Alibaba Cloud
Aliyun Container for Kubernetes

FAQ

Issue: 20190410

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

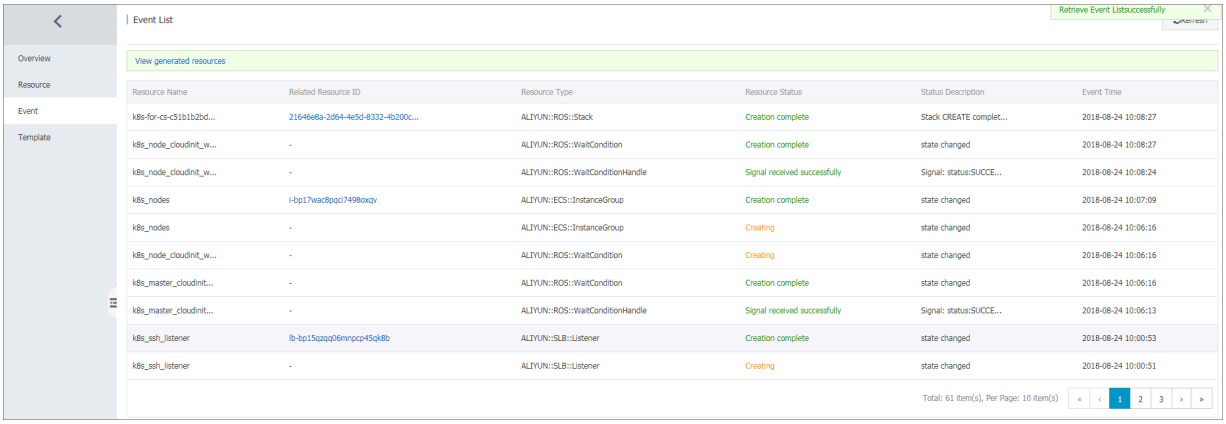
1 Failed to create a Kubernetes cluster

Check the cause of failure

You can check the cause of cluster creation failure by viewing the cluster creation events.

Log on to the *Resource Orchestration Service (ROS) console*.

Select the region where the cluster resides. Then, click Manage at the right of the cluster. In the left-side navigation pane, click Event. Rest the pointer on the failed event to view the specific error message of the failure.



Failure codes and solutions

- Resource CREATE failed: ResponseException: resources.k8s_SNat_Eip: Elastic IP address quota exceeded Code: QuotaExceeded.Eip

  Solution: Release unused EIPs, or open a ticket to raise the EIP quota.
- Resource CREATE failed: ResponseException: resources.k8s_master_slb_internet: The maximum number of SLB instances is exceeded. Code: ORDER.QUANTITY_INVALID

  Solution: Release unused SLB instances, or open a ticket to raise the SLB quota.
- Resource CREATE failed: ResponseException: resources.k8s_vpc: VPC quota exceeded. Code: QuotaExceeded.Vpc

  Solution: Release unused VPCs, or open a ticket to raise the VPC quota.

- Status Code: 403 Code: InvalidResourceType.NotSupported Message: This resource type is not supported;

  Solution: No ECS in stock or the type is not supported. Select other ECS specifications and try again.
- Resource CREATE failed: ResponseException: resources.k8s_master_1: The specified image does not support cloud-init. Code: ImageNotSupportCloudInit

  Solution: When a custom image is used to create a cluster, the custom image must be based on the latest CentOS image.
- Resource CREATE failed: ResponseException: resources.k8s_nodes: The resource is out of stock in the specified zone. Please try other types, or choose other regions and zones. Code: OperationDenied.NoStock

  Solution: The instances of your selected specifications are sold out. Select other availability zones or specifications, and try again.
- Resource CREATE failed: ResponseException: resources.k8s_NAT_Gateway: A route entry already exists, which CIDR is '0.0.0.0/0' Code: RouterEntryConflict. Duplicated

  Solution: Current route table of the VPC includes system route entries. Delete the system route entries, or clear the Configure SNAT for VPC check box, and try again.
- Resource CREATE failed: ResponseException: resources.KubernetesWorkerRole: The number of role is limited to 200. Code: LimitExceeded.Role

  Solution: The number of RAM roles has reached the quota. Delete some RAM roles, or open a ticket to raise the quota.
- Resource CREATE failed: ResponseException: resources.k8s_NAT_Gateway: The Account failed to create order. Code: OrderFailed

  Solution: Failed to create an order. Open a ticket for consultation.
- Resource CREATE failed: ResponseException: resources.k8s_master_1: This operation is forbidden by Aliyun RiskControl system. Code: Forbidden.RiskControl

  Solution: An exception occurs to your account. For more information, see *What do I do if I get a security notification?*.
- Resource CREATE failed: WaitConditionFailure: resources.k8s_node_cloudinit_wait_cond: See output value for more details.

  Solution: Failed to create a cluster. Try again later, or open a ticket for consultation.

- **Resource CREATE failed: WaitConditionTimeout: resources.k8s_master1_cloudinit_wait_cond: 0 of 2 received:**

  Solution: Failed to create a cluster. Try again later, or open a ticket for consultation.
- **Resource CREATE failed: ResponseException: resources.k8s_master_1: The request processing has failed due to some unknown error. Code: UnknownError**

  Solution: Unknown error. Try again later, or open a ticket for consultation.
- **Resource CREATE failed: ResponseException: resources.k8s_nodes: The request processing has failed due to some unknown error. Code: UnknownError**

  Solution: Unknown error. Try again later, or open a ticket for consultation.

2 Failed to delete Kubernetes clusters: ROS stack cannot be deleted

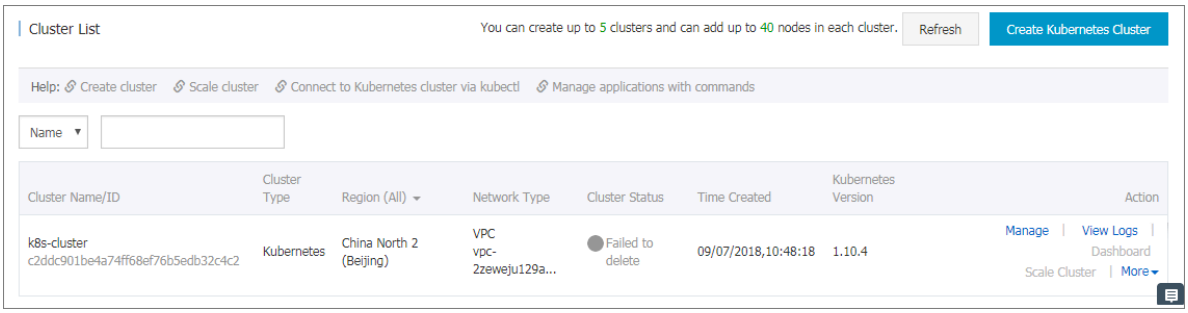
Root cause

Some resources are manually added (for example, manually add a VSwitch under the Virtual Private Cloud (VPC) created by Resource Orchestration Service (ROS)) under the resources created by ROS. ROS does not have permissions to delete those resources. This causes ROS to fail to process the VPC when deleting the Kubernetes resources and then the cluster fails to be deleted.

