

Alibaba Cloud Aliyun Container for Kubernetes

常見問題

檔案版本：20190418

目錄

1 叢集建立失敗.....	1
2 刪除 Kubernetes 叢集失敗：ROS stack 無法刪除.....	2
3 收集 Kubernetes 診斷資訊.....	4
4 Helm 手動升級.....	5
5 如何支援私人鏡像.....	6
6 儲存卷常見問題.....	9
7 如何手動安裝alicloud-application-controller.....	13
8 如何給Kubernetes叢集指定安全性群組.....	14
9 如何在Kubernetes叢集指定RAM中的自訂角色.....	15

1 叢集建立失敗

查看失敗原因

您可以通過查看叢集的建立事件來查看叢集建立失敗的原因。

登入 [ROS #####](#)

選擇叢集所在的地區，選擇所需的叢集並單擊右側的管理，單擊左側導覽列中的事件，將滑鼠移動到失敗事件上查看具體的失敗報錯資訊。

資源名稱	失敗資源ID	資源類型	資源狀態	狀態描述	事件發生時間
k8s_dev	dcb38ca9-fb8b-4471-b415-694cc2...	ALYUN::ROS::Stack	異常完成	Stack ROLLBACK compl...	2017-05-21 10:47:57
k8s_vpc	-	ALYUN::ECS::VPC	刪除完成	state changed	2017-05-21 10:47:57
k8s_vpc	-	ALYUN::ECS::VPC	刪除中	state changed	2017-05-21 10:47:56
k8s_master_cloudinit...	k8s_master_cloudinit_wait_cond...	ALYUN::ROS::WaitConditionHandle	刪除完成	state changed	2017-05-21 10:47:55
k8s_master_cloudinit...	k8s_master_cloudinit_wait_cond...	ALYUN::ROS::WaitConditionHandle	刪除中	state changed	2017-05-21 10:47:54
k8s_node_cloudinit_w...	k8s_node_cloudinit_wait_h...	ALYUN::ROS::WaitConditionHandle	刪除完成	state changed	2017-05-21 10:47:54
k8s_node_cloudinit_w...	k8s_node_cloudinit_wait_cond_h...	ALYUN::ROS::WaitConditionHandle	刪除中	Resource CREATE failed: Netpo... rsException: resources.k8s_vo... c: VPC quota exceeded. Code: ... QuotaExceeded.Vpc. RequestId: ... 694f730c-468b-4e63-9789-0E... D83F4A7294	2017-05-21 10:47:53
k8s_dev	dcb38ca9-fb8b-4471-b415-694cc2...	ALYUN::ROS::Stack	異常中	Resource CREATE fail...	2017-05-21 10:47:53
k8s_dev	dcb38ca9-fb8b-4471-b415-694cc2...	ALYUN::ROS::Stack	創建失敗	Resource CREATE fail...	2017-05-21 10:47:52
k8s_node_cloudinit_w...	k8s_node_cloudinit_wait_h...	ALYUN::ROS::WaitConditionHandle	創建完成	state changed	2017-05-21 10:47:52

上圖中的報錯資訊顯示由於 VPC 達到配額導致叢集建立失敗。

失敗異常碼及解決方案

- Code: QuotaExceeded.Eip, Message: Elastic IP address quota exceeded
解決方案：釋放多餘的 EIP 或者提交 VPC 工單提高 EIP 限額。
- The maximum number of SLB instances is exceeded. Code: ORDER.QUANTITY_INVALID
解決方案：釋放多餘的 SLB 執行個體或者提交 SLB 工單提高 SLB 限額。
- Resource CREATE failed: ResponseException: resources.k8s_vpc: VPC quota exceeded. Code: QuotaExceeded.Vpc
解決方案：釋放多餘的 VPC 或者提交 VPC 工單提高 VPC 限額。
- Resource CREATE failed: ResponseException: resources.k8s_master_1: The specified image does not support cloud-init. Code: ImageNotSupportCloudInit
解決方案：使用自訂鏡像建立叢集，自訂鏡像必須是基於最新的 CentOS 鏡像。
- Status Code: 403 Code: InvalidResourceType.NotSupported Message: This resource type is not supported;
解決方案：ECS 沒有庫存或者類型不支援。

