v2.3 | May 2022 | BP-2052

BEST PRACTICES

Cisco ACI with Nutanix

NUTANIX
YOUR ENTERPRISE CLOUD

Copyright

Contents

1. Executive Summary

Cisco Application Centric Infrastructure (ACI)™ empowers your applications by automatically translating application requirements into infrastructure configuration. Combining the power of software-defined networking (SDN) via Cisco ACI with the Nutanix Cloud Platform allows you to build a datacenter that performs well and is easy to manage and scale, freeing IT to focus on the applications instead of the infrastructure.

Cisco ACI defines your desired network state using GUI or API-driven policy. This policy-based approach to SDN enables the network to scale beyond the limits of an imperative, controller-oriented model. ACI integrates intelligent control of hardware switches in a leaf-spine topology with management and automation for software virtual switches. Using this policy framework, ACI delivers tenant isolation, microsegmentation, automation, programmability, ease of management, and deep network visibility.

Nutanix has performed functional testing and validation with multiple hypervisors and virtual switches in a Cisco ACI environment. Based on this testing process, Nutanix has developed recommendations for deploying Nutanix in a Cisco ACI environment to achieve maximum performance and reliability. Refer to the best practices checklist in the appendix for a summary of these recommendations.

Document Version History

Version Number	Published	Notes
1.0	September 2016	Original publication.
2.0	August 2019	Major technical updates throughout.
2.1	September 2019	Removed static-channel mode because it's not compatible with LCM or Foundation.

Version Number	Published	Notes
2.2	April 2021	Updated the Nutanix overview and the General ACI Best Practices for Nutanix section.
2.3	May 2022	Added proxy ARP warning.

Trademark Disclaimer

2. Cisco ACI Overview

Cisco Application Centric Infrastructure (ACI) is an application-centered networking fabric that can provision and enforce application policies in both physical and virtual switches. The ACI fabric consists of physical Cisco Nexus 9000 series switches running in ACI mode and a cluster of at least three centrally managed Application Policy Infrastructure Controller (APIC) servers. Cisco ACI uses a declarative policy model, which allows you to configure policy centrally in the APIC cluster; the APIC cluster then pushes the policy out to all leaf and spine switches in the fabric. ACI can also integrate with VMware vCenter to manage and configure the vSphere Distributed Switch (VDS) and provide microsegmentation using the Cisco ACI Virtual Edge (AVE).

Most importantly, ACI implements an allowlist policy model, which means that it allows no traffic by default. Administrators create contracts to explicitly define traffic allowed between endpoint groups (EPGs). EPGs contain endpoints that require similar treatment on the network. When you apply a contract between EPGs, only traffic specified in the contract is allowed on the fabric. For more details on Cisco ACI policy and architecture, read the Cisco ACI Design Guide.

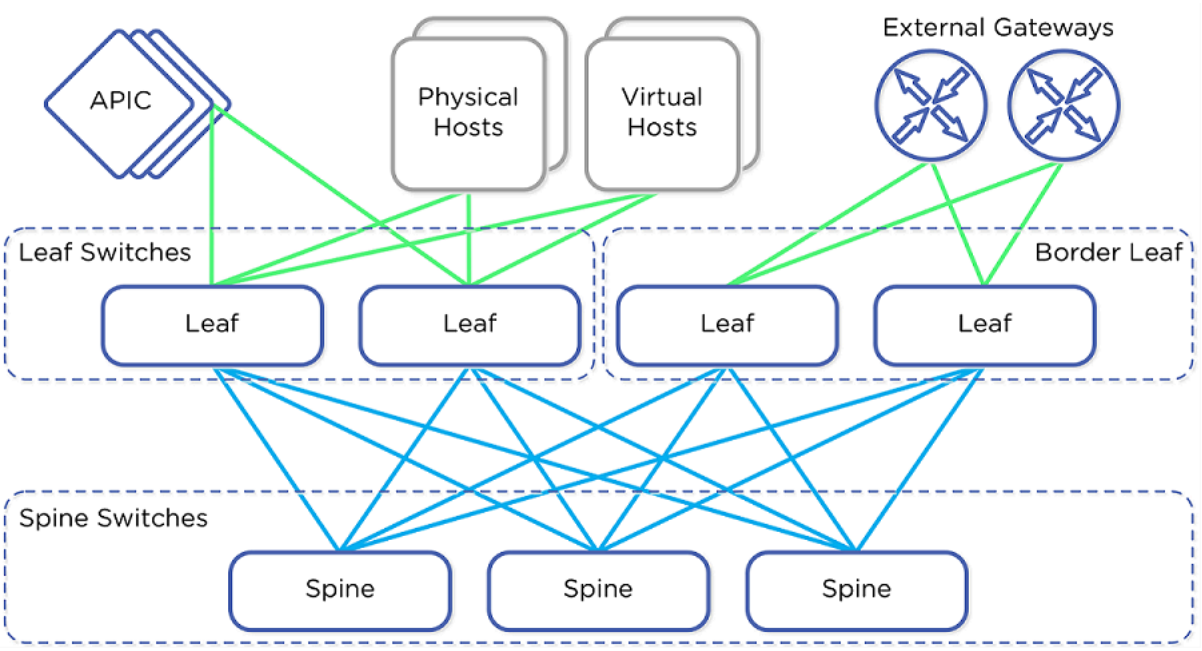

Figure 1: Cisco ACI Component Overview

Leaf-Spine Architecture and Encapsulation

ACI enforces a true leaf-spine design and automatically detects switches in either the leaf or spine position. Connections between leaf switches aren't allowed, nor are connections between spines. In this type of architecture, also referred to as a Clos network, every leaf connects directly to every spine. All hosts, devices, switches, and routers connect to the leaf layer. The spine layer serves as a high-speed transit backbone for the leaf switches. In a single-pod deployment, only the leaves can connect to the spines.

In the ACI fabric, traffic is encapsulated on leaf entry and routed through the most efficient path to the destination leaf, where it's decapsulated. From a packet's perspective, the entire ACI fabric acts as one switch, and the packet looks the same on egress as it did on ingress. The protocols used in the fabric are locally significant—they aren't visible when a packet leaves the fabric.

Cisco ACI Virtual Edge

Cisco ACI Virtual Edge (AVE) provides microsegmentation and network visibility inside supported hypervisors with a VM-based solution. With ESXi, AVE runs on top of the distributed vSwitch and intercepts all VM traffic for selected EPGs. AVE enforces Cisco ACI policy at the hypervisor level.

Use Cases and Automation

Cisco ACI enables an application-centric policy-based approach, automation, ease of management, multitenancy, network isolation, and microsegmentation in the datacenter. Administrators control the entire ACI fabric through the APIC using either a GUI or an open, RESTful API. You don't need to configure individual physical switches manually, and you can provision new switches automatically as you add them. The fabric abstraction and encapsulation layers can implement a multitenant policy defined in the APIC rapidly in the physical network. Coupled with hypervisor VMM integration, network policies in the fabric can apply at the virtual switch level as well.

3. Cisco ACI Test Methodology and Results

Nutanix has successfully validated compatibility with a Cisco ACI leaf-spine architecture using the following network topology and components.

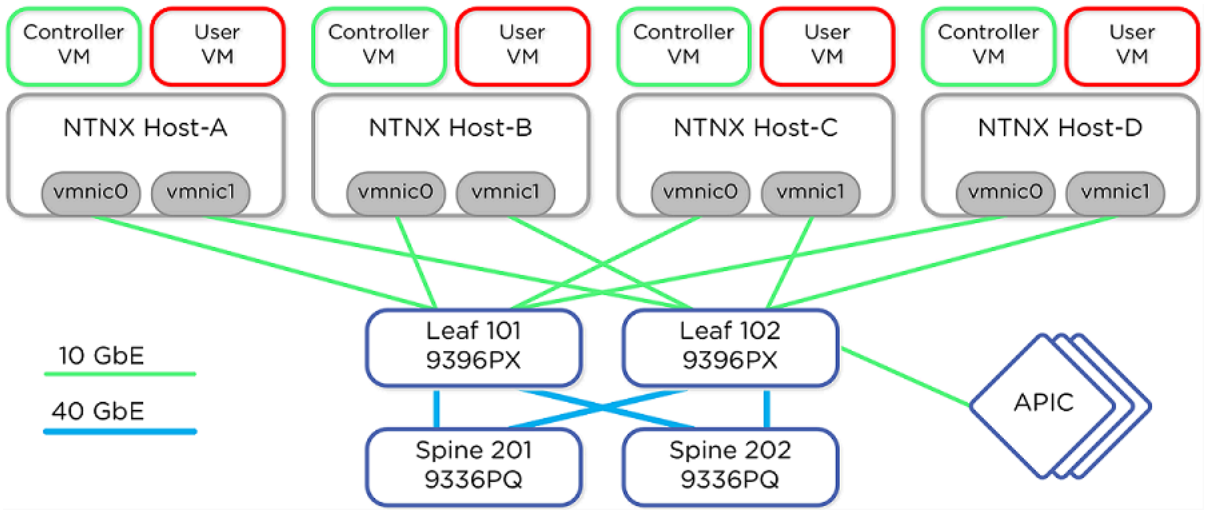

Figure 2: Cisco ACI Network Test Topology

Each of the four Nutanix hosts connects to two Cisco Nexus leaf switches in ACI mode. Two Cisco Nexus switches form the spine of the Cisco ACI fabric. Three Cisco APICs connect to the leaf switches to manage the ACI fabric. The Nutanix CVM and a Linux user VM run on each hypervisor node.

