



# **Deploying NetApp HCI with Cisco ACI**

## **NetApp Solutions**

NetApp  
May 19, 2021

This PDF was generated from [https://docs.netapp.com/us-en/netapp-solutions/infra/hcicaci\\_vmware\\_vsphere.html](https://docs.netapp.com/us-en/netapp-solutions/infra/hcicaci_vmware_vsphere.html) on May 19, 2021. Always check docs.netapp.com for the latest.

# Table of Contents

- Deploying NetApp HCI with Cisco ACI . . . . . 1
  - VMware vSphere: NetApp HCI with Cisco ACI . . . . . 1
  - Red Hat Virtualization: NetApp HCI with Cisco ACI . . . . . 12
  - KVM on RHEL: NetApp HCI with Cisco ACI . . . . . 17
  - ONTAP on AFF: NetApp HCI and Cisco ACI . . . . . 20
  - ONTAP Select with VMware vSphere: NetApp HCI and Cisco ACI . . . . . 22
  - StorageGRID with VMware vSphere: NetApp HCI and Cisco ACI . . . . . 24

# Deploying NetApp HCI with Cisco ACI

## VMware vSphere: NetApp HCI with Cisco ACI

VMware vSphere is an industry-leading virtualization platform that provides a way to build a resilient and reliable virtual infrastructure. vSphere contains virtualization, management, and interface layers. The two core components of VMware vSphere are ESXi server and the vCenter Server. VMware ESXi is hypervisor software installed on a physical machine that facilitates hosting of VMs and virtual appliances. vCenter Server is the service through which you manage multiple ESXi hosts connected in a network and pool host resources. For more information on VMware vSphere, see the documentation [here](#).

### Workflow

The following workflow was used to up the virtual environment. Each of these steps might involve several individual tasks.

1. Install and configure Nexus 9000 switches in ACI mode and APIC software on the UCS C-series server. See the Install and Upgrade [documentation](#) for detailed steps.
2. Configure and setup ACI fabric by referring to the [documentation](#).
3. Configure the tenants, application profiles, bridge domains, and EPGs required for NetApp HCI nodes. NetApp recommends using one BD to one EPG framework, except for iSCSI. See the documentation [here](#) for more details. The minimum set of EPGs required are in-band management, iSCSI, iSCSI-A, iSCSI-B, VM motion, VM-data network, and native.



iSCSI multipathing requires two iSCSI EPGs: iSCSI-A and iSCSI-B, each with one active uplink.



NetApp mNode requires an iSCSI EPG with both uplinks active.

4. Create the VLAN pool, physical domain, and AEP based on the requirements. Create the switch and interface profiles for individual ports. Then attach the physical domain and configure the static paths to the EPGs. See the [configuration guide](#) for more details.

## VLAN Pool - HCI-Internal-Phys-Dom-VLAN (Static Allocation)

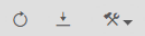


Policy

Operational

Faults

History



### Properties

Name: HCI-Internal-Phys-Dom-VLAN

Description: optional

Alias:

Allocation Mode: Static Allocation

Encap Blocks:

| VLAN Range  | Allocation Mode               | Role                                   |
|-------------|-------------------------------|--|
| [2]         | Inherit allocMode from parent | External or On the wire encapsulations |
| [3201-3250] | Inherit allocMode from parent | External or On the wire encapsulations |

| Domains: | Name                  | Type            |
|----------|-----------------------|-----------------|
|          | HCI-Internal-Phys-Dom | Physical Domain |

Show Usage

Close

Submit

## Leaf Access Port Policy Group - HCI-Compute-ESX



### Properties

Name: HCI-Compute-ESX

Description: optional

Alias:

Link Level Policy: 10G-Auto

CDP Policy: CDP-Disabled

MCP Policy: select a value

CoPP Policy: select a value

LLDP Policy: LLDP-Enabled



Use an access port policy group for interfaces connecting to NetApp HCI compute nodes, and use vPC policy group for interfaces to NetApp HCI storage nodes.

5. Create and assign contracts for tightly-controlled access between workloads. For more information on

configuring the contracts, see the guide [here](#).

6. Install and configure NetApp HCI using NDE. NDE configures all the required parameters, including VDS port groups for networking, and also installs the mNode VM. See the [deployment guide](#) for more information.
7. Though VMM integration of Cisco ACI with VMware VDS is optional, using the VMM integration feature is a best practice. When not using VMM integration, an NDE-installed VDS can be used for networking with physical domain attachment on Cisco ACI.
8. If you are using VMM integration, NDE-installed VDS cannot be fully managed by ACI and can be added as read-only VMM domain. To avoid that scenario and make efficient use of Cisco ACI's VMM networking feature, create a new VMware VMM domain in ACI with a new VMware vSphere Distributed Switch (vDS) and an explicit dynamic VLAN pool. The VMM domain created can integrate with any supported virtual switch.
  - a. **Integrate with VDS.** If you wish to integrate ACI with VDS, select the virtual switch type to be VMware Distributed Switch. Consider the configuration best practices noted in the following table. See the [configuration guide](#) for more details.

## Properties

|                              |                        |
|------------------------------|------------------------|
| Name:                        | hci-aci-vds-02         |
| Virtual Switch:              | Distributed Switch     |
| Associated Attachable Entity | <a href="#">▲ Name</a> |
| Profiles:                    | HCI-Internal           |

---


|                                    |  |
|------------------------------------|--|
| Encapsulation:                     | vlan                                     |
| Delimiter:                         |  |
| Enable Tag Collection:             | <input checked="" type="checkbox"/>      |
| Enable VM Folder Data Retrieval:   | <input type="checkbox"/>                 |
| Access Mode:                       | <div>Read Only ModeRead Write Mode</div> |
| Endpoint Retention Time (seconds): | <div>0</div>                             |
| VLAN Pool:                         | <div>hci-aci-vmware(dynamic)</div>       |

- b. **Integrate with Cisco AVE.** If you are integrating Cisco AVE with Cisco ACI, select the virtual switch type to be Cisco AVE. Cisco AVE requires a unique VLAN pool of type Internal for communicating between internal and external port groups. Follow the configuration best practices noted in this table. See the [installation guide](#) to install and configure Cisco AVE.


## Properties

Name: hci-vmware-ave

Virtual Switch: Cisco AVE

AVE Time-out Time (seconds):  

Host Availability Assurance: ☐


Associated Attachable Entity  Name

Profiles:

|              |
|--------------|
| HCI-Internal |
|--------------|

---

Switching Preference:


Enhanced Lag Policy:  


Encapsulation: vxlan

Default Encap Mode:

Enable Tag Collection: ☒


Enable VM Folder Data Retrieval: ☐

Endpoint Retention Time (seconds):  

VLAN Pool:  

AVE Fabric-Wide Multicast

Address: Must Use a Multicast Address different from the Multicast Address Ranges.

Pool of Multicast Addresses (one per-EPG):  

9. Attach the VMM domain to the EPGs using Pre-Provision Resolution Immediacy. Then migrate all the VMNICs, VMkernel ports, and VNICs from the NDE-created VDS to ACI-created VDS or AVE and so on. Configure the uplink failover and teaming policy for iSCSI-A and iSCSI-B to have one active uplink each. VMs can now attach their VMNICs to ACI-created port groups to access network resources. The port groups on VDS that are managed by Cisco ACI are in the format of `<tenant-name>|<application-profile-name>|<epg-name>`.