2 刪除 Kubernetes 叢集失敗：ROS stack 無法刪除

問題原因

使用者在 ROS 建立的資源下手動添加了一些資源（比如在 ROS 建立的 VPC 下手動添加了一個 VSwitch），ROS 是沒有許可權刪除這些資源的。這就會導致 ROS 刪除 Kubernetes 資源時無法處理該 VPC，最終導致刪除失敗。



註：

有關建立 Kubernetes 叢集時 ROS 自動建立的資源，參見##Kubernetes##。

解決辦法

1. 叢集刪除失敗時（叢集的狀態顯示刪除失敗），跳轉到 ROS #####。

名稱	叢集名稱/ID	叢集類型	地域	網絡類型	叢集狀態	創建時間	Kubernetes 版本	操作
	k8stest c77862d75bda644679b48d15f1a42e831	Kubernetes	華東 1	虛擬專用網絡 vpc-bp15k6x6fhdz2jw4daz0	刪除失敗	2018-01-04 19:47:08	1.8.4	管理 查看日志 刪除 控制台 更多

2. 選擇叢集所在的地區，找到叢集對應的資源棧 `k8s - for - cs -{ cluster - id }`，可以看到其狀態為刪除失敗。

名稱	狀態 (所有)	超時 (分鐘)	失敗回滾	狀態描述	創建時間	操作
k8s-for-cs-c77862d75bda644679b...	刪除失敗	60	否	Resource DELETE failed: ResponseExceptio...	2018-01-04 19:47:10	管理 刪除 更多
k8s-for-cs-cdea45b4604b44389ac...	刪除失敗	60	否	Resource DELETE failed: ResponseExceptio...	2017-10-26 14:33:55	管理 刪除 更多
test	刪除失敗	60	是	Resource DELETE failed: ResponseExceptio...	2017-05-22 14:25:14	管理 刪除 更多

3. 單擊資源棧的名稱進入資源棧詳情頁面，單擊左側導覽列中的資源。

您可以看到哪些資源刪除失敗了。本樣本中負載平衡下的 VSwitch 刪除失敗。

資源名稱	資源ID	資源類型	狀態	狀態描述	創建日期	更新日期	操作
k8s_api_server_liste...	lb-bp1kbi9oewty30azwir6	ALIYUN::SLB::Listener	刪除完成	state changed	2017-10-26 14:33:55	2018-01-03 11:14:14	詳情
k8s_dashboard_liste...	lb-bp1kbi9oewty30azwir6	ALIYUN::SLB::Listener	刪除完成	state changed	2017-10-26 14:33:55	2018-01-03 11:14:14	詳情
k8s_vswitch	vsw-bp19v3gdubfcbt7b1sniy	ALIYUN::ECS::VSwitch	刪除失敗	ResponseException: r...	2017-10-26 14:33:55	2018-01-15 16:35:21	詳情

4. 進入刪除失敗的資源所在產品的控制台，並找到該資源。

本樣本中，登入 VPC 管理主控台，找到叢集所在的 VPC，並在該 VPC 下找到刪除失敗的 VSwitch。



交换机 ID/名称	ECS实例数	网段	状态	可用区	可用私有IP数	创建时间	默认交换机	描述	操作
vsw-bp19v3gdubfcb7b1snly	4	192.168.0.0/16	可用	华东 1 可用区 F	65515	2017-10-26 14:34:07	否		编辑 删除 创建实例

5. 單擊 VSwitch 右側的刪除 嘗試手動刪除。

本樣本中，由於 VSwitch 下還有資源未釋放，所以刪除失敗。



手動釋放該 VSwitch 下的資源，然後再次嘗試刪除該 VSwitch。

6. 使用類似的方法手動刪除 Kubernetes 叢集下所有刪除失敗的資源，然後再次嘗試刪除 Kubernetes 叢集。

3 收集 Kubernetes 診斷資訊

1. 在 master 節點下載診斷指令碼，並增加運行許可權。

```
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. 執行診斷指令碼。

