Improving Cisco ACI Virtual Edge Availability with VMware vSphere Proactive HA

Improving Cisco ACI Virtual Edge Availability

You can use VMware vSphere Proactive HA in vCenter 6.5 and later to improve Cisco ACI Virtual Edge availability.

Cisco Application Policy Infrastructure Controller (APIC) and VMware work together to detect a nonworking Cisco ACI Virtual Edge, isolate its host, and move its virtual machines (VMs) to a working host. Otherwise, if Cisco ACI Virtual Edge crashes, all its VMs can lose network connectivity.

You enable and configure vSphere Proactive HA in VMware vCenter, and in Cisco APIC, where the feature is called **Host Availability Assurance**. You can specify the amount of time that Cisco ACI Virtual Edge is not working before its host is quarantined and its VMs are moved.

Note

- Permission of the Cisco APIC account that you use for registration on VMware vCenter must have administrator rights or right to access the Cisco Application Centric Infrastructure (ACI) vCenter plug-in.
- vSphere Proactive HA is not available for Cisco ACI Virtual Edge when it is part of Cisco ACI Virtual Pod.
- For Host Availability Assurance to work, the VMware vCenter account used to create the Cisco APIC vCenter domain must have "Health Provider" write permission on the VMware vCenter.

How Improving Availability with vSphere Proactive HA Works

When you enable Host Availability Assurance, Cisco APIC creates a vSphere Proactive HA provider object in VMware vCenter. The object enables VMware vCenter to quarantine a host with a nonworking Cisco ACI Virtual Edge and move VMs out of that host. In Cisco APIC, you also specify how aggressively you want to trigger quarantine. You perform these tasks when you create a vCenter domain for Cisco ACI Virtual Edge.

When Host Availability Assurance is configured and enabled, Cisco APIC monitors Cisco ACI Virtual Edge on VMware vCenter. It uses the VMware vCenter inventory and OpFlex status to determine if Cisco ACI Virtual Edge is in a good or bad state. If Cisco APIC detects that Cisco ACI Virtual Edge is in a bad state, it tells VMware vCenter to put the affected host into quarantine.

VMware vCenter puts a host in quarantine mode according to one of three remediation modes, which you configure for the cluster:

- **Quarantine**: Hosts with health at yellow and red levels are put into quarantine mode.

  Note In Cisco ACI Virtual Edge Release 2.1(1), you can ensure that VM groups are moved out of Cisco ACI Virtual Edge hosts when the hosts stop working. The configuration overrides any affinity groups that would otherwise keep the VMs with particular hosts. For more information, see the section *VM Group Quarantine Protection*, in this guide.

- **Mixed**: Hosts with health at the yellow level are put into quarantine mode; hosts with health at the red level are put into maintenance mode.

  Note Although you can choose mixed remediation mode in VMware vCenter, the resulting behavior is the same as quarantine remediation mode.

- **Maintenance**: Hosts with health at yellow and red levels are put into maintenance mode.

  Important Do not choose maintenance mode remediation when you use vSphere Proactive HA. Maintenance mode requires that Cisco ACI Virtual Edge be powered off, which prevents the host from ever returning to a healthy state. Only use quarantine or mixed mode.

VMware vCenter also moves the VMs on that host to a host with a working Cisco ACI Virtual Edge. However, hosts in quarantine still might run data VMs if no healthy host is available, and any VM pinned by Distributed Resource Scheduler (DRS) rules to a quarantined host stays on the host. VMware vCenter also avoids moving any VMs to a quarantined host. However, you can deploy new VMs on a host in quarantine.

Enabling vSphere Proactive HA in Cisco APIC

Improving Cisco Application Centric Infrastructure Virtual Edge in Cisco Application Policy Infrastructure Controller (APIC) consists of the following tasks:

- Enabling host availability assurance on the Cisco Application Centric Infrastructure (ACI) Virtual Edge VMM domain
- Specifying the time period before VMware vCenter quarantines any hosts on with Cisco ACI Virtual Edge has stopped working

You can perform these tasks in the Cisco APIC GUI when you create a vCenter domain for Cisco ACI Virtual Edge. See the section Create a VMM Domain Profile for Cisco ACI Virtual Edge in this guide for instructions.

