Cisco ACI and Nutanix AHV Integration

New and Changed Information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Cisco APIC Release Version	Feature	Description
6.0(3)	Support for Nutanix AHV integration	You can integrate Nutanix Acropolis Hypervisor (AHV) with Cisco Application Centric Infrastructure (ACI). Integration enables you to use Cisco Application Policy Infrastructure Controller (APIC) to create and work with Nutanix network constructs.

Overview

Beginning with Cisco Application Policy Infrastructure Controller (APIC) Release 6.0(3), you can integrate Nutanix Acropolis Hypervisor (AHV) with Cisco Application Centric Infrastructure (ACI).

The Cisco APIC integrates with Nutanix AHV and enhances the network management capabilities. The integration provides virtual and physical network automation and VM endpoints visibility in Cisco ACI.

This document provides information for integrating Nutanix AHV with Cisco ACI, including prerequisites and installation. You should be familiar with Nutanix AHV and Cisco ACI. For detailed information about Nutanix AHV, see the *Nutanix website*.

Benefits of the Cisco APIC- Nutanix AHV Integration

Following are the benefits of the integration:

- Native integration with Nutanix cluster running AHV.
- Visibility into the cluster (Nutanix) from APIC. Fetch inventory data like VMs, hosts, switches, subnets, security policies from Nutanix.
- Collect statistics and provide statistics display from APIC. The collected statistics are:
    - VM Nic Stats (Transmit Packets and Bytes, Received Packets and Bytes)
    - Host Nic Stats (Transmit Packets and Bytes, Received Packets and Bytes)
    - Host Stats (CPU and memory usage)
    - VM stats (CPU and memory usage)
- Support for EPGs to configure networking on Nutanix.
- Support for intra-EPG policies (intra-EPG contract is not supported).

Cisco ACI and Nutanix Terminology

Some terminology differs between Cisco ACI and Nutanix. The following table lists differences to be aware of.

Cisco ACI	Nutanix AHV
EPG/ port group	Subnet
Data center	Cluster
Cluster controller	Prism Element
Cluster	Prism Central

Guidelines and Limitations

Following are the guidelines and limitations for the Cisco ACI-Nutanix AHV integration:

- One VMM domain can be associated to only one Prism Central and one Prism Element.

- No two subnets can have the same VLAN on a vSwitch.

- Nutanix VMM domain supports only the pre-provision resolution immediacy.

- If a subnet is in use by a VM, the following operations cannot be done on Nutanix even if the configuration is changed on APIC:

    - the subnet VLAN, IP address pool cannot be changed.

    - the subnet cannot be deleted.

- Intra-EPG isolation is supported but intra-EPG contract is not supported. uSeg EPG and Endpoint Security Groups(ESG) are not supported.

- Bond type configuration for uplink of virtual switch is not supported from Cisco APIC.

- NetFlow, floating L3Out and layer 4 to layer 7 device running on Nutanix VMM domain are not supported.

- Multi-site integration is not supported, that is, no support for association of EPG to Nutanix VMM from NDO (Nexus Dashboard Orchestrator).

Workflow for the Integration

The following section elaborates the tasks involved for the integration. It is a combination of procedures to be accomplished on the Cisco APIC 6.0(3) GUI and the Nutanix Prism Central GUI. The tasks to be performed on the Cisco APIC GUI and the Nutanix Prism Central GUI are listed below.

1. (on Cisco APIC) Creating a VMM Domain.

2. (on Nutanix Prism Central) Assign host links to the virtual switch.

3. (on Cisco APIC) Associating an EPG to a VMM Domain .

4. (on Nutanix Prism Central) Assign VMs to subnets and categories.

The details of the procedures performed on the Cisco APIC GUI are available in the subsequent pages. The Nutanix-relevant tasks are explained in the context of the integration, for more details about the procedure and GUI, refer the *Nutanix website*.

