云容器引擎
Autopilot
常见问题

文档版本 01

发布日期 2025-01-22

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 计费类.....1
1.1 CCE Autopilot 集群如何定价/收费？.....1
1.2 Pod 所需的 CPU/内存计费模式如何由按需改为套餐包？.....2
2 工作负载.....4
2.1 工作负载异常问题排查.....4
2.1.1 创建工作负载时无法拉取 SWR 镜像如何解决？.....4
2.1.2 创建工作负载时无法拉取公网镜像如何解决？.....4
2.1.3 工作负载事件中出现 Cluster pod max limit exceeded 如何解决？.....5
2.1.4 创建工作负载时，Pod 不断被重建如何解决？.....6
2.2 监控日志.....7
2.2.1 容器监控的内存使用率与实际弹性伸缩现象不一致.....7
3 网络管理.....9
3.1 如何正确配置集群安全组规则？.....9
3.2 如何确认网卡不被集群占用？.....11
4 存储管理.....13
4.1 CCE Autopilot 集群中的 EVS 存储卷被删除或者过期后是否可以恢复？.....13
4.2 创建存储卷失败如何解决？.....13
4.3 CCE Autopilot 集群云存储 PVC 能否感知底层存储故障？.....13
4.4 删除动态创建的 PVC 之后，底层存储有残留如何解决？.....14
5 权限.....15
5.1 能否只配置命名空间权限，不配置集群管理权限？.....15
5.2 如果不配置集群管理权限的情况下，是否可以使用 API 呢？.....15
5.3 如果不配置集群管理权限，是否可以使用 kubectl 命令呢？.....16
5.4 IAM 用户无法使用调用 API.....16

1 计费类

1.1 CCE Autopilot 集群如何定价/收费?

计费模式

CCE Autopilot集群提供按需计费和套餐包（生效周期可按月/年）两种计费模式，以满足不同场景下的用户需求。

- 按需计费是一种后付费模式，即先使用再付费，按照实际使用时长计费。按照实际使用时长（秒级）计费，每一个小时整点结算一次费用，结算完毕后进入新的结算周期。按需计费模式下您可以根据实际业务需求灵活地调整资源使用，无需提前预置资源，从而降低预置过多或不足的风险。一般适用于电商抢购等设备需求量瞬间大幅波动的场景。
- 套餐包是一种预付费模式，即先付费再使用，每一个小时整点结算一次用量，结算完毕后进入新的结算周期。您可以根据实际需求购买套餐包获取更多的优惠。一般适用于需求量长期稳定的成熟业务。

  说明

  套餐包需要在集群内的“概览”页购买，并且仅支持购买Pod所需的CPU或内存的套餐包。**购买套餐包后，对应区域的所有CCE Autopilot集群在Pod中自动使用该套餐包。**

  除Pod所需的CPU和内存外，CCE Autopilot集群涉及的集群管理费、终端节点费用暂时不支持套餐包。其他云服务资源计费项无法从CCE控制台购买套餐包，通过CCE控制台创建时均默认为按需计费。如需购买其他云服务资源计费项的套餐包或包年/包月资源，请前往各自的云服务控制台购买，计费详情请参考对应云服务的计费说明。

