



CISCO ACI Virtual Machine Networking User Guide

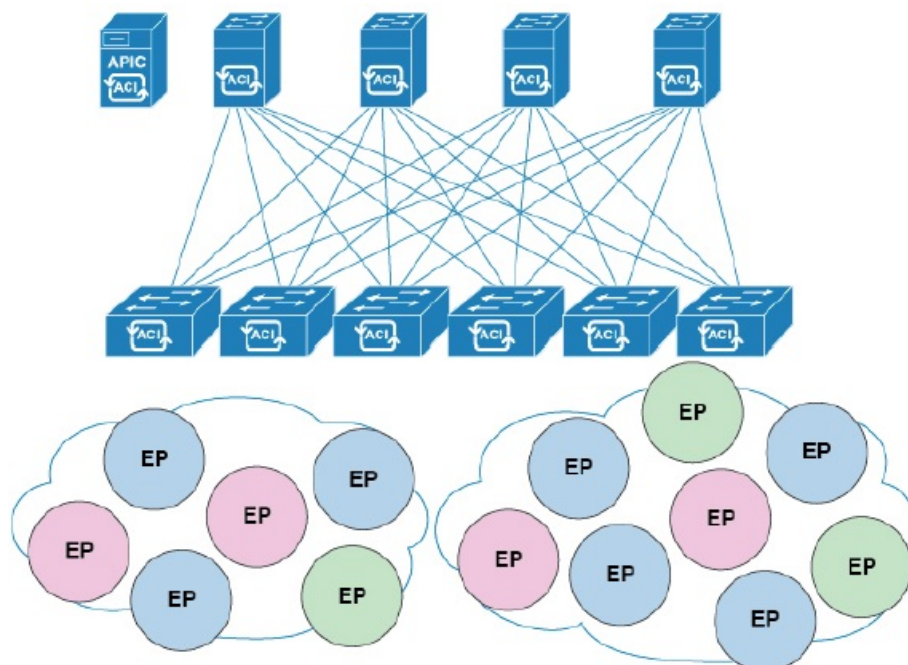
[Home](#) » [Cisco](#) » CISCO ACI Virtual Machine Networking User Guide 

Contents

- 1 CISCO ACI Virtual Machine Networking
- 2 Product Information
- 3 Product Usage Instructions
- 4 Networking Support
- 5 Mapping Cisco ACI and VMware Constructs
- 6 VMM Domain EPG Association
- 7 About Trunk Port Group
- 8 Attachable Entity Profile
- 9 Deployment Immediacy
- 10 NetFlow with Virtual Machine Networking
- 11 Documents / Resources
 - 11.1 References



CISCO ACI Virtual Machine Networking



Product Information

• Specifications:

- **Supported Products and Vendors:** Cisco ACI supports virtual machine managers (VMMs) from various products and vendors. Refer to the Cisco ACI Virtualization Compatibility Matrix for the most current list of verified interoperable products.

Product Usage Instructions

- **Mapping Cisco ACI and VMware Constructs:** Cisco Application Centric Infrastructure (ACI) and VMware use different terms to describe the same constructs. The following table provides a mapping of Cisco ACI and VMware terminology relevant to VMware vSphere Distributed Switch (VDS).

Cisco ACI Terms	VMware Terms
Endpoint group (EPG)	Port group, portgroup
LACP Active	LACP Passive
MAC Pinning	MAC Pinning-Physical-NIC-Load
Static Channel – Mode ON	Virtual Machine Manager (VMM) domain VDS
VM controller	vCenter (Datacenter)

• Virtual Machine Manager Domain Main Components:

- ACI fabric virtual machine manager (VMM) domains allow administrators to configure connectivity policies for virtual machine controllers. The main components of an ACI VMM domain policy include:
- Virtual Machine Manager (VMM) domain
- VM controller
- vCenter (Datacenter)
- **Note:** A single VMM domain can contain multiple instances of VM controllers, but they must be from the

same vendor (e.g., VMware or Microsoft).

- **Virtual Machine Manager Domains:**

- An APIC VMM domain profile is a policy that defines a VMM domain. The VMM domain policy is created in APIC and pushed into the leaf switches. VMM domains provide the following:

- **VMM Domain VLAN Pool Association**

- VLAN pools represent blocks of traffic VLAN identifiers. A VLAN pool is a shared resource and can be consumed by multiple domains such as VMM domains and Layer 4 to Layer 7 services.
- A VMM domain can be associated with only one dynamic VLAN pool.
- By default, VLAN identifiers are dynamically assigned to EPGs associated with VMM domains by the Cisco APIC.
- However, administrators can statically assign a VLAN identifier to an endpoint group (EPG) instead.
- In such cases, the identifiers used must be selected from the encapsulation blocks in the VLAN pool associated with the VMM domain, and their allocation type must be changed to static.
- The Cisco APIC provisions VMM domain VLAN on leaf ports based on EPG events, either statically binding on leaf ports or based on VM events from controllers like VMware vCenter or Microsoft SCVMM.
- **Note:** In dynamic VLAN pools, if a VLAN is disassociated from an EPG, it will automatically reassociate with the EPG after five minutes.
- Dynamic VLAN association is not a part of configuration rollback, meaning if an EPG or tenant was initially removed and then restored from the backup, a new VLAN will automatically be allocated from the dynamic VLAN pools.