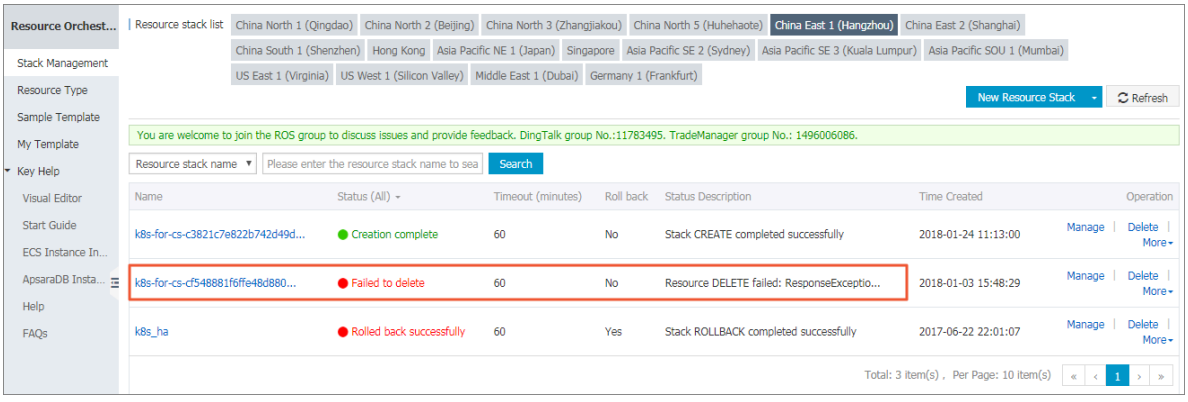
> **Note:**
> For more information about the resources automatically created by ROS when the Kubernetes cluster is created, see *Create a Kubernetes cluster*.

Solutions

1. If the cluster fails to be deleted (the cluster status is Failed to delete), go to the *ROS console*.

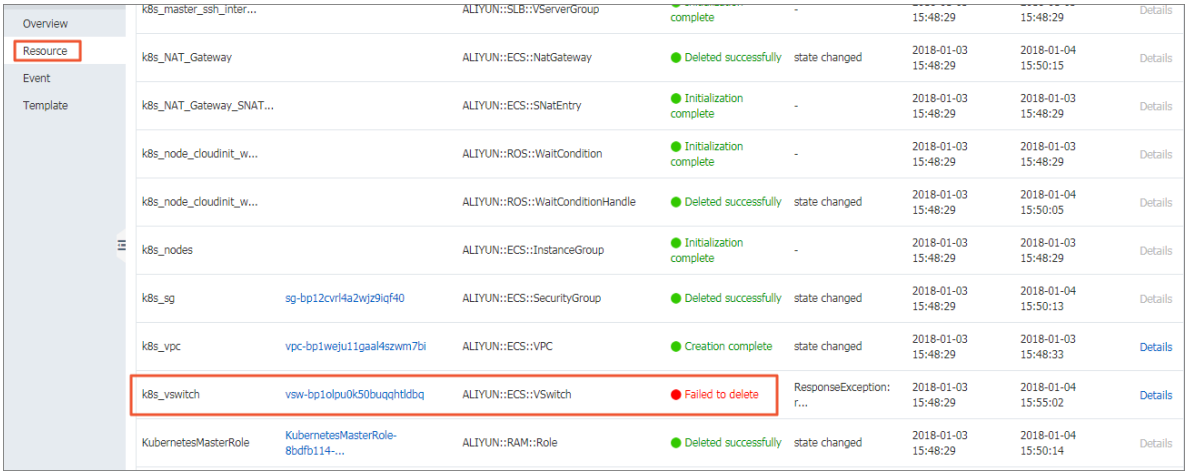


2. Select the region in which the cluster resides and find the stack `k8s - for - cs -{ cluster - id }` corresponding to the cluster. You can see the status is Failed to delete.



3. Click the stack name to go to the stack details page. Click Resource in the left-side navigation pane.

   You can see what resources failed to be deleted. In this example, the VSwitch under Server Load Balancer failed to be deleted.

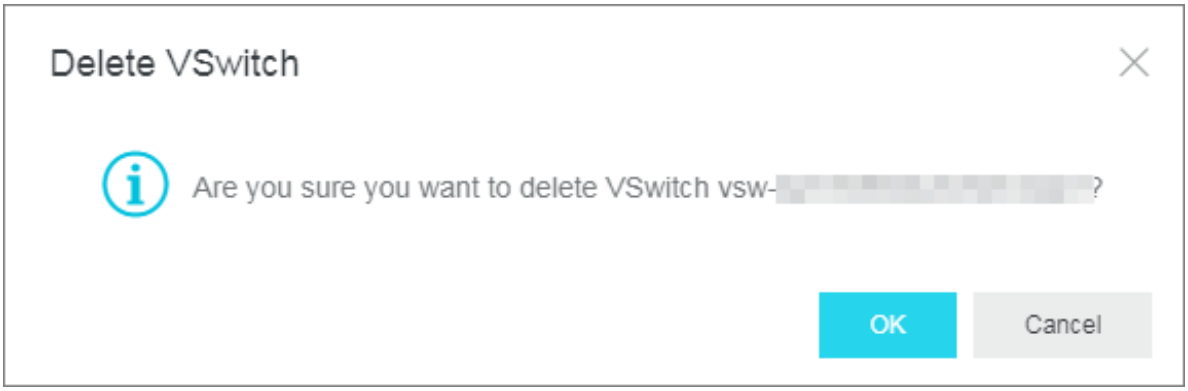


4. Go to the console in which the resource that failed to be deleted resides and find that resource.

   In this example, log on to the VPC console and find the VPC in which the cluster resides. Find the VSwitch that failed to be deleted under that VPC.

5. Click Delete at the right of the VSwtich to manually delete it.

   In this example, the VSwitch has resources to release and cannot be deleted.



   Manually release the resources under this VSwitch and try to delete this VSwitch again.

6. **Manually delete all the resources that failed to be deleted under the Kubernetes cluster in this way and try to delete the Kubernetes cluster again.**

3 How do I collect Kubernetes diagnosis information when a Kubernetes cluster exception or a cluster node exception occurs?

Context

If exceptions occur to the Kubernetes cluster, you need to collect diagnosis information on the Master node.

If exceptions occur to Worker nodes, you need to collect diagnosis information on the Master node and the abnormal Worker nodes.

Procedure

1. **Download the diagnosis script on the Master and Worker nodes, and add the permission to run the script.**

```
curl  - o  / usr / local / bin / diagnose_k  8s . sh   http ://
aliacs - k8s - cn - hangzhou . oss - cn - hangzhou . aliyuncs . com
/ public / diagnose / diagnose_k  8s . sh
chmod   u + x  / usr / local / bin / diagnose_k  8s . sh
```

2. **Run the diagnosis script.**

```
diagnose_k  8s . sh
......
+  echo  ' please   get   diagnose_1  514939155 . tar . gz   for
diagnostic  s '   ## The   name   of   a   generated   log   file
varies   each   time   when   you   run   the   diagnosis   script
.
 please   get   diagnose_1  514939155 . tar . gz   for
diagnostic  s
+  echo  ' upload   diagnose_1  514939155 . tar . gz '
 Upload   the   diagnose_1  514939155 . tar . gz   file .
```

3. **List and upload the generated log file.**

```
cd  / usr / local / bin
ls  - ltr | grep   diagnose_1  514939155 . tar . gz           ##
Replace   this   example   file   name   with   the   name   of
your   generated   log   file .
```

4 Upgrade Helm manually

Log on to the master node of the Kubernetes cluster, see *Connect to a Kubernetes cluster by using kubectl*.