表 1-1 集群计费模式

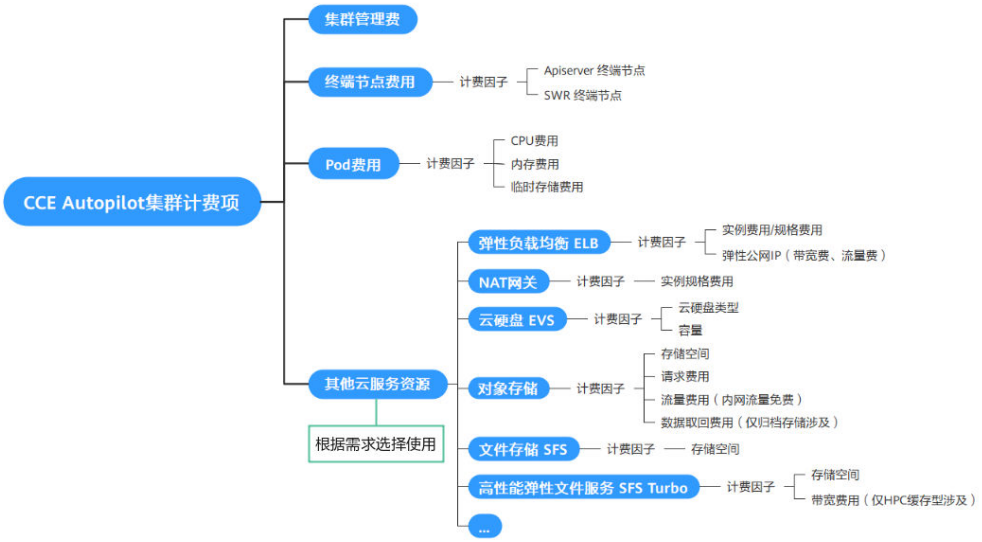
计费模式	按需计费	套餐包
付费方式	后付费，按照资源实际使用时长计费。	预付费，按需套餐包，购买周期内优先扣除套餐包中的使用量。
计费周期	秒级计费，按小时结算。	按订单的购买周期计费。
适用计费项	集群涉及的所有费用。	Pod所需的CPU和内存。

适用场景	适用于计算资源需求波动的场景，可以随时开通，随时删除。	适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。对于长期使用者，推荐该方式。

计费项

使用云容器引擎服务时，产生的总费用由集群管理费、Pod费用、终端节点费用和其他云服务资源费用组成，具体说明请参见文档“计费说明 > 计费项”。

图 1-1 计费项



1.2 Pod 所需的 CPU/内存计费模式如何由按需改为套餐包?

在使用CCE Autopilot集群时，Pod所需的CPU和内存默认为按需计费模式。在按需计费模式下，如果创建Pod所需的CPU和内存不满足用户需求，用户可根据需求购买套餐包，享受更多的优惠。具体购买操作请参见**操作步骤**。

说明

套餐包购买注意事项：

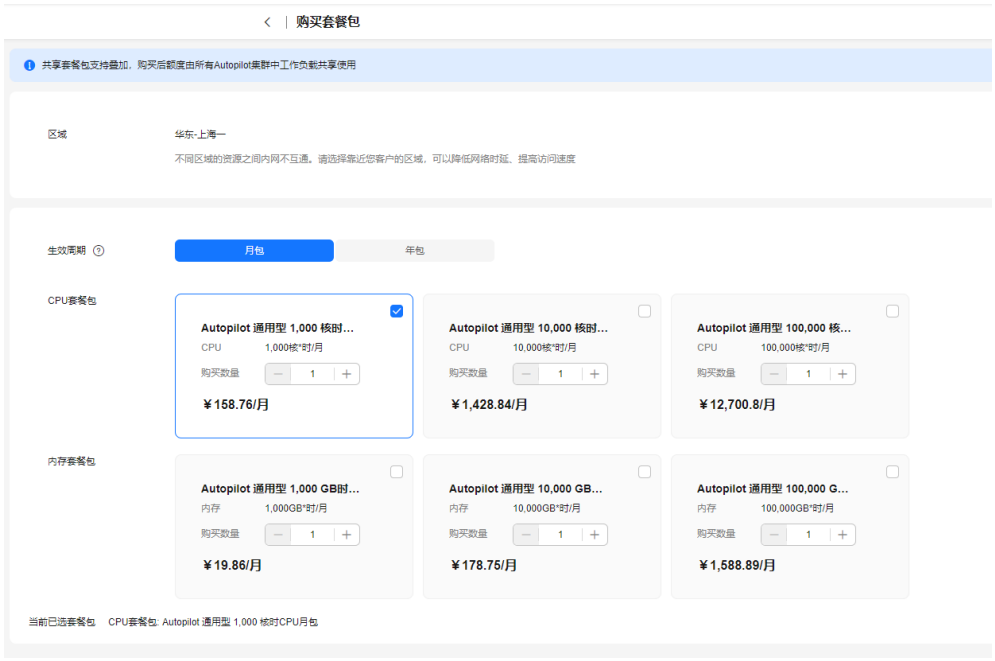
- 费用一次性支付，即刻生效，不支持指定日期生效，不支持退订。
- 套餐包到期后，不会影响您使用CCE Autopilot集群。您只要保证云服务账号上有足够的余额，系统会自动以按需计费的模式进行结算。
- 有效期支持选择1个月或1年，到期后剩余资源将无法使用。

