Service VM Orchestration

Service VM Orchestration

Service virtual machine (VM) orchestration is a policy-based feature that enables you to create and manage service VMs easily with Cisco Application Policy Infrastructure Controller (APIC). Service VM orchestration is a new feature for VMware vCenter environments in Cisco APIC 4.0(1).

Previously, you had to create a service VM in VMware vCenter, define the data center that it belonged to, and associate it with a data store. You also had to configure its management network settings and then attach it to Cisco APIC. However, service VM orchestration enables you to perform all these tasks in Cisco APIC.

Service VM orchestration streamlines the process of configuring the service VMs, also known as concrete devices (CDev). The CDevs are grouped into a device cluster, also known as a logical device (LDev). Configuration and policy that are applied to the LDev are applied to each CDev that it contains.

To use service VM orchestration, you create and upload a configuration file. You then configure a VM instantiation policy, create the Layer 4 to Layer 7 LDev, and then create CDevs associated with the LDev. Read and understand the section Service VM Orchestration Guidelines and Limitations, on page 2 before configuring service VM orchestration.

You can perform Service VM orchestration tasks using the Cisco APIC GUI, the NX-OS style CLI, or REST API. See the the following sections for instructions:

- Configuring Service VM Orchestration Using the Cisco APIC GUI, on page 2
- Configuring Service VM Orchestration Using the NX-OS Style CLI, on page 8
- Configuring Service VM Orchestration Using REST API, on page 8

Service VM Orchestration Guidelines and Limitations

Keep the following guidelines and limitations in mind when using service VM orchestration:

- Service VM orchestration is supported only for Cisco Adaptive Security Virtual Appliance (ASAv) and Palo Alto Networks devices.
- High-availability (HA) virtual machine (VM) deployment using service VM orchestration is supported only on shared storage. It is not supported on a local data store.
- Dynamic Host Configuration Protocol (DHCP) IP addressing is not supported for single or HA service VM deployments.
- Any port group or VM template created on VMware vCenter requires manual inventory sync on Cisco Application Policy Infrastructure Controller (APIC) before you use service VM orchestration. Check the configuration documentation on how to trigger inventory sync.
- Palo Alto deployment works only with the default username **`admin`** and the password **`admin`**.
- After a Palo Alto device is deployed, you see a `Script error: force config push is required` fault on Cisco APIC for 10 minutes. The message is due to an internal process running on the Palo Alto device; the fault will be cleared when the configuration is pushed successfully and the device becomes stable.
- Cisco APIC cannot reach a Cisco Adaptive Security Virtual Appliance (ASAv) device after deletion and redeployment. This issue occurs because the old MAC address is not cleared in the upstream switches. Clear the MAC entry of the IP address that is used for service VMs on the upstream switch and then redeploy the service VM using service VM orchestration.
- If you are cloning an existing policy, do not change a VM instantiation policy that is associated with a logical device before the cloning is completed.
- To deploy service VMs using service VM orchestration, enable additional VMware vCenter privileges. See the section "Custom User Account with Minimum VMware vCenter Privileges" in the chapter "Cisco ACI with VMware VDS Integration" in the *Cisco ACI Virtualization Guide*.

Configuring Service VM Orchestration Using the Cisco APIC GUI

You can perform several tasks in the Cisco Application Policy Infrastructure Controller (APIC) GUI to configure Service VM orchestration.

Creating a VM Instantiation Policy Using the Cisco APIC GUI

Creating a virtual machine (VM) instantiation file is the first task in the process of using service virtual machine (VM) orchestration to deploy and manage service VMs with the Cisco Application Policy Infrastructure Controller. The policy is created for a device cluster or logical device (LDev) and is then applied to concrete devices (CDev) that belong to the LDev.

Step 1 Log in to Cisco APIC.

Step 2 Go to **Tenants** > ***tenant*** > **Policies** > **VMM** > **VM Instantiation Policies**.

Step 3 In the upper-right corner of the work pane, click the icon of a hammer and wrench, and then choose **Create VM Instantiation Policy**.

