阿里云
专有云Enterprise版

告警参考

产品版本：V3.3.0

文档版本：20180312

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

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

1 基础告警

1.1 Alarm-01.100.0000.0000-硬盘使用率过高

当检测到任何一个分区磁盘使用率或者inode使用率超过80%时，产生P4告警，超过90%时产生P1告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件,tianji.TianjiClient

处理方法

1. 登录天基控制台。
2. 选择**运维** > **机器运维**，查找报警的host或ip。
3. 选中需要的机器，打开terminal service。
4. 执行df和df -i命令，查看硬盘空间占用情况。
5. 执行du命令，查找空间占用大的目录。
6. 执行docker images命令，查找是否是过期docker images太多。
7. 如果该服务的硬盘空间虽然占用较大，但使用率恒定，可以在**服务运维** > **监控实例**下编辑报警规则，调大报警阈值。

1.2 Alarm-01.100.0005.0000-NTP时间出现偏移

${sync}!=0 ${offset}>500。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件,tianji.TianjiClient

处理方法

1. 登录天基控制台。
2. 选择**运维** > **机器运维**，查找报警的host或IP。
3. 选中需要的机器，打开terminal service。
4. 执行date命令，查看该host机器时间是否正常。

5. 执行ntpdate time.ntp.org命令，找到ntp服务器。
6. 在crontab中添加"0 12 * * * * /usr/sbin/ntpdate"。

1.3 Alarm-01.100.0010.0000-内存使用率过高

$util_max>95。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件,tianji.TianjiClient

处理方法

1. 登录天基控制台。
2. 选择**运维** > **机器运维**，查找报警的host或ip。
3. 选中需要的机器，打开terminal service。

   一般情况下，linux服务器内存占用率较高时，还要同时判断服务是否正常，服务正常可以不做任何处理。
4. 如果服务不正常，执行top命令，并按内存列排序，找出内存占用最大的进程，重启进程。
5. 同步报备阿里云技术支持。

1.4 Alarm-01.100.0015.0000-CPU负载过高

$load5_max>20。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件,tianji.TianjiClient

处理方法

1. 登录天基控制台。
2. 选择**运维** > **机器运维**，查找报警的host或IP。
3. 选中需要的机器，打开terminal service。

   一般情况下，linux服务器cpu load较高时，同时判断服务是否正常，服务正常可以不做任何处理。

4. 如果服务不正常，执行top命令，按cpu占用率排序，找出cpu占用最大的进程，重启进程。
5. 同步报备阿里云技术支持。

1.5 Alarm-01.100.0020.0000-网络流量过高

$ifin_max>52428800||$ifout_max>52428800。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件,tianji.TianjiClient

处理方法

1. 登录天基控制台。
2. 选择**运维** > **机器运维**，查找报警的host或IP。
3. 选中需要的机器，打开terminal service。

   一般情况下，linux服务器cpu load较高时，需要同时判断服务是否正常，服务正常可以不做任何处理。

1.6 Alarm-01.100.0025.0000-CPU使用率过高

$util_max>200。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件,tianji.TianjiClient

处理方法

1. 登录天基控制台。
2. 选择**运维** > **机器运维**，查找报警的host或IP。
3. 选中需要的机器，打开terminal service。

   一般情况下，linux服务器cpu 使用率较高时，需要同时判断服务是否正常，服务正常可以不做任何处理。
4. 如果服务不正常，执行top命令，按CPU占用率排序，找出cpu占用最大的进程，重启进程。
5. 同步报备阿里云技术支持。

1.7 Alarm-01.100.0030.0000-TCP连接数据过多

$_ports_max>500||$_timewait_max>100000||$_closed_max>100000||$_estab_max>100000||$_TCP_max>100000。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件,tianji.TianjiClient

处理方法

1. 登录天基控制台。
2. 选择**运维** > **机器运维**，查找报警的host或IP。
3. 选中需要的机器，打开terminal service。
4. 在TianjiPortal的机器视图中，查看流量监控图。
5. 如果是网络突发抖动，请观察是否还会出现类似情况。

   如果是持续上涨，请扩容该服务，或者增强硬件配置。
6. 其它情况请联系阿里云技术支持。

1.8 Alarm-01.100.0035.0005-主机Ping响应超时

$rta_avg>500||$loss_max>80。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	tianji	远程,tianji.TianjiClient

处理方法

各业务引入时自定义。

1.9 Alarm-01.100.0035.0010-主机SSH无响应

$state!=0。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	tianji	远程,tianji.TianjiClient

处理方法

各业务引入时自定义。

1.10 Alarm-01.100.0035.0015-HTTP探测无响应

$state!=0。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1		远程,tianji.TianjiClient

处理方法

各业务引入时自定义。

1.11 Alarm-01.100.0035.0020-页面探测无响应

$state!=0。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	-	远程,tianji.TianjiClient

处理方法

各业务引入时自定义。

1.12 Alarm-01.100.0035.0025-主机Ping无响应

$state!=0。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	-	远程,tianji.TianjiClient

处理方法

各业务引入时自定义。

1.13 Alarm-01.100.0035.0030-端口探测失败

$state!=0。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	-	远程,tianji.TianjiClient

处理方法

各业务引入时自定义。

1.14 Alarm-01.100.0035.0035-vip探测失败

$state!=0。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1		远程,tianji.TianjiClient

处理方法

各业务引入时自定义。

1.15 Alarm-01.100.0035.0040-URL检查失败

$state!=0。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1		远程,tianji.TianjiClient

处理方法

各业务引入时自定义。

1.16 Alarm-01.100.0080.0000-JVM线程状态异常

$count_max>2000||$deadlock_count_max>0。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件,tianji.TianjiClient

处理方法

1. 登录天基控制台。
2. 选择**运维** > **机器运维**，查找报警的host或IP。
3. 选中需要的机器，打开terminal service。
4. 执行docker ps命令，查找相应的容器。
5. 查看jvm进程，是否可以自动恢复。

   如果可以自动恢复，建议修改报警规则，增加出现异常次数。

   如果规律的多次出现，建议对该服务进行扩容。

1.17 Alarm-01.100.0090.0000-JVM GC次数过多

$count_max>2000。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件，tianji.TianjiClient

处理方法

1. 进入TianjiPortal，选择**运维** > **机器运维**，查找报警的host或IP。
2. 选中你要的机器，打开terminal service，执行docker ps命令，查找到相应的容器。
3. 查看jvm进程，看是否可以自动恢复，如果可以自动恢复，建议修改报警规则，增加出现异常次数。

   如果规律的多次出现，建议对该服务进行扩容。

1.18 Alarm-01.100.0115.0000-JVM堆内存使用率过高

$usage_max>93。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件,tianji.TianjiClient

处理方法

1. 登录天基控制台。
2. 选择**运维** > **机器运维**，查找报警的host或IP。
3. 选中需要的机器，打开terminal service。
4. 执行docker ps命令，查找相应的容器。
5. 查看jvm进程，是否可以自动恢复，如果可以自动恢复，建议修改报警规则，增加出现异常次数
6. 如果规律的多次出现，建议对服务进行扩容。

1.19 Alarm-01.100.0125.0000-容器硬盘使用率过高

当检测到任何一个分区磁盘使用率或者inode使用率超过80%时，产生P4告警，超过90%时，产生P1告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件,tianji.TianjiClient

处理方法

1. 登录天基控制台。
2. 选择**运维** > **机器运维**，查找报警的host或IP。
3. 选中需要的机器，打开terminal service。
4. 执行docker ps命令，查找到相应的容器。
5. 执行df和df -i命令，查看硬盘空间占用情况。
6. 执行du命令，查看空间占用大的目录。
7. 执行docker images命令，查找是否是过期docker images太多。

如果该服务的硬盘空间虽然占用较大，但使用率恒定，可以在**服务运维** > **监控实例**下编辑报警规则，调大报警阈值。

1.20 Alarm-01.100.0130.0000-容器NTP时间出现偏移

${sync}!=0 ${offset}>500。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件,tianji.TianjiClient

处理方法

1. 登录天基控制台。
2. 选择**运维** > **机器运维**，查找报警的host或IP。
3. 选中需要的机器，打开terminal service。

   执行docker ps命令，查找到相应的容器。
4. 执行date命令，查看该host机器时间是否正常。
5. 找到ntp服务器，执行ntpdate time.ntp.org命令。

   在crontab中添加"0 12 * * * * /usr/sbin/ntpdate"。

1.21 Alarm-01.100.0135.0000-容器内存使用率过高

$util_max>95。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件,tianji.TianjiClient

处理方法

1. 登录天基控制台。
2. 选择**运维** > **机器运维**，查找报警的host或IP。
3. 选中你要的机器，打开terminal service。
4. 执行docker ps命令，查找到相应的容器。

一般情况下，linux服务器内存占用率较高时，需要同时判断服务是否正常，服务正常可以不做任何处理。

5. 如果服务不正常，执行top命令，按内存列排序，找出内存占用最大的进程，重启进程。
6. 同步报备阿里云技术支持。

1.22 Alarm-01.100.0140.0000-容器CPU负载过高

$load5_max>20。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件,tianji.TianjiClient

处理方法

1. 登录天基控制台。
2. 选择**运维** > **机器运维**，查找报警的host或IP。
3. 选中需要的机器，打开terminal service。
4. 执行docker ps命令，查找到相应的容器。

   一般情况下，linux服务器cpu load较高时，需要同时判断服务是否正常，服务正常可以不做任何处理。
5. 如果服务不正常，执行top命令，按CPU占用率排序，找出CPU占用最大的进程，重启进程。
6. 同步报备阿里云技术支持。

1.23 Alarm-01.100.0145.0000-容器网络流量过高

$ifin_max>52428800||$ifout_max>52428800。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件、tianji.TianjiClient

处理方法

1. 登录天基控制台。
2. 选择**运维** > **机器运维**，查找报警的host或IP。

3. 选中需要的机器，打开terminal service。
4. 执行docker ps命令，查找到相应的容器。

   一般情况下，linux服务器cpu load较高时，还要同时判断服务是否正常，服务正常可以不做任何处理。

1.24 Alarm-01.100.0150.0000-容器CPU使用率过高

$util_max>200。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件、tianji.TianjiClient

处理方法

1. 登录天基控制台。
2. 选择**运维** > **机器运维**，查找报警的host或IP。
3. 选中需要的机器，打开terminal service。
4. 执行docker ps命令，查找到相应的容器。

   一般情况下，linux服务器cpu 使用率较高时，需要同时判断服务是否正常，服务正常可以不做任何处理。
5. 如果服务不正常，执行top命令，按cpu占用率排序，找出cpu占用最大的进程，重启进程。
6. 同步报备阿里云技术支持。

1.25 Alarm-01.100.0155.0000-容器TCP连接数据过多

$_ports_max>500||$_timewait_max>100000||$_closed_max>100000||$_estab_max>100000||$_TCP_max>100000。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	tianji	硬件,tianji.TianjiClient

处理方法

1. 登录天基控制台。

2. 选择**运维** > **机器运维**，查找报警的host或IP。
3. 选中需要的机器，打开terminal service。
4. 执行docker ps命令，查找到相应的容器。
5. 在TianjiPortal的机器视图中，查看流量监控图。

