华为云 UCS

常见问题

文档版本 01

发布日期 2024-09-11

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 产品咨询

1.1 UCS 有哪些配额限制?

什么是 UCS 配额?

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。UCS具有集群、舰队、权限、集群联邦，以及容器智能分析实例配额限制。

- 集群配额：UCS支持接入的集群数量上限，华为云集群和附着集群的数量均占用该配额值。
- 舰队配额：用户拥有的舰队数量上限。
- 权限配额：用户可以在“权限管理”页面创建的权限数量上限。
- 集群联邦配额：用户可以开通的集群联邦数量上限。
- 容器智能分析实例配额：用户可以创建的容器智能分析实例数量上限。

用户在使用UCS时也会使用其他云服务，例如弹性云服务器、云硬盘、虚拟私有云、弹性负载均衡、容器镜像服务、云解析服务等。其他云服务配额与UCS配额相互独立，由各服务自行管理，详情请参见**关于配额**。

UCS 配额是多少?

UCS的配额限制项及其默认值如**表1 UCS配额项**所示。如UCS提供的默认配额无法满足使用需要，您可以申请扩大配额。

说明

暂不支持申请扩大集群联邦和容器智能分析实例的配额。

表 1-1 UCS 配额项

配额项	默认配额值
集群	50
舰队	50

配额项	默认配额值
权限	50
集群联邦	1
容器智能分析实例	1

如何申请扩大 UCS 配额?

如需扩大UCS配额，需要您联系技术支持进行申请。

步骤1 登录管理控制台。

步骤2 在页面右上角，选择“工单 > 新建工单”。

系统进入“新建工单”页面。

步骤3 在“新建工单”页面提交工单。

其中，问题所属产品选择“业务类 > 配额类”，问题类型选择“配额申请”，问题描述填写需要调整的内容和申请原因，其他参数按需填写。

步骤4 填写完毕后，勾选协议并单击“提交”。

----结束

2 计费相关

2.1 UCS 如何定价/收费?

计费模式

UCS提供包年/包月和按需计费两种计费模式，以满足不同场景下的用户需求。

- 包年/包月：一种预付费模式，即先付费再使用，按照订单的购买周期进行结算。购买周期越长，享受的折扣越大。一般适用于接入集群规模长期稳定的成熟业务。
- 按需计费：一种后付费模式，即先使用再付费，按照UCS实际使用时长计费，按小时结算。按需计费模式允许您根据实际业务需求灵活地调整服务使用，无需提前购买付费，灵活性高。一般适用于接入集群规模较小的业务场景。

计费项

使用UCS服务时，会产生UCS服务管理费用，具体内容如**表1 UCS计费项**所示。

表 2-1 UCS 计费项

计费项	说明	适用的计费模式	计费公式
UCS集群管理服务	• UCS集群管理服务费用由集群类型（包括华为云集群、本地集群、附着集群、多云集群和伙伴云集群）、集群vCPU容量和购买时长决定。 • UCS服务管理费用不包括任何资源（例如计算节点、网络服务等）相关的费用。	包年/包月、按需计费	**集群规模 * 规格单价 * 购买时长** 具体定价请参见**UCS价格详情**。

2.2 集群在何种状态下时，UCS 会产生计费?

集群状态的变化会影响UCS对其vCPU数量的统计，从而影响UCS服务的计费。若集群需要使用UCS服务，请保证其在正常运行状态；若集群不再需要使用，请及时注销，避免持续扣款。

不同集群状态是否造成UCS计费的情况见**表1 集群状态与计费**。

表 2-2 集群状态与计费

集群状态	是否计费
运行中	是
不可用	是 **说明** 当集群接入UCS之后，UCS会获取用户集群vCPU的使用量并记录。如果之后集群状态变为“不可用”，导致UCS无法获取到最新的集群vCPU使用量信息，UCS会根据最后一次记录到的vCPU使用量进行计费。
等待接入	否
注册超时	否
注销中	否
注销失败	否

2.3 已购买资源包，为什么仍然产生按需计费?

请按**表2-3**识别产生按需计费的原因，并重新选择正确的资源包或保证账户中的余额充足。

表 2-3 排查思路

可能原因	处理措施
购买套餐包中集群类型与实际接入的集群类型不一致	购买所接入集群类型对应的套餐包
购买套餐包中集群规模小于实际接入的集群规模	购买集群规模更大的、符合所接入集群规模的套餐包，或保证账户中的余额充足

2.4 UCS 服务的计费方式如何由按需改为包年/包月?

当前UCS支持“按需计费”和“包年/包月”两种计费方式。当您希望以包年/包月套餐包的优惠价格使用UCS时，只需按照所接入UCS的集群类型、集群规模购买对应的套餐包，即可由按需计费模式转变为包年/包月计费模式。

2.5 华为云支持哪几种开具发票模式?

华为云支持“按账期索取发票”和“按订单索取发票”模式。

您可在费用中心的**发票管理**开具发票。

2.6 资源包是否支持退订或修改?

已购买的套餐包暂时不支持退订或修改。

3 权限相关

3.1 如何配置 UCS 控制台各功能的访问权限?

问题描述

UCS控制台的各项功能主要通过IAM进行权限控制，未经授权的用户访问UCS控制台中相应的页面，将出现“无访问权限”、“权限认证失败”等类似错误信息。

解决方案

管理员需要为用户授予UCS控制台各功能的权限，通过IAM系统策略（包括UCS FullAccess、UCS CommonOperations、UCS CIAOperations和UCS ReadOnlyAccess）来界定用户的权限范围。

表 3-1 UCS 系统权限

系统角色/策略名称	描述	类别
UCS FullAccess	UCS服务管理员权限，拥有该权限的用户拥有服务的所有权限（包含制定权限策略、安全策略等）。	系统策略
UCS CommonOperations	UCS服务基本操作权限，拥有该权限的用户可以执行创建工作负载、流量分发等操作。	系统策略
UCS CIAOperations	UCS服务容器智能分析管理员权限。	系统策略
UCS ReadOnlyAccess	UCS服务只读权限（除容器智能分析只读权限）。	系统策略

另外，华为云各服务之间存在业务交互关系，UCS也依赖其他云服务实现一些功能（如镜像仓库、域名解析），因此，上述几种系统策略经常和其他云服务的角色或策

略结合使用，以达到精细化授权的目的。管理员在为IAM用户授权时，应该遵循权限最小化的安全实践原则，**表3-2**列举了UCS各功能管理员、操作、只读权限所需要的最小权限。

说明

授予用户IAM系统策略的详细操作请参见**UCS服务资源权限**；授予用户UCS RBAC权限的详细操作请参见**集群中Kubernetes资源权限**。

表 3-2 UCS 功能所需的最小权限

功能	权限类型	权限范围	最小权限
容器舰队	管理员权限	• 创建、删除舰队 • 注册华为云集群（CCE集群、CCE Turbo集群）、本地集群或附着集群 • 注销集群 • 将集群加入、移出舰队 • 为集群或舰队关联权限 • 开通集群联邦、联邦管理相关操作（如创建联邦工作负载、创建域名访问等）	UCS FullAccess
	只读权限	查询集群、舰队的列表或详情	UCS ReadOnlyAccess
华为云集群	管理员权限	对华为云集群及集群下所有Kubernetes资源对象（包含节点、工作负载、任务、服务等）的读写权限。	UCS FullAccess + CCE Administrator
	操作权限	对华为云集群及集群下大多数Kubernetes资源对象的读写权限，对命名空间、资源配额等Kubernetes资源对象的只读权限。	UCS CommonOperations + CCE Administrator
	只读权限	对华为云集群及集群下所有Kubernetes资源对象（包含节点、工作负载、任务、服务等）的只读权限。	UCS ReadOnlyAccess + CCE Administrator
本地/附着/多云/伙伴云集群	管理员权限	本地/附着/多云/伙伴云集群及集群下所有Kubernetes资源对象（包含节点、工作负载、任务、服务等）的读写权限。	UCS FullAccess
	操作权限	本地/附着/多云/伙伴云集群及集群下大多数Kubernetes资源对象的读写权限，对命名空间、资源配额等Kubernetes资源对象的只读权限。	UCS CommonOperations + UCS RBAC权限（需要包含namespaces资源对象的list权限）

功能	权限类型	权限范围	最小权限
	只读权限	本地/附着/多云/伙伴云集群及集群下所有Kubernetes资源对象（包含节点、工作负载、任务、服务等）的只读权限。	UCS ReadOnlyAccess + UCS RBAC权限（需要包含namespaces资源对象的list权限）
镜像仓库	管理员权限	容器镜像服务的所有权限，包括创建组织、上传镜像、查看镜像列表或详情、下载镜像等操作。	SWR Administrator
权限管理	管理员权限	● 创建、删除权限 ● 查看权限列表或详情 **说明** 创建权限需要同时授予子用户IAM ReadOnlyAccess权限（IAM服务的只读权限），用于获取IAM用户列表。	UCS FullAccess + IAM ReadOnlyAccess
	只读权限	查看权限列表或详情	UCS ReadOnlyAccess + IAM ReadOnlyAccess
策略中心	管理员权限	● 启用策略中心 ● 创建、停用策略实例 ● 查看策略列表 ● 查看策略实施详情	UCS FullAccess
	只读权限	对于已启用策略中心的舰队和集群，拥有该权限的用户可以查看策略列表和查看策略实施详情。	UCS CommonOperations 或 UCS ReadOnlyAccess
服务网格	管理员权限	应用服务网格的所有权限，包括创建网格、添加集群、sidecar注入、查看网格列表或详情、卸载网格等。	CCE Administrator
流量分发	管理员权限	创建流量策略、暂停调度策略、删除调度策略等操作。	（推荐）UCS CommonOperations + DNS Administrator 或 UCS FullAccess + DNS Administrator
	只读权限	查看流量策略列表或详情	UCS ReadOnlyAccess + DNS Administrator
容器智能分析	管理员权限	● 接入、取消接入集群 ● 查看基础设施、应用负载等多维度监控数据	UCS CIAOperations

功能	权限类型	权限范围	最小权限
云原生服务中心	管理员权限	云原生服务中心的所有权限，包括订阅服务、查看服务列表或详情、创建服务实例、查看实例列表或详情、删除服务实例、退订服务等操作。	UCS FullAccess
	只读权限	云原生服务中心的只读权限，包括查看服务列表或详情、查看实例列表或详情等操作。	UCS ReadOnlyAccess

3.2 IAM 用户登录 UCS 无法获取集群或舰队怎么办?

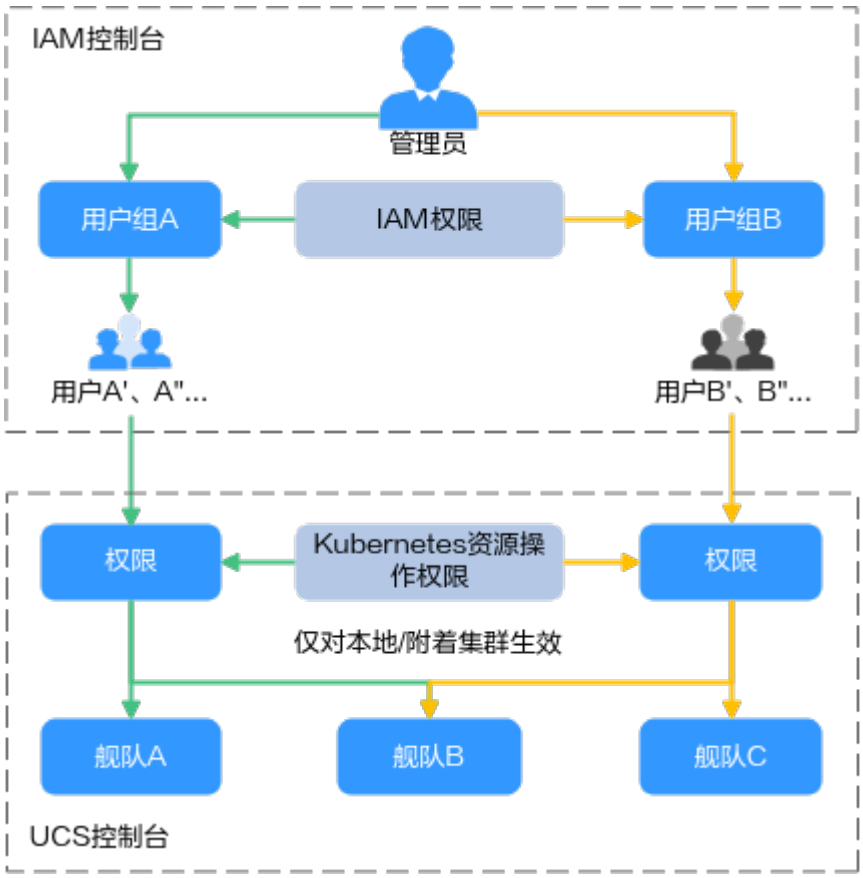
问题描述

IAM用户登录UCS控制台，前往“容器舰队”页面后，无法获取已创建的舰队和已注册的集群（“容器舰队”和“未加入舰队的集群”页面均为空）。

解决方案

大多数IAM用户无法获取集群的问题，都和权限未设置或者设置不正确有关，IAM用户必须同时拥有UCS系统策略权限和集群资源对象操作权限，才可以获取集群信息。您需要联系管理员按照**图3-1**所示流程为自己授权。