We used the following combinations of hypervisors and virtual switches to verify functionality and compatibility in the most common scenarios.

Table: Hypervisor and Virtual Switch Combinations Used in Nutanix Testing with Cisco ACI

Hypervisor	Virtual Switch	Description
Nutanix AHV	Open vSwitch (OVS)	Open vSwitch bundled with AHV

Hypervisor	Virtual Switch	Description
VMware ESXi	vSphere Standard Switch (VSS)	Default standard switch
VMware ESXi	vSphere Distributed Switch (VDS)	Distributed switch managed by vSphere

In each hypervisor and virtual switch scenario, we performed the following tests:

- Generated line-rate network load between CVMs.
  - Used the iPerf tool to validate network connectivity and throughput between all Nutanix CVMs. High bandwidth and low-latency networking are critical for optimal performance. The test systems should achieve network throughput within 10 percent of the theoretical line-rate maximum.
- Generated storage I/O load simultaneously on all nodes.
  - Used the Nutanix diagnostics.py tool to generate read and write I/O on all nodes simultaneously to verify synthetic storage workload performance. The test system should achieve storage throughput numbers within 10 percent variance of Nutanix internal test results for identical server hardware.
- Verified CVM autopath recovery during CVM unavailability.
  - During CVM unavailability due to a manual restart, user VM functionality and I/O should continue normally without errors.
- Verified EPG separation between user VMs and CVMs.
  - A Cisco ACI contract configured between the CVM and user VM EPGs should allow only approved management traffic from the user VM to the CVM and hypervisor hosts. The CVM and hypervisor hosts should be able to communicate on all open ports in the same EPG. Our testing found that each test and hypervisor-vSwitch combination successfully met all criteria, as summarized in the following table. The following sections describe the best practices that we implemented to achieve these results.

Table: Test Results

Test Combination	iPerf	Storage I/O	Autopath Recovery	Contract Separation
AHV and OVS	Pass	Pass	Pass	Pass
ESXi and VSS	Pass	Pass	Pass	Pass
ESXi and VDS	Pass	Pass	Pass	Pass

4. General ACI Best Practices for Nutanix

Nutanix has developed the following general best practices for deploying in a Cisco ACI environment. For recommendations specific to your hypervisor and virtual switch, see the corresponding sections.

Physical Connections

Connect each Nutanix node directly to at least two ACI leaf switches for load balancing and fault tolerance. We recommend establishing a direct connection to the ACI leaf, without any intermediate switches, to guarantee maximum throughput and minimal latency between nodes. We performed the interoperability tests described here with direct connections to the leaf. Topologies with intermediate switches are allowed, but ensure line-rate, nonblocking connectivity for east-west traffic between Nutanix nodes in the same cluster with a maximum of three switch hops.

Bridge Domains

In the Cisco ACI bridge domain dedicated to the Nutanix server hypervisors and CVMs, configure the following settings to allow Nutanix node discovery and addition:

- L3 unknown multicast flooding: flood
- Multidestination flooding: flood in BD
- ARP flooding: enabled
- GARP-based detection: enabled

Without these settings, automated Nutanix node discovery and addition may fail and you must add new Nutanix nodes to the cluster directly by IPv4 address using the command line.

Endpoint Groups and Contracts

Use Cisco ACI EPGs as a policy enforcement tool. Contracts between EPGs explicitly allow traffic to flow from one EPG to another. No traffic is allowed until you apply contracts between EPGs. Nutanix recommends placing all CVMs and hypervisor hosts in a single Nutanix cluster in the same EPG to ensure full network connectivity and functionality and low storage latency and to allow storage communication between nodes in the Nutanix cluster.

Nutanix recommends placing hypervisor hosts and the CVMs in an untagged, or native, VLAN and guest VMs in tagged VLANs. In the CVM and hypervisor EPG, ensure that the port mode is Access (802.1p) to allow this VLAN configuration.

Don't enable proxy ARP inside the Nutanix EPG, as doing so can cause unexpected failure in Nutanix processes that use ARP to determine endpoint availability.

We recommend using contracts that allow only management traffic from other EPGs into the Nutanix EPGs to restrict network-level access to the Nutanix compute and storage infrastructure. Using features that present storage and services for external clients, like Nutanix Volumes and Files, requires more permissive contracts.

If necessary, you can place Nutanix CVMs and hypervisor hosts in different EPGs and separate them using contracts but take care to allow all required ports and protocols between endpoints. Failure to allow all required ports may lead to loss of the storage fabric. Even in separate EPGs, Nutanix hosts and CVMs must still be in the same layer 2 broadcast domain and same layer 3 IP subnet.

Switch Port Channel Configuration: ACI

For individual ports in ACI, map each interface directly into the desired EPG.

If you use a virtual portal channel (vPC), create a vPC policy group that contains the two leaf switches for each Nutanix node in the APIC. Specify the desired port channel policy in each vPC policy group, matching the hypervisor load balancing configuration (Static Channel Mode On or LACP).

Create an interface profile with an interface selector for each pair of uplinks corresponding to a Nutanix node and associate this interface profile with the vPC policy group for the node. Associate these interface profiles with the switch policies for the pair of leaf switches.

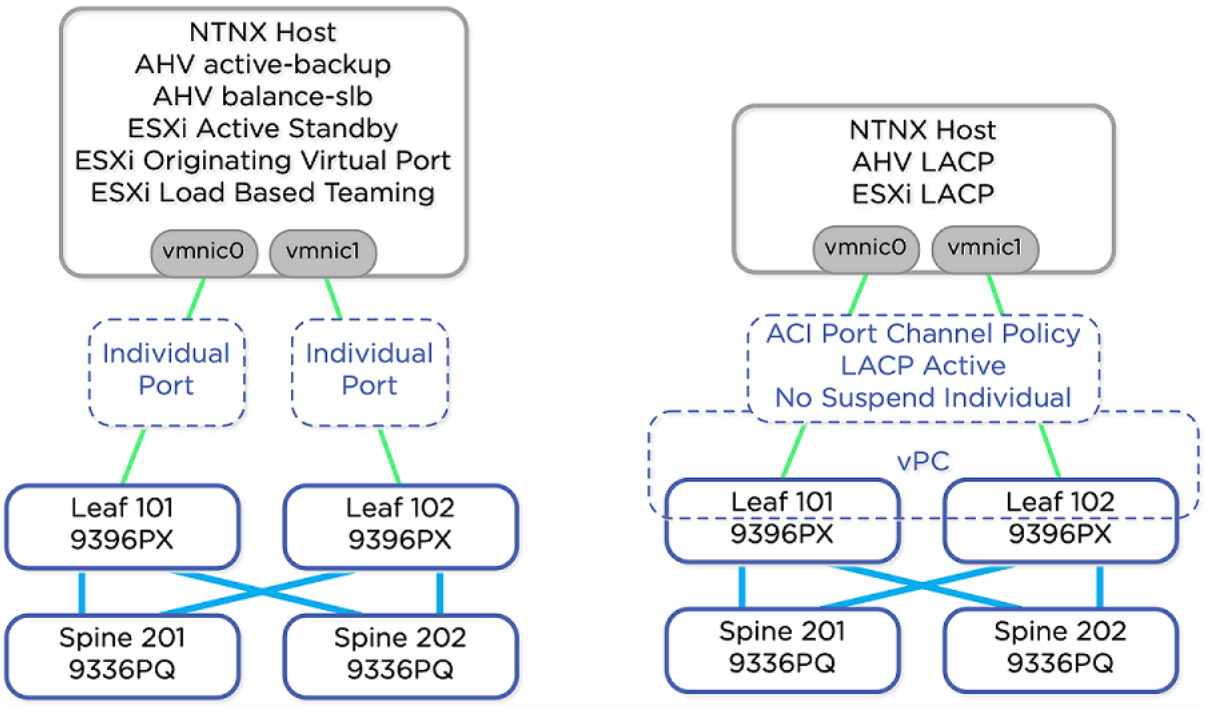

Figure 3: ACI Port Channel Policy Matches Hypervisor Policy

Don't use MAC pinning in Cisco ACI. Cisco has documented a limitation of MAC pinning that can cause traffic disruption during a leaf switch reload.