```
diagnose_k 8s .sh
.....
+ echo ' please get diagnose_1 514939155 .tar .gz for
diagnostic s ' ##每次執行診斷指令碼，產生的記錄檔的名稱不同
please get diagnose_1 514939155 .tar .gz for
diagnostic s
+ echo '請上傳 diagnose_1 514939155 .tar .gz '
請上傳 diagnose_1 514939155 .tar .gz
```

3. 列出產生的記錄檔。

```
cd /usr/local/bin
ls -ltr | grep diagnose_1 514939155 .tar .gz ##注
意替換為產生的記錄檔名
```

4 Helm 手動升級

登入到Kubernetes叢集master節點，參見## `kubectl` ## `Kubernetes` ##。

執行以下命令。

```
helm init --tiller-image registry.cn-hangzhou.aliyuncs.com/acs/tiller:v2.9.1 --upgrade
```

其中鏡像地址可使用對應region的vpc網域名稱，比如杭州region的機器就可以替換為registry-vpc.cn-hangzhou.aliyuncs.com/acs/tiller:v2.9.1。

然後等待 `tiller` 健全狀態檢查通過，就可以通過執行 `helm version` 查看版本升級情況。



说明:

這裡只會升級Helm 服務端版本，用戶端可以通過直接下載對應的client binary 使用。

Helm 2.9.1 client 下載地址: <https://github.com/kubernetes/helm/releases/tag/v2.9.1>。目前阿里雲支援的最新版本為2.9.1。

Helm 用戶端和服務端版本都升級完畢後，執行 `helm version` 命令，可看到如下資訊。

```
# helm version
Client: &version.Version{SemVer:"v2.9.1", GitCommit:"a80231648a 1473929271 764b920a8e 346f6de844", GitTreeState:"clean"}
Server: &version.Version{SemVer:"v2.9.1", GitCommit:"a80231648a 1473929271 764b920a8e 346f6de844", GitTreeState:"clean"}
```

5 如何支援私人鏡像

```
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
```

其中：

- `regsecret`：指定密鑰的鍵名稱，可自行定義。
- `--docker-server`：指定 Docker 倉庫地址。
- `--docker-username`：指定 Docker 倉庫使用者名。
- `--docker-password`：指定 Docker 倉庫登入密碼。
- `--docker-email`：指定郵件地址（選填）。

yml 檔案加入密鑰參數。

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

其中：

- `imagePullSecrets` 是聲明拉取鏡像時需要指定密鑰。
- `regsecret` 必須和上面產生密鑰的鍵名一致。
- `image` 中的 Docker 倉庫名稱必須和 `--docker-server` 中的 Docker 倉庫名一致。

詳情資訊參見官方文檔 #####。

實現無密鑰編排

為了避免每次使用私人鏡像部署時，都需要引用密鑰，您可將secret添加到namespace的default service account中，參見[Add ImagePullSecrets to a service account](#)。

首先找到前面建立的拉取私人鏡像的secret。

```
# kubectl get secret regsecret
NAME                TYPE                                DATA      AGE
regsecret           kubernetes.io/dockerconfigjson    1          13m
```

本例中採用手動設定的方式，修改命名空間的預設服務帳戶default，從而將此secret作為imagePullSecret。

首先建立一個 `sa . yml` 設定檔，將服務帳號default的配置匯入到該檔案中。

```
kubectl get serviceaccounts default -o yaml > ./ sa .
yaml

cat sa . yml

apiVersion : v1
kind : ServiceAccount
metadata :
  creationTimestamp : 2015 - 08 - 07T22 : 02 : 39Z
  name : default
  namespace : default
  resourceVersion : " 243024 "          ##注意該項
  selfLink : / api / v1 / namespaces / default / serviceaccounts /
default
  uid : 052fb0f4 - 3d50 - 11e5 - b066 - 42010af0d7 b6
secrets :
- name : default - token - uudegoken - uudeg
```

執行 `vim sa . yml` 命令，刪除resourceVersion，並增加拉取鏡像的密鑰配置項imagePullSecrets。修改後的配置如下。

