阿里云
容器服务

运维指南

产品版本：V1.1.0

文档版本：20180416

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

表 -1: 格式约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	**禁止**： 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	**警告**： 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	**说明**： 导出的数据中包含敏感信息，请妥善保存。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	**说明**： 您也可以通过按**Ctrl** + **A**选中全部文件。
>	多级菜单递进。	**设置** > **网络** > **设置网络类型**
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
courier字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[]或者[a|b]	表示可选项，至多选择一个。	ipconfig *[-all|-t]*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *{stand | slave}*

目录

法律声明.....I
通用约定.....I
1 例行维护.....1
1.1 运维信息梳理.....1
1.2 容器服务-专有云Agility版重启.....1
1.3 管控重启.....1
2 安全维护.....2
2.1 网络安全维护.....2
2.2 证书安全.....2
3 节点伸缩.....3
3.1 扩容.....3
3.2 缩容.....3
4 故障处理.....4
4.1 故障处理方法.....4
4.2 应用故障处理.....5
4.2.1 管控系统故障处理.....6
4.2.2 Troopers或Console启动失败.....6
4.2.3 无法登录.....6
4.2.4 集群证书不可用.....7
4.2.5 DB不可用.....7
4.3 Volume driver故障处理.....7
4.3.1 Volume driver运行异常.....7
4.3.2 无法创建NAS数据卷.....7
4.3.3 无法删除NAS数据卷.....8
4.4 Proxy故障处理.....8
4.4.1 查看Proxy日志.....8
4.4.2 Proxy运行异常.....8
4.4.3 重启Proxy容器.....9
4.4.4 通过curl访问https://master_ip:4243/hosts/接口不通.....9
4.5 监控服务故障处理.....9
4.5.1 数据采集端.....9
4.5.2 数据写入端.....10
4.5.3 数据存储端.....10
4.5.4 数据展示端.....11
4.6 日志服务故障排查.....12

1 例行维护

1.1 运维信息梳理

整个运维过程中，需要如下组件：控制台、Troopers、DB、Proxy、Monitoring、Logging。

您还需要获取容器服务-专有云Agility版管控节点所在的机器。

1.2 容器服务-专有云Agility版重启

容器服务-专有云Agility版系统由多个容器服务组成，通过多台管理节点实现系统服务的高可用。一般不需要执行重启操作，如果出现节点异常，参考以下链接进行状态恢复：*https://docs.docker.com/datacenter/ucp/2.1/guides/admin/monitor-and-troubleshoot/troubleshoot-node-messages/*

1.3 管控重启

容器管控节点采用容器方式部署。如果需要重启，可以采用如下的步骤。

登录UCP界面，在服务界面找到相应服务的界面，单击右上角的**Restart**。

也可以找到服务部署的节点，执行docker ps | grep [app]命令，查找容器ID。 其中，*[app]*是要查找的应用名。然后，执行docker restart [container_id]命令，重启容器。

2 安全维护

2.1 网络安全维护

节点机器需要放开22、4242、4243、18080、5601、3306、8090、8083、8086、9092、3000。

端口	介绍
22	提供节点通过SSH方式登录
4242、4243	Proxy对外提供服务的端口
18080	控制台对外提供访问接口，禁止此端口将不能访问控制台
5601	日志服务的对外服务端口
8090	Troopers对外服务端口
3306、3307	数据库对外服务端口
8086、9092、3000	监控服务对外服务需要的端口

2.2 证书安全

容器服务-专有云Agility版支持通过证书访问控制节点，下载证书后，务必保证证书的安全性，只允许有权限的用户接触到证书。

如果证书发生泄漏，可以在容器服务-专有云Agility版控制台上吊销证书。

图 2-1: 下载证书

3 节点伸缩

您可以根据每个节点的CPU、Memory的使用情况进行节点伸缩。

您可以通过UCP控制台Dashboard界面查看CPU、Memory额占用比评估集群中节点资源的使用情况，也可以打开Resource - Nodes界面，查看每个节点的CPU、Memory的使用情况。