- **FAQ:**

- **Q:** What products and vendors are supported by Cisco ACI?
- **A:** Cisco ACI supports virtual machine managers (VMMs) from various products and vendors. Please refer to the Cisco ACI Virtualization Compatibility Matrix for the most current list of verified interoperable products.
- **Q:** Can I statically assign a VLAN identifier to an EPG instead of dynamically assigning it?
- **A:** Yes, you can statically assign a VLAN identifier to an endpoint group (EPG) associated with a VMM domain. However, the identifier must be selected from the encapsulation blocks in the VLAN pool associated with the VMM domain, and the allocation type must be changed to static.
- **Q:** What happens if a VLAN is disassociated from an EPG in a dynamic VLAN pool?
- **A:** If a VLAN is disassociated from an EPG in a dynamic VLAN pool, it will automatically reassociate with the EPG after five minutes.
- **Q:** Is dynamic VLAN association part of configuration rollback?
- **A:** No, dynamic VLAN association is not a part of configuration rollback. If an EPG or tenant was initially removed and then restored from the backup, a new VLAN will automatically be allocated from the dynamic VLAN pools.

This chapter contains the following sections:

- Cisco ACI VM Networking Support for Virtual Machine Managers, on page 1
- Mapping Cisco ACI and VMware Constructs, on page 2
- Virtual Machine Manager Domain Main Components, on page 3
- Virtual Machine Manager Domains, on page 4
- VMM Domain VLAN Pool Association, on page 4

- VMM Domain EPG Association, on page 5
- About Trunk Port Group, on page 7
- Attachable Entity Profile, on page 8
- EPG Policy Resolution and Deployment Immediacy, on page 9
- Guidelines for Deleting VMM Domains, on page 10
- NetFlow with Virtual Machine Networking, on page 11
- Troubleshooting VMM Connectivity, on page 13

Networking Support

Cisco ACI VM Networking Support for Virtual Machine Managers

Benefits of ACI VM Networking

- Cisco Application Centric Infrastructure (ACI) virtual machine (VM) networking supports hypervisors from multiple vendors.
- It provides the hypervisor's programmable and automated access to high-performance scalable virtualized data centre infrastructure.
- Programmability and automation are critical features of scalable data centre virtualization infrastructure.
- The Cisco ACI open REST API enables virtual machine integration with and orchestration of the policy model-based Cisco ACI fabric.
- Cisco ACI VM networking enables consistent enforcement of policies across both virtual and physical workloads that are managed by hypervisors from multiple vendors.
- Attachable entity profiles easily enable VM mobility and placement of workloads anywhere in the Cisco ACI fabric.
- The Cisco Application Policy Infrastructure Controller (APIC) provides centralized troubleshooting, application health score, and virtualization monitoring.
- Cisco ACI multi-hypervisor VM automation reduces or eliminates manual configuration and manual errors. This enables virtualized data centres to support large numbers of VMs reliably and cost-effectively.

Supported Products and Vendors

- Cisco ACI supports virtual machine managers (VMMs) from the following products and vendors:
- Cisco Unified Computing System Manager (UCSM)
- Integration of [Cisco UCSM is supported beginning in Cisco APIC Release 4.1\(1\)](#). For information, see the chapter "Cisco ACI with Cisco UCSM Integration in the Cisco ACI Virtualization Guide, Release 4.1(1).

Cisco Application Centric Infrastructure (ACI) Virtual Pod (iPod)

- Cisco ACI vPod is in general availability beginning in Cisco APIC Release 4.0(2). For information, see the Cisco ACI vPod documentation on [Cisco.com](#).

Cloud Foundry

- Cloud Foundry integration with Cisco ACI is supported beginning with Cisco APIC Release 3.1(2). For information, see the knowledge base article, Cisco ACI and Cloud Found Integration on [Cisco.com](#).

Kubernetes

- For information, see the knowledge base article, [Cisco ACI and Kubernetes Integration](#) on [Cisco.com](#).

Microsoft System Center Virtual Machine Manager (SCVMM)

- For information, see the chapters “Cisco ACI with Microsoft SCVMM” and “Cisco ACI with Microsoft Windows Azure Pack” in the [Cisco ACI Virtualization Guide](#) on [Cisco.com](#).