Execute the following command:

```
helm init --tiller-image registry.cn-hangzhou.aliyuncs.com/acs/tiller:v2.11.0 --upgrade
```

The image address can use the VPC domain name of the region corresponding to the image. For example, the image address of a machine in the Hangzhou region can be replaced by registry-vpc.cn-hangzhou.aliyuncs.com/acs/tiller:v2.11.0.

Wait for `tiller` passing through health check. Then you can execute `helm version` to view the upgraded version.

Note:

Only the Helm server version is upgraded here. To use the Helm client, download the corresponding client binary.

Helm 2.11.0 client download address: *https://github.com/helm/helm/releases/tag/v2.11.0*. Currently, the latest version of Helm supported by Alibaba Cloud is 2.11.0.

After the Helm client and server are both upgraded, you can see the following information by executing the `helm version`:

```
$ helm version
Client: &version.Version{SemVer:"v2.11.0", GitCommit:"2e55dbe1fdb5fdb96b75ff144a339489417b146b", GitTreeState:"clean"}
Server: &version.Version{SemVer:"v2.11.0", GitCommit:"2e55dbe1fdb5fdb96b75ff144a339489417b146b", GitTreeState:"clean"}
```

5 How to use private images in Kubernetes clusters

```
kubectl create secret docker-registry regsecret --docker-server=registry-internal.cn-hangzhou.aliyuncs.com --docker-username=abc@aliyun.com --docker-password=xxxxxx --docker-email=abc@aliyun.com
```

where:

- regsecret: Specifies the secret key name and the name is customizable.
- —docker-server: Specifies the Docker repository address.
- —docker-username: Specifies the user name of the Docker repository.
- —docker-password: Specifies the logon password of the Docker repository.
- —docker-email: Specifies the email address (optional).

Add secret key parameters in the YML file.

```
containers:
  - name: foo
    image: registry-internal.cn-hangzhou.aliyuncs.com/abc/test:1.0
imagePullSecrets:
  - name: regsecret
```

where:

- `imagePullSecrets` declares that a secret key must be specified when you pull the image.
- `regsecret` must be the same as the preceding secret key name.
- The Docker repository name in `image` must be the same as that in `--docker-server`.

For more information, see the official documentation *Use private repository*.

Implement keyless orchestration

To avoid referencing keys each time when using private images to deploy, you can add secret to the default service account of namespace. For more information, see *Add ImagePullSecrets to a service account*.

First find the secret created to pull the private image.

```
# kubectl get secret regsecret
NAME          TYPE                                  DATA      AGE
```

```
regsecret     kubernetes . io / dockerconf  igjson     1
13m
```

In this example, manually configure the default service account default of the namespace to use this secret as the imagePullSecret.

Create a *sa . yaml* **configuration file to export the configurations of the service account default to this file.**

```
kubectl   get   serviceacc  ounts   default  - o   yaml  > ./ sa .
yaml

cat    sa . yaml

apiVersion :  v1
kind :  ServiceAcc  ount
metadata :
  creationTi  mestamp :  2015 - 08 - 07T22 : 02 : 39Z
  name :  default
  namespace :  default
  resourceVe  rsion : " 243024 "             ## Pay   attention   to
  this   item
  selfLink : / api / v1 / namespaces / default / serviceacc  ounts /
default
  uid :  052fb0f4 - 3d50 - 11e5 - b066 - 42010af0d7  b6
secrets :
-  name :  default - token - uudgeoken - uudge
```

Execute the `vim   sa . yaml` **command to delete resourceVersion and add the secret configuration item, imagePullSecrets which is used to pull images. The modified configuration is as follows:**

```
apiVersion :  v1
kind :  ServiceAcc  ount
metadata :
  creationTi  mestamp :  2015 - 08 - 07T22 : 02 : 39Z
  name :  default
  namespace :  default
  selfLink : / api / v1 / namespaces / default / serviceacc  ounts /
default
  uid :  052fb0f4 - 3d50 - 11e5 - b066 - 42010af0d7  b6
secrets :
-  name :  default - token - uudge
imagePullS  ecrets :                ## Add   this   item
-  name :  regsecret
```

Use the *sa . yaml* **configuration file to replace the service account configurations of default.**

```
kubectl   replace   serviceacc  ount   default  - f  ./ sa . yaml
```

```
serviceacc  ount  " default "  replaced
```

Execute the `kubectl create -f` **command to create a tomcat orchestration as an example.**

```
apiVersion :  apps / v1beta2  #  for  versions  before  1 . 8 . 0
  use  apps / v1beta1
kind :  Deployment
metadata :
  name :  tomcat - deployment
  labels :
    app :  tomcat
spec :
  replicas :  1
  selector :
    matchLabel  s :
      app :  tomcat
  template :
    metadata :
      labels :
        app :  tomcat
    spec :
      containers :
     -  name :  tomcat
        image :  registry - internal . cn - hangzhou . aliyuncs . com
/ abc / test : 1 . 0              # Replace  this  with  your
own  private  image  address
        ports :
       -  containerP  ort :  8080contai  nerPort :  8080
```

If you have configured properly, the pod starts successfully. Execute the `kubectl get pod tomcat - xxx - o yaml` **command. The following configuration items are displayed:**

```
spec :
  imagePullS  ecrets :
 -  nameregsec  retey
```

6 Volume FAQ

What do I do if a volume cannot be mounted to the Kubernetes cluster?

Check whether the flexvolume plugin is installed

Run the following command on the Master node:

```
# kubectl get pod -n kube-system | grep flexvolume

flexvolume-4wh8s              1/1     Running     0
  8d
flexvolume-65z49              1/1     Running     0
  8d
flexvolume-bpc6s              1/1     Running     0
  8d
flexvolume-l8pml              1/1     Running     0
  8d
flexvolume-mzkpv              1/1     Running     0
  8d
flexvolume-wbfhv              1/1     Running     0
  8d
flexvolume-xf5cs              1/1     Running     0
  8d
```

If the flexvolume plugin is installed, check whether flexvolume pods is running and that the number of running pods is the same as the number of nodes.

If no flexvolume plugin is installed, see *Install the plug-in*.

If the flexvolume pod is not running, see the running logs of the plugin to further analyze the cause.

Check whether the dynamic storage plugin is installed

To use the dynamic storage function of a cloud disk, you must install the dynamic storage plugin. Run the following command to check whether the dynamic storage plugin is installed:

```
# kubectl get pod -n kube-system | grep alicloud-
disk

alicloud-disk-controller-8679c9fc76-lq6zb       1/1
Running     0     7d
```

If no dynamic storage plugin is installed, see *Install the plug-in*.

If the pod is not running, see the running logs of the plugin to further analyze the cause.

How do I view storage logs?