Topology

Figure 1: Cisco APIC-Nutanix Prism Integration
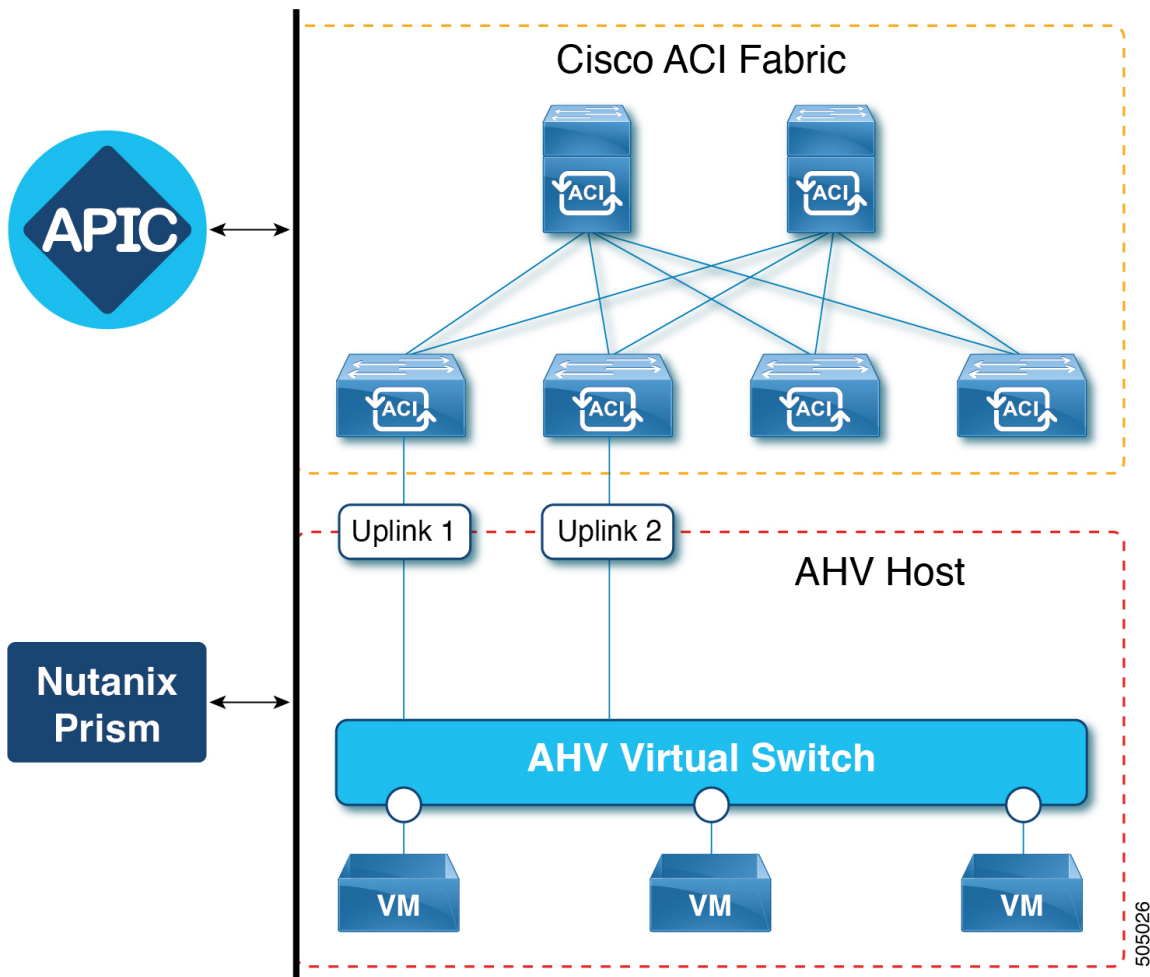
The image above shows a sample topology. The Cisco APIC manages the ACI fabric and policies. The VMs connected to the virtual switch are managed by the Nutanix Prism. ACI fabric provides network connectivity for VMs in AHV Hosts with the uplinks (Uplink1 and 2).

EPG Association with Nutanix VMM

Each EPG created on the Cisco APIC can be associated with a Nutanix VMM domain. The VMM domain creates a corresponding subnet on the Nutanix Prism. The EPG configuration also creates default categories. They are:

- `AppType : aci-domainname~TenantName~APName`

- `AppTier : aci-domainname~TenantName~APName~EPGName`

- `AciOwnerTag : aci-domainname~Tenantname~APName~EPGName`

The subnet(s) created on Nutanix are:

- *aci-domainname|TenantName|APName|EPGName* (default)

- custom epg name if *Custom EPG Name* is specified

Intra-EPG Isolation

Intra-EPG Isolation is an option to prevent physical or virtual endpoints that are in the same EPG from communicating with each other. By default, endpoints included in the same EPG are allowed to communicate with one another. However, conditions exist in which total isolation of the endpoints from one another within an EPG is desirable.