Step 4 In the **Create VM Instantiation Policy** dialog box, complete the following steps:

a) In the **Name** field, enter the name of the policy.

b) From the **Controller** drop-down list, choose the controller.

c) From the **VM Template** drop-down list, choose the template for the service VM that you want to create.

The drop-down list shows you VM templates associated with the controller.

Note If you do not see the VM template created on VMware vCenter, complete the following steps:

1. Click the blue icon next to the controller drop-down list.
2. In the **Controller Instance** dialog box, click the wrench-and-hammer icon on the right, and then click **Trigger Inventory Sync**, and then click **Yes** to trigger the sync.
3. Close the **Controller Instance** dialog box to return to the **Create VM Instantiation Policy** dialog box.

d) From the **Host Name** drop-down list, choose the host where you want to deploy the service VM.

You can choose a VMware vSphere Distributed Resource Scheduler (DRS) cluster or an individual host.

e) From the **Data Store** drop-down list, choose the data store where you want to put the VM disk.

f) Click **Submit**.
The work pane shows the VM instantiation policies.

Creating a Layer 4 to Layer 7 services device and Associating the Device with the VM Instantiation Policy Using the GUI

In this procedure, you create a Layer 4 to Layer 7 services device and associate it with the virtual machine (VM) instantiation policy that you created earlier.

When you create a Layer 4 to Layer 7 services device, you can connect to either a physical device or a virtual machine. The fields are slightly different depending on the type to which you are connecting. When you connect to a physical device, you specify the physical interface. When you connect to a virtual machine, you specify the VMM domain, the virtual machine, and the virtual interfaces. Also, you can select an unknown model, which allows you to configure the connections manually.

When you create a Layer 4 to Layer 7 services device to be associated with the VM instantiation policy, you also specify the policy and create the new service VM.

Note When you configure a Layer 4 to Layer 7 services device that is a load balancer, the context aware parameter is not used. The context aware parameter has a default value of single context, which can be ignored.

Before you begin

- You must have configured a tenant.
- You must have created a VM instantiation policy. See the section Creating a VM Instantiation Policy Using the Cisco APIC GUI, on page 2.

Step 1 Log in to Cisco Application Policy Infrastructure Controller (APIC).

Step 2 Go to **Tenants** > ***tenant*** > **Services** > **L4-L7** > **Devices**.

Step 3 Right-click **Devices** and then choose **Create L4-L7 Devices**.

Alternatively, in the upper right of the work pane you can click the actions icon (crossed hammer and wrench) and then choose **Create L4-L7 Devices**.

Step 4 In the **Create L4-L7 Devices** dialog box, in the **General** section, complete the following fields:

Name	Description
Name	Enter a name for the Layer 4 to Layer 7 services device.
Service Type	Choose a service type from the drop-down list. You can choose one of the following service types: • **ADC** (Application Delivery Controller). **ADC** is the default service type. • **Firewall**: Choose routed or transparent deployment mode. • **Other**: any other mode. **Note** For a policy-based redirect configuration, choose **Firewall** or **ADC** as the service type.
Device Type	Choose **Virtual** (virtual Layer 4 to Layer 7 services device).
VMM Domain	Choose a VMM domain from the drop-down list.
VM Instantiation Policy	From the drop-down list, choose the VM instantiation policy that you created earlier. Choosing the policy associates it with the new Layer 4 to Layer 7 services device. It also helps creating the VM automatically on VMware vCenter.
Promiscuous Mode	Check the checkbox to enable promiscuous mode on Cisco Application Centric Infrastructure (ACI)-managed port groups that are generated after deploying a service graph. Enabling promiscuous mode allows all the traffic in a port group to reach a VM attached to a promiscuous port.

Name	Description
Context Aware	Choose **Single**, the default, or **Multiple**. If you choose **Single**, the device cluster cannot be shared across multiple tenants of a given type that are hosted on the provider network. You must give the device cluster to a specific tenant for a given user. If you choose **Multiple**, the device cluster can be shared across multiple tenants of a given type that you are hosting on the provider network. For example, there could be two hosting companies that share the same device.
Function Type	You can choose: • **GoThrough** (transparent mode) • **GoTo** (routed mode)

Step 5 In the **Devices** section, click the plus icon.