View flexvolume logs by running commands on Master1 node

Run the get command to view the error pod as follows:

```
# kubectl get pod -n kube-system | grep flexvolume
```

Run the log command to view the logs of the error pod as follows:

```
# kubectl logs flexvolume-4wh8s -n kube-system
# kubectl describe pod flexvolume-4wh8s -n kube-system

# The last several lines of the pod descriptio n
 describe the status of the pod . You can analyze
 errors according to the status of the pod .
```

View the driver logs of a cloud disk, NAS, and OSS:

```
# View the persistent logs on the host node .
# If a volume cannot be mounted to a pod , run the
   following command to view the address of the node
 where the pod resides :

# kubectl describe pod nginx-97dc96f7b-xbx8t | grep
 Node
 Node : cn-hangzhou . i-bp19myla3u vnt6zihejb / 192 . 168 . 247
 . 85
 Node-Selectors : < none >

# Log on to the node to view logs .

# ssh 192 . 168 . 247 . 85
# ls / var / log / alicloud / flexvolume *
 flexvolume _disk . log flexvolume _nas . log flexvolume _o #
 ss . log

 The logs mounted to the cloud disk , NAS , and OSS
 are displayed .
```

Run the following commands on Master1 node to view provsioner plugin logs

Run the get command to view the error pod as follows:

```
# kubectl get pod -n kube-system | grep alicloud-disk
```

Run the log command to view the logs of the error pod as follows:

```
# kubectl logs alicloud-disk-controller-8679c9fc76-lq6zb
 -n kube-system
# kubectl describe pod alicloud-disk-controller-
 8679c9fc76-lq6zb -n kube-system
```

```
# The last several lines of the pod descriptio n
 describe the status of the pod . You can analyze
 errors according to the status of the pod .
```

View kubelet logs

```
# If a volume cannot be mounted to a pod , run the
   following command to view the address of the node
 where the pod resides :

# kubectl describe pod nginx - 97dc96f7b - xbx8t | grep
 Node
 Node : cn - hangzhou . i - bp19myla3u vnt6zihejb / 192 . 168 . 247
 . 85
 Node - Selectors : < none >

# Log on to the node to view kubelet logs :

# ssh 192 . 168 . 247 . 85
# journalctl - u kubelet - r - n 1000 &> kubelet . log

# The value of - n indicates the number of log lines
   that you expect to display .
```

The preceding content describes the methods to obtain the logs of errors that occurred to flexvolume, provsioner, and kubelet. If you cannot fix the errors according to the logs, we recommend that you submit a ticket with the log informatio n for further consultation.

Cloud disk volume FAQ

What do I do if a cloud disk fails to be mounted to the cluster and a timeout error is displayed?

If the cluster node is added manually, this problem may be caused by insufficient STS permissions. We recommend that you manually configure RAM permissions. For more information, see *Use the instance RAM role in the console*.

What do I do if a cloud disk fails to be mounted to the cluster and a Size error is displayed?

Depending on the type of cloud disk you create, you must confirm that the following requirements are met:

Note:

- The minimum capacity of a basic cloud disk is 5 GiB.
- The minimum capacity of an Ultra disk is 20 GiB.
- The minimum capacity of an SSD disk is 20 GiB.

What do I do if a cloud disk fails to be mounted to the cluster and a zone error is displayed?

To mount a cloud disk to your Kubernetes cluster, you must select the cloud disk that is in the same region and zone as the ECS instances used by the Kubernetes cluster.

What do I do if the input/output error is displayed by the cloud disk after the system is upgraded?

1. **Upgrade the flexvolume to v1.9.7-42e8198 or later.**
2. **Recreate the faulty pods.**

Run the following command to upgrade the flexvolume:

```
# kubectl set image daemonset/flexvolume acs-flexvolume=
registry.cn-hangzhou.aliyuncs.com/acs/flexvolume:v1.9
.7-42e8198 -n kube-system
```

To obtain the latest flexvolume version, log on to the Container Registry console, click Search in the left-side navigation pane, and search for acs/flexvolume.

NAS volume FAQ

What do I do if it takes a long time to mount a NAS file system to a Kubernetes cluster?

This problem may occur if the NAS file system contains a large amount of data and you set the chmod parameter in the mount template. We recommend that you remove the chmod parameter setting.

What do I do if a NAS file system fails to be mounted to a Kubernetes cluster and a timeout error is displayed?

Check whether the NAS mount point and the cluster are in the same VPC. Otherwise, the NAS file system cannot be mounted to the cluster.

OSS volume FAQ

What do I do if an OSS bucket fails to be mounted to a Kubernetes cluster?

- **Check whether the submitted Access Key is valid.**
- **Check whether the URL used to mount the OSS bucket is accessible through network.**

What do I do if the OSS mount directory within the container becomes unavailable after the cluster is upgraded?

If you upgrade your Kubernetes cluster or restart a kubelet, the ossfs process restarts because the container network restarts.

After the ossfs process restarts, the mapping to the container directory from your host becomes invalid. In this case, you need to restart the container or recreate the pod.

We recommend that you configure the liveness probe for heath checks so that the container or pod can automatically restart when such a problem occurs. For more information, see *Use Alibaba Cloud OSS volumes*.

7 Do I select the Terway or Flannel plugin for my Kubernetes cluster network?

This topic describes Terway and Flannel, two network plugins provided by Container Service for creating a Kubernetes cluster. This information helps you select an appropriate network plugin when creating a cluster.

When you create a Kubernetes cluster, Alibaba Cloud Container Service provides two network plugins: Terway and Flannel.

- Flannel: a simple and stable community *Flannel* CNI plugin. Flannel works with the high-speed network of Alibaba Cloud VPC, providing a high-performance and stable container network for clusters. However, it provides only a few simple features. For example, it does not support the Kubernetes Network Policy.
- Terway: a network plugin developed by Alibaba Cloud Container service. It is fully compatible with Flannel, and can allocate Alibaba Cloud Elastic Network Interfaces (ENIs) to containers. It can also define the access policies between containers according to the Kubernetes Network Policy. In addition, it supports bandwidth limiting for individual containers. If you do not need to use a Network Policy, we recommend that you select Flannel. In other cases, we recommend that you select Terway. For more information, see *Terway network plugin*.

8 How to manually install alicloud-application-controller

By default, alicloud-application-controller is installed in Alibaba Cloud Container Service in version 1.10.4 and later to provide the release based on custom resource definition (CRD).

Note:

In the Kubernetes cluster of the latest version, alicloud-application-controller is installed by default. In Kubernetes clusters of old versions, manually install alicloud-application-controller and the oldest version of Kubernetes cluster must be 1.9.3.

Use the `kubectl create -f alicloud-applicatio n-controller.yml` command to deploy alicloud-application-controller. In *alicloud-applicatio n-controller.yml* , enter the following orchestration template:

```
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: alicloud-applicatio n-controller
  labels:
    owner: aliyun
    app: alicloud-applicatio n-controller
  namespace: kube-system
spec:
  replicas: 1
  selector:
    matchLabels:
      owner: aliyun
      app: alicloud-applicatio n-controller
  template:
    metadata:
      labels:
        owner: aliyun
        app: alicloud-applicatio n-controller
      annotations:
        scheduler.alpha.kubernetes.io/critical-pod: ''
    spec:
      tolerations:
      - effect: NoSchedule
        operator: Exists
        key: node-role.kubernetes.io/master
      - effect: NoSchedule
        operator: Exists
        key: node.cloudprovider.kubernetes.io/uninitialized
      containers:
       - name: alicloud-applicatio n-controller
         image: registry.cn-hangzhou.aliyuncs.com/acs/aliyun-app-lifecycle-manager:0.1-c8d5da8
```

```
            imagePullP  olicy :  IfNotPrese  nt
        serviceAcc  ount :  admin
```

9 Kubernetes cluster network failures caused by security group settings

This topic describes the Kubernetes cluster network failures caused by cluster security group settings, and provides corresponding resolutions.