Pre-Provision Resolution Immediacy is required to ensure the port policies are downloaded to the leaf switch even before the VMM controller is attached to the virtual switch.

hci-aci-vds-02 | ACTIONS ▾

Summary Monitor Configure Permissions Ports Hosts VMs Networks

Manufacturer: VMware, Inc.  
Version: 6.6.0  
[Upgrades available](#)

Switch Details ▾

Notes ▴

APIC Virtual Switch  
[Edit Notes...](#)

## VMkernel adapters

Add Networking... Refresh Edit... Remove

| Device ▾ | Network Label ▾  | Switch ▾       | IP Address ▾ | TCP/IP Stack ▾ | vMotion ▾ | Provisioning ▾ |
|----------|------------------|----------------|--------------|----------------|-----------|----------------|
| vmk0     | HCI-InfraHCLH... | hci-vmware-ave | 172.22.9.60  | Default        | Disabled  | Disabled       |
| vmk1     | HCI-InfraHCLH... | hci-vmware-ave | 172.22.10.60 | Default        | Disabled  | Disabled       |
| vmk2     | HCI-InfraHCLH... | hci-vmware-ave | 172.22.10.58 | Default        | Disabled  | Disabled       |
| vmk3     | HCI-InfraHCLH... | hci-vmware-ave | 172.22.13.60 | Default        | Enabled   | Disabled       |
| vmk4     | HCI-InfraHCLH... | hci-vmware-ave | 172.22.15.60 | Default        | Disabled  | Disabled       |

10. If you intend to use micro-segmentation, then create micro-segment (uSeg) EPGs attaching to the right BD. Create attributes in VMware vSphere and attach them to the required VMs. Ensure the VMM domain has Enable Tag Collection enabled. Configure the uSeg EPGs with the corresponding attribute and attach the VMM domain to it. This provides more granular control of communication on the endpoint VMs.

Tenant HCI-Infra

uSeg Attributes

Policy History

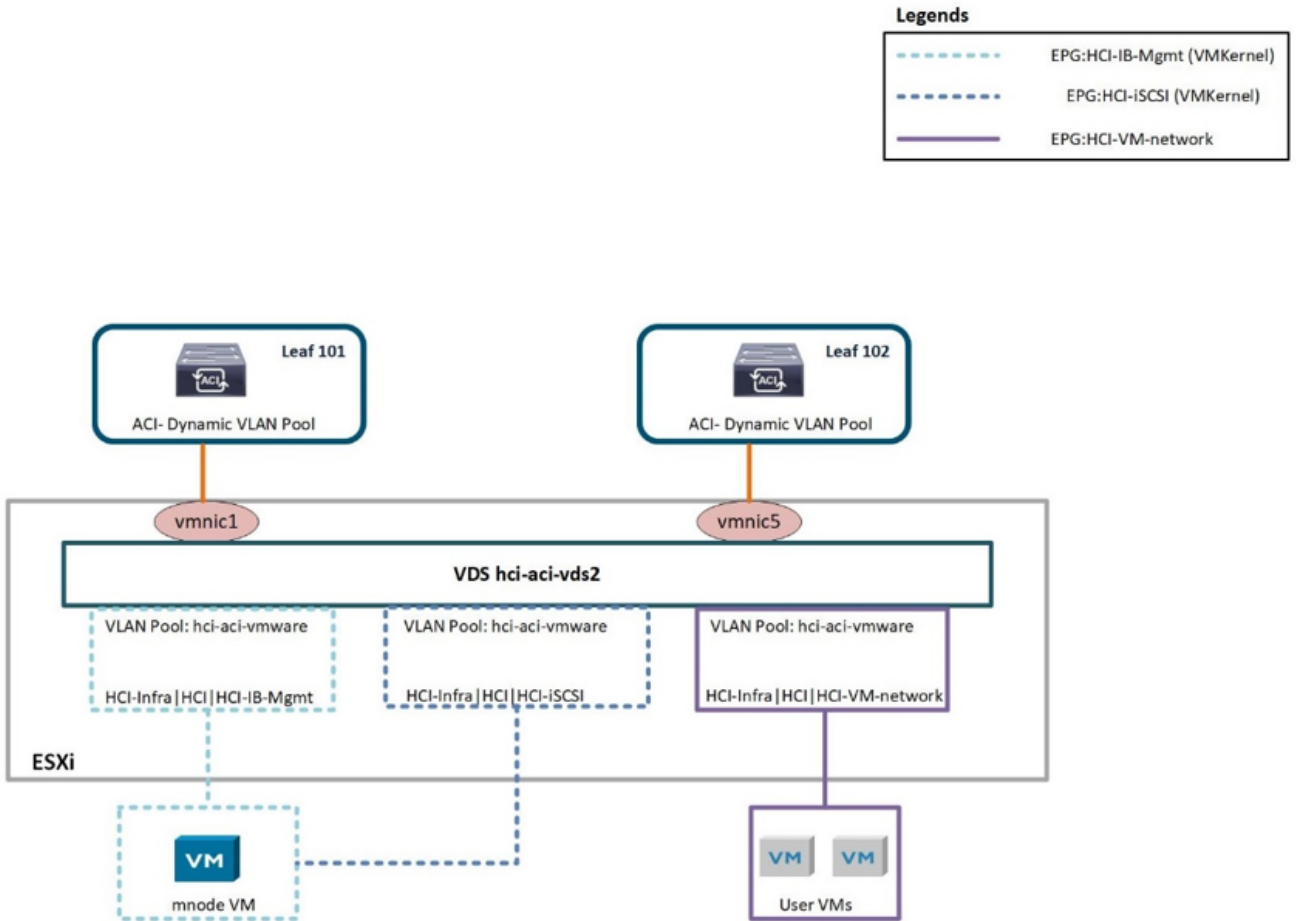
Match Any ▾

VM - Tag ▾ ubuntu Contains ▾ ubuntu-prod

The networking functionality for VMware vSphere on NetApp HCI in this solution is provided either using VMware VDS or Cisco AVE.

## VMware VDS

VMware vSphere Distributed Switch (VDS) is a virtual switch that connects to multiple ESXi hosts in the cluster or set of clusters allowing virtual machines to maintain consistent network configuration as they migrate across multiple hosts. VDS also provides for centralized management of network configurations in a vSphere environment. For more details, see the [VDS documentation](#).



The following table outlines the necessary parameters and best practices for configuring and integrating Cisco ACI with VMware VDS.



| Resource         | Configuration Considerations   | Best Practices  |
|------------------|--|---|
| Endpoint groups  | <ul style="list-style-type: none"> <li>• Separate EPG for native VLANs</li> <li>• Static binding of interfaces to HCI storage and compute nodes in native VLAN EPG uses 802.1P mode. This is required for node discovery to run NDE.</li> <li>• Separate EPGs for iSCSI, iSCSI-A, and iSCSI-B with a common BD</li> <li>• iSCSI-A and iSCSI-B are for iSCSI multipathing and are used for VMkernel ports on ESXi hosts</li> <li>• Physical domain to be attached to iSCSI EPG before running NDE</li> <li>• VMM domain to be attached to iSCSI, iSCSI-A, and iSCSI-B EPGs</li> </ul> | <ul style="list-style-type: none"> <li>• Contracts between EPGs to be well defined. Allow only required ports for communication.</li> <li>• Use unique native VLAN for NDE node discovery</li> <li>• For EPGs corresponding to port-groups being attached to VMkernel ports, VMM domain to be attached with Pre-Provision for Resolution Immediacy</li> </ul> |
| Interface policy | <ul style="list-style-type: none"> <li>• A common leaf access port policy group for all ESXi hosts</li> <li>• One vPC policy group per NetApp HCI storage node</li> <li>• LLDP enabled, CDP disabled</li> </ul>  | <ul style="list-style-type: none"> <li>• Separate VLAN pool for VMM domain with dynamic allocation turned on</li> <li>• Recommended to use vPC with LACP Active port-channel policy for interfaces towards NetApp HCI storage nodes</li> <li>• Recommended to use individual interfaces for compute nodes, no LACP.</li> </ul>                                |
| VMM Integration  | <ul style="list-style-type: none"> <li>• Local switching preference</li> <li>• Access mode is Read Write.</li> </ul>   | <ul style="list-style-type: none"> <li>• MAC-Pinning-Physical-NIC-Load for vSwitch policy</li> <li>• LLDP for discovery policy</li> <li>• Enable Tag collection if micro-segmentation is used</li> </ul>  |
| VDS              | <ul style="list-style-type: none"> <li>• Both uplinks active for iSCSI port-group</li> <li>• One uplink each for iSCSI-A and iSCSI-B</li> </ul>  | <ul style="list-style-type: none"> <li>• Load balancing method for all port-groups to be 'Route based on physical NIC load'</li> <li>• iSCSI VMkernel port migration to be done one at a time from NDE deployed VDS to ACI integrated VDS</li> </ul>  |