Step 6 In the **Create Device STEP 1 > Device** dialog box, complete the following fields to configure a concrete device (CDev) and associate it with the Layer 4 to Layer 7 services device:

Name	Description
Gateway IP	Enter the gateway IP address of the new service VM.
Subnet Mask	Enter the subnet mask for the new service VM.
Management vNIC	Choose the management vNIC for the new service VM from the drop-down list.
VM	Enter the VM name for the new service VM to appear in VMware vCenter.

Name	Description
Host (Optional)	From the drop-down list, choose the host for the new service VM. If you do not choose a host, the host that is chosen in VM instantiation policy will be used. For policy-based redirect (PBR) and direct server return (DSR) functionality, selection of particular host is important based on topology. In that case, choose the correct host. For DSR and PDR, compute VMs and service VMs cannot reside on the same top-of-rack (TOR) switch pair. So you need to choose the host for deploying service VMs for PBR or DSR topology. Oherwise, the feature could deploy the service VMs on the same host as the compute VMs. For devices to be connected on Cisco Application Centric Infrastructure (ACI) Virtual Edge, you cannot deploy high-availability Layer 4 to Layer 7 services devices on same host. Therefore, choose different hosts for primary and secondary VMs.
Port Group Name (Optional)	From the drop-down list, choose the port group for the new service VM to be deployed. If you do not choose one, the port group that is used in the VM template will be used.
HA EPG (Optional)	From the drop-down list, choose the high-availability (HA) endpoint group (EPG) or vSwitch or distributed virtual switch (DVS) port group for HA communication for the new service VM.
HA Network Adapter (Optional)	Choose an HA network adapter for the new service VM from the drop-down list.
Username	Enter the username for the new service VM.
Password	Enter the password for the new service VM.
Confirm Password	Re-enter the password.

Step 7 Click **Next**.

Step 8 In the **Create Device STEP 2 > Interfaces** dialog box, in the **Interfaces** section, click the plus icon.

Step 9 Complete the following fields in the dialog box to configure the interface for the CDev:

Name	Description
Name	Choose the name of the Layer 4 to Layer 7 services device interface from the drop-down list.
VNIC (Virtual device type only)	Choose the name of the VM network adapter from the drop-down list.

Name	Description
Path (Optional if the Layer 4 to Layer 7 services device is a virtual device)	Choose a port, port channel (PC), or virtual port channel (VPC) that the interface will connect to.

Step 10 In the **Interfaces** section, click the plus icon again and configure another interface.

Step 11 Click **Update**.

Step 12

Step 13 To add extra service VMs to the Layer 4 to Layer 7 services device, repeat Step 8 through Step 13.

Step 14 If you have multiple service VMs, in the **Create Device STEP 1 > Device** dialog box, in the **Cluster** section, complete the following fields for each device:

For an HA cluster, make sure that the cluster interfaces are mapped to the corresponding interfaces on both concrete devices in the cluster.

Name	Description

Cluster Interfaces area	Complete the following fields to configure outside connectivity for the Layer 4 to Layer 7 services device:
	• From the **Type** drop-down list, choose a cluster interface type. The type can be:
	  • **failover_link**
	  • **utility**
	  • **consumer**
	  • **provider**
	  • **mgmt**
	  • **cluster_ctrl_lk**
	  • **failover-lan**
	  • **consumer and provider**
	• From the **Name** drop-down list, choose the cluster interface name.
	• From the **Concrete Interfaces** drop-down list, choose the associated concrete interfaces.

Step 15 Click **Finish**.

What to do next

You can view creation of the new service VM in the VMware vCenter under **Recent Tasks**. It can take a while for it to appear.

Configuring Service VM Orchestration Using the NX-OS Style CLI

You can use the NX-OS style CLI to create the virtual machine (VM) instantiation policy and the Layer 4 to Layer 7 concrete device and map the device to the instantiation policy. You can then map the internal and external interfaces to the VM network adapter.

Step 1 Create the VM instantiation policy.