图 3-1 授权示意图



步骤1 管理员登录IAM控制台，为IAM用户所在用户组授予UCS系统策略权限。

根据操作范围选择授予何种系统策略。例如：查询集群、舰队的列表或详情，查询集群资源对象（包含节点、工作负载、任务、服务等），这些操作只需要授予UCS ReadOnlyAccess只读权限即可，如图3-2所示。

图 3-2 用户组只读权限

集群、舰队权限列表中展示了不同权限范围所需的最小权限，管理员依据该表格来授权就可以。

步骤2 管理员登录UCS控制台，为IAM用户授予集群资源对象操作权限。

操作方法如下：

说明

UCS控制台的“权限管理”仅针对本地或附着集群生效，对于华为云集群的资源操作权限，请授予CCE Administrator权限。

1. 在“权限管理”页面创建权限（选择“只读权限”类型，表示对所有集群资源对象的只读权限）。
2. 将创建的权限关联至舰队，或者未加入舰队的集群。

----结束

集群、舰队权限列表

功能	权限类型	权限范围	最小权限
容器舰队	管理员权限	• 创建、删除舰队 • 注册华为云集群（CCE集群、CCE Turbo集群）、本地集群或附着集群 • 注销集群 • 将集群加入、移出舰队 • 为集群或舰队关联权限 • 开通集群联邦、联邦管理相关操作（如创建联邦工作负载、创建域名访问等）	UCS FullAccess
	只读权限	查询集群、舰队的列表或详情	UCS ReadOnlyAccess
华为云集群	管理员权限	对华为云集群及所有集群资源对象（包含节点、工作负载、任务、服务等）的读写权限。	UCS FullAccess + CCE Administrator
	操作权限	对华为云集群及大多数集群资源对象的读写权限，对命名空间、资源配额等Kubernetes资源对象的只读权限。	UCS CommonOperations + CCE Administrator
	只读权限	对华为云集群及所有集群资源对象（包含节点、工作负载、任务、服务等）的只读权限。	UCS ReadOnlyAccess + CCE Administrator
本地/附着集群	管理员权限	对本地/附着集群及所有集群资源对象（包含节点、工作负载、任务、服务等）的读写权限。	UCS FullAccess
	操作权限	对本地/附着集群及大多数集群资源对象的读写权限，对命名空间、资源配额等Kubernetes资源对象的只读权限。	UCS CommonOperations + UCS RBAC权限（需要包含namespaces资源对象的list权限）

功能	权限类型	权限范围	最小权限
	只读权限	对本地/附着集群及所有集群资源对象（包含节点、工作负载、任务、服务等）的只读权限。	UCS ReadOnlyAccess + UCS RBAC权限（需要包含namespaces资源对象的list权限）

3.3 误删除或修改 ucs_admin_trust 委托后如何恢复?

问题描述

ucs_admin_trust委托为管理员账号首次登录UCS控制台时，由用户授权UCS云服务后创建的。删除或者修改委托（如：修改委托账号op_svc_ucs，删除其中的Tenant Administrator权限）均会导致UCS服务功能异常，例如：“容器舰队”页面无法获取舰队和舰队中的集群。

本文指导您恢复ucs_admin_trust委托。

操作步骤

步骤1 使用管理员账号登录IAM控制台。

步骤2 在左侧导航栏选择“委托”。

步骤3 选择“ucs_admin_trust”委托，单击操作列的“删除”，在弹出的确认窗口中单击“是”。

步骤4 在左侧导航栏选择“委托”。

说明

ucs_admin_trust委托已经删除的情况下不需要执行本步骤。其他误修改的操作（例如删除了其中的Tenant Administrator权限）均需要删除当前委托，以便创建新的委托。

步骤5 进入UCS控制台，在弹出的“授权说明”对话框，单击“确认”，UCS会重新创建ucs_admin_trust委托，恢复业务。

----结束

3.4 舰队或集群关联权限异常怎么办?

问题描述

在舰队或未加入舰队的集群关联权限过程中，可能会因为集群接入异常而导致权限关联异常。当这种情况发生时，舰队或集群的“关联权限”页面会显示详细的权限关联异常事件。请先排查并修复集群中出现的异常，然后单击“重试”按钮重新关联权限策略。

排查思路

舰队或集群关联权限时出现异常事件的排查思路大致可根据报错信息进行定位，如表3-3所示。

表 3-3 报错信息说明

报错信息	说明	推荐排查项
ClusterRole failed reason:Get \"https://kubernetes.default.svc.cluster.local/apis/rbac.authorization.k8s.io/v1/clusterroles/XXXXXXX?timeout=30s\": Precondition Required" Or Get ClusterRole failed reason:an error on the server (\"unknown\") has prevented the request from succeeding (get clusterroles.rbac.authorization.k8s.io	出现该错误的原因大概率为集群还未接入，接入集群中的proxy-agent运行状态异常，或者网络异常。	• 排查项一：proxy-agent的运行状态 • 排查项二：集群与UCS网络连接状态
Unauthorized	出现该错误的原因可能是多样的，请根据实际状态码进行排查。 例如状态码401表示用户没有访问权限，可能的原因是集群认证信息过期。	• 排查项三：集群认证信息变化
Get cluster namesapce[x] failed. Or Reason:namespace "x" not found.	出现该错误的原因是集群内没有对应的命名空间。	在集群下创建对应的命名空间并进行重试操作。 如：**kubectl create namespace** *ns_name* 如果不需要使用该命名空间，该异常事件可以忽略。

排查项一：proxy-agent 的运行状态

须知

集群从UCS注销后，原有proxy-agent配置文件中包含的认证信息将会失效，请同时删除集群中已部署的proxy-agent实例。如需再次接入UCS，必须重新从UCS控制台下载proxy-agent配置文件进行部署。

步骤1 登录目标集群Master节点。

步骤2 查看集群代理部署状态。

kubectl -n kube-system get pod | grep proxy-agent

如果部署成功，预期输出如下：

```
proxy-agent-*** 1/1 Running 0 9s
```

说明proxy-agent部署正常，如proxy-agent没有处于正常Running状态，可以使用**kubectl -n kube-system describe pod proxy-agent-***查看Pod的告警信息，详细排查思路可参考**proxy-agent部署失败怎么办？** 。

说明

proxy-agent默认部署两个Pod实例，存在一个Pod正常Running即可使用基本功能，但是高可用性无法保证。

步骤3 打印proxy-agent的Pod日志，查看代理程序是否可以连接到UCS。

kubectl -n kube-system logs proxy-agent-* | grep "Start serving"**

如没有“Start serving”的日志打印但是proxy-agent实例状态正常，则需要继续检查其他排查项。

----结束

排查项二：集群与 UCS 网络连接状态

公网接入：

步骤1 检查集群是否绑定公网IP或配置公网NAT网关。

步骤2 检查集群安全组的出方向是否放通。如需对出方向做访问控制，请联系技术支持获取目的地址和端口号。

步骤3 解决网络问题后，删掉已有的proxy-agent Pod使其重新生成Pod资源，查看新建Pod的日志中是否存在“Start serving”的日志打印。

kubectl -n kube-system logs proxy-agent-* | grep "Start serving"**

步骤4 日志正常打印后，刷新UCS控制台页面，查看集群是否正常连接。

----结束

私网接入：

步骤1 检查集群安全组的出方向是否放通。如需对出方向做访问控制，请联系技术支持获取目的地址和端口号。

步骤2 排除集群与UCS和IDC之间的网络连接故障。

根据网络连接方式不同，请参考以下文档进行故障排除。

- 云专线（DC）：请参考**故障排除**。
- 虚拟专用网络（VPN）：请参考**故障排除**。

步骤3 排除集群私网接入的VPCEP故障，VPCEP状态需为“已接受”。如VPCEP被误删除，则需重新创建，请参见**私网接入的集群误删除VPCEP后如何恢复？** 。

图 3-3 VPCEP 状态

步骤4 解决网络问题后，删掉已有的proxy-agent Pod使其重新生成Pod资源，查看新建Pod的日志中是否存在“Start serving”的日志打印。

kubectl -n kube-system logs proxy-agent-* | grep "Start serving"**

步骤5 日志正常打印后，刷新UCS控制台页面，查看集群是否正常连接。

----结束

排查项三：集群认证信息变化

如错误显示“cluster responded with non-successful status: [401] [Unauthorized]”，通过观察集群三个Master节点“/var/paas/sys/log/kubernetes/auth-server.log”日志，可能是IAM网络连通故障。请确认IAM域名解析能力，及IAM服务连通性正常。

常见问题日志如下：

- Failed to authenticate token: *******: dial tcp: lookup iam.myhuaweicloud.com on *.*.*.*:53: no such host

  此类日志说明，节点缺少对iam.myhuaweicloud.com解析能力，请参考**安装前准备**，配置对应的域名解析。

- Failed to authenticate token: Get *******: dial tcp *.*.*.*:443: i/o timeout

  此类日志说明，节点访问IAM服务超时，请确保节点与华为云IAM服务能正常通信。

- currently only supports Agency token

  此类日志说明请求不是从UCS服务发起，目前本地集群只支持UCS服务IAM Token访问。

- IAM assumed user has no authorization/iam assumed user should allowed by TEAdmin

  此类日志说明UCS服务访问集群故障，请联系华为技术人员进行排障。

- Failed to authenticate token: token expired, please acquire a new token

  此类日志说明Token存在过期现象，请使用**date**命令确定时间是否差距过大，如果节点时间与标准时间差距过大，请同步时间后，查看集群是否恢复。如果长时间未恢复，可能需要重装集群，请联系华为技术人员进行排障。

解决上述问题后，请使用**crictl ps | grep auth | awk '{print $1}' | xargs crictl stop**命令重启auth-server容器。

3.5 集群注销后如何清理权限相关资源?

在集群从UCS注销后，可能会存在一些RBAC资源残留，您可以根据以下建议清理这些资源。

UCS创建的RBAC资源带有标签"ucs.rbac.policy=true"，您可以利用此标签对UCS创建的RBAC资源进行查询、删除等操作。

例如：

```
root@lijunhui-ucs-test-0001:~# kubectl get clusterrolebinding -l ucs.rbac.policy=true
NAME                                          ROLE                                                AGE
7281269b-caf5-11ed-82cb-0255ac10018e-binding   ClusterRole/7281269b-caf5-11ed-82cb-0255ac10018e   52s
```

```
root@lijunhui-ucs-test-0001:~# kubectl get rolebinding -n default -l ucs.rbac.policy=true
NAME                                          ROLE                                          AGE
7281269b-caf5-11ed-82cb-0255ac10018e-binding   Role/7281269b-caf5-11ed-82cb-0255ac10018e   45h
```

3.6 如何精细化管理集群联邦权限?