   如果是网络突发抖动，请观察是否还会出现类似情况。
6. 如果是持续上涨，请扩容该服务，或者增强硬件配置。
7. 其它情况，请报备阿里云技术支持。

2 女娲（nvwa）

2.1 Alarm-02.005.0001.00001-check_nuwa_config

查看nuwa config。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P1)	nuwa	nuwa

可能原因

配置文件丢失。

影响范围

影响集群服务。

处理方法

联系nuwa开发排查问题。

2.2 Alarm-02.005.0003.00001-check_nuwa_election_event

这个脚本检查女娲后端zk是否发生了选举，以及zxid低32位是否快耗尽。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P3)	Nuwa	Nuwa系统中的NuwaZK serverrole

可能原因

nuwa zk发生了重新选举，后端zk的zxid低32位已经快接近耗尽的边缘。

影响范围

nuwa发生选举影响不大。

处理方法

登录到集群中看下发生选举原因即可，不需要做什么操作。

2.3 Alarm-02.005.0001.00002-check_nuwa_proxy_log

通过从集群ag上扫描女娲proxy的log，检查是否存在长时间没有log输出的情形。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P1)	Nuwa	Nuwa系统中的NuwaProxy serverrole

可能原因

该机器上的nuwa proxy停止工作了，磁盘是否只读了，或者其他什么原因。

影响范围

影响nuwa proxy进程。

处理方法

登录到集群中看这台机器出现了什么问题；

- 进程依赖的挂载磁盘可能只读了导致日志的缺失，需要重启机器。
- nuwa proxy进程有问题，需要重启进程进行检查。
- 如果是其他相关问题，需要特殊情况特殊处理。

2.4 Alarm-02.005.0002.00001-check_nuwa_zookeeper_log

通过从集群ag上扫描女娲zk的log，检查是否存在长时间没有log输出的情形，或者是依赖的磁盘变成只读模式。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P1)	Nuwa	Nuwa系统中的NuwaZK serverrole

可能原因

该机器上的nuwa ZK停止工作了，磁盘是否只读了，或者其他什么原因。

影响范围

影响nuwa zk进程。

处理方法

登录到集群中看这台机器出现了什么问题：

- 机器的磁盘可能只读了导致日志的缺失，这个时候应该需要重启机器。
- nuwa zk进程有问题，需要重启进程进行检查。
- 如果是其他相关问题，需要特殊情况特殊处理。

2.5 Alarm-02.005.0001.00003-check_nuwa_proxy_service

针对女娲的proxy，逐台Server检查服务是否可用。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P1)	Nuwa	Nuwa系统中的NuwaProxy serverrole

可能原因

该nuwa proxy有异常，可能是机器挂掉，有可能ssh不通，有可能nuwa proxy进程有问题。

影响范围

影响nuwa proxy进程。

处理方法

登录到集群中看这台机器出现了什么问题；

- 当机器ping不通或者ssh不通的话，需要重启机器，如果机器重启不成功，替换机器。
- 如果是其他相关问题，需要特殊情况特殊处理。

2.6 Alarm-02.005.0002.00002-check_nuwa_zk_service

针对女娲的ZK，逐台Server检查服务是否可用。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P1)	Nuwa	Nuwa系统中的NuwaZK serverrole

可能原因

该nuwa zk有异常，可能是机器挂掉，有可能ssh不通，有可能nuwa zk进程有问题。

影响范围

影响nuwa zk进程。

处理方法

登录到集群中看这台机器出现了什么问题；

- 当机器ping不通或者ssh不通的话，需要重启机器，如果机器重启不成功，就需要替换机器。
- 如果是其他相关问题，需要特殊情况特殊处理。

2.7 Alarm-01.005.0003.00002-check_nuwa_server_disk

针对女娲后端ZK的依赖/apsara盘，snapshot盘以及txnlog盘进行监控，并且针对proxy/zk的log输出情况进行监控。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P1)	Nuwa	Nuwa系统中的NuwaZK/NuwaProxy serverrole

可能原因

/apsara盘使用率超过85%，snapshot盘以及txnlog盘使用率超过70%，或者是proxy/zk的log超过5min没有任何输出。

影响范围

影响proxy和zk进程的磁盘读写，进而影响进程。

处理方法

登录到集群中看这台机器的磁盘与目录空间；

- 磁盘空间满了，需要清理。
- 目录空间满了，需要清理。
- 如果是其他相关问题，需要特殊情况特殊处理。

2.8 Alarm-02.005.0004.00001-check_nuwa_config_in_tianji

检查所有的机器的配置文件是否和tianji中的终态一致(适用于跨集群配置打通)。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	Nuwa	Nuwa系统中的NuwaConfig serverrole

可能原因

跨集群打通配置遇到了问题，会造成跨集群访问的失败。

影响范围

影响nuwa跨集群访问的功能。

处理方法

需要调查tianji下打通集群为什么失败，失败的原因有很多，模板配置的出错，tianji api的访问失败等。

3 云控制台

3.1 Alarm-01.105.0008.0001-内存使用率过高

内存使用率过高。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	ClusterOwner	软件

可能原因

服务接收metaq数据过多。

影响范围

DTCenter服务可能出现异常。

处理方法

1. 重启容器中的dtcenter服务，将*/alidata/www/logs/tomcat7/*，*/opt/tomcat7/logs/* 的日志文件保存下来，发给技术支持人员。
2. 执行free，查看内存是否使用率仍然很高，如果很高需要做内存扩容。

3.2 Alarm-01.105.0008.0002-CPU负载过高

CPU负载过高。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	ClusterOwner	软件

可能原因

业务过于繁忙。

影响范围

DTCenter服务可能出现异常。

处理方法

重启容器中的dtcenter服务，将*/alidata/www/logs/tomcat7/*， */opt/tomcat7/logs/*的日志文件保存下来。

3.3 Alarm-01.105.0008.0003-网络流量过高

网络流量过高。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	ClusterOwner	软件

可能原因

可能受到攻击。

影响范围

DTCenter服务可能出现异常。

处理方法

查看是否受到攻击。

3.4 Alarm-01.105.0008.0004-CPU使用率过高

CPU使用率过高。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	ClusterOwner	软件

可能原因

业务过于繁忙。

影响范围

DTCenter服务可能出现异常。

处理方法

重启容器中的DTCenter服务，将*/alidata/www/logs/tomcat7/*， */opt/tomcat7/logs/*的日志文件保存下来。

3.5 Alarm-01.105.0008.0005-主机Ping响应超时

主机Ping响应超时。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	ClusterOwner	软件

可能原因

业务过于繁忙。

影响范围

DTCenter服务可能出现异常。

处理方法

1. 重启容器中的dtcenter服务，将*/alidata/www/logs/tomcat7/*， */opt/tomcat7/logs/*的日志文件保存下来。
2. 执行df，查看磁盘空间是否满了，如果满了，查找*1*日志文件以及diamond目录下的日志文件。

3.6 Alarm-01.105.0008.0006-主机Ping无响应

主机Ping无响应。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	ClusterOwner	软件

可能原因

业务过于繁忙。

影响范围

DTCenter服务可能出现异常。

处理方法

1. 重启容器中的dtcenter服务，将*/alidata/www/logs/tomcat7/*， */opt/tomcat7/logs/*的日志文件保存下来。
2. 执行df，查看磁盘空间是否满了，如果满了，查找*1*日志文件以及diamond目录下的日志文件。

3.7 Alarm-01.105.0008.0007-vip探测失败

vip探测失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	ClusterOwner	软件

可能原因

业务过于繁忙。

影响范围

DTCenter服务可能出现异常。

处理方法

1. 重启容器中的dtcenter服务，将*/alidata/www/logs/tomcat7/*， */opt/tomcat7/logs/*的日志文件保存下来。
2. 执行df，查看磁盘空间是否满了，如果满了，查找*1*日志文件以及diamond目录下的日志文件。

3.8 Alarm-01.105.0008.0008-HTTP探测无响应

HTTP探测无响应。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	ClusterOwner	软件

可能原因

可能服务启动不正常。

影响范围

DTCenter服务可能出现异常。

处理方法

1. 执行free，查看内存是否使用率很高，如果很高需要做内存扩容。
2. 执行df，查看磁盘空间是否满了，如果满了，查找日志文件以及diamond目录下的日志文件并删除，恢复磁盘空间。

3. 执行netstat -nao；ps aux| grep tomcat，看是否在监听18080端口，以及tomcat进程是否存在。如不存在需要执行4
4. 重启容器中的tomcat服务，将*/alidata/www/logs/tomcat7/*， */opt/tomcat7/logs/*的日志文件保存下来。

3.9 Alarm-01.105.0008.0009-页面探测无响应

页面探测无响应。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	ClusterOwner	软件

可能原因

可能服务启动不正常。

影响范围

DTCenter服务可能出现异常。

处理方法

1. 执行free，查看内存是否使用率很高，如果很高需要做内存扩容。
2. 执行df，查看磁盘空间是否满了，如果满了，查找1下面的日志文件以及diamond目录下的日志文件并删除，恢复磁盘空间。
3. 执行netstat -nao；ps aux| grep tomcat，看是否在监听18080端口，以及tomcat进程是否存在。如不存在需要执行4
4. 重启容器中的tomcat服务，将*/alidata/www/logs/tomcat7/*， */opt/tomcat7/logs/*的日志文件保存下来。

3.10 Alarm-01.105.0008.0010-Url检查失败

Url检查失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	ClusterOwner	软件

可能原因

可能服务启动不正常。

影响范围

DTCenter服务可能出现异常。

处理方法

1. 执行free，查看内存是否使用率很高，如果很高需要做内存扩容。
2. 执行df，查看磁盘空间是否满了，如果满了，查找1下面的日志文件以及diamond目录下的日志文件并删除，恢复磁盘空间。
3. 执行netstat -nao；ps aux| grep tomcat，看是否在监听18080端口，以及tomcat进程是否存在。如不存在需要执行4。
4. 重启容器中的tomcat服务，将*/alidata/www/logs/tomcat7/*， */opt/tomcat7/logs/*的日志文件保存。

4 伏羲

4.1 Nuwaaddressalert-send title- odps-service-controller _serviceNamenuwaaddressalert

判断女娲是否会丢失odps某些节点。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

Nvwa关联的odps节点有丢失。

影响范围

严重。

处理方法

无。

4.2 Alarm-02.010.0002.00003-odps_apsara_fm_ag-check_fuxi _master_hang

集群中的FuxiMaster不服务。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	紧急(P1)	fuxi	FuxiMaster

可能原因

FuxiMaster进程无法响应请求。

影响范围

无法向伏羲提交任务。

处理方法

1. FuxiMaster会自动处理这种情况，收到报警后请登录集群使用/apsara/deploy/rpc_wrapper/rpc.sh al命令，检查是否恢复 。
2. 如果未恢复，请检查nuwa 服务是否正常，是否存在压力过大的情况。

4.3 Alarm-01.010.0002.00004-odps_apsara_fm_ag-check_fuxi_job_num

FuxiMaster提交的任务数过多。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	紧急(P1)	fuxi	FuxiMaster