Switch Port Channel Configuration: VMware ESXi

With VMware ESXi, Nutanix recommends using individual ports for each Nutanix node. Configure each Nutanix node with an active-active load-based teaming uplink configuration to both leaf switches. This configuration aligns with the Nutanix vSphere networking best practice of using the VDS and Route Traffic Based on Physical NIC Load option. For ESXi Active Standby, or Route Based on Originating Virtual Port, use individual ports in ACI as well.

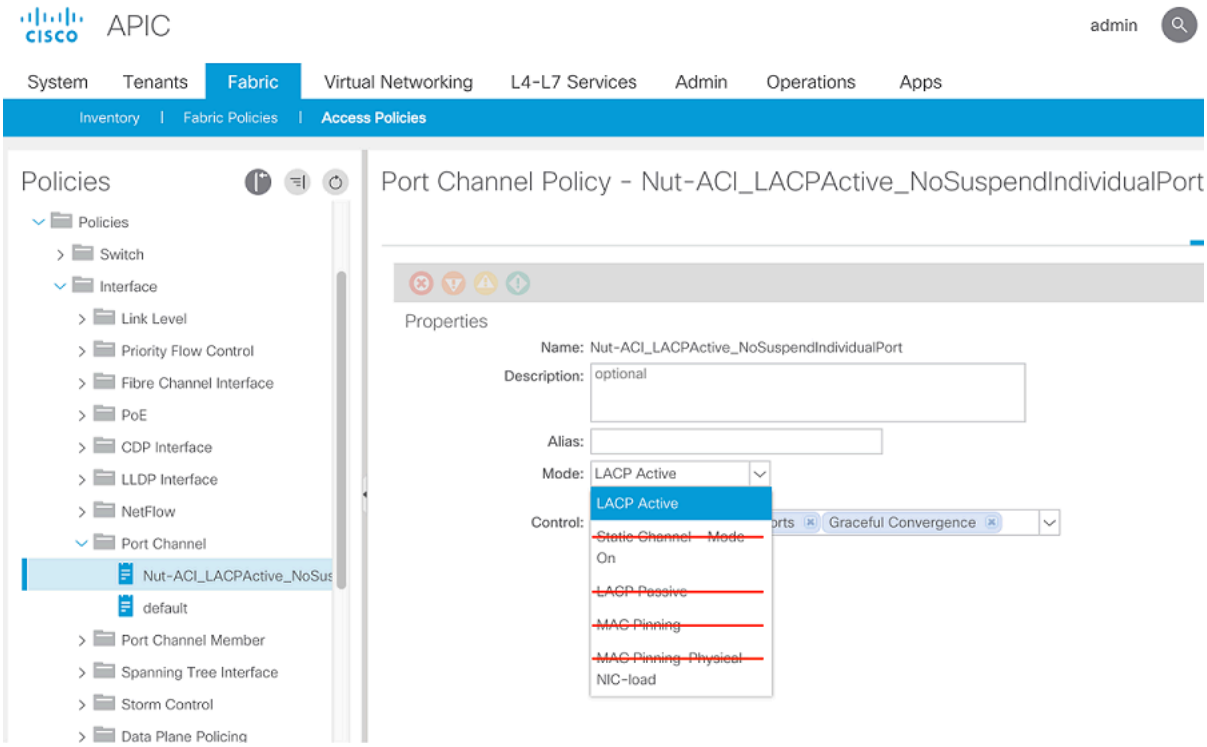

Figure 4: Port Channel Policy MAC Pinning NIC Load

To use LACP with ESXi, change the port channel mode to LACP Active and remove the Suspend Individual control. Nutanix doesn't recommend Static Channel Mode On because it drops traffic during the LCM and Foundation reboot process.

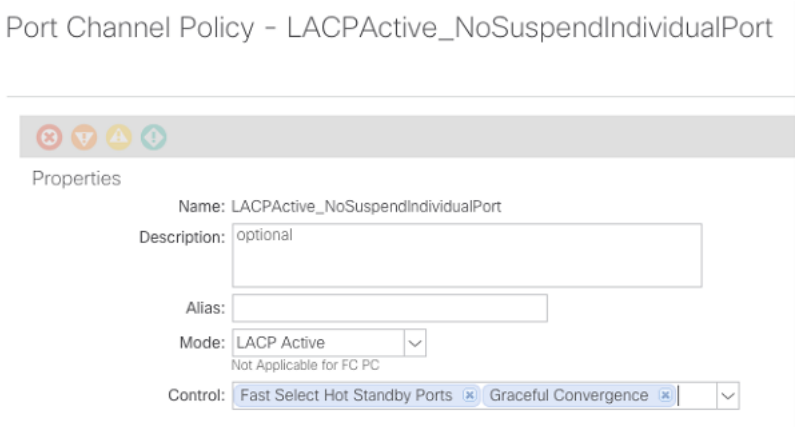

Figure 5: Port Channel Policy LACP Active and No Suspend

Switch Port Channel Configuration: Nutanix AHV

For Nutanix AHV, we recommend ACI individual ports instead of a vPC port channel with the default AHV active-backup configuration. If you want to select active-active on AHV, use LACP in AHV with an LACP Active port channel policy in ACI and remove Suspend Individual from the policy control to allow LACP fallback. Nutanix doesn't recommend using balance-slb because of known limitations with multicast traffic, but you can use ACI individual ports if you must use balance-slb in AHV. For more information, consult the AHV Networking best practices guide.

Default Virtual Switches

Don't alter the default vSwitchNutanix in ESXi or virbr0 in AHV. These internal-only virtual switches contain no external network uplinks and pass traffic between the CVM and the local hypervisor.

5. ACI Best Practices for Nutanix and AHV

With Nutanix AHV, the virtual switch management domain encompasses all nodes and is managed centrally through Prism. The Cisco ACI environment doesn't integrate directly with the Nutanix Open vSwitch (OVS), so administrators must provision nodes the same way they provision bare-metal servers in the APIC, extending VLANs to each node statically with an ACI physical domain.

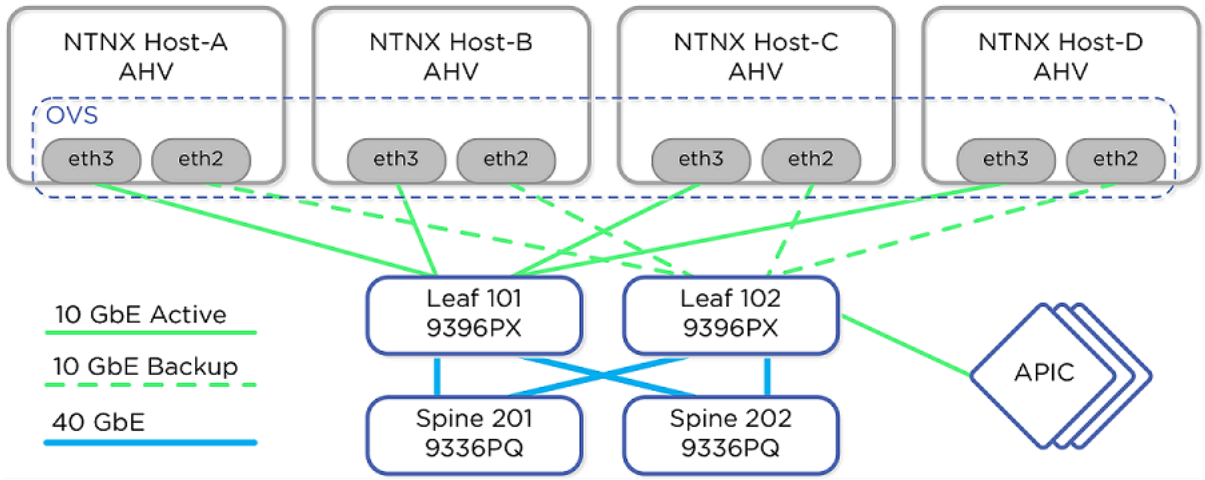

Figure 6: Cisco ACI AHV Test Topology

Configure a physical domain in the APIC that encompasses all the switch ports connected to Nutanix AHV servers and is associated with the required VLAN pools for the hosts, CVMs, and user VMs. Create an attachable entity profile (AEP) with an associated interface policy group and make sure that the AEP contains the physical domain created in the first step. The following figure shows the association between the AEP and the physical domain, performed under the Fabric tab.