Example:

```
APIC1(config-tenant)# inst-pol VMPolName VMMname VcentercontrollerName VMtemplateName ClusterName
datastorename
```

Step 2 Create the Layer 4 to Layer 7 concrete device and associate it with the VM instantiation policy.

Example:

```
APIC1(config)# tenant T0
APIC1(config-tenant)# l4l7 cluster name ASA-Single type virtual vlan-domain ASAVMM switching-mode
AVE vm-instantiation-policy ASA-Template-Pol  service FW function go-to context single trunking
disable
```

Step 3 Map the internal and external interfaces to the VM network adapter.

Example:

```
APIC1(config-cluster)# cluster-interface external
APIC1(config-cluster-interface)# member device ASA-Cdev device-interface GigabitEthernet0/0
APIC1(config-member)# vnic "Network adapter 2"
APIC1(config-member)# exit
APIC1(config-cluster)# cluster-interface internal
APIC1(config-cluster-interface)# member device ASA-Cdev device-interface GigabitEthernet0/1
APIC1(config-member)# vnic "Network adapter 3"
APIC1(config-member)# exit
APIC1(config-cluster-interface)# exit
APIC1(config-cluster)#
```

Configuring Service VM Orchestration Using REST API

You can configure service VM orchestration using the REST API.

Configure service VM orchestration.