Symptom

Containers cannot communicate with each other over the Kubernetes cluster network .

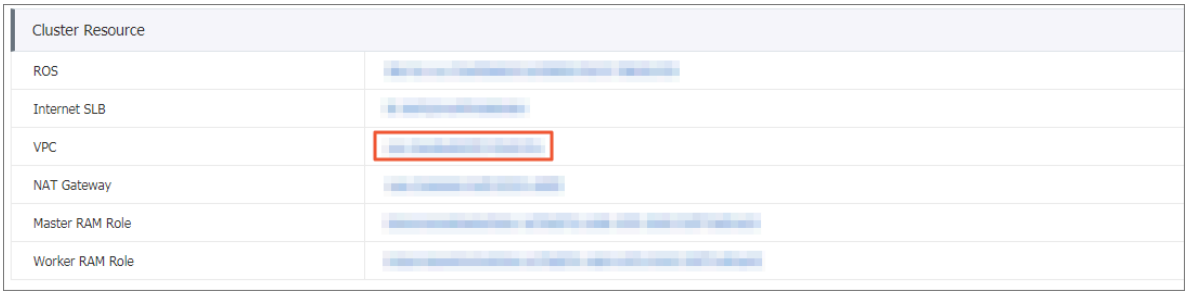
Causes

- A relevant ingress security group rule is removed. The following are the details of the rule: the ingress Authorization Objects is Pod Network CIDR and the Protocol Type is All.
- Newly added ECS instances and the Kubernetes cluster are located in different security groups.

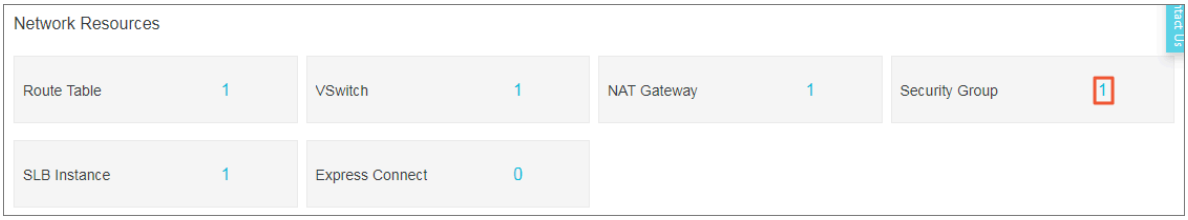
Resolution

Cause 1: A relevant ingress security group rule is removed. The following are details of the rule: the ingress Authorization Objects is Pod Network CIDR and the Protocol Type is All.

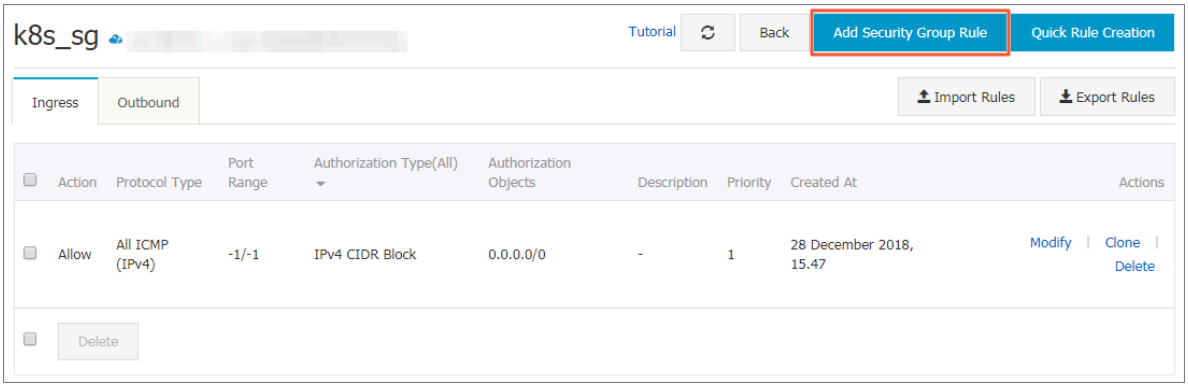
1. Log on to the *Container Service console*.
2. In the left-side navigation pane under Kubernetes, click Clusters.
3. Click the target cluster name to view cluster details.
4. In the Cluster Resource area, click VPC.



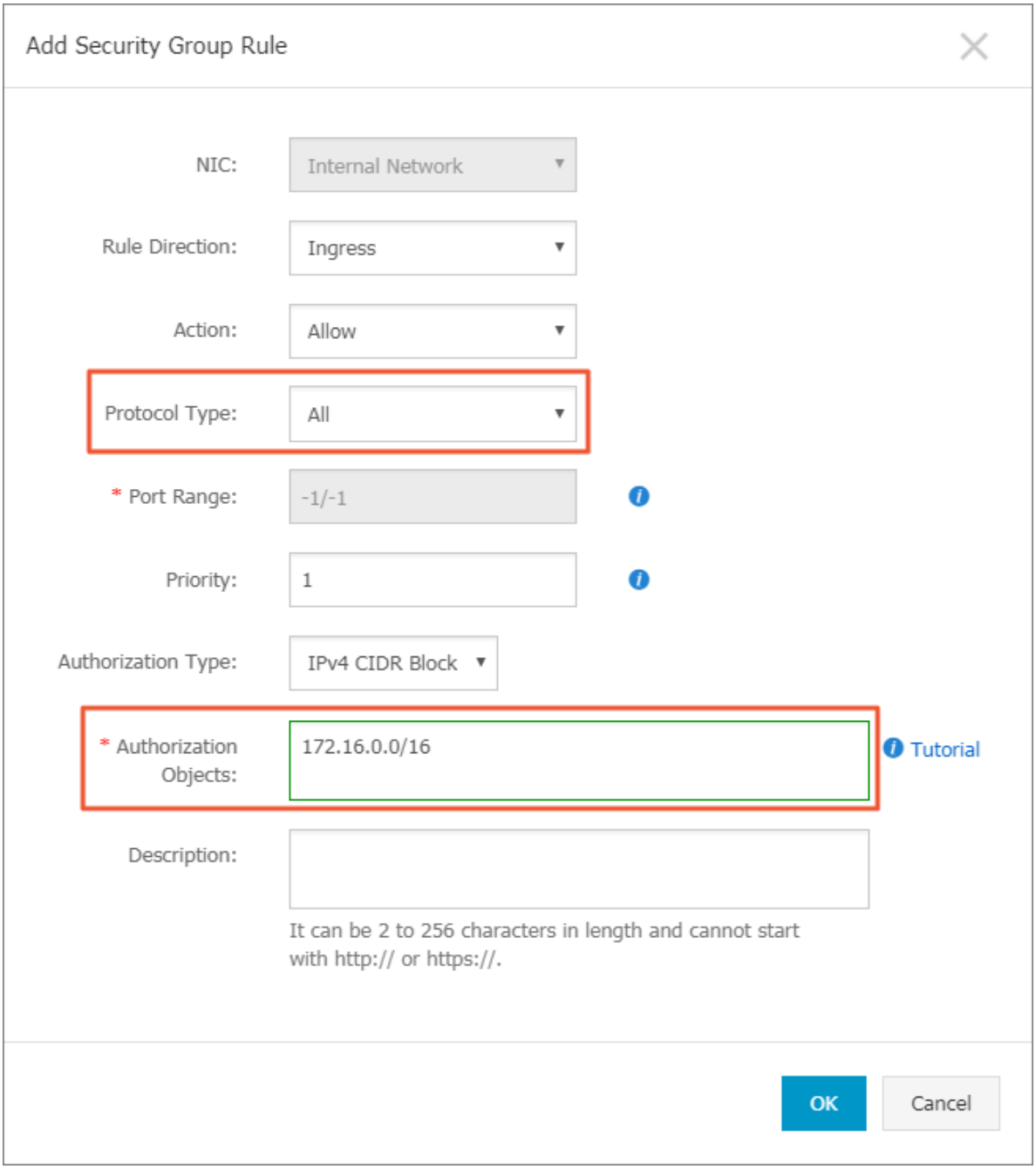
5. In the Network Resources area, click the number on the right of Security Group.