3.1 扩容

当集群中节点资源出现紧张的时候，需要向集群中添加节点。

操作步骤

1. 登录集群的管理节点。
   - 若添加管理节点，执行 docker swarm join-token manager。
   - 若添加工作节点，执行 docker swarm join-token worker。
2. 或者登录UCP界面，打开Resource - Nodes，单击**Add Node**。
   - 若添加管理节点，勾选**Add node as a manager**。
   - 若添加工作节点，勾选**Add node as a worker**。
3. 上面的操作会输出一个节点添加的命令。登录节点（计划添加的节点）执行上面输出的命令。

3.2 缩容

当集群中节点资源使用率很低的时候，可以删除集群中部分节点。

操作步骤

1. 登录集群的管理节点。
   - 若删除管理节点，需要先把管理节点降级为Worker节点再删除。执行docker node demote manager1然后执行docker node rm manager1。
   - 若删除工作节点，执行docker node rm manager1。
2. 或者登录UCP界面，打开Resource - Nodes，单击要删除的节点。
   - 若删除的是管理节点，需要先把管理节点降级为Worker节点再删除。在**Details** 中单击**Worker**，并单击**Save Changes**。降级成功后再单击**Remove Node**。
   - 若删除的是工作节点，单击**Remove Node**。

4 故障处理

4.1 故障处理方法

您可以在UCP控制台通过集群的状态、资源占用、应用或服务日志来判断故障的原因。此外，也可以通过Docker命令行工具来查看，参考如下步骤。

操作步骤

1. 登录容器服务-专有云Agility版管理控制台。
2. 单击左侧导航栏中的**集群**。
3. 选择所需的集群并单击**管理**。

4. 单击**下载证书**下载证书到指定目录。

5. 解压证书文件。

   `unzip –o certFiles.zip`

6. 复制下图中的环境变量配置，粘贴到命令行中执行，就可以使用Docker Client连接到集群进行故障排查。

4.2 应用故障处理

您可以排查和处理应用、容器和集群的故障。

- 应用故障：应用执行状态与预期不一致
- 容器故障：无法正确创建、停止、更新容器等
- 集群故障：集群创建失败、更新失败、无法连接等

您可以查看容器列表，定位、查找容器。

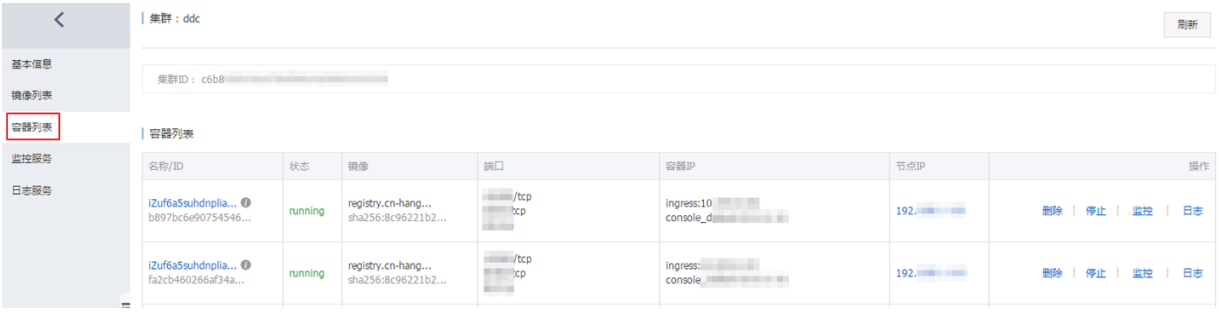
在命令行中输入下面的命令，会列出集群中所有运行的容器。

`docker ps`

在命令行中输入下面的命令，会列出集群中所有的容器（包括非运行状态的容器）。

`docker ps -a`

也可在容器服务-专有云Agility版控制台中，选择指定集群并单击**管理**，在集群详情页面单击**容器列表** 来列出集群中所有容器。



4.2.1 管控系统故障处理

管控系统的组件包括三个部分：控制台，Troopers和DB。普通用户只会直接操作Console。Troopers和DB为集群和用户管理操作提供数据支持和服务。其中Console和Troopers都是无状态应用，如果遇到故障，主要是由于组件之间的连通性和证书。