1. 如果您在访问联邦资源时出现如下错误提示，说明您没有对应资源的操作权限，请您向您的管理员申请授予对应的权限，创建对应的Role/RoleBinding或者ClusterRole/ClusterRolebinding权限。

   ```
   root@wm-0:/tmp#
   root@wm-0:/tmp# kubectl --kubeconfig config get deploy
   Error from server (Forbidden): deployments.apps is forbidden: User "0bbdb118ec314ebfa54d6e83fe7e9b3c" cannot list resource "deployments" in API group "apps" in the namespace "default"
   root@wm-0:/tmp#
   ```

2. 如果出现“no such host”问题，请按以下步骤进行排查：

   ```
   root@wm-0:/tmp#
   root@wm-0:/tmp# kubectl  --kubeconfig config  get pods
   Unable to connect to the server: dial tcp: lookup vpcep-dc7a9852[redacted]d7ae.cn-north-7.huaweicloud.com on 127.0.0.53:53: no such host
   ```

   查询VPCEP节点是否存在，是否被误删，使用以下命令获取 vpcep 终端节点 id：

   ```
   server=`cat config  | jq '.clusters[0].cluster.server'` echo ${server:15:36}
   ```

   检查上述终端节点是否存在，如果存在，检查执行机是否和 VPCEP 终端节点位于同一VPC中，二者之间网络是否连通。

3. 如果出现“You must be logged in to the server (Unauthorized)”问题，请按以下步骤检查：

   ```
   root@wm-0:/tmp#
   root@wm-0:/tmp# kubectl  --kubeconfig kubeconfig get pods
   error: You must be logged in to the server (Unauthorized)
   root@wm-0:/tmp#
   ```

   - 校验证书是否有误：

     将证书保存至临时文件中。

     ```
     cd ~/.kube
     cat config  | jq '.clusters[0].cluster."certificate-authority-data"' | tr -d '"' | base64 -d > ca.crt
     cat config  | jq '.users[0].user."client-certificate-data"' | tr -d '"' | base64 -d > tls.crt
     cat config  | jq '.users[0].user."client-key-data"' | tr -d '"' | base64 -d > tls.key
     ```

     进行校验。

     ```
     openssl verify -CAfile ca.crt tls.crt
     ```

     如果输出"tls.crt: OK"说明CA无误，否则需要重新下载kubeconfig。

   - 输入如下命令，检查证书公钥和私钥是否匹配：

     ```
     diff -eq <(openssl x509 -pubkey -noout -in tls.crt) <(openssl rsa -pubout -in tls.key)
     ```

     如果输出"writing RSA key"，说明证书公钥和私钥匹配，否则说明不匹配，需要重新下载kubeconfig，验证完毕后删除临时文件：

     ```
     rm -f ca.crt tls.crt tls.key
     ```

   - 检查证书是否过期。

     首先保存证书到临时文件：

     ```
     cd ~/.kube
     cat config  | jq '.users[0].user."client-certificate-data"' | tr -d '"' | base64 -d > tls.crt
     ```

     查看证书有效期。

     ```
     openssl x509 -noout -text -in tls.crt  | grep -E "Not Before|Not After"
     ```

     会输出如下图所示的证书有效区间，请确认当前证书是否在有效期内，如果过期请重新下载 kubeconfig，并删除临时文件。


```
rm -f tls.crt
```

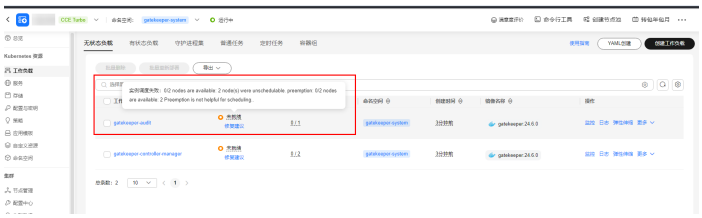
```
root@ecs-9c87:/tmp/tmpd.vw7YeK# openssl x509 -noout -text -in tls.crt  | grep -E "Not Before|Not After"
            Not Before: Jul 31 14:55:43 2023 GMT
            Not After : Jul 29 14:55:43 2028 GMT
```

4 策略中心

4.1 启用策略中心失败怎么办?

策略中心启用失败时，根据失败情况请使用以下方案排查修复：

- 如果提示“wait for plugins status become health time out”，请检查集群状态是否正常，集群资源是否足够。检查无误后单击“重新启用”。
- 如果在启用策略中心后，集群列表页面或者策略实例页面显示启用失败，请按以下步骤进行排查：
  a. 请至集群列表页面，跳转至集群的工作负载页面，检查gatekeeper-system命名空间下的策略管理实例插件是否运行正常。
  b. 如果运行异常，请通过工作负载的事件排查插件实例异常的原因。
  如下图：



- 如果提示其他错误信息，请直接单击“重新启用”。

4.2 策略中心运行异常怎么办?

策略中心运行异常的可能原因为Gatekeeper插件损坏，或者被删除。根据失败情况请使用以下方案排查修复：

- 检查gatekeeper-system命名空间中gatekeeper-controller-manager、gatekeeper-audit这两个Deployment是否为就绪状态，如果不是，请自行排查未就绪原因。
- 如果这两个Deployment被删除，则可以先将策略中心功能停用后再重新启用。

4.3 如何清理策略中心相关资源?

对于已启用策略中心功能的集群，在以下场景中，可能会存在资源残留情况：

- 集群连接中断时，停用策略中心
- 集群停用策略中心过程中，连接中断
- 集群连接中断后，注销集群
- 集群连接中断后，移出舰队

因此需要执行如下命令，清理残留资源：

kubectl delete namespace gatekeeper-system

5 容器舰队

5.1 舰队开通联邦校验失败怎么办?

问题背景

舰队开通集群联邦功能后，UCS服务会把当前舰队已存在的集群及新加入到舰队的集群自动添加到联邦中。添加过程中，舰队会对集群的网络状态、集群版本、clusterrole、clusterrolebinding等项目做校验。如果添加过程中校验存在问题，集群加入联邦会失败。参考本章节内容修复问题后，可以单击“重新接入”尝试再次接入集群联邦。

现象一：提示 clusterrole、clusterrolebinding 已存在

问题原因：一个集群不能同时加入两个或两个以上的联邦。有这个报错提示，说明当前集群已经添加到联邦中，或者曾经加入过联邦但是存在资源残留。

解决方案：手工清理残留资源。

操作步骤：

步骤1 获取报错集群的kubeconfig配置文件，并准备kubectl及运行节点，将kubeconfig文件放在运行节点/tmp目录。

步骤2 执行如下命令，清理残留资源。

```
alias kubectl='kubectl --kubeconfig=/tmp/kubeconfig'

kubectl delete clusterrolebinding `kubectl get clusterrolebinding |grep karmada-controller-manager | awk '{print $1}'`

kubectl delete clusterrole `kubectl get clusterrole |grep karmada-controller-manager | awk '{print $1}'`

kubectl delete namespace `kubectl get namespace |egrep 'karmada-[0-9a-f]{8}-([0-9a-f]{4}-){3}[0-9a-f]{12}' |awk '{print $1}'`
```

----结束

现象二：提示 CCE 集群需要绑定 EIP

问题原因：舰队启用联邦后，访问CCE集群，当前需要通过EIP解决网络连接问题。

解决方案：给CCE集群绑定EIP。详细操作请参考**使用kubectl连接集群**。

现象三：CCE 集群已绑定 EIP，集群加入联邦仍失败，报错：network in cluster is stable, please retry it later

问题原因：联邦需要访问CCE集群的5443端口，但是CCE集群的控制面安全组入方向规则不允许124.70.21.61（源地址）访问CCE集群的5443端口。

解决方案：修改CCE控制面入方向安全组，允许124.70.21.61（源地址）访问CCE集群的5443端口。

现象四：显示已接入集群联邦，状态异常，报错：cluster is not reachable

请在对应的成员集群中执行以下命令，查询ServiceAccount是否存在。其中{cluster_name}请替换为集群名称。

kubectl get sa -A|grep karmada-{cluster_name}.clusterspace.{cluster_name}

若回显显示ServiceAccount不存在，请先将该成员集群移出舰队，再重新添加该集群至对应舰队。

5.2 集群联邦升级前检查不通过怎么办?

问题背景

升级集群联邦前，UCS会对联邦运行状态、集群运行状态、集群接入状态三方面进行检查，尽可能避免升级失败。如有检查异常项，请先参考本章节内容排查与修复问题。问题修复后，可以尝试再次升级集群联邦。

升级联邦前，请您对联邦运行状态、集群运行状态、集群接入状态三方面进行检查，以避免升级失败。

现象一：集群联邦状态检查异常

问题原因：集群联邦运行状态异常。

解决方案：可尝试关闭集群联邦能力后再重新开通，详细操作请参考**开通集群联邦**。若由于业务方面原因不能关闭集群联邦，请提交工单，联系技术支持人员进行处理。

现象二：集群状态检查异常

问题原因：舰队内集群运行状态异常或接入状态异常。

解决方案：

- 若集群运行状态异常，可对集群进行修复。
- 若集群接入状态异常，可尝试重新将其加入联邦；若无法重新加入联邦，请提交工单，联系技术支持人员进行处理。

5.3 将已接入联邦且状态异常的集群移出舰队失败怎么办?

问题背景

舰队已开通集群联邦，对在舰队中运行状态异常的集群进行移出舰队操作，移出失败。

解决方案

步骤1 再次单击目标集群右上角的，重新尝试将其移出舰队。

步骤2 若重试后仍移出失败，请提交工单，联系技术支持人员进行处理。

----结束

5.4 集群加入联邦失败怎么办?

问题背景

集群加入联邦失败，报错“the same cluster has been registered with name clusterName”或“cluster(clusterName) is joined successfully”。

可能原因

集群节点故障、Pod重启导致加入失败，由于karmadactl join命令不幂等，失败后再次执行会报错。

解决方案

请将集群从联邦中移出，然后执行kubectl get cluster命令，校验集群联邦中是否存在该集群。

若存在，请执行kubectl edit cluster clusterName命令，编辑YAML删除finalizers字段，再执行kubectl get cluster命令校验集群联邦中是否存在该集群

若不存在，再将集群重新加入联邦即可。

5.5 集群加入联邦时，状态校验失败如何排查?

问题背景

集群加入联邦失败，错误提示“状态校验失败，不支持”，错误码“UCS.01100007”，错误信息“Update associated clusters validate failed”，错误原因：“vpcep: Required value: all subnets in vpc xxx have endpoint connected to xxx.vpcep-src-open.xxx but not managed by ucs”。

图 5-1 状态校验失败

解决方案

如果出现以上问题，请检查报错的VPC中所有的子网下，是否已经存在自行创建的绑定至报错的终端节点服务的VPCEP终端节点，如果有，请至该绑定终端节点服务的VPCEP终端节点的详情页面并给其添加标签"managed-by=service-ucs"。

5.6 联邦管理面创建 HPA 后分发到成员集群失败怎么办?

问题背景

在集群联邦管理面创建HPA后，创建PropagationPolicy将其分发到版本低于v1.23的成员集群失败。

可能原因

当前，UCS集群联邦API Server版本为v1.25，因此HPA对象有autoscaling/v2和autoscaling/v1两个版本。然而，不论您创建的HPA版本为autoscaling/v2还是autoscaling/v1，联邦均会以autoscaling/v2版本进行分发。版本低于v1.23的集群不支持autoscaling/v2版本的HPA对象，因此HPA无法分发到该集群。查看HPA对应的resourceBinding，可以在其conditions中得到如下报错：cluster(s) did not have the API resource。

解决方案

您可以在分发HPA前，将成员集群版本升级至v1.23及以上的版本，该版本默认支持autoscaling/v2的HPA。

若您仍想分发autoscaling/v1版本的HPA到成员集群，您的PropagationPolicy对象中的resourceSelectors[i].apiVersion字段应配置为autoscaling/v2，如示例YAML所示。分发成功后，您可以在成员集群中查询到autoscaling/v1版本的HPA。

```
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
metadata:
  name: test-hpa
spec:
  maxReplicas: 5
  minReplicas: 1
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: nginx
  targetCPUUtilizationPercentage: 10
---
apiVersion: policy.karmada.io/v1alpha1
kind: PropagationPolicy
metadata:
  name: test-hpa-pp
spec:
  placement:
    clusterAffinity:
      clusterNames:
        - member1
  resourceSelectors:
    - apiVersion: autoscaling/v2
      kind: HorizontalPodAutoscaler
      name: test-hpa
      namespace: default
```

5.7 部署 Nginx Ingress 后状态为未就绪怎么办?

问题背景

创建Nginx Ingress后，Ingress处于“未就绪”状态。

解决方案

在创建Nginx Ingress前应为对应集群安装Nginx Ingress Controller插件，若未安装会导致Ingress处于“未就绪”状态。安装插件的具体操作请参见：

- 为CCE集群安装插件请参见**通过控制台创建Nginx Ingress**。
- 为本地集群安装插件请参见**使用L7负载均衡Ingress-nginx**。
- 为其他类型集群安装插件请参见开源社区文档**Nginx Ingress Controller**。

5.8 创建 MCI 对象失败怎么办?

