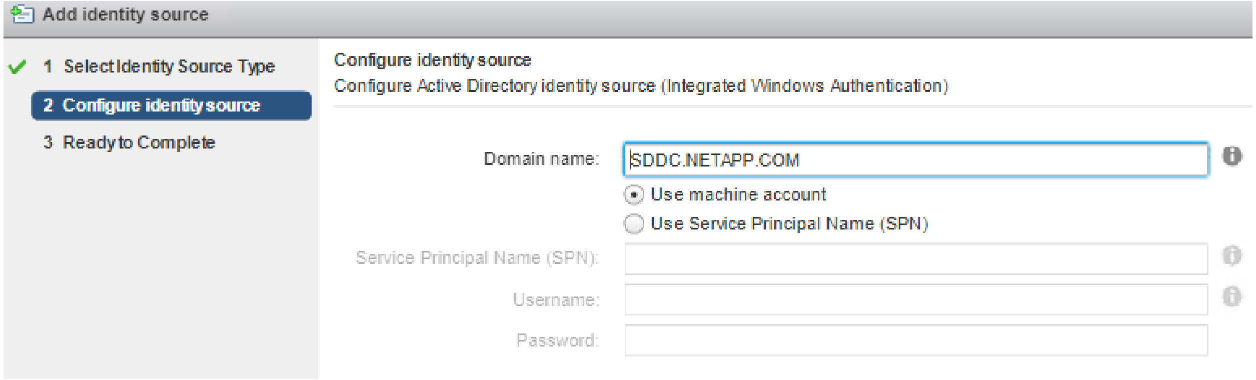
● Active Directory (Integrated Windows Authentication)
Users will be authenticated automatically using the client integration plugin

○ Active Directory as an LDAP server
Users will be authenticated to Active Directory using LDAP

○ OpenLDAP
Users will be authenticated using a generic LDAP server

○ Local OS
Users will be authenticated using the OS of the Single Sign-On server

4. Select Active Directory (Integrated Windows Authentication), and then click Next.



Add identity source

✓ 1 Select Identity Source Type

2 Configure identity source

3 Ready to Complete

Configure identity source

Configure Active Directory identity source (Integrated Windows Authentication)

Domain name: SDDC.NETAPP.COM

● Use machine account

○ Use Service Principal Name (SPN)

Service Principal Name (SPN):

Username:

Password:

5. Click Finish.

VMware Licensing

NetApp HCI uses VMware vCenter Server to manage and monitor the VMware ESXi hypervisor installed on each compute node. In this validation, a new vCenter was deployed during the installation process.

The vCenter Server license used during NDE is a temporary evaluation license. For continued operation after the evaluation period, you must obtain a new license key from VMware and add it to the vCenter Server license inventory. Navigate to the licensing pane within vCenter and add the Enterprise Plus license.

VMware vSphere Distributed Switch (VDS) Configuration

A SDDC requires VMware's software-defined networking offering, NSX. The NDE deploys a single vDS as part of the initial configuration. In preparation for NSX, the two-cable configuration takes advantage of this single vDS. However, a separate vDS is created for workload cluster ESXi hosts and the deafult vDS created by NDE is used by the ESXi host from the management and edge clusters.

6.2 HyTrust CloudControl Deployment

HTCC offers system managers and administrators an end-to-end virtualization security platform to manage access, standardize and control configuration, and protect a virtual infrastructure within a customer's environment.

Network Architecture and Topology

HTCC relies on customers' network topology to gain visibility to the virtual infrastructure's management traffic to be able to intercept it. HTCC works as a proxy server and does not require any architectural changes to the virtual infrastructure (VI) network. Each CloudControl-protected host is assigned a dedicated IP address (PIP), which management clients use to access the host.

To proxy the management traffic within the existing network requires the following prerequisites:

- CloudControl should be able to communicate with the service console (VMkernel port for ESXi) of each protected host.
- For each protected host, a new PIP address is used by end users to access the host.
- The PIP addresses must be on a subnet local to the CloudControl Connection 1 (eth0) interface and not an address that belongs to a remote, routed network.

HTCC is deployed in HA mode, with primary and secondary CloudControl instances. To facilitate HA configuration, HTCC requires a dedicated private network between the two HTCC instances. The HTCC HA VLAN is used for this purpose.

Install HyTrust CloudControl in High-Availability Configuration

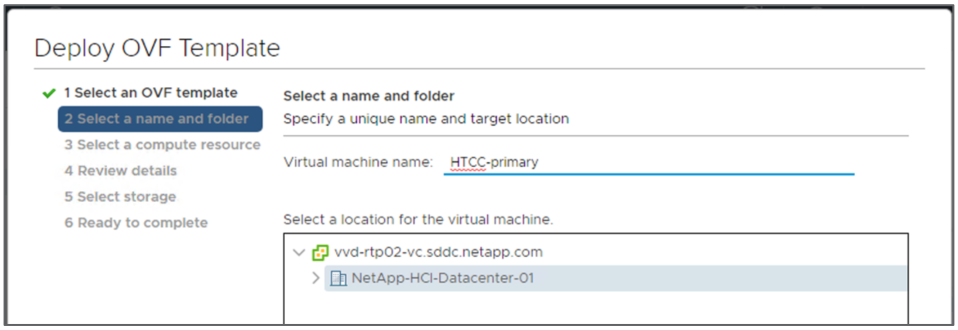
HTCC is installed in the management cluster within the VMware environment.

Obtaining the Software

Log in to the HyTrust website or follow the directions you received from HyTrust Support to obtain the download URL of the HTCC OVF file.

Install Primary HTCC Appliance

1. From the Home menu in the vSphere Web Client, select VMs and Templates under the Inventories section.
2. Right-click the data center NetApp-HCI-Datacenter-01 or the VM folder, and select Deploy OVF Template.
3. Click Allow.
4. Browse to the OVF file of the HTCC appliance and click Open.
5. Click Next.
6. Review the OVF template details and click Next.
7. Accept the license agreement and click Next.
8. Enter a name for the HTCC primary appliance and select a folder or data center where it should reside.


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 a name and folder

Specify a unique name and target location

Virtual machine name: HTCC-primary

Select a location for the virtual machine.

vvd-rtp02-vc.sddc.netapp.com

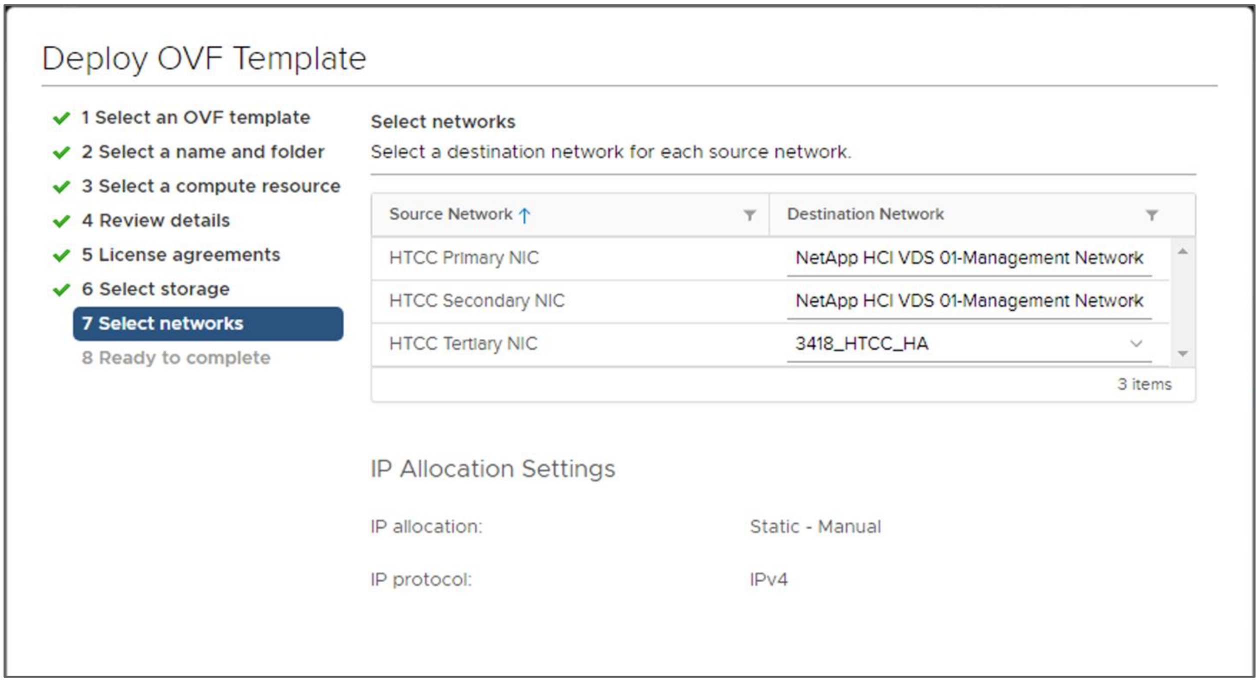
NetApp-HCI-Datacenter-01

9. Click Next.
10. Select the NetApp-HCI-Cluster-MGMT cluster and click Next.
11. Select NetApp-HCI-Datastore-01 as the storage and click Next.
12. Assign the appliance NICs as follows:
13. HTCC primary NIC (eth0) → NetApp HCI VDS-01 management network

– HTCC secondary NIC (eth1) → NetApp HCI VDS-01 management network (this NIC is unused)

14. HTCC tertiary NIC (eth2) → 3418_HTCC_HA

© 2020 NetApp, Inc. All rights reserved.



Deploy OVF Template

Select networks

Select a destination network for each source network.

Source Network ↑	Destination Network
HTCC Primary NIC	NetApp HCI VDS 01-Management Network
HTCC Secondary NIC	NetApp HCI VDS 01-Management Network
HTCC Tertiary NIC	3418_HTCC_HA

3 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

15. Click Next.
16. Review the settings and click Finish.
17. Wait for the OVF template to be deployed.
18. Select the HTCC primary VM from the Inventory pane and from the Summary tab click Launch Remote Console.
19. Click Launch Application if prompted.
20. Click the green button (second from left) to power on the VM.

Configure Primary HTCC Management Network Interface

1. In the console window of the HTCC VM, log in as `ascadminuser` with the password `Pa$$w0rd123!`.
2. Enter the current password, `Pa$$w0rd123!`.
3. Assign a new password for the ascadminuser and reenter the password to confirm.
4. Start the setup procedure by running the `setup` command.
5. Enter `y` when asked to configure a virtual management IP address.
6. Enter the IPv4 address for virtual management, `<<var_htcc_virt_mgmt_ip>>`.

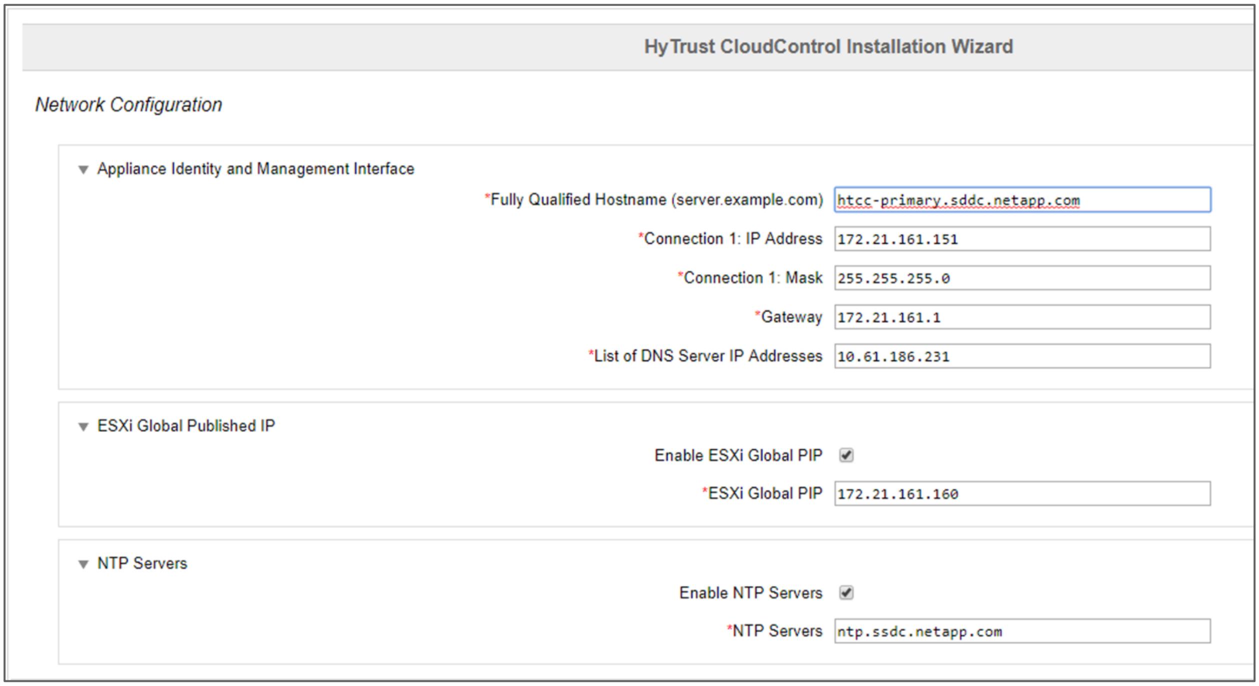
   Note: The virtual management IP is used for HA.
7. Enter the IPv4 address for the HTCC primary node network connection (eth0) interface, `<<var_htcc_pri_mgmt_ip>>`.
8. Enter the netmask, `<<var_htcc_pri_netmask>>`.
9. Enter the gateway, `<<var_htcc_pri_gw>>`.
10. Enter the DNS server IP addresses.
11. Review the network settings and confirm.
12. Log out after the network settings are updated.

13. Open a web browser and navigate to `https://<<var_htcc_pri_mgmt_ip>>/asc`.

    Note: FQDN is not supported until the installation wizard completes.

    Note: Use the IPv4 address.

14. Allow the security exceptions if prompted.
15. Log in using the default user name `superadminuser` and password `Pa$$w0rd123!`.
16. Accept the license agreement and click Next.
17. Upload the license file with the `.xml` extension and click Next.
18. In the Network Configuration page, assign a host name for the HTCC primary appliance and review the network settings.



HyTrust CloudControl Installation Wizard

Network Configuration

▼ Appliance Identity and Management Interface

*Fully Qualified Hostname (server.example.com): htcc-primary.sddc.netapp.com

*Connection 1: IP Address: 172.21.161.151

*Connection 1: Mask: 255.255.255.0

*Gateway: 172.21.161.1

*List of DNS Server IP Addresses: 10.61.186.231

▼ ESXi Global Published IP

Enable ESXi Global PIP ☑

*ESXi Global PIP: 172.21.161.160

▼ NTP Servers

Enable NTP Servers ☑

*NTP Servers: ntp.ssdc.netapp.com

19. Update the (comma separated) list of DNS servers if necessary.

    Note: Provide only IP addresses for DNS servers.

20. Check the checkbox to enable the use of a global PIP instead of individual PIP addresses for each ESXi host.
21. Enter the IP address to use for the global PIP.
22. Select the Enable NTP Servers checkbox and enter the NTP server IP addresses (comma separated).