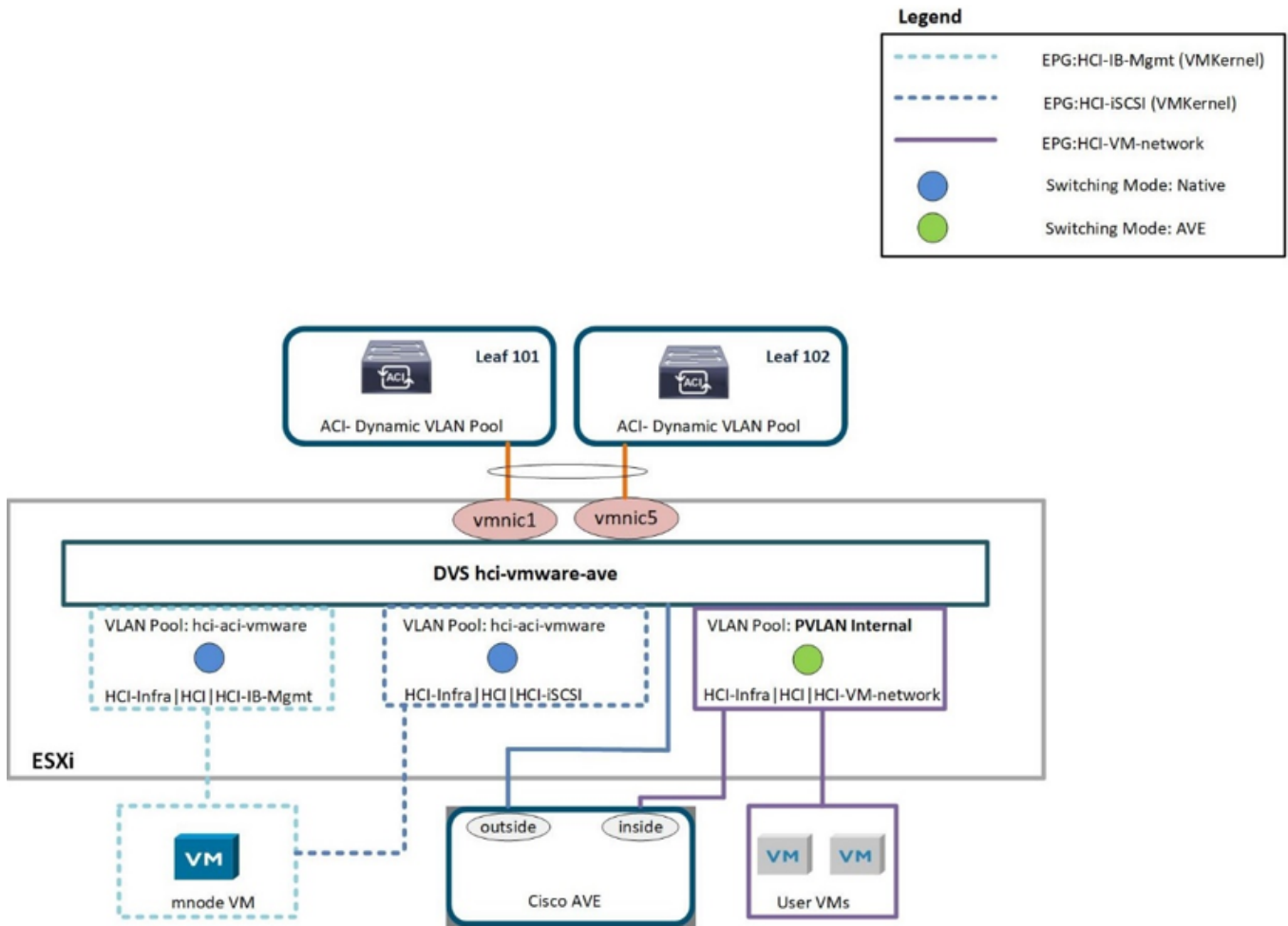
| Resource   | Configuration Considerations   | Best Practices  |
|------------|--|---|
| Easy Scale | <ul style="list-style-type: none"> <li>• Run NDE scale by attaching the same leaf access port policy group for ESXi hosts to be added</li> <li>• One vPC policy group per NetApp HCI storage node</li> <li>• Individual interfaces (for ESXi hosts) and vPCs (for storage nodes) should be attached to native, in-band management, iSCSI, VM motion EPGs for successful NDE scale</li> <li>• LLDP enabled, CDP disabled</li> </ul> | <ul style="list-style-type: none"> <li>• Recommended to use vPC with LACP Active port-channel policy for interfaces towards NetApp HCI storage nodes</li> <li>• Recommended to use individual interfaces for compute nodes, no LACP.</li> </ul> |



For traffic load-balancing, port channels with vPCs can be used on Cisco ACI along with LAGs on VDS with LACP in active mode. However, using LACP can affect storage performance when compared to iSCSI multipathing.

## Cisco AVE

Cisco ACI Virtual Edge (AVE) is a virtual switch offering by Cisco that extends the Cisco ACI policy model to virtual infrastructure. It is a hypervisor- independent distributed network service that sits on top of the native virtual switch of the hypervisor. It leverages the underlying virtual switch using a VM-based solution to provide network visibility into the virtual environments. For more details on Cisco AVE, see the [documentation](#). The following figure depicts the internal networking of Cisco AVE on an ESXi host (as tested).



The following table lists the necessary parameters and best practices for configuring and integrating Cisco ACI with Cisco AVE on VMware ESXi. Cisco AVE is currently only supported with VMware vSphere.

| Resource         | Configuration Considerations  | Best Practices   |
|------------------|---|--|
| Endpoint Groups  | <ul style="list-style-type: none"> <li>• Separate EPG for native VLANs</li> <li>• Static binding of interfaces towards HCI storage and compute nodes in native VLAN EPG uses 802.1P mode. This is required for node discovery to run NDE.</li> <li>• Separate EPGs for iSCSI, iSCSI-A and iSCSI-B with a common BD</li> <li>• iSCSI-A and iSCSI-B are for iSCSI multipathing and are used for VMkernel ports on ESXi hosts</li> <li>• Physical domain to be attached to iSCSI EPG before running NDE</li> <li>• VMM domain is attached to iSCSI, iSCSI-A, and iSCSI-B EPGs</li> </ul> | <ul style="list-style-type: none"> <li>• Separate VLAN pool for VMM domain with dynamic allocation turned on</li> <li>• Contracts between EPGs to be well defined. Allow only required ports for communication.</li> <li>• Use unique native VLAN for NDE node discovery</li> <li>• Use native switching mode in VMM domain for EPGs that correspond to port groups being attached to host's VMkernel adapters</li> <li>• Use AVE switching mode in VMM domain for EPGs corresponding to port groups carrying user VM traffic</li> <li>• For EPGs corresponding to port-groups being attached to VMkernel ports, VMM domain is attached with Pre-Provision for Resolution Immediacy</li> </ul> |
| Interface Policy | <ul style="list-style-type: none"> <li>• One vPC policy group per NetApp HCI storage node</li> <li>• LLDP enabled, CDP disabled</li> <li>• Before running NDE, for NDE discovery: <ul style="list-style-type: none"> <li>◦ Leaf Access port policy group for all ESXi hosts</li> </ul> </li> <li>• After running NDE, for Cisco AVE: <ul style="list-style-type: none"> <li>◦ One vPC policy group per ESXi host</li> </ul> </li> </ul>   | <ul style="list-style-type: none"> <li>• NetApp recommends using vPCs to ESXi hosts for Cisco AVE</li> <li>• Use static mode on port-channel policy for vPCs to ESXi</li> <li>• Use Layer-4 SRC port load balancing hashing method for port-channel policy</li> <li>• NetApp recommends using vPC with LACP active port-channel policy for interfaces to NetApp HCI storage nodes</li> </ul>   |