问题描述

创建MCI对象失败。

排查思路

请运行kubectl describe mci mci-example -n demo命令，查看事件。

- 情况一，事件显示如下：

```
Events:
  Type     Reason       Age    From                        Message
  ----     ------       ----   ----                        -------
  Warning  LoadBalance  3m19s  multicluster-cloud-provider  mci [demo/mci-example] create loadBalance failed:status code:409 resp body:{"error_msg":"L
oad Balancer 057                    already has a listener with protocol_port of 6001.","error_code":"ELB.8907","request_id":"d9
                  "} message:
```

- 情况二，事件显示如下：

```
Events:
  Type      Reason       Age   From                        Message
  ----      ------       ----  ----                        -------
  Warning   LoadBalance  51s   multicluster-cloud-provider  get loadBalancer by mci [defaul
t/zhctest] failed: status code:401 resp body:{"error_msg":"Incorrect IAM authentication in
formation: get token error,status:400","error_code":"APIGW.0301","request_id":"fb
                  df"}
```

解决方案

若出现情况一中报错，原因为创建MCI对象时配置的监听器端口已被使用，您可以任选以下解决方案中的一种：

- 编辑创建失败的MCI对象，修改为未使用的监听器端口。
- 登录ELB控制台，删除对应端口的监听器。

若出现情况二中报错，原因为创建MCI对象时配置的karmada.io/elb.projectid有误，您需要删除所创建的MCI，并重新创建配置正确的MCI。

5.9 通过 MCI 访问服务失败，如何排查?

若您在创建MCI后访问服务失败，请检查MCI对象是否配置成功。

请登录ELB控制台，根据MCI绑定的ELB实例ID，找到并单击对应的ELB实例名称进入elb监听器页面，找到对应的监听器单击“添加/编辑转发策略”，进入ELB监听器的转发策略页面，单击后端服务器组名称，进入后端服务器组页面，切换至后端服务器页签，查看该ELB是否成功绑定对应工作负载。

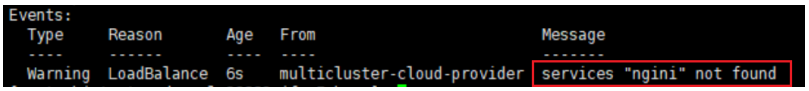
1. 若后端服务器状态为已删除，请检查Pod的IP网段是否与ELB的VPC网段冲突。

2. 若后端服务器组为空，请执行如下命令查询对应事件，根据事件信息排查具体异常情况。其中{MCIname}请替换为MCI的名称。

   kubectl describe mci {MCIname}

   若出现如下报错信息，请检查ELB实例的监听器端口是否已被占用。

   若出现如下报错信息，请检查MCI中的服务名称是否存在。



   若出现如下报错信息，请检查MCI中配置的服务端口是否正确。

5.10 创建 MCS 对象失败怎么办?

问题描述

创建MCS对象失败，运行kubectl describe mcs mcs-example -n demo命令查看事件，显示如下：

```
Events:
  Type     Reason       Age   From                          Message
  ----     ------       ----  ----                          -------
  Warning  LoadBalance  12s   multicluster-cloud-provider  get loadBalancer by mcs [defaul
t/nginx-v1] failed: status code:401 resp body:{"error_msg":"Incorrect IAM authentication i
nformation: get token error,status:400","error_code":"APIGW.0301","request_id":"36
                            "}
```

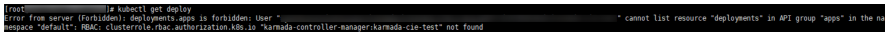
解决方案

问题出现的原因为创建MCS对象时配置的karmada.io/elb.projectid有误，您需要删除所创建的MCS，并重新创建配置正确的MCS。

5.11 执行 kubectl 命令报错 Error from server (Forbidden)怎么办?

问题描述

在使用集群联邦的过程中，执行kubectl命令，出现如下所示的报错信息。



可能原因

可能是由于集群联邦内成员集群的资源对象ClusterRole或者ClusterRoleBinding被删除。集群联邦内若有一个及以上的成员集群出现上述情况，就会导致kubectl命令请求中断并返回该错误。

解决方案

重新创建该成员集群的ClusterRole与ClusterRoleBinding资源对象。

ClusterRole的YAML文件示例如下。其中，{clusterName}请替换为成员集群的名称。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: karmada-controller-manager:karmada-{clusterName}
rules:
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - '*'
- nonResourceURLs:
  - '*'
  verbs:
  - get
```

ClusterRoleBinding的YAML文件示例如下。其中，{clusterName}请替换为成员集群的名称，{karmada-manage-namespace}请替换为karmada管理的命名空间名称，您可以通过执行**kubectl get ns|grep karmada**获取。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: karmada-controller-manager:karmada-{clusterName}
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: karmada-controller-manager:karmada-{clusterName}
subjects:
- kind: ServiceAccount
  name: karmada-{clusterName}
  namespace: {karmada-manage-namespace}
```


6 华为云集群

6.1 华为云集群状态不可用，报 cce cluster not found 怎么办?

问题描述

华为云集群状态显示不可用，错误信息为cce cluster not found，please unregister cluster。

可能原因

您在CCE集群控制台手动删除了已注册在UCS中的集群，导致UCS中集群状态显示为不可用。

解决方案

请您及时登录UCS控制台，单击该集群右上角的注销按钮，注销该集群，以停止对不可用状态集群的计费。

7 附着集群

7.1 附着集群接入失败怎么办?

问题描述

本文为集群接入的异常排查思路以及解决方案。集群接入UCS可能出现的异常情况如下:

- 在UCS控制台中注册集群后，已在集群中部署proxy-agent，但界面一直提示“等待接入”，或在接入超时后提示“注册失败”。

  说明

  如集群已处于“注册失败”状态，请单击右上角按钮重新注册集群，然后根据**排查思路**进行问题定位。

- 已接入的集群状态显示为“不可用”，请参考本文档中的**排查思路**解决。

排查思路

集群处于异常状态的排查思路大致可根据报错信息进行定位，如**表7-1**所示。

表 7-1 报错信息说明

报错信息	说明	推荐排查项
“currently no agents available, please make sure the agents are correctly registered”	出现该错误的原因大概率为接入集群中的proxy-agent运行状态异常或网络异常。	• **排查项一：proxy-agent的运行状态** • **排查项二：集群与UCS网络连接状态**
“please check the health status of kube apiserver: ...”	出现该错误的原因大概率为集群内部kube-apiserver无法访问。	• **排查项三：集群kube-apiserver状态**

报错信息	说明	推荐排查项
“cluster responded with non-successful status code: ...”	出现该错误的原因可能是多样的，请根据实际状态码进行排查。 例如状态码401表示用户没有访问权限，可能的原因是集群认证信息过期。	• **排查项四：集群认证信息变化**
“cluster responded with non-successful message: ...”	出现该错误的原因可能是多样的，请根据实际信息进行排查。 例如“Get "https://172.16.0.143:6443/readyz?timeout=32s\": context deadline exceeded”显示访问apiserver超时，可能是因为集群apiserver发生故障。	-
“Current cluster version is not supported in UCS service.”	出现该错误的原因是集群版本不符合要求：接入UCS服务的Kubernetes集群版本必须为1.19及以上。	-

排查项一：proxy-agent 的运行状态

须知

集群从UCS注销后，原有proxy-agent配置文件中包含的认证信息将会失效，请同时删除集群中已部署的proxy-agent实例。如需再次接入UCS，必须重新从UCS控制台下载proxy-agent配置文件进行部署。

步骤1 登录目标集群Master节点。

步骤2 查看集群代理部署状态。

kubectl -n kube-system get pod | grep proxy-agent

如果部署成功，预期输出如下：

```
proxy-agent-*** 1/1 Running 0 9s
```

说明proxy-agent部署正常，如proxy-agent没有处于正常Running状态，可以使用**kubectl -n kube-system describe pod proxy-agent-***查看Pod的告警信息，详细排查思路可参考**proxy-agent部署失败怎么办？** 。

说明

proxy-agent默认部署两个Pod实例，存在一个Pod正常Running即可使用基本功能，但是高可用性无法保证。

步骤3 打印proxy-agent的Pod日志，查看代理程序是否可以连接到UCS。

kubectl -n kube-system logs proxy-agent-* | grep "Start serving"**

如没有“Start serving”的日志打印但是proxy-agent实例状态正常，则需要继续检查其他排查项。

----结束

排查项二：集群与 UCS 网络连接状态

公网接入：

步骤1 检查集群是否绑定公网IP或配置公网NAT网关。

步骤2 检查集群安全组的出方向是否放通。如需对出方向做访问控制，请联系技术支持获取目的地址和端口号。

步骤3 解决网络问题后，删掉已有的proxy-agent Pod使其重新生成Pod资源，查看新建Pod的日志中是否存在“Start serving”的日志打印。

kubectl -n kube-system logs proxy-agent-* | grep "Start serving"**

步骤4 日志正常打印后，刷新UCS控制台页面，查看集群是否正常连接。

----结束

私网接入：

步骤1 检查集群安全组的出方向是否放通。如需对出方向做访问控制，请联系技术支持获取目的地址和端口号。

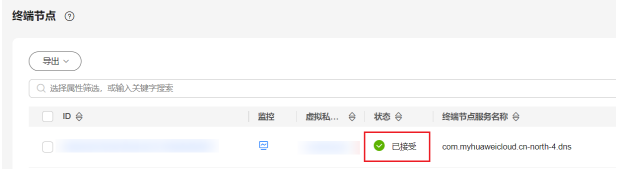
步骤2 排除集群与UCS和IDC/第三方云之间的网络连接故障。

根据网络连接方式不同，请参考以下文档进行故障排除。

- 云专线（DC）：请参考**故障排除**。
- 虚拟专用网络（VPN）：请参考**故障排除**。

步骤3 排除集群私网接入的VPCEP故障，VPCEP状态需为“已接受”。如VPCEP被误删除，则需重新创建，请参见**私网接入的集群误删除VPCEP后如何恢复**。

图 7-1 VPCEP 状态



步骤4 解决网络问题后，删掉已有的proxy-agent Pod使其重新生成Pod资源，查看新建Pod的日志中是否存在“Start serving”的日志打印。

kubectl -n kube-system logs proxy-agent-* | grep "Start serving"**

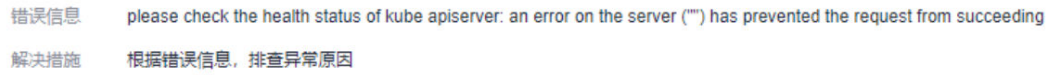
步骤5 日志正常打印后，刷新UCS控制台页面，查看集群是否正常连接。

----结束

排查项三：集群 kube-apiserver 状态

集群接入UCS时，可能出现如图7-2所示的异常信息，错误显示“please check the health status of kube apiserver: ...”。

图 7-2 kube-apiserver 状态异常



如出现以上信息，说明proxy-agent无法和集群apiserver进行正常通信，由于不同用户待接入集群的网络环境配置不同，这里无法提供统一的解决方案，需要您自行解决集群网络问题后进行重试。

步骤1 登录UCS控制台，在左侧导航栏选择“容器舰队”页面。

步骤2 登录目标集群Master节点，查看apiserver地址。

kubectl get po `kubectl get po -nkube-system | grep kube-apiserver | awk {'print $1'}` -nkube-system -oyaml | grep advertise-address.endpoint

步骤3 查看集群的KubeConfig文件中“clusters.cluster.server”字段是否与步骤2中查询的集群apiserver地址一致。

如不一致，可能是集群提供商做了apiserver的地址转换，请替换KubeConfig文件中的集群apiserver地址后，在UCS控制台重新注册集群，并重新部署proxy-agent。

说明

若KubeConfig文件中“clusters.cluster.server”字段为“https://kubernetes.default.svc.cluster.local:443”可无需替换，该域名为kubernetes服务（即apiserver的ClusterIP）的本地域名。

步骤4 检查proxy-agent的Pod是否可以访问待接入集群的apiserver。

参考命令：

```
kubectl exec -ti proxy-agent-*** -n kube-system /bin/bash
# 访问集群的kube-apiserver
curl -kv https://*.*.*.*:*/readyz
```

如无法正常访问，请解决集群网络问题后，在UCS控制台重新注册集群，并重新部署proxy-agent。

----结束

排查项四：集群认证信息变化

如错误显示“cluster responded with non-successful status: [401] [Unauthorized]”，可能是集群认证信息过期或者发生了变化，从而导致UCS无法访问集群kube-apiserver，请您注销该集群，使用新的KubeConfig文件重新注册集群，并重新部署proxy-agent。

说明

- 建议您使用永久的KubeConfig文件，防止由于集群认证信息过期导致UCS无法管理集群。
- 部分厂商提供的第三方集群在欠费后重新续费会导致认证信息变化，请尽量避免集群欠费的情况发生。

7.2 私网接入的集群误删除 VPCEP 后如何恢复?