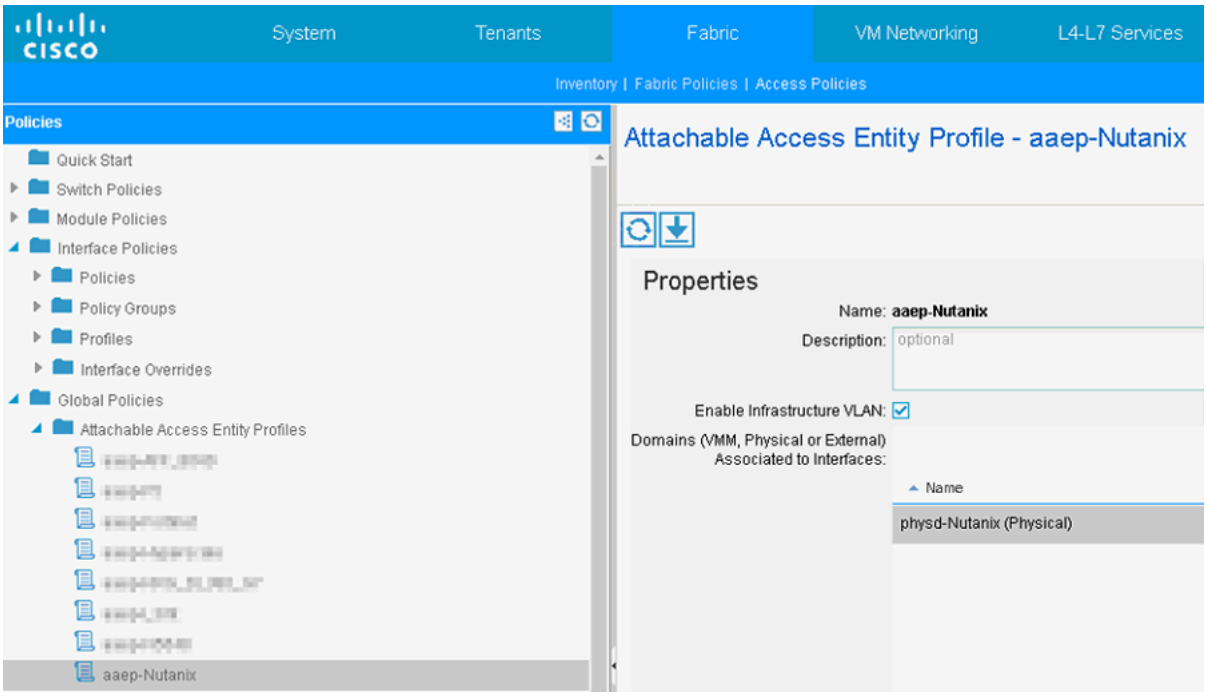

Figure 7: APIC AEP to Domain Mapping

The infrastructure VLAN is optional in the AEP configuration when using AHV.

The following figure shows the static binding (or static port in newer ACI versions) configuration for individual ports, located under the Tenant tab. Create EPG static bindings for each VLAN trunked to the AHV hosts. Here you can see VLAN 3000 on ports 1/37 through 1/40 placed into epg-prod-ib-mgmt, where the AHV hosts and CVMs are connected. The EPG Domains (VMs and Bare-Metal) menu item in this figure contains the physical domain physd-Nutanix, which holds the ports for the Nutanix servers.

Set the port mode for this CVM and hypervisor EPG to Access (802.1p).

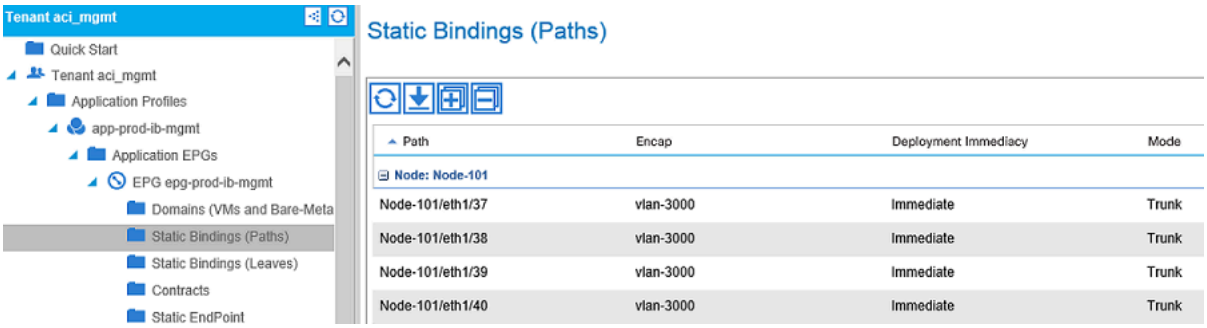

Figure 8: APIC EPG Static Binding

In the Nutanix cluster, keep the AHV OVS bond mode at the default active-backup setting for ease of configuration. In the following example, traffic from the CVM and user VMs flows out from the active adapter eth3 toward Leaf 101. In the event of a failure or link loss, traffic flows out from eth2 toward Leaf 102. Alternatively, if you need the bandwidth from both adapters, use LACP and the balance-tcp bond mode combined with a Cisco ACI LACP Active port channel policy. You can find additional information on AHV bond modes in the AHV Networking best practices guide.

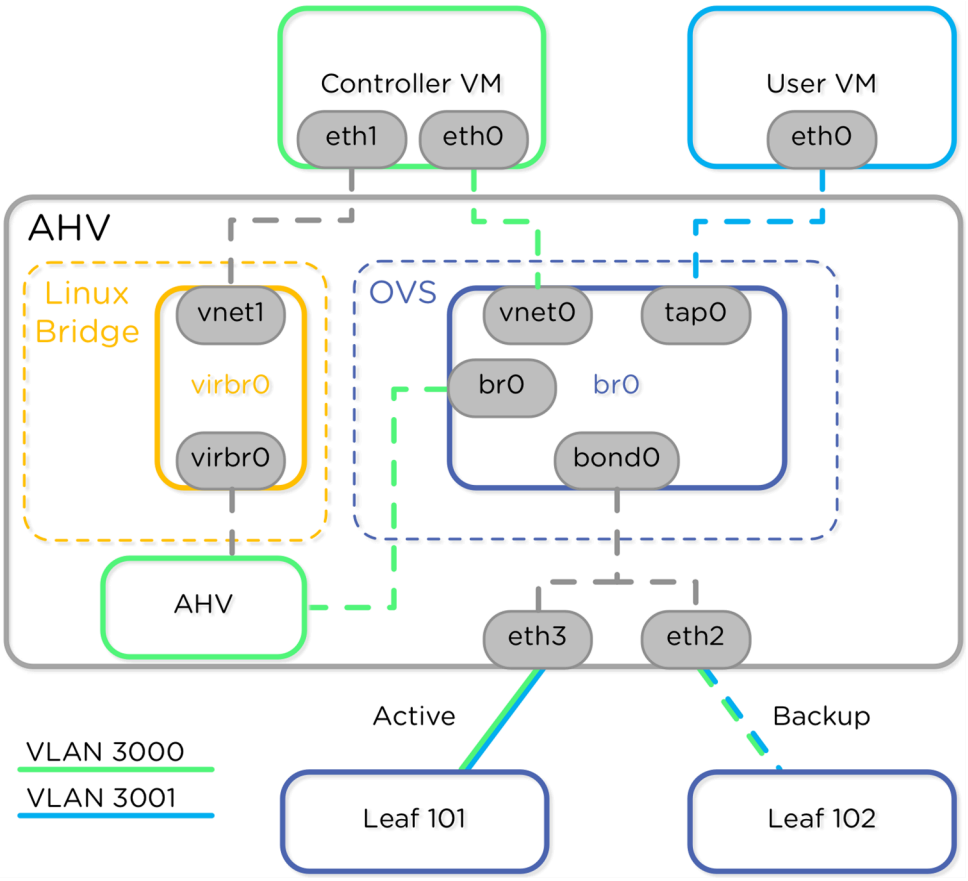

Figure 9: AHV Host Detail

In addition to the CVM and AHV EPG, create EPGs and static bindings for user VM VLANs. In our test example, we created an ACI application profile (app-NTNX-WEB) and an EPG (epg-NTNX-WEB) to separate user VM traffic from the CVM and AHV traffic. User VM traffic used VLAN 3001; CVM and AHV traffic used VLAN 3000.