OpenShift

- For information, see the [OpenShift documentation](#) on [Cisco.com](#).

OpenStack

- For information, see the [OpenStack documentation](#) on [Cisco.com](#).

Red Hat Virtualization (RHV)

- For information, see the knowledge base article, [Cisco ACI and Red Hat Integration](#) on [Cisco.com](#).

VMware Virtual Distributed Switch (VDS)

- For information, see the chapter “Cisco “ACI with VMware VDS Integration” in the [Cisco ACI Virtualization Guide](#).
- See the [Cisco ACI Virtualization Compatibility Matrix](#) for the most current list of verified interoperable products.

Mapping Cisco ACI and VMware Constructs

Cisco Application Centric Infrastructure (ACI) and VMware use different terms to describe the same constructs. This section provides a table for mapping Cisco ACI and VMware terminology; the information is relevant to VMware vSphere Distributed Switch (VDS).

Cisco ACI Terms	VMware Terms
Endpoint group (EPG)	Port group, portgroup

Cisco ACI Terms	VMware Terms
LACP Active	<ul style="list-style-type: none"> • Route based on IP hash (downlink port group) • LACP Enabled/Active (uplink port group)
LACP Passive	<ul style="list-style-type: none"> • Route based on IP hash (downlink port group) • LACP Enabled/Active (uplink port group)
MAC Pinning	<ul style="list-style-type: none"> • Route based on originating virtual port • LACP Disabled
MAC Pinning-Physical-NIC-Load	<ul style="list-style-type: none"> • Route based on physical NIC load • LACP Disabled
Static Channel – Mode ON	<ul style="list-style-type: none"> • Route based on IP Hash (downlink port group) • LACP Disabled
Virtual Machine Manager (VMM) domain	VDS
VM controller	vCenter (Datacenter)

Virtual Machine Manager Domain Main Components

ACI fabric virtual machine manager (VMM) domains enable an administrator to configure connectivity policies for virtual machine controllers. The essential components of an ACI VMM domain policy include the following:

- **Virtual Machine Manager Domain Profile**—Groups VM controllers with similar networking policy requirements. For example, VM controllers can share VLAN pools and application endpoint groups (EPGs). The APIC communicates with the controller to publish network configurations such as port groups that are then applied to the virtual workloads. The VMM domain profile includes the following essential components:
 - **Credential**—Associates a valid VM controller user credential with an APIC VMM domain.
 - **Controller**—Specifies how to connect to a VM controller that is part of a policy enforcement domain.
 - For example, the controller specifies the connection to a VMware vCenter that is part a VMM domain.

Note

A single VMM domain can contain multiple instances of VM controllers, but they must be from the same vendor (for example, from VMware or from Microsoft).

- **EPG Association**—Endpoint groups regulate connectivity and visibility among the endpoints within the scope of the VMM domain policy. VMM domain EPGs behave as follows: The APIC pushes these EPGs as port groups into the VM controller. An EPG can span multiple VMM domains, and a VMM domain can contain

multiple EPGs.

- **Attachable Entity Profile Association**—Associates a VMM domain with the physical network infrastructure. An attachable entity profile (AEP) is a network interface template that enables deploying VM controller policies on a large set of leaf switch ports. An AEP specifies which switches and ports are available, and how they are configured.
- **VLANPool Association**—A VLAN pool specifies the VLAN IDs or ranges used for VLAN encapsulation that the VMM domain consumes.

Virtual Machine Manager Domains

- An APIC VMM domain profile is a policy that defines a VMM domain. The VMM domain policy is created in APIC and pushed into the leaf switches.

VMM domains provide the following:

- A common layer in the ACI fabric that enables scalable fault-tolerant support for multiple VM controller platforms.
- VMM support for multiple tenants within the ACI fabric. VMM domains contain VM controllers such as VMware vCenter or Microsoft SCVMM Manager and the credential(s) required for the ACI API to interact with the VM controller.
- A VMM domain enables VMmobility within the domain but not across domains.
- A single VMM domain can contain multiple instances of VM controllers but they must be the same kind.
- For example, a VMM domain can contain many VMware vCenters managing multiple controllers each running multiple VMs but it may not also contain SCVMM Managers.
- A VMM domain inventories controller elements (such as pNICs, vNICs, VM names, and so forth) and pushes policies into the controller(s), creating port groups, and other necessary elements.
- The ACI VMM domain listens for controller events such as VM mobility and responds accordingly.