A Cisco ACI Nutanix VMM domain creates a security policy in the Nutanix Prism Central for each EPG that has intra-EPG isolation enabled. Nutanix applies the security policy for the `AppType` category (see categories mentioned in the section above) and prevents the communication of VMs in the associated `AppTier`.

> ✎ **Note** Intra-EPG isolation is not supported for IPv6 traffic because intra-EPG solution is implemented by Nutanix security policy for the Nutanix VMM domain. Nutanix security policy is applicable to IPv4 traffic only. However, IPv6 traffic is allowed by default even if intra EPG isolation is configured from APIC. You can change the security policy setting on the Nutanix UI to deny IPv6 traffic. This will deny all IPv6 traffic to and from the VMs which are associated with the security policy.

IP Address Management

When you enable IP Address Management (IPAM) on an EPG, Nutanix creates an internal DHCP server for the subnet corresponding to the EPG. IPv4 addresses for VMs in this subnet are allocated by this internal DHCP server. If the EPG is created without enabling IPAM, you may need to use an external DHCP server for VM IP assignment. See the Associating an EPG to a VMM Domain , on page 7 section for details about IPAM configuration.

Creating a VMM Domain

Use this procedure to create a VMM domain. A VMM domain needs to be created to specify the connectivity details to the Nutanix Controller. The VMM domain will also provide visibility into the Nutanix Cluster.

Before you begin

Confirm that the Nutanix cluster is up; Prism Central and Prism Element are healthy.

Procedure

Step 1	Log in to Cisco APIC.
Step 2	Go to **Virtual Networking** > **Nutanix**.
	The Domains page appears.
Step 3	At the upper right of the Domains page, click **Actions** > **Create Domain**.
Step 4	In the Create Domain page, complete the following steps:
	a) In the General area, in the **Name** field, enter a name for the domain.

b) In the Settings area > for the **Access Mode** field, choose *Read Only* or *Read Write*.

If you select Read Only, the VMM domain enables you to view inventory information for a vSwitch in the Prism Central that Cisco APIC does not manage.

c) Enter the **Custom vSwitch Name**.

To use an existing vSwitch (on Nutanix), enter the name. For this task (VMM domain creation), you can use an existing switch or Cisco APIC can create a vSwitch. If you leave the field blank, Cisco APIC creates a virtual switch on Nutanix while creating the VMM domain. The virtual switch cannot be modified after creation.

> **Note** You can create a new switch if you are using AOS version 6.6 and Prism Central that supports Nutanix v4 APIs. If you are using AOS version 6.5, use an existing virtual switch. It is recommended to check the relevant *Nutanix documentation* to confirm that your AOS and Prism Central versions support Nutanix v4 APIs.

d) For the VLAN Pool field, click **Select VLAN Pool**. In the Select VLAN Pool dialog box, choose an existing VLAN pool or create a new one.

e) For the **Attachable Access Entity Profile** field, click **Select Attachable Access Entity Profile**. In the Select Attachable Access Entity Profile dialog box, choose an existing attachable access entity profile or create a new one.

f) For the **Security Domains** field, click Add **Security Domain** and select the security domain from the displayed list.

This is a security feature where you can assign access to the required domains.

g) In the Controller area, click **Add Controller**. In the displayed pop-up window, enter the following details:

1. **Name** – enter the controller name (Prism Central in Nutanix).

2. **Hostname or IP Address** – enter the IP address of the Nutanix Prism Central.

3. **Datacenter** – enter the cluster name (as created on Nutanix) that the Cisco APIC needs to manage.

4. **Cluster AOS Version** – select the minimum cluster version (Nutanix Acropolis OS (AOS) version). The communication between Cisco APIC and Nutanix is based on the selected AOS version.

5. **Stats Mode** – select the Enabled check-box to fetch the information from Network Statistics in Nutanix.

6. For the Credentials field, click Select **Credentials** > Create Credentials. In the **Create Credentials** dialog box, enter a name for the credentials, a description, a username, and a password. Click **Save**.