Create and apply contracts between the user VM EPGs and between the user VM EPGs and the Nutanix EPG to enforce network policies. In our testing scenarios, we created a simple contract named Nutanix for management purposes that allows only SSH, ICMP (ping), and Prism web traffic on port 9440 from the user VM EPG (epg-NTNX-WEB) to the CVM and AHV EPG (epg-prod-ib-management).

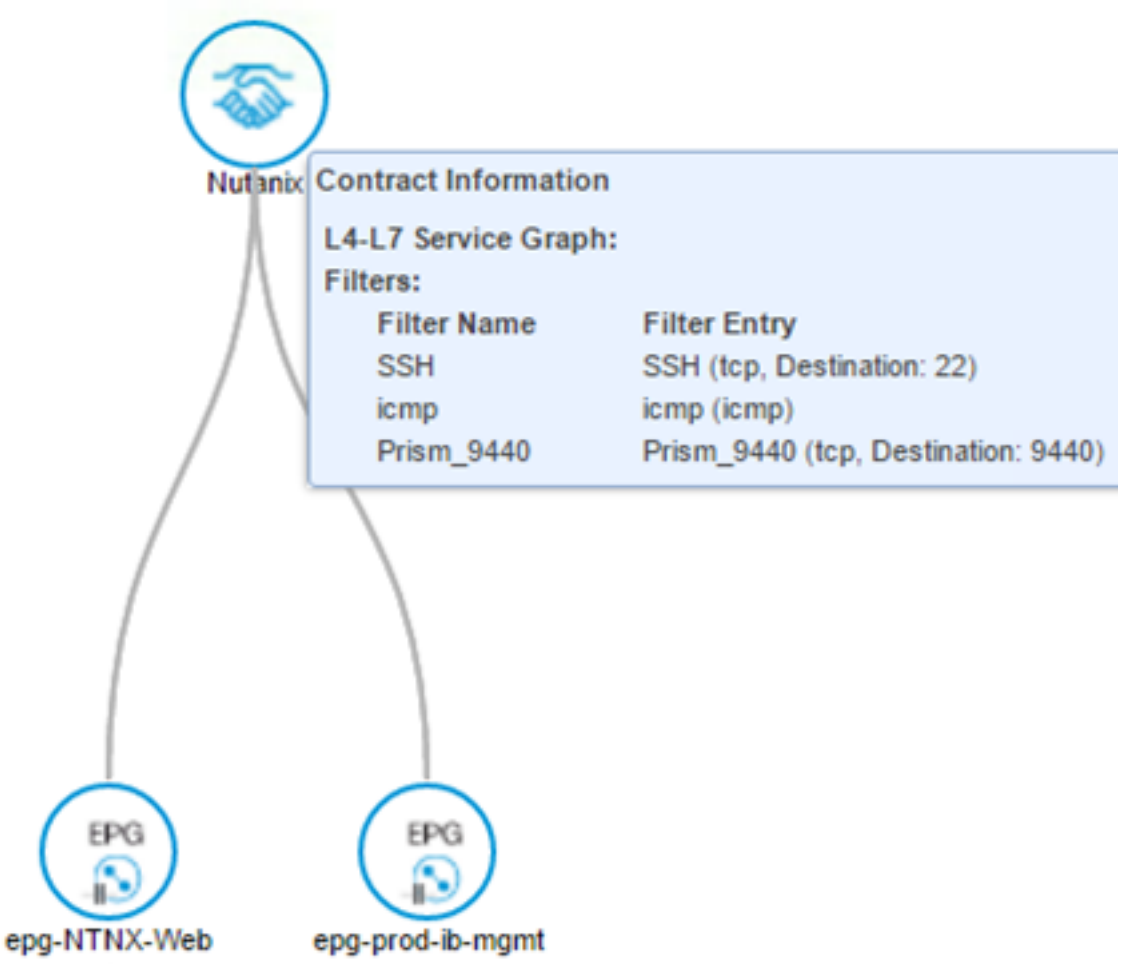

Figure 10: APIC Nutanix Contract Between EPGs

6. ACI Best Practices for Nutanix and ESXi

VMware vSphere allows you to configure multiple types of virtual switches in the hypervisor, so choose the virtual switch that works best for your deployment.

- The VSS is simple to configure for a small number of nodes, but managing it can become more difficult as node count increases. Standard switches are local to each host and must be configured independently of one another, compounding the complexity every time new hosts are added. The VSS is also limited to basic network functionality and doesn't provide Cisco ACI VMM integration.
- The VDS provides additional network functionality, easy management at scale, and integration with the Cisco ACI APIC using VMM domains. VDS requires additional configuration, licensing, and vCenter. The VDS is configured centrally in vCenter, and the configuration is pushed to each participating host.

Nutanix recommends the VDS for its ease of management and load balancing flexibility. The ability to use the Cisco APIC VMM domain out of the box without any extra installation also makes the VDS an appealing choice to unify virtual and physical network administration.

Nutanix has tested these virtual switches in our lab environment and developed the following recommendations.

vSphere Standard Switch

The VSS is installed by default in the ESXi host. The VSS management domain extends only to the individual host as shown in the following image, and you must configure each VSS independently. ACI VMM domain integration requires the VDS, using vCenter as a central configuration point for integration, so the

VSS can't use the VMM domain. Instead, statically bind VLANs to EPGs and use a physical domain and AEP for the Nutanix switch ports in ACI. Use the default Route Based on Originating Virtual Port load balancing method in the virtual switch port groups.

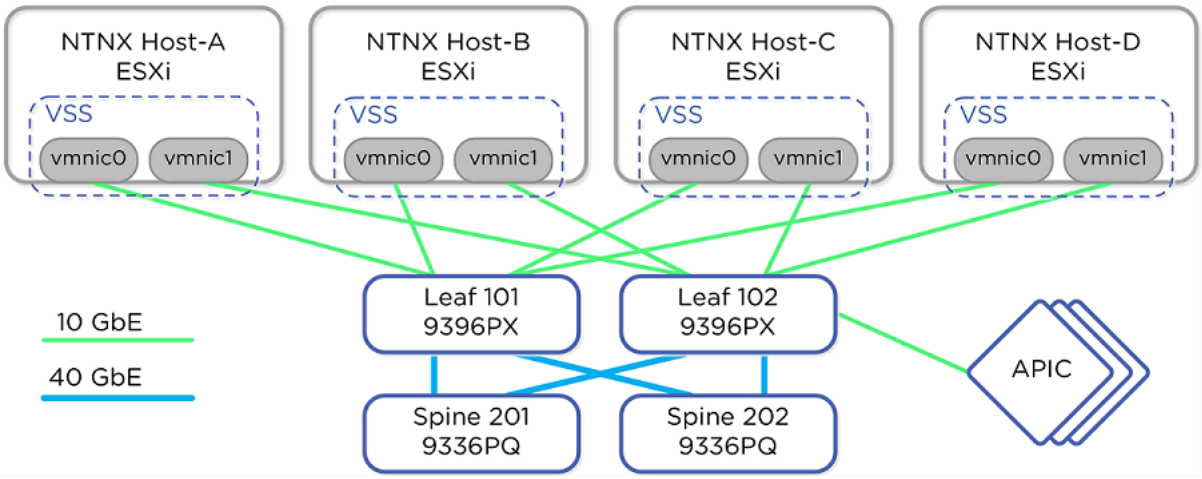

Figure 11: ESXi vSphere Standard Switch Topology

Each Nutanix ESXi host contains two virtual switches: the standard vSwitchNutanix for internal control traffic and the default vSwitch0 for the 10 GbE CVM and user VM traffic. In our testing we added a third switch, vSwitchMgmt, for dedicated 1 GbE management connections. The third vSwitch is optional; choose this design if you want to separate management traffic onto a different uplink NIC team. The following diagram illustrates the internal host layout as tested.