VMM Domain VLAN Pool Association

- VLAN pools represent blocks of traffic VLAN identifiers. A VLAN pool is a shared resource and can be consumed by multiple domains such as VMM domains and Layer 4 to Layer 7 services.
- Each pool has an allocation type (static or dynamic), defined at the time of its creation.
- The allocation type determines whether the identifiers contained in it will be used for automatic assignment by the Cisco APIC (dynamic) or set explicitly by the administrator (static).
- By default, all blocks contained within a VLAN pool have the same allocation type as the pool but users can change the allocation type for encapsulation blocks contained in dynamic pools to static. Doing so excludes them from dynamic allocation.
- A VMM domain can be associated with only one dynamic VLAN pool.
- By default, the assignment of VLAN identifiers to EPGs that are associated with VMM domains is done dynamically by the Cisco APIC.
- While dynamic allocation is the default and preferred configuration, an administrator can statically assign a VLAN identifier to an endpoint group (EPG) instead.
- In that case, the identifiers used must be selected from encapsulation blocks in the VLAN pool associated with

the VMM domain, and their allocation type must be changed to static.

- The Cisco APIC provisions VMM domain VLAN on leaf ports based on EPG events, either statically binding on leaf ports or based on VM events from controllers such as VMware vCenter or Microsoft SCVMM.

Note

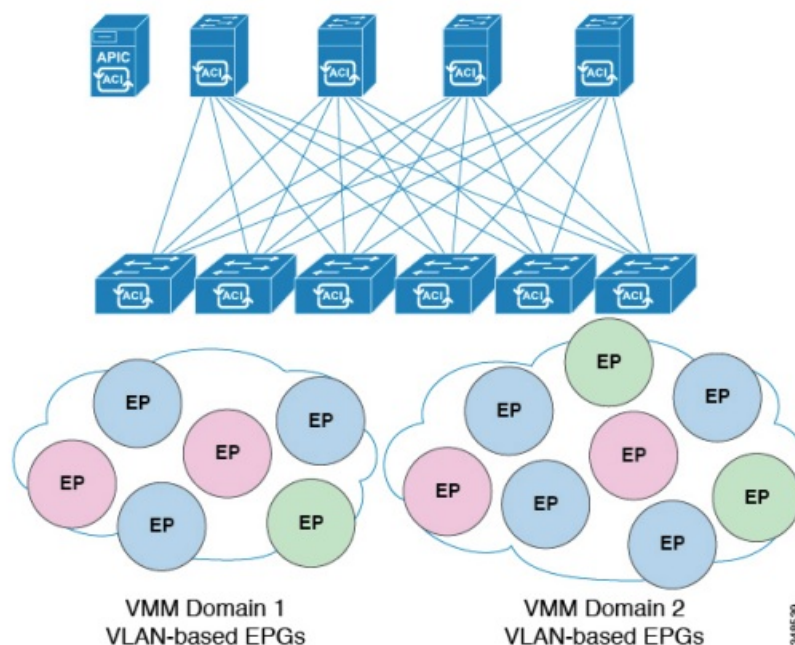
- In dynamic VLAN pools, if a VLAN is disassociated from an EPG, it is automatically reassociated with the EPG in five minutes.

Note

- Dynamic VLAN association is not a part of configuration rollback, that is, in case an EPG or tenant was initially removed and then restored from the backup, a new VLAN is automatically allocated from the dynamic VLAN pools.

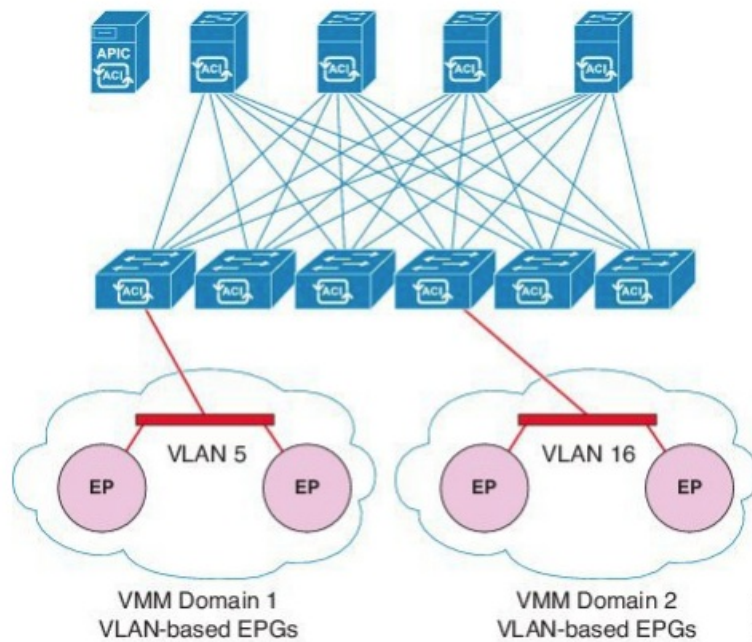
VMM Domain EPG Association

The Cisco Application Centric Infrastructure (ACI) fabric associates tenant application profile endpoint groups (EPGs) to virtual machine manager (VMM) domains. The Cisco ACI does so either automatically by an orchestration component such as Microsoft Azure, or by a Cisco Application Policy Infrastructure Controller (APIC) administrator creating such configurations. An EPG can span multiple VMM domains, and a VMM domain can contain multiple EPGs.