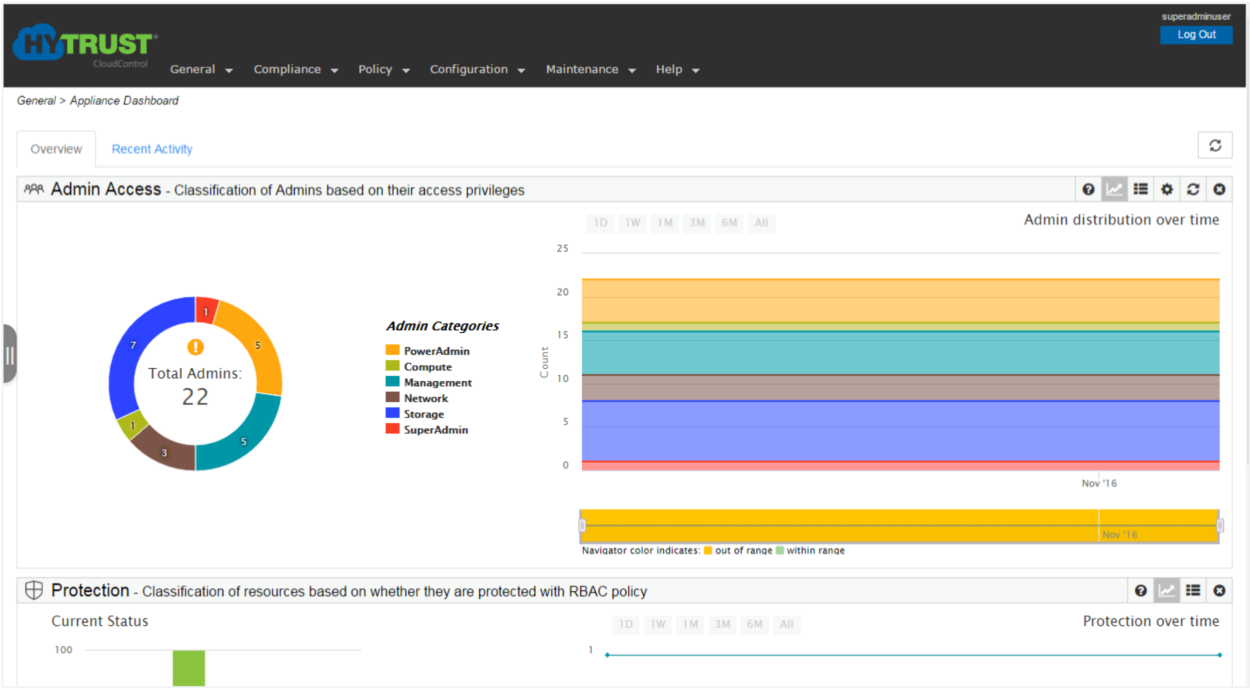
    Note: Provide only IP addresses for NTP servers.

23. Click Next.
24. Click Finish to complete the installation wizard.

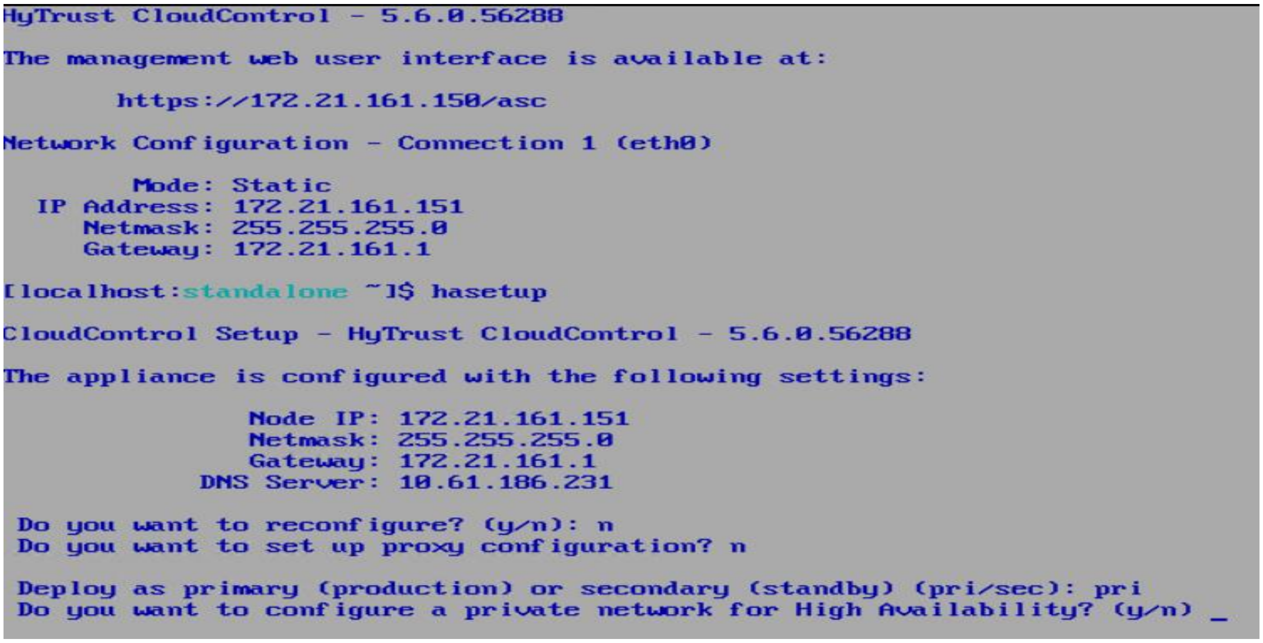
    Note: The Finish button is not enabled until the installation wizard completes.

25. Upon successful installation, the HTCC Management Console Appliance dashboard appears.

© 2020 NetApp, Inc. All rights reserved.



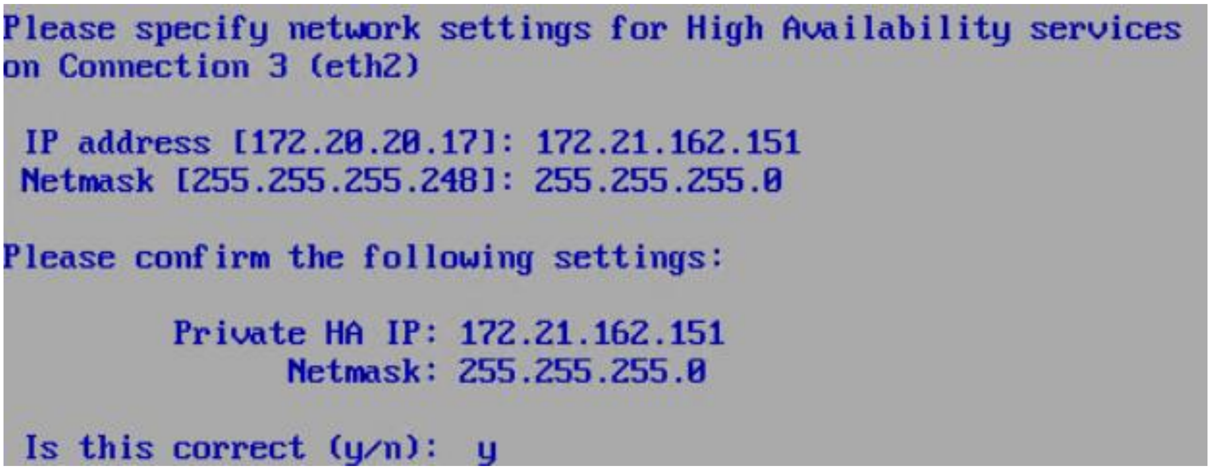
26. From the vSphere Web Client, connect to the console of the HTCC primary VM.
27. Log in as `ascadminuser`.
28. Start the HA setup procedure by running the `hasetup` command.
29. At the `Please specify network settings for the Connection 1 (eth0)` interface prompt, confirm the settings assigned to the primary HTCC. Enter `n` to skip reconfiguring the network settings and Proxy Configuration settings.
30. At the `Deploy as primary (production) or secondary (standby) (pri/sec)` prompt, type `pri`.
31. Enter `y` to configure a private network for HA.



```
HyTrust CloudControl - 5.6.0.56288

The management web user interface is available at:

       https://172.21.161.150/asc

Network Configuration - Connection 1 (eth0)

        Mode: Static
  IP Address: 172.21.161.151
     Netmask: 255.255.255.0
     Gateway: 172.21.161.1

[localhost:standalone ~]$ hasetup

CloudControl Setup - HyTrust CloudControl - 5.6.0.56288

The appliance is configured with the following settings:

               Node IP: 172.21.161.151
               Netmask: 255.255.255.0
               Gateway: 172.21.161.1
            DNS Server: 10.61.186.231

 Do you want to reconfigure? (y/n): n
 Do you want to set up proxy configuration? n

 Deploy as primary (production) or secondary (standby) (pri/sec): pri
 Do you want to configure a private network for High Availability? (y/n) _
```

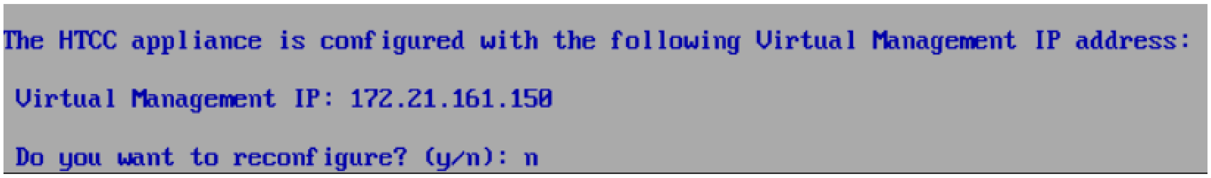
32. At the `Please specify network settings for High Availability services on Connection 3 (eth2)` prompt, enter the primary HTCC connection 3 (eth2) details.

    Note: The `<<var_htcc_pri_ha_ip>>` and `<<var_htcc_pri_ha_netmask>>` network parameters defined for the HTCC-HA-VLAN must be used.



```
Please specify network settings for High Availability services
on Connection 3 (eth2)

 IP address [172.20.20.17]: 172.21.162.151
 Netmask [255.255.255.248]: 255.255.255.0

Please confirm the following settings:

         Private HA IP: 172.21.162.151
               Netmask: 255.255.255.0

 Is this correct (y/n):  y
```

33. Enter `y` when prompted to save the settings.
34. Enter `n` when asked to configure a virtual management IP address.



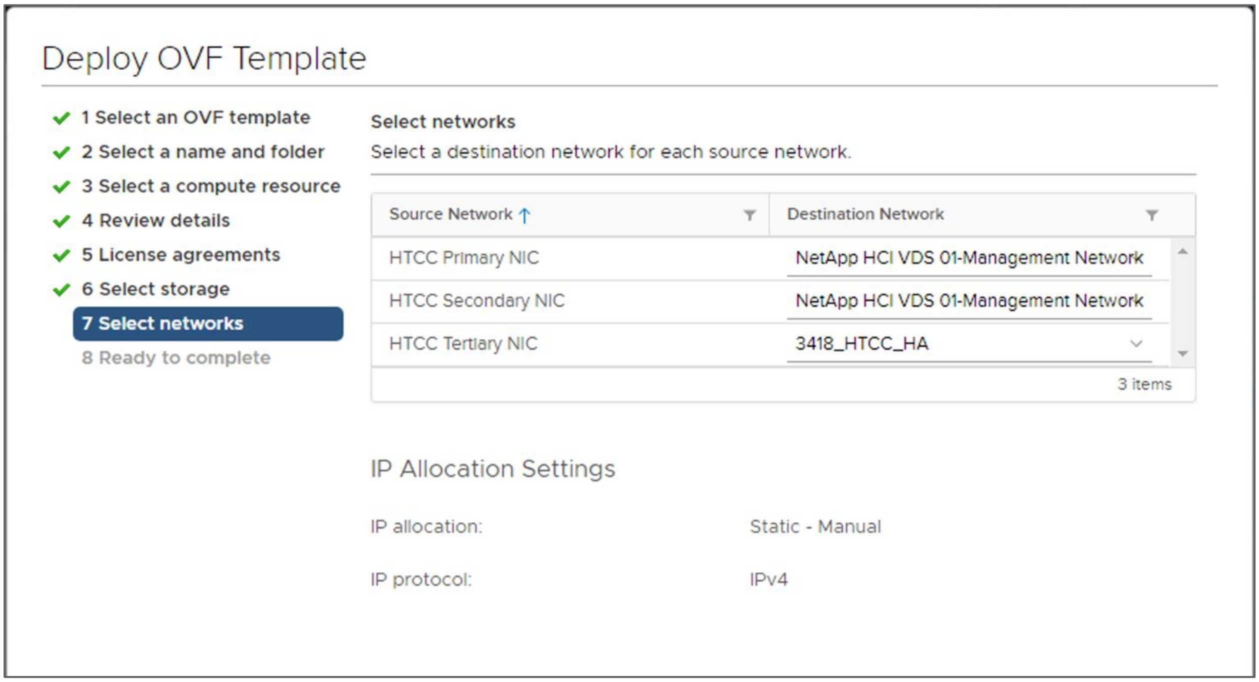
```
The HTCC appliance is configured with the following Virtual Management IP address:

 Virtual Management IP: 172.21.161.150

 Do you want to reconfigure? (y/n): n
```

The HA setup for primary HTCC is now complete. Next, you must install and configure a second HTCC instance and join the two HTCC instances to create an HTCC-HA cluster.

Install Secondary HTCC Appliance

1. From the Home menu in the vSphere Web Client, select VMs and Templates under the Inventories section.
2. Right-click the data center NetApp-HCI-Datacenter-01 or the VM folder, and select Deploy OVF Template.
3. Click Allow.
4. Browse to the OVF file of the HTCC appliance and click Open.
5. Click Next.
6. Review the OVF template details and click Next.
7. Accept the license agreement and click Next.
8. Enter a name for the HTCC secondary appliance and select a folder or data center where it should reside.
9. Click Next.
10. Select the NetApp-HCI-Cluster-MGMT cluster and click Next.
11. Select NetApp-HCI-Datastore-02 as the storage and click Next.
12. Assign the appliance NICs as follows:
    - HTCC primary NIC (eth0) → NetApp HCI VDS-01 management network

- HTCC secondary NIC (eth1) → NetApp HCI VDS-01 management network (This NIC is unused)
- HTCC tertiary NIC (eth2) → 3418_HTCC_HA



Deploy OVF Template

Select networks

Select a destination network for each source network.

Source Network ↑	Destination Network
HTCC Primary NIC	NetApp HCI VDS 01-Management Network
HTCC Secondary NIC	NetApp HCI VDS 01-Management Network
HTCC Tertiary NIC	3418_HTCC_HA

3 items

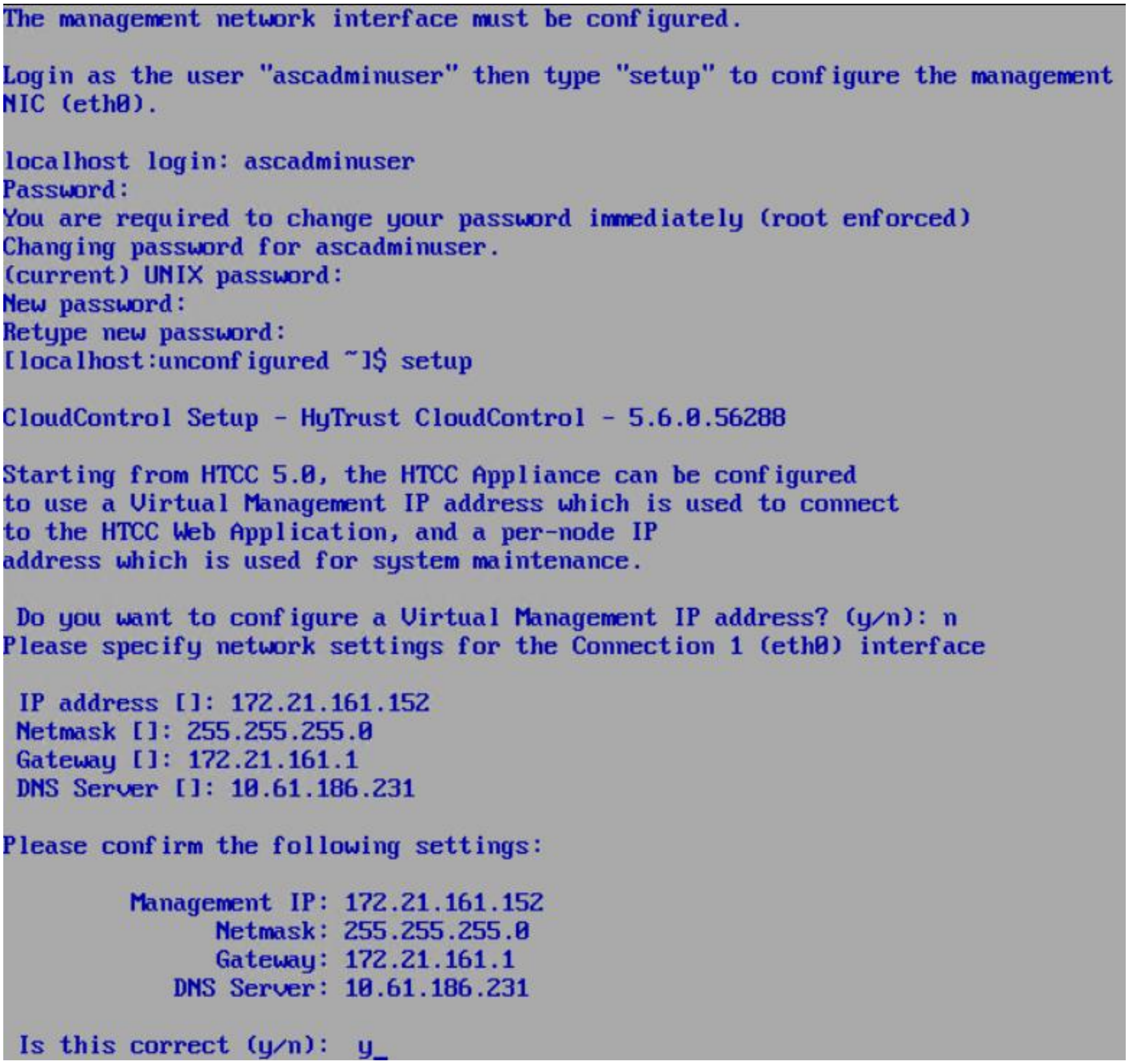
IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

13. Click Next.
14. Review the settings and click Finish.
15. Wait for the OVF template to be deployed.
16. Select the HTCC secondary VM from the Inventory pane. From the Summary tab, click Launch Remote Console.
17. Click Launch Application if prompted.
18. Click the green button (second from left) to power on the VM.