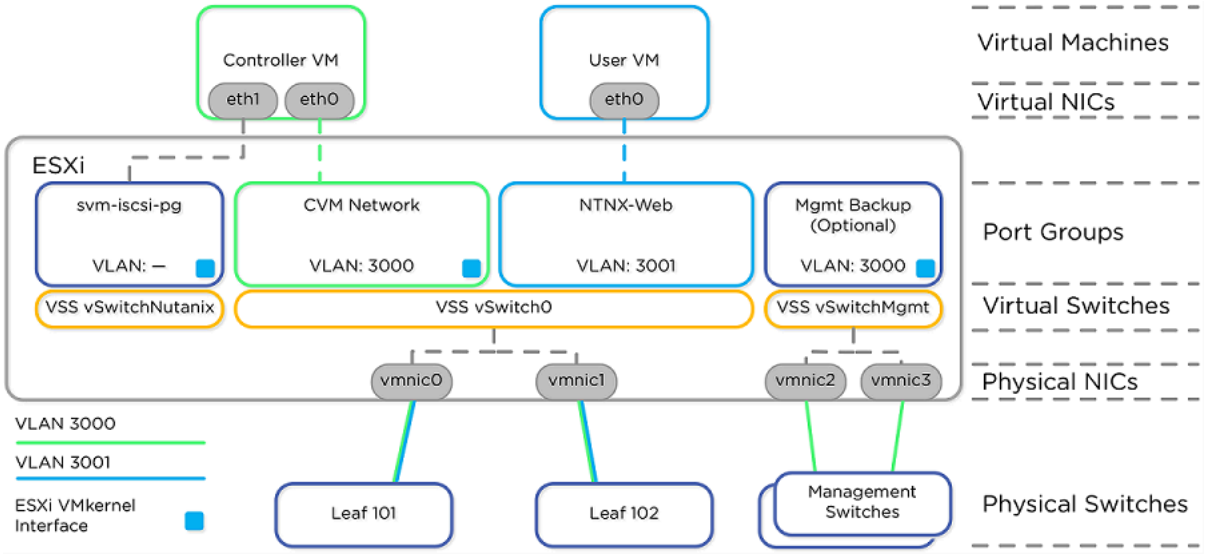

Figure 12: ESXi vSphere Standard Switch Host Detail

vSphere Distributed Switch

The VDS requires additional configuration, licensing, and vCenter, but it also stretches the management domain among multiple hosts. This means that vCenter centrally manages virtual switch configuration for all hosts, rather than configuring each host individually. The VDS also supports ACI VMM domain integration, allowing the APIC to push policies down to the ESXi host VDS using vCenter. Using the VMM integration is optional with the VDS, and the other recommendations in this section still apply even without VMM integration.

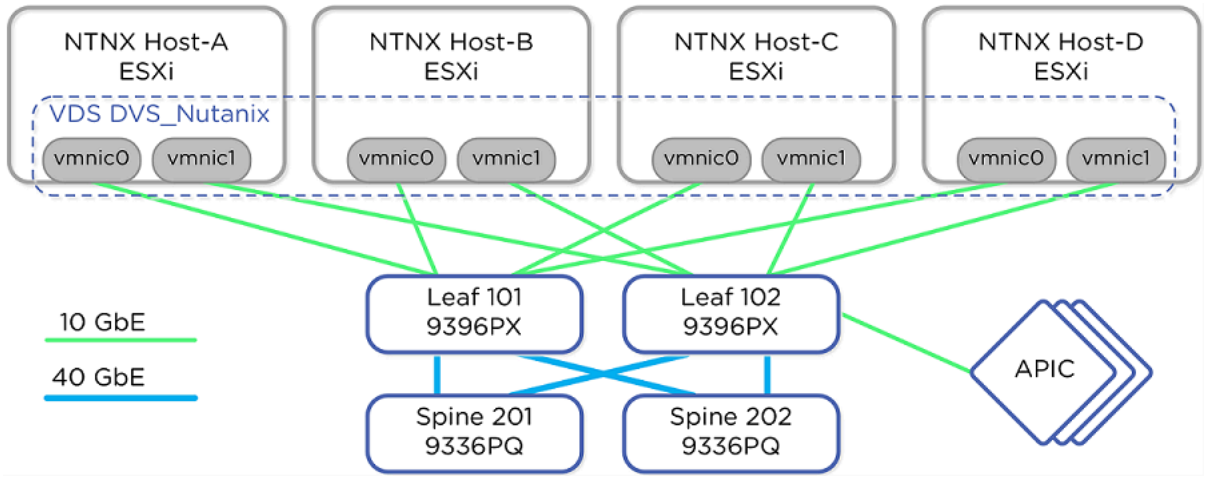

Figure 13: ESXi vSphere Distributed Switch Topology

Using the VMware VDS VMM domain integration, ACI automatically provisions the EPGs created in the APIC in the virtual switch as port groups in vCenter. The APIC configures the port group from the dynamic or static VLAN pool associated with the VMM domain. With dynamic pools, the APIC selects an available VLAN to assign to the EPG. With a static pool, the admin selects the specific VLAN when selecting the VMM domain in the EPG.

When you use a VMM domain, you don't need to have a physical domain with static EPG port bindings. Instead, when you create the VMM domain, associate it with the AEP as shown in the following figure.

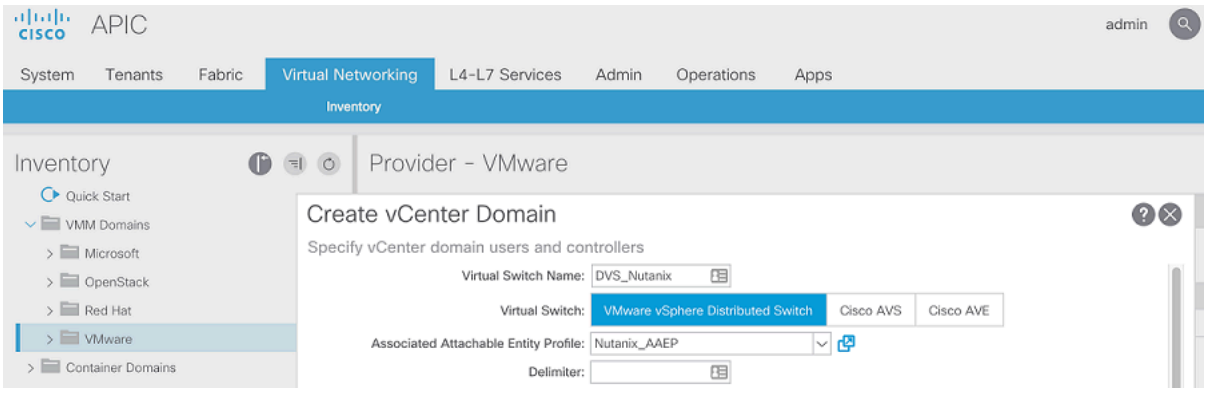

Figure 14: VMM Domain Creation and AEP Mapping

In our example, we created two EPGs—epg-ib-mgmt and epg-NTNX-Web—tied to the VMM domain. The EPG epg-ib-mgmt represents the CVMs and

hypervisors, while epg-NTNX-Web represents the user VMs in the tests. These EPGs in ACI create port groups in vCenter with names based on the combination of ACI tenant, application, and EPG. The following figure shows how the application profile ties together the VMM domain and EPG for epg-NTNX-Web.

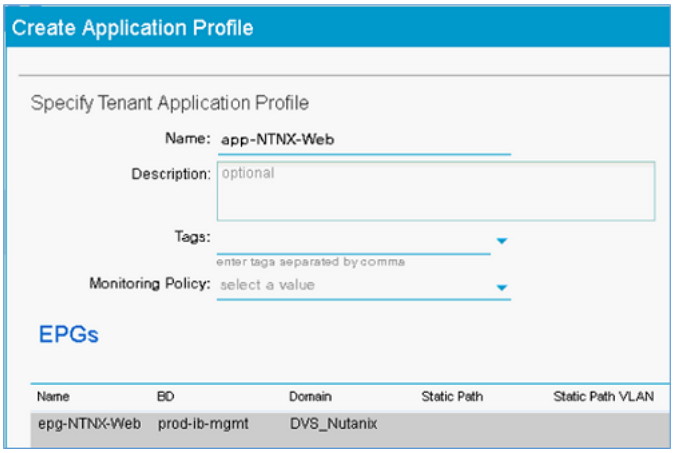

Figure 15: Application Profile to EPG and Domain Mapping

The following figure has port groups named aci_mgmt|app-prod-ib-mgmt|epg-ib-mgmt and aci_mgmt|app-NTNX-Web|epg-NTNX-Web that the APIC automatically configured on the VDS. Each EPG has its own port group.

The VDS in each hypervisor host is configured as shown in the following diagram.