In the preceding illustration, endpoints (EPs) of the same colour are part of the same EPG. For example, all the green EPs are in the same EPG although they are in two different VMM domains. See the latest Verified Scalability Guide for Cisco ACI for virtual network and VMM domain EPG capacity information.

Figure 2: VMM Domain EPG VLAN Consumption



Note

- Multiple VMM domains can connect to the same leaf switch if they do not have overlapping VLAN pools on the same port.
- Similarly, you can use the same VLAN pools across different domains if they do not use the same port of a leaf switch.

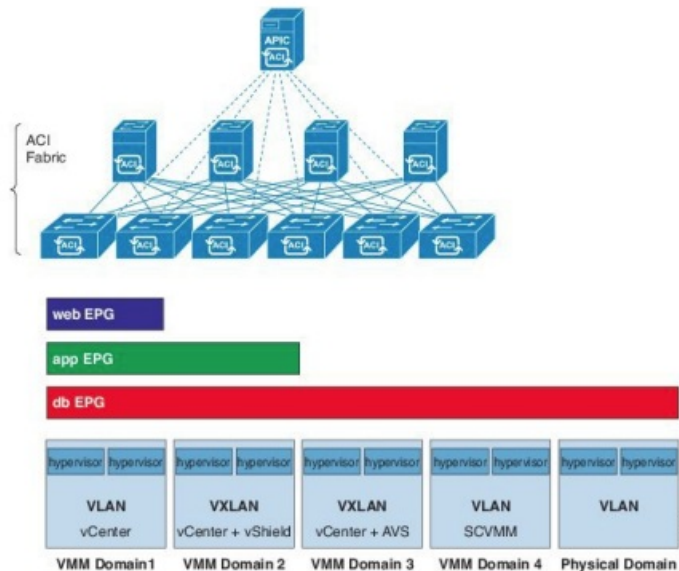
EPGs can use multiple VMM domains in the following ways:

- An EPG within a VMM domain is identified by using an encapsulation identifier. Cisco APIC can manage the identifier automatically, or the administrator can statically select it. An example is a VLAN, a Virtual Network ID (VNID).
- An EPG can be mapped to multiple physicals (for bare metal servers) or virtual domains. It can use different VLAN or VNID encapsulations in each domain.

Note

- By default, the Cisco APIC dynamically manages the allocation of a VLAN for an EPG.
- VMware DVS administrators have the option to configure a specific VLAN for an EPG.
- In that case, the VLAN is chosen from a static allocation block within the pool that is associated with the VMM domain.
- Applications can be deployed across VMM domains.

Figure 3: Multiple VMM Domains and Scaling of EPGs in the Fabric



- While live migration of VMs within a VMM domain is supported, live migration of VMs across VMM domains is not supported.

Note

- When you change the VRF on a bridge domain that is linked to an EPG with an associated VMM domain, the port group is deleted and then added back on vCenter.
- This results in the EPG being undeployed from the VMM domain. This is expected behaviour.

About Trunk Port Group

- You use a trunk port group to aggregate the traffic of endpoint groups (EPGs) for VMware virtual machine manager (VMM) domains.
- Unlike regular port groups, which are configured under the Tenants tab in the Cisco Application Policy Infrastructure Controller (APIC) GUI, trunk port groups are configured under the VM Networking tab.
- Regular port groups follow the T|A|E format of EPG names.
- The aggregation of EPGs under the same domain is based on a VLAN range, which is specified as encapsulation blocks contained in the trunk port group.
- Whenever the encapsulation of an EPG is changed or the encapsulation block of a trunk port group is changed, the aggregation is re-evaluated to determine if the EGP should be aggregated.
- A trunk port group controls the leaf deployment of network resources, such as VLANs, that are allocated to the EPGs being aggregated.
- The EPGs include both base EPG and microsegmented (uSeg) EPGs. In the case of a user EPG, the VLAN ranges of the trunk port group are needed to include both the primary and secondary VLANs.

For more information, see the following procedures:

- [Creating a Trunk Port Group Using the GUI.](#)
- [Creating a Trunk Port Group Using the NX-OS Style CLI.](#)
- [Creating a Trunk Port Group Using the REST API.](#)

Attachable Entity Profile

The ACI fabric provides multiple attachment points that connect through leaf ports to various external entities such as bare metal servers, virtual machine hypervisors, Layer 2 switches (for example, the Cisco UCS fabric interconnect), or Layer 3 routers (for example Cisco Nexus 7000 Series switches). These attachment points can be physical ports, FEX ports, port channels, or a virtual port channel (vPC) on leaf switches.

