Managing Kubernetes Policies

The following sections provide information about the IKS policies that you can configure on Intersight:

Creating Add-on Policy

Add-ons are Kubernetes applications that provide enhanced features to Kubernetes clusters.

Many of the core add-ons are automatically created when you deploy a cluster. For example, nginx-ingress, cert-manager, and metallb. Optional add-ons can be added any time later according to your requirement. For example, logging, monitoring, and UI dashboard for management.

To create an add-on policy:

Step 1 In the left pane, click **Policies**.
The **Policies** screen appears, displaying the list of available policies.

Step 2 Click **Create Policy** to create a new policy.

Step 3 In the **Select Policy Type** screen, click **Kubernetes Cluster** > **Add-ons**, and then click **Start**.

Step 4 In the **General** screen:

a) From the **Organization** drop-down list, choose the default organization or a specific organization to which the policy should belong.

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

c) In the **Add Tag** field, enter the metadata that you want to associate with the policy.

Add Tag is an optional field. If you are adding a tag, you must enter the tag in the **`key:value`** format. This tag will be used internal to Intersight.

d) In the **Description** field, enter a description for the policy.
Description is an optional field.
e) Click **Next**.

Step 5 In the **Policy Details** screen, under **Add-ons**, click **Add Add-on**.

The **Add Add-on** dialog box appears.

a) From the **Add-on Definition** drop-down list, choose an add-on:
- **kubernetes-dashboard**: To deploy and manage your applications.
- **ccp-monitor**: To monitor the cluster.
- **efk**: To collect and monitor log data from your applications for troubleshooting purposes.

b) Skip the **Overrides** and **Override Sets** fields.
c) From the **Upgrade Strategy** field, select one of the following options:
- No Action
- Upgrade Only
- Reinstall on Failure
- Always Reinstall

d) Click **Add**.
e) If you want to include more add-ons in the policy, repeat these steps for each add-on.
f) Click **Create**.

The newly created policy is displayed in the **Policies** screen.

Creating Container Runtime Policy

The policy for Container Runtime enables you to configure the proxy settings for a cluster profile.

To create a Container Runtime policy:

Step 1 In the left pane, click **Policies**.
The **Policies** screen appears, displaying the list of available policies.

Step 2 Click **Create Policy** to create a new policy.

Step 3 In the **Select Policy Type** screen, click **Kubernetes Cluster** > **Container Runtime**, and then click **Start**.

Step 4 In the **General** screen:

a) From the **Organization** drop-down list, choose the default organization or a specific organization to which the policy should belong.
b) In the **Name** field, enter a name for the policy.
c) In the **Add Tag** field, enter the metadata that you want to associate with the policy.
Add Tag is an optional field. If you are adding a tag, you must enter the tag in the `key:value` format. This tag will be used internal to Intersight.

d) In the **Description** field, enter a description for the policy.
Description is an optional field.

e) Click **Next**.

Step 5 In the **Policy Details** screen:

a) Under **Docker HTTP Proxy**:

1. From the **Protocol** drop-down list, choose the protocol for the HTTP proxy server.
2. In the **Hostname** field, enter the FQDN or IP address of the HTTP proxy server.
3. In the **Port** field, enter the port number for the HTTP proxy server.
4. In the **Username** field, enter the username of the HTTP proxy server.
5. In the **Password** field, enter the password of the HTTP proxy server.

b) Under **Docker HTTPS Proxy server**:

1. From the **Protocol** drop-down list, choose the protocol for the HTTPS proxy server.
2. In the **Hostname** field, enter the FQDN or IP address of the HTTPS proxy server.
3. In the **Port** field, enter the port number for the HTTPS proxy server.
4. In the **Username** field, enter the username of the HTTPS proxy server.
5. In the **Password** field, enter the password of the HTTPS proxy server.
6. In the **Docker Bridge Network CIDR** field, enter a valid CIDR to override the default Docker bridge.
7. In the **Docker No Proxy** field, add the host that you want to exclude from proxy.

c) Click **Create**.

The newly created policy is displayed in the **Policies** screen.