问题描述

私网接入的集群误删除对应的VPCEP终端节点后，集群状态显示异常。

操作步骤

说明

由于proxy-agent中已配置VPCEP的IP地址，在新建VPCEP时需要指定IP，请确保IP未被占用。

步骤1 登录VPC终端节点控制台检查UCS服务所在区域的VPCEP是否被删除。如确认对接UCS的VPCEP被删除，则可继续执行以下步骤。

步骤2 登录接入异常集群的Master节点。

步骤3 查询proxy-agent中配置的IP信息。

kubectl get deploy -n kube-system proxy-agent -oyaml | grep -A3 hostAliases

回显如下：

```
hostAliases:
- hostnames:
  - proxyurl.ucs.myhuaweicloud.com
  ip: 10.0.0.182
```

步骤4 在UCS所在区域新建一个VPCEP，并指定该IP地址，单击“查看已使用IP地址”以确保该IP地址未使用。如IP地址已占用，则需编辑集群中的proxy-agent配置，请参考编辑proxy-agent配置。

图 7-3 购买终端节点（指定节点 IP）

步骤5 单击“立即购买”，重新创建一个VPCEP。

步骤6 等待1-3分钟，前往UCS控制台重新刷新集群状态。

----结束

编辑 proxy-agent 配置

步骤1 在UCS所在区域新建一个VPCEP。

图 7-4 购买终端节点（自动分配节点 IP）

步骤2 单击新创建VPCEP的ID，查看自动分配的节点IP。

图 7-5 VPCEP 详情

步骤3 登录接入异常集群的Master节点。

步骤4 编辑proxy-agent中配置的IP信息。

kubectl edit deploy -n kube-system proxy-agent

修改hostAliases字段下的IP：


```
hostAliases:
- hostnames:
  - proxyurl.ucs.myhuaweicloud.com
  ip: 10.0.0.122
```

按“ESC”，输入**:wq**，按“ENTER”完成编辑。

步骤5 等待1-3分钟，前往UCS控制台重新刷新集群状态。

----结束

7.3 proxy-agent 部署失败怎么办?

问题描述

在集群中部署proxy-agent后，proxy-agent处于为非“Running”状态。

操作步骤

步骤1 登录集群Master节点。

步骤2 查看proxy-agent运行状态。

kubectl -n kube-system get pod | grep proxy-agent

回显如下，pod状态处于ImagePullBackOff或Pending：

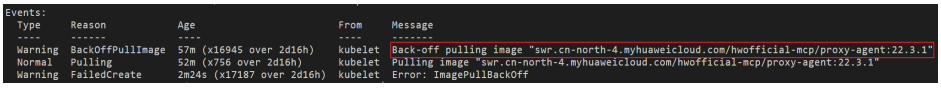
```
proxy-agent-59ddf7597b-rq4j6          0/1     ImagePullBackOff   0          2d16h
proxy-agent-59ddf7597b-sjf55          0/1     Pending            0          2d16h
```

步骤3 查看Pod的详细信息。

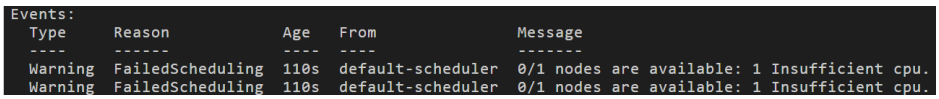
kubectl describe pod proxy-agent-* -nkube-system**

可能出现如下错误：

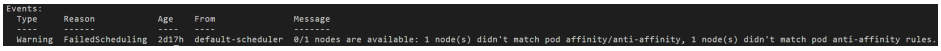
- K8s事件显示集群无法拉取proxy-agent镜像，请您确保集群具备访问公网的能力，可正常拉取SWR镜像。



- K8s事件显示节点的CPU或内存资源不足，请您扩容节点资源。



- K8s事件显示没有符合调度规则的节点。proxy-agent为实现高可用性，默认将两个实例调度至不同的节点，请您确保集群中至少存在两个节点具有足够的资源。



- K8s事件显示gatekeeper相关字样，可能是由于创建的策略实例进行了拦截。为解决此问题，请在集群上执行以下命令删除相应策略实例。

  kubectl delete constraint --all

步骤4 以上问题解决后，重新查看proxy-agent运行状态，所有Pod处于“Running”状态。

----结束

8 本地集群

8.1 本地集群接入失败怎么办?

问题描述

本文为集群接入的异常排查思路以及解决方案。集群接入UCS可能出现的异常情况如下:

- 在UCS控制台中注册集群后，已在集群中部署proxy-agent，但界面一直提示“等待接入”，或在接入超时后提示“注册失败”。

  说明

  如集群已处于“注册失败”状态，请单击右上角按钮重新注册集群，然后根据**排查思路**进行问题定位。

- 已接入的集群状态显示为“不可用”，请参考本文档中的**排查思路**解决。

排查思路

集群处于异常状态的排查思路大致可根据报错信息进行定位，如**表8-1**所示。

表 8-1 报错信息说明

报错信息	说明	推荐排查项
“currently no agents available, please make sure the agents are correctly registered”	出现该错误的原因大概率为接入集群中的proxy-agent运行状态异常或网络异常。	• **排查项一：proxy-agent的运行状态** • **排查项二：集群与UCS网络连接状态**
“please check the health status of kube apiserver: ...”	出现该错误的原因大概率为集群内部kube-apiserver无法访问。	• **排查项三：集群kube-apiserver状态**

报错信息	说明	推荐排查项
“cluster responded with non-successful status code: ...”	出现该错误的原因可能是多样的，请根据实际状态码进行排查。 例如状态码401表示用户没有访问权限，可能的原因是集群认证信息过期。	• **排查项四：集群认证信息变化**
“cluster responded with non-successful message: ...”	出现该错误的原因可能是多样的，请根据实际信息进行排查。 例如“Get "https://172.16.0.143:6443/readyz?timeout=32s\": context deadline exceeded”显示访问apiserver超时，可能是因为集群apiserver发生故障。	-
“Current cluster version is not supported in UCS service.”	出现该错误的原因是集群版本不符合要求：接入UCS服务的Kubernetes集群版本必须为1.19及以上。	-

排查项一：proxy-agent 的运行状态

须知

集群从UCS注销后，原有proxy-agent配置文件中包含的认证信息将会失效，请同时删除集群中已部署的proxy-agent实例。如需再次接入UCS，必须重新从UCS控制台下载proxy-agent配置文件进行部署。

步骤1 登录目标集群Master节点。

步骤2 查看集群代理部署状态。

kubectl -n kube-system get pod | grep proxy-agent

如果部署成功，预期输出如下：

```
proxy-agent-*** 1/1 Running 0 9s
```

说明proxy-agent部署正常，如proxy-agent没有处于正常Running状态，可以使用**kubectl -n kube-system describe pod proxy-agent-***查看Pod的告警信息，详细排查思路可参考**proxy-agent部署失败怎么办？** 。

说明

proxy-agent默认部署两个Pod实例，存在一个Pod正常Running即可使用基本功能，但是高可用性无法保证。

步骤3 打印proxy-agent的Pod日志，查看代理程序是否可以连接到UCS。

kubectl -n kube-system logs proxy-agent-* | grep "Start serving"**

如没有“Start serving”的日志打印但是proxy-agent实例状态正常，则需要继续检查其他排查项。

----结束

排查项二：集群与 UCS 网络连接状态

公网接入：

步骤1 检查集群是否绑定公网IP或配置公网NAT网关。

步骤2 检查集群安全组的出方向是否放通。如需对出方向做访问控制，请联系技术支持获取目的地址和端口号。

步骤3 解决网络问题后，删掉已有的proxy-agent Pod使其重新生成Pod资源，查看新建Pod的日志中是否存在“Start serving”的日志打印。

kubectl -n kube-system logs proxy-agent-* | grep "Start serving"**

步骤4 日志正常打印后，刷新UCS控制台页面，查看集群是否正常连接。

----结束

私网接入：

步骤1 检查集群安全组的出方向是否放通。如需对出方向做访问控制，请联系技术支持获取目的地址和端口号。

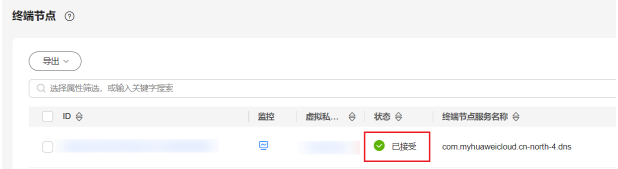
步骤2 排除集群与UCS和IDC之间的网络连接故障。

根据网络连接方式不同，请参考以下文档进行故障排除。

- 云专线（DC）：请参考**故障排除**。
- 虚拟专用网络（VPN）：请参考**故障排除**。

步骤3 排除集群私网接入的VPCEP故障，VPCEP状态需为“已接受”。如VPCEP被误删除，则需重新创建，请参见**私网接入的集群误删除VPCEP后如何恢复？**。

图 8-1 VPCEP 状态



步骤4 解决网络问题后，删掉已有的proxy-agent Pod使其重新生成Pod资源，查看新建Pod的日志中是否存在“Start serving”的日志打印。

kubectl -n kube-system logs proxy-agent-* | grep "Start serving"**

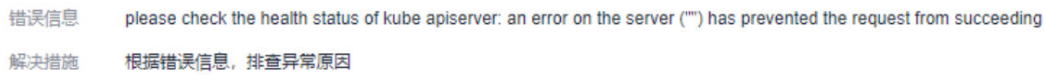
步骤5 日志正常打印后，刷新UCS控制台页面，查看集群是否正常连接。

----结束

排查项三：集群 kube-apiserver 状态

集群接入UCS时，可能出现如图8-2所示的异常信息，错误显示“please check the health status of kube apiserver: ...”。

图 8-2 kube-apiserver 状态异常



如出现以上信息，说明proxy-agent无法和集群apiserver进行正常通信，由于不同用户待接入集群的网络环境配置不同，这里无法提供统一的解决方案，需要您自行解决集群网络问题后进行重试。

步骤1 登录UCS控制台，在左侧导航栏选择“容器舰队”页面。

步骤2 登录目标集群Master节点，检查proxy-agent的Pod是否可以访问待接入集群的apiserver。

参考命令：

```
kubectl exec -ti proxy-agent-*** -n kube-system /bin/bash
# 访问集群的kube-apiserver
curl -kv https://kubernetes.default.svc.cluster.local/readyz
```

如无法正常访问，请解决集群网络问题后，在UCS控制台重新注册集群，并重新部署proxy-agent。

----结束

排查项四：集群认证信息变化

如错误显示“cluster responded with non-successful status: [401] [Unauthorized]”，通过观察集群三个Master节点“/var/paas/sys/log/kubernetes/auth-server.log”日志，可能是IAM网络连通故障。请确认IAM域名解析能力，及IAM服务连通性正常。

常见问题日志如下：

- Failed to authenticate token: *******: dial tcp: lookup iam.myhuaweicloud.com on *.*.*.*:53: no such host

  此类日志说明，节点缺少对iam.myhuaweicloud.com解析能力，请参考**安装前准备**，配置对应的域名解析。
- Failed to authenticate token: Get *******: dial tcp *.*.*.*:443: i/o timeout

  此类日志说明，节点访问IAM服务超时，请确保节点与华为云IAM服务能正常通信。
- currently only supports Agency token

  此类日志说明请求不是从UCS服务发起，目前本地集群只支持UCS服务IAM Token访问。
- IAM assumed user has no authorization/iam assumed user should allowed by TEAdmin

此类日志说明UCS服务访问集群故障，请联系华为技术人员进行排障。

- Failed to authenticate token: token expired, please acquire a new token

  此类日志说明Token存在过期现象，请使用**date**命令确定时间是否差距过大，如果节点时间与标准时间差距过大，请同步时间后，查看集群是否恢复。如果长时间未恢复，可能需要重装集群，请联系华为技术人员进行排障。

解决上述问题后，请使用**crictl ps | grep auth | awk '{print $1}' | xargs crictl stop**命令重启auth-server容器。

8.2 如何手动清理本地集群节点?

使用须知

节点清理属于高危操作，会将节点上已安装的进程（包括kubernetes进程、containerd等）和数据（包括容器、镜像等）全部清理，一旦执行清理操作节点状态将不可恢复。因此，执行之前请确认节点是否已经不再被本地集群使用。

使用场景

本地集群**ucs-ctl delete cluster**和**ucs-ctl delete node**命令执行失败时，需要参考本文档手动清理节点。

操作步骤

步骤1 于安装节点获取节点清理脚本。

在解压后的“/var/paas/.ucs-package/ucs-onpremise/scripts/”目录下，即可获取清理脚本uninstall_node.sh。

步骤2 将清理脚本拷贝到待清理的节点。

步骤3 登录到待清理的节点上，执行以下命令进行清理操作：

bash uninstall_node.sh

说明

为了尽可能减少残留进程或者数据，清理脚本支持多次执行。

步骤4 清理脚本执行完成后，重启节点。

步骤5 重复执行上述操作，清理其他节点。

----结束

8.3 如何进行 Cgroup 降级?