可能原因

- 用户odps任务提交过多，或者提交了太多的merge task

影响范围

- fuxi性能下降，甚至完全无法响应

处理方法

停掉不低优先级的作业

4.4 Alarm-02.010.0003.00005-odps_apsara_fm_ag-check_fuxi service_status

集群中aos_fuxi包不存在。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	紧急(P1)	fuxi	Package

可能原因

- 误删除了aos_fuxi包

影响范围

- 无法启动job或者service

处理方法

检查Package这个serverrole进程是否存在，如果存在重启该进程。

4.5 Alarm-02.010.0002.00006-odps_apsara_fm_ag-check_fuxi_master_switch

FuxiMaster发生了主备切换。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	fuxi	FuxiMaster

可能原因

FuxiMaster原机器无法连接到nuwa。

影响范围

FuxiMaster主机数目减少，服务能力降低。

处理方法

检查切换前的fuximaster机器是否正常，是否存在软件硬件故障。

4.6 Alarm-02.010.0002.00007-odps_apsara_fm_ag-check_fuxi_master_alive

FuxiMaster进程不存在或者FuxiMaster不工作。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	紧急(P1)	fuxi	FuxiMaster

可能原因

FuxiMaster主机无法联系、FuxiMaster进程不存在。

影响范围

FuxiMaster无法正常服务。

处理方法

检查FuxiMaster机器能否联通，如果能联通，检查Fuximaster进程是否存活。

5 盘古

5.1 Alarm-01.000.0002.00001-盘古Master checkpoint数量不足

当维护工具检测到盘古Master做的checkpoint数量不符合阈值的时候，产生该告警，检测周期为一小时。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

- 盘古Master服务异常，长时间没有做checkpoint。
- 新集群。

影响范围

- 没有足够的checkpoint，会影响master进程启动时候的记载时间。
- 对数据安全性有一定影响。

处理方法

1. 检查集群是否是新创建集群。
   - 如果是，请忽略。
   - 如果否，请跳转至2。
2. 登录报警机器，查看/apsarapangu空间是否足够，如果空间不足，释放一下磁盘空间。

5.2 Hivegclogalert-send title-odps-service-controller_serviceNamehivegclogalert

统计hive heap内存是否泄漏。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

Hive heap内存泄漏。

影响范围

严重。

处理方法

重启hive server进程。

5.3 Schedulerpoolsizaalert-send title-odps-service-controller _serviceNameschedulerpoolsizaalert

Schedulepoolsize totalSize的值超过阈值。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

Odps各类任务堆积。

影响范围

严重。

处理方法

1. 可能是正常现场，任务本身就多，此时无需处理，等待即可。
2. 如果是某个组件挂了，导致其他任务在排队，则需要检查并修复该组件。

5.4 Alarm-02.000.0003.00001-盘古chunkserver发生core dump

当维护工具检测到集群中chunkserver有core dump发生的时候，产生该告警，检测周期为15秒。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	盘古	盘古Chunkserver

可能原因

盘古Chunkserver程序运行异常，导致core dump。

影响范围

导致盘古Chunkserver进程重启，可能会造成上层服务发生core dump当时读写延迟高。

处理方法

保留*/cloud/data/corefile*目录下的core dump文件，联系盘古的开发人员，查看core dump的原因。

5.5 Alarm-02.000.0003.00002-盘古Chunkserver有特殊的事件发生

当维护工具检测到集群中chunkserver evet log中有Error级别的告警的时候，产生该告警，检测周期为一小时。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	盘古	盘古Chunkserver

可能原因

发生了诸如磁盘上下线，磁盘状态变ERROR，网络错误等错误事件。

影响范围

可能会影响发生问题的Chunkserver的状态。

处理方法

查看*/apsara/pangu_chunkserver/log*目录下的pangu_event.LOG，查看发生了哪些event，针对event采取相关的措施。

5.6 Alarm-01.000.0003.00003-盘古Chunkserver机器上的load过高

当维护工具检测到集群中chunkserver load高于指定阈值的时候，产生该告警，检测周期为15秒。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Chunkserver

可能原因

盘古Chunkserver上的进程数量过多。

影响范围

影响盘古Chunkserver的运行环境。

处理方法

登录报警的Chunkserver，查看哪些进程占用了大量CPU，确认该进程的运行状态是否符合预期。

5.7 Alarm-01.000.0003.00004-盘古Chunkserver map的so过多

当维护工具检测到集群中chunkserver map的so过多的时候，产生该告警，检测周期为1分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Chunkserver

可能原因

操作系统该异常。

影响范围

影响Chunkserver正常运行。

处理方法

1. 查看*/var/log/messages*是否存在异常。
2. 修复系统的异常。

5.8 Alarm-01.000.0003.00005-盘古Chunkserver内存使用过高

当维护工具检测到集群中chunkserver 内存使用高于指定阈值的时候，产生该告警，检测周期为10分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Chunkserver

可能原因

盘古Chunkserver上的chunk数量过多。

影响范围

影响该Chunkserver的运行状态，有OOM风险。

处理方法

登录PanguTools机器，执行/apsara/deploy/pu quota命令，查看是否创建的文件数量是否过多，联系应用确认写入文件量是否合理。

5.9 Alarm-01.000.0003.00006-盘古Chunkserver网络的recv流量过高

当维护工具检测到集群中chunkserver recv的网络流量过高时，产生该告警，检测周期为15秒。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Chunkserver

可能原因

盘古Chunkserver压力过大。

影响范围

影响该Chunkserver的服务质量。

处理方法

降低Client写压力。

5.10 Alarm-01.000.0003.00007-盘古Chunkserver网络的send流量过高

当维护工具检测到集群中chunkserver send的网络流量过高时，产生该告警，检测周期为15秒。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Chunkserver

可能原因

盘古Chunkserver压力过大。

影响范围

影响该Chunkserver的服务质量。

处理方法

降低Client读压力。

5.11 Alarm-01.000.0003.00008-盘古Chunkserver打开的文件句柄数目过多

当维护工具检测到集群中chunkserver 打开的文件句柄数过多的时候，产生该告警，检测周期为15秒。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Chunkserver

可能原因

盘古Chunkserver打开的chunks文件过多。

影响范围

影响该Chunkserver的服务质量。

处理方法

1. 执行ls -l /proc/<pid>/fd命令，查看Chunkserver进程打开的文件句柄。
2. 删除无用的文件。

5.12 Alarm-02.000.0003.00009-盘古Chunkserver进程有重启

当维护工具检测到集群中chunkserver 有重启的时候，产生该告警，检测周期为1分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	盘古	盘古Chunkserver

可能原因

盘古Chunkserer进程发生了重启，有可能是因为OOM。

影响范围

影响该Chunkserver的正常运行。

处理方法

1. 登录到该Chunkserver，查看dmesg信息，查看是否有OOM。
   - 如果有，确定是因为OOM，造成进程重启，查看Chunkserver内存增长原因。
   - 如果没有，请跳转至2。
2. 查看*/apsara/pangu_chunkserver/log*目录下pangu_chunkserver.LOG.1，搜索FATAL log，查看上一次进程死掉原因。

5.13 Alarm-02.000.0003.00010-盘古Chunkserver ulimit 设置错误告警

当维护工具检测到集群中chunkserver 机器ulimit设置不为unlimited的时候，产生该告警，检测周期为1分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	盘古	盘古Chunkserver

可能原因

ulimit设置错误。

影响范围

可能会影响Chunkserver正常运行。

处理方法

设置盘古Chunkserver机器**ulimit**为**unlimited**。

5.14 Alarm-01.000.0003.00011-盘古Chunkserver 机器/apsara目录空间不足

当维护工具检测到集群中chunkserver 机器/apsara空间不足的时候，产生该告警，检测周期为15秒。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Chunkserver

可能原因

/apsara目录被其他进程大量占用。

影响范围

影响Chunkserver正常运行。

处理方法

登录Chunkserver机器，查看/apsara目录使用情况，联系集群管理员进行清理。

5.15 Alarm-01.000.0003.00012-盘古Chunkserver 机器/apsarapangu目录空间不足

当维护工具检测到集群中chunkserver 机器/apsarapangu空间不足的时候，产生该告警，检测周期为15秒。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Chunkserver

可能原因

/apsarapangu目录被其他进程大量占用。

影响范围

影响Chunkserver正常运行。

处理方法

登录Chunkserver机器，查看/apsarapangu空间使用情况，联系集群管理员进行清理。

5.16 Alarm-01.000.0003.00013-盘古Chunkserver 机器根目录空间不足

当维护工具检测到集群中chunkserver 机器根目录空间不足的时候，产生该告警，检测周期为15秒。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Chunkserver

可能原因

根目录被其他进程大量占用。

影响范围

影响Chunkserver正常运行。

处理方法

登录Chunkserver机器，查看根目录空间使用情况，联系集群管理员清理。

5.17 Alarm-02.000.0002.00002-盘古master发生core dump

当维护工具检测到集群中master有core dump发生时，产生该告警，检测周期为15秒。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	盘古	盘古Master

可能原因

盘古Master程序运行异常，导致core dump。

影响范围

导致盘古Master进程重启，对服务安全性有风险。

处理方法

保留*/cloud/data/corefile*目录下的core dump文件，联系盘古开发人员，查看core dump的原因。

5.18 Alarm-02.000.0002.00003-盘古Master有特殊的事件发生

当维护工具检测到集群中Master evet log中有Error级别的告警时，产生该告警，检测周期为一小时。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	盘古	盘古Master

可能原因

发生了诸如磁盘上下线，磁盘状态变ERROR，网络错误等错误事件。

影响范围

影响发生问题的Master的状态。

处理方法

查看*/apsara/pangu_master/log*目录下的pangu_event.LOG，查看发生了哪些event，针对event采取相关的措施。

5.19 Alarm-01.000.0002.00004-盘古Master机器上的load过高

当维护工具检测到集群中Master load高于指定阈值时，产生该告警，检测周期为15秒。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

盘古Master上的进程数量过多。

影响范围

影响盘古Master的运行环境。

处理方法

登录报警的Master，查看哪些进程占用了大量CPU，确认该进程的运行状态是否符合预期。

5.20 Alarm-01.000.0002.00005-盘古Master map的so过多

当维护工具检测到集群中master map的so过多时，产生该告警，检测周期为1分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

操作系统异常。

影响范围

影响Master正常运行。

处理方法

1. 查看*/var/log/messages*是否存在异常。
2. 修复系统的异常。

5.21 Alarm-01.000.0002.00006-盘古Master内存使用过高

当维护工具检测到集群中Master 内存使用高于指定阈值的时候，产生该告警，检测周期为10分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

盘古上保存的文件数目太多。

影响范围

影响该Master的运行状态，有OOM风险。

处理方法

登录PanguTools机器上执行*/apsara/deploy/pu quota*查看是否创建的文件数量是否过多，联系应用确认写入文件量是否合理

5.22 Alarm-02.000.0002.00007-盘古Master内存overcommit参数配置错误

当维护工具检测到集群中Master 内存overcommit参数配置错误的时候，产生该告警，检测周期为10分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	盘古	盘古Master