Note

When creating a VPC domain between two leaf switches, both switches must be in the same switch generation, one of the following:

- **Generation 1** – Cisco Nexus N9K switches without “EX” or “FX” at the end of the switch name; for example, N9K-9312TX
- **Generation 2** – Cisco Nexus N9K switches with “EX” or “FX” at the end of the switch model name; for example, N9K-93108TC-EX

Switches such as these two are not compatible with VPC peers. Instead, use switches of the same generation. An Attachable Entity Profile (AEP) represents a group of external entities with similar infrastructure policy requirements. The infrastructure policies consist of physical interface policies that configure various protocol options, such as Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), or Link Aggregation Control Protocol (LACP). An AEP is required to deploy VLAN pools on leaf switches. Encapsulation blocks (and associated VLANs) are reusable across leaf switches. An AEP implicitly provides the scope of the VLAN pool to the physical infrastructure. The following AEP requirements and dependencies must be accounted for in various configuration scenarios, including network connectivity, VMM domains, and multi pod configuration:

- The AEP defines the range of allowed VLANs but it does not provision them. No traffic flows unless an EPG is deployed on the port. Without defining a VLAN pool in an AEP, a VLAN is not enabled on the leaf port even if an EPG is provisioned.
- A particular VLAN is provisioned or enabled on the leaf port that is based on EPG events either statically binding on a leaf port or based on VM events from external controllers such as VMware vCenter or Microsoft Azure Service Center Virtual Machine Manager (SCVMM).
- Attached entity profiles can be associated directly with application EPGs, which deploy the associated application EPGs to all those ports associated with the attached entity profile. The AEP has a configurable generic function (infraGeneric), which contains a relation to an EPG (infraRsFuncToEpg) that is deployed on all interfaces that are part of the selectors that are associated with the attachable entity profile.
- A virtual machine manager (VMM) domain automatically derives physical interface policies from the interface policy groups of an AEP.
- An override policy at the AEP can be used to specify a different physical interface policy for a VMM domain. This policy is useful in scenarios where a VM controller is connected to the leaf switch through an intermediate Layer 2 node, and a different policy is desired at the leaf switch and VM controller physical ports. For example, you can configure LACP between a leaf switch and a Layer 2 node. At the same time, you can disable LACP between the VM controller and the Layer 2 switch by disabling LACP under the AEP override policy.

Deployment Immediacy

EPG Policy Resolution and Deployment Immediacy

Whenever an endpoint group (EPG) associates to a virtual machine manager (VMM) domain, the administrator can choose the resolution and deployment preferences to specify when a policy should be pushed into leaf switches.

Resolution Immediacy

- **Pre-provision:** Specifies that a policy (for example, VLAN, VXLAN binding, contracts, or filters) is downloaded to a leaf switch even before a VM controller is attached to the virtual switch (for example, VMware vSphere Distributed Switch (VDS). This pre-provisions the configuration on the switch.
- This helps the situation where management traffic for hypervisors/VM controllers is also using the virtual switch associated to the Cisco Application Policy Infrastructure Controller (APIC) VMM domain (VMM switch).
- Deploying a VMM policy such as VLAN on a Cisco Application Centric Infrastructure (ACI) leaf switch requires Cisco APIC to collect CDP/LLDP information from both hypervisors through the VM controller and Cisco ACI leaf switch. However, if the VM controller is supposed to use the same VMM policy (VMM switch) to communicate with its hypervisors or even Cisco APIC, the CDP/LLDP information for hypervisors can never be collected because the policy that is required for VM controller/hypervisor management traffic is not deployed yet.
- When using pre-provision immediacy, the policy is downloaded to the Cisco ACI leaf switch regardless of CDP/LLDP neighborship. Even without a hypervisor host that is connected to the VMM switch.
- **Immediate:** Specifies that EPG policies (including contracts and filters) are downloaded to the associated leaf switch software upon ESXi host attachment to a DVS. LLDP or OpFlex permissions are used to resolve the VM controller to leaf node attachments.
- The policy will be downloaded to Leaf when you add a host to the VMM switch. CDP/LLDP neighborship from host to leaf is required.
- **On-Demand:** Specifies that a policy (for example, VLAN, VXLAN bindings, contracts, or filters) is pushed to the leaf node only when an ESXi host is attached to a DVS and a VM is placed in the port group (EPG).
- The policy will be downloaded to the leaf when the host is added to the VMM switch. The VM needs to be placed into a port group (EPG). CDP/LLDP neighborship from host to leaf is required. With both immediate and on-demand, if the host and leaf lose LLDP/CDP neighborship the policies are removed.