问题描述

etcd kubernetes容器无法拉起，执行**journalctl -u containerd**查看containerd日志，看到以下日志：

```
applying cgroup configuration for process caused \\\"mountpoint for cgroup not found\\\"\"\n
```


使用**stat -fc %T /sys/fs/cgroup/**查看cgroup版本为cgroup2fs，该问题根因为当前kubernetes版本cgroup v2暂未GA，需要进行cgroup降级。

操作步骤

步骤1 修改“/etc/default/grub”文件的GRUB_CMDLINE_LINUX配置项，添加systemd.unified_cgroup_hierarchy=no，关闭cgroup v2。

```
GRUB_CMDLINE_LINUX="net.ifnames=0 biosdevname=0 systemd.unified_cgroup_hierarchy=no"
```

步骤2 使用**sudo grub-mkconfig -o /boot/grub/grub.cfg**命令重新生成引导。

步骤3 执行**reboot**重启机器。

----结束

8.4 虚拟机 SSH 连接超时怎么办?

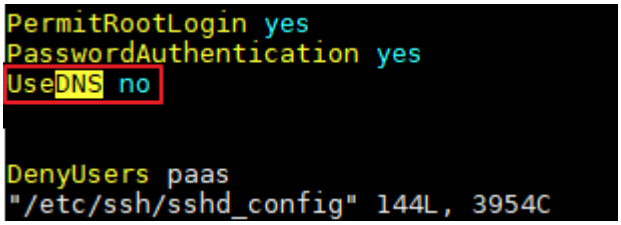
由于部分虚拟机性能不满足使用需求，偶尔会出现SSH连接超时现象，此时可以通过修改虚拟机SSH配置来解决问题。

步骤1 执行以下命令：

vim /etc/ssh/sshd_config

步骤2 按“i”进入编辑模式。

步骤3 将useDNS的值设置为no。



步骤4 按“ESC”，并输入**:wq!**保存退出。

----结束

8.5 本地集群如何扩容容器智能分析插件的存储磁盘?

问题描述

当容器智能分析插件（kube-prometheus-stack）所依赖的PVC存储中的磁盘写满时，prometheus-server-0 Pod的日志标准输出会出现“no space left on device”报错，此时普罗无法正常工作，需要对PVC所处的节点磁盘进行扩容并重启prometheus-server-0 Pod。

操作步骤

步骤1 检查Prometheus的PVC信息，获取PVC绑定的PV所在的节点和路径。

kubectl describe pvc pvc-prometheus-server-0 -nmonitoring|grep volume.kubernetes.io/selected-node

kubectl describe pvc pvc-prometheus-server-0 -nmonitoring|grep volume.kubernetes.io/targetPath

步骤2 登录到存储的节点，执行**df -TH**，查询节点磁盘配置，并根据节点磁盘的配置进行扩容。扩容完成后，还需要完成磁盘的分区，分区操作可参考《云硬盘用户指南》**扩展磁盘分区和文件系统（linux）**。

步骤3 扩容及分区完成后，重启普罗插件。

kubectl delete pod prometheus-server-0 -nmonitoring

须知

重启prometheus-server-0将导致重启期间容器智能分析功能不可用，请合理选择重启时间。

----结束

8.6 Master 节点关机后集群控制台不可用怎么办?

问题描述

Master节点关机后，出现集群控制台不可用的情况。

操作步骤

此类问题是由于Cilium社区对“Terminating”状态的Pod并不会进行Cilium Endpoint摘除，导致部分请求分流到关机节点，从而导致请求失败。请按照如下指导处理：

步骤1 执行以下命令，删除“Terminating”状态的Pod。

kubectl get pods -nkube-system | grep Terminating | awk '{print $1}'|xargs kubectl delete pods -nkube-system

步骤2 执行以下命令确定没有异常Pod。

kubectl get pods -nkube-system

步骤3 等待数分钟后，集群控制台恢复正常。

----结束

8.7 节点扩容规格后未就绪怎么办?

问题描述

本地集群节点扩容规格后，有时会出现节点的Kubernetes启动不了的情况，即节点未就绪。

操作步骤

“/mnt/paas/kubernetes/kubelet/cpu_manager_state”文件储存的是原先的cpu_manager_policy，是针对原先CPU核数的绑核设置，需要进行删除。然后重启

kubelet，让cpu_manager根据现有的CPU Topology进行绑核，重新生成cpu_manager_state。

因此，需要执行以下命令：

rm /mnt/paas/kubernetes/kubelet/cpu_manager_state

systemctl restart kubelet

等待一段时间，节点恢复正常。

8.8 如何更新本地集群 ca/tls 证书?

前提条件

- 本地集群各个组件运行正常。
- 集群各个节点处于ready状态。

操作步骤

步骤1 下载ucs-ctl二进制工具，放到任一台本地集群的管控节点/root/ucs目录下。

步骤2 将所有节点密码信息记录到表格中，并保存到二进制所在节点/root/ucs/update_cert.csv。格式请参考表8-2。

表 8-2 表格模板

字段	说明
Node IP	必填，节点IP地址
Node Role	必填，节点角色（选填master/node）
User	必填，节点登录用户
Password	选填，节点登录密码
Auth Type	选填，节点认证类型（选填password/key）
Key Path	选填，节点登录密钥路径

样例如下：

Node IP,Node Role,User,Password,Auth Type,Key Path

192.168.0.145,master,root,xxx,password,

192.168.0.225,master,root,xxx,password,

192.168.0.68,master,root,xxx,password,

192.168.0.89,node,root,xxx,password,

步骤3 导出环境变量

export CUSTOM_DOMAIN={ucs_endpoint},10.247.0.1

说明

其中ucs_endpoint为server访问地址，可通过以下方式获取。
cat /var/paas/srv/kubernetes/kubeconfig | grep server

步骤4 执行证书更新。

cd /root/ucs

./ucs-ctl kcm update-cert {cluster_name} -c update_cert.csv

步骤5 失败后重试。

./ucs-ctl kcm update-cert {cluster_name} -c update_cert.csv -r

步骤6 失败后回滚。

./ucs-ctl kcm rollback-cert {cluster_name} -c update_cert.csv

----结束

9 多云集群

9.1 如何清理多云集群资源?

在多云集群注销过程中，若因某些原因导致注销失败，您可以尝试重新进行注销操作。但在此之前，请确保已经在AWS控制台手动删除了集群关联的资源。本章节将为您提供这些资源的名称和数量，您可以分别访问AWS的EC2面板和VPC面板，查看并删除相应资源。

说明

表9-1中，${clusterName}为您的集群名称，${random5}为长度是5的随机字符串。

表 9-1 资源的名称和数量

控制台	资源类型	数量	名称
EC2面板	EC2	控制节点：3 工作节点：n	控制节点：${clusterName}-cp-${random5} 工作节点：${clusterName}-md-${i}-${random5}，其中${i}默认为0
	安全组	5	• ${clusterName}-node • ${clusterName}-lb • ${clusterName}-apiserver-lb • ${clusterName}-controlplane • default 以上安全组对应的VPC均为：${clusterName}-vpc
	弹性IP	3	${clusterName}-eip-apiserver
	存储卷	节点总数 * 2	根据卷挂载的EC2实例名，判断该卷属于哪个节点

控制台	资源类型	数量	名称
	ELB	1	${clusterName}-apiserver，对应VPC为：${clusterName}-vpc
	网络接口	4	Name为空，对应VPC均为：${clusterName}-vpc
VPC面板	VPC	1	${clusterName}-vpc
	NAT	3	● ${clusterName}-nat 对应VPC为：${clusterName}-vpc；对应子网为：${clusterName}-subnet-public-${az1} ● ${clusterName}-nat 对应VPC为：${clusterName}-vpc；对应子网为：${clusterName}-subnet-public-${az2} ● ${clusterName}-nat 对应VPC为：${clusterName}-vpc；对应子网为：${clusterName}-subnet-public-${az3}
	子网	6	● ${clusterName}-subnet-public-${az1} ● ${clusterName}-subnet-private-${az1} ● ${clusterName}-subnet-public-${az2} ● ${clusterName}-subnet-private-${az2} ● ${clusterName}-subnet-public-${az3} ● ${clusterName}-subnet-private-${az3} 以上子网对应的VPC均为：${clusterName}-vpc

控制台	资源类型	数量	名称
	路由表	7	• ${clusterName}-rt-public-${az1}，显式子网关联为：${clusterName}-subnet-public-${az1} • ${clusterName}-rt-private-${az1}，显式子网关联为：${clusterName}-subnet-private-${az1} • ${clusterName}-rt-public-${az2}，显式子网关联为：${clusterName}-subnet-public-${az2} • ${clusterName}-rt-private-${az2}，显式子网关联为：${clusterName}-subnet-private-${az2} • ${clusterName}-rt-public-${az3}，显式子网关联为：${clusterName}-subnet-public-${az3} • ${clusterName}-rt-private-${az3}，显式子网关联为：${clusterName}-subnet-private-${az3} • Name为空，显式子网关联为空 以上路由表对应的VPC均为：${clusterName}-vpc
	互联网网关	1	${clusterName}-igw，对应VPC为：${clusterName}-vpc
	网络ACL	1	Name为空，关联对象为“6子网”，对应VPC为：${clusterName}-vpc

9.2 如何获取访问密钥 AK/SK?

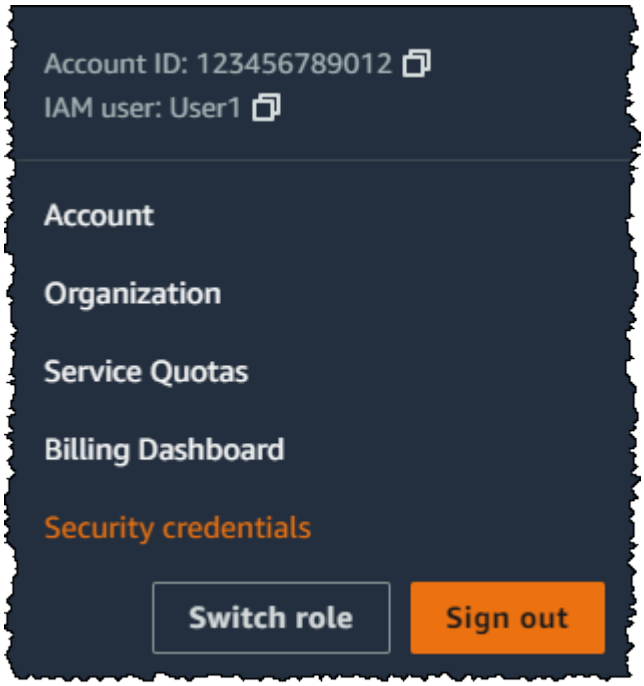
在注册多云集群时，您需要获取访问密钥AK/SK（Access Key ID/Secret Access Key），以便在AWS账户中创建与多云集群相关的资源（如EC2实例、安全组、弹性IP和负载均衡器等）。本文将为您提供获取访问密钥AK/SK的方法。

说明

该密钥将被加密妥善保存，您无需担心信息泄露的风险。

1. 使用AWS 账户 ID 或账户别名、您的 IAM 用户名和密码登录到 IAM 控制台。
   要获取 AWS 账户 ID，请联系您 AWS 账户的管理员。
2. 在右上角的导航栏中，选择您的用户名，然后选择“安全凭据”。

图 9-1 选择“安全凭据”



3. 在“访问密钥”区域中，单击“创建访问密钥”。如果您已经有两个访问密钥，则此按钮将被停用，您必须先删除一个访问密钥，然后才能创建新的访问密钥。您也可以使用已有的密钥来创建UCS on AWS集群。

图 9-2 创建访问密钥

4. 在“检索访问密钥”页面上，单击“显示”获取用户的秘密访问密钥的值，或单击“下载 .csv 文件”按钮。这是您保存秘密访问密钥的唯一机会。将秘密访问密钥保存在安全位置后，请单击“完成”。

图 9-3 获取秘密访问密钥

> **注意**
>
> 在您使用UCS on AWS期间，在对应的集群被删除之前，请不要轮转、停用或者删除该密钥，否则会影响集群的后续更新和删除操作。

9.3 如何更新多云集群证书?