| Resource        | Configuration Considerations   | Best Practices  |
|-----------------|--|---|
| VMM Integration | <ul style="list-style-type: none"> <li>• Create a new VLAN range [or Encap Block] with role Internal and Dynamic allocation' attached to the VLAN pool intended for VMM domain</li> <li>• Create a pool of multicast addresses (one address per EPG)</li> <li>• Reserve another multicast address different from the pool of multicast addresses intended for AVE fabric-wide multicast address</li> <li>• Local switching preference</li> <li>• Access mode to be Read Write mode</li> </ul>  | <ul style="list-style-type: none"> <li>• Static mode on for vSwitch policy</li> <li>• Ensure that vSwitch port-channel policy and interface policy group's port-channel policy are using the same mode</li> <li>• LLDP for discovery policy</li> <li>• Enable Tag collection if using micro-segmentation</li> <li>• Recommended option for Default Encap mode is VXLAN</li> </ul> |
| VDS             | <ul style="list-style-type: none"> <li>• Both uplinks active for iSCSI port-group</li> <li>• One uplink each for iSCSI-A and iSCSI-B</li> </ul>  | <ul style="list-style-type: none"> <li>• iSCSI VMkernel port migration is done one at a time from NDE deployed VDS to ACI integrated VDS</li> <li>• Load balancing method for all port-groups to be Route based on IP hash</li> </ul>   |
| Cisco AVE       | <ul style="list-style-type: none"> <li>• Run NDE with access port interface policy groups towards ESXi hosts. Individual interfaces towards ESXi hosts should be attached to native, in-band management, iSCSI, VM motion EPGs for successful NDE run.</li> <li>• Once the environment is up, place the host in maintenance mode, migrate interface policy group to vPC with static mode on, assign vPC to all required EPGs and remove the host from maintenance mode. Repeat the same process for all hosts.</li> <li>• Run the AVE installation process to install AVE control VM on all hosts</li> </ul> | <ul style="list-style-type: none"> <li>• Use local datastore on the hosts for installing AVE control VM. Each host should have one AVE control VM installed on it</li> <li>• Use network protocol profile on the in-band management VLAN if DHCP is not available on that network</li> </ul>  |

| Resource   | Configuration Considerations  | Best Practices   |
|------------|---|--|
| Easy Scale | <ul style="list-style-type: none"> <li>• Run NDE scale with access port interface policy group for ESXi hosts to be added. Individual interfaces should be attached to native, in-band management, iSCSI, VM motion EPGs for successful NDE run.</li> <li>• <b>Once the ESXi host is added to the vSphere cluster, place the host in maintenance mode and migrate the interface policy group to vPC with static mode on. Then attach the vPC to required EPGs.</b></li> <li>• Run AVE installation process on the new host for installing AVE control VM on that host</li> <li>• One vPC policy group per NetApp HCI storage node to be added to the cluster</li> <li>• LLDP enabled, CDP disabled</li> </ul> | <ul style="list-style-type: none"> <li>• Use local datastore on the host for installing AVE control VM</li> <li>• Use network protocol profile on the in-band management VLAN if DHCP is not available on that network</li> <li>• Recommended to use vPC with LACP Active port-channel policy for interfaces towards NetApp HCI storage nodes</li> </ul> |

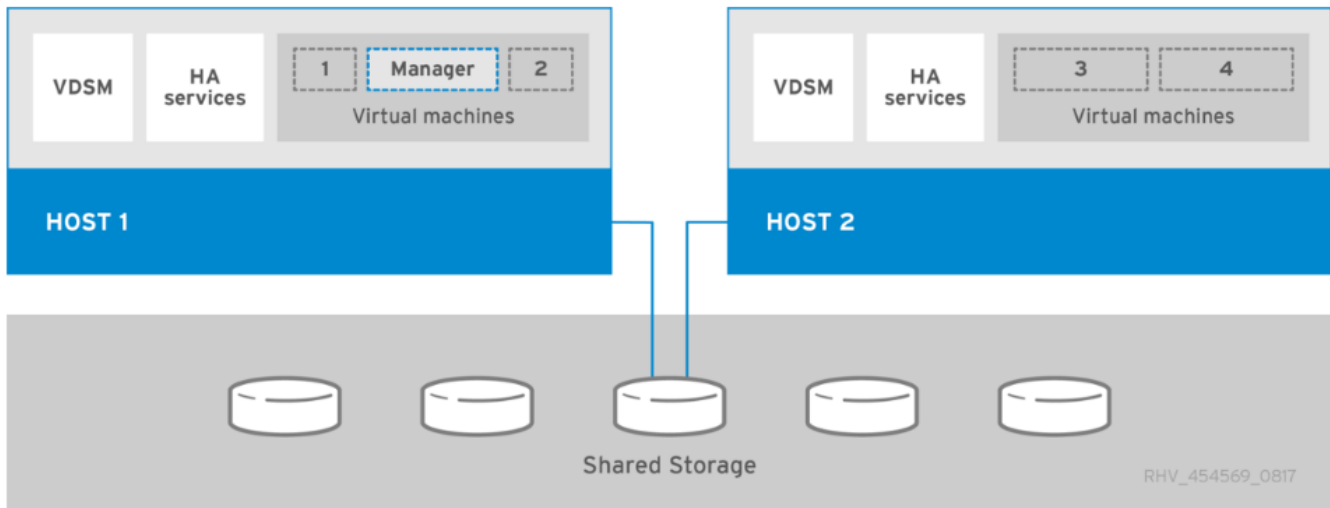


For traffic load balancing, port channel with vPCs can be used on Cisco ACI along with LAGs on ESXi hosts with LACP in active mode. However, using LACP can affect storage performance when compared to iSCSI multipathing.

Next: [Red Hat Virtualization: NetApp HCI with Cisco ACI](#)

## Red Hat Virtualization: NetApp HCI with Cisco ACI

Red Hat Virtualization (RHV) is an enterprise virtual data center platform that runs on Red Hat Enterprise Linux using the KVM hypervisor. The key components of RHV include Red Hat Virtualization Hosts (RHV-H) and the Red Hat Virtualization Manager (RHV-M). RHV-M provides centralized, enterprise-grade management for the physical and logical resources within the virtualized RHV environment. RHV-H is a minimal, light-weight operating system based on Red Hat Enterprise Linux that is optimized for the ease of setting up physical servers as RHV hypervisors. For more information on RHV, see the documentation [here](#). The following figure provides an overview of RHV.



Starting with Cisco APIC release 3.1, Cisco ACI supports VMM integration with Red Hat Virtualization environments. The RHV VMM domain in Cisco APIC is connected to RHV-M and directly associated with a data center object. All the RHV-H clusters under this data center are considered part of the VMM domain. Cisco ACI automatically creates logical networks in RHV-M when the EPGs are attached to the RHV VMM domain in ACI. RHV hosts that are part of a Red Hat VMM domain can use Linux bridge or Open vSwitch as its virtual switch. This integration simplifies and automates networking configuration on RHV-M, saving a lot of manual work for system and network administrators.

## Workflow

The following workflow is used to set up the virtual environment. Each of these steps might involve several individual tasks.

1. Install and configure Nexus 9000 switches in ACI mode and APIC software on the UCS C-series server. Refer to the Install and Upgrade [documentation](#) for detailed steps.
2. Configure and setup the ACI fabric by referring to the [documentation](#).
3. Configure tenants, application profiles, bridge domains, and EPGs required for NetApp HCI nodes. NetApp recommends using one BD to one EPG framework, except for iSCSI. See the [documentation here](#) for more details. The minimum set of EPGs required are in-band management, iSCSI, VM motion, VM-data network, and native.
4. Create the VLAN pool, physical domain, and AEP based on the requirements. Create the switch and interface profiles and policies for vPCs and individual ports. Then attach the physical domain and configure the static paths to the EPGs. see the [configuration guide](#) for more details. This table lists best practices for integrating ACI with Linux bridge on RHV.

# PC/VPC Interface Policy Group - HCI-RHVH01



## Properties

Name: HCI-RHVH01

Description: optional

Link Aggregation Type: Port Channel **VPC**

Link Level Policy: 10G-Auto 

CDP Policy: CDP-Disabled 

MCP Policy: select a value

CoPP Policy: select a value

LLDP Policy: LLDP-Enabled 

STP Interface Policy: select a value

Egress Data Plane Policing Policy: select a value

Ingress Data Plane Policing Policy: select a value

Priority Flow Control Policy: select a value

Fibre Channel Interface Policy: select a value

Slow Drain Policy: select a value

Port Channel Policy: LACP-Active 



Use a vPC policy group for interfaces connecting to NetApp HCI storage and compute nodes.