Note

- In OpFlex-based VMM domains, an OpFlex agent on the hypervisor reports a VM/EP virtual network interface card (vNIC) attachment to an EPG to the leaf OpFlex process.
- When using On Demand Resolution Immediacy, the EPG VLAN/VXLAN is programmed on all leaf port channel ports, virtual port channel ports, or both when the following are true:
 - Hypervisors are connected to leaves on the port channel or virtual port channel attached directly or through blade switches.
 - A VM or instance vNIC is attached to an EPG.
 - Hypervisors are attached as part of the EPG or VMM domain.
- Opflex-based VMM domains are Microsoft Security Center Virtual Machine Manager (SCVMM) and HyperV, and Cisco Application Virtual Switch (AVS).

Deployment Immediacy

- Once the policies are downloaded to the leaf software, deployment immediacy can specify when the policy is pushed into the hardware policy content-addressable memory (CAM).
- **Immediate:** Specifies that the policy is programmed in the hardware policy CAM as soon as the policy is downloaded in the leaf software.
- **On-demand:** Specifies that the policy is programmed in the hardware policy CAM only when the first packet is received through the data path. This process helps to optimize the hardware space.

Note

- When you use on-demand deployment immediacy with MAC-pinned VPCs, the EPG contracts are not pushed to the leaf ternary content-addressable memory (TCAM) until the first endpoint is learned in the EPG on each leaf.
- This can cause uneven TCAM utilization across VPC peers. (Normally, the contract would be pushed to both peers.)

Guidelines for Deleting VMM Domains

Follow the sequence below to ensure that the APIC request to delete a VMM domain automatically triggers the associated VM controller (for example VMware vCenter or Microsoft SCVMM) to complete the process normally and that no orphan EPGs are stranded in the ACI fabric.

1. The VM administrator must detach all the VMs from the port groups (in the case of VMware vCenter) or VM networks (in the case of SCVMM), created by the APIC. In the case of Cisco AVS, the VM admin also needs to delete VMK interfaces associated with the Cisco AVS.
2. The ACI administrator deletes the VMM domain in the APIC. The APIC triggers the deletion of VMware VDS Cisco AVS or SCVMM logical switch and associated objects.

Note

The VM administrator should not delete the virtual switch or associated objects (such as port groups or VM networks); allow the APIC to trigger the virtual switch deletion upon completion of step 2 above. EPGs could be orphaned in the APIC if the VM administrator deletes the virtual switch from the VM controller before the VMM domain is deleted in the APIC. If this sequence is not followed, the VM controller deletes the virtual switch associated with the APIC VMM domain. In this scenario, the VM administrator must manually remove the VM and vtep associations from the VM controller, and then delete the virtual switch(es) previously associated with the APIC VMM domain.

NetFlow with Virtual Machine Networking

About NetFlow with Virtual Machine Networking

- The NetFlow technology provides the metering base for a key set of applications, including network traffic accounting, usage-based network billing, network planning, as well as denial of services monitoring, network monitoring, outbound marketing, and data mining for both service providers and enterprise customers.
- Cisco provides a set of NetFlow applications to collect NetFlow export data, perform data volume reduction, perform post-processing, and provide end-user applications with easy access to NetFlow data.
- If you have enabled NetFlow monitoring of the traffic flowing through your data centres, this feature enables you

to perform the same level of monitoring of the traffic flowing through the Cisco Application Centric Infrastructure (Cisco ACI) fabric.

- Instead of hardware directly exporting the records to a collector, the records are processed in the supervisor engine and are exported to standard NetFlow collectors in the required format. For more information about NetFlow, see the Cisco APIC and NetFlow knowledge base article.

About NetFlow Exporter Policies with Virtual Machine Networking

A virtual machine manager exporter policy (`netflowVmmExporterPol`) describes information about the data collected for a flow that is sent to the reporting server or NetFlow collector. A NetFlow collector is an external entity that supports the standard NetFlow protocol and accepts packets marked with valid NetFlow headers.

An exporter policy has the following properties:

- **VmmExporterPol.dstAddr**—This mandatory property specifies the IPv4 or IPv6 address of the NetFlow collector that accepts the NetFlow flow packets. This must be in the host format (that is, “/32” or “/128”). An IPv6 address is supported in vSphere Distributed Switch (vDS) version 6.0 and later.
- **VmmExporterPol.dstPort**—This mandatory property specifies the port on which the NetFlow collector application is listening, which enables the collector to accept incoming connections.
- **VmmExporterPol.srcAddr**—This optional property specifies the IPv4 address that is used as the source address in the exported NetFlow flow packets.