Configure Secondary HTCC Management Network Interface



```
The management network interface must be configured.

Login as the user "ascadminuser" then type "setup" to configure the management
NIC (eth0).

localhost login: ascadminuser
Password:
You are required to change your password immediately (root enforced)
Changing password for ascadminuser.
(current) UNIX password:
New password:
Retype new password:
[localhost:unconfigured ~]$ setup

CloudControl Setup - HyTrust CloudControl - 5.6.0.56288

Starting from HTCC 5.0, the HTCC Appliance can be configured
to use a Virtual Management IP address which is used to connect
to the HTCC Web Application, and a per-node IP
address which is used for system maintenance.

 Do you want to configure a Virtual Management IP address? (y/n): n
Please specify network settings for the Connection 1 (eth0) interface

 IP address []: 172.21.161.152
 Netmask []: 255.255.255.0
 Gateway []: 172.21.161.1
 DNS Server []: 10.61.186.231

Please confirm the following settings:

         Management IP: 172.21.161.152
               Netmask: 255.255.255.0
               Gateway: 172.21.161.1
            DNS Server: 10.61.186.231

 Is this correct (y/n):  y_
```

1. In the console window of the HTCC VM, log in as `ascadminuser` with the password `Pa$$w0rd123!`.
2. Enter the current password, `Pa$$w0rd123!`.

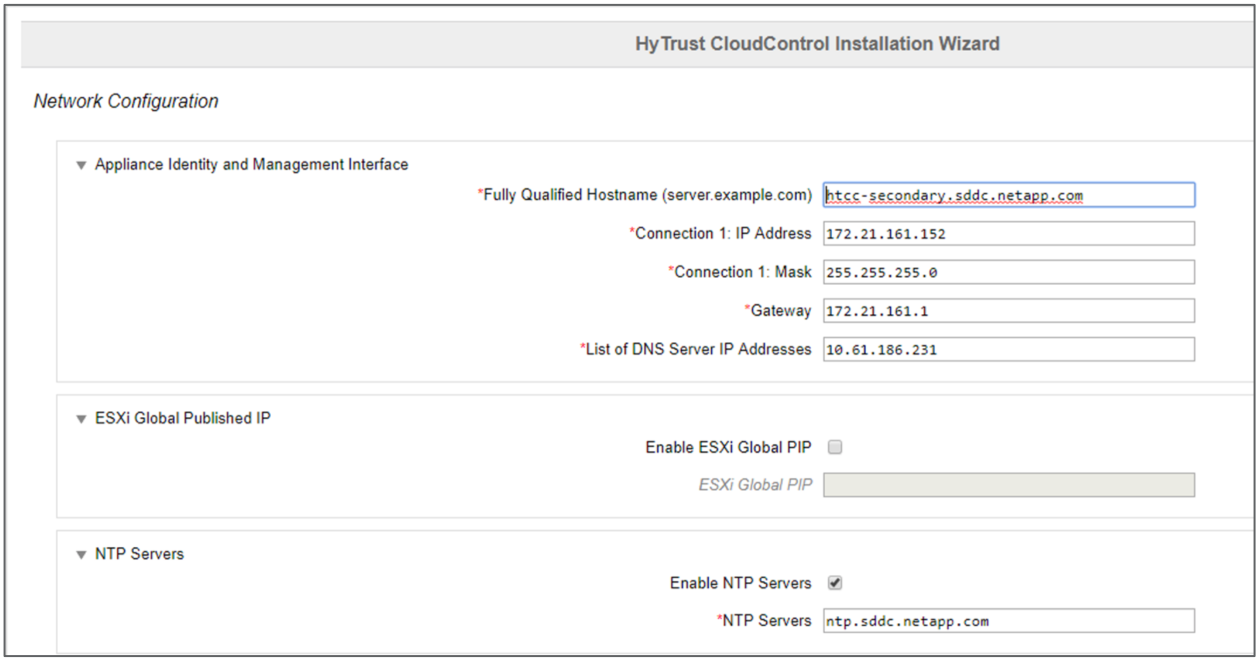
   Note: The `ascadminuser` password must be changed after the first login.
3. Assign a new password for the `ascadminuser` and reenter the password to confirm.
4. Start the setup procedure by running the setup command.
5. Enter `n` when asked to configure a virtual management IP address.
6. Enter the IPv4 address for the management network connection (eth0) interface, `<<var_htcc_sec_ip>>`.
7. Enter the netmask, `<<var_htcc_sec_netmask>>`.
8. Enter the gateway, `<<var_htcc_sec_gw>>`.
9. Enter the DNS server IP addresses.

10. Review the network settings and confirm.
11. When prompted with “Do you want to set up proxy configuration?” enter `n`.
12. Log out after the network settings have been updated.
13. Open a web browser and navigate to `https://<<var_htcc_sec_ip>>/asc`.

    Note: FQDN is not supported until the installation wizard completes.

    Note: Use the IPv4 address.

14. Allow the security exceptions if prompted.
15. Log in using the default user name `superadminuser` and the password `Pa$$w0rd123!`.
16. Accept the license agreement and click Next.
17. Upload the license file with the .xml extension and click Next.
18. In the Network Configuration page, assign a host name for the HTCC secondary appliance and review the network settings.



HyTrust CloudControl Installation Wizard

Network Configuration

▾ Appliance Identity and Management Interface

*Fully Qualified Hostname (server.example.com): htcc-secondary.sddc.netapp.com

*Connection 1: IP Address: 172.21.161.152

*Connection 1: Mask: 255.255.255.0

*Gateway: 172.21.161.1

*List of DNS Server IP Addresses: 10.61.186.231

▾ ESXi Global Published IP

Enable ESXi Global PIP: □

ESXi Global PIP:

▾ NTP Servers

Enable NTP Servers: ☑

*NTP Servers: ntp.sddc.netapp.com

19. Update the list of (comma-separated) DNS servers if necessary.

    Note: Provide only IP addresses for DNS servers.

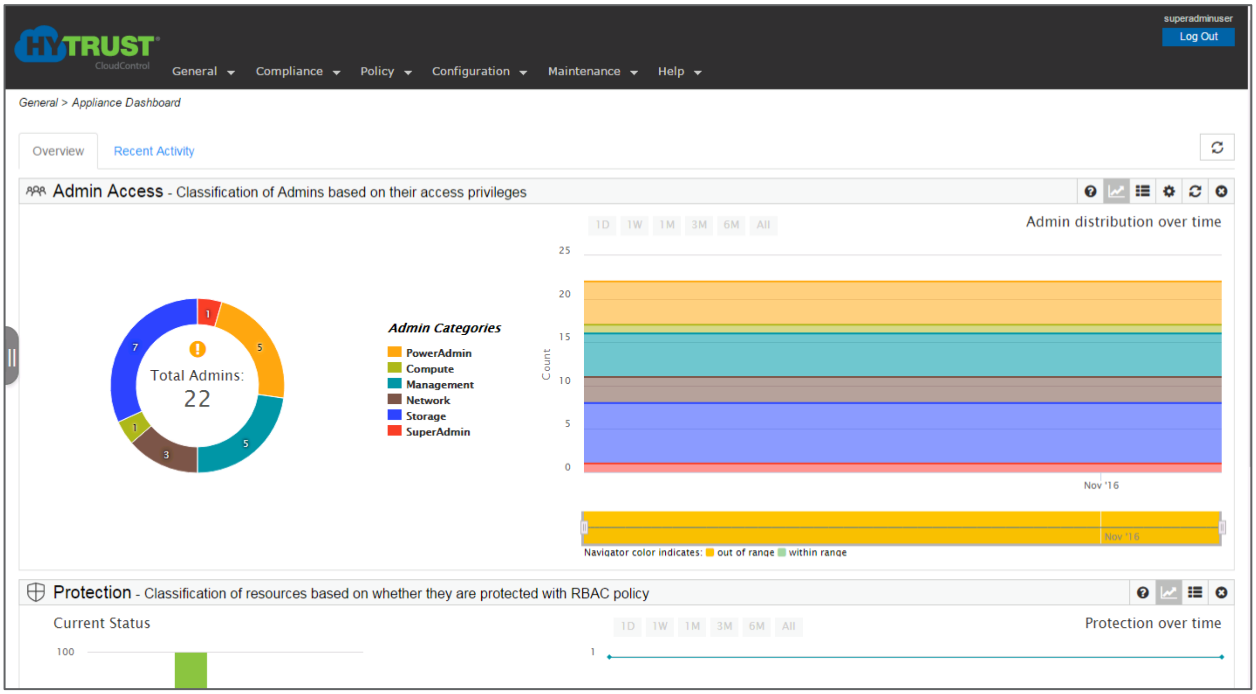
20. Click the Enable NTP Servers checkbox and enter the NTP server IP addresses (comma separated).

    Note: Provide only IP addresses for NTP servers.

21. Click Next.
22. Click Finish to complete the installation wizard.

    Note: The Finish button is not enabled until the installation wizard completes.

23. The HTCC Management Console Appliance dashboard appears upon successful installation.



24. From the vSphere Web Client, connect to the console of the HTCC secondary VM.

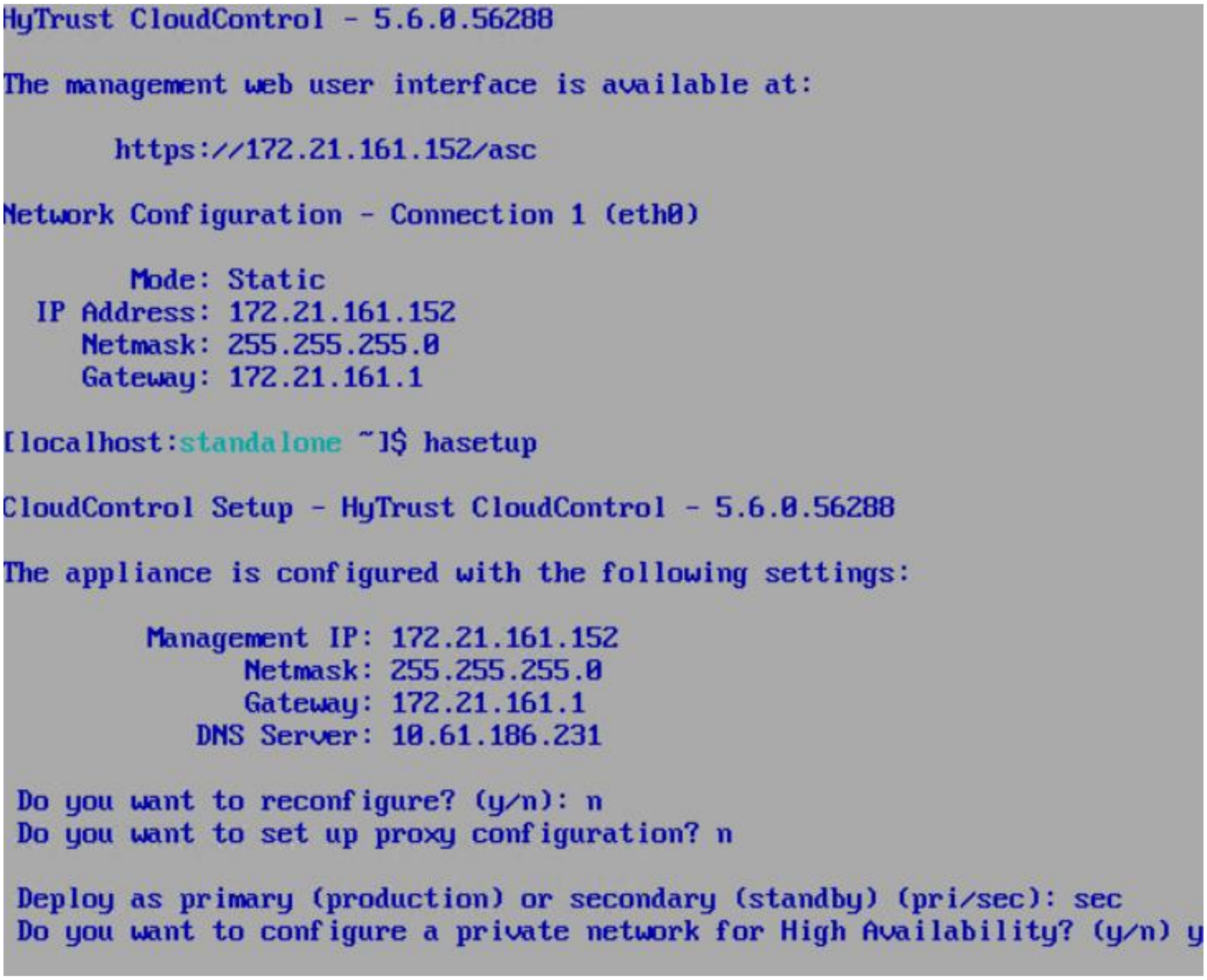
25. Log in as `ascadminuser`.

26. Start the HA setup procedure by running the `hasetup` command.

27. At the `Please specify network settings for the Connection 1 (eth0) interface` prompt, confirm the settings assigned to the secondary HTCC. Enter `n` to skip reconfiguring the network settings and Proxy Configuration settings.

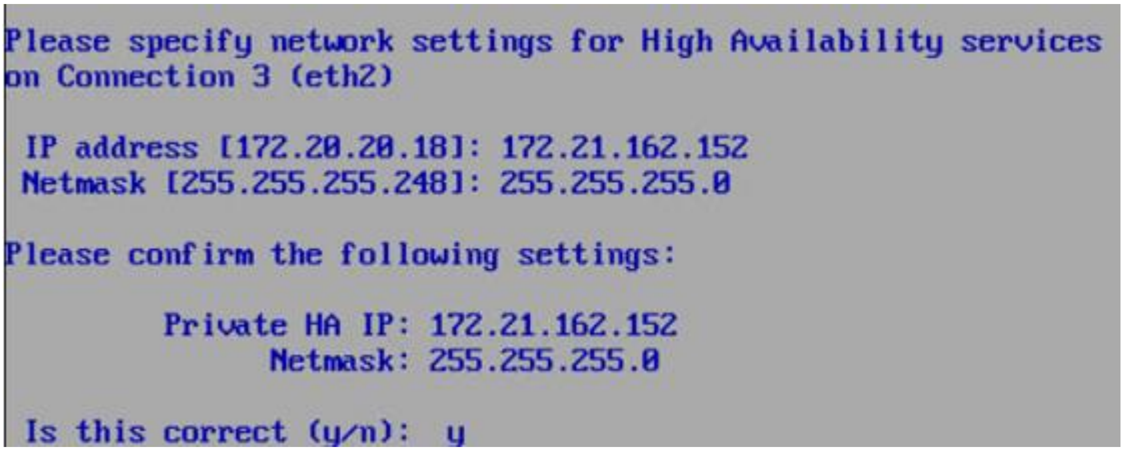
28. At the `Deploy as primary (production) or secondary (standby) (pri/sec)` prompt, type sec.