```
apiVersion : v1
kind : ServiceAccount
metadata :
  creationTimestamp : 2015 - 08 - 07T22 : 02 : 39Z
  name : default
  namespace : default
  selfLink : / api / v1 / namespaces / default / serviceaccounts /
default
  uid : 052fb0f4 - 3d50 - 11e5 - b066 - 42010af0d7 b6
secrets :
- name : default - token - uudeg
imagePullSecrets :          ##增加該項
- name : regsecret
```

隨後用 `sa . yml` 設定檔替換default的服務帳號配置。

```
kubectl replace serviceaccount default -f ./ sa . yml
serviceaccount " default " replaced
```

以一個tomcat編排為例，執行 `kubectl create -f` 命令建立。

```
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 :
    matchLabels :
      app : tomcat
  template :
```

```
metadata :
  labels :
    app : tomcat
spec :
  containers :
  - name : tomcat
    image : registry - internal . cn - hangzhou . aliyuncs . com
/ abc / test : 1 . 0 #替換為您自己的私人鏡像地址
    ports :
    - containerPort : 8080containerPort : 8080
```

若配置正常，Pod會啟動成功。然後執行 `kubectl get pod tomcat - xxx - o`
`yaml` 命令，你可看到以下配置項。

```
spec :
  imagePullSecrets :
  - name:registrysecret
```

6 儲存卷常見問題

儲存卷掛載不上

檢查Flexvolume是否安裝

在master節點上執行下面命令。

```
# 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
```

查看flexvolume pod狀態是否為Running，且啟動並執行數量與節點數量相同；

如果沒有安裝，請參考#####。

如果運行狀態不對，請參考外掛程式作業記錄分析。

檢查動態儲存裝置外掛程式是否安裝

如果使用雲端硬碟的動態儲存裝置功能，需要確認是否安裝動態儲存裝置外掛程式，執行下面命令。

```
# kubectl get pod -n kube-system | grep alicloud -
disk
alicloud - disk - controller - 8679c9fc76 - lq6zb      1 / 1
Running    0      7d
```

如果沒有安裝，請參考#####。

如果運行狀態不對，請參考外掛程式作業記錄分析。

如何查看儲存相關日誌

Flexvolume日誌（master1上執行）

執行get命令查看出錯的pod:

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

執行log命令, 查看出錯pod的日誌:

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

#在 pod 描述最後若干行是 pod 運行狀態的描述, 可以根據描述分析錯誤;

雲端硬碟、NAS、OSS驅動日誌查看:

```
# 查看 host 節點上持久化的日誌;
# 如果某個 Pod 掛載失敗, 查看 pod 所在的節點地址:

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

# 登陸節點, 查看日誌:

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

可以看到雲端硬碟、 nas 、 oss 掛載的日誌;

provisioner外掛程式日誌 (master1上執行)

執行get命令查看出錯的pod:

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

執行log命令, 查看出錯pod的日誌:

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

#在 pod 描述最後若干行是 pod 運行狀態的描述, 可以根據描述分析錯誤;

Kubelet日誌

```
# 如果某個 Pod 掛載失敗, 查看 pod 所在的節點地址:

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

# 登陸節點, 查看 kubelet 日誌:
```