You can perform these tasks with the NX-OS style CLI and REST API instead of the Cisco APIC GUI. See the sections Enabling vSphere Proactive HA Using NX-OS Style CLI, on page 3 and Enabling vSphere Proactive HA Using REST API, on page 4 in this guide.

Enabling vSphere Proactive HA Using NX-OS Style CLI

You can use the NX-OS style CLI to perform several tasks in Cisco Application Policy Infrastructure Controller (APIC):

- Enable host availability assurance, which creates a vSphere Proactive HA provider object that resides in VMware vCenter. The object enables VMware vCenter to quarantine a host with a nonworking Cisco Application Centric Infrastructure Virtual Edge and move its VMs.
- Set the time period before VMware vCenter quarantines the host with the nonworking Cisco ACI Virtual Edge and move VMs from the host.

Procedure

Step 1 Enable host availability assurance:

```
apic1# config
apic1(config)# vmware-domain mininet
apic1(config-vmware)# avail-monitor enable
apic1(config-vmware)# show run
# Command: show running-config vmware-domain mininet
# Time: Mon Aug  6 22:05:58 2018
  vmware-domain mininet
    vlan-domain member mininet type vmware
    vcenter 172.23.143.235 datacenter mininet dvs-version 6.0
      # username admin
      esx-avail-override 172.23.143.228 yellow
      exit
    configure-ave
      switching mode vxlan
      multicast-address 225.1.1.1
      vxlan multicast-pool 225.2.1.1-225.2.1.100
      exit
    avail-monitor enable
    exit
apic1(config-vmware)#
```

Step 2 Set the Cisco ACI Virtual Edge timeout:

```
apic1# config
apic1(config)# vmware-domain mininet
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# ave-timeout 10
```

You can choose any value between 10 and 100 seconds, inclusive. The default is 30 seconds.

What to do next

Enable the VMware vSphere Proactive HA feature in VMware vCenter if you have not done so already. See the section Enabling vSphere Proactive HA in VMware vCenter, on page 5 in this guide.

You can set a state for a given host to override the default state, which is based on the health of the Cisco ACI Virtual Edge. See the section Manually Setting the Health Level of the ESXi Host, on page 5.

Enabling vSphere Proactive HA Using REST API

You can use REST API to perform several tasks in Cisco Application Policy Infrastructure Controller (APIC):

- Enable host availability assurance, which creates a vSphere Proactive HA provider object that resides in VMware vCenter. The object enables VMware vCenter to quarantine a host with a nonworking Cisco Application Centric Infrastructure Virtual Edge and move its VMs.
- Set the time period before VMware vCenter quarantines the host with the nonworking Cisco ACI Virtual Edge and move VMs from the host.

Procedure

Step 1 Enable host availability assurance:

```
{{ifc}}/api/node/mo/.xml
<polUni>
  <vmmProvP vendor="VMware”  >
      <vmmDomP name="mininet" hvAvailMonitor=”yes”>
 </vmmDomP>
  </vmmProvP>
</polUni>
```

Step 2 Set the Cisco ACI Virtual Edge timeout:

```
{{ifc}}/api/node/mo/.xml
<polUni>
  <vmmProvP vendor="VMware">
      <vmmDomP name="mininet” aveTimeOut=”10">
      </vmmDomP>
  </vmmProvP>
</polUni>
```

You can choose any value between 10 and 100 seconds, inclusive. The default is 30 seconds.

What to do next

Enable the VMware vSphere Proactive HA feature in VMware vCenter if you have not done so already. See the section Enabling vSphere Proactive HA in VMware vCenter, on page 5 in this guide.

You can set a state for a given host to override the default state, which is based on the health of the Cisco ACI Virtual Edge. See the section Manually Setting the Health Level of the ESXi Host, on page 5.

Enabling vSphere Proactive HA in VMware vCenter

Before you begin

Using vSphere Proactive High Availability (HA) requires VMware vCenter 6.5 or later.