4.2.2 Troopers或Console启动失败

查看Troopers和Console的日志。

Console和Troopers是无状态应用，启动失败普遍有以下原因。

- 证书加载失败。

  检查证书的合法性。Console在节点的*/usr/ddc/cert/console*。Troopers的证书地址分别为节点的*/usr/ddc/cert/troopers/client*和*/usr/ddc/cert/troopers/server*。

- DB无法连通。

  查看Console和Troopers的环境变量。首先检查Service声明DB的IP地址是否正确。然后进入容器测试下连通性。如果不能连通查看DB的状态。

4.2.3 无法登录

Console遇到的普遍问题是无法登录。如果遇到账号无法登录，需要查看容器的日志，Console调Troopers的*/standalone/authenticate*接口做账号验证。根据返回结果排查问题。

普遍原因包括以下几个。

- Troopers没有正常启动。

  查看Troopers容器的启动状态，以及Console对Troopers调用的地址和端口是否正确。并且查看Troopers的日志是否有对应的请求记录。

- DB没有正常启动。

  查看DB容器的启动状态，并查看Troopers中配置的DB的地址和端口是否正确。在DB中查看*troopers_standalone_user_info*中是否有对应用户的数据。

- Console和Troopers的证书不匹配。

  查看控制台调用Troopers的地址是否是https。如果是，查看调用记录是否有*java.security.cert*相关的信息。如果有，需要通过openssl排查Console和Troopers的证书合法性。

4.2.4 集群证书不可用

Troopers负责管理集群的证书。如果出现集群的证书不可用，普遍是因为Troopers中获取到的的根证书信息不正确。

排查方式： 连接DB（直接进入DB容器连接，或者通过3306端口连接），查看*cert_info*表中是否有**path**为root和control/root的记录，以及**cluster/{clusterId}/ca**。如果没有，需要重新生成证书。

4.2.5 DB不可用

DB中存储用户的集群和账号信息。如果DB出现异常，可以通过UCP的控制面板或者在DB对应的机器上执行`docker exec`进入DB容器中，通过容器中的MySQL client登录到MySQL中，查看数据的完整性。或者连接UCP的3306端口，登录查看数据库。

默认配置Master的端口是3306，slave的端口是3307。如果Master节点出现故障完全不可用，需要快速恢复数据可用，可在slave的MySQL上执行`stop slave`，停止从库的复制，并将Console和Troopers的引用的DB端口改为3307。

假如只是Master容器出现故障，数据没有异常，可以直接重启Master容器，重启后数据不会丢失。

4.3 Volume driver故障处理

4.3.1 Volume driver运行异常

操作步骤

1. 在节点后台查看volume driver是否运行正常。

   `docker ps -a| grep volumedriver`

2. 查看容器日志。

   `docker logs volumedriver`

   运行异常的常见原因有：

   - 访问ETCD失败，需要检查ETCD证书和IP配置。
   - 安装nfs-common失败，可能是由于集群无法访问公网，无法通过yum进行安装，需要手动安装nfs-common，然后重启volume driver。

4.3.2 无法创建NAS数据卷

操作步骤

1. 首先检查volume driver是否安装成功。

登录每台节点，执行`docker ps -a| grep volumedriver`，查看容器是否正常运行。

2. 如果数据卷容器运行正常，则查看容器日志。

   `docker logs volumedriver`

   一般在日志的最后部分会显示出无法创建NAS数据卷的原因；例如网络不通可能会提示**Cannot connect to nas host:****。

3. 如果数据卷容器运行异常，则重新部署volumedriver。

4.3.3 无法删除NAS数据卷

操作步骤

1. 首先检查volume driver是否安装成功。

   登录每台节点，执行`docker ps -a| grep volumedriver`，查看容器是否正常运行。

2. 如果数据卷容器运行正常，查看volume driver日志。如果是数据卷正在忙或者正在被其他容器使用，需要先停止相关服务再删除NAS数据卷。

   `docker logs volumedriver`

4.4 Proxy故障处理

4.4.1 查看Proxy日志

操作步骤

1. 登录UCP的服务界面。
2. 单击Proxy服务的task列表，可以看到Proxy具体运行的节点信息。
3. 登录相应节点，执行`docker ps –a | grep ddcproxy`，然后执行`docker logs` *ddcproxy_ID* 获取相关日志。

