云容器引擎
Autopilot
常见问题

文档版本 01

发布日期 2024-10-16

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 工作负载

1.1 工作负载异常问题排查

1.1.1 创建工作负载时无法拉取 SWR 镜像如何解决?

问题现象

在Autopilot集群中创建工作负载时，出现以下错误：

```
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
```

问题定位

报错信息中说明创建工作负载时无法拉取SWR镜像，请检查OBS和SWR终端节点是否正常。

解决方案

如果未创建OBS和SWR终端节点，请参考**配置访问SWR和OBS服务的VPC终端节点**进行配置。

1.1.2 创建工作负载时无法拉取公网镜像如何解决?

问题现象

在Autopilot集群中创建工作负载时，事件中出现以下错误：

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


问题定位

Autopilot集群从公网拉取镜像时，请检查NAT网关是否可正常访问公网。如果集群的子网路由表缺失，则会导致集群NAT网关无法访问公网。

解决方案

集群的子网需要在默认路由表下或者自定义表中添加0.0.0.0/0到NAT网关的路由。

步骤1 登录CCE控制台，单击集群名称进入集群。

步骤2 在左侧选择“总览”，在“网络信息”中查看集群容器子网。

步骤3 在网络控制台中，单击左侧导航栏中的“虚拟私有云 > 子网”，筛选集群容器子网名称，并单击对应的路由表名称。

步骤4 在路由表页面，单击“基本信息”页签，检查是否存在NAT网关的路由。

如果没有，则需要手动添加路由，单击“添加路由”。

- 目的地址：填写为0.0.0.0/0，表示所有IP地址。
- 下一跳类型：选择“NAT网关”。
- 下一跳：选择NAT网关名称。

填写完成后单击“确定”。

----结束

1.1.3 工作负载事件中出现 Cluster pod max limit exceeded 如何解决?

问题现象

创建工作负载时，事件中出现以下错误：

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


问题定位

该事件信息表示集群中的Pod数量达到上限值，无法再新建Pod，其中x为集群Pod数量上限，默认为500。

解决方案

请合理规划集群中的Pod数量，避免达到上限值。

说明

集群中安装的插件实例会占用Pod配额，请合理规划。

2 网络管理

2.1 如何正确配置集群安全组规则?

Autopilot集群在创建时将会自动创建两个安全组，其中Master节点的安全组名称是：**{集群名}-cce-control-{随机ID}**；ENI的安全组的名称是：**{集群名}-cce-eni-{随机ID}**。

用户可根据安全需求，登录CCE控制台，单击服务列表中的“网络 > 虚拟私有云VPC”，在网络控制台单击“访问控制 > 安全组”，找到集群对应的安全组规则进行修改和加固。

须知

- 安全组规则的**修改和删除可能会影响集群的正常运行**，请谨慎操作。如需修改安全组规则，请尽量避免对CCE运行依赖的端口规则进行修改。
- 在集群中添加新的安全组规则时，需要**确保新规则与原有规则不会发生冲突**，否则可能导致原有规则失效，影响集群正常运行。

Master 节点安全组

集群自动创建的Master节点安全组名称为**{集群名}-cce-control-{随机ID}**，默认端口说明请参见**表2-1**。

表 2-1 Master 节点安全组默认端口说明

方向	端口	默认源地址	说明	是否支持修改	修改建议
入方向规则	全部	本安全组	属于本安全组的源地址需全部放通。	不可修改	不涉及

方向	端口	默认源地址	说明	是否支持修改	修改建议
出方向规则	全部	所有IP地址（0.0.0.0/0及::/0）	默认全部放通。	不可修改	不涉及

ENI 安全组

Autopilot集群会创建名为**{集群名}-cce-eni-{随机ID}**的ENI安全组，默认为集群中的容器绑定该安全组，默认端口说明请参见**表2-2**。

表 2-2 ENI 安全组默认端口说明

方向	端口	默认源地址	说明	是否可修改	修改建议
入方向规则	全部	本安全组	属于本安全组的源地址需全部放通。	不可修改	不涉及
		Master节点网段	Master节点主动访问kubelet（如执行kubectl exec {pod}）。	不可修改	不涉及
出方向规则	全部	所有IP地址（0.0.0.0/0及::/0）	默认全部放通。	可以修改	如需加固出方向规则，请注意指定端口需要放通，详情请参见**ENI安全组出方向规则加固建议**。

ENI 安全组出方向规则加固建议

对于**出方向规则**，Autopilot集群创建的ENI安全组默认全部放通，通常情况下不建议修改。如需加固出方向规则，请注意如下端口需要放通。

表 2-3 ENI 安全组出方向规则最小范围

端口	放通地址段	说明
所有端口	本安全组	属于本安全组的目的地址需全部放通，容器间网络互访。
TCP：5443	VPC网段	kube-apiserver服务端口，提供K8s资源的生命周期管理。

端口	放通地址段	说明
TCP：443	100.125.0.0/16网段	访问OBS端口或者SWR端口，拉取镜像。
UDP：53	100.125.0.0/16网段	用于域名解析。
TCP：443	VPC网段	通过SWR终端节点，拉取镜像。
所有端口	198.19.128.0/17网段	访问VPCEP服务。
TCP：9443	VPC网段	Node节点网络插件访问Master节点。