操作步骤

步骤1 登录**CCE控制台**，单击对应集群名称，进入集群“概览”页。在“概览”页右侧“Autopilot 套餐包”模块单击“购买套餐包”。

步骤2 进入购买套餐包页面后，根据界面信息提示选择您需要的套餐包规格。

图 1-2 购买套餐包



步骤3 确定规格无误后，在右下角单击“去支付”，提示信息中单击“确定”。

步骤4 在“购买云容器引擎”页面中，根据界面提示进行订单支付。

----结束

2 工作负载

2.1 工作负载异常问题排查

2.1.1 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。

2.1.2 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

2.1.3 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

如果配额不足，您可以**提交工单**申请扩容。

说明

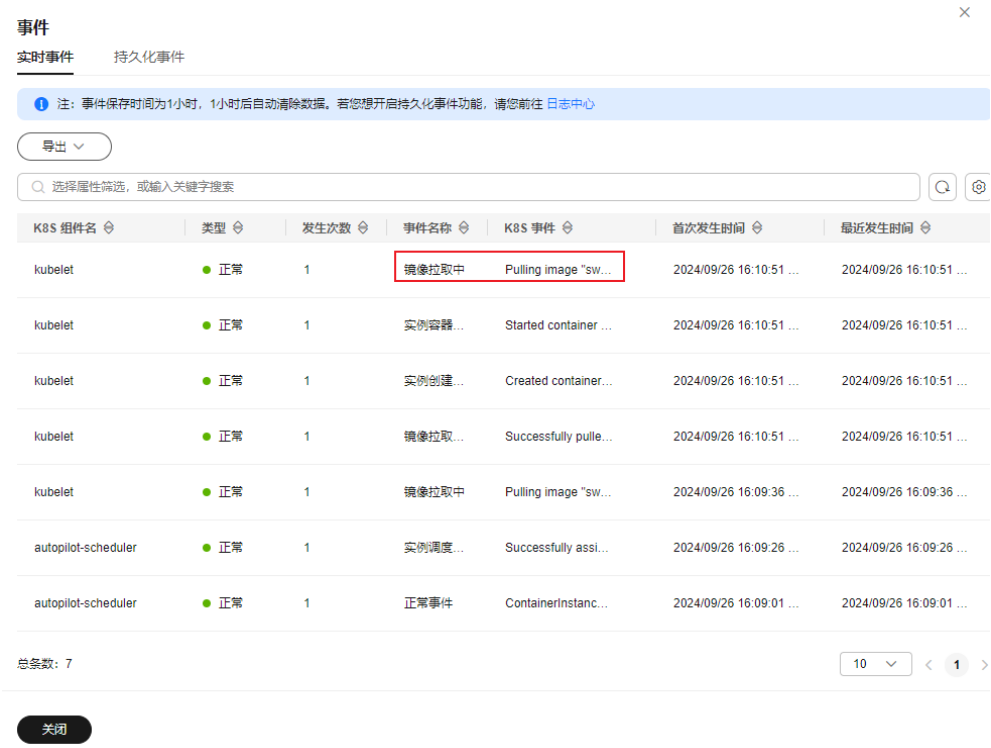
集群中安装的插件实例会占用Pod配额，请合理规划。

2.1.4 创建工作负载时，Pod 不断被重建如何解决?