可能原因

内存overcommit 配置错误。

影响范围

对盘古Master正常运行有风险。

处理方法

登录该盘古Master机器，设置overcommit参数为0。

5.23 Alarm-01.000.0002.00008-盘古Master内存速度不符合预期告警

当维护工具检测到集群中Master内存速度不符合预期的时候，产生该告警，检测周期为1小时。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

盘古Master内存硬件错误。

影响范围

对盘古Master运行有影响。

处理方法

更换内存。

5.24 Alarm-01.000.0002.00009-盘古Master网络的recv流量过高

当维护工具检测到集群中Master recv的网络流量过高的时候，产生该告警，检测周期为15秒。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

盘古Master压力过大。

影响范围

影响该Master的服务质量。

处理方法

减少读写，删除，创建文件相关的操作。

5.25 Alarm-01.000.0002.00010-盘古Master网络的send流量过高

当维护工具检测到集群中Master send的网络流量过高的时候，产生该告警，检测周期为15秒。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

盘古Master压力过大。

影响范围

影响该Master的服务质量。

处理方法

减少读写，删除，创建文件相关的操作。

5.26 Alarm-01.000.0002.00011-盘古Master打开的文件句柄数目过多

当维护工具检测到集群中Master 打开的文件句柄数过多时，产生该告警，检测周期为15秒。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

盘古Master打开的chunks文件过多。

影响范围

影响该Master的服务质量。

处理方法

1. 执行ls -l /proc/<pid>/fd命令，查看Master进程打开的文件句柄。
2. 删除不需要的文件。

5.27 Alarm-02.000.0002.00012-盘古Master进程有重启

当维护工具检测到集群中Master 有重启时，产生该告警，检测周期为1分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	盘古	盘古Master

可能原因

盘古Master进程发生了重启，可能是因为OOM。

影响范围

Master进程重启比较严重，影响该Master的正常运行。

处理方法

1. 登录到该Master，看dmesg信息，查看是否有OOM。
   - 如果有，确定是由于OOM造成进程重启，查看Master内存增长原因。

- 如果没有，请跳转至2。

2. 查看 */apsara/pangu_master/log*路径下pangu_master.LOG.1，搜索FATAL log，查看上一次进程坏死原因。

5.28 Alarm-02.000.0002.00013-盘古Master ulimit 设置错误告警

当维护工具检测到集群中master 机器**ulimit**没有设置为**unlimited**时，产生该告警，检测周期为1分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	盘古	盘古Master

可能原因

ulimit设置错误。

影响范围

可能会影响Master正常运行。

处理方法

设置盘古Master机器**ulimit**为**unlimited**。

5.29 Alarm-02.000.0004.00001-盘古Supervisor进程发生重启

当维护工具检测到集群中Supervisor 有重启时，产生该告警，检测周期为1分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	盘古	盘古Supervisor

可能原因

盘古Supervisor进程发生了重启，有可能是因为OOM。

影响范围

可能影响相关的运维操作。

处理方法

1. 登录到Supervisor，看dmesg信息，查看是否有OOM。
   - 如果有，确定是因为OOM造成进程重启，查看Supervisor内存增长原因。
   - 如果没有，请跳转至2。
2. 查看*/apsara/pangu_supervisor/log*路径下pangu_supervisor.LOG.1，搜FATAL log，看上一次进程坏死原因。

5.30 Alarm-01.000.0003.00014-检查混合存储机型有效文件在ssd盘的长度

维护工具检测对所有的CS的机器检查有效数据的容量是否超过指定的容量大小，如果超出则产生该警告，检测周期为1分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Chunkserver

可能原因

cs机器的压力太大，或者ssd盘的读写速度太慢。

影响范围

可能会影响数据安全。

处理方法

设置对应的机器为 READONLY:

`puadmin cs -stat tcp://<cs ip>:10260 --set=READONLY`

5.31 Alarm-01.000.0003.00015-检查混合存储机型ssd盘中数据失败的次数

维护工具检测对所有的CS的机器检查replay ssd盘失败的次数，如果存在失败则产生该警告，检测周期为1分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Chunkserver

可能原因

SSD盘可能坏了。

影响范围

可能会影响数据安全。

处理方法

设置对应的机器为 READONLY:

```
puadmin cs -stat tcp://<cs ip>:10260 --set=READONLY
```

5.32 Alarm-02.000.0002.00014-盘古Master发生切换告警

维护工具检测到集群中Master发生主备切换时，产生该告警，检测周期为1分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	盘古	盘古Master

可能原因

盘古Master因为进程本身或者网络原因造成主备切换。

影响范围

切换时，可能会影响盘古Master的服务质量。

处理方法

登录到PanguTools所在的机器，执行/apsara/deploy/puadmin gems命令，查看盘古Master状态，查看所有Master是否处于NORMAL状态：

- 如果是，盘古Master状态正常，可能是当时网络问题。
- 如果不是，查看错误Master的原因。

5.33 Alarm-01.000.0003.00016-盘古Chunkserver坏盘数量过多告警

维护工具检测到集群中Chunkserver上坏盘过多时，产生该告警，检测周期为1分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	盘古	盘古Chunkserver

可能原因

磁盘损坏。

影响范围

盘古存储容量下降。

处理方法

登录PanguTools所在机器，执行/apsara/deploy/puadmin lscs命令，查看状态非DISK_OK的磁盘，并将坏盘下线。

5.34 Alarm-01.000.0003.00017-盘古Chunkserver写满的磁盘数量过多告警

维护工具检测到集群中Chunkserver上被写满的磁盘数量过多时，产生该告警，检测周期为1分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	盘古	盘古Chunkserver

可能原因

写入盘古数据过多。

影响范围

盘古存储容量下降。

处理方法

登录PanguTools所在机器，执行/apsara/deploy/puadmin lscs命令，查看盘古使用情况，如果使用过多，请联系集群负责人扩容。

5.35 Alarm-01.000.0003.00018-盘古Chunkserver HANG盘数量过多告警

维护工具检测到集群中Chunkserver上HANG盘过多的时候，产生该告警，检测周期为1分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Chunkserver

可能原因

磁盘HANG住。

影响范围

造成过多僵尸进程。

处理方法

登录PanguTools所在机器，执行/apsara/deploy/puadmin lscs命令，查看状态DISK_HANG的磁盘，将HANG盘的机器重启。

5.36 Hivechildprocessexistalert-send title-odps-service-controller_serviceNamehivechildprocessexistalert

判断hive子进程是否存在。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

Hive子进程不存在。

影响范围

严重。

处理方法

重启hive server进程。

5.37 Alarm-01.000.0001.00004-check_pangu_diskfull

查看集群盘古磁盘空余空间。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	pangu

可能原因

临时数据过多。

影响范围

影响集群作业数据保存。

处理方法

清理回收站、作业临时文件。

5.38 Alarm-01.000.0001.00005-盘古replication流量过大

维护工具检测到集群中replication流量过大时，产生该告警，检测周期为5分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古整体

可能原因

同一时间大量的机器或者磁盘损坏。

影响范围

存在数据安全性隐患。

处理方法

登录PanguTools机器，执行/apara/deploy/puadmin lscs命令，查看是否有过多的DISCONNECTED机器或者DISK_ERROR的盘。

5.39 Alarm-02.000.0002.00015-盘古Master主从之间log同步差距过大

维护工具检测到集群中Master主从log同步差距过大时，产生该告警，检测周期为5分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	盘古	盘古Master

可能原因

盘古Maste主从之间网络存在问题。

影响范围

影响盘古Master的服务安全性。

处理方法

查看盘古Master主从之间的网络情况。

5.40 Alarm-02.000.0002.00016-盘古Master工作队列过长

维护工具检测到集群中Master工作队列过长时，产生该告警，检测周期为半小时。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

盘古Master压力过大。

影响范围

影响盘古运行状态。

处理方法

减少读写，删除，创建文件相关的操作。

5.41 Alarm-02.000.0002.00017-盘古Master状态告警

维护工具检测到集群中Master状态不对时，产生该告警，检测周期为一分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

盘古Maste因为硬件，网络等原因导致状态不对。

影响范围

影响盘古Master的服务安全性。

处理方法

登录PanguTools机器，执行/apsara/deploy/puadmin gems命令，查看哪个master状态不对并调查原因。

5.42 Alarm-01.000.0001.00006-check_pangu_free_size

集群盘古空闲空间。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	集群

可能原因

数据量过多。

影响范围

影响集群正常存储服务。

处理方法

扩容或者清理数据。

5.43 Alarm-01.000.0001.00007-盘古工作模式告警

维护工具检测到集群中盘古工作模式不对的时候，产生该告警，检测周期为三分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	盘古	盘古整体

可能原因

大于一半的master机器挂了。

影响范围

影响盘古的可用性。

处理方法

修复没有运行的pangu master所在机器。

5.44 Alarm-01.000.0001.00008-盘古总文件数量过多告警

维护工具检测到集群中盘古文件数目过多时，产生该告警，检测周期为一分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古整体

可能原因

盘古中文件数量过大。

影响范围

影响盘古的可用性。

处理方法

删除一些不需要的文件，或者扩大盘古master，cs的内存。

5.45 Alarm-01.000.0001.00009-盘古空间使用超限告警

维护工具检测到集群中盘古使用量超限的时候，产生该告警，检测周期为一天。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古整体

可能原因

盘古中的文件容量过大。

影响范围

影响盘古的可用性。

处理方法

删除不需要使用的文件，或者扩容一些CS。

5.46 Alarm-01.000.0001.00010-盘古SECONDARY master数量不对告警

维护工具检测到集群中盘古SECONDARY master数量不足时，产生该告警，检测周期为半小时。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古整体

可能原因

存在master机器挂了。

影响范围

影响盘古的可用性。

处理方法

修复没有运行的pangu master所在机器。

5.47 Alarm-01.000.0001.00011-盘古binary文件不一致告警

维护工具检测到集群中盘古binary文件版本不一致时，产生该告警，检测周期为一小时。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古整体

可能原因

所有master的二进制文件md5不一致。

影响范围

影响盘古的可用性。

处理方法

将所有的second master 进程修复为一致。

如果是primary master不一致，先切换再修复。

5.48 Alarm-02.000.0002.00018-盘古Normal file的操作队列过长告警

维护工具检测到集群中盘古Master Normal file操作队列过长的时候，产生该告警，检测周期为两分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

Normal File相关的操作过多。

影响范围

影响盘古的可用性。

处理方法

减少Normal File 相关的：读写，删除，创建文件相关的操作。

5.49 Alarm-01.000.0003.00019-盘古Chunkserver sendbuffer过高报警

维护工具检测到集群中盘古Chunkserver sendbuffer过大时，产生该告警，检测周期为两分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Chunkserver

可能原因

读写压力过多。

影响范围

影响盘古的可用性。

处理方法

减少前端读写压力。

5.50 Alarm-02.000.0002.00019-盘古normal file的读操作队列过长告警

维护工具检测到集群中盘古Master 读操作队列过长时，产生该告警，检测周期为两分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

Normal File读压力过大。

影响范围

影响盘古的可用性。

处理方法

减少前端Normal File 的读。

5.51 Alarm-02.000.0002.00020-盘古normal file的写操作队列过长告警

维护工具检测到集群中盘古Master 写操作队列过长时，产生该告警，检测周期为两分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