前提条件

- 集群各个组件运行正常。
- 集群各个节点处于ready状态。

操作步骤

步骤1 下载ucs-ctl二进制工具，放到任一台本地集群的管控节点/root/ucs目录下。

步骤2 将所有节点密码信息记录到表格中，并保存到二进制所在节点/root/ucs/update_cert.csv，格式请参考表9-2。

表 9-2 表格模板

字段	说明
Node IP	必填，节点IP地址
Node Role	必填，节点角色（选填master/node）
User	必填，节点登录用户
Password	选填，节点登录密码
Auth Type	选填，节点认证类型（选填password/key）
Key Path	选填，节点登录密钥路径

样例如下：

Node IP,Node Role,User,Password,Auth Type,Key Path

192.168.0.145,master,root,xxx,password

192.168.0.225,master,root,xxx,password

192.168.0.68,master,root,xxx,password

192.168.0.89,node,root,xxx,password

步骤3 登录AWS控制台，编辑安全组{cluster_name}-node，将该安全组放通22端口，以保证可以访问。

步骤4 开启密码访问，登录集群内所有节点，执行以下命令。

```
sed -i 's/PasswordAuthentication no/PasswordAuthentication yes/g' /etc/ssh/sshd_config
echo "PermitRootLogin yes" >> /etc/ssh/sshd_config
```

```
systemctl restart sshd
passwd
```

设置节点密码，并记录到本地。

步骤5 配置环境变量。

```
export CUSTOM_DOMAIN={ucs_endpoint},10.247.0.1
```

说明

- 其中ucs_endpoint为server访问地址，可通过以下方式获取。

  cat /var/paas/srv/kubernetes/kubeconfig | grep server
- 如果在安装集群的执行机上操作，可不用配置环境变量。

步骤6 执行证书更新。

```
cd /root/ucs
cp /var/paas/srv/kubernetes/ca.key /var/paas/srv/kubernetes/ca_key.pem
./ucs-ctl kcm update-cert {cluster_name} -c update_cert.csv
```

步骤7 失败后重试。

```
./ucs-ctl kcm update-cert {cluster_name} -c update_cert.csv -r
```

步骤8 失败后回滚。

```
./ucs-ctl kcm rollback-cert {cluster_name} -c update_cert.csv
```

----结束

10 流量分发

10.1 如何添加第三方域名?

问题描述

域名在第三方域名注册商处注册，需要使用UCS进行流量管理，此时可通过添加域名至华为云云解析服务（DNS）来解决，UCS流量管理控制台将自动获取已添加解析的域名。

步骤一：添加域名

通过第三方域名注册商注册的域名，需要通过“创建公网域名”操作添加至云解析服务。

1. 登录管理控制台。
2. 将鼠标悬浮于页面左侧的 图标，在服务列表中，选择“网络 > 云解析服务 DNS”。
   进入“云解析”页面。
3. 在左侧树状导航栏，选择“公网域名”，单击右上角“创建公网域名”。
4. 在“创建公网域名”页面中，输入注册的域名（如“example.com”），将域名添加至云解析服务。
   更多参数说明，请参见**创建公网域名**。
5. 单击“确定”，完成公网域名“example.com”的创建。
   创建完成后，您可以在“公网域名”页面查看新创建的域名信息。
   若提示“域名已经被其他租户创建”，请参考**找回域名**。

   说明

   单击“域名”列的域名名称，可以看到系统已经为您创建了SOA类型和NS类型的记录集。其中，

   - SOA类型的记录集标识了对此域名具有最终解释权的主权威服务器。
   - NS类型的记录集标识了此域名的权威服务器。
     您可以根据域名所在区域修改NS记录集的值，详细内容请参考**华为云DNS对用户提供域名服务的DNS是什么？**。

步骤二：更改域名的 DNS 服务器

域名的DNS服务器定义了域名用于解析的权威DNS服务器。

当通过云解析服务创建公网域名后，系统默认生成的NS类型记录集的值即为云解析服务的DNS服务器地址。

若域名的DNS服务器设置与NS记录集的值不符，则域名无法正常解析，您需要到域名注册商处将域名的DNS服务器修改为华为云云解析服务的DNS服务器地址。

说明

更改后的DNS服务器地址将于48小时内生效，具体生效时间请以域名注册商处的说明为准。

步骤1 查询云解析服务DNS服务器地址。

1. 登录管理控制台。
2. 将鼠标悬浮于页面左侧的 图标，在服务列表中，选择“网络 > 云解析服务 DNS”。
   进入“云解析”页面。
3. 在左侧树状导航栏，选择“公网域名”。
   进入“公网域名”页面。
4. 在“公网域名”页面新创建的域名所在行，单击“域名”列的域名名称。
   “类型”为“NS”的记录集，其对应的“值”即为DNS服务器的域名。

图 10-1 系统返回的 NS 类型记录集

步骤2 更改域名的DNS服务器。

登录域名注册商网站，修改域名的DNS服务器为华为云DNS服务器地址：

ns1.huaweicloud-dns.com

ns1.huaweicloud-dns.cn

ns1.huaweicloud-dns.net

ns1.huaweicloud-dns.org

详细操作请参考域名注册商网站操作指导。

----结束

步骤三：在 UCS 添加调度策略

步骤1 DNS解析添加完成后，回到UCS控制台“创建流量策略”页面，选择新添加的域名。
如域名未同步，可单击右侧 按钮进行刷新。

图 10-2 创建流量策略

步骤2 参考**创建流量策略**，为新添加的域名添加调度策略。

图 10-3 调度策略

步骤3 检验新增调度策略是否生效。

以Linux系统为例，您可以在已经连接Internet的终端的命令窗口使用如下命令测试调度策略是否生效，命令格式如下：

dig 目标域名

说明

如果Linux终端的操作系统没有自带dig命令，需要手动安装后才能使用。例如CentOS系统，可执行**yum install bind-utils**安装。

如下图所示，回显中“ANSWER SECTION”的IP地址为目标集群负载均衡IP，则表示调度策略创建成功。

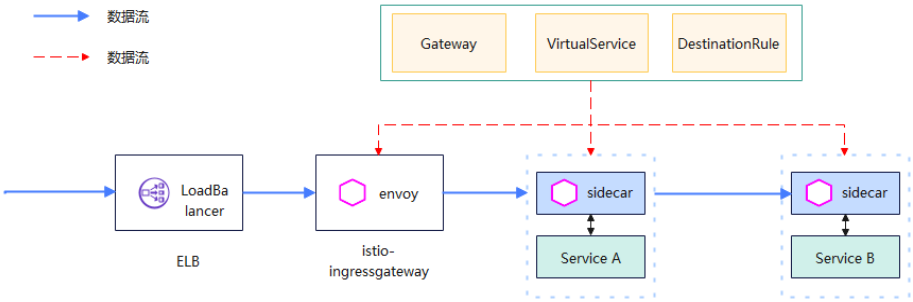
```
[root@no-del-cluster-                    -08211 ~]# dig demo.

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> demo.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7171
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;demo.                          IN      A

;; ANSWER SECTION:
demo.                   300     IN      A       123.

;; Query time: 38 msec
;; SERVER: 100.125.1.250#53(100.125.1.250)
;; WHEN: Thu Jul 21 19:30:37 CST 2022
;; MSG SIZE  rcvd: 61
```

----结束

11 服务网格

11.1 如何使用 Istio API 配置网关路由规则

ASM支持使用Istio API（Gateway, VirtualService, DestinationRule）配置网关、路由规则策略。本文介绍如何通过YAML创建资源对象启用该能力。



步骤1 使用以下内容，保存为deployment.yaml文件，创建istio-ingressgateway deployment工作负载。

```
kind: Deployment
apiVersion: apps/v1
metadata:
  name: istio-ingressgateway
  namespace: default # 命名空间名称，按需替换
spec:
  replicas: 1 # 工作负载实例数，按需替换
  selector:
    matchLabels:
      app: istio-ingressgateway
      istio: ingressgateway
  template:
    metadata:
      labels:
        app: istio-ingressgateway
        istio: ingressgateway
        istio.io/rev: default
        service.istio.io/canonical-name: istio-ingressgateway
        service.istio.io/canonical-revision: latest
        sidecar.istio.io/inject: 'false'
      annotations:
        sidecar.istio.io/inject: 'false'
    spec:
```

```
    volumes:
      - name: workload-socket
        emptyDir: {}
      - name: credential-socket
        emptyDir: {}
      - name: workload-certs
        emptyDir: {}
      - name: istiod-ca-cert
        configMap:
          name: istio-ca-root-cert
          defaultMode: 384
      - name: podinfo
        downwardAPI:
          items:
            - path: labels
              fieldRef:
                apiVersion: v1
                fieldPath: metadata.labels
            - path: annotations
              fieldRef:
                apiVersion: v1
                fieldPath: metadata.annotations
          defaultMode: 416
      - name: istio-envoy
        emptyDir: {}
      - name: istio-data
        emptyDir: {}
      - name: istio-token
        secret:
          defaultMode: 420
          optional: false
          secretName: cp-access-default
      - name: config-volume
        configMap:
          name: istio
          defaultMode: 416
          optional: true
      - name: ingressgateway-certs
        secret:
          secretName: istio-ingressgateway-certs
          defaultMode: 384
          optional: true
      - name: ingressgateway-ca-certs
        secret:
          secretName: istio-ingressgateway-ca-certs
          defaultMode: 384
          optional: true
    containers:
      - name: istio-proxy
        image: swr.cn-north-7.myhuaweicloud.com/asm/proxyv2:1.15.5-r1-20230719152011 # proxyv2镜像地址替换
        args:
          - proxy
          - router
          - '--domain'
          - $(POD_NAMESPACE).svc.cluster.local
          - '--proxyLogLevel=warning'
          - '--proxyComponentLogLevel=misc:error'
          - '--log_output_level=default:info'
        ports:
          - containerPort: 15021
            protocol: TCP
          - containerPort: 8080
            protocol: TCP
          - containerPort: 8443
            protocol: TCP
          - name: http-envoy-prom
            containerPort: 15090
            protocol: TCP
```



```
        env:
          - name: JWT_POLICY
            value: third-party-jwt
          - name: PILOT_CERT_PROVIDER
            value: istiod
          - name: CA_ADDR
            value: asm-mesh.kube-system.svc.cluster.local:15012
          - name: NODE_NAME
            valueFrom:
              fieldRef:
                apiVersion: v1
                fieldPath: spec.nodeName
          - name: POD_NAME
            valueFrom:
              fieldRef:
                apiVersion: v1
                fieldPath: metadata.name
          - name: POD_NAMESPACE
            valueFrom:
              fieldRef:
                apiVersion: v1
                fieldPath: metadata.namespace
          - name: INSTANCE_IP
            valueFrom:
              fieldRef:
                apiVersion: v1
                fieldPath: status.podIP
          - name: PROXY_CONFIG
            value: |
              {"discoveryAddress":"asm-mesh.kube-system.svc.cluster.local:15012"}
          - name: HOST_IP
            valueFrom:
              fieldRef:
                apiVersion: v1
                fieldPath: status.hostIP
          - name: SERVICE_ACCOUNT
            valueFrom:
              fieldRef:
                apiVersion: v1
                fieldPath: spec.serviceAccountName
          - name: ISTIO_META_WORKLOAD_NAME
            value: istio-ingressgateway
          - name: ISTIO_META_OWNER
            value: kubernetes://apis/apps/v1/namespaces/default/deployments/istio-ingressgateway  # default
替换为对应的命名空间名称
          - name: ISTIO_META_MESH_ID
            value: whtest # 替换为实际的网格名称
          - name: TRUST_DOMAIN
            value: cluster.local
          - name: ISTIO_META_UNPRIVILEGED_POD
            value: 'true'
          - name: ISTIO_ADDITIONAL_METADATA_EXCHANGE_KEYS
            value: ASM_MESH_ID,ASM_CLUSTER_ID
          - name: ISTIO_META_ASM_CLUSTER_ID
            value: 92311000-df43-11ed-b108-0255ac1001bb # 替换为实际的集群ID
          - name: ISTIO_META_ASM_MESH_ID
            value: a8653674-3fd2-11ee-9e48-0255ac100695 # 替换为实际的网格ID
          - name: ISTIO_META_CLUSTER_ID
            value: mesh-test # 替换为实际的集群名称
        resources:
          limits:
            cpu: '2'
            memory: 1Gi
          requests:
            cpu: 100m
            memory: 128Mi
        volumeMounts:
          - name: workload-socket
            mountPath: /var/run/secrets/workload-spiffe-uds
```



```
      - name: credential-socket
        mountPath: /var/run/secrets/credential-uds
      - name: workload-certs
        mountPath: /var/run/secrets/workload-spiffe-credentials
      - name: istio-envoy
        mountPath: /etc/istio/proxy
      - name: config-volume
        mountPath: /etc/istio/config
      - name: istiod-ca-cert
        mountPath: /var/run/secrets/istio
      - name: istio-token
        readOnly: true
        mountPath: /var/run/secrets/tokens
      - name: istio-data
        mountPath: /var/lib/istio/data
      - name: podinfo
        mountPath: /etc/istio/pod
      - name: ingressgateway-certs
        readOnly: true
        mountPath: /etc/istio/ingressgateway-certs
      - name: ingressgateway-ca-certs
        readOnly: true
        mountPath: /etc/istio/ingressgateway-ca-certs
    readinessProbe:
      httpGet:
        path: /healthz/ready
        port: 15021
        scheme: HTTP
      initialDelaySeconds: 1
      timeoutSeconds: 1
      periodSeconds: 2
      successThreshold: 1
      failureThreshold: 30
    terminationMessagePath: /dev/termination-log
    terminationMessagePolicy: File
    imagePullPolicy: IfNotPresent
    securityContext:
      capabilities:
        drop:
          - ALL
      privileged: false
      readOnlyRootFilesystem: true
      allowPrivilegeEscalation: false
restartPolicy: Always
terminationGracePeriodSeconds: 30
dnsPolicy: ClusterFirst
securityContext:
  runAsUser: 1337
  runAsGroup: 1337
  runAsNonRoot: true
  fsGroup: 1337
  seccompProfile:
    type: RuntimeDefault
affinity:
  nodeAffinity:
    preferredDuringSchedulingIgnoredDuringExecution:
      - weight: 1
        preference:
          matchExpressions:
            - key: istio
              operator: In
              values:
                - master
  podAntiAffinity:
    requiredDuringSchedulingIgnoredDuringExecution:
      - labelSelector:
          matchExpressions:
            - key: app
              operator: In
```



```
                values:
                  - istio-ingressgateway
            topologyKey: kubernetes.io/hostname
      schedulerName: default-scheduler
      tolerations:
        - key: istio
          operator: Exists
          effect: NoExecute
  strategy:
    type: RollingUpdate
    rollingUpdate:
      maxUnavailable: 1
      maxSurge: 10%
  revisionHistoryLimit: 10
  progressDeadlineSeconds: 600
```