6. In the Actions column of the target security group, click Add Rules.
7. On the Ingress page, click Add Security Group Rule in the upper-right corner.



8. Set Protocol Type and Authorization Objects.

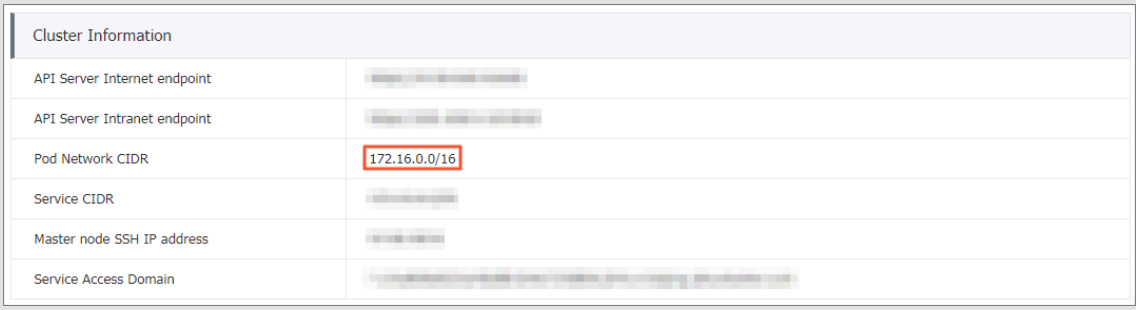


Select All from the Protocol Type drop-down list.

Enter the Pod Network CIDR of the Kubernetes cluster for Authorization Objects.

Note:

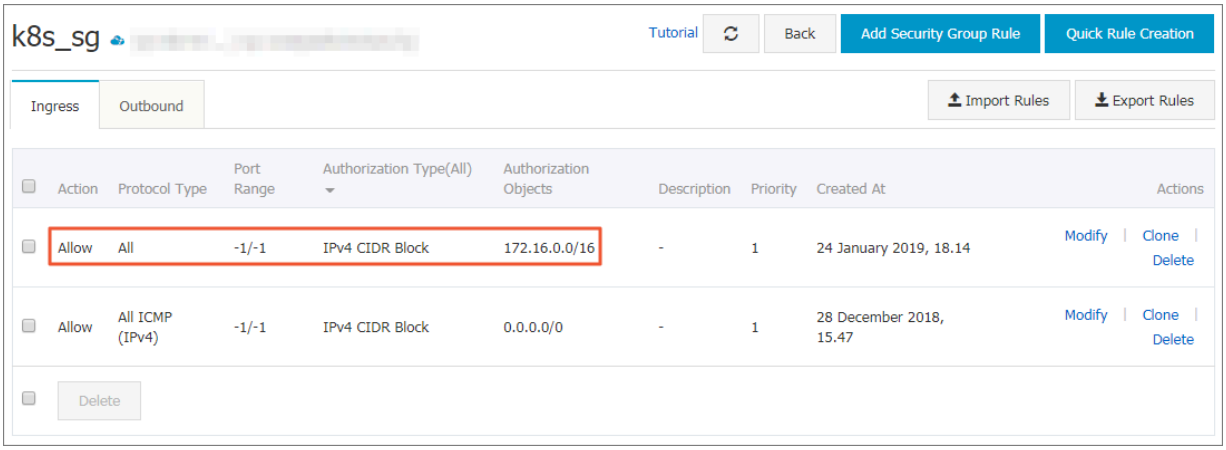
- You can view the Pod Network CIDR of the Kubernetes cluster in the Cluster Information area on the cluster basic information page.



- For more information about theAuthorization Objects settings, see *Scenarios*.

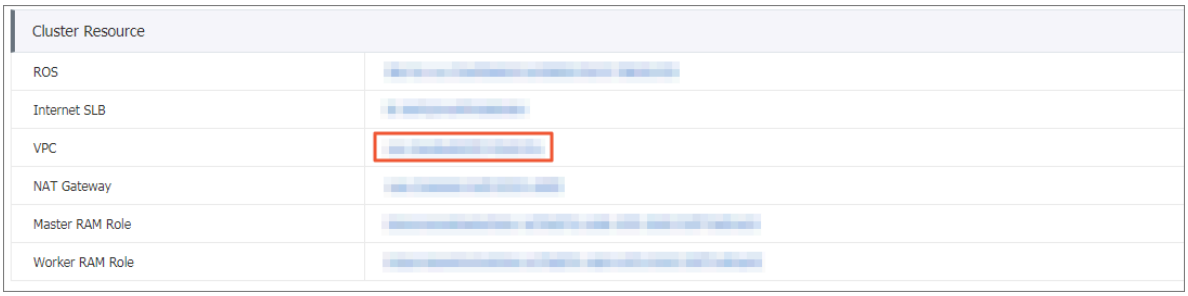
Verify the results

The required ingress security group rule is added. The following are details of the rule: the ingress Authorization Objects is Pod Network CIDR and the Protocol Type is All.

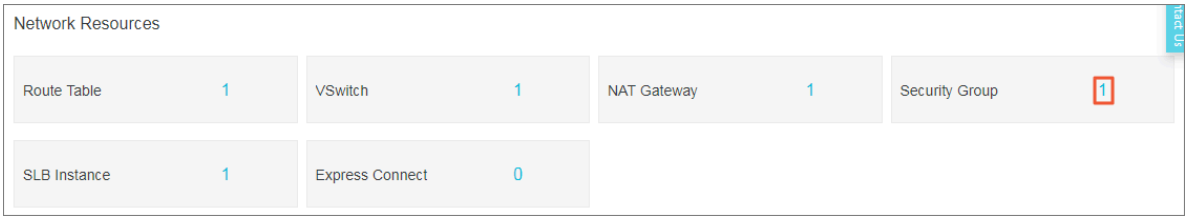


Cause 2: Newly added ECS instances and the Kubernetes cluster are located in different security groups.

