Configuring Policy Based Redirect

Policy-Based Redirect

Cisco Application Centric Infrastructure (ACI) policy-based redirect (PBR) enables provisioning service appliances, such as firewalls or load balancers, as managed or unmanaged nodes without requiring a Layer 4 to Layer 7 package. Typical use cases include provisioning service appliances that can be pooled, tailored to application profiles, scaled easily, and have reduced exposure to service outages. PBR simplifies the deployment of service appliances by enabling the provisioning consumer and provider endpoint groups to be all in the same virtual redirect and forwarding (VRF) instance.

PBR deployment consists of configuring a route redirect policy and a cluster redirect policy, and creating a service graph template that uses the route and cluster redirect policies. After the service graph template is deployed, use the service appliance by enabling endpoint groups to consume the service graph provider endpoint group. This can be further simplified and automated by using vzAny. While performance requirements may dictate provisioning dedicated service appliances, virtual service appliances can also be deployed easily using PBR.

Creating Layer 4-Layer 7 Policy Based Redirect

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Policy Based Redirect**.

Step 7 Click **Add**.

Step 8 On the **Create Policy Based Redirect** screen, complete the following fields:

- Enter a unique name and description for the Policy Based Redirect.
- Check the **Enable Pod ID Aware Redirection** check box to enable pod ID aware redirection and associate the pod IDs with the preferred PBR nodes to program redirect destinations in the leaf switches located in the specific pods.
- Choose one of the following hashing algorithms:
  - dip—Destination IP address
  - sip—Source IP address
  - sip-dip-prototype—Source IP address, Destination IP address and Protocol Type (also called Symmetric) based algorithm
- Check the **Resilient Hashing Enabled** check box to enable resilient hashing for mapping traffic flows to physical nodes and for avoiding the rehashing of any traffic other than the flows from the failed node.
- Check the **Anycast Endpoint** check box to enable anycast endpoint.
- Click **Select** and check the IP SLA monitoring policy that you want to use for PBR tracking.
- The **Threshold Enable** check box appears when you choose an IP SLA monitoring policy. Check this check box to enable threshold when you want to disable the redirect destination group completely and prevent any redirection. When there is no redirection, the traffic is directly sent between the consumer and the provider. The following threshold settings are available:
  - **Min Threshold Percent (Percentage)** field—Enter the minimum threshold percentage. If the traffic goes below the minimum percentage, the packet is permitted instead of being redirected. The default value is 0. The allowed threshold range is from 0 to 100.
  - **Max Threshold Percent (Percentage)** field—Enter the maximum threshold percentage. When the minimum threshold is reached, to revert to the operational state, the maximum threshold percentage must be reached first. The default value is 0. The allowed threshold range is from 0 to 100.
  - **Threshold Down Action** drop-down list—Choose **permit action** or **deny action** from the drop-down list to apply the threshold settings on traffic.

Step 9 Click **Submit**.

Creating Layer 4 - Layer 7 Redirect Health Group

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **L4 L7 Redirect Health Group**.
Step 7 Click **Add**.

Step 8 On the **Create L4-L7 Redirect Health Group** screen, enter a unique name and description for L4-L7 Redirect Health Group.

Step 9 Click **Submit**.

When a redirect health group is no longer consumed by the PBR, you can delete the redirect health group. To delete the redirect health group, click the row with the redirect health group on the **L4 L7 Redirect Health Group** screen and click **Delete**.

Creating a Destination of Redirect Traffic

Before you begin

The redirect health group that needs to be associated with the redirect traffic is created.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Policy Based Redirect**.

Step 7 Click the row with the L4-L7 policy based rediect record that you want to update and click **View Details**.

Step 8 Click **Destination of Redirect Traffic**.

Step 9 Click **Add**.

Step 10 On the **Add Destination of Redirected Traffic** screen, complete the following fields:

- Enter the IP address for the Layer 4 to Layer 7 device. The IP address must be in the same subnet as the IP address that you have given to the bridge domain.
- Enter a short description for the destination of redirected traffic.
- Enter the MAC address for the Layer 4 to Layer 7 device. You should use a MAC address that is valid upon failover of the Layer 4 to Layer 7 device.
- Enter the secondary IP address for the Layer 4 to Layer 7 device.
- Enter the pod identification value. By default, 1 is set as the pod ID. The valid pod ID range is from 1 to 255.
- Click **Select** and check the check box for the redirect health group that you want to associate to an existing health group.

Step 11 Click **Submit**.

Creating an IP SLA Monitoring Policy

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **IP SLA Monitoring Policy**.

Step 7 Click **Add**.

Step 8 On the **Create IP SLA Monitoring Policy** screen, complete the following fields:

a) Enter a unique name and description for the IP SLA Monitoring Policy.

b) In the **SLA Frequency** field, enter the interval probe time to track a packet. The allowed SLA frequency range is 1 to 65535 seconds. The default value is 60 seconds.

c) Choose **icmp** or **tcp** as the SLA type. If you choose **tcp**, then enter the SLA port number in the **SLA Port** field.

Step 9 Click **Submit**.