创建工作负载时，工作负载状态为“处理中”或“未就绪”，内部Pod实例不断被重建。并且查看Pod事件可以发现，创建Pod实例过程中“镜像拉取中（Pulling image xx）”事件停留的时间过长。该现象表明Pod免费提供的30GiB临时存储，不能满足拉取镜像所需的磁盘空间大小，需要对磁盘进行扩容。

图 2-1 Pod 实例被重建

图 2-2 Pod 实例的事件



解决方案

您可以为工作负载添加临时存储空间，以满足拉取镜像所需的磁盘空间。

步骤1 返回CCE控制台，单击集群名称进入集群。

步骤2 左侧列表单击“工作负载”，选择需要重启的工作负载，然后在右侧点击“升级”。在“规格确认 > 单Pod临时存储”中，单击编辑图标，调整至合适的存储大小。

图 2-3 修改单 Pod 临时存储

步骤3 勾选“我已知晓上述计费规则”，单击“升级工作负载”。

----结束

2.2 监控日志

2.2.1 容器监控的内存使用率与实际弹性伸缩现象不一致

问题现象

容器监控的内存使用率与实际弹性伸缩现象不一致，例如容器内存使用率在界面上显示为40%左右，而HPA设置缩容阈值为70%，但界面上显示的内存使用率低于HPA阈值后并没有发生缩容。

问题根因

界面上显示的容器内存使用率与HPA弹性伸缩的内存使用率在计算方式上存在差异：

- 界面上显示的容器内存使用率计算方式为：**container_memory_rss**/内存Limit

  container_memory_rss（即Resident Set Size，RSS）包含了部分可能并不活跃或未被有效利用的内存部分。
- HPA对于内存使用率弹性伸缩的计算方式为：**container_memory_working_set_bytes**/内存Request

  container_memory_working_set_bytes（即Working Set Size，WSS）的计算方式如下：

在Pod中执行**cat /sys/fs/cgroup/memory/memory.stat**，得到total_cache（缓存内存量）、total_rss（当前应用进程实际使用内存量）、total_inactive_file（不活跃文件内存使用量）。

WSS = total_cache + total_rss - total_inactive_file

如果您的应用存在以下情况，均可能导致HPA的扩容行为与预期不符，出现界面上显示的内存使用率低于HPA缩容阈值后并没有发生缩容，或者界面上显示的内存使用率未高于HPA扩容阈值但发生扩容等现象。

- 应用缓存占用非常高，WSS明显大于RSS，导致界面上显示的容器内存使用率小于HPA计算的内存使用率。
- Limit与Request配置差异较大时，Request明显小于Limit，导致界面上显示的容器内存使用率小于HPA计算的内存使用率。

3 网络管理

3.1 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3-1。

表 3-1 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3-2**。

表 3-2 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 3-3 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。

3.2 如何确认网卡不被集群占用?