Normal File写压力过大。

影响范围

影响盘古的可用性。

处理方法

减少前端Normal File 的写。

5.52 Alarm-02.000.0002.00021-盘古Master batch 操作队列过长告警

维护工具检测到集群中盘古Master batch操作队列过长时，产生该告警，检测周期为两分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

Batch相关的操作过多。

影响范围

影响盘古的可用性。

处理方法

减少前端Batch相关的操作。

5.53 Alarm-02.000.0002.00022-盘古Master batch 读操作队列过长告警

维护工具检测到集群中盘古Master batch读操作队列过长时，产生该告警，检测周期为两分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

Batch 读相关的操作过多。

影响范围

影响盘古的可用性。

处理方法

减少前端Batch读相关的操作。

5.54 Alarm-02.000.0002.00023-盘古Master batch 写操作队列过长告警

维护工具检测到集群中盘古Master batch写操作队列过长时，产生该告警，检测周期为两分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

Batch 写相关的操作过多。

影响范围

影响盘古的可用性。

处理方法

减少前端Batch写相关的操作。

5.55 Alarm-02.000.0002.00024-盘古Master 选举队列过长告警

维护工具检测到集群中盘古Master 选举队列过长的时候，产生该告警，检测周期为两分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	盘古	盘古Master

可能原因

网络状态可能有问题。

影响范围

影响盘古的可用性。

处理方法

修复网络相关的错误。

5.56 Alarm-02.000.0002.00025-盘古Master 紧急操作队列过长告警

维护工具检测到集群中盘古Master 紧急操作队列过长时，产生该告警，检测周期为两分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	盘古	盘古Master

可能原因

紧急操作比较多。

影响范围

影响盘古的可用性。

处理方法

降低前端读写，减小盘古自身的压力。

5.57 Alarm-02.000.0002.00026-盘古Master 心跳队列告警

维护工具检测到集群中盘古Master 心跳队列过长时，产生该告警，检测周期为两分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	盘古	盘古Master

可能原因

网络状态可能有问题。

影响范围

影响盘古的可用性。

处理方法

修复网络相关的错误。

5.58 Alarm-02.000.0002.00027-盘古Master高优先级队列过长告警

维护工具检测到集群中盘古Master 高优先级队列过长时，产生该告警，检测周期为两分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古Master

可能原因

高优先级的操作比较多。

影响范围

影响盘古的可用性。

处理方法

降低前端读写，减小盘古自身的压力。

6 云服务器ECS

6.1 Alarm-01.200.0011.00001-libvirtd进程异常

监控项用于KVM虚拟化libvirtd进程的监控。检测时间间隔为60秒，当检测到libvirtd进程无法正常链接时对外报警，并自动重启libvirtd进程。

告警信息

告警类型	告警级别	告警对象	告警模块
阀值告警	重要(P2)	ECS虚拟化平台，libvirtd接口	libvirtd模块告警

可能原因

内核模块bug。

影响范围

导致无法通过libvirtd接口访问虚拟化相关组件，影响虚拟机的创建，迁移，重启以及通过libvirtd访问虚拟机的相关信息。

处理方法

执行ps aux | grep libvirtd | grep -v grep命令，查看libvirtd运行状态。

执行sudo service libvirtd restart命令，如果异常，尝试重启活启动libvirtd进程。

6.2 Alarm-02.200.0013.00001-kvm_acache_io_hang

检查acache组件是否有异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	ECS存储,acache	acache

可能原因

网络异常，物理机异常。

影响范围

vm iohang。

6.3 Alarm-02.200.0013.00002-check_kvm_io_hang

检查kvm集群的物理机上面有没有出现Iohang。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	ECS存储，磁盘io链路	kvm磁盘io链路

可能原因

网络异常，物理机异常。

影响范围

vm iohang。

处理方法

选择**tdc** > **river_server** > **pangu**。

6.4 Alarm-02.200.0013.00003-check_vm_io_hang

检查xen集群的物理机上面有没有出现Iohang。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	ECS存储，磁盘io链路	xen磁盘io链路

可能原因

网络异常，物理机异常。

影响范围

vm iohang。

处理方法

选择**tdc** > **river_server** > **pangu**。

6.5 Alarm-02.200.0013.00004-check_iorepeater

检查iorepeater。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	ECS存储，iorepeater	iorepeater

可能原因

网络异常，物理机异常。

影响范围

vm iohang。

处理方法

需要结合具体情况分析。

6.6 Alarm-01.200.0013.00005-kvm_qos_monitor

检查kvm的acache的各项qos。

告警信息

告警类型	告警级别	告警对象	告警模块
阀值告警	重要(P2)	ECS存储，acache	acache

可能原因

网络异常，物理机异常。

影响范围

vm iohang。

6.7 Alarm-01.200.0011.00002-xenwatch,xend,xenstore出现异常

用于xen虚拟化相关关键服务进程监控。监控xend，xenwatch，xenstore的运行状态。检测时间间隔为90秒。

告警信息

告警类型	告警级别	告警对象	告警模块
阀值告警	重要(P2)	ECS虚拟化平台，xen管理接口	xend模块告警

可能原因

内核模块bug。

影响范围

导致无法通过xen相关接口访问虚拟化相关组件，影响虚拟机的创建，迁移，重启以及通过xen访问虚拟机的相关信息。

处理方法

1. 登录相关物理机，执行/tmp/check_xen_process.log.xxxxxx命令，查看报错信息。
2. 执行ps aux | grep xen命令，查看当前xen相关进程的运行状态。

   如果xend进程不是3或5个，则可判定xend进程出现异常。
3. 执行sudo kill命令，停止当前进程。
4. 执行sudo service xend start命令，重启xend服务 。

   如果检测到xen相关进程异常，执行/proc/pid/stack sudo dmesg 命令，查看相关信息记录，请联系阿里工程师。

6.8 Alarm-01.200.0011.00003-xenbaked进程异常

检查xenbaked进程的运行状态，采集时间间隔为120秒。

告警信息

告警类型	告警级别	告警对象	告警模块
阀值告警	重要(P2)	ECS虚拟化平台，xenbaked进程。	xenbaked

可能原因

内核模块bug。

影响范围

xenbaked进程不可用。

处理方法

脚本自动处理，收到报警后应检查自动处理的结果。

6.9 Alarm-01.200.0011.00004-xenstore残留

处理xenstore残留，检查间隔时间为600秒。

告警信息

告警类型	告警级别	告警对象	告警模块
阀值告警	重要(P2)	ECS虚拟化平台，xenstore进程。	xenstore

可能原因

内核模块bug。

影响范围

xenstore残留积累。

处理方法

脚本自动处理，收到报警后应检查自动处理的结果。

6.10 Alarm-01.200.0011.00005-xenstore进程异常

监控xen环境中热迁移相关daemon(xenstore-networkd, xenstore-storaged)是否存在以及内存占用是否超标。

告警信息

告警类型	告警级别	告警对象	告警模块
阀值告警	重要(P2)	ECS虚拟化平台，xenstore进程。	xenstore

可能原因

内核模块bug。

影响范围

相关进程未启动会产生xen环境中管理虚拟机出现异常。

处理方法

脚本可配置自动修复，通过重启服务修复。

6.11 Alarm-01.200.0013.0006-磁盘resize失败异常

监控磁盘resize出现失败或异常。

告警信息

告警类型	告警级别	告警对象	告警模块
阀值告警	重要(P2)	ECS块存储	tdc

影响范围

单个device无法正常使用。

处理方法

具体需要查看日志定位。

6.12 Alarm-01.200.0014.00001-pync进程异常

监控NC上管控pync进程是否异常,检测间隔时间120s。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	ECS控制系统, pync进程	pync

影响范围

业务无法对VM进行重启/停止等操作。

处理方法

1. pync进程数不对告警：登录NC，执行`ps aux |grep pync-master`命令，确认进程是否不存在。

不存在执行sudo /etc/init.d/pync restart 命令恢复。

2. pync进程D告警：登录NC，执行ps aux |grep pync-master命令，确认进程是否有D状态的进程。

   若没有，走主动运维流程重启NC。

3. pync 的cpu、内存、句柄数告警：执行sudo /etc/init.d/pync reload命令恢复。

6.13 Alarm-01.001.0001.00001-数据库占用率过高

当维护工具检测（检测周期为5分钟）到数据库表空间占用率大于产生门限95%时，产生该告警。当数据库表空间占用率小于清除门限85%时，该告警会自动清除。

告警信息

告警类型	告警级别	告警对象	告警模块
阀值告警，事件告警	重要(P2)	具体到产品，包括客户可见的产品和内部依赖的公共组件。	• 硬件：硬件对应服务器中的CPU、硬盘、内存、风扇等。 • 软件对应天基的service role或者service。 • 库存告警。

可能原因

数据库表空间占用率的产生门限值设置不合理。 对于Oracle数据库，数据被导出或转储后，数据库表空间未及时释放。

影响范围

数据库表空间占用率过高可能会导致数据库相关操作失败，如告警等信息入库可能会失败。

该告警发生时，若不及时处理，可能会导致系统运行异常。

处理方法

1. 检查数据库表空间占用率告警的产生门限值设置是否合理。

   Y：请重新设置门限值。

   N：请转至步骤2。

2. 确认是否是Oracle数据库数据被导出或转储后，数据库表空间未及时释放。

   Y：以管理员用户连接数据库后，执行如下命令释放数据库表空间。

   alter table <table_name> enable row movement

   alter table <table_name> shrink space

   N：请转至步骤3。

3. 请收集上述告警处理过程中的信息，联系技术支持。

6.14 Alarm-01.200.0011.00003-xen "ballon"异常

检查xen虚拟化中的ballon机制进行内存分配产生的异常。检测时间间隔为600秒。

告警信息

告警类型	告警级别	告警对象	告警模块
阀值告警	重要(P2)	ECS虚拟化平台，xen中dom的内存管理机制。	balloon driver

可能原因

内核模块bug。

影响范围

导致物理机的内存泄露，domU的不可用。

处理方法

需要结合具体情况分析。

6.15 Alarm-02.200.0013.00007-检查是否有进程coredump

检查是否有进程coredump。

告警信息

表 6-1: 告警说明

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	ECS存储	ECS存储，river_server，pangu_chunkserver。

可能原因

进程异常退出。

影响范围

vm会有slow io。

处理方法

看进程是否恢复，如果没有恢复，可以尝试重启进程，如果coredump多，需要debug具体的原因。

6.16 Alarm-01.200.0013.00008-快照oss进程依赖

监控打快照功能的oss进程依赖kfc进程，如果oss进程在而kfc不存在则会影响打快照。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	ECS块存储	oss

可能原因

kfc进程异常退出，没有被自动拉起。

影响范围

NC上的VM打快照功能。

处理方法

如果报警则需要关闭掉oss_server(方法sudo /etc/init.d/supervisord stop）。

6.17 Alarm-01.200.0013.00009-acache存储设备io hang

监控存储设备acache层 io hang。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	ECS块存储	acache