5. Create and assign contracts for tightly controlled access between workloads. For more information on configuring the contracts, see the guide [here](#).
6. Install and configure the NetApp HCI Element cluster. Do not use NDE for this install; rather, install a standalone Element cluster on the HCI storage nodes. Then configure the required volumes for installation of RHV. Install RHV on NetApp HCI. Refer to [RHV on NetApp HCI NVA](#) for more details.
7. RHV installation creates a default management network called ovirtmgmt. Though VMM integration of Cisco ACI with RHV is optional, leveraging VMM integration is preferred. Do not create other logical networks manually. To use Cisco ACI VMM integration, create a Red Hat VMM domain and attach the VMM domain to all the required EPGs, using Pre- Provision Resolution Immediacy. This process automatically creates corresponding logical networks and vNIC profiles. The vNIC profiles can be directly



used to attach to hosts and VMs for their communication. The networks that are managed by Cisco ACI are in the format `<tenant-name>|<application-profile-name>|<epg-name>` tagged with a label of format `aci_<rhv-vmm-domain-name>`. See [Cisco's whitepaper](#) for creating and configuring a VMM domain for RHV. Also, see this table for best practices when integrating RHV on NetApp HCI with Cisco ACI.



Except for ovirtmgmt, all other logical networks can be managed by Cisco ACI.

Network > Networks

| Name                         | Comment | Data Center | Description        | Role | VLAN Tag | QoS Nam | Label           | Provider | MTU            |
|------------------------------|---------|-------------|--------------------|------|----------|---------|-----------------|----------|----------------|
| HCI-Infra AFF-A200 AFF-NFS   |         | Default     |                    |      | 1569     | -       | aci_hci-aci-rhv |          | 9000           |
| HCI-Infra HCI HCI-IB-Mgmt    |         | Default     |                    |      | 1567     | -       | aci_hci-aci-rhv |          | Default (1500) |
| HCI-Infra HCI HCI-IB-SCSI    |         | Default     |                    |      | 1568     | -       | aci_hci-aci-rhv |          | 9000           |
| HCI-Infra HCI HCI-VM-motion  |         | Default     |                    |      | 1634     | -       | aci_hci-aci-rhv |          | Default (1500) |
| HCI-Infra HCI HCI-VM-network |         | Default     |                    |      | 1570     | -       | aci_hci-aci-rhv |          | Default (1500) |
| ovirtmgmt                    |         | Default     | Management Network |      | 3201     | -       | -               |          | Default (1500) |
| quarantine                   |         | Default     |                    |      | 666      | -       | aci_hci-aci-rhv |          | Default (1500) |
| uplinkNetwork                |         | Default     | uplinkNetwork      |      | -        | -       | -               |          | Default (1500) |

### Setup Host hci-aci-rtp-rhvh01.cie.netapp.com Networks

Drag to make changes

Interfaces

Assigned Logical Networks

bond0

eno1

ens14f1

eno2

no network assigned

HCI-Infra|AFF-A200|... (VLAN 1569)

HCI-Infra|HCI|HCI-IS... (VLAN 1568)

HCI-Infra|HCI|HCI-V... (VLAN 1634)

HCI-Infra|HCI|HCI-V... (VLAN 1570)

ovirtmgmt (VLAN 3201)

[New Label]

aci\_hci-aci-rhv

HCI-Infra|AFF-A200... (VLAN 1569)

HCI-Infra|HCI|HCI-IB-Mg... (VLAN 1567)

HCI-Infra|HCI|HCI-i... (VLAN 1568)

HCI-Infra|HCI|HCI-V... (VLAN 1634)

HCI-Infra|HCI|HCI-V... (VLAN 1570)

☒ Verify connectivity between Host and Engine
 ☒ Save network configuration

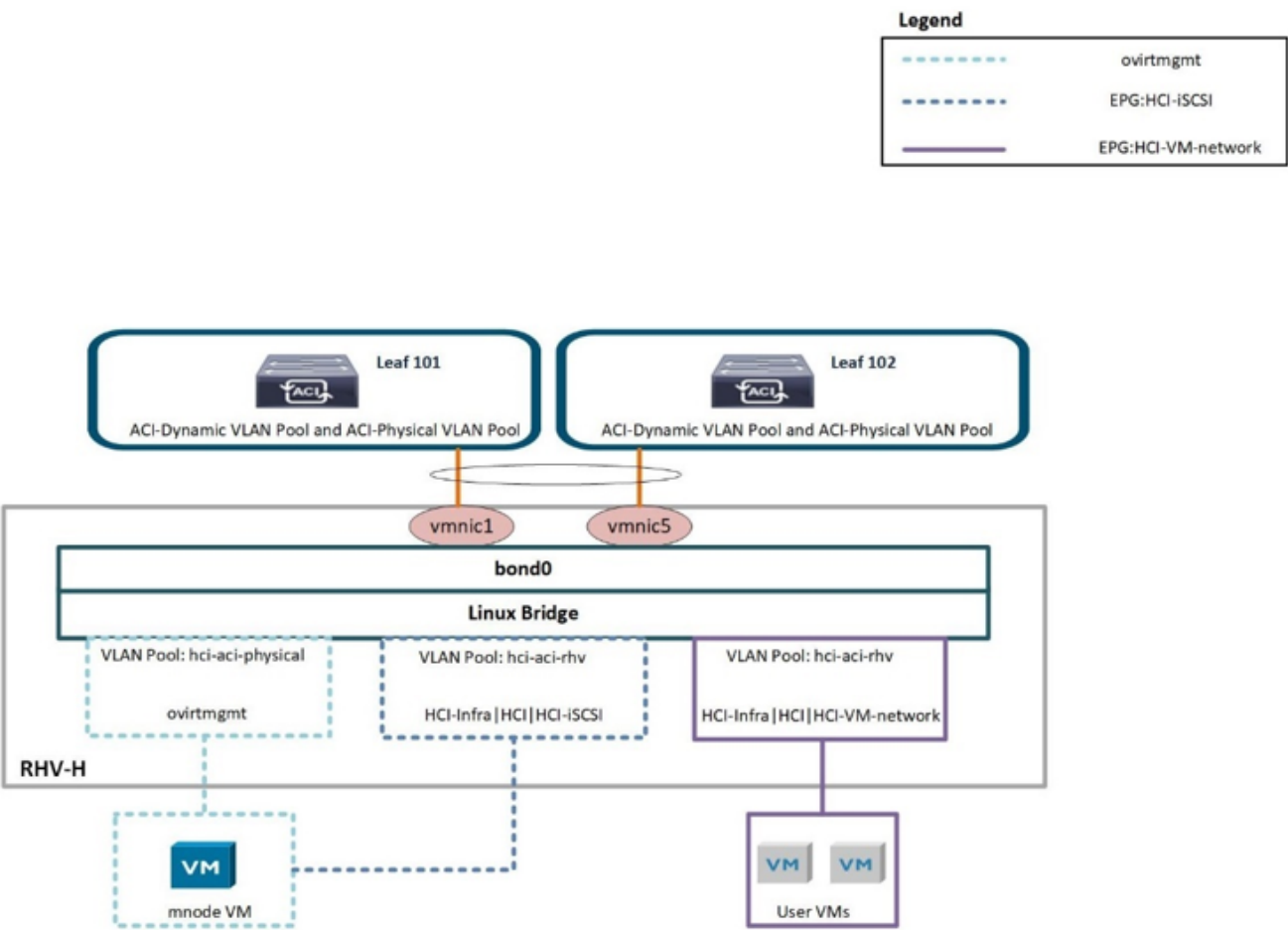
OK

Cancel

The networking functionality for RHVH hosts in this solution is provided by Linux bridge.

# Linux Bridge

Linux Bridge is a default virtual switch on all Linux distributions that is usually used with KVM/QEMU-based hypervisors. It is designated to forward traffic between networks based on MAC addresses and thus is regarded as a layer-2 virtual switch. For more information, see the documentation [here](#). The following figure depicts the internal networking of Linux Bridge on RHV-H (as tested).