Example:

```
<vnsLDevVip contextAware="single-Context" devtype="VIRTUAL"
  dn="uni/tn-T0/lDevVip-NEW-HA-LDEV-20" funcType="GoTo" isCopy="no" mode="legacy-Mode"
  name="NEW-HA-LDEV-20" promMode="no" svcType="FW" trunking="no">
    <vnsLIf encap="unknown" name="client">
        <vnsRsMetaIf isConAndProv="no"
          tDn="uni/infra/mDev-CISCO-ASA-1.3/mIfLbl-external"/>
        <vnsRsCIfAttN
```

```
      tDn="uni/tn-T0/lDevVip-NEW-HA-LDEV-20/cDev-CDEV-HA-S1-NEW/cIf-[GigabitEthernet0/0]"/>
    <vnsRsCIfAttN
      tDn="uni/tn-T0/lDevVip-NEW-HA-LDEV-20/cDev-CDEV-HA-P1-NEW/cIf-[GigabitEthernet0/0]"/>
</vnsLIf>
<vnsLIf encap="unknown" name="server">
    <vnsRsMetaIf isConAndProv="no" tDn="uni/infra/mDev-CISCO-ASA-1.3/mIfLbl-internal"/>
    <vnsRsCIfAttN
      tDn="uni/tn-T0/lDevVip-NEW-HA-LDEV-20/cDev-CDEV-HA-S1-NEW/cIf-[GigabitEthernet0/1]"/>
    <vnsRsCIfAttN
      tDn="uni/tn-T0/lDevVip-NEW-HA-LDEV-20/cDev-CDEV-HA-P1-NEW/cIf-[GigabitEthernet0/1]"/>
</vnsLIf>
<vnsRsLDevVipToInstPol tDn="uni/tn-T0/svcCont/instPol-HA-POL"/>
<vnsRsALDevToDomP switchingMode="AVE" tDn="uni/vmmp-VMware/dom-mininet"/>
<vnsCDev cloneCount="0" host="10.197.146.188" isCloneOperation="no" isTemplate="no"
  name="CDEV-HA-S1-NEW" vcenterName="orionin103-vcenter1" vmName="ASA-S1-VM-20">
    <vnsHAPortGroup portGroupName="10.197.146.188 | VLAN2500-172-25"
      vnicName="Network adapter 10"/>
    <vnsDevFolder key="FailoverConfig" name="FailoverConfig">
        <vnsDevParam key="lan_unit" name="lan_unit" value="secondary"/>
        <vnsDevParam key="failover" name="failover" value="enable"/>
        <vnsDevFolder key="mgmt_standby_ip" name="mgmt_standby_ip">
            <vnsDevParam key="standby_ip" name="standby_ip" value="10.197.146.178"/>
        </vnsDevFolder>
        <vnsDevFolder key="polltime" name="polltime">
            <vnsDevParam key="interval_value" name="interval_value" value="1"/>
            <vnsDevParam key="interval_unit" name="interval_unit" value="second"/>
            <vnsDevParam key="holdtime_value" name="holdtime_value" value="3"/>
        </vnsDevFolder>
        <vnsDevFolder key="failover_link_interface" name="failover_link_interface">
            <vnsDevParam key="use_lan" name="use_lan" value="fover"/>
            <vnsDevParam key="interface_name" name="interface_name" value="fover"/>
            <vnsDevParam key="interface" name="interface" value="GigabitEthernet0/8"/>
        </vnsDevFolder>
        <vnsDevFolder key="failover_ip" name="failover_ip">
            <vnsDevParam key="interface_name" name="interface_name" value="fover"/>
            <vnsDevParam key="active_ip" name="active_ip" value="172.25.0.178"/>
            <vnsDevParam key="netmask" name="netmask" value="255.255.0.0"/>
            <vnsDevParam key="standby_ip" name="standby_ip" value="172.25.0.179"/>
        </vnsDevFolder>
        <vnsDevFolder key="failover_lan_interface" name="failover_lan_interface">
            <vnsDevParam key="interface_name" name="interface_name" value="fover"/>
            <vnsDevParam key="interface" name="interface" value="GigabitEthernet0/8"/>
        </vnsDevFolder>
    </vnsDevFolder>
    <vnsCIf name="GigabitEthernet0/1" vnicName="Network adapter 3"/>
    <vnsCIf name="GigabitEthernet0/0" vnicName="Network adapter 2"/>
</vnsCDev>
<vnsCDev cloneCount="0" host="10.197.146.187" isCloneOperation="no" isTemplate="no"
  name="CDEV-HA-P1-NEW" vcenterName="orionin103-vcenter1" vmName="ASA-P1-VM-20">
    <vnsHAPortGroup portGroupName="10.197.146.187 | VLAN2500-172-25"
      vnicName="Network adapter 10"/>
    <vnsDevFolder key="FailoverConfig" name="FailoverConfig">
        <vnsDevParam key="lan_unit" name="lan_unit" value="primary"/>
        <vnsDevParam key="failover" name="failover" value="enable"/>
        <vnsDevFolder key="failover_ip" name="failover_ip">
            <vnsDevParam key="interface_name" name="interface_name" value="fover"/>
            <vnsDevParam key="standby_ip" name="standby_ip" value="172.25.0.179"/>
            <vnsDevParam key="netmask" name="netmask" value="255.255.0.0"/>
            <vnsDevParam key="active_ip" name="active_ip" value="172.25.0.178"/>
        </vnsDevFolder>
        <vnsDevFolder key="failover_lan_interface" name="failover_lan_interface">
            <vnsDevParam key="interface_name" name="interface_name" value="fover"/>
            <vnsDevParam key="interface" name="interface" value="GigabitEthernet0/8"/>
        </vnsDevFolder>
```

```
            <vnsDevFolder key="mgmt_standby_ip" name="mgmt_standby_ip">
                <vnsDevParam key="standby_ip" name="standby_ip" value="10.197.146.179"/>
            </vnsDevFolder>
            <vnsDevFolder key="failover_link_interface" name="failover_link_interface">
                <vnsDevParam key="interface_name" name="interface_name" value="fover"/>
                <vnsDevParam key="use_lan" name="use_lan" value="fover"/>
                <vnsDevParam key="interface" name="interface" value="GigabitEthernet0/8"/>
            </vnsDevFolder>
            <vnsDevFolder key="polltime" name="polltime">
                <vnsDevParam key="holdtime_value" name="holdtime_value" value="3"/>
                <vnsDevParam key="interval_unit" name="interval_unit" value="second"/>
                <vnsDevParam key="interval_value" name="interval_value" value="1"/>
            </vnsDevFolder>
        </vnsDevFolder>
        <vnsCIf name="GigabitEthernet0/1" vnicName="Network adapter 3"/>
        <vnsCIf name="GigabitEthernet0/0" vnicName="Network adapter 2"/>
    </vnsCDev>
    <vnsRsMDevAtt tDn="uni/infra/mDev-CISCO-ASA-1.3"/>
</vnsLDevVip>
```

Troubleshooting Service VM Orchestration

This section contains known issues and limitations with service VM orchestration and instructions for troubleshooting issues if they occur.

