## Cloud Container Engine

# FAQs

| | |
|---|---|
| **Issue** | 01 |
| **Date** | 2024-10-16 |

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

## Trademarks and Permissions

HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

## Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

**Huawei Cloud Computing Technologies Co., Ltd.**

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

# Contents

# 1 Workloads

## 1.1 Workload Exceptions

### 1.1.1 What Do I Do If an Image Can't Be Pulled from SWR During Workload Creation?

#### Symptom

The following information is displayed when a workload is created in a CCE Autopilot cluster:

```
Failed to pull image "swr.cn-north-**.myhuaweicloud.com/**/nginx:latest": rpc error: code = Unknown desc =
failed to pull and unpack image "swr.cn-north-7.myhuaweicloud.com/**/nginx:latest": failed to resolve
reference "swr.cn-north-7.myhuaweicloud.com/**/nginx/latest": failed to do request: Head "https://swr.cn-
north-**.myhuaweicloud.com/v2/**/nginx/manifests/latest": dial tcp 100.79.**.**:443: i/o timeout
```

#### Fault Location

The error information indicates that the SWR image cannot be pulled during workload creation. Check whether the VPC endpoints for accessing OBS and SWR are running properly.

#### Solution

**Create VPC endpoints for accessing OBS and SWR.**

### 1.1.2 What Do I Do If a Public Image Can't Be Pulled During Workload Creation?

#### Symptom

The following information is displayed when a workload is created in a CCE Autopilot cluster:

```
Failed to pull image "100.125.**.**:32334/**/nginx:1.0": rpcerror: code =DeadlineExceeded desc = failed to
pull and unpack image "100.125.**.**:32334/**/nginx:1.0": failed to resolve reference "100.125.**.**:32334/**/
```

```
nginx:1.0": failed to do request Head: Head "https://100.125.**.**:32334/v2/**/nginx/manifests/1.0": dial tcp
100.125.**.**:32334: i/o timeout
```

## Fault Location

When the CCE Autopilot cluster pulls the image from the public network, the NAT gateway cannot access the public network because there is no route destined for the NAT gateway in the route table of the subnet.

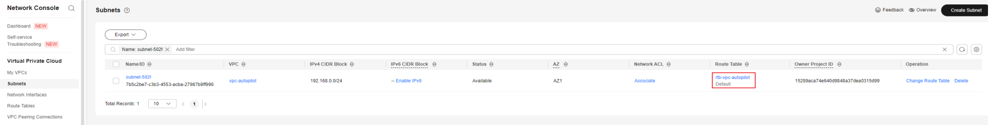
## Solution

Add the route destined for 0.0.0.0/0 over the NAT gateway in the default route table or custom route table of the subnet.

**Step 1** Log in to the CCE console and click the cluster name to access the cluster console.

**Step 2** In the navigation pane, choose **Overview**. In the **Networking Configuration** area, view the cluster subnet.

**Step 3** Switch to the **Network Console**. In the navigation pane, choose **Virtual Private Cloud** > **Subnets**. Locate the subnet by name and click the route table name.



Name: subnet-502f

| Name/ID | VPC | IPv4 CIDR Block | IPv6 CIDR Block | Status | AZ | Network ACL | Route Table | Owner Project ID | Operation |
|---|---|---|---|---|---|---|---|---|---|
| subnet-502f<br>7b5c2be7-c3b3-4553-acba-27987b9ff996 | vpc-autopilot | 192.168.0.0/24 | -- Enable IPv6 | Available | AZ1 | Associate | rtb-vpc-autopilot<br>Default | 15289aca74e640d9848a37dea0315d99 | Change Route Table Delete |

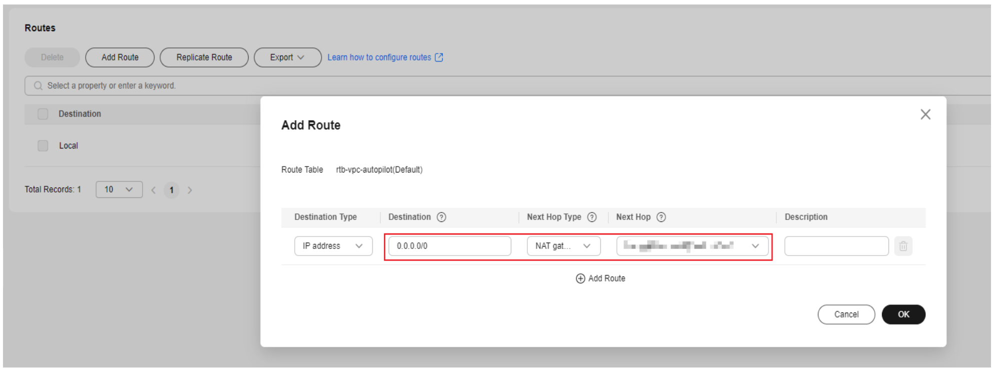
Total Records: 1 10 1

**Step 4** On the **Summary** tab, check whether a route to the NAT gateway exists.

If no, manually add a route. Click **Add Route**.