The following table outlines the necessary parameters and best practices for configuring and integrating Cisco ACI with Linux Bridge on RHV hosts.

| Resource         | Configuration considerations  | Best Practices   |
|------------------|---|--|
| Endpoint groups  | <ul style="list-style-type: none"> <li>• Separate EPG for native VLAN</li> <li>• Static binding of interfaces towards HCI storage and compute nodes in native VLAN EPG to be on 802.1P mode</li> <li>• Static binding of vPCs required on In-band management EPG and iSCSI EPG before RHV installation</li> </ul> | <ul style="list-style-type: none"> <li>• Separate VLAN pool for VMM domain with dynamic allocation turned on</li> <li>• Contracts between EPGs to be well defined. Allow only required ports for communication.</li> <li>• Use unique native VLAN for discovery during Element cluster formation</li> <li>• For EPGs corresponding to port-groups being attached to VMkernel ports, VMM domain to be attached with 'Pre-Provision' for Resolution Immediacy</li> </ul> |
| Interface policy | <ul style="list-style-type: none"> <li>• One vPC policy group per RHV-H host</li> <li>• One vPC policy group per NetApp HCI storage node</li> <li>• LLDP enabled, CDP disabled</li> </ul>   | <ul style="list-style-type: none"> <li>• Recommended to use vPC towards RHV-H hosts</li> <li>• Use 'LACP Active' for the port-channel policy</li> <li>• Use only 'Graceful Convergence' and 'Symmetric Hashing' control bits for port-channel policy<br/>Use 'Layer4 Src-port' load balancing hashing method for port-channel policy<br/>Recommended to use vPC with LACP Active port-channel policy for interfaces towards NetApp HCI storage nodes</li> </ul>        |
| VMM Integration  | <ul style="list-style-type: none"> <li>• Do not migrate host management logical interfaces from ovirtmgmt to any other logical network</li> </ul>   | <ul style="list-style-type: none"> <li>• iSCSI host logical interface to be migrated to iSCSI logical network managed by ACI VMM integration</li> </ul>  |



Except for the ovirtmgmt logical network, it is possible to create all other infrastructure logical networks on Cisco APIC and map them to the VMM domain. 'ovirtmgmt' logical network uses the static path binding on the In-band management EPG attached with the physical domain.

[Next: KVM on RHEL: NetApp HCI with Cisco ACI](#)

## KVM on RHEL: NetApp HCI with Cisco ACI

KVM (for Kernel-based Virtual Machine) is an open-source full virtualization solution for

Linux on x86 hardware such as Intel VT or AMD-V. In other words, KVM lets you turn a Linux machine into a hypervisor that allows the host to run multiple, isolated VMs.

KVM converts any Linux machine into a type-1 (bare-metal) hypervisor. KVM can be implemented on any Linux distribution, but implementing KVM on a supported Linux distribution—like Red Hat Enterprise Linux—expands KVM’s capabilities. You can swap resources among guests, share common libraries, and optimize system performance.

## Workflow

The following high-level workflow was used to set up the virtual environment. Each of these steps might involve several individual tasks.

1. Install and configure Nexus 9000 switches in ACI mode, and install and configure APIC software on a UCS C-series server. See the Install and Upgrade [documentation](#) for detailed steps.
2. Configure and set up the ACI fabric by referring to the [documentation](#).
3. Configure the tenants, application profiles, bridge domains, and EPGs required for NetApp HCI nodes. NetApp recommends using a one-BD-to-one-EPG framework except for iSCSI. See the [documentation here](#) for more details. The minimum set of EPGs required are in-band management, iSCSI, VM Motion, VM-data network, and native.
4. Create the VLAN pool, physical domain, and AEP based on the requirements. Create the switch and interface profiles and policies for vPCs and individual ports. Then attach the physical domain and configure the static paths to the EPGs. See the [configuration guide](#) for more details. Also see this table [<link>](#) for best practices for integrating ACI with Open vSwitch on the RHEL–KVM hypervisor.



Use a vPC policy group for interfaces connecting to NetApp HCI storage and compute nodes.

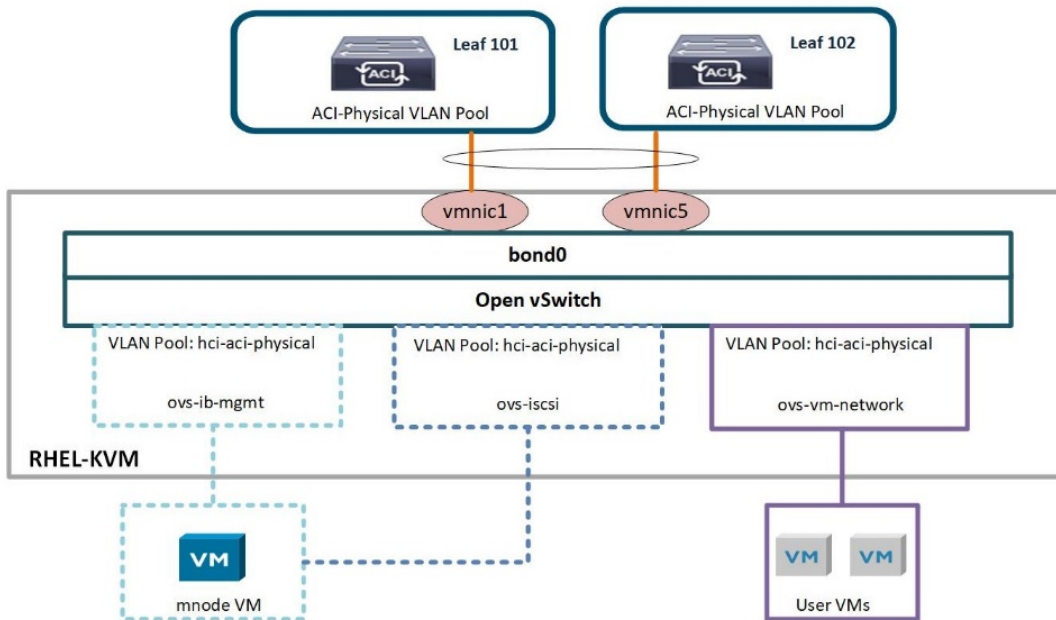
5. Create and assign contracts for tightly-controlled access between workloads. For more details on configuring the contracts, see the guide [here](#).
6. Install and configure a NetApp HCI Element cluster. Do not use NDE for this installation; rather, install a standalone Element cluster on HCI storage nodes. Then configure the required volumes for the installation of RHEL. Install RHEL, KVM, and Open vSwitch on the NetApp HCI compute nodes. Configure storage pools on the hypervisor using Element volumes for a shared storage service for hosts and VMs. For more details on installation and configuration of KVM on RHEL, see the [Red Hat documentation](#). See the [OVS documentation](#) for details on configuring Open vSwitch.
7. RHEL KVM hypervisor’s Open vSwitch cannot be VMM integrated with Cisco ACI. Physical domain and static paths must be configured on all required EPGs to allow the required VLANs on the interfaces connecting the ACI leaf switches and RHEL hosts. Also configure the corresponding OVS bridges on RHEL hosts and configure VMs to use those bridges. The networking functionality for the RHEL KVM hosts in this solution is achieved using Open vSwitch virtual switch.

## Open vSwitch

Open vSwitch is an open-source, enterprise-grade virtual switch platform. It uses virtual network bridges and flow rules to forward packets between hosts. Programming flow rules work differently in OVS than in the standard Linux Bridge. The OVS plugin does not use VLANs to tag traffic. Instead, it programs flow rules on the virtual switches that dictate how traffic should be manipulated before forwarded to the exit interface. Flow rules determine how inbound and outbound traffic should be treated. The following figure depicts the internal networking of Open vSwitch on an RHEL-based KVM host.