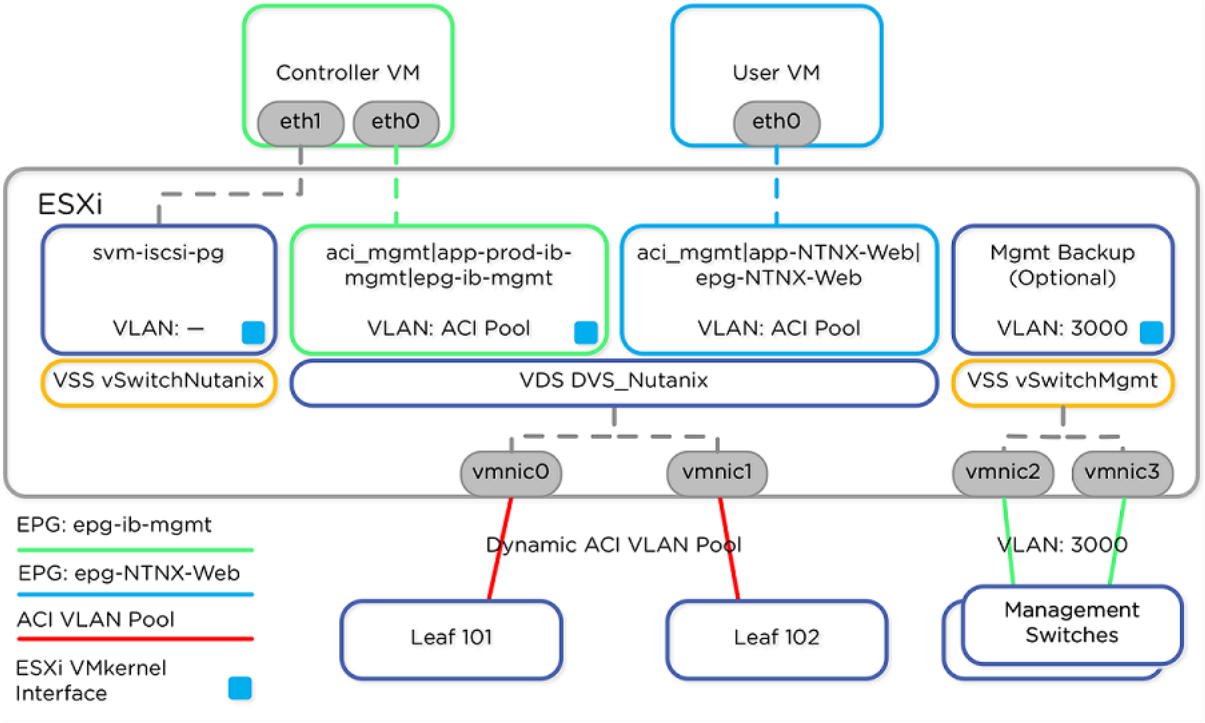

Figure 16: ESXi vSphere Distributed Switch Host Detail

If you choose to migrate from the VSS to the VDS, follow Nutanix KB 1037. Ensure that the internal CVM adapter remains in the port group svm-iscsi-pg by selecting Do not migrate for the adapter. This setting ensures that the adapter remains in the default vSwitchNutanix. This step can be easy to overlook when using the vSphere migration wizard, as shown in the following figure.

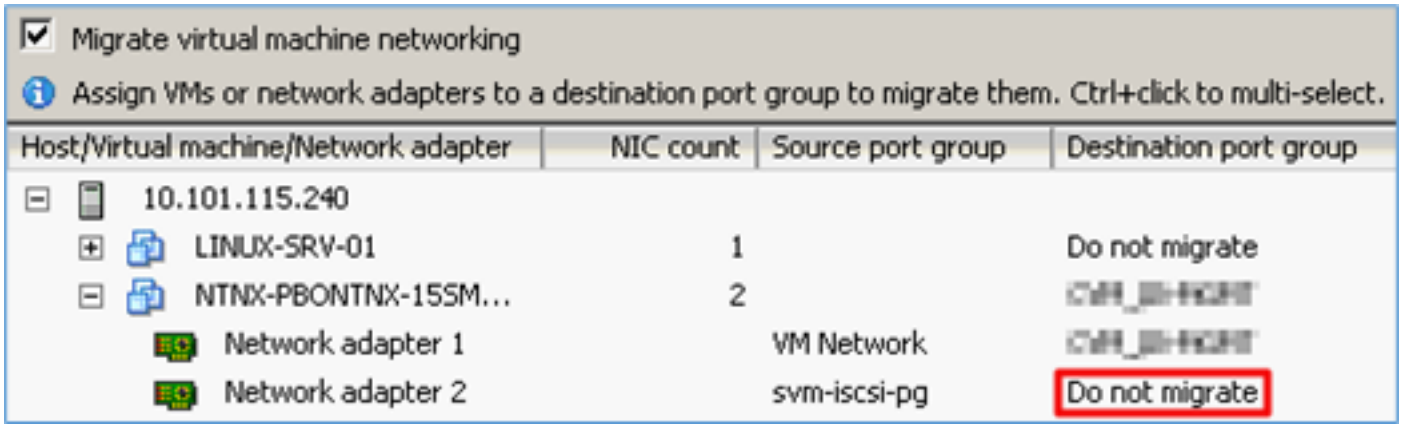

Figure 17: Do Not Migrate svm-iscsi-pg Adapter

To avoid disconnecting any nodes in the cluster, ensure that you're only migrating one physical adapter at a time from the VSS to the VDS. Place the CVM and primary VMkernel adapter in the same EPG (epg-ib-mgmt in our example) by assigning them to the same port group in vCenter. Connect user VMs to port group EPGs, such as epg-NTNX-Web. Optionally, use a second VMkernel adapter created in a VSS (vSwitchMgmt in our example) to provide a backup connection to the ESXi host while migrating to the VDS. The virtual switch port groups that the APIC creates should follow the Nutanix VDS best practice of using Route Based on Physical NIC Load for load balancing.

Two-Uplink Configuration

The previous diagram shows a four-uplink configuration, with a second pair of uplink adapters used as a management backup in case of communication failures on the ACI-controlled VDS. If you don't have or want four adapters, you can build a two-uplink configuration using Cisco ACI preprovision resolution immediacy for the EPG containing the ESXi VMkernel port and CVM. The preprovision option causes the ACI fabric to statically provision the VLAN for the Nutanix CVM and ESXi host on the leaf switch ports where the AEP is associated. Using the preprovision option on the EPG avoids the chicken-and-egg scenario that occurs when ACI waits to hear from vCenter to provision the port but the host can't talk to vCenter until ACI provisions the port.

Cisco ACI Virtual Edge

The AVE is a user space VM that runs on top of the VDS as shown in the previous examples. Traffic between VMs is directed through the AVE with a pool of PVLANs (private VLANs) and the APIC controls the AVE using OpFlex.

Nutanix recommends that the VMM domain use local switching mode for AVE deployments. This switching mode keeps traffic local to the ESXi host for policy enforcement when possible, instead of hairpinning traffic to the leaf switch. Nutanix also recommends bypassing the AVE for the CVM and the VMkernel EPGs by configuring the switching mode as Native. Consult Cisco documentation for configuration of items not discussed here.

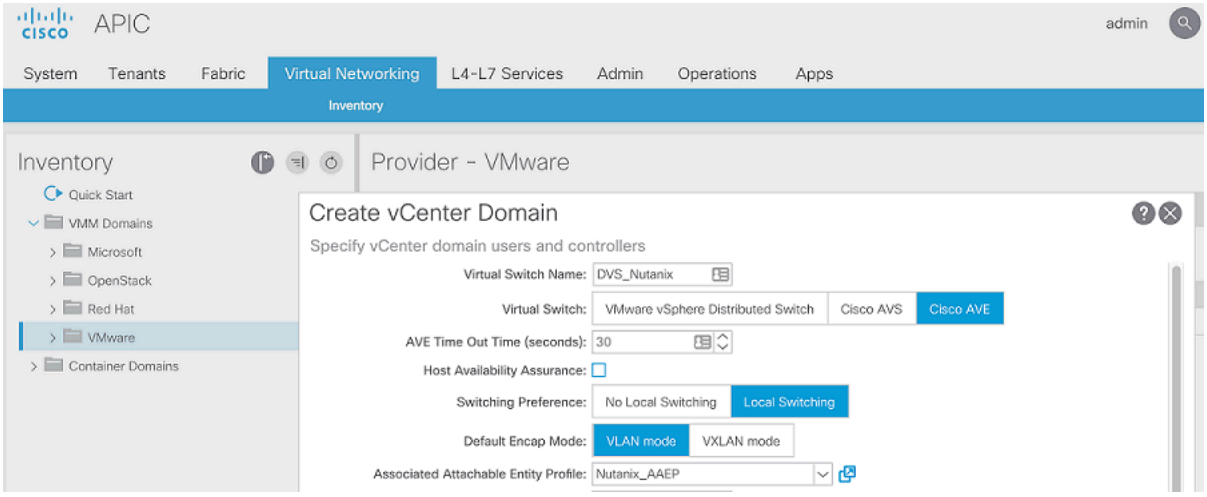

Figure 18: ACI VMM Domain for AVE

As shown in the following diagram, each ESXi host configured with Cisco AVE looks similar to the configuration with the VDS. Traffic for the AVE switching mode port groups is passed through the AVE using host internal PVLANs.