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

# - n 的值表示期望看到的日誌行數；
```

上述為擷取flexvolume、provsioner、Kubelet錯誤記錄檔的方法，如果無法根據日誌修復狀態，可以附帶日誌資訊聯絡阿里雲支援人員；

雲端硬碟常見問題

雲端硬碟掛載失敗，出現timeout錯誤

如果節點為手動添加，可能是由於sts許可權的問題導致，需要手動設定RAM許可權：[#####](#)
[## RAM ##](#)。

雲端硬碟掛載失敗，出現Size錯誤

建立雲端硬碟對Size有如下要求。



说明:

- 普通雲端硬碟：最小5Gi
- 高效雲端硬碟：最小20Gi
- SSD雲端硬碟：最小20Gi

雲端硬碟掛載失敗，出現zone錯誤；

ECS掛載雲端硬碟時，必須在同一個region下面的相同zone內，否則不能掛載成功。

升級系統後，雲端硬碟有時報錯：input/output error

1. 升級flexvolume到v1.9.7-42e8198或以後版本。
2. 對於已經出問題的Pod，需要重建。

升級命令：

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

Flexvolume版本資訊：可登入Container Registry控制台，單擊左側導覽列中的鏡像搜尋，搜尋acs/flexvolume，擷取Flexvolume最新版本資訊。

NAS常見問題

NAS掛載時間太長

如果NAS卷包含的檔案量很大，且在掛載模板中配置了chmod參數，可能導致掛載時間過長的問題；可以去掉chmod參數。

NAS掛載失敗，出現timeouot錯誤

檢查nas掛載點和叢集是否在同一個vpc內，否則無法掛載。

OSS常見問題

oss掛載失敗

檢查使用的ak是否正確。

7 如何手動安裝alicloud-application-controller

在阿里雲Container Service中，1.10.4及以上版本預設安裝alicloud-application-controller，來提供一種基於CRD的分批發布的能力。



说明:

Kubernetes最新叢集已經預設安裝alicloud-application-controller，舊版本叢集可以通過手動安裝的方式部署alicloud-application-controller，要求Kubernetes叢集版本最低為v1.9.3。

您可通過 `kubectl create -f alicloud - application - controller . yml` 命令部署alicloud-application-controller，在 `alicloud - application - controller . yml` 中輸入如下的編排模板。