执行以下命令，在当前集群中创建网关工作负载。

```
kubectl create -f deployment.yaml
```

步骤2 使用以下内容，保存为svc.yaml文件，创建istio-ingressgateway loadbalancer service。

```
apiVersion: v1
kind: Service
metadata:
  name: gw-svc1
  namespace: default # 命名空间名称，按需替换
  annotations:
    kubernetes.io/elb.class: union # elb实例类型，union共享型，performance独享型
    kubernetes.io/elb.id: 73febb1c-b191-4fd9-832e-138b2657d3b1 # elb实例ID，可通过在cce服务发现创建负载均衡类型服务页查看可选择的elb实例
spec:
  ports:
    - name: http-gw-svc1-port1 # 端口名称，注意以服务协议打头
      protocol: TCP
      port: 707 # 对外访问端口
      targetPort: 1026 # 容器端口，必须大于1024，且不能与网格内其他网关服务使用的targetPort端口重复
  selector:
    app: istio-ingressgateway
    istio: ingressgateway
  type: LoadBalancer
  sessionAffinity: None
  externalTrafficPolicy: Cluster
  ipFamilies:
    - IPv4
  ipFamilyPolicy: SingleStack
  allocateLoadBalancerNodePorts: true
  internalTrafficPolicy: Cluster
```

执行以下命令，在当前集群中创建网关工作负载对应的loadbalancer service。

```
kubectl create -f svc.yaml
```

⚠ 注意

以上步骤1、2使用的kubectl连接的是当前集群。

步骤3 使用以下内容，保存为gw.yaml文件，创建Istio Gateway配置。

```
apiVersion: networking.istio.io/v1beta1
kind: Gateway
metadata:
  name: my-gateway
  namespace: default # 命名空间名称，按需替换
spec:
  selector:
```



```
    istio: ingressgateway
  servers:
    - hosts:
        - 100.85.115.86 # 使用的elb实例公网IP
      port:
        name: http-48382bd9
        number: 1026 # 同上lb svc的targetPort
        protocol: http
```

执行以下命令，在网格控制面中创建网关Gateway资源对象。

```
kubectl create -f gw.yaml
```

步骤4 使用以下内容，保存为vs.yaml文件，创建Istio VirtualService配置。

```
apiVersion: networking.istio.io/v1beta1
kind: VirtualService
metadata:
  name: nginx
  namespace: default # 命名空间名称，按需替换
spec:
  hosts:
  - 100.95.150.38  # 使用的elb实例公网IP
  gateways:
  - default/my-gateway # 使用步骤3的gw的命名空间、名称
  http:
  - match:
    - headers:
        cookie:
          exact: "user=dev-123"
    route:
    - destination:
        port:
          number: 1234
        host: nginx.default.svc.cluster.local
```

执行以下命令，在网格控制面中创建VirtualService资源对象。

```
kubectl create -f vs.yaml
```

步骤5 结果验证。执行以下命令，访问nginx服务成功。

```
[root@cluster [redacted] 92754-v64am ~]# curl http://100.95.150.38:707/ --cookie "user=dev-123"
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
```

----结束

11.2 网格使用时无法创建代理，istio 组件调度失败，一直处于 pending 状态

解决方案

请检查节点的istiod的标签（ istio=master ）是否存在，如果不存在请将istiod的标签istio=master加上。

可能原因

在CCE集群中把节点移除之后又再次纳管进去会重置节点，清除节点的标签。

11.3 如何对接 Jaeger/Zipkin 查看调用链

ASM支持向Jaeger/Zipkin导出追踪数据，导出后可在Jaeger/Zipkin界面查看应用的调用链信息。下文以对接zipkin为例介绍完整的使用流程。

前提条件

已明确待安装zipkin的集群和命名空间。

操作步骤

步骤1 创建zipkin deploy。

登录云容器引擎CCE界面，依次单击“集群名称-工作负载-无状态工作负载-YAML创建”，复制粘贴下面的内容到YAML创建输入框中。

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: zipkin
  namespace: monitoring
spec:
  progressDeadlineSeconds: 600
  replicas: 1
  revisionHistoryLimit: 10
  selector:
    matchLabels:
      app.kubernetes.io/instance: zipkin
      app.kubernetes.io/name: zipkin
  strategy:
    rollingUpdate:
      maxSurge: 25%
      maxUnavailable: 25%
    type: RollingUpdate
  template:
    metadata:
      labels:
        app.kubernetes.io/instance: zipkin
        app.kubernetes.io/name: zipkin
    spec:
      automountServiceAccountToken: false
      containers:
      - env:
        - name: STORAGE_TYPE
          value: mem
        image: openzipkin/zipkin-slim:latest                    # 社区zipkin镜像地址，请自行确保网络可达
        imagePullPolicy: IfNotPresent
        name: zipkin
        readinessProbe:
          failureThreshold: 3
          httpGet:
            path: /health
            port: 9411
            scheme: HTTP
          initialDelaySeconds: 5
          periodSeconds: 5
          successThreshold: 1
          timeoutSeconds: 1
        resources:
          limits:
            cpu: 500m
            memory: 4Gi
          requests:
```



```
        cpu: 100m
        memory: 128Mi
    securityContext:
      readOnlyRootFilesystem: true
      runAsNonRoot: true
      runAsUser: 1000
    terminationMessagePath: /dev/termination-log
    terminationMessagePolicy: File
  terminationGracePeriodSeconds: 30
```

预期结果：

创建完成后会在无状态负载页面新增一条名称为zipkin的记录，其状态变为运行中表示zipkin已成功安装到该集群的monitoring命名空间下。

说明

也可参考**zipkin官网资料**自行完成安装。

步骤2 创建负载均衡服务。

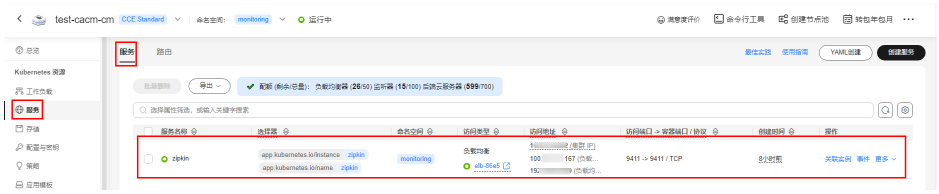
在集群详情页面，单击“服务-服务-创建服务”，如下设置参数：

- Service名称：自定义填写，此处以zipkin为例。
- 访问类型：选择负载均衡。
- 选择器：单击“引用负载标签”，自动添加。
- 端口配置：配置容器端口和服务端口，此处以9411为例。

其他参数使用默认值即可。

预期结果：

设置完成后会在服务页面增加一条服务名称为zipkin的记录。如下：



注意

如果不需要访问UI，访问类型可选择集群内访问。

步骤3 创建容器舰队，添加集群选择**步骤1**中的集群。

步骤4 创建网格，配置对接Zipkin服务。

登录华为云UCS服务页面，单击“创建网格”，绑定容器舰队选择**步骤3**创建的容器舰队，“可观测性配置--调用链”选择“第三方Jaeger/Zipkin服务”，填写服务地址和服务端口，其他参数根据需要自行填写。

注意

服务地址为**步骤2**中所创建服务的<服务名称>.<命名空间>.svc.cluster.local。

服务端口为**步骤2**填写的9411。

步骤5 部署体验服务。

步骤6 访问productpage触发产生调用链数据。

进入ASM网格详情页，单击服务管理页面productpage服务的外部访问地址http://ip:19100/productpage。

步骤7 在zipkin客户端页面查看调用链信息。

说明

zipkin 客户端登录的IP地址和端口可从如下路径获取：

- IP地址：进入安装zipkin集群详情页面，“服务-服务”页面中zipkin服务的负载均衡公网IP。
- 端口：“服务-服务”页面中zipkin服务的访问端口。

----结束

12 容器智能分析

12.1 集群因插件资源残留开启监控失败怎么办?

问题现象

- 集群开启监控时，接口返回报错，报错信息中含有“release name already exists”字段。
- 集群开启监控请求下发成功，但是监控状态为“安装失败”或“未知”，在开启监控页面查看kube-prometheus-stack插件接口，插件安装未成功原因含有“resource that already exists”字段。

原因分析

kube-prometheus-stack插件存在资源残留。

处理手段

可执行如下操作进行资源残留清理，并在清理后重新开启监控。

kubectl delete ns monitoring

kubectl delete ClusterRole cluster-problem-detector custom-metrics-resource-aggregated-reader event-exporter prometheus-operator prometheus-server ucsaddon-cie-collector-kube-state-metrics

kubectl delete ClusterRoleBinding ucsaddon-cie-collector-kube-state-metrics cluster-problem-detector event-exporter prometheus-operator prometheus-server

kubectl delete apiservice v1beta1.custom.metrics.k8s.io

12.2 集群因策略拦截开启监控失败怎么办?

问题现象

- 集群开启监控时，接口返回报错，报错信息中含有gatekeeper字段。

- 集群开启监控请求下发成功，但是监控状态一直显示“安装中”，超时后显示“安装失败”，前往集群中检查插件的Pod状态，Pod的事件中含有gatekeeper字段。

原因分析

如果开启监控的集群在策略中心配置了拦截级别的策略规则，则可能导致开启监控失败。

处理手段

请在指定集群的策略实例中，取消针对kube-system和monitoring命名空间的拦截策略。

12.3 如何修改 kube-state-metrics 组件的采集配置?

问题描述

kube-prometheus-stack插件的kube-state-metrics组件负责将Prometheus的metrics数据格式转换成K8s API接口能识别的格式。kube-state-metrics组件在默认配置下，不采集K8s资源的所有labels和annotation。如需采集则需要在启动参数中修改采集配置，并同时检查名称为kube-state-metrics的ServiceMonitor中采集白名单是否添加相应指标。

操作步骤

步骤1 执行以下命令打开kube-state-metrics工作负载对应的YAML文件。

kubectl edit deployment kube-state-metrics -nmonitoring

步骤2 修改kube-state-metrics的启动参数。

例如需要采集Pod的所有labels时，则将kube-state-metrics的启动参数修改为：

```
--metric-labels-allowlist=pods=[*],nodes=[node,failure-domain.beta.kubernetes.io/
zone,topology.kubernetes.io/zone]
```

kube-state-metrics将开始采集Pod和Node的labels指标，并通过**kubectl edit servicemonitor kube-state-metrics -nmonitoring**查询kube_pod_labels是否在普罗的采集任务中。

如需采集annotation，则在启动参数中以相同方法添加参数--metric-annotations-allowlist。

参考文档：**https://github.com/kubernetes/kube-state-metrics/blob/v2.2.3/docs/cli-arguments.md**

----结束