- **Destination**: Set this parameter to **0.0.0.0/0**, which means any IP address.
- **Next Hop Type**: Select **NAT gateway**.
- **Next Hop**: Select the NAT gateway configured for the subnet.

Click **OK**.



Route Table rtb-vpc-autopilot(Default)

| Destination Type | Destination | Next Hop Type | Next Hop | Description |
|---|---|---|---|---|
| IP address | 0.0.0.0/0 | NAT gat... | [redacted] | |

**----End**

# 1.1.3 What Do I Do If "Cluster pod max limit exceeded" Is Displayed for a Workload?

## Symptom

The following error occurs when a workload is created:

```
Cluster pod max limit exceeded(x)
```

## Fault Location

This indicates that the maximum number of pods in the cluster is reached and no more pods can be created. *x* indicates the maximum of pods allowed in the cluster. The default value is **500**.

## Solution

Plan the number of pods in the cluster appropriately.

**NOTE**

The add-on pods installed in the cluster occupy the pod quota. Plan the pod quota properly.

# 2 Network Management

## 2.1 How Do I Configure Security Group Rules for a Cluster?

When a CCE Autopilot cluster is created, two security groups are automatically created, one for master nodes, and the other for elastic network interfaces (ENIs). The security group for master nodes is named in the format of *{Cluster name}-cce-control-{Random ID}*, and that for ENIs is in the format of *{Cluster name}-cce-eni-{Random ID}*.

You can modify the security group rules on the VPC console as required. (Log in to the management console, choose **Service List** > **Networking** > **Virtual Private Cloud**. On the page displayed, choose **Access Control** > **Security Groups** in the navigation pane, locate the target security groups, and modify their rules.)

NOTICE

- Modifying or deleting default rules in a security group may affect cluster running. If you need to modify security group rules, do not modify the rules of the port that CCE running depends on.
- When adding a security group rule, ensure that **this rule does not conflict with the existing rules**. If there is a conflict, existing rules may become invalid, affecting cluster running.

### Security Group for Master Nodes

The security group automatically created for master nodes is named *{Cluster name}***-cce-control-***{Random ID}*. **Table 2-1** lists the default ports in the security group.

**Table 2-1** Default ports in the security group of the master nodes

| Direction | Port | Source | Description | Modifiable | Modification Suggestion |
|---|---|---|---|---|---|
| Inbound | All | IP addresses of this security group | Allow traffic from all IP addresses in this security group | No | None |
| Outbound | All | All IP addresses: 0.0.0.0/0 or ::/0 | Allow traffic on all ports by default. | No | None |

## Security Group for ENIs

When a CCE Autopilot cluster is created, a security group named *{Cluster name}*-**cce-eni-***{Random ID}* is automatically created for ENIs. By default, pods in the cluster are associated with this security group. **Table 2-2** lists the default ports in the security group.

**Table 2-2** Default ports in the security group for ENIs

| Direction | Port | Source | Description | Modifiable | Modification Suggestion |
|---|---|---|---|---|---|
| Inbound | All | IP addresses of this security group | Allow traffic from all IP addresses in this security group | No | None |
| | | CIDR block of the master nodes | Allow the master nodes to access kubelet on each worker node, for example, by running **kubectl exec** *{Pod}*. | No | None |

| Direction | Port | Source | Description | Modifiable | Modification Suggestion |
|---|---|---|---|---|---|
| Outbound | All | All IP addresses: 0.0.0.0/0 or ::/0 | Allow traffic on all ports by default. | Yes | If you want to harden security by allowing traffic over specific ports, you can modify the rule to allow these ports. For details, see **Hardening Outbound Rules for the Security Group of ENIs**. |

## Hardening Outbound Rules for the Security Group of ENIs

By default, all ENI security groups created by CCE Autopilot allow all outbound traffic. You are advised to retain this configuration. If you want to harden security by allowing traffic over specific ports, configure the ports listed in the following table.

**Table 2-3** Minimum scope for outbound rules in an ENI security group

| Port | Allowed CIDR Block | Description |
|---|---|---|
| All | IP addresses of this security group | Allow mutual access within the security group so containers can communicate with each other. |
| TCP port 5443 | VPC CIDR block | Allow access from kube-apiserver, which provides lifecycle management for Kubernetes resources. |
| TCP port 443 | 100.125.0.0/16 | Access the OBS port or SWR port to pull images. |
| UDP port 53 | 100.125.0.0/16 | Allow traffic over the port for DNS resolution. |
| TCP port 443 | VPC CIDR block | Pull the images through the SWR endpoint. |
| All | 198.19.128.0/17 | Allow worker nodes to access the VPC Endpoint (VPCEP) service. |
| TCP port 9443 | VPC CIDR block | Allow the network add-ons of the worker nodes to access master nodes. |