# Legend

|  |                |
|--|----------------|
| <span style="color: #00FFFF;">---</span> | ovs-ib-mgmt    |
| <span style="color: #0000FF;">---</span> | ovs-iscsi      |
| <span style="color: #800080;">---</span> | ovs-vm-network |



The following table outlines the necessary parameters and best practices for configuring Cisco ACI and Open vSwitch on RHEL based KVM hosts.

| Resource        | Configuration Considerations  | Best Practices  |
|-----------------|---|---|
| Endpoint groups | <ul style="list-style-type: none"> <li>• Separate EPG for native VLAN</li> <li>• Static binding of interfaces towards HCI storage and compute nodes in native VLAN EPG to be on 802.1P mode</li> <li>• Static binding of vPCs required on in-band management EPG and iSCSI EPG before KVM installation</li> </ul> | <ul style="list-style-type: none"> <li>• Separate VLAN pool for physical domain with static allocation turned on</li> <li>• Contracts between EPGs to be well defined. Allow only required ports for communication.</li> <li>• Use unique native VLAN for discovery during Element cluster formation</li> </ul> |

| Resource         | Configuration Considerations   | Best Practices  |
|------------------|--|---|
| Interface Policy | <ul style="list-style-type: none"> <li>• One vPC policy group per RHEL host</li> <li>• One vPC policy group per NetApp HCI storage node</li> <li>• LLDP enabled, CDP disabled</li> </ul> | <ul style="list-style-type: none"> <li>• NetApp recommends using vPC towards RHV-H hosts</li> <li>• Use LACP Active for the port-channel policy</li> <li>• Use only Graceful Convergence and Symmetric Hashing control bits for port-channel policy</li> <li>• Use Layer4 Src-Port load-balancing hashing method for port-channel policy</li> <li>• NetApp recommends using vPC with LACP Active port-channel policy for interfaces towards NetApp HCI storage nodes</li> </ul> |

Next: [ONTAP on AFF: NetApp HCI and Cisco ACI](#)

## ONTAP on AFF: NetApp HCI and Cisco ACI

NetApp AFF is a robust storage platform that provides low-latency performance, integrated data protection, multiprotocol support, and nondisruptive operations. Powered by NetApp ONTAP data management software, NetApp AFF ensures nondisruptive operations, from maintenance to upgrades to complete replacement of your storage system.

NetApp ONTAP is a powerful storage operating system with capabilities like inline compression, nondisruptive hardware upgrades, and cross-storage import. A NetApp ONTAP cluster provides a unified storage system with simultaneous data access and management of Network File System (NFS), Common Internet File System (CIFS), iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), and NVMe/FC protocols. ONTAP provides robust data protection capabilities, such as NetApp MetroCluster, SnapLock, Snapshot copies, SnapVault, SnapMirror, SyncMirror technologies and more. For more information, see the [ONTAP documentation](#).

To extend the capabilities of storage to file services and add many more data protection abilities, ONTAP can be used in conjunction with NetApp HCI. If NetApp ONTAP already exists in your environment, you can easily integrate it with NetApp HCI and Cisco ACI.

### Workflow

The following high-level workflow was used to set up the environment. Each of these steps might involve several individual tasks.

1. Create a separate bridge domain and EPG on ACI for NFS and/or other protocols with the corresponding subnets. You can use the same HCI-related iSCSI EPGs.
2. Make sure you have proper contracts in place to allow inter-EPG communication for only the required

ports.

3. Configure the interface policy group and selector for interfaces towards AFF controllers. Create a vPC policy group with the LACP Active mode for port-channel policy.

## PC/VPC Interface Policy Group - Storage-AFF-01

Properties

Name: Storage-AFF-01

Description: optional

Link Aggregation Type:

Port Channel

VPC

Link Level Policy:

10G-Auto

CDP Policy:

CDP-Enabled

MCP Policy:

select a value

CoPP Policy:

select a value

LLDP Policy:

LLDP-Enabled

STP Interface Policy:

select a value

Egress Data Plane Policing Policy:

select a value

Ingress Data Plane Policing Policy:

select a value

Priority Flow Control Policy:

select a value

Fibre Channel Interface Policy:

select a value

Slow Drain Policy:

select a value

Port Channel Policy:

LACP-Active

4. Attach both a physical and VMM domain to the EPGs created. Attach the vPC policy as static paths and, in the case of theCisco AVE virtual switch, use Native switching mode when you attach the VMM domain.

VMware/hci-vmware-ave

VMM Domain

On Demand

Immediate

formed

e.g., vlan-1

e.g., vian-1

native

VLAN

Update

Cancel

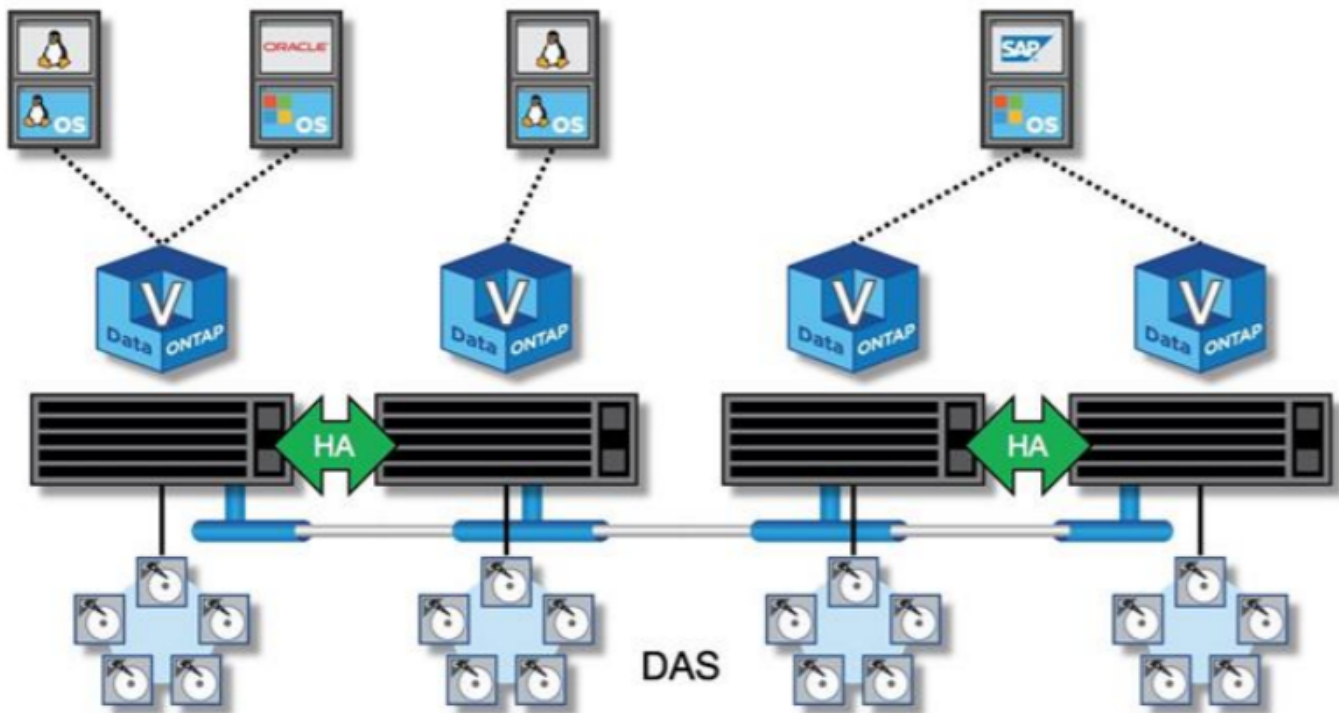
5. Install and configure an ONTAP cluster on the AFF controllers. Then create and configure NFS and/or iSCSI volumes/LUNs. See the [AFF and ONTAP documentation](#) for more information.
6. Create a VMkernel adapter (in the case of VMware ESXi) or a logical interface (in the case of RHV-H and RHEL-KVM hosts) attaching the NFS (or other protocols) port group or logical network.
7. Create additional datastores, storage domains, or storage pools on hypervisors (VMware, RHV, or KVM) using AFF storage.



## ONTAP Select with VMware vSphere: NetApp HCI and Cisco ACI

NetApp ONTAP Select is the NetApp solution for software-defined storage (SDS), bringing enterprise-class storage management features to the software-defined data center. ONTAP Select extends ONTAP functionality to extreme edge use cases including IoT and tactical servers as a software-defined storage appliance that acts as a full storage system. It can run as a simple VM on top of a virtual environment to provide a flexible and scalable storage solution.