NetFlow Support with VMware vSphere Distributed Switch

The VMware vSphere Distributed Switch (VDS) supports NetFlow with the following caveats:

- The external collector must be reachable through the ESX. ESX does not support virtual routing and forwardings (VRFs).
- A port group can enable or disable NetFlow.
- VDS does not support flow-level filtering.

Configure the following VDS parameters in VMware vCenter:

- Collector IP address and port. IPv6 is supported on VDS version 6.0 or later. These are mandatory.
- Source IP address. This is optional.
- Active flow timeout, idle flow timeout, and sampling rate. These are optional.

Configuring a NetFlow Exporter Policy for VM Networking Using the GUI

The following procedure configures a NetFlow exporter policy for VM networking.

Procedure

- **Step 1** On the menu bar, choose Fabric > Access Policies.
- **Step 2** In the navigation pane, expand Policies > Interface > NetFlow.
- **Step 3** Right-click NetFlow Exporters for VM Networking and choose Create NetFlow Exporter for VM Networking.
- **Step 4** In the Create NetFlow Exporter for VM Networking dialogue box, fill in the fields as required.

- **Step 5** Click Submit.

Consuming a NetFlow Exporter Policy Under a VMM Domain Using the GUI

The following procedure consumes a NetFlow exporter policy under a VMM domain using the GUI.

Procedure

- **Step 1** On the menu bar, choose Virtual Networking > Inventory.
- **Step 2** In the Navigation pane, expand the VMMDomains folder, right-click VMware, and choose Create Center Domain.
- **Step 3** In the Create vCenter Domain dialog box, fill in the fields as required, except as specified:
 - **a)** In the NetFlow Exporter Policy drop-down list, choose the desired exporter policy or create a new one.
 - **b)** In the Active Flow Timeout field, enter the desired active flow timeout, in seconds. The Active Flow Timeout parameter specifies the delay that NetFlow waits after the active flow is initiated, after which NetFlow sends the collected data. The range is from 60 to 3600. The default value is 60.
 - **c)** In the Idle Flow Timeout field, enter the desired idle flow timeout, in seconds. The Idle Flow Timeout parameter specifies the delay that NetFlow waits after the idle flow is initiated, after which NetFlow sends the collected data. The range is from 10 to 300. The default value is 15.
 - **d)** (VDS only) In the Sampling Rate field, enter the desired sampling rate. The Sampling Rate parameter specifies how many packets NetFlow will drop after every collected packet. If you specify a value of 0, then NetFlow does not drop any packets. The range is from 0 to 1000. The default value is 0.
- **Step 4** Click Submit.

Enabling NetFlow on an Endpoint Group to VMM Domain Association Using the GUI

The following procedure enables NetFlow on an endpoint group to VMM domain association.

Before you begin

You must have configured the following:

- An application profile
- An application endpoint group

Procedure

- **Step 1** On the menu bar, choose Tenants > All Tenants.
- **Step 2** In the Work pane, double-click the tenant's name.
- **Step 3** In the left navigation pane, expand tenant_name > Application Profiles > application_profile_name > Application EPGs > application_EPG_name
- **Step 4** Right-click Domains (VMs and Bare-Metals) and choose Add VMM Domain Association.
- **Step 5** In the Add VMM Domain Association dialog box, fill in the fields as required; however, in the NetFlow area, choose Enable.
- **Step 6** Click Submit.


Troubleshooting VMM Connectivity

The following procedure resolves VMM connectivity issues:

Procedure

- **Step 1** Trigger inventory resync on the Application Policy Infrastructure Controller (APIC). For more information about how to trigger an inventory resync on APIC, see the following knowledge base article:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_KB_VMM_OnDemand_Invento
- **Step 2** If step 1 does not fix the issue, for the impacted EPGs, set the resolution immediately to use preprovisioning in the VMM domain. "Pre-Provision" removes the need for neighbor adjacencies or OpFlex permissions and subsequently the dynamic nature of VMM Domain VLAN Programming. For more information about Resolution Immediacy types, see the following EPG Policy Resolution and Deployment Immediacy section:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/aci-fundamentals/b_ACI-Fundamentals/b_ACI-Fundamentals_chapter_01011.html#concept_EF87ADDAD4EF47BDA741EC6EFDAECBBB.
- **Step 3** If steps 1 and 2 do not fix the issue and you see the issue on all of the VMs, then delete the VM controller policy and read the policy.
- **Note** Deleting the controller policy impacts traffic for all VMs that are on that controller. Cisco ACI Virtual Machine Networking.

Documents / Resources

	CISCO ACI Virtual Machine Networking [pdf] User Guide ACI Virtual Machine Networking, ACI, Virtual Machine Networking, Machine Networking, Network
---	---

References

- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.