29. Enter `y` to configure a private network for HA.



```
HyTrust CloudControl - 5.6.0.56288

The management web user interface is available at:

       https://172.21.161.152/asc

Network Configuration - Connection 1 (eth0)

        Mode: Static
  IP Address: 172.21.161.152
     Netmask: 255.255.255.0
     Gateway: 172.21.161.1

[localhost:standalone ~]$ hasetup

CloudControl Setup - HyTrust CloudControl - 5.6.0.56288

The appliance is configured with the following settings:

         Management IP: 172.21.161.152
               Netmask: 255.255.255.0
               Gateway: 172.21.161.1
            DNS Server: 10.61.186.231

 Do you want to reconfigure? (y/n): n
 Do you want to set up proxy configuration? n

 Deploy as primary (production) or secondary (standby) (pri/sec): sec
 Do you want to configure a private network for High Availability? (y/n) y
```

30. At the `Please specify network settings for High Availability services on Connection 3 (eth2)` prompt, enter the secondary HTCC Connection 3 (eth2) details.

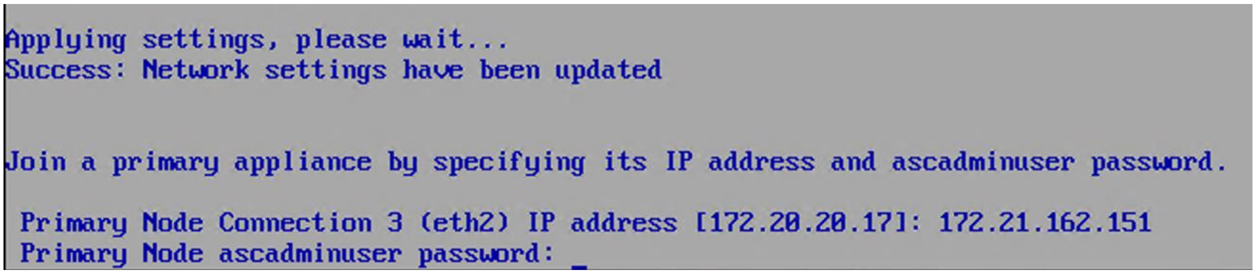


```
Please specify network settings for High Availability services
on Connection 3 (eth2)

 IP address [172.20.20.18]: 172.21.162.152
 Netmask [255.255.255.248]: 255.255.255.0

Please confirm the following settings:

         Private HA IP: 172.21.162.152
               Netmask: 255.255.255.0

 Is this correct (y/n):  y
```

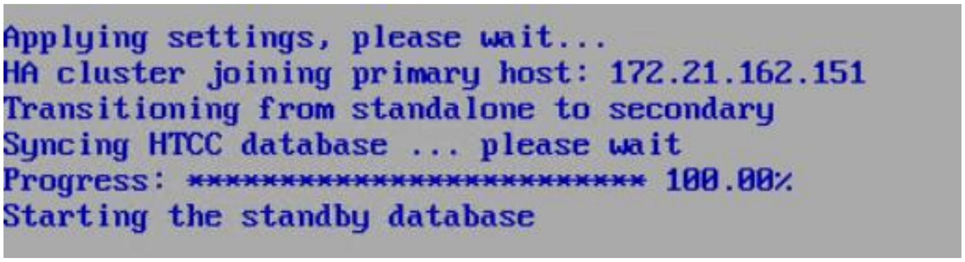
31. Join the primary instance by specifying its IP address and ascadminuser password.

    Note: You should use the `<var_htcc_pri_ha_ip>>` network parameter defined for the HTCC-HA-VLAN.

Note: This process might take several minutes as the secondary HTCC establishes communication with the primary HTCC.



```
Applying settings, please wait...
Success: Network settings have been updated


Join a primary appliance by specifying its IP address and ascadminuser password.

 Primary Node Connection 3 (eth2) IP address [172.20.20.17]: 172.21.162.151
 Primary Node ascadminuser password: _
```



```
Applying settings, please wait...
HA cluster joining primary host: 172.21.162.151
Transitioning from standalone to secondary
Syncing HTCC database ... please wait
Progress: ************************* 100.00%
Starting the standby database
```

After this process completes, the secondary HTCC updates and displays the HyTrust high-availability (HA) system status as `Enabled` and the mode as `Secondary`. The HA status is also updated on the primary HTCC and shows the mode as `Primary` after the CLI command window is refreshed.

Configure HyTrust CloudControl to Directory Service Mode

Configure HTCC to perform authentication against a Microsoft Active Directory service for a streamlined access policy to the HTCC appliance.

Create a Service Account

1. Log in to the Windows machine running the Active Directory server using credentials that have sufficient privileges to create accounts.
2. In Active Directory, add a new user to serve as the HTCC service account.
   - Full name: `HtaServiceAccount`
   - User login name: `htaserviceaccount`

Create Security Groups

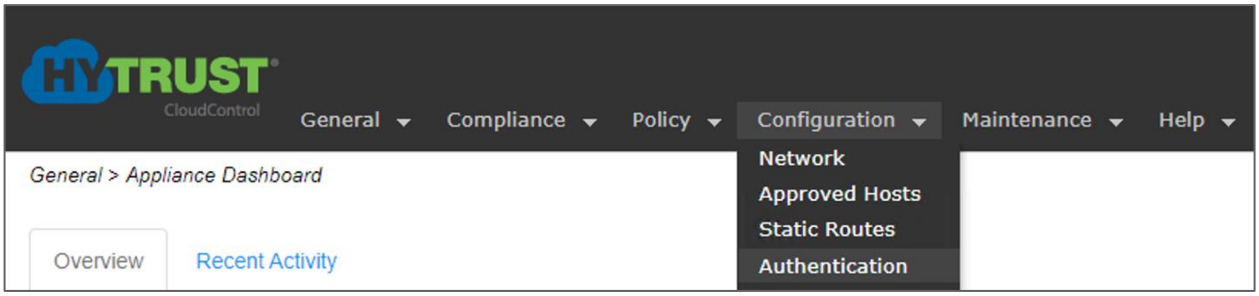
The default HTCC rules are created by mapping existing user groups in Active Directory to default roles in HTCC when HTCC is converted to Directory Service mode.

Refer to the HyTrust CloudControl Administration Guide to create the necessary Security Groups.

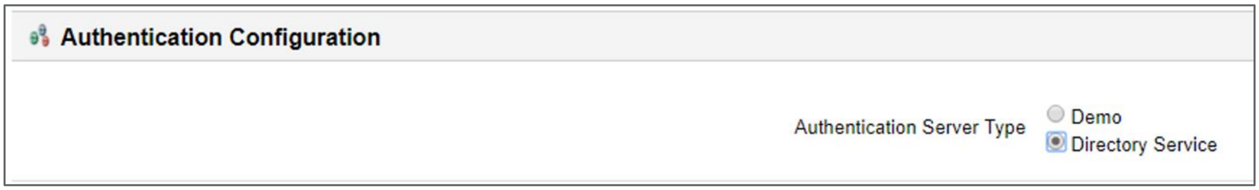
Integrate HTCC with Active Directory

Note: Converting HTCC to Directory Service mode for authentication and authorization cannot be reversed.

1. Browse to the HTCC ,management console.
2. Click the Configuration tab and click Authentication from the drop-down.



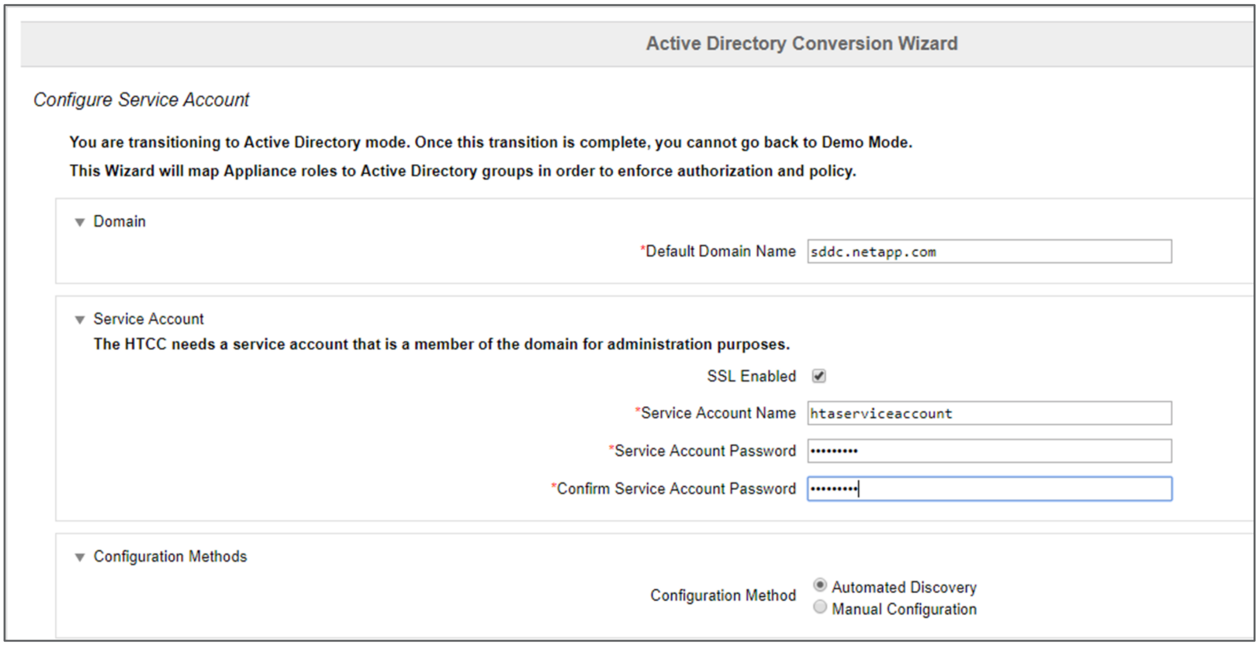
3. Select the Directory Service button and click Apply.



Authentication Configuration

Authentication Server Type ○ Demo ● Directory Service

4. Enter the domain name.
5. Enter the service account name created earlier and enter the password.
6. Select Automated Discovery under the Configuration Method and click Next.



Active Directory Conversion Wizard

Configure Service Account

You are transitioning to Active Directory mode. Once this transition is complete, you cannot go back to Demo Mode.

This Wizard will map Appliance roles to Active Directory groups in order to enforce authorization and policy.

▼ Domain

*Default Domain Name: sddc.netapp.com

▼ Service Account

The HTCC needs a service account that is a member of the domain for administration purposes.

SSL Enabled ☑

*Service Account Name: htaserviceaccount

*Service Account Password: •••••••••

*Confirm Service Account Password: •••••••••

▼ Configuration Methods

Configuration Method ● Automated Discovery ○ Manual Configuration

7. Select the View Active Directory Advanced Settings checkbox and click Next.
8. Review the preferred global catalog, domain details, user search context, and group search context. Make any necessary changes and click Next.
9. Map the HTCC roles to the Active Directory security groups created and click Next.
10. Review the settings and click Finish.
11. After the conversion is complete, log in to the HTCC management console with the Active Directory credentials.

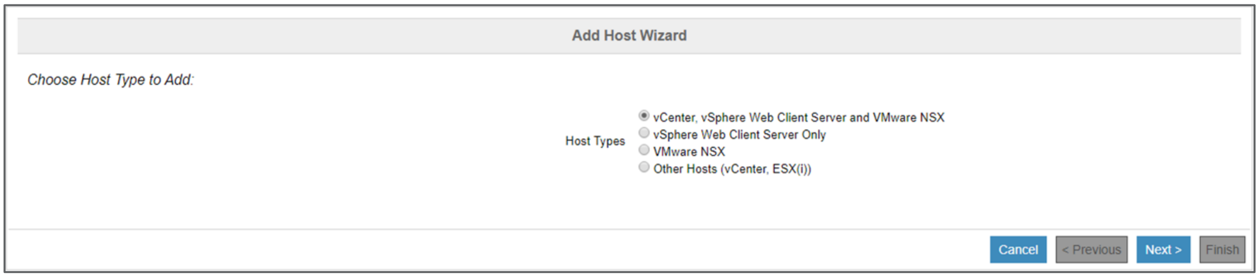
Note: Before logging in to the HTCC management console, the security groups in Active Directory must be populated with the required users.

Add HTCC Protected Hosts

Note: NetApp recommends using FQDNs in place of IP addresses wherever possible for the host IP and PIP.

vCenter, ESXi and NSX

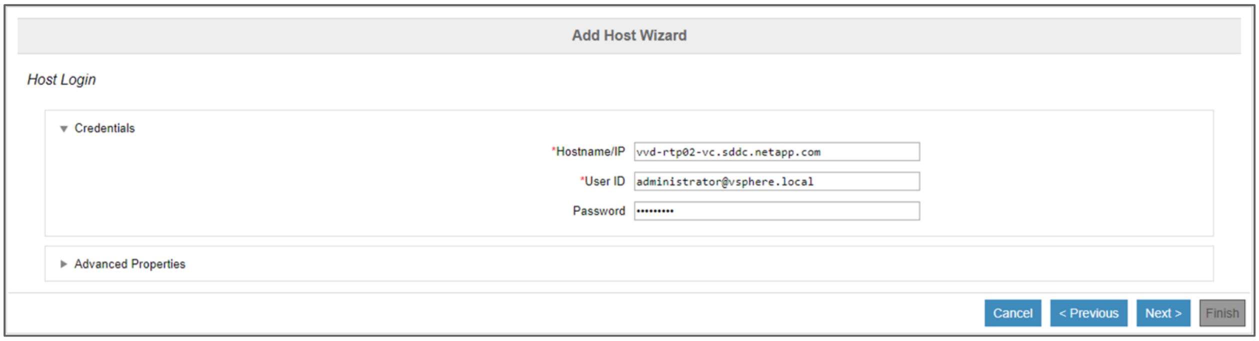
1. From the HTCC management console, click Compliance. From the drop-down, click Hosts.
2. Click Add. The Add Host wizard appears.
3. Select vCenter, vSphere Web Client Server and VMware NSX. Then click Next.



Choose Host Type to Add:

Host Types
● vCenter, vSphere Web Client Server and VMware NSX
○ vSphere Web Client Server Only
○ VMware NSX
○ Other Hosts (vCenter, ESX(i))

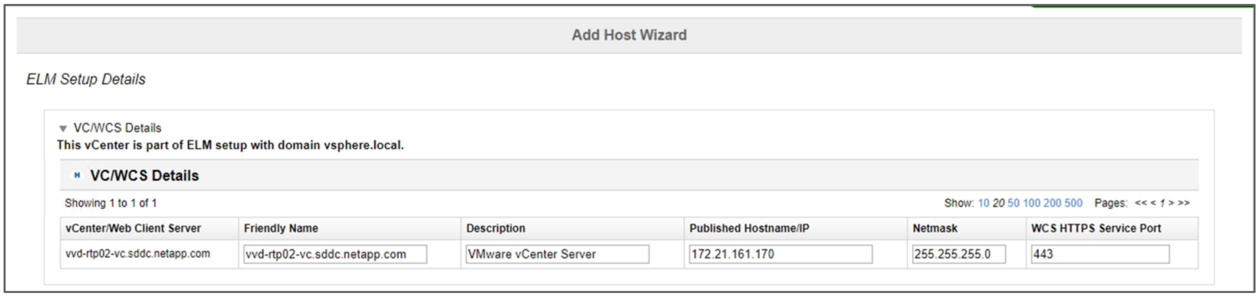
4. Enter the vCenter host name/IP followed by the user ID and password. Then click Next.