可能原因

具体分析。

影响范围

ECS device io hang

处理方法

具体分析处理。

6.18 Alarm-01.200.0013.00010-acache错误日志

监控存储设备acache层异常日志。

告警信息

表 6-2: 告警说明

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	ECS存储	硬件SSD盘

可能原因

到达设计寿命。

影响范围

对用户层面无影响，底层pangu数据量减少。

处理方法

硬件生命周期管理。

6.19 Alarm-01.200.0013.00011-存储SSD盘寿命

监控硬件SSD盘的寿命健康度。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	ECS块存储	acache

可能原因

具体分析处理。

影响范围

ECS device io有异常。

处理方法

具体分析处理。

6.20 Alarm-01.200.0013.00012-acache存储设备延时

监控存储设备acache层的io latency。

告警信息

告警类型	告警级别	告警对象	告警模块
阀值告警	重要(P2)	ECS块存储	acache

可能原因

具体问题具体分析。

影响范围

ECS device io延时高。

处理方法

具体问题具体分析。

6.21 Alarm-01.200.0013.00013-磁盘空间使用量过高

监控关键分区/和/apsara的磁盘使用空间。

告警信息

告警类型	告警级别	告警对象	告警模块
阀值告警	重要(P2)	基础环境与系统	基础环境与系统

可能原因

程序打日志异常，没有轮转等。

影响范围

对ECS理论无影响。

处理方法

清理日志回收空间。

6.22 Alarm-01.200.0013.00014-检查是否有进程coredump

检查是否有进程coredump。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	ECS核心进程	ECS核心进程，xend，tdc，pync

可能原因

进程异常退出。

影响范围

VM会有异常，如io卡，管控异常等。

处理方法

看进程是否恢复，如果没有恢复，可以尝试重启进程，如果coredump多，需要debug具体的原因。

6.23 Alarm-02.200.0015.00014-logrotate日志轮转异常

如果 /var/lib/logrotate.status 超过一定天数未更新，说明日志轮转异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P4		

可能原因

lograte 配置错误，/var/lib/logrotate.status 写入异常数据。

影响范围

nc 日志无法轮转，可能异常磁盘打满。

处理方法

带参数 1 运行时发现异常会进行自动修复。

6.24 Alarm-01.200.0013.00015-系统负载高

系统负载高。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	基础环境与系统	基础环境与系统

可能原因

需要具体分析。

影响范围

ECS卡顿或异常。

处理方法

具体分析处理。

6.25 Alarm-01.200.0013.00016-系统盘制只读

监控系统盘sda只读。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	基础环境与系统	基础环境与系统

可能原因

系统盘磁盘故障。

影响范围

ECS状态变化出错。

处理方法

NC作宕机迁移。

6.26 Alarm-01.200.0013.00017-磁盘错误

监控硬件磁盘错误。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	基础环境与系统	基础环境与系统

可能原因

硬件错误。

影响范围

理论无影响，但是如果夯盘影响到底层服务进程则ECS状态变化出错。

处理方法

一般不用处理，如果夯盘则NC作宕机迁移。

6.27 Alarm-01.200.0013.00018-系统盘IO压力高

监控系统盘sda的io util压力。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	基础环境与系统	基础环境与系统

可能原因

具体分析。

影响范围

ECS卡顿或异常。

处理方法

具体分析处理。

6.28 Alarm-01.200.0015.00015-nc 内存使用异常

总内存 25% 或 NcMemUsed 超过总内存 95%。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P4		

可能原因

内存泄露或使用过多。

影响范围

可能出现 nc 内存不足，性能异常。

处理方法

具体分析处理。

6.29 Alarm-02.200.0015.00001-vswitchd 阻塞

vswitchd 阻塞导致大量 vswctl 调用卡住。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P3	虚拟化网络	

可能原因

vswitchd 阻塞。

影响范围

nc

处理方法

带参数 1 执行时出现告警可自动修复。

6.30 Alarm-02.200.0015.00002-mac 地址冲突

mac 地址冲突极有可能是 vport 残留导致的。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P3	虚拟化网络	

可能原因

vport 残留。

影响范围

冲突的 vm。

处理方法

找到并确认残留 vport 并删除 。

6.31 Alarm-02.200.0015.00003-安全组内存分配失败

刷新安全组时，内核内存不够分配失败产生该告警，当执行时带参数1时会自动修复。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	虚拟化网络	

可能原因

内存不足或内存碎片化严重导致无法分配连续内存。

影响范围

nc 上所有 vm 网络不通。

处理方法

带参数 1 执行时出现告警可自动修复 。

6.32 Alarm-02.200.0015.00004-安全攻击告警

VM 流量异常监控。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P4	虚拟化网络	

可能原因

流量异常或ddos攻击。

影响范围

nc 所有 vm 网络延时增大，NC 负载增大。

处理方法

根据告警输出找到对应VM迁移到独立NC。

6.33 Alarm-02.200.0015.00005-VPC VM 路由表满告警

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P4	虚拟化网络	

可能原因

具体分析。

影响范围

VM 到某些目的网络不通。

处理方法

具体分析处理。

6.34 Alarm-02.200.0015.00006-VPC ctk_proxy 配置告警

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P4	虚拟化网络	

说明：

以下2个配置不正确：

- net.ipv4.ctk_proxy.vpc_per_vm_tcp_conn_max=500000
- net.ipv4.ctk_proxy.vpc_per_vm_udp_conn_max=200000

可能原因

配置异常。

影响范围

nc

处理方法

具体分析处理。

6.35 Alarm-02.200.0015.00008-vswitch 配置告警

日志级别、网卡bond模式或模块参数不合要求，具体看监控输出。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P4	虚拟化网络	

可能原因

配置异常。

影响范围

nc

处理方法

具体分析处理。

6.36 Alarm-02.200.0015.00009-vpc 相关内核模块未加载告警

相关内核模块未加载或加载失败或被误卸载。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P4	虚拟化网络	

可能原因

VPC内核模块异常。

影响范围

nc

处理方法

具体分析处理。

6.37 Alarm-02.200.0015.00010-VPC vswitch 配置告警

vxlan 端口监听、mtu 检查等异常引起。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P4	虚拟化网络	

可能原因

配置异常。

影响范围

nc

处理方法

具体分析处理。

6.38 Alarm-02.200.0015.00011-vswitch 错误日志告警

vswitch 有错误日志输出。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P4	虚拟化网络	

可能原因

具体分析处理。

影响范围

具体分析处理。

处理方法

具体分析处理。

6.39 Alarm-02.200.0015.00012-havs 异常告警

havs监控项告警，具体要看告警内容。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值&事件告警	P4	虚拟化网络	

可能原因

具体分析处理。

影响范围

具体分析处理。

处理方法

具体分析处理。

6.40 Alarm-02.200.0015.00013-网卡异常告警

双网卡绑定状态监控。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P4	虚拟化网络	

可能原因

单网卡异常或lacp协商失败。

影响范围

nc

处理方法

网卡修复。

7 对象存储OSS

7.1 Alarm-02.305.0001.00001-check_nginx_port

当ocm所在机器的80端口无法连接时，会产生该告警， 当80端口可以连接时，该告警会自动清除。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	oss-ocm-server	oss-ocm-server. TEngine#

可能原因

- 机器坏了。
- 进程未启动。

影响范围

如果所有OCM都不能连接，OSS就不能正常工作。如果还有OCM能工作，可能不会影响OSS正常服务。

处理方法

1. 执行curl IP命令，检查是否有响应。
   - 如果有，表示误报。
   - 如果没有，请跳转至2。
2. 执行ps auxf|grep -e "tengine\|nginx"|grep -v grep命令，检查是否有nginx相关的进程。
   - 如果有，收集信息联系技术支持。
   - 如果没有，查看天基没有启动tengine或者nginx进程的原因，查看*apsara/apache/logs/*路径下是否有当天日志，收集信息联系技术支持。

7.2 Alarm-02.305.0001.00002-check_ocm_server_process_fix

当ocm_server进程重启的时候，会产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	oss-ocm-server	oss-ocm-server.OcmServer#

可能原因

- 资源不够。
- 配置不对导致重启程序bug。
- 升级后，重启了进程忘记关报警。

影响范围

OCM不能服务可能会影响正常的OSS读写。

处理方法

1. 执行ps auxf|grep ocm_server|grep -v grep命令，查看日志，找到ocm_server启动的进程所在的目录。
2. 进入目录，查看apsara_log_conf.json，查找日志打印的位置。
3. 收集相关日志和配置文件ocm_conf.json。
4. 收集本机的系统日志dmsg。
5. 联系技术支持。

7.3 Alarm-02.305.0001.00003-oss_check_net_error_drop

当网卡有丢包的时候，会产生该告警，当不丢包时会恢复。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P4	oss-ocm-server	oss-ocm-server.TEngine#

可能原因

- 网卡不好。

- 网络有问题。

影响范围

OCM不能服务可能会影响正常的OSS读写。

处理方法

需要配合OSS整体服务来看，如果OSS服务正常，不影响OSS的正确请求可暂时不处理。

检查网卡流量是否超过上限。

- 如果是，表示正常，可能需要扩容，以减少网络的流量。
- 如果否，联系硬件工程师，查看网卡是否正常。

7.4 Alarm-02.305.0001.00004-check_tengine_ssl_cert_expire_stat

检查tengine的ssl证书文件是否快要过期，证书有效期小于30天则报警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	oss-ocm-server	oss-ocm-server.TEngine#

可能原因

有证书，且证书过期。

处理方法

1. 申请新的证书。
2. 替换证书。

专有云一般情况下没有证书。

7.5 Alarm-02.305.0001.00005-check_2ethstatus_oss

检查网卡是否工作正常，使用自己的脚本可以灵活指定需要的网络监测规则，比如10000M网卡，包括是否在正常设置的speed，是否双工。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	oss-ocm-server	oss-ocm-server.TEngine#

可能原因

- 网卡坏了。
- 配置不对。

处理方法

联系驻场工程师替换网卡。

7.6 Alarm-02.305.0001.00006-check_nginx_process

当nginx进程重启的时候，会产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	oss-ocm-server	oss-ocm-server.TEngine#

可能原因

- 资源不够。
- 配置不对导致重启程序bug。
- 升级后，重启了进程忘记关报警。

影响范围

OCM不能服务可能会影响正常的OSS读写。

处理方法

1. 查看*/apsara/apache/logs*目录access log中是否正常。

2. 执行curl http://IP地址/systermoperation/checkocmstatus -i命令，查看是否为200，OSS服务是否恢复正常。
   - 如果正常，记录进程重启时间，如果不影响服务，可以暂时不用处理。
   - 如果不正常，服务不可用，联系技术支持。

7.7 Alarm-02.305.0001.00007-check_tsar_nginx

检查tsar模块配置是否正确. 检查tsar是否采集nginx的相关数据。如果tsar未采集nginx的QPS，则无法获取应用的QPS情况。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	oss-ocm-server	oss-ocm-server.TEngine#

可能原因

没有进行相关配置。

影响范围

影响后续调查问题。

处理方法

开启 tsar 的 nginx 采集功能。

1. 将*/etc/tsar/tsar.conf*文件中**mod_nginx off** 修改为**mod_nginx on**。
2. 在**output_studio_mod**的末尾加上**mod_nginx**。
3. 对 nginx 进行设置，添加如下配置至默认主机：

```
location /nginx_status {
stub_status on;
access_log off;
allow 127.0.0.1;
deny all;
}
```