7. Select **Advanced Settings**.

   The **Port Details** field is displayed.

   Port is set to the default value, 0. Use the default setting to connect to Nutanix Prism Central on port 9440. Enter a non-zero value if Nutanix Prism Central is using a custom port other than 9440.

8. For the **Cluster Controller** field, click **Add Cluster Controller**. In the Add Cluster Controller pop-up window, enter the details of the cluster which is part of the controller. Each cluster is referred to as Prism Element in Nutanix. Enter the name, IP address of the Nutanix Prism Element, the cluster name (Nutanix Prism Element Cluster), port, and credentials. Ensure that the cluster name entered here is the same as the Datacenter name in the **Add Controller** screen.

   (Optional) In Advanced Settings, enter the **Port Details** as mentioned in Step 7.

9. Click **OK**.

h) Click **Save** (Create Domain screen).

After the creation of the VMM domain, the created domain is displayed under **Virtual Networking** > **Nutanix**> **Domains** screen. Click the Domain Name (first column) to get the VMM inventory details about each domain. The inventory details are displayed as tabs. To check for faults, click the **Event Analytics** tab.

| **Note** | Only one cluster per VMM domain is supported; that is, one Prism Central can have one Prism Element. If you need more clusters, repeat the above procedure to create more VMM domains. |

What to do next

Assign host uplink links (using the Nutanix Prism Central GUI)

1. Log in to Nutanix Prism Central.

2. Navigate to **Network and Security** > **Subnets** > **Network Config**.

3. On the Network Configuration window that is displayed, select the **Virtual Switch** tab. The list of virtual switches available on Nutanix is displayed. You can use a virtual switch from the available list or create new one (see sub-step (c) in the above procedure).

4. Configure the interfaces of the virtual switch. Select the interfaces in the hosts that are connected to the ACI fabric.

5. To set the uplink configuration, select the **Bond type**. The bond types and the associated APIC configurations are:

Bond Type	APIC Configuration
No Uplink Bond	Configure Leaf Access Port Policy Group and associate to the Interface
Active-Active	Configure PC or VPC Policy Group and associate to the interfaces
Active-Backup	Configure Leaf Access Port Policy Group and associate to the Interface
Active-Active with MAC pinning	Configure Leaf Access Port Policy Group and associate to the Interface

For details about port policy configurations, see the Cisco APIC Basic Configuration Guide, Release 6.0(x).

6. If intra-EPG isolation is configured, microsegmentation needs to be enabled in Prism Central for the clusters managed by VMM domains. Navigate to **Prism Central Settings** > **Flow** > **Microsegmentation**.

Associating an EPG to a VMM Domain

Use this procedure for associating an EPG to a VMM domain. You can enable IPAM if you need Nutanix to create an internal DHCP server for the subnet corresponding to the EPG.

Each EPG created on APIC, which is associated with an Nutanix VMM domain, will create a corresponding subnet on Nutanix Prism. The EPG configuration will also create a few default categories corresponding to the EPG.

Following are the guidelines and restrictions, if IPAM is enabled using the procedure given below:

• IPAM Gateway is mandatory, cannot be modified after creation.

• DHCP Server Override address is optional, cannot be modified after creation.

• DHCP pool can be dynamically modified but ensure the VM address usage is valid during DHCP pool changes.

• After enabling IPAM on an EPG, you cannot disable it. You need to delete the VMM association and re-associate (with IPAM disabled).

• IPAM configuration can be modified if the subnet is not associated to a VM NIC.

Note It is recommended to manage IPAM configuration from Cisco APIC. If you must manage IPAM directly on Nutanix, do not configure IPAM on Cisco APIC. Ensure that you are configuring IPAM on either Cisco APIC or on Nutanix.

Before you begin

The required prerequisites are:

• Create a VMM domain.

• Create a tenant, application profile and at least one EPG.

• If you are enabling intra-EPG isolation using the procedure detailed below, ensure to enable microsegmentation on Nutanix Prism Central for the clusters managed by VMM domains.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Go to **Tenants** > *tenant* > **Application Profiles** > *application_profile* > **Application EPGs** > *application_epg* > **Domains (VMs and Bare-Metals)**.