Host Login

*Hostname/IP: vvd-rtp02-vc.sddc.netapp.com
*User ID: administrator@vsphere.local
Password: •••••••••

5. Enter a description and friendly name for the vCenter host.
6. Enter the Published Hostname/IP and the Netmask and click Next.



ELM Setup Details

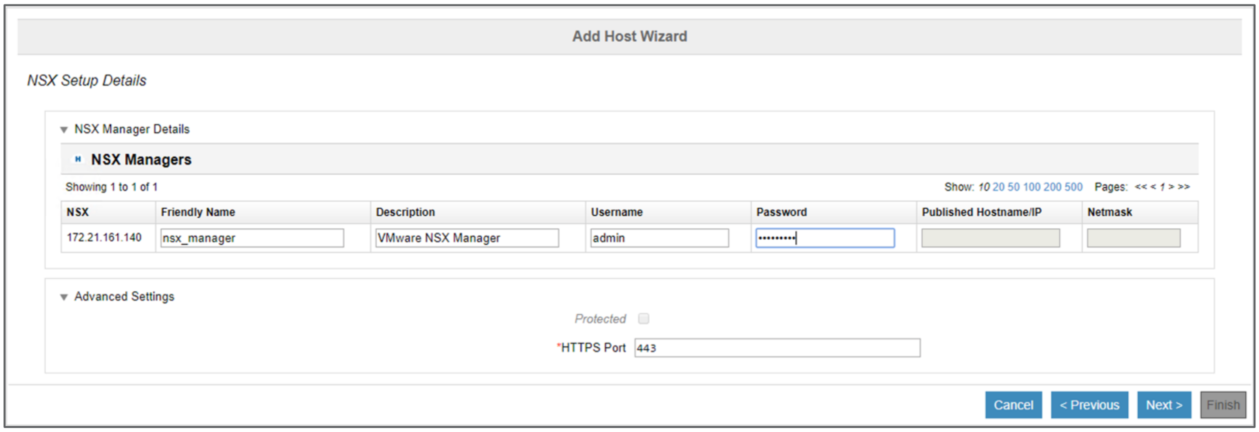
This vCenter is part of ELM setup with domain vsphere.local.

Showing 1 to 1 of 1

vCenter/Web Client Server	Friendly Name	Description	Published Hostname/IP	Netmask	WCS HTTPS Service Port
vvd-rtp02-vc.sddc.netapp.com	vvd-rtp02-vc.sddc.netapp.com	VMware vCenter Server	172.21.161.170	255.255.255.0	443

7. Provide a friendly name and description for the NSX Manager.
8. Enter the username and password for the NSX Manager and click Next.

© 2020 NetApp, Inc. All rights reserved.



Add Host Wizard

NSX Setup Details

▼ NSX Manager Details

NSX Managers

Showing 1 to 1 of 1

Show: *10* 20 50 100 200 500 Pages: << < *1* > >>

NSX	Friendly Name	Description	Username	Password	Published Hostname/IP	Netmask
172.21.161.140	nsx_manager	VMware NSX Manager	admin	•••••••••		

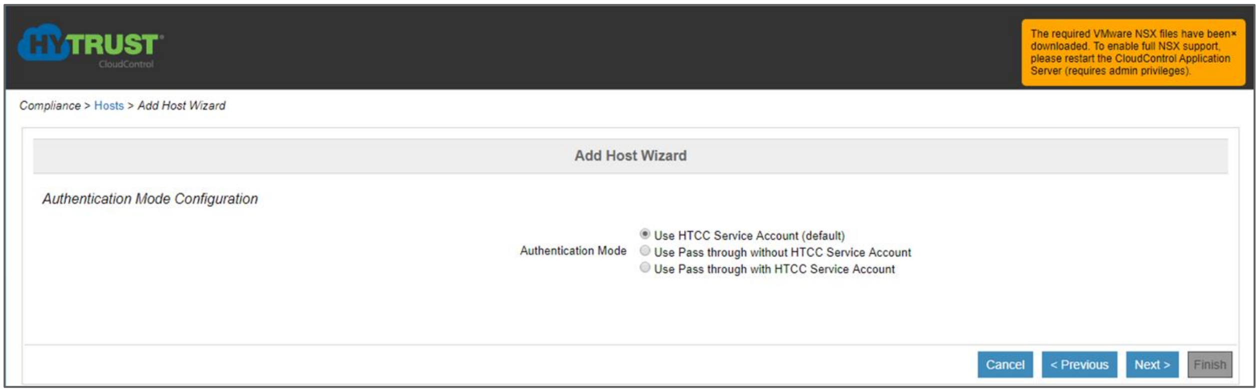
▼ Advanced Settings

Protected □

*HTTPS Port 443

Note: The Protected checkbox is disabled until CloudControl can verify the compatibility and enabled after the detected version of VMware NSX is determined to be supported.

9. Select Use HTCC Service Account (Default) as the Authentication Mode. Click Next.



The required VMware NSX files have been downloaded. To enable full NSX support, please restart the CloudControl Application Server (requires admin privileges). ×

Compliance > Hosts > *Add Host Wizard*

Add Host Wizard

Authentication Mode Configuration

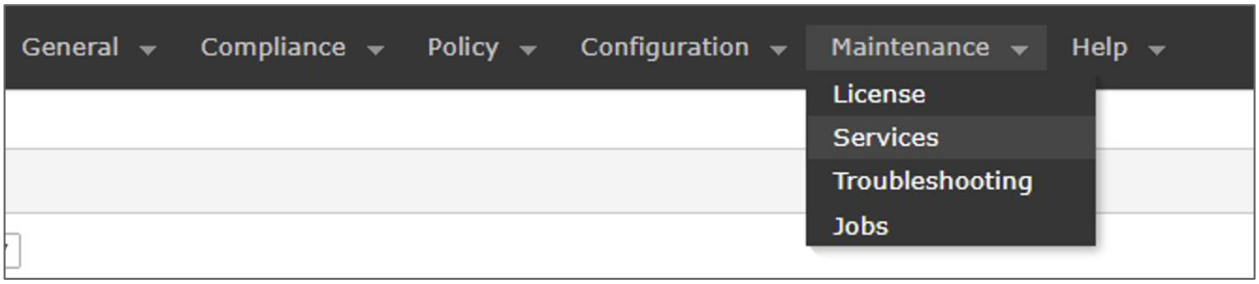
Authentication Mode
● Use HTCC Service Account (default)
○ Use Pass through without HTCC Service Account
○ Use Pass through with HTCC Service Account

10. Click Finish to add the hosts to HTCC.

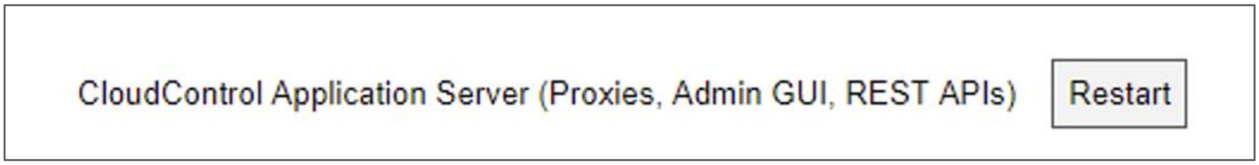
Note: This operation might take a few minutes to complete depending on the number of hosts.

Note: Additional NSX files are downloaded by CloudControl for NSX and this requires a restart of the CloudControl application server to enable full VMware NSX support.

11. Select the Maintenance tab and click Services.

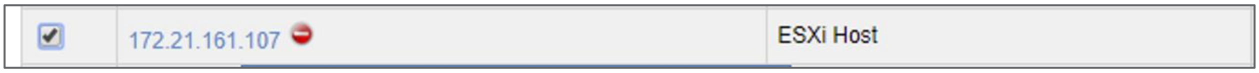


12. Click Restart and then click OK.

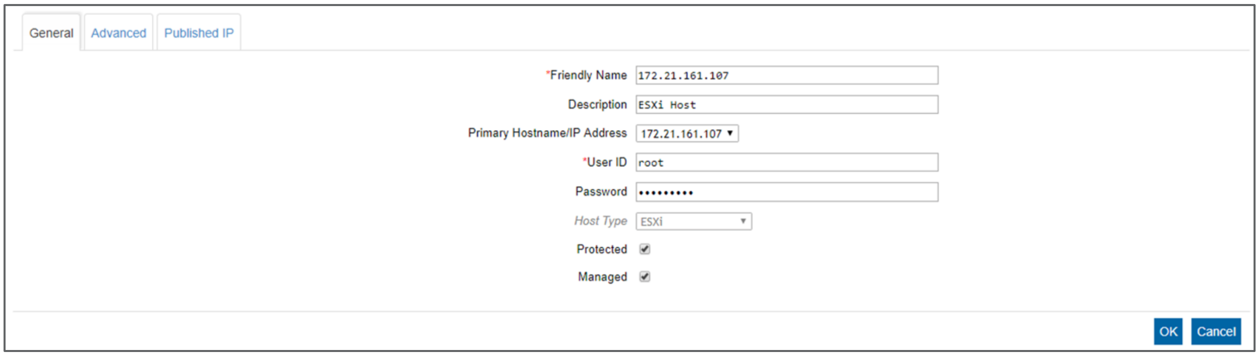

CloudControl Application Server (Proxies, Admin GUI, REST APIs)
Restart

Protect ESXi Hosts

1. Select Compliance and click Hosts.
2. Click an ESXi host with a sign as shown below.

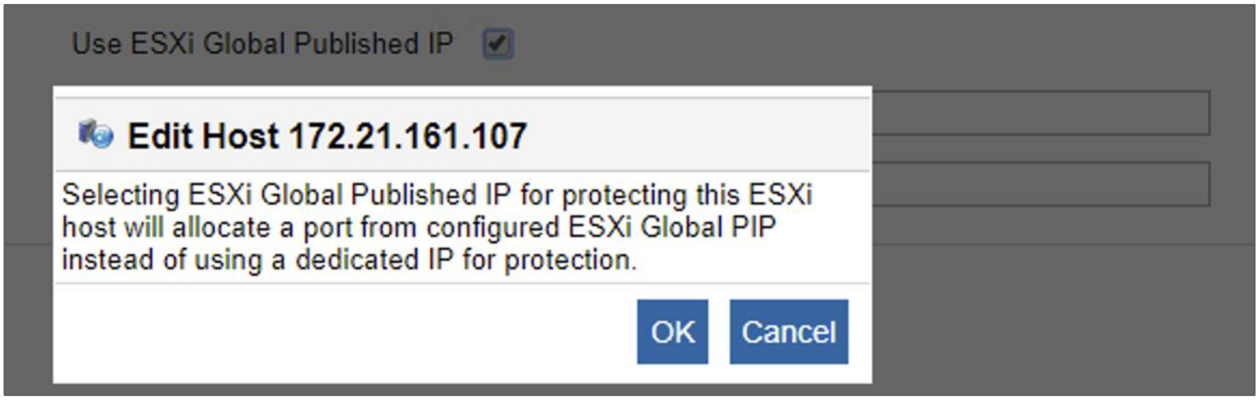


3. In the General Tab, enter a description (optional), the User ID, and the Password.



*Friendly Name	172.21.161.107
Description	ESXi Host
Primary Hostname/IP Address	172.21.161.107 ▾
*User ID	root
Password	•••••••••
Host Type	ESXi ▾
Protected	☑
Managed	☑

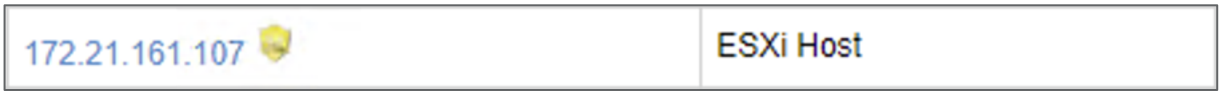
4. Click on the Published IP tab and select the Use ESXi Global Published IP checkbox. Click OK.



Edit Host 172.21.161.107

Selecting ESXi Global Published IP for protecting this ESXi host will allocate a port from configured ESXi Global PIP instead of using a dedicated IP for protection.

5. The sign for the ESXi host should look as follows:

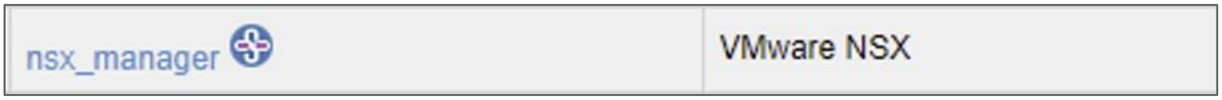


6. Repeat steps 14 to 17 for other ESXi hosts that must be protected.

Protect NSX Manager

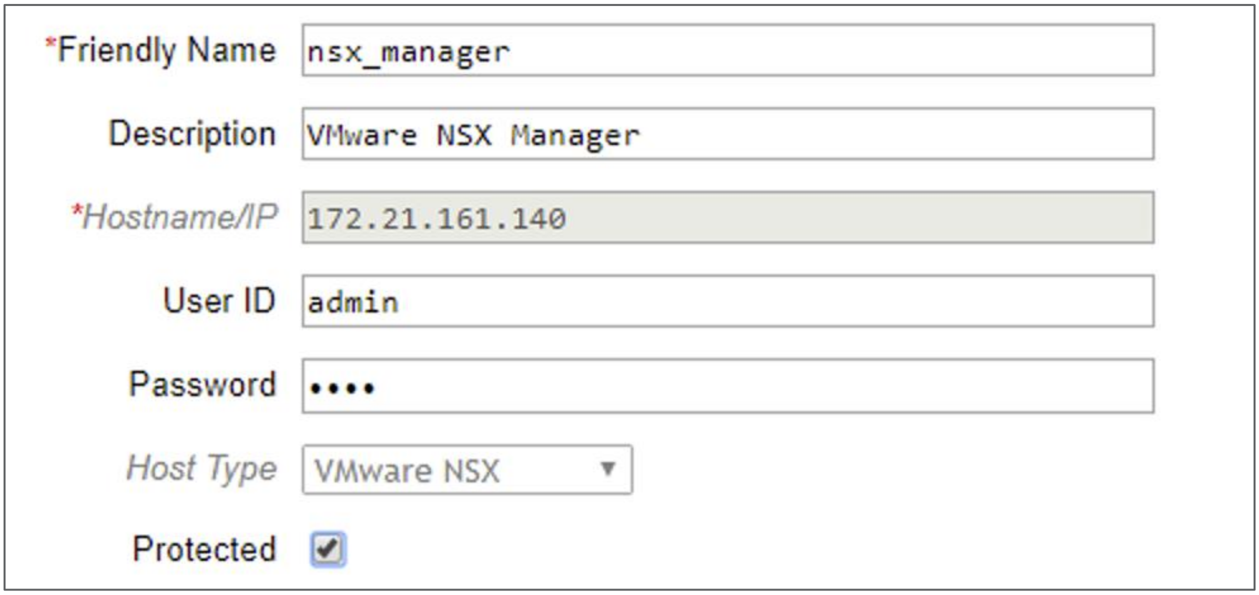
1. Select Compliance and click Hosts.

2. Click NSX Manager.



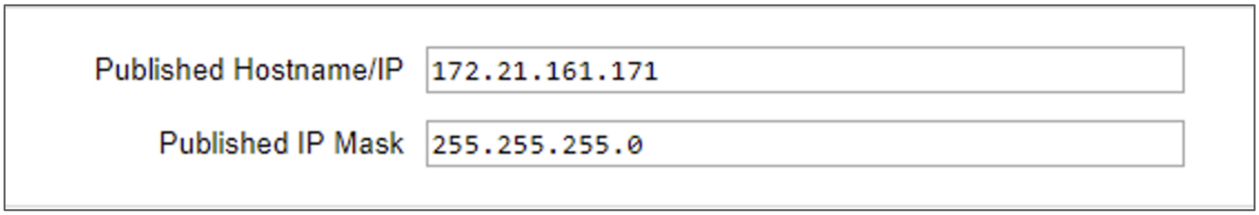
nsx_manager	VMware NSX

3. In the General tab, select the checkbox to protect the NSX Manager.



*Friendly Name	nsx_manager
Description	VMware NSX Manager
*Hostname/IP	172.21.161.140
User ID	admin
Password	••••
Host Type	VMware NSX ▼
Protected	☑

4. Click the Published IP tab and provide the Published Hostname/IP and Published IP Mask. Click OK.



Published Hostname/IP	172.21.161.171
Published IP Mask	255.255.255.0

Configure SAML Data Provider

1. Log in to the console of the HTCC primary appliance as the `ascadminuser`.
2. Enter the following command in the console:

```
asc certs -b
```

3. Enter `y` to import certificates for all the hosts.
4. After all certificates are imported, log in to the HTCC web interface with SuperAdmin privileges.
5. Click the Compliance tab and select Hosts.
6. Select the checkbox beside the vSphere Web Client Server and click Download Web Client Metadata.
7. Log in to the vSphere Web Client.