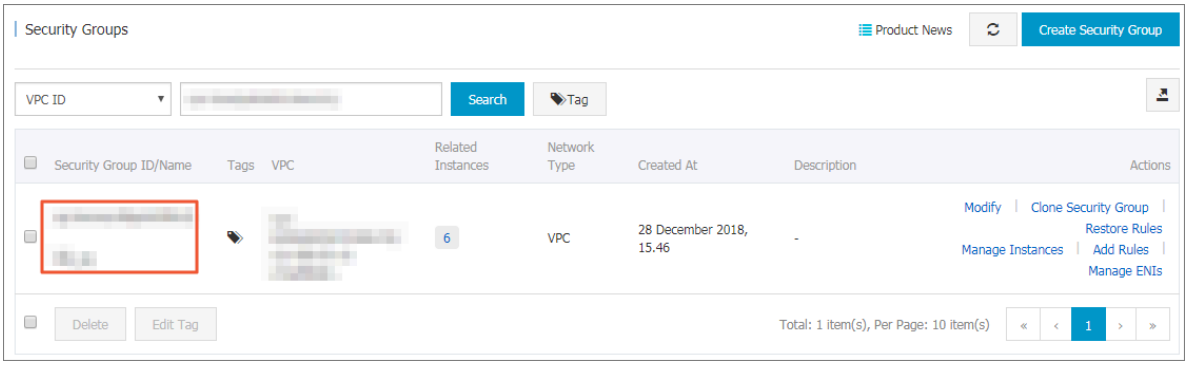
1. Log on to the *Container Service console*.
2. In the left-side navigation pane, click Clusters.
3. Click the target Cluster Name.
4. In the Cluster Resource area, click VPC.



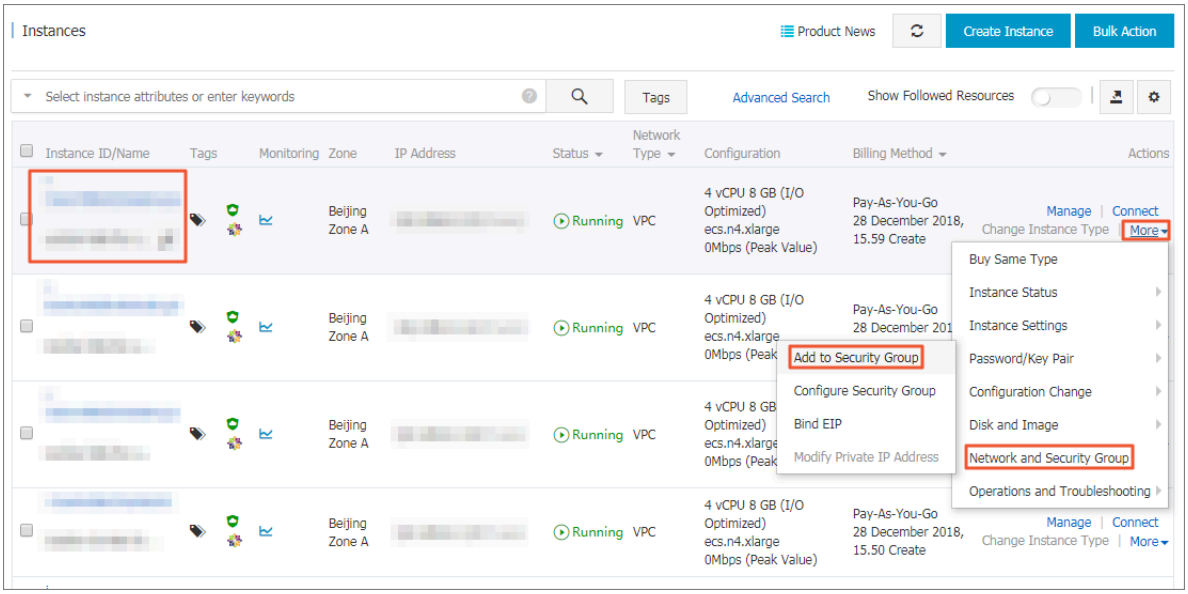
5. On the VPC Details page, click the number on the right of Security Group in the Network Resources area.



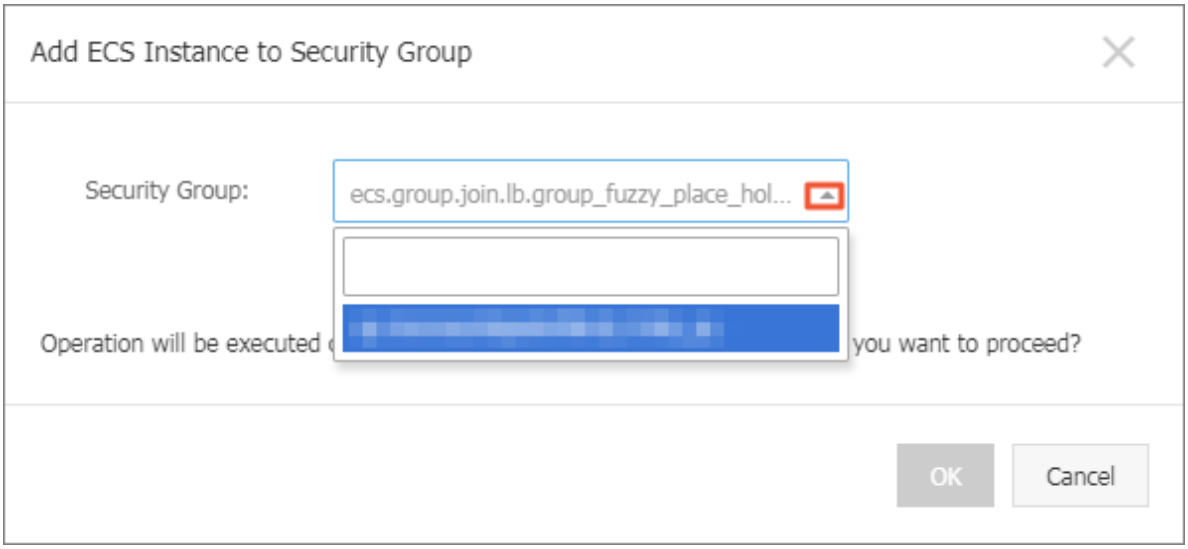
6. On the Security Groups page, view the target security group name.



7. In the Elastic Compute Service console, click Instances in the left-side navigation pane.
8. On the Instances page, choose More > Network and Security Group > Add to Security Group in the Actions column of the target instance.



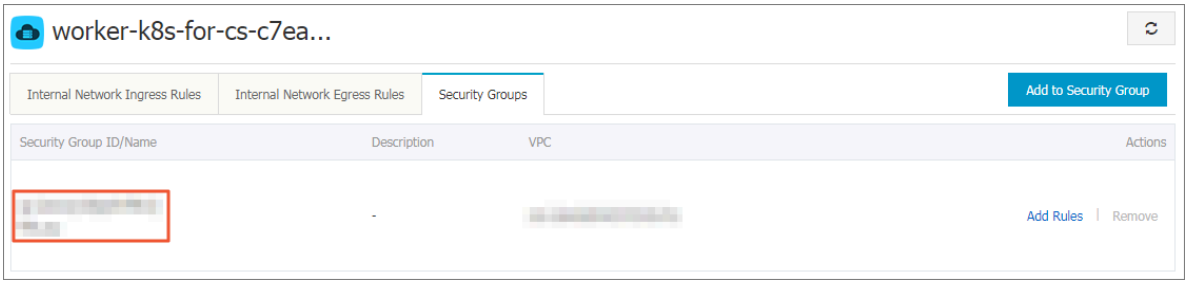
9. Click the drop-down arrow on the right of the Security Group box, and enter the cluster security group name obtained in step 6.