4. 重新载入，设置生效后等候片刻。

   tsar 的采集间隔是5分钟，修改crontab文件，即可在 tsar 输出中看到 nginx 的相关数据，对于 tengine 的设置与此相同。
5. 如果采集不正常，检查http://localhost/nginx_status。

执行tsar --nginx 命令，查看是否有正确内容输出。

7.8 Alarm-02.305.0001.00008-check_toa_module

检测toa模块是否加载到内存，toa模块是为了让后端的realserver能够看到真实的clientip而不是lvs的dip。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	oss-ocm-server	oss-ocm-server.TEngine#

可能原因

没有进行相关配置。

影响范围

会影响后续调查问题。

处理方法

安装toa模块 slb toa：注意要跟内核版本匹配，下面的例子是1089内核。

sudo yum install slb-vtoa-ali1089 -b current -y

sudo /sbin/modprobe slb_vtoa

7.9 Alarm-02.305.0001.00009-check_kernel_param

检查内核参数是否符合需求，这些内核参数是OSS在运行过程中的一些经验积累。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	oss-ocm-server	oss-ocm-server.TEngine#

可能原因

没有进行相关配置。

影响范围

OCM不能服务可能会影响正常的OSS读写。

处理方法

执行如下脚本：

```
oss_init_kernel_param.sh
alios7_judge(){
local alios7_flag=false
release_output=`cat /etc/redhat-release 2>/dev/null`
echo "${release_output}"|grep -i "release 7" 1>/dev/null 2>&1 && alios7_flag=true
echo ${alios7_flag}
}
alios7_flag=`alios7_judge`
if [ "x${alios7_flag}" == "xtrue" ];then
echo "this is a alios7 machine,no need to init_kernel_param"
exit 0
fi
uuid=`cat /proc/sys/kernel/random/uuid`
date_str=`date +%Y%m%d%H%M`
working_dir="/tmp/kuorong_tmp/${date_str}/${uuid}"
mkdir -p ${working_dir}
echo "conf copy working dir is ${working_dir}"
#随机端口范围指定原因参考：http://wiki.aliyun-inc.com/projects/apsara/wiki/ApsaraPort ，所以最小从32768开始。
cat << EOF > ${working_dir}/kernel_parameter_output
#ADD BY OSS_INIT_KERNEL_PARAM BEGIN
vm.max_map_count = 8388608
net.ipv4.tcp_rmem = 4096 87380 4194304
net.ipv4.tcp_wmem = 4096 16384 4194304
net.core.wmem_default = 8388608
net.core.rmem_default = 8388608
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.core.netdev_max_backlog = 204800
net.core.somaxconn = 204800
net.ipv4.tcp_max_orphans = 3276800
net.ipv4.tcp_max_syn_backlog = 204800
net.ipv4.tcp_tw_recycle = 0
net.ipv4.tcp_tw_reuse = 1
net.ipv4.tcp_tw_timeout = 15
net.ipv4.tcp_fin_timeout = 15
net.ipv4.ip_local_port_range = 32768 61000
net.ipv4.tcp_syncookies = 0
#ADD BY OSS_INIT_KERNEL_PARAM END
EOF
cat /etc/sysctl.conf |grep "ADD BY OSS_INIT_KERNEL_PARAM" 2>/dev/null
init_kernel_param_flag=$?
if [ "x${init_kernel_param_flag}" == "x0" ];then
 #随机端口范围指定原因参考：http://wiki.aliyun-inc.com/projects/apsara/wiki/ApsaraPort ，所以最小从32768开始
cat /etc/sysctl.conf |grep "net.ipv4.ip_local_port_range = 32768 61000" > /dev/null
port_range_fix_flag=$?
 if [ "x${port_range_fix_flag}" != "x0" ];then
 sudo sed -i 's@net.ipv4.ip_local_port_range = .*@net.ipv4.ip_local_port_range = 32768 61000@' /etc/sysctl.conf
 sudo /sbin/sysctl -p
 echo "change port range to 32768 61000 done"
 fi
cat /etc/sysctl.conf |grep "net.ipv4.tcp_tw_timeout = 15"
tw_timeout_flag=$?
 if [ "x${tw_timeout_flag}" != "x0" ];then
```

```
sudo sed -i '/net.ipv4.tcp_tw_reuse = 1/a\net.ipv4.tcp_tw_timeout = 15' /etc/sysctl.conf > /dev/
null
sudo /sbin/sysctl -p
echo "add tw timeout to 15 done"
fi
exit 0
fi
sudo bash -c "sudo cat ${working_dir}/kernel_parameter_output >> /etc/sysctl.conf" || { echo "
add kernel param failed";exit 12; }
echo "init kernel param..."
sudo /sbin/sysctl -p #默认参数中有net.nf_conntrack_max会导致sysctl -p报错，所以我们不对其
做容错处理
```

7.10 Alarm-01.305.0001.00010-OCM_ACCESSLOG_WEBSERVER

OCM前端机使用的模板，目前只有对于5xx的监控，可以根据ocm需求定制。60秒采集一次。检查前端机的5XX错误比例，${code_5xxRa}>2&&${code_5xx}>30 。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	oss-ocm-server	oss-ocm-server.TEngine#

可能原因

- 请求失败。
- 压力过大。
- 数据库异常。

处理方法

1. 找到access log，一般在/apsara/apache/logs/，假如今天是20170301，则为 access_log.20170301。
2. 执行grep InternalError access_log.20170301命令，找到32位的RequestID。
3. 通过request id收集相关日志发送给技术支持。

7.11 Alarm-01.305.0002.00001-OSS_ACCESSLOG_WEBSERVER_ALL

OCM前端机使用的模板，目前只有对于5xx的监控，可以根据ocm需求定制。60秒采集一次。检查前端机的5XX错误比例，${code_5xxRa}>2&&${code_5xx}>30 。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	oss-server	oss-server.TEngine#

可能原因

- 请求失败
- 压力过大
- 数据库异常

处理方法

1. 找到access log，一般在*/apsara/apache/logs/*，假如今天是20170301，access_log.20170301。
2. 执行grep InternalError access_log.20170301命令，找到32位的RequestId。
3. 通过request id收集相关日志发送给技术支持。

7.12 Alarm-02.305.0002.00003-oss_check_net_error_drop

当网卡有丢包的时候，会产生该告警，当不丢包时会恢复。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P4	oss-server	oss-server.TEngine#

可能原因

- 网卡不好。
- 网络有问题。

影响范围

影响正常的OSS读写。

处理方法

需要配合OSS整体服务查看，如果OSS服务正常不影响，OSS的正确请求可暂时不处理。

检查网卡流量是否超过上限。

- 如果超过上限，表示正常，可能需要扩容，以减少网络的流量。
- 如果没有超过，联系硬件工程师，查看网卡是否正常。

7.13 Alarm-02.305.0002.00004-check_tengine_ssl_cert_expire_stat

检查tengine的ssl证书文件是否快要过期，证书有效期小于30天则报警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	oss-server	oss-server.TEngine#

可能原因

有证书，且证书过期。

处理方法

- 申请新的证书。
- 替换证书。

专有云一般情况下都没有证书。

7.14 Alarm-02.305.0002.00005-check_2ethstatus_oss

检查网卡是否工作正常，使用自己的脚本可以灵活指定需要的网络监测规则，比如10000M网卡，包括是否在正常设置的speed，是否双工。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	oss-server	oss-server.TEngine#

可能原因

- 网卡坏了。
- 配置不对。

处理方法

联系驻场工程师替换网卡。

7.15 Alarm-02.305.0002.00006-check_nginx_process

当nginx进程重启的时候，会产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	oss-server	oss-server.TEngine#

可能原因

- 配置不对，导致重启。
- 程序bug，导致重启。
- 升级重启进程，忘记关报警。

影响范围

影响正常的OSS读写。

处理方法

1. 查看*/apsara/apache/logs*路径下access log日志是否正常。
2. 执行curl http://IP地址/systermoperation/checkossstatus -i 命令，查看OSS服务是否恢复，是否返回200。
   - 如果恢复，记录进程重启时间，如果不影响服务，可以暂时不用处理。
   - 如果没有恢复，服务不可用，联系技术支持。

7.16 Alarm-02.305.0002.00007-check_tsar_nginx

检查tsar模块配置是否正确. 检查tsar是否采集nginx的相关数据。如果tsar未采集nginx的QPS，这样一方面无法获取应用的QPS情况。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	oss-server	oss-server.TEngine#

可能原因

没有进行相关配置。

影响范围

影响后续调查问题。

处理方法

开启 tsar 的 nginx 采集功能。

1. 将*/etc/tsar/tsar.conf*文件中**mod_nginx off**修改为**mod_nginx on**。
2. 在**output_studio_mod**的末尾加上**mod_nginx**。
3. 对 nginx 进行设置，添加如下配置至默认主机：

```
location /nginx_status {
stub_status on;
access_log off;
allow 127.0.0.1;
deny all;
}
```

4. 重新载入设置生效后，等候片刻，即可在 tsar 输出中看到 nginx 的相关数据，对于 tengine 的设置与此相同。

   tsar 的采集间隔是5分钟，可以在crontab中修改。
5. 如果采集不正常，检查 http://localhost/nginx_status。
6. 执行tsar --nginx命令，查看是否有正确内容输出。

7.17 Alarm-02.305.0002.00008-check_toa_module

检测toa模块是否加载到内存，toa模块是为了让后端的realserver能够看到真实的clientip而不是lvs的dip。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	oss-server	oss-server.TEngine#

可能原因

没有进行相关配置。

影响范围

影响后续调查问题。

处理方法

安装toa模块&& slb toa：注意要跟内核版本匹配，下面的例子是1089内核。

sudo yum install slb-vtoa-ali1089 -b current -y

sudo /sbin/modprobe slb_vtoa

7.18 Alarm-02.305.0002.00009-check_kernel_param

检查内核参数是否符合需求，这些内核参数是OSS在运行过程中的一些经验积累。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	oss-server	oss-server.TEngine#