Creating DNS, NTP, and Timezone Policy

The policy for DNS, NTP, and Timezone enables you to configure the DNS, NTP, and timezone for your cluster profile.

To create a DNS, NTP, and Timezone policy:

Step 1 In the left pane, click **Policies**.
The **Policies** screen appears, displaying the list of available policies.

Step 2 Click **Create Policy** to create a new policy.

Step 3 In the **Select Policy Type** screen, click **Kubernetes Cluster** > **DNS, NTP and Timezone**, and then click **Start**.

Step 4 In the **General** screen:

a) From the **Organization** drop-down list, choose the default organization or a specific organization to which the policy should belong.

b) In the **Name** field, enter a name for the policy.
c) In the **Add Tag** field, enter the metadata that you want to associate with the policy.

Add Tag is an optional field. If you are adding a tag, you must enter the tag in the **`key:value`** format. This tag will be used internal to Intersight.

d) In the **Description** field, enter a description for the policy.

Description is an optional field.

e) Click **Next**.

Step 5 In the **Policy Details** screen:

a) From the **Timezone** drop-down list, choose the timezone for the system clock of your node.
b) In the **DNS Suffix** field, enter the DNS search domain name.
c) In the **DNS Server** field, enter the IP address of the DNS server.
d) In the **NTP Server** field, enter the IP address of the NTP server.
e) Click **Create**.

The newly created policy is displayed in the **Policies** screen.

Creating Kubernetes Version Policy

The policy for Kubernetes Version enables you to configure the Kubernetes version for your cluster profile.

To create a Kubernetes version policy:

Step 1 In the left pane, click **Policies**.
The **Policies** screen appears, displaying the list of available policies.

Step 2 Click **Create Policy** to create a new policy.

Step 3 In the **Select Policy Type** screen, click **Kubernetes Cluster** > **Kubernetes Version**, and then click **Start**.

Step 4 In the **General** screen:

a) From the **Organization** drop-down list, choose the default organization or a specific organization to which the policy should belong.
b) In the **Name** field, enter a name for the policy.
c) In the **Add Tag** field, enter the metadata that you want to associate with the policy.

Add Tag is an optional field. If you are adding a tag, you must enter the tag in the **`key:value`** format. This tag will be used internal to Intersight.

d) In the **Description** field, enter a description for the policy.

Description is an optional field.

e) Click **Next**.

Step 5 In the **Policy Details** screen:

a) Choose the Kubernetes version that you want to attach to this policy.
b) Click **Create**.

The newly created policy is displayed in the **Policies** screen.

Creating Network CIDR Policy

The policy for Network CIDR enables you to configure the internal networks in a Kubernetes cluster.

To create a network CIDR policy:

Step 1 In the left pane, click **Policies**.

The **Policies** screen appears, displaying the list of available policies.

Step 2 Click **Create Policy** to create a new policy.

Step 3 In the **Select Policy Type** screen, click **Kubernetes Cluster** > **Network CIDR**, and then click **Start**.

Step 4 In the **General** screen:

a) From the **Organization** drop-down list, choose the **`default`** organization or a specific organization to which the policy should belong.

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

c) In the **Add Tag** field, enter the metadata that you want to associate with the policy.

Add Tag is an optional field. If you are adding a tag, you must enter the tag in the **`key:value`** format. This tag will be used internal to Intersight.

d) In the **Description** field, enter a description for the policy.

Description is an optional field.

e) Click **Next**.

Step 5 In the **Policy Details** screen:

a) In the **Service CIDR** field, enter the CIDR block from which the IP address for the cluster service can be allocated.

b) In the **Pod Network CIDR** field, enter the CIDR block from which the IP address for the pod network can be allocated.

c) Click **Create**.

The newly created policy is displayed in the **Policies** screen.

Creating Trusted Certificate Authorities Policy

The policy for Trusted Certificate Authorities enables you to configure the trusted certificates for your cluster profile.

To create a Trusted Certificate Authorities policy:

Step 1 In the left pane, click **Policies**.
The **Policies** screen appears, displaying the list of available policies.