Service VM Templates Not Seen in VM Instantiation Policy

Complete the following steps if you do not see the service VM templates that were created on VMware vCenter in the VM Instantiation policy.

Step 1 Check Visore using **vnsInstPol** and look for `vmTemplate`.

If there is no value for **vnsInstPol** field or if the value is null, go to the next step.

Step 2 Trigger an inventory synchronization:

a) In Cisco Application Policy Infrastructure Controller (APIC), go to **Virtual Networking** > **Inventory** and expand the **VMM Domains** and **VMware** folders.

b) Click the VMM domain.

c) In the central pane, double-click the controller.

d) In the **VMM Controller** dialog box, from the hammer-and-wrench drop-down list, choose **Trigger Inventory Sync** and when prompted, click **Yes**.

Step 3 Check the virtual machine (VM) instantiation policy: Choose the controller that is mapped to the VMM domain, and see if the VM template is present.

Port Groups Created in VMware vCenter Do Not Appear for CDev

Complete the following steps if port groups created in VMware vCenter do not appear for a concrete device (CDev).

Step 1 Trigger an inventory synchronization:

a) In Cisco Application Policy Infrastructure Controller (APIC), go to **Virtual Networking** > **Inventory** and expand the **VMM Domains** and **VMware** folders.
b) Click the VMM domain.
c) In the central pane, double-click the controller.
d) In the **VMM Controller** dialog box, from the hammer-and-wrench drop-down list, choose **Trigger Inventory Sync** and when prompted, click **Yes**.

Step 2 Check if the port group appears:

a) Go to **Tenants** > ***tenant*** > **Services** > **L4-L7** > **Devices** > ***device*** and then click the device.

Step 3 In the **Concrete Device** work pane, check the **Port Group Name** drop-down list to see if a port group is present.

Unable to Reach Service VM IP Address

Complete the following steps if you cannot reach the service virtual machine (VM) IP address after deploying the service virtual machine (VM).

Step 1 In Cisco Application Policy Infrastructure Controller (APIC), check the service VM connectivity.

Cisco APIC cannot reach a Cisco Adaptive Security Virtual Appliance (ASAv) device after deletion and redeployment. This issue occurs because the old MAC address is not cleared in the upstream switches. Clear the MAC entry of the IP address that is used for service VMs and then redeploy the service VM.

Step 2 If device management uses vSwitch port groups, check all intermediate switches and devices between Cisco APIC and the VMware vCenter to see if VLANs and routes are present.

Cisco APIC should be able to ping the device IP address if the service VM was deployed successfully.

Step 3 Make sure that the correct port group or EPG is chosen for the management interface for the concrete device (CDev).

Step 4 Check connectivity to make sure that the service VM can reach the upstream gateway.

Device State Shows Init

Complete the following steps if the device state shows init.

Step 1 From the NX-OS style CLI, ping the service device to verify reachability.

Step 2 Verify that the login credentials to the service device match the username and password that are supplied in the device configuration.

Step 3 Verify that the service device's virtual IP address and port are open.

Step 4 Verify that the username and password are correct in the Cisco Application Policy Infrastructure Controller (APIC) configuration.

LIF Configuration Is Invalid

Complete the following steps if you see an F0772 fault saying that the logical interface (LIF) configuration is invalid because of `lif-invalid-Clf` in the logical device.

Step 1 Determine what items are called the LIF and the concrete interface (ClF).

With this particular fault, the LIF is the element that is not rendering properly. This is where the Function Node maps the LIF to the actual, or concrete, interface to form a relationship.

F0772 means one of the following problems:

- The LIF is not created.
- The LIF is not mapped to the correct concrete interface.

Step 2 For other Layer 4 to Layer 7 device state problems, see the troubleshooting content in this document.