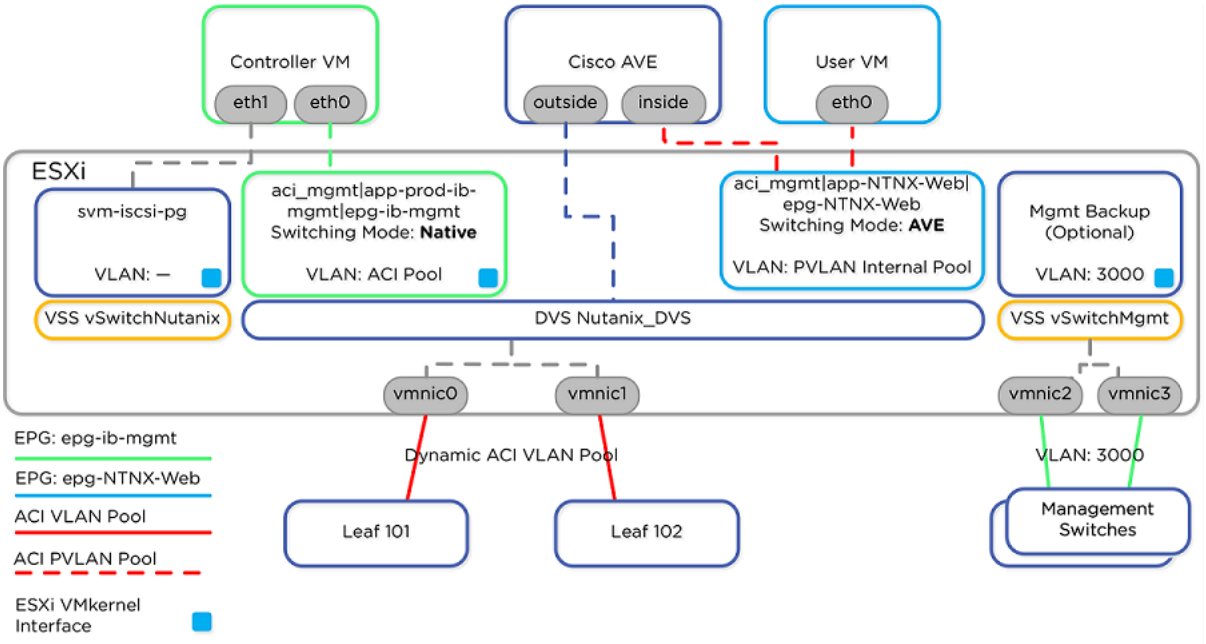

Figure 19: Cisco Application Virtual Switch ESXi Host Detail

The CVM and VMkernel adapter for ESXi should share the same EPG (epg-ib-mgmt in our test) set to Native switching mode. Place user VMs into additional EPGs (such as our test's NTNX-Web) and set the switching mode to AVE. Through the VMM integration, the APIC creates each EPG as a port group using vCenter. AVE encapsulates traffic between the host and the leaf switch and automates VLAN configuration, so no VLAN configuration is needed in vCenter, further simplifying configuration.

The four physical NIC configuration is optional with AVE, so you can use a two-port configuration if you want.

Microsegmentation with Cisco AVE

Nutanix no longer recommends using the Cisco AVS and instead recommends Cisco AVE for hypervisor microsegmentation for Cisco ACI environments on ESXi. You can only use Cisco AVE with Nutanix AOS on VMware ESXi, not on Nutanix AHV.

If desired, use microsegmented EPGs and contracts for user VMs running on the Nutanix cluster. When using AVE, Nutanix recommends setting the switching mode to Native in Cisco ACI for the EPG containing the storage VMkernel adapter and the CVM.

If required, you can also use microsegmented EPGs (in AVE mode) for the Nutanix CVMs and hypervisor hosts, but take care to allow required traffic between CVMs and hosts. Consult the Network Requirements section of the Nutanix Field Installation Guide for the required ports and protocols.

> Note: If Cisco AVE delays or fails to forward traffic, storage fabric reliability problems or increased storage write latency can occur.

7. Conclusion

Running the Cisco ACI network fabric with Nutanix creates a compute and storage infrastructure that puts applications first. Whether you're using the native Nutanix hypervisor, AHV, with the default Open vSwitch, or ESXi with the vSphere Standard Switch or vSphere Distributed Switch, Cisco ACI provides a high-performance, easy-to-manage, and scalable leaf-spine architecture for building a web-scale Nutanix Cloud Platform. Based on our extensive testing of these configurations, we provide a best practices checklist in the appendix.

Nutanix eliminates the need to focus on storage and compute infrastructure configuration by providing an invisible cluster of resources to applications. Similarly, the Cisco ACI fabric simplifies network setup using policy attuned to application requirements to automate individual switch configuration. In addition to physical network and L4–7 device automation, the ACI hypervisor integration extends the network fabric into the virtual switch, allowing administrators to stop provisioning VLANs manually on each node and leaf and surpass the existing 4,000 VLAN limit for building security zones.

For feedback or questions, contact us using the Nutanix NEXT Community forums.

8. Appendix

Best Practices Checklist

General

- Connect each physical host directly to two ACI leaf switches.
- Place the Nutanix CVMs and hypervisor hosts in the same ACI EPG to allow full communication between nodes in the same Nutanix cluster.
- If using separate EPGs for the CVM and hypervisor or a microsegmented Nutanix EPG, ensure that all ports are open for communication between CVMs and hosts.
- Use ACI contracts between the Nutanix EPG and other EPGs to restrict management access.
- Use the following bridge domain settings to allow Nutanix cluster expansion and node addition:
  - L3 unknown multicast flooding: flood
  - Multidestination flooding: flood in BD
  - ARP flooding: enabled
  - GARP-based detection: enabled
- Set the EPG port type to Access (802.1p) to allow CVMs and hypervisors to use the untagged VLAN.
  - Don’t enable proxy ARP inside the Nutanix EPG.

AHV

- Use an ACI physical domain and static bindings to map EPGs and VLANs to Nutanix AHV node network ports. Create one EPG for the AHV host and CVM. Create additional EPGs for each AHV user VM network.

- Use the default active-backup bond mode unless you need the bandwidth of multiple network adapters.
  - Use individual ports with a static binding and don't use a port channel policy for active-backup.
- Use balance-tcp with LACP if you need active-active adapters.
  - Use an LACP-Active port channel policy within the ACI vPC policy for active-active.
  - Remove the Suspend Individual configuration from the port channel policy to enable LACP fallback.
- Don't alter the default virbr0 in AHV.

ESXi Standard vSwitch

- Use individual port static bindings instead of a vPC.
  - Use the default Route Based on Originating Virtual Port load balancing method.
  - If you need active-standby, use individual ports as well.
- Don't use a MAC pinning or Static Channel - Mode On port channel policy within the vPC policy.
- Don't alter the default vSwitchNutanix.

ESXi Distributed vSwitch

- If desired, use a VMware VDS vCenter VMM domain.
  - VMM domain integration is optional and all other recommendations still apply.
- Use local switching mode in the VMM domain vSwitch configuration.
- Place the CVM and ESXi VMkernel adapter in the VDS following KB 1037.
- Migrate one physical adapter on the host at a time to the VDS.
  - Don't migrate the svm-iscsi-pg port group.

- If four network adapters are available and you need out-of-band management, create a second VMkernel adapter in a VSS to provide a management connection to vCenter.
- If only two network adapters are available or the CVM and VMkernel adapters are in a VMM domain EPG, set the CVM and VMkernel EPG resolution immediacy to Pre-provision.
- Use individual ports with a static binding.
- Use the Route Based on Physical NIC Load load balancing method in the VDS.
- If you need LACP on ESXI, use an LACP-Active port channel policy.
  - Remove the Suspend Individual configuration from the port channel policy to enable LACP fallback.
- Don't use a MAC pinning or Static Channel - Mode On port channel policy in the vPC policy.
- Don't alter the default vSwitchNutanix.

ESXi with DVS and Cisco AVE

- Nutanix recommends Native switching mode for the CVM and VMkernel adapter. Using AVE switching mode for the Nutanix CVM may add latency that disrupts storage performance.
- Use AVE switching mode for microsegmentation in the hypervisor for user VMs if desired.

References

1. Cisco ACI Design Guide
2. Cisco ACI Virtual Edge Installation Guide

About the Author

Jason Burns is a Sr. Manager in Technical Marketing Engineering at Nutanix.

About Nutanix

Nutanix is a global leader in cloud software and a pioneer in hyperconverged infrastructure solutions, making clouds invisible and freeing customers to focus on their business outcomes. Organizations around the world use Nutanix software to leverage a single platform to manage any app at any location for their hybrid multicloud environments. Learn more at www.nutanix.com or follow us on Twitter @nutanix.

List of Figures