Step 2 Click **Create Policy** to create a new policy.

Step 3 In the **Select Policy Type** screen, click **Kubernetes Cluster** > **Trusted Certificate Authorities**, and then click **Start**.

Step 4 In the **General** screen:

a) From the **Organization** drop-down list, choose the default organization or a specific organization to which the policy should belong.
b) In the **Name** field, enter a name for the policy.
c) In the **Add Tag** field, enter the metadata that you want to associate with the policy.

   Add Tag is an optional field. If you are adding a tag, you must enter the tag in the **`key:value`** format. This tag will be used internal to Intersight.

d) In the **Description** field, enter a description for the policy.

   Description is an optional field.

e) Click **Next**.

Step 5 In the **Policy Details** screen:

a) In the **Root CA Registries** field, add the root CS certificate that allows tenant clusters to securely connect to additional services.
b) In the **Unsigned Registries** field, add the docker registries created with unsigned certificates.
c) Click **Create**.

The newly created policy is displayed in the **Policies** screen.

Creating VM Instance Type Policy

The policy for VM Instance Type enables you to configure the system disk size, number of CPUs, and memory of the Virtual Machines.

To create a VM Instance Type policy:

Step 1 In the left pane, click **Policies**.
The **Policies** screen appears, displaying the list of available policies.

Step 2 Click **Create Policy** to create a new policy.

Step 3 In the **Select Policy Type** screen, click **Kubernetes Cluster** > **VM Instance Type**, and then click **Start**.

Step 4 In the **General** screen:

a) From the **Organization** drop-down list, choose the default organization or a specific organization to which the policy should belong.
b) In the **Name** field, enter a name for the policy.
c) In the **Add Tag** field, enter the metadata that you want to associate with the policy.

   Add Tag is an optional field. If you are adding a tag, you must enter the tag in the **`key:value`** format. This tag will be used internal to Intersight.

d) In the **Description** field, enter a description for the policy.

   Description is an optional field.

e) Click **Next**.

Step 5 In the **Policy Details** screen:

a) In the **CPU** field, enter the number of CPUs you want to allocate to the Virtual Machine.
b) In the **System Disk Size** field, enter the disk capacity along with its units.

For example, `10GiB`.

c) In the **Memory** field, enter the memory for the virtual machine in mebibytes.
d) Click **Create**.

The newly created policy is displayed in the **Policies** screen.

Creating Infra Provider Policy

The policy for Infra Provider enables you to configure the infrastructure provider that you want to use.

To create an Infra Provider policy:

Step 1 In the **General** screen:

a) From the **Organization** drop-down list, choose the default organization or a specific organization to which the policy should belong.
b) In the **Name** field, enter a name for the policy.
c) In the **Add Tag** field, enter the metadata that you want to associate with the policy.
Add Tag is an optional field. If you are adding a tag, you must enter the tag in the `key:value` format. This tag will be used internal to Intersight.
d) In the **Description** field, enter a description for the policy.
Description is an optional field.
e) Click **Next**.

Step 2 In the **Policy Details** screen:

a) If you want to use vCenter as the infrastructure provider:
   1. Click the **vCenter** tab.
   2. Select the infra provider from the table.
   3. In the **Datastore** field, enter the datastore that you want to use.
   4. In the **vSphere Admin Passphrase** field, enter the vSphere passphrase.
b) In the **Resource Pool** field, enter a resource pool.
c) In the **Interface** field, enter the name of the network you want to create the infra provider.
d) Click **Create**.

The newly created policy is displayed in the **Policies** screen.

Editing Kubernetes Cluster Policy

To edit a policy:

1. In the left pane, click **Policies**.

   The **Policies** screen appears, displaying the list of available policies.

2. Select the policy that you want to edit, and then click the **Edit** icon.

Deleting Kubernetes Cluster Policy

To delete a policy:

1. In the left pane, click **Policies**.

   The **Policies** screen appears, displaying the list of available policies.

2. Select the policy that you want to delete, and then click the **Delete** icon.