Step 3 Choose **Domains** (VMs and Bare-Metals), click the **Action** icon at the upper right of the central pane and choose **Add VMM Domain Association**. The action icon is indicated by a crossed hammer and wrench.

Step 4 In the **Add VMM Domain Association** dialog box, enter the following details:

    a. From the **VMM Domain Profile** drop-down list, choose the Nutanix domain (that you earlier created, using Creating a VMM Domain, on page 5).

    b. Select the required **Deploy Immediacy**. The options are Immediate and On Demand.

    The only supported Resolution Immediacy is Pre-provision (which is not displayed on the GUI).

    c. For **VLAN Mode**, choose either *Static* or *Dynamic*.

    By default, a VLAN is dynamically assigned from the VLAN pool. If you select Static, enter the Port Encapsulation. Ensure to enter the correct value (from the VLAN pool range).

Note Nutanix does not allow VLAN ID change for an existing subnet, and a subnet cannot be deleted if there is a VM using it. If you change the VLAN ID of an EPG on Cisco APIC, then, either of the following is possible:

> • If there is no VM using the subnet, APIC will update the subnet with the new VLAN ID.
>
> • If there is a VM using the subnet, APIC will change the existing subnet to *original_name*|**inactive**, and create a new one with the *original_name* and a new VLAN ID. VM administrator needs to update the VM VNIC to subnet association.

The inactive subnet using the earlier VLAN will not be automatically deleted by APIC. Nutanix administrator will need to delete it after all the VMs are migrated to the new subnet.

    d. IPAM Enabled – Check the check-box to enable IP Address Management (IPAM).

    e. IPAM gateway Address – enter the gateway address the VMs can use to connect to the network.

    f. DHCP Server Override – enter the DHCP server IP address used by Nutanix. Set this field to specify the address to be used by the DHCP server (Nutanix). If you do not specifically mention this, Nutanix will auto-derive the IP address, which is the highest in the subnet.

    g. DHCP Address Pool – enter the DHCP address pool. Select the DHCP address pool or create a new one. On the APIC GUI, navigate to **Policies** > **VMM** > **Address Management Policies** to view or manage the IP Address pools.

    h. Custom EPG Name – Enter a name for the EPG.

    When you associate an EPG with a VMM domain, a default name is generated in this format - *TenantName|ApplicationProfile|EPGName*. When you enter a name here, the Nutanix subnet is created with the custom EPG name (as entered here), instead of the default name.

Step 5 Click **Submit**.

Step 6 (Optional) To enable intra-EPG isolation, navigate to **Tenant** > **Application Profiles** > *AP_name* > **Application EPGs** > *EPG_name.*

    a) On the work pane, go to **Policy** > **General** tab.

    b) For the **Intra EPG Isolation** field, select the **Enforced** option. (By default, **Unenforced** is selected.)

What to do next

Attach VMs (using the Nutanix Prism Central GUI)

1. Log in to Nutanix Prism Central.

2. Navigate to **Compute and Storage** > **VMs**.

3. From the displayed list of VMs, select the required VM. Click the **Actions** button > **Update**.

4. On the Update VM window, in the **Resources** tab > **Networks** area, click **Attach to Subnet**. Select the subnet.

   When an EPG is created and associated to a domain, a subnet is created on Nutanix (as described in the *Associate EPG to a VMM Domain* procedure, above).

5. Click **Next**.

6. On the Management tab, select the **Category** from the drop down list. Associate two categories for each EPG. They are- `AppTier:aci`, `AppType:aci`. These two categories are default category types on Prism Central. The values/ tags are created for these categories after EPG association to the VMM domain (as seen below).

```
AppType : aci-domainname~TenantName~APName
AppTier : aci-domainname~TenantName~APName~EPGName
```

7. (Optional) If intra EPG isolation is enabled on the EPG, navigate to **Network and Security** > **Security Policies** to confirm if the rule has been created. Security policies (in **Enforced** status) are created by the Cisco APIC to support intra EPG isolation.

CISCO

Americas Headquarters	**Asia Pacific Headquarters**	**Europe Headquarters**
Cisco Systems, Inc.	CiscoSystems(USA)Pte.Ltd.	CiscoSystemsInternationalBV
San Jose, CA 95134-1706	Singapore	Amsterdam,TheNetherlands
USA		

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the
Cisco Website at www.cisco.com/go/offices.