   Note: Do not login to the HTML 5-based client.

8. From the Home menu, click Administration.
9. Under Single Sign-On, select Configuration.

10. Select SAML Service Providers in the right pane and click Import.
11. Click Import from File and navigate to the downloaded SAML metadata.
12. Click Import.

6.3 HyTrust DataControl Deployment

HTDC provides encryption and key management for VMs. Its major components are HyTrust KeyControl and HTDC Policy Agent. The HTDC installation procedure includes installing the HyTrust KeyControl nodes in a cluster configuration and the policy agents in the VMs. A clustered instance of HTDC was installed in the tenant-workload cluster to protect the VMs residing within the tenant cluster.

To install HTDC, complete the following steps:

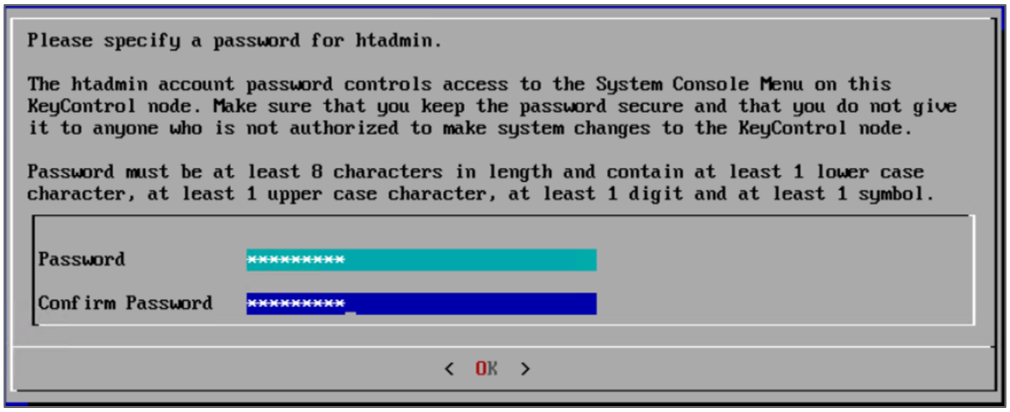
Install First HyTrust KeyControl Node

1. Log in to the vSphere Web Client.
2. From the Home menu, click Hosts and Clusters.
3. Right-click the tenant-workload cluster and click Deploy OVF Template.
4. Click Allow to enable the Client Integration Plug-in, if prompted.
5. Browse to the HyTrust DataControl.ova file and click Open.
6. Click Next.
7. Review the details and click Next.
8. Enter a name for the first HyTrust KeyControl VM and select a folder to house it. Click Next.
9. In the Configuration section, select the default recommended option and click Next.
10. Select the HCI-Tenant-Datastore-01 provisioned for that cluster and click Next.
11. In the Network selection, select the VM Port-Group created for the respective tenant cluster for secure connections within the cluster. Click Next.

    Note: A microsegment was created using VMware NSX to make sure that VMs running in the tenant-workload cluster alone can communicate with the HTDC instances.

    Note: External connections to HTDC were regulated by using a Jump machine in the Tenant cluster.

12. In the Customization template, enter the following information:
    a. The first KeyControl system IP address
    b. The first KeyControl system host name
    c. The domain name
    d. The netmask
    e. The gateway
    f. The primary DNS server
13. Click Next.
14. Review the settings and click Finish.
15. After HyTrust KeyControl is deployed, launch the remote console for the VM.
16. Click Launch Application if prompted.
17. Click the green button (second from left) to power on the VM.
18. Enter a new password for HyTrust KeyControl and confirm the password.



Please specify a password for htadmin.

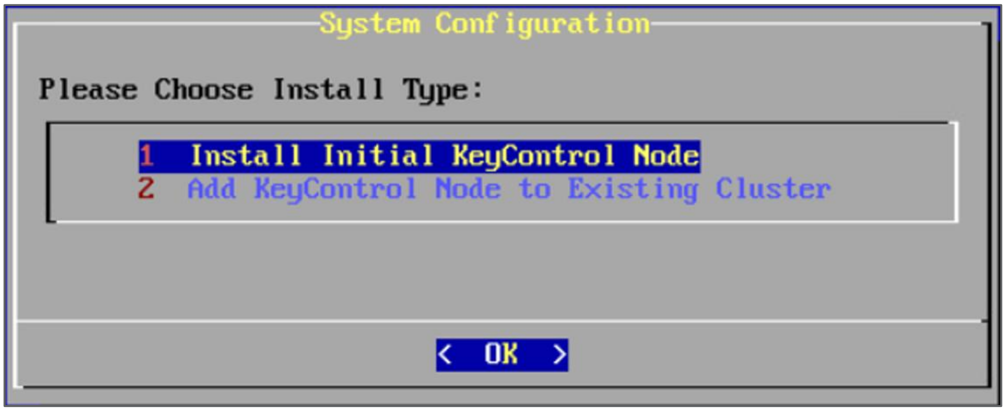
The htadmin account password controls access to the System Console Menu on this KeyControl node. Make sure that you keep the password secure and that you do not give it to anyone who is not authorized to make system changes to the KeyControl node.

Password must be at least 8 characters in length and contain at least 1 lower case character, at least 1 upper case character, at least 1 digit and at least 1 symbol.

Password **********

Confirm Password **********

19. Select Install Initial KeyControl Node and select OK.



System Configuration

Please Choose Install Type:

1 Install Initial KeyControl Node
2 Add KeyControl Node to Existing Cluster

20. Reboot the KeyControl system.
21. Open a web browser and navigate to the IP address of the first HyTrust KeyControl system.
22. Log in with the user name `secroot` and password `secroot`.
23. Read and accept the license agreement.
24. Enter and confirm a new password for the WebGUI. Click Update Password.
25. Configure the e-mail and mail server settings according to your organization’s standards. Click Update Mail settings.

Install Second HyTrust KeyControl Node

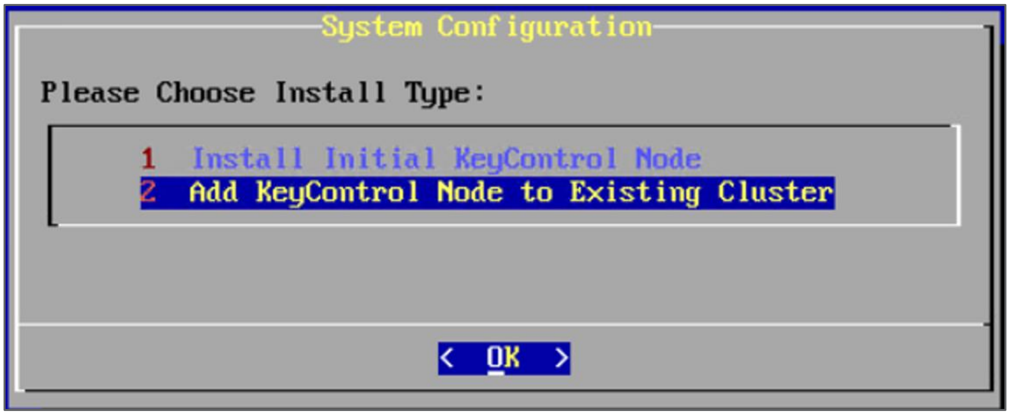
1. Log in to the vSphere Web Client.
2. From the Home menu, click Hosts and Clusters.
3. Right-click the tenant-workload cluster and click Deploy OVF Template.
4. Click Allow to enable the Client Integration Plug-in, if prompted.
5. Browse to the HyTrust DataControl.ova file and click Open.
6. Click Next.
7. Review the details and click Next.
8. Enter a name for the second HyTrust KeyControl VM and select a folder to house it. Click Next.
9. In the Configuration section, select the default recommended option and click Next.
10. Select the HCI-Tenant-Datastore-01 provisioned for that cluster and click Next.

11. In the Network selection, select the VM Port-Group created for the respective tenant cluster for secure connections within the cluster. Click Next.

    Note: A microsegment was created using VMware NSX to make sure that VMs running in the tenant-workload cluster alone can communicate with the HTDC instances.

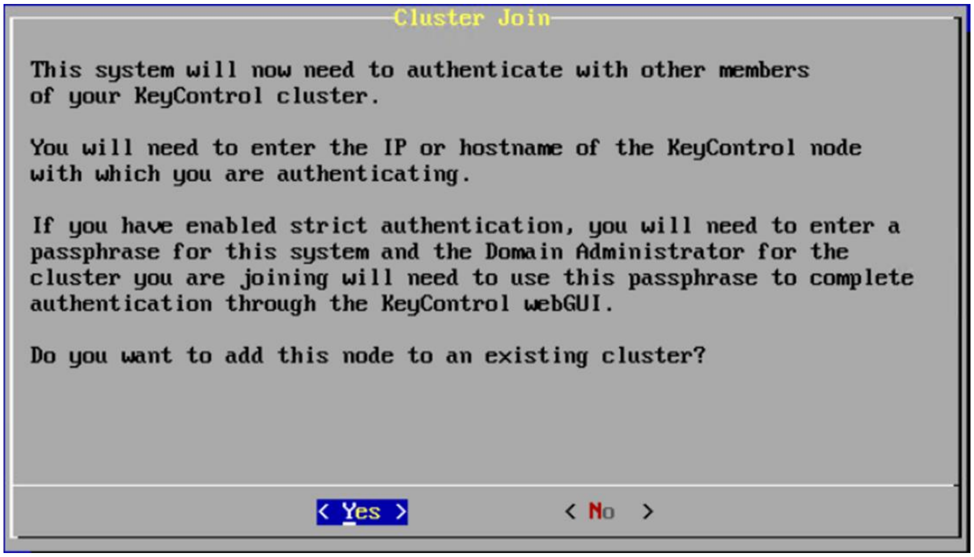
    Note: External connections to HTDC were regulated by using a Jump machine in the Tenant cluster.

12. In the Customization template, enter the following information:
    a. The second KeyControl system IP address
    b. The second KeyControl system host name
    c. The domain name
    d. The netmask
    e. the gateway
    f. The primary DNS server
13. Click Next.
14. Review the settings and click Finish.
15. After the HyTrust KeyControl is deployed, launch the remote console for the VM.
16. Click Launch Application if prompted.
17. Click the green button (second from left) to power on the VM.
18. Enter a new password for HyTrust KeyControl and confirm the password.
19. Select Add KeyControl Node to Existing Cluster and select OK.



```
System Configuration

Please Choose Install Type:

    1  Install Initial KeyControl Node
    2  Add KeyControl Node to Existing Cluster

                    < OK >
```

20. Select Yes to add the Node to an existing cluster.

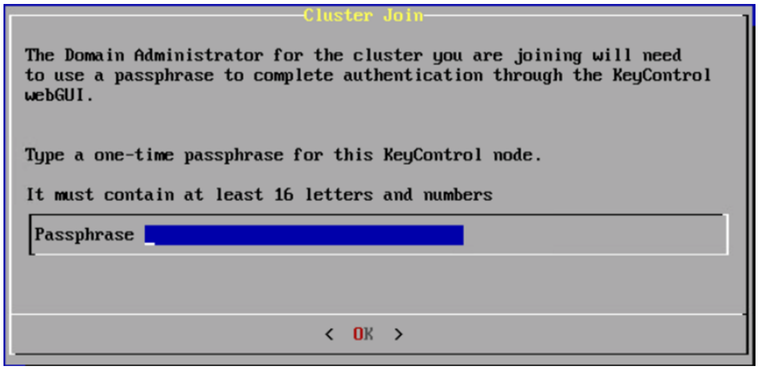


Cluster Join

```
This system will now need to authenticate with other members
of your KeyControl cluster.

You will need to enter the IP or hostname of the KeyControl node
with which you are authenticating.

If you have enabled strict authentication, you will need to enter a
passphrase for this system and the Domain Administrator for the
cluster you are joining will need to use this passphrase to complete
authentication through the KeyControl webGUI.

Do you want to add this node to an existing cluster?
```

21. Enter the IP address of the First HyTrust KeyControl system.
22. Enter a passphrase for the system.

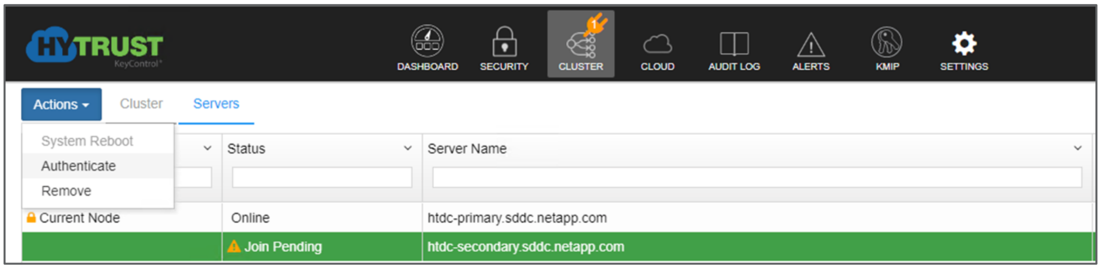
    Note: Remember this passphrase; you will need to provide it again.



Cluster Join

```
The Domain Administrator for the cluster you are joining will need
to use a passphrase to complete authentication through the KeyControl
webGUI.


Type a one-time passphrase for this KeyControl node.

It must contain at least 16 letters and numbers

Passphrase
```

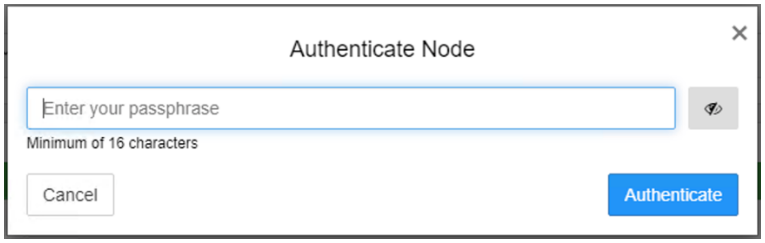
23. Log in to the WebGUI of the first KeyControl system.
24. Click Cluster in the top pane and click the Servers tab.
25. Select the second KeyControl system, click Actions, and then click Authenticate.



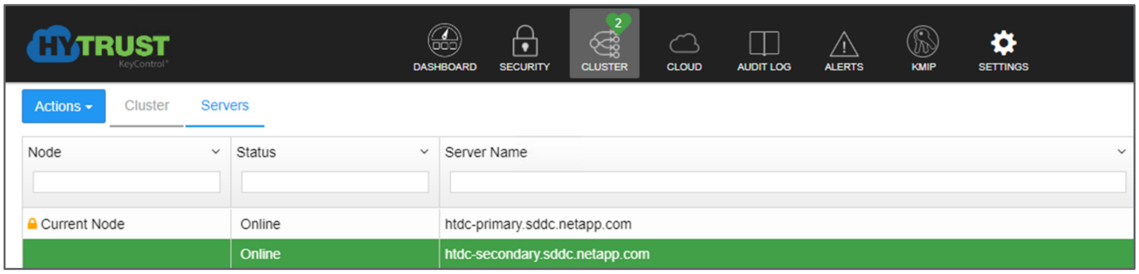
	Status	Server Name
Current Node	Online	htdc-primary.sddc.netapp.com
	⚠ Join Pending	htdc-secondary.sddc.netapp.com

26. Enter the passphrase that was entered previously and click Authenticate.

© 2020 NetApp, Inc. All rights reserved.



27. After authentication completes, the KeyControl node is listed as Authenticated but Unreachable until cluster synchronization completes and the cluster is ready for use.