Running ONTAP as software on top of another software application allows you to leverage much of the qualification work done by the hypervisor. This capability is critical for helping us to rapidly expand our list of supported platforms. Also, positioning ONTAP as a virtual machine (VM) allows customers to plug into existing management and orchestration frameworks, which allows rapid provisioning and end-to-end automation from deployment to sunsetting. The following figure provides an overview of a four-node ONTAP Select instance.



Deploying ONTAP Select in the environment to use the storage offered by NetApp HCI extends the capabilities of NetApp Element.

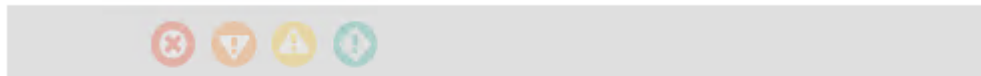
### Workflow

The following workflow was used to set up the environment. In this solution, we deployed a two-node ONTAP Select cluster. Each of these steps might involve several individual tasks.

1. Create an L2 BD and EPG for the OTS cluster's internal communication and attach the VMM domain to the EPG in the Native switching mode (in case of a Cisco AVE virtual switch) with Pre-Provision Resolution Immediacy.



# EPG - HCI-Select-Internal



## Properties

Contract Exception Tag:

QoS class:

Custom QoS:

Data-Plane Policer:

Intra EPG Isolation:

Preferred Group Member:

Flood on Encapsulation:

Configuration Status: applied

Configuration Issues:

Label Match Criteria:

Bridge Domain:

Resolved Bridge Domain: HCI-Infra/SELECT-Internal

Monitoring Policy:

FHS Trust Control Policy:



2. Verify that you have a VMware vSphere license.
3. Create a datastore that hosts OTS.
4. Deploy and configure ONTAP Select according to the [ONTAP Select documentation](#).

### Cluster Details

|                     |                      |                     |                                 |
|---------------------|----------------------|---------------------|---------------------------------|
| Name                | hci-aci-ontap-select | Cluster Size        | 2 node cluster (1 HA Pairs)     |
| ONTAP Image Version | 9.7                  | Licensing           | evaluation                      |
| IPv4 Address        | 172.22.9.81          | Cluster MTU         | 9000                            |
| Netmask             | 255.255.255.0        | Domain Names        | cie.netapp.com                  |
| Gateway             | 172.22.9.1           | Server IP Addresses | 10.61.184.251,<br>10.61.184.252 |
| Mediator Status     | HA Active            | NTP Server          | 10.61.184.48                    |
| Last Refresh        | -                    |                     |                                 |

### Node Details

#### > HA Pair 1

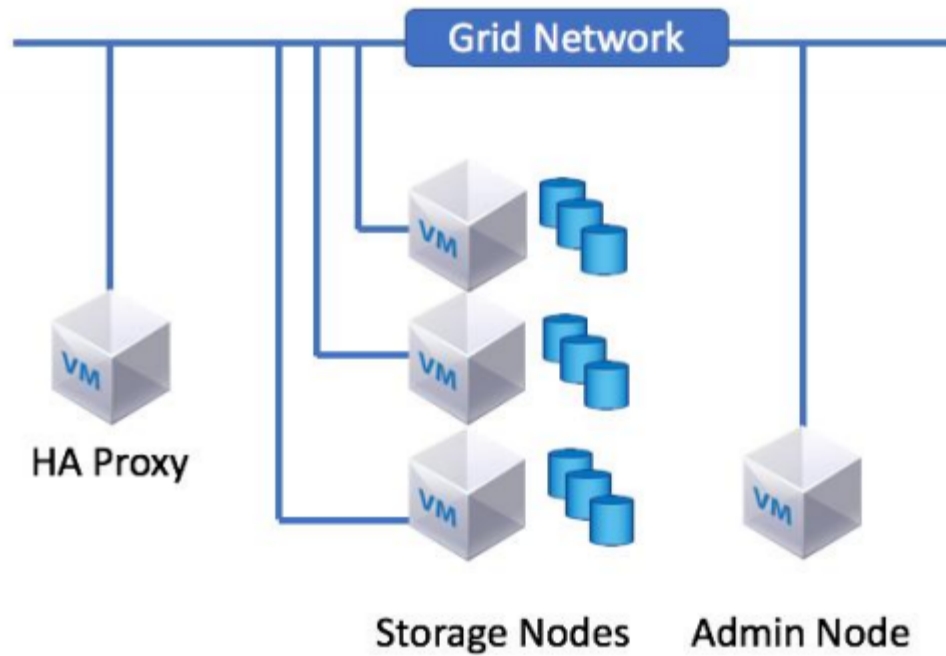
|   |  |   |
|---|--|---|
|  | <b>Node 1</b> hci-aci-ontap-select... — 2 TB + | <b>Host 1</b> 172.22.9.61 — (Small (4 CPU, 16 GB Memory)) |
|  | <b>Node 2</b> hci-aci-ontap-select... — 2 TB + | <b>Host 2</b> 172.22.9.60 — (Small (4 CPU, 16 GB Memory)) |

5. Create additional datastores using ONTAP Select to make use of additional capabilities.

Next: [StorageGRID with VMware vSphere: NetApp HCI and Cisco ACI](#)

## StorageGRID with VMware vSphere: NetApp HCI and Cisco ACI

StorageGRID is a robust software-defined, object-based storage platform that stores and manages unstructured data with a tiered approach along with intelligent policy-driven management. It allows you to manage data while optimizing durability, protection, and performance. StorageGRID can also be deployed as hardware or as an appliance on top of a virtual environment that decouples storage management software from the underlying hardware. StorageGRID opens a new realm of supported storage platforms, increasing flexibility and scalability. StorageGRID platform services are also the foundation for realizing the promise of the hybrid cloud, letting you tier and replicate data to public or other S3-compatible clouds. See the [StorageGRID](#) documentation for more details. The following figure provides an overview of StorageGRID nodes.



## Workflow

The following workflow was used to set up the environment. Each of these steps might involve several individual tasks.

1. Create an L2 BD and EPG for the grid network used for internal communication between the nodes in the StorageGRID system. However, if your network design for StorageGRID consists of multiple grid networks, then create an L3 BD instead of an L2 BD. Attach the VMM domain to the EPG with the Native switching mode (in the case of a Cisco AVE virtual switch) and with Pre-Provision Resolution Immediacy. The corresponding port group is used for the grid network on StorageGRID nodes.

# EPG - GridNetwork

### Properties

|                           |                          |            |
|---------------------------|--------------------------|------------|
| QoS class:                | Unspecified              | ▼          |
| Custom QoS:               | select a value           | ▼          |
| Data-Plane Policer:       | select a value           | ▼          |
| Intra EPG Isolation:      | Enforced                 | Unenforced |
| Preferred Group Member:   | Exclude                  | Include    |
| Flood on Encapsulation:   | Disabled                 | Enabled    |
| Configuration Status:     | applied                  |            |
| Configuration Issues:     |                          |            |
| Label Match Criteria:     | AtleastOne               | ▼          |
| Bridge Domain:            | GridNetwork-BD           | ▼          |
| Resolved Bridge Domain:   | HCI-Infra/GridNetwork-BD |            |
| Monitoring Policy:        | select a value           | ▼          |
| FHS Trust Control Policy: | select a value           | ▼          |
| EPG Contract Master:      |                          |            |

2. Create a datastore to host the StorageGRID nodes.
3. Deploy and configure StorageGRID. For more details on installation and configuration, see the [StorageGRID documentation](#). If the environment already has ONTAP or ONTAP Select, then you can use the NetApp Fabric Pool feature. Fabric Pool is an automated storage tiering feature in which active data resides on local high-performance solid-state drives (SSDs) and inactive data is tiered to low-cost object storage. It was first made available in NetApp ONTAP 9.2. For more information on Fabric Pool, see the documentation [here](#).

[Next: Validation Results](#)

## Copyright Information

Copyright © 2021 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.