4.4.2 Proxy运行异常

登录运行Proxy的节点，查看Proxy容器日志。

- 如果容器处于exited状态，查看日志并检查容器的启动参数。

  `docker inspect`*container_id*

- 如果容器正在运行，查看容器日志，基于日志信息判断是证书配置不对还是网络连接的问题。

4.4.3 重启Proxy容器

可以通过UCP控制台重启Proxy服务，也可以登录节点后台，执行docker stop*container_id*。

4.4.4 通过curl访问https://master_ip:4243/hosts/接口不通

操作步骤

1. 检查Proxy启动命令，检查其中的配置参数都是否正确。
   - H 0.0.0.0:4243配置Proxy对外服务端口。
   - trooper_addr配置troopers地址，用来做用户权限管理。
   - cluster_id配置集群ID地址，用来做用户权限管理。
   - ucp_address配置UCP的服务地址和端口。
   - ucp_cert_path用来配置UCP证书目录。
   - tlsverify(--tlskey，--tlscert --tlscacert)用来配置Proxy对外服务证书。
2. 检查用户证书配置是否正确。

   在集群的管理界面，单击**下载证书**进行证书配置。

4.5 监控服务故障处理

监控服务组件众多，各自职责不同，整体服务采用了高可用的架构，在普通用户层面一般只感知控制台对应集群内的监控服务页面，用户可以在该页面内查看集群节点、服务、容器的各项监控指标；也可以在后续使用熟练的情况下自行配置关注的指标展示等等。

当页面展示数据异常，或者弹性伸缩没有按照预期进行容器级别的自动伸缩时可以参考以下方式做故障分析排查和纠错。

一般按以下几个组件分别运维、排查异常。

4.5.1 数据采集端

数据采集端对应服务monitoring-agent，主要用来采集每个节点上容器的监控指标和宿主机的监控指标。如果数据采集端发生故障，则各项容器监控指标和节点指标无法传递给监控服务端，没有数据上报，也就不能做监控数据的展示。所以一般情况下如果监控指标展示时显示数据不全、有漏报，则问题一般出在对应节点的数据采集端。

操作步骤

1. 确认缺少哪部分监控数据，比如是缺少某个节点的还是缺少某些服务的某个容器的指标，通过此信息，确认可能出问题的节点。

2. 登录控制台查看monitoring-agent下是否有容器停止。如果没有异常容器，则需要查看具体的容器日志。
3. 在控制台的monitoring-agent容器列表中，查找到运行于步骤1中定位的节点上的监控agent，单击对应的**日志** 按钮，查看日志输出详情。
4. monitoring-agent容器是无状态的，如果查看的日志中显示异常信息，一般可以通过重启容器解决问题。

4.5.2 数据写入端

由于采用了高可用架构，所以所有数据采集端上报的数据都会经过数据写入端同时写入两个时序数据库。如果数据展示异常，排除了数据采集端的问题以后，可以按照数据流转链路排查数据写入端是否出现问题。

操作步骤

1. 登录控制台，查看monitoring-server-relay对应的容器列表，分别查看每个容器的输出日志。
2. 每个容器主要的作用就是将数据采集端收到的数据同时写入两个数据库中，保证数据的安全性。日志中会输出具体的写入情况，如果看到异常信息，则可以判断是对应的数据库有问题还是网络问题。一般情况下如果没有手动变更过网络信息或者服务信息，网络不会出现异常。如果自行修改过一些配置的话，网络问题的可能性更大一些。这种情况下需要排查容器间网络是否连通。