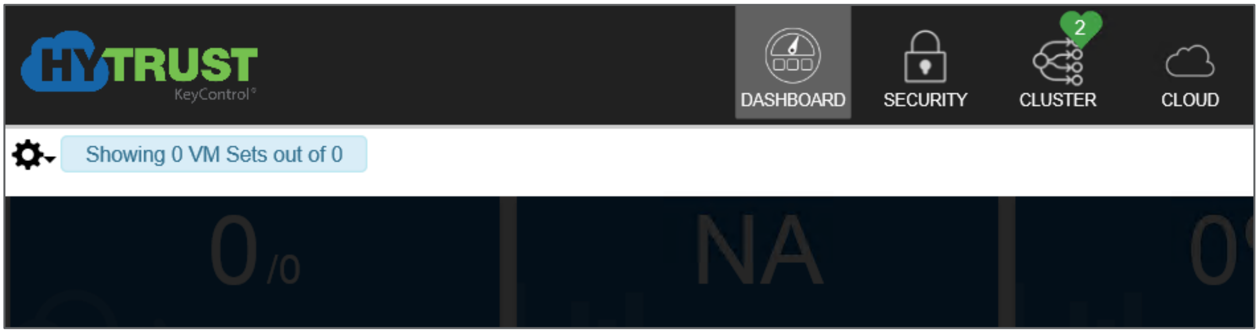


Node	Status	Server Name
Current Node	Online	htdc-primary.sddc.netapp.com
	Online	htdc-secondary.sddc.netapp.com

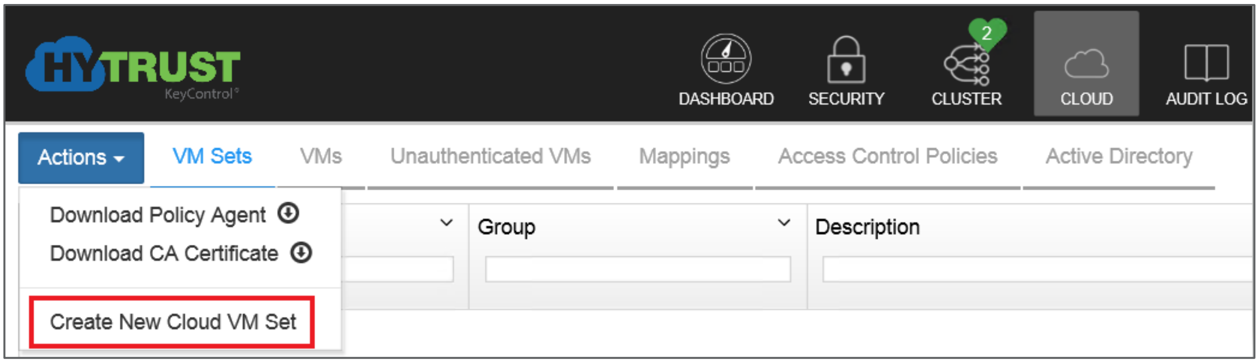
Create VM Sets

All protected VMs in the HTDC environment are managed through VM sets. A VM set is a logical grouping of related VMs. Also, authentication between the protected VMs and the KeyControl cluster requires the use of a per-VM certificate that is used during registration of the VM with the KeyControl cluster. This process ties the VM to a specific administration group and VM set.

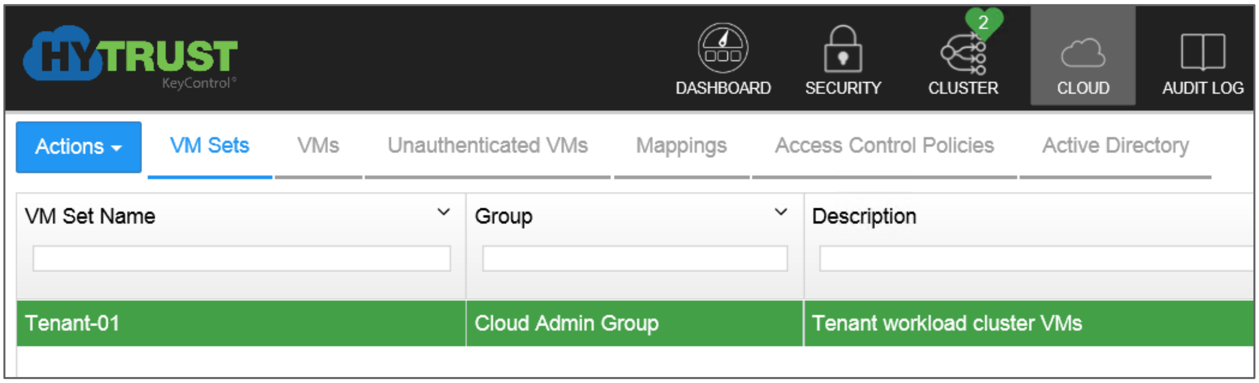
1. Log in to the KeyControl WebGUI.
2. Click the Cloud icon.



3. Click Actions and select Create New Cloud VM Set.



4. Enter a name and provide a description. Leave Cloud Admin Group selected by default.
5. Click Create and then click Close.



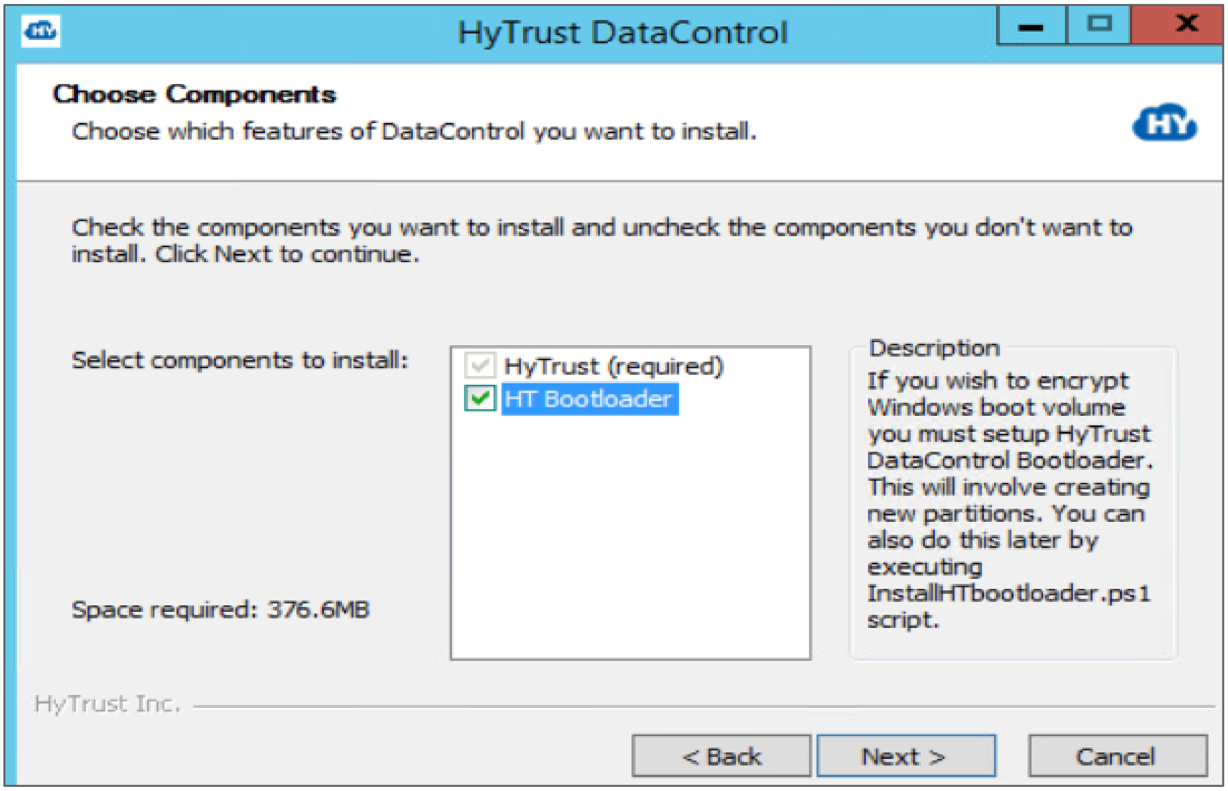
VM Set Name	Group	Description
Tenant-01	Cloud Admin Group	Tenant workload cluster VMs

Install the HyTrust DataControl Policy Agent

Complete the following procedure to install the HTDC Policy Agent. The DataControl Policy Agent is installed in the VMs in the tenant-workload cluster to be protected by HTDC.

Note: This deployment focuses only on protecting Windows VMs. Therefore, the following procedure describes the installation of HTDC Policy Agent on Windows VMs. To install the Policy Agent on Linux VMs, refer to the “HyTrust DataControl Administration Guide.”

1. Select the Windows VM on which you would like to install the DataControl Policy Agent.
2. Log in to the VM. Download and install .NET Framework version 4.
3. Before proceeding with installation, make sure that all drives in the VMs have been assigned a drive letter.
4. Log in to the WebGUI of the KeyControl system. Click Cloud. Under Actions, click Download Policy Agent.
5. Extract the downloaded agent file and navigate to the Windows client.
6. Make sure that the Disk Defragmenter service on each client computer is enabled before installing the Policy Agent software.
7. Right-click the Windows Policy Agent Client and select Run as Administrator.
8. Click Next on the Welcome screen.
9. Accept the license agreement.
10. Choose a destination to install and click Next.
11. Verify that the HT Bootloader checkbox is selected and click Next.



Choose Components

Choose which features of DataControl you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

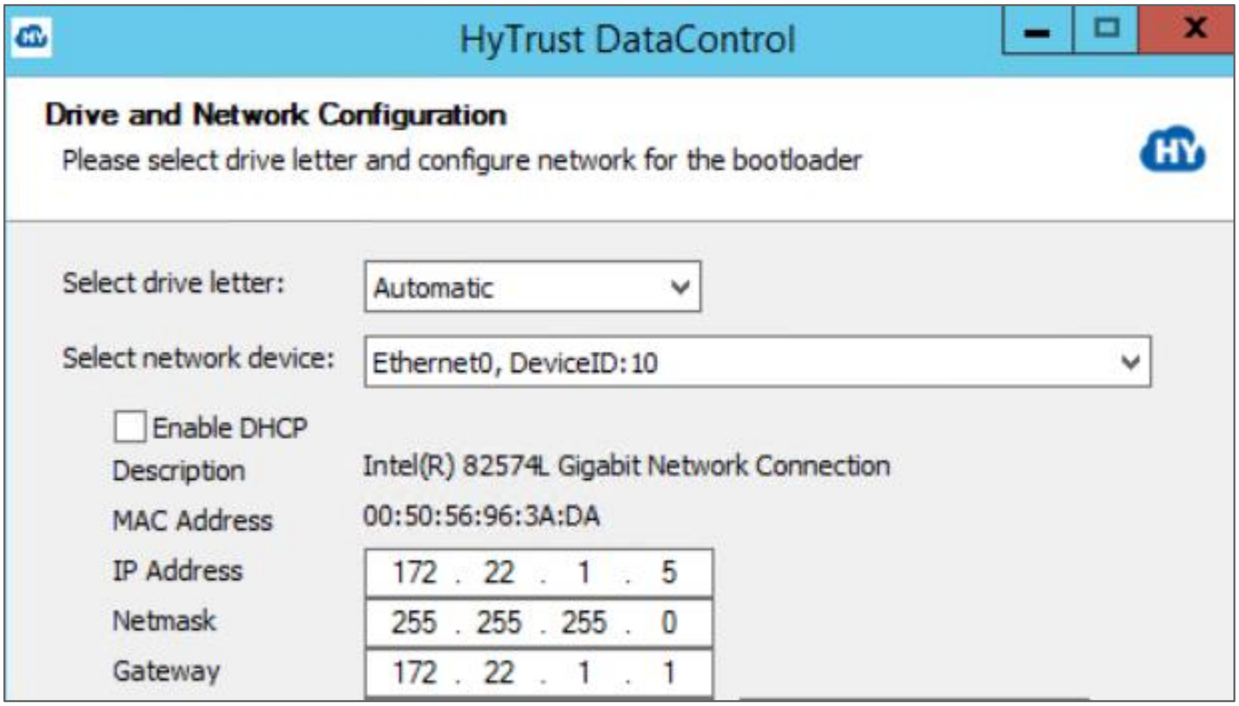
Select components to install:

☑ HyTrust (required)
☑ HT Bootloader

Description
If you wish to encrypt Windows boot volume you must setup HyTrust DataControl Bootloader. This will involve creating new partitions. You can also do this later by executing InstallHTbootloader.ps1 script.

Space required: 376.6MB

12. Leave drive letter assignment on Automatic.



Drive and Network Configuration

Please select drive letter and configure network for the bootloader

Select drive letter: Automatic

Select network device: Ethernet0, DeviceID:10

□ Enable DHCP

Description Intel(R) 82574L Gigabit Network Connection

MAC Address 00:50:56:96:3A:DA

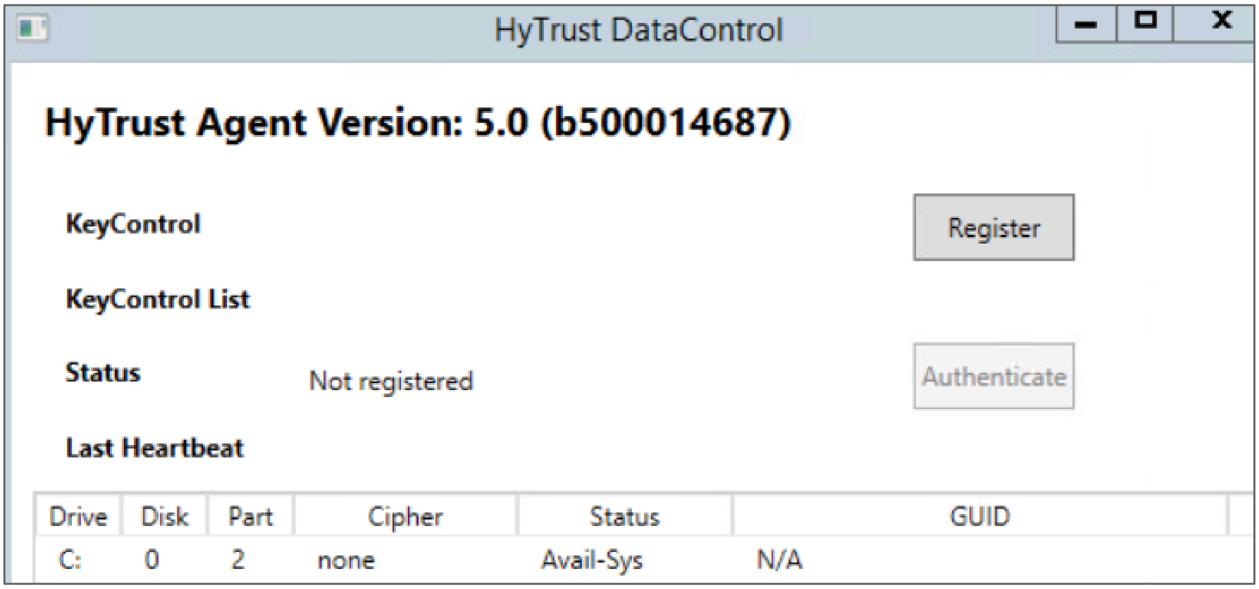
IP Address 172 . 22 . 1 . 5

Netmask 255 . 255 . 255 . 0

Gateway 172 . 22 . 1 . 1

13. Review the VM’s network details and click Install.
14. Leave the Reboot Now button selected and click Finish.

15. After reboot, log in to the VM and navigate to the installation location of the Policy Agent.
16. Click Start, select HyTrust GUI, and click Register.