10. Click OK.

Verify the results

1. In the left-side navigation pane of the Elastic Computer Service console, click Instances and then click the target instance.
2. In the left-side navigation pane, click Security Groups.
3. The Security Groups area shows that the target ECS instance has been added to the security group to which the Kubernetes cluster belongs.



10 Istio FAQ

This topic lists common Istio FAQ and their corresponding solutions.

What do I do if the services in the cluster cannot access external URLs?

Symptom

The services in the cluster cannot access external URLs.

Cause

By default, this is because the pod in the Istio service mesh uses iptables to transparently forward all outbound traffic to the sidecar. The sidecar can only handle the traffic destined for addresses within the cluster.

Solutions

- Define `ServiceEnt ry` to call external services.
- Configure Istio to allow access to a specific range of IP addresses.

For more information, see ***Control Egress Traffic***.

What do I do if Tiller is in an earlier version?

Symptom

The following message is displayed during the installation process:

```
Can ' t  install  release  with  errors :  rpc  error :  code
=  Unknown  desc  =  Chart  incompatib  le  with  Tiller  v2 . 7
. 0
```

Cause

Your current version of Tiller needs to be upgraded.

Solution

Run the following command to upgrade the Tiller version:

```
$  helm  init  -- tiller - image  registry . cn - hangzhou .
 aliyuncs . com / acs / tiller : v2 . 9 . 1
```

What do I do if Custom Resource Definitions (CRDs) are in an invalid version?

Symptom

The following message is displayed when you create Istio for the first time or upgrade from Istio 1.0:

```
Can ' t  install  release  with  errors :  rpc  error :  code
 =  Unknown  desc  =  apiVersion  " networking . istio . io /
v1alpha3 "  in  ack - istio / charts / pilot / templates / gateway .
yaml  is  not  available
```

Cause

CRDs do not exist or are of an earlier version.

Note:

This problem occurs only in Helm 2.10.0 and earlier versions. For Helm later than V2.10.0, the system automatically upgrades CRDs.

Solution

1. Download the latest Istio. For more information, see ***Downloading the Release***.
2. Run the following command to install the latest CRDs:

```
$  kubectl  apply  - f  install / kubernetes / helm / istio /
 templates / crds . yaml  - n  istio - system
```

3. If you have enabled `certmanager` , you must run the following command to install the relevant CRDs:

```
$  kubectl  apply  - f  install / kubernetes / helm / istio /
 charts / certmanager  r / templates / crds . yaml
```

What do I do if Istio cannot be installed when I log on as a RAM user?

Symptom

The following message or a similar one is displayed during the installation process:

```
Error  from  server  ( Forbidden ):  error  when  retrieving
current  configurat  ion  of :
Resource : " apiextensi  ons . k8s . io / v1beta1 ,  Resource =
customreso  urcedefini  tions ",  GroupVersi  onKind : " apiextensi
ons . k8s . io / v1beta1 ,  Kind = CustomReso  urceDefini  tion "
```

Cause

The RAM user does not have permission to install Istio.

Solutions

- Log on to Alibaba Cloud by using the primary account.

- Grant the RAM user the required permissions. For example, you can grant the RAM user the `cluster - admin` custom role. For more information, see *Kubernetes permission configuration guide for RAM users*.

What do I do if CRDs are not removed after Istio is uninstalled?

Symptom

CRDs are not removed after Istio is uninstalled.

Cause

The system does not remove CRDs when you uninstall Istio.

Solution

1. If you use Helm later than V2.9.0, perform step 2 directly. If you use Helm 2.9.0 or earlier, you must first run the following command to delete Job resources:

```
$ kubectl - n istio - system delete job -- all
```

2. Run the following command to delete CRDs:

```
$ kubectl delete - f install / kubernetes / helm / istio /
 templates / crds . yaml - n istio - system
```

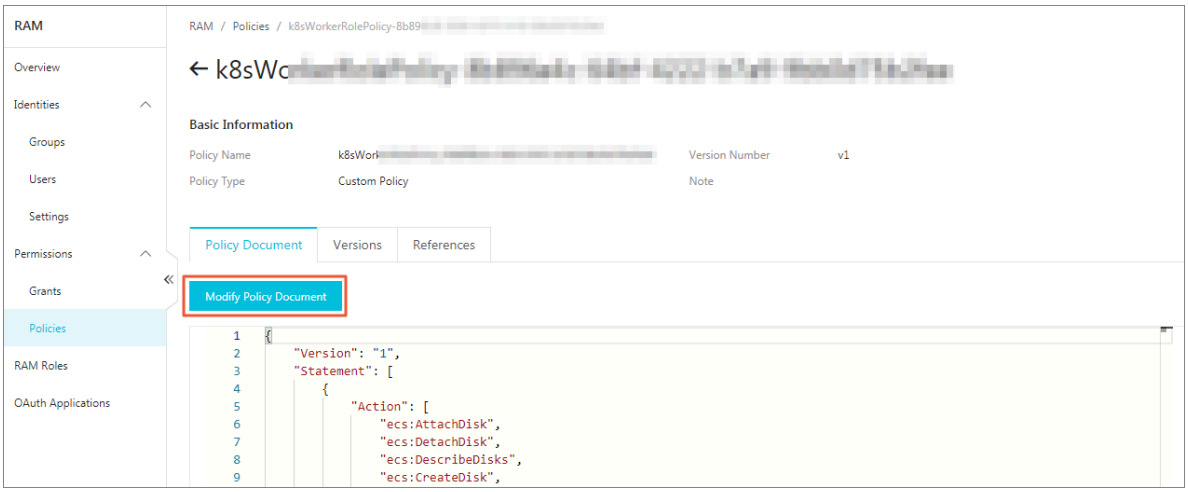
11 Can I manually set a security group for a Kubernetes cluster?

No, an existing security group cannot be manually set for a Kubernetes cluster. A security group can only be set automatically for a Kubernetes cluster when the cluster is created.

12 How do I customize a RAM role for a Kubernetes cluster?

You cannot create a RAM role manually. However, when cluster Worker nodes are created, a Worker RAM role is automatically created for the Kubernetes cluster. You can then add policies to the Worker RAM role to grant the role the required permissions.

1. Log on to the *Container Service console*.
2. In the left-side navigation pane under Kubernetes, choose Clusters > Clusters .
3. Click the target cluster name to view the cluster details.
4. In the Cluster Resources area, click Worker RAM Role.
5. On the RAM Roles page, click the policy name on the Permission tab page to view the policy details.
6. Click Modify Policy Document on the Policy Document tab page.



7. Add the target policies to the Policy Document area, and then click OK. In this example, the policies containing the permissions of scaling and deleting clusters are added to the policy document. For more information about permissions supported by a Kubernetes cluster, see *Container Service RAM actions*.

```
{
            " Action ": [
              " cr : ScaleClust  er ",
              " cr : DeleteClus  ter "
            ],
            " Resource ": "*",
            " Effect ": " Allow "
```

```
        }
```


Modify Policy Document
Policy Name
k8sWorkerRolePolicy-
Policy Document
68],
69 "Resource": [
70 "*"
71],
72 "Effect": "Allow"
73 },
74 {
75 "Action": [
76 "cr:ScaleCluster",
77 "cr:DeleteCluster"
78],
79 "Resource": "*",
80 "Effect": "Allow"
81 }
82]
83 }
OK
Close
Contact Us