操作场景

在CCE Autopilot集群中，1.27.8-r0，1.28.6-r0及以上版本的集群支持删除容器子网。

删除集群容器子网属于高危操作，您需要确保当前集群正在使用的网卡中没有网卡属于该子网。

操作步骤

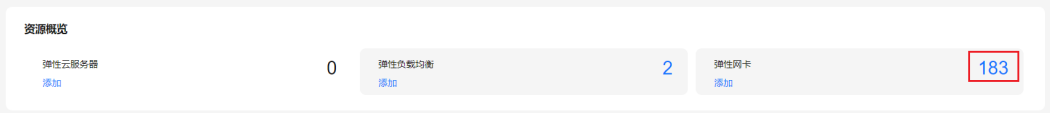
步骤1 登录**CCE控制台**，单击集群列表中的集群名称。

步骤2 在左侧导航栏中选择“配置中心”，切换至“网络配置”页签。

步骤3 查看“容器网络配置”，以default-network（默认容器子网）为例，复制容器子网的“网络ID”。

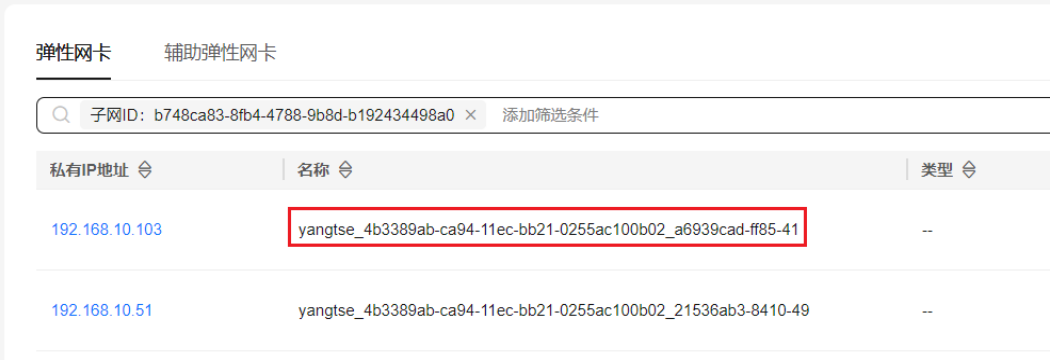
步骤4 登录**网络控制台**，在左侧导航栏中选择“虚拟私有云 > 子网”，并根据容器子网的“网络ID”进行过滤，找到对应的子网。

步骤5 单击进入子网，选择“基本信息”页签，在“资源概览”中单击进入弹性网卡，查看该子网下的“弹性网卡”和“辅助弹性网卡”。



步骤6 查看网卡“名称”或者“描述”，如果其中包含当前集群的ID，表示网卡被集群占用。您可以在**CCE控制台**的集群“概览”页中查看集群ID。

如果需要清理集群内使用的子网网卡，需要提交**提交工单**。



----结束

4 存储管理

4.1 CCE Autopilot 集群中的 EVS 存储卷被删除或者过期后是否可以恢复?

云硬盘EVS存储需要人工配置备份策略。如果卷被删除或者释放，可以使用云硬盘备份恢复数据。

详细请参见**备份云硬盘**。

4.2 创建存储卷失败如何解决?

现象描述

创建PV或PVC失败，在事件中看到如下信息。

```
{"message": "Your account is suspended and resources can not be used.", "code": 403}
```

问题根因

事件信息表示账号被停用或没有权限，请检查账号状态是否正常。

如账号正常请查看该用户的命名空间权限，您需要拥有该命名空间的开发权限、运维权限或管理员权限之一，或者包含PVC/PV读写操作的自定义权限。详情请参见**配置命名空间权限（控制台）**。

4.3 CCE Autopilot 集群云存储 PVC 能否感知底层存储故障?

CCE Autopilot集群PVC按照社区逻辑实现，PVC本身的定义是存储声明，与底层存储解耦，不负责感知底层存储细节，因此没有感知底层存储故障的能力。

云监控服务CES 具备查看云服务监控指标的能力：云监控服务基于云服务自身的服务属性，已经内置了详细全面的监控指标。当用户在云平台上开通云服务后，系统会根据服务类型自动关联该服务的监控指标，帮助用户实时掌握云服务的各项性能指标，精确掌握云服务的运行情况。

建议有存储故障感知诉求的用户配套云监控服务CES的云服务监控能力使用，实现对底层存储的监控和告警通知。

4.4 删除动态创建的 PVC 之后，底层存储有残留如何解决?

问题现象

删除集群中动态创建的PVC，PVC使用的StorageClass中reclaimPolicy为Delete模式，但删除PVC时底层存储却没有被同步删除。

触发场景

- 同时删除PVC和与其绑定的PV，会出现底层存储没有被同步删除的情况。
- 在删除PVC前，尝试直接删除PV，但由于PV被PVC绑定而受到保护无法直接删除。然后再删除PVC，就会出现底层存储没有被同步删除的情况。

问题根因

在开源csi-provisioner模块业务逻辑中，常规情况下删除动态创建的PVC，会先删除PVC，待PVC资源删除成功后，将PV状态更新为Released。csi-provisioner会监听到PV更新事件，开始执行删底层卷的流程，等底层卷删除成功后，再下发删除PV的请求，这样即完成了“PVC-底层卷-PV”的完整删除链。

异常操作过程中，未删除PVC的情况下直接删除PV，但由于PV上有kubernetes.io/pv-protection这个finalizer，无法立即删除，但会给PV加上deletionTimestamp。随后删除PVC，PVC资源删除成功后，PV状态更新为Released，csi-provisioner监听到PV更新事件，但由于PV上有deletionTimestamp，csi-provisioner认为不需要删除底层卷，于是跳过删底层卷的流程，直接开始删除PV，这样PVC和PV被成功删除，但是底层卷残留。关于此问题的逻辑代码请参见**controller**。

解决方案

1. 对于已残留的底层存储，请通过手动删除的方式进行清理。
2. 对于未删除的动态创建PVC，请直接删除PVC，其绑定的PV和底层存储会被自动删除，无需手动删除。

5 权限

5.1 能否只配置命名空间权限，不配置集群管理权限?