Procedure

Step 1 Log in to the VMware vCenter Web Client.

Step 2 Choose **Home** > **Host and Cluster** > ***cluster*** > **Configure** > **Edit**.

Step 3 In the **Edit Cluster Settings** dialog box, choose **vSphere Availability** in the left navigation pane and then check the **Turn on Proactive HA** check box in the work pane.

Step 4 In the left navigation pane, choose **Proactive HA Failures and Responses**complete the following steps:

a) From the **Remediation** drop-down list, choose a remediation level.

   You can choose one of three levels: **Quarantine**, which puts hosts with yellow and red levels into quarantine mode; **Mixed**, which puts yellow hosts into quarantine mode and red hosts into maintenance mode; and **Maintenance**, which puts yellow and red hosts into maintenance mode.

b) Check the check box next to the vSphere Proactive HA provider to enable it.

   The Cisco Application Policy Infrastructure Controller (APIC)-created provider would have "vmm-domain-name_APIC" as its name.

Manually Setting the Health Level of the ESXi Host

By default, the state of the VMware host is determined by the state of the Cisco Application Centric Infrastructure (ACI) Virtual Edge that resides on it.

You might want to override the default if you must do maintenance on the Cisco Application Centric Infrastructure Virtual Edge. Setting the host state to yellow or red while Cisco ACI Virtual Edge is working properly puts the corresponding host into quarantine mode.

Or you might not want a specific host to go into quarantine, even if the Cisco ACI Virtual Edge on it goes down. Setting the state to green keeps the host active, disabling vSphere Proactive HA on the host.

Setting the health state manually to green prevents Cisco Application Policy Infrastructure Controller (APIC) from changing host status to yellow or red. You can set the health state using the Cisco APIC GUI, NX-OS style CLI, or REST API.

Setting a State on the Cisco ACI Virtual Edge Host Using the Cisco APIC GUI

Before you begin

- You must have a host that contains Cisco ACI Virtual Edge.

- Host Availability Assurance must be enabled for the VMM domain on Cisco Application Policy Infrastructure Controller (APIC).

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Go to **Virtual Networking** > **Inventory** > **VMM Domains** > **VMware** > *VMM domain* > **Controllers** and click the controller.

Step 3 In the **Controller Instance** work pane, in the **Health Policy** area, click the **+** (plus icon).

Step 4 Enter the host IP address and the state that you want to set, and then click **Update**.

Step 5 Click **Submit**.

Setting a State on the Cisco ACI Virtual Edge Host Using NX-OS Style CLI

Before you begin

You must have a host that contains Cisco ACI Virtual Edge.

Procedure

Set a state for the host:

```
apic1# config
apic1(config)# vmware-domain mininet
apic1(config-vmware)# vcenter 192.168.0.235 datacenter apic1(config-vmware)# vcenter
172.23.143.235 datacenter mininet
apic1(config-vmware-vc)# esx-avail-override 192.168.0.1 yellow
apic1(config-vmware-vc)# show run
# Command: show running-config vmware-domain mininet vcenter 192.168.0.235 datacenter
 mininet
# Time: Mon Aug  6 23:47:17 2018
  vmware-domain mininet
    vcenter 192.168.0.235 datacenter mininet dvs-version 6.0
      # username admin
      esx-avail-override 192.168.0.1 yellow
      exit
    exit
apic1(config-vmware-vc)#
```

Setting a State on the Cisco ACI Virtual Edge Host Using REST API

Before you begin

You must have a host that contains Cisco ACI Virtual Edge.

Procedure

Set a state for the host:

```
{{ifc}}/api/node/mo/.xml
<polUni>
  <vmmProvP vendor="VMware">
      <vmmDomP name="mininet">
         <vmmCtrlrP name="vc65.xyz.com">
        <vmmHvAvailPol>
       <vmmHvDesiredSt host=”172.23.143.228" state="yellow"/>
        </vmmHvAvailPol>
         </vmmCtrlrP>
     </vmmDomP>
  </vmmProvP>
</polUni>
```