4.5.3 数据存储端

如果数据展示异常并排除了数据采集端、数据写入端的问题后，需要根据实际情况排查监控数据存储服务的运行情况。

监控数据存储服务对应为monitoring-server和monitoring-server-backup，两个数据库存储相同的数据。monitoring-server服务对应的容器为默认数据库，用来查看监控数据图表的monitoring-client默认链接 monitoring-server，而monitoring-server-backup作为备用数据库。

操作步骤

1. 登录控制台查看monitoring-server对应的容器状态是否正常。
2. 在容器正常的情况下，在浏览器中输入http://控制台的 *IP* 地址:8083用来访问monitoring-server的管控界面。在界面右上角的**Datasource**下拉框中，选择telegraf数据源，然后在页面的**Query**输入框中，输入SHOW MEASUREMENTS，按下回车，列出所有的数据表。可以使用select * from数据表名称order by time desc limit 100来查看最近上报的100条数据。

3. 如果查看对应的数据都没有问题，而展示上显示有问题，则需要继续排查数据展示系统中的配置是否正确。具体操作参见数据展示端运维。
4. 如果查看对应的数据有缺少，或者容器状态异常，则可以尝试把数据展示端的数据源切换到备用的monitoring-server-backup数据库上。具体操作方式参见数据展示端运维。

4.5.4 数据展示端

数据展示端对应monitoring-client服务，主要是连接monitoring-server查询监控指标，根据自定义配置或预先配置好的图表展示监控数据。一般情况下如果看不到监控数据或者数据展示异常，在排查了数据采集端、数据写入端、数据存储端都没有问题的情况下，需要排查数据展示端的配置项。

操作步骤

1. 使用控制台管理员角色登录控制台。
2. 选择所需的集群并单击**管理**。
3. 单击**监控服务**，进入集群对应的监控服务页面。
4. 单击左上角的**Monitoring Service** > **Data Sources**，进入数据源管理界面。
5. 在数据源管理界面，单击 acsmonitoring 数据源。
6. 单击**Save & Test**，测试数据源的连通性。
   - 如果没有异常提示则表示数据源连接正常且能够读取到数据。
   - 如果有异常提示，可以尝试在**Http settings**的配置部分修改**Url**的值，由原来的http://monitoringserver:8086改为http://monitoringserver-backup:8087（注意端口号的变更）。然后，单击**Save & Test**。

     上边**Url** 的改动意味着数据展示从默认的数据库切换到了备用数据库。一般情况下在默认数据库异常时才会做此变动；此外，在修改完以后，您需要尽快恢复默认数据库。
   - 如果两个数据源都不能正常连接，而对应的monitoring-server和monitoring-server-backup服务下的容器都处于正常运行状态，则一般是网络问题导致无法建立连接。这种情况下需要排查一下网络防火墙是否开放了数据存储服务对外提供数据写入、数据读取的端口号，一般默认为8083和8086（备用数据库的端口为8084、8087）。
7. 如果数据源连接没问题，则需要进入到展示异常的dashboard 中，排查对应的图表的配置。

   一般是数据查询语句书写有问题，可以参考未出异常的配置进行修改。

4.6 日志服务故障排查

当部署应用之后，在界面上查不到日志，需要按照以下步骤进行排查。

操作步骤

1. 检查应用label。

   应用上正确声明了日志收集label 的情况下，fluentd-pilot才会收集日志。如果没有正常收集日志，先检查label配置是否正确。

2. 检查fluentd-pilot是否正常运行。

   a) 登录应用容器所在的节点，执行`docker ps|grep fluentd-pilot`，查看fluentd-pilot是否正常运行。

   b) 执行`docker logs fluentd-pilot-container`，根据fluentd-pilot的日志判断是否正确处理了应用容器。

3. 检查Kibana索引配置。fluentd-pilot会把应用日志写到特定的ElasticSearch索引下，在Kibana上先要创建索引才能正确的查询日志。应用和索引的对应关系详见*fluentd-pilot使用文档*。