命名空间权限和集群管理权限是相互独立又相互补充的两个权限体系：

- 命名空间权限：作用于集群内部，用于管理集群资源操作（如创建工作负载等）。
- 集群管理（IAM）权限：云服务层面的权限，用于管理CCE Autopilot集群与周边资源（如VPC、ELB、ECS等）的操作。

对于IAM Admin用户组的管理员用户来说，可以为IAM子用户授予集群管理权限（如CCE Administrator、CCE FullAccess等），也可以在CCE控制台授予某个集群的命名空间权限。但由于CCE控制台界面权限是由IAM系统策略进行判断，如果IAM子用户未配置集群管理（IAM）权限，该子用户将无法进入CCE控制台。

如果您无需使用CCE控制台，只使用kubectl命令操作集群中的资源，则不受集群管理（IAM）权限的影响，您只需要获取具有命名空间权限的配置文件（kubeconfig），详情请参考**如果不配置集群管理权限的情况下，是否可以使用API呢？**。集群配置文件在传递过程中可能存在泄露风险，应在实际使用中注意。

5.2 如果不配置集群管理权限的情况下，是否可以使用 API 呢?

CCE Autopilot集群提供的API可以分为云服务接口和集群接口：

- 云服务接口：支持操作云服务层面的基础设施（如创建节点），也可以调用集群层面的资源（如创建工作负载）。

  使用云服务接口时，必须配置集群管理（IAM）权限。
- 集群接口：直接通过Kubernetes原生API Server来调用集群层面的资源（如创建工作负载），但不支持操作云服务层面的基础设施（如创建节点）。

  使用集群接口时，无需配置集群管理（IAM）权限，仅需在调用集群接口时带上集群证书。但是，集群证书需要有集群管理（IAM）权限的用户进行**下载**，在证书传递过程中可能存在泄露风险，应在实际使用中注意。

5.3 如果不配置集群管理权限，是否可以使用 kubectl 命令呢?

使用kubectl命令无需经过IAM认证，因此理论上不配置集群管理（IAM）权限是可以使用kubectl命令的。但前提是需要获取具有命名空间权限的kubectl配置文件（kubeconfig），以下场景认证文件传递过程中均存在安全泄露风险，应在实际使用中注意。

- 场景一

  如果某IAM子用户先配置了集群管理权限和命名空间权限，然后在界面下载kubeconfig认证文件。后面再删除集群管理权限（保留命名空间权限），依然可以使用kubectl来操作Kubernetes集群。因此如需彻底删除用户权限，必须同时删除该用户的集群管理权限和命名空间权限。

- 场景二

  如果某IAM用户拥有一定范围的集群管理权限和命名空间权限，然后在界面下载kubeconfig认证文件。此时CCE Autopilot集群根据用户信息的权限判断kubectl有权限访问哪些Kubernetes资源，即哪个用户获取的kubeconfig文件，kubeconfig中就拥有哪个用户的认证信息，任何人都可以通过这个kubeconfig文件访问集群。

5.4 IAM 用户无法使用调用 API

问题现象

使用IAM用户调用API时，出现以下报错：

```
"code":403,"message":"This user only supports console access, not programmatic access."
```

该错误表示IAM用户没有编程访问权限。

解决方案

步骤1 请联系主账号管理员，登录**统一身份认证服务**。

步骤2 找到需要修改的IAM用户，单击用户名称。

步骤3 修改“访问方式”，同时勾选“编程访问”和“管理控制台访问”。

图 5-1 修改 IAM 用户访问方式

步骤4 单击“确定”。

----结束