```
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 :
    matchLabel s :
      owner : aliyun
      app : alicloud - applicatio n - controller
  template :
    metadata :
      labels :
        owner : aliyun
        app : alicloud - applicatio n - controller
    annotation s :
      scheduler . alpha . kubernetes . io / critical - pod : ''
    spec :
      toleration s :
        - effect : NoSchedule
          operator : Exists
          key : node - role . kubernetes . io / master
        - effect : NoSchedule
          operator : Exists
          key : node . cloudprovi der . kubernetes . io / uninitiali
zed
      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
```

8 如何給Kubernetes叢集指定安全性群組

當前暫不支援給Kubernetes叢集指定安全性群組。但是建立Kubernetes叢集時，Container ServiceACK會自動建立一個預設安全性群組，您可以通過修改預設安全性群組的規則，達到指定安全性群組的效果。

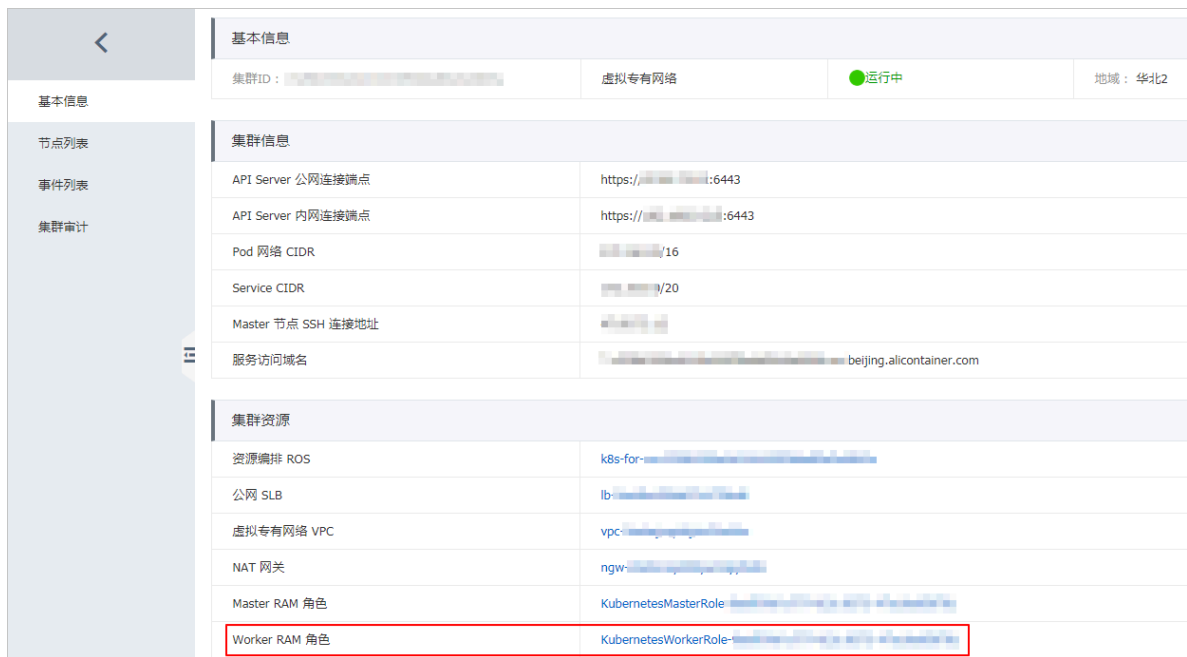
9 如何在Kubernetes叢集指定RAM中的自訂角色

Kubernetes叢集暫不支援指定RAM中的自訂角色，但是在Kubernetes叢集中建立worker時會自動產生一個角色，您可以通過給該角色添加policy的方式，來實現zh-CN角色授權。

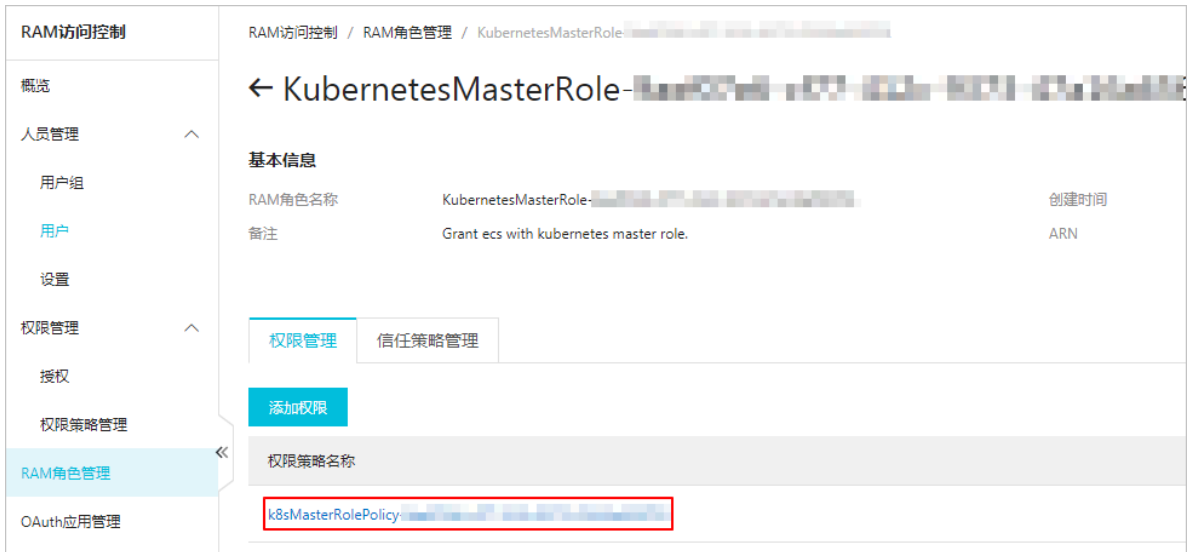
1. 登入 [Container Service####](#)。
2. 在 Kubernetes 菜單下，選擇叢集 > 叢集，在叢集列表頁面，單擊目的地組群。



3. 進入基本資料頁面，在叢集資源地區，單擊Worker RAM 角色。



4. 跳轉到RAM控制台頁面，在RAM 角色管理頁面，單擊權限原則名稱。



5. 進入策略許可權管理頁面，單擊修改策略內容，將如下內容填入後，單擊確定。本樣本中是給該角色授予伸縮和刪除叢集的許可權，如果您想瞭解更多的許可權，請參見# 1。

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