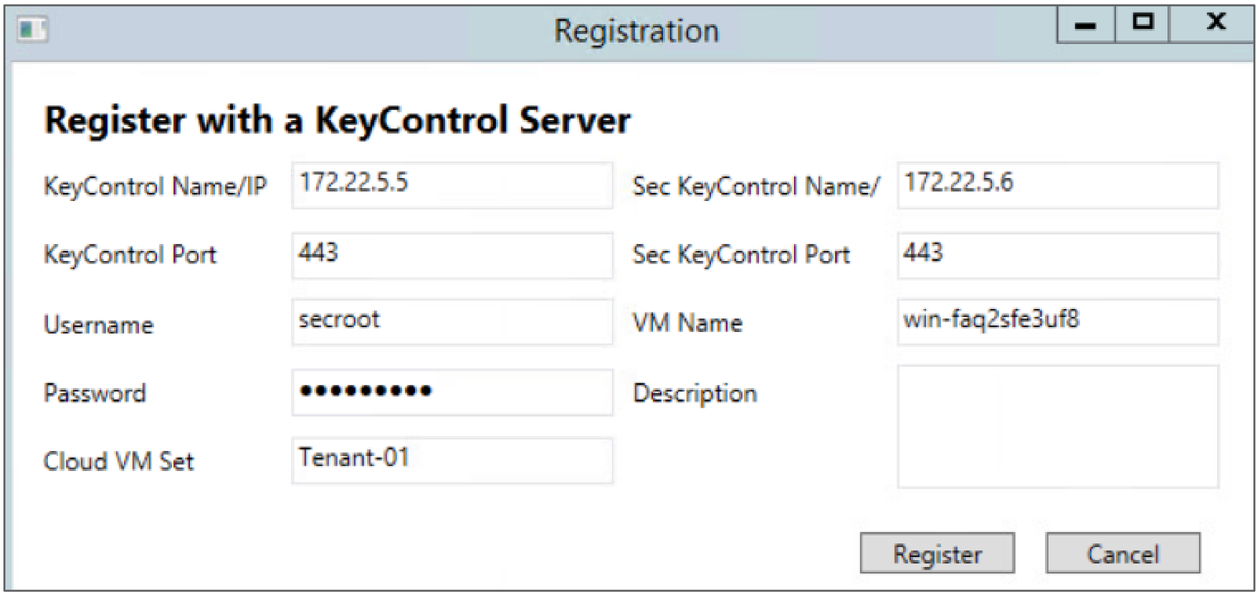


HyTrust Agent Version: 5.0 (b500014687)

KeyControl	
KeyControl List	
Status	Not registered
Last Heartbeat	

Drive	Disk	Part	Cipher	Status	GUID
C:	0	2	none	Avail-Sys	N/A

17. Enter the following details in the Registration dialog box:



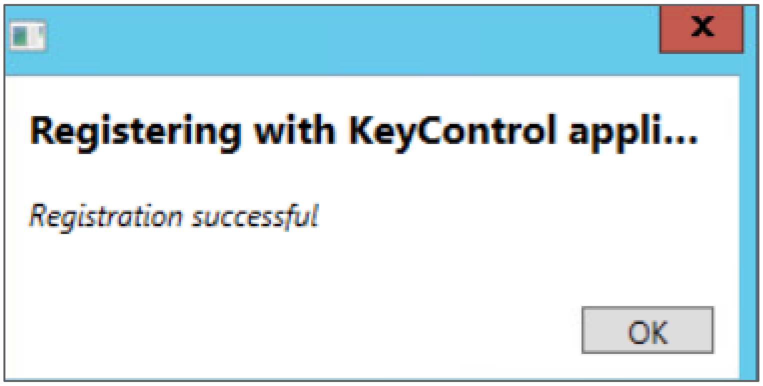
Register with a KeyControl Server

KeyControl Name/IP	172.22.5.5	Sec KeyControl Name/	172.22.5.6
KeyControl Port	443	Sec KeyControl Port	443
Username	secroot	VM Name	win-faq2sfe3uf8
Password	••••••••••	Description	
Cloud VM Set	Tenant-01		

   a. The primary KeyControl Name/IP
   b. The secondary KeyControl Name/IP
   c. The password for the secroot WebGUI user
   d. The name of the Cloud VM set created earlier
   e. A description (optional)

18. Click Register.
19. Click OK after registration is successful.

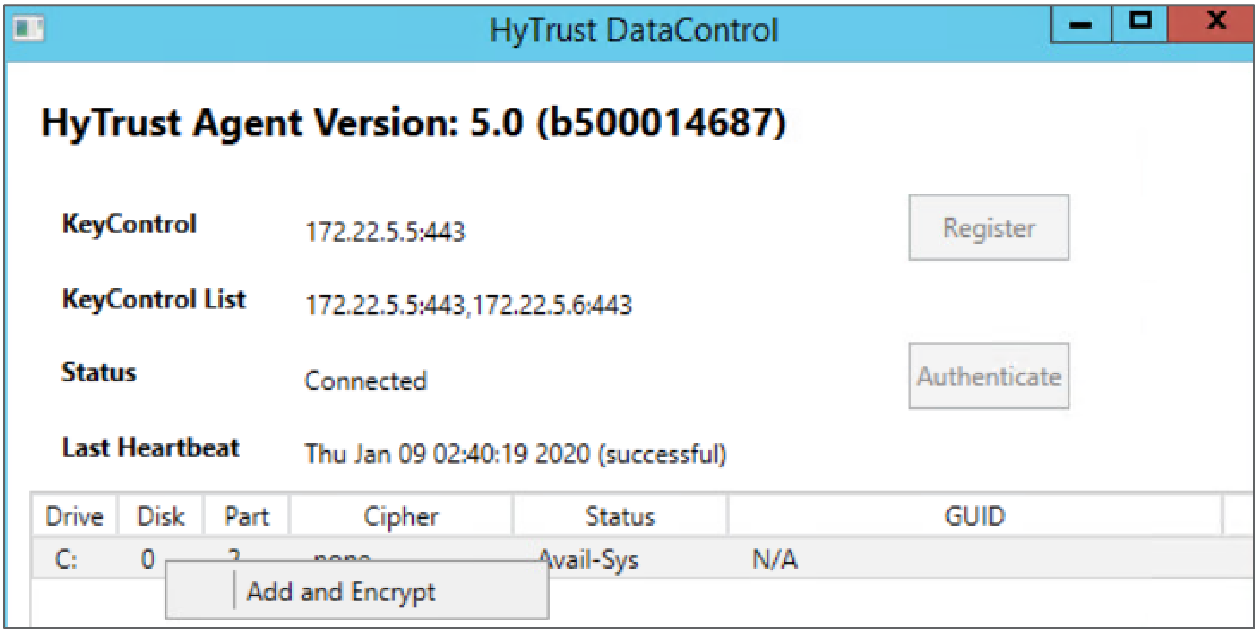
© 2020 NetApp, Inc. All rights reserved.



Registering with KeyControl appli...

Registration successful

20. In the WebGUI, right-click each drive you want to encrypt and protect, and select Add and Encrypt.



HyTrust DataControl

HyTrust Agent Version: 5.0 (b500014687)

KeyControl 172.22.5.5:443

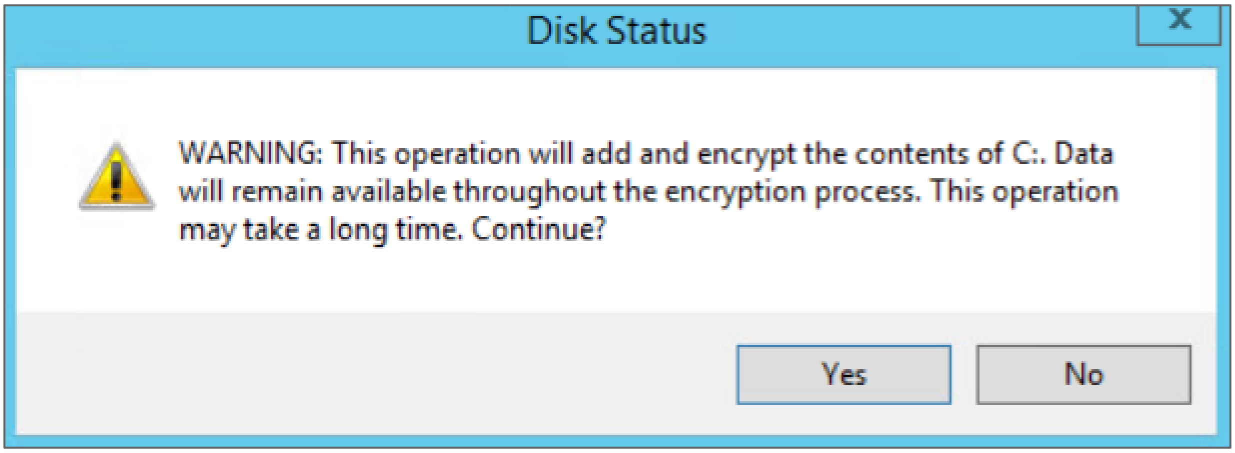
KeyControl List 172.22.5.5:443,172.22.5.6:443

Status Connected

Last Heartbeat Thu Jan 09 02:40:19 2020 (successful)

Drive	Disk	Part	Cipher	Status	GUID
C:	0	2	none	Avail-Sys	N/A

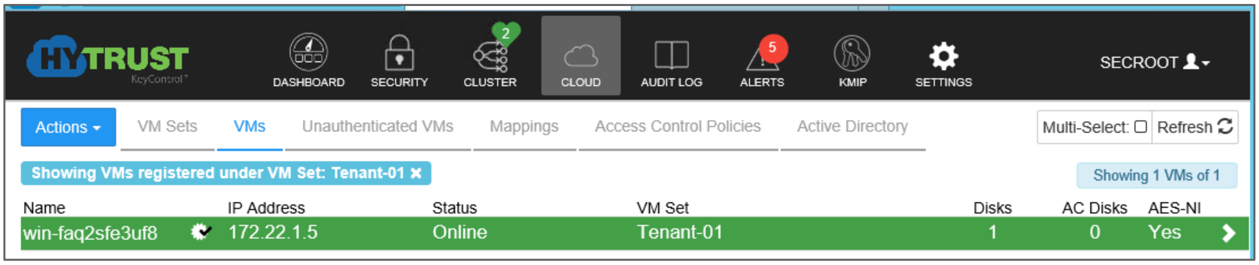
21. Click Yes to continue.



Disk Status

WARNING: This operation will add and encrypt the contents of C:. Data will remain available throughout the encryption process. This operation may take a long time. Continue?

22. The registered VM status is visible in the KeyControl GUI.



Showing VMs registered under VM Set: Tenant-01 ✖

Showing 1 VMs of 1

Name	IP Address	Status	VM Set	Disks	AC Disks	AES-NI
win-faq2sfe3uf8	172.22.1.5	Online	Tenant-01	1	0	Yes

23. Repeat steps 1 through 21 for any other VMs that you would like to protect.

6.4 Set VM Restart Priority

To set up the VM restart priority for the HTCC and KeyControl appliances, complete the following steps:

1. From the vSphere Web Client, select Hosts and Clusters.
2. Navigate to the management cluster. On the right pane, click Manage and then select Settings.
3. Under the Configuration pane, select VM Overrides and then click Add.
4. Click the + button to add VMs. Select the HTCC primary and secondary VMs from the list and click OK.
5. From the VM restart priority drop-down list, select High and then click OK.
6. Repeat steps 2 to 5 for the HTDC VMs running in the tenant-workload cluster.

7 NIST SP 800-53 Revision 4 Controls

Table 6 lists the FedRAMP moderate impact security controls that were addressed by the information system.

Note: Because there are several ways that these measures can be correctly implemented, the implementation steps are out of scope for this document.

Table 6) HCI NIST Security Controls.

Control Family	Control # Addressed	Total Controls
ACCESS CONTROL	AC-2, AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-2(5), AC-2(7), AC-2(11), AC-3, AC-4, AC-4(21), AC-5, AC-6, AC-6(1), AC-6(2), AC-6(5), AC-6(8), AC-6(9), AC-6(10), AC-7, AC-8, AC-10, AC-11, AC-11(1), AC-12, AC-12(1), AC-14, AC-17,	28
AUDIT AND ACCOUNTABILITY	AU-2, AU-2(3), AU-3, AU-3(1), AU-3(2), AU-7, AU-7(1), AU-8, AU-8(1), AU-9, AU-9(2), AU-9(3), AU-12, AU-12(1)	14
SECURITY ASSESSMENT AND AUTHORIZATION	CA-3(5), CA-7, CA-9	3
CONFIGURATION MANAGEMENT	CM-2, CM-2(1), CM-2(2), CM-2(7), CM-3, CM-4, CM-6, CM-6(1), CM-7, CM-7(2), CM-8, CM-8(2), CM-8(3), CM-8(4), CM-9	15
CONTINGENCY PLANNING	CP-9, CP-10	2
IDENTIFICATION AND AUTHENTICATION	IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(4), IA-2(5), IA-2(8), IA-2(9), IA-2(11), IA-5, IA-5(1),IA-	20

© 2020 NetApp, Inc. All rights reserved.

Control Family	Control # Addressed	Total Controls
	5(2), IA-5(4), IA-5(6), IA-6, IA-7, IA-8(1), IA-8(2), IA-8(3), IA-8(4)	
INCIDENT RESPONSE	IR-7	1
RISK ASSESSMENT	RA-5	1
SYSTEM AND SERVICES ACQUISITION	SA-3, SA-5, SA-8, SA-10, SA-11, SA-11(1), SA-11(2), SA-12, SA-17	9
SYSTEM AND COMMUNICATIONS PROTECTION	SC-2, SC-3, SC-4, SC-5, SC-6, SC-7, SC-7(12), SC-7(13), SC-8(1), SC-10, SC-12, SC-13, SC-23, SC-23(1), SC-28, SC-39	16
SYSTEM AND INFORMATION INTEGRITY	SI-4, SI-4(5), SI-5, SI-7, SI-7(1), SI-11, SI-16	8

8 Conclusion

NetApp HCI as a Private Cloud IT infrastructure supports a diverse range of workloads. The flexibility of NetApp HCI as a datacenter opens up several avenues where it can be deployed. Although flexibility is highly desirable, it could also make the system vulnerable to a wide variety of attacks, both internal and external. To safeguard the system and its users from these attacks, it is important to implement an appropriate level of security measures in the system.

The goal of this solution was to highlight the security and privacy features that can be made available on NetApp HCI while adhering to the standards prescribed in the NIST SP 800-53 Revision 4 Moderate Level Security and Privacy controls. We chose and implemented relevant and appropriate controls by using features there are natively available in the HCI system. We also used additional products including VMware NSX and HyTrust CloudControl and DataControl.

The NetApp HCI system has addressed a significant number of moderate-level controls across various control families and thus provides a robust, flexible, and secure platform for hosting a wide variety of workloads.

Acknowledgements

The authors would like to thank the following James Bradshaw at NetApp for their support during the creation of this document.

Where to Find Additional Information

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

- NIST SP 800-53 Rev 4 Moderate Impact Controls
  https://nvd.nist.gov/800-53/Rev4/impact/moderate
- NetApp HCI Theory of Operations
  https://www.netapp.com/us/media/wp-7261.pdf
- NetApp HCI Reference Architecture for FISMA
  https://fieldportal.netapp.com/content/1000800
- HyTrust CloudControl Documentation – Installation & Administration Guides
  https://docs.hytrust.com/CloudControl/5.6.0/Online/Content/OLH-Files/Online-Doc-Set.html

© 2020 NetApp, Inc. All rights reserved.

- HyTrust DataControl Installation & Upgrade Guide https://docs.hytrust.com/DataControl/5.0/HyTrust_DataControl_Installation_and_Upgrade_Guide_v5.0.pdf
- HyTrust DataControl Administration Guide https://docs.hytrust.com/DataControl/5.0/HyTrust_DataControl_Administration_Guide_v5.0.pdf
- NetApp HCI for VMWare Private Cloud References
  - Design Guide: https://www.netapp.com/us/media/nva-1122-design.pdf
  - Deployment Guide: https://www.netapp.com/us/media/nva-1122-deploy.pdf
- VMware NSX 6.4 Data Center for vSphere Documentation https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/index.html
- NetApp Product Documentation docs.netapp.com
- HCI Resources page https://mysupport.netapp.com/info/web/ECMLP2831412.html

Version History

Version	Date	Document Version History
Version 1.0	January 2020	Initial release.

© 2020 NetApp, Inc. All rights reserved.

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 © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

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