可能原因

没有进行相关配置。

影响范围

大压力下会影响正常的OSS读写。

处理方法

执行如下脚本：

```
oss_init_kernel_param.sh
alios7_judge(){
local alios7_flag=false
release_output=`cat /etc/redhat-release 2>/dev/null`
echo "${release_output}"|grep -i "release 7" 1>/dev/null 2>&1 && alios7_flag=true
echo ${alios7_flag}
}
alios7_flag=`alios7_judge`
if [ "x${alios7_flag}" == "xtrue" ];then
echo "this is a alios7 machine,no need to init_kernel_param"
exit 0
fi
uuid=`cat /proc/sys/kernel/random/uuid`
date_str=`date +%Y%m%d%H%M`
working_dir="/tmp/kuorong_tmp/${date_str}/${uuid}"
mkdir -p ${working_dir}
echo "conf copy working dir is ${working_dir}"
#随机端口范围指定原因参考：http://wiki.aliyun-inc.com/projects/apsara/wiki/ApsaraPort ，所以最小从32768开始
```

```
cat << EOF > ${working_dir}/kernel_parameter_output
#ADD BY OSS_INIT_KERNEL_PARAM BEGIN
vm.max_map_count = 8388608
net.ipv4.tcp_rmem = 4096 87380 4194304
net.ipv4.tcp_wmem = 4096 16384 4194304
net.core.wmem_default = 8388608
net.core.rmem_default = 8388608
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.core.netdev_max_backlog = 204800
net.core.somaxconn = 204800
net.ipv4.tcp_max_orphans = 3276800
net.ipv4.tcp_max_syn_backlog = 204800
net.ipv4.tcp_tw_recycle = 0
net.ipv4.tcp_tw_reuse = 1
net.ipv4.tcp_tw_timeout = 15
net.ipv4.tcp_fin_timeout = 15
net.ipv4.ip_local_port_range = 32768 61000
net.ipv4.tcp_syncookies = 0
#ADD BY OSS_INIT_KERNEL_PARAM END
EOF
cat /etc/sysctl.conf |grep "ADD BY OSS_INIT_KERNEL_PARAM" 2>/dev/null
init_kernel_param_flag=$?
if [ "x${init_kernel_param_flag}" == "x0" ];then
#随机端口范围指定原因参考：http://wiki.aliyun-inc.com/projects/apsara/wiki/ApsaraPort ，所以最小从32768开始
cat /etc/sysctl.conf |grep "net.ipv4.ip_local_port_range = 32768 61000" > /dev/null
port_range_fix_flag=$?
if [ "x${port_range_fix_flag}" != "x0" ];then
sudo sed -i 's@net.ipv4.ip_local_port_range = .*@net.ipv4.ip_local_port_range = 32768 61000@' /etc/sysctl.conf
sudo /sbin/sysctl -p
echo "change port range to 32768 61000 done"
fi
cat /etc/sysctl.conf |grep "net.ipv4.tcp_tw_timeout = 15"
tw_timeout_flag=$?
if [ "x${tw_timeout_flag}" != "x0" ];then
sudo sed -i '/net.ipv4.tcp_tw_reuse = 1/a\net.ipv4.tcp_tw_timeout = 15' /etc/sysctl.conf > /dev/null
sudo /sbin/sysctl -p
echo "add tw timeout to 15 done"
fi
exit 0
fi
sudo bash -c "sudo cat ${working_dir}/kernel_parameter_output >> /etc/sysctl.conf" || { echo "add kernel param failed";exit 12; }
echo "init kernel param..."
```

```
sudo /sbin/sysctl -p #默认参数中有net.nf_conntrack_max会导致sysctl -p报错，所以我们不对其做容错处理
```

7.19 Alarm-01.305.0002.00010-check_ossserver_openfilelimit_all

OSS前端机使用的监控 ，检查oss_server已经打开的fd个数和最大限制的limit个数。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值报警	P2	oss-server	oss-server.OssServer #

可能原因

没有进行相关配置。

影响范围

大压力下会影响正常的OSS读写。

处理方法

- 当fd个数大于20000时，需要重启oss_server进程。
- 当最大可以打开的fd个数小于1024时，需要查看启动的环境变量设置的fd最大是多少。

  工作时间不发送短信，非工作时间发送短信。

  - warning：oss_server fd限制为1024,需要修改bash环境变量。
  - critical：oss_server已经打开的fd>20000,需要重启进程。

7.20 Alarm-02.305.0002.00011-check_oss_server_process_restart_fix

当oss_server进程重启的时候，会产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	oss-server	oss-server.OssServer #

可能原因

- 资源不够。
- 配置不对，导致重启。
- 程序bug，导致重启。
- 升级重启进程，忘记关报警。

影响范围

影响正常的OSS读写。

处理方法

1. 执行ps auxf|grep oss_server|grep -v grep命令，查看日志，找到oss_server启动的进程所在的目录。
2. 进入目录，查看*apsara_log_conf.json*文件，获取日志打印的位置。
3. 收集相关日志和配置文件ocm_conf.json。
4. 收集本机的系统日志dmsg。
5. 联系技术支持。

7.21 Alarm-02.305.0002.00012-check_ossserver_mem

采集指定进程名的虚机内存，物理内存，当前状态大于45%报警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	oss-server	oss-server.OssServer#

可能原因

内存没有控制好，流量过大。

影响范围

影响正常的OSS读写。

处理方法

收集配置文件，查看是否设置了*"DataCacheCapacity":"8589934592"*。

- 如果已经设置，查看是否设置为本机内存的30%以下。

如果是，可能发生了内存泄露，联系技术支持，收集相关信息后，重启进程。

- 如果没有设置，设置为本机内存30%以下，重启进程。

7.22 Alarm-02.305.0002.00013-check_nginx_port

当oss所在机器的80端口无法连接时，会产生该告警. 当80端口可以连接时，该告警会自动清除。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	oss-server	oss-server.OssServer #

可能原因

- 机器损坏。
- 进程未启动。

影响范围

- 如果所有OSS都不能连接，OSS就不能正常工作。
- 如果还有OSS能工作，可能不会影响OSS正常服务。

处理方法

1. 执行curl IP命令，检查是否有响应。
   - 如果有响应，表示误报。
   - 如果没响应，请跳转至2。
2. 执行ps auxf|grep -e "tengine\|nginx"|grep -v grep命令，检查是否有nginx相关的进程。
   - 如果有，收集信息联系技术支持。
   - 如果没有，查看天基没有启动tengine或者nginx进程的原因，查看*/apsara/apache/logs/*目录下是否有当天的日志，收集信息联系技术支持。

7.23 Alarm-02.305.0002.00014-working_online_me_alarm

检查机器me不正常的时候，机器是否是working online，或者机器是否是天基API有问题。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	oss-server	oss-server.OssServer #

可能原因

没有安装me或者是天基的基础组件。

影响范围

影响后续调查问题。

处理方法

联系技术支持。

7.24 Alarm-02.305.0003.00001-check_quota_client

OSS产品系列的quota check，check quota 同步情况，没有同步会报警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	oss-server	oss-server.OssServer #

可能原因

- 没有日志。
- 日志所在磁盘损坏。

影响范围

影响计量数据。

处理方法

1. 执行df -lh命令，查看access log所在磁盘是否满了。
   - 如果满了，清除日志，保留空间。

日志文件一般在*/apsara/apache/logs*路径下。

- 如果没满，请跳转至*2*。

2. 在磁盘上创建一个临时文件，查看是否能够创建成功。
   - 如果能，确认磁盘没有问题。

     收集quota agent日志所在目录 logs下的所有日志，联系技术支持工程师。
   - 如果不能，磁盘坏了，联系硬件工程师，维修磁盘。

7.25 Alarm-02.305.0003.00002-_quota_agent_process_fix

当quota agent进程重启的时候，产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	oss-server	oss-server.OssServer #

可能原因

- 程序bug，导致重启。
- 升级重启进程，忘记关报警。

影响范围

对OSS应用几乎无影响，可能会影响计量数据。

处理方法

1. 执行ps auxf|grep quota_agent|grep -v grep命令，查看日志，找到启动的进程所在的目录。
2. 进入目录，在*apsara_log_conf.json*文件中，查看日志打印的位置。
3. 收集相关日志和配置文件。
4. 收集本机的系统日志dmsg。
5. 联系技术支持。

7.26 Alarm-02.305.0003.00003-check_quota_agent_mem

采集指定进程名的虚机内存和 物理内存，当前状态大于10GB报警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	oss-server	oss-server.OssServer#

可能原因

没有控制好内存。

影响范围

对OSS应用几乎无影响，可能会影响计量数据。

处理方法

1. 执行ps auxf|grep quota_agent|grep -v grep命令，查看日志，找到启动进程所在的目录。
2. 进入目录，查看*apsara_log_conf.json*文件下日志打印的位置。
3. 收集相关日志和配置文件。
4. 收集本机的系统日志dmsg。
5. 联系技术支持。

7.27 Alarm-02.305.0004.00001-check_quota_data_to_sls

检查quota数据推送到云监控是否正常，不正常就报警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	oss-quota-master	oss-quota-master.QuotaMaster#

可能原因

连接到SLS网络不通。

影响范围

对OSS应用几乎无影响，可能会影响计量数据。

处理方法

1. 执行ps auxf|grep quotamaster_main| grep -v grep命令，查看日志，找到启动进程所在的目录。
2. 进入目录，在*apsara_log_conf.json*文件中查看日志打印的位置。
3. 收集相关日志和配置文件。
4. 收集本机的系统日志dmsg。
5. 联系技术支持。

7.28 Alarm-02.305.0004.00002-check_oss_quota_master

当quotamaster_main进程重启的时候，会产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	oss-quota-master	oss-quota-master. QuotaMaster#

可能原因

- 程序bug，导致重启。
- 升级重启了进程，忘记关报警。

影响范围

对OSS应用几乎无影响，可能会影响计量数据。

处理方法

1. 执行ps auxf|grep quotamaster_main| grep -v grep命令，查看日志，找到启动进程所在的目录。
2. 进入目录，在*apsara_log_conf.json*文件下，查看日志打印的位置。
3. 收集相关日志和配置文件。
4. 收集本机的系统日志dmsg。
5. 联系技术支持。

7.29 Alarm-02.305.0004.00003-check_oss_quota_master_syncpoint

oss产品系列的quota check，check quota 同步情况，没有同步会报警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	oss-quota-master	oss-quota-master.QuotaMaster#

可能原因

- quota service的数据没有收集成功。
- 推送到OMS失败，可能是OMS有问题，也有可能是到OMS的网络有问题。

影响范围

影响计量数据。

处理方法

1. 执行**ps auxf|grep quotamaster_main| grep -v grep**命令，查看日志，找到启动进程所在的目录。
2. 进入目录，在apsara_log_conf.json文件下，查看日志打印的位置。
3. 收集相关日志和配置文件。
4. 收集本机的系统日志dmsg。
5. 联系技术支持。

8 表格存储TableStore

8.1 Alarm-02.310.0010.00020-表格存储sqlonline_master进程发生重启

当sqlonline_master发生重启时，产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	表格存储	TableStore

可能原因

- sqlonline_master所在机器有硬件故障，导致重启。
- 触发sqlonline_master未知bug，导致重启。

影响范围

- 在sqlonline_master重启期间删建表以及修改、获取表meta操作会失败。
- 在sqlonline_master重启期间，数据读写可能出现失败。

处理方法

1. 登录到sqlonline_master所在机器：在OTS ag上执行r wl命令，找到sys/sqlonline-OTS对应replyAddress，登录到对应的机器。
2. 执行cd /apsara/tubo/TempRoot/sys/sqlonline-OTS/sqlonline/命令，打开sqlonline_master所在的目录。
3. 收集该目录下的所有日志，联系技术支持。

8.2 Alarm-02.310.0100.10101-表格存储前端机出现5XX报警

当表格存储前端机检测，检测周期为1分钟，到5xx错误请求数超过50时，产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	表格存储	TableStore

可能原因

常见的5xx错误原因：

- 分区在自动分裂过程中会出现短时间服务不可用。
- 用户瞬时压力过大超过分区性能极限或机器性能极限时，出现服务忙错误。

影响范围

用户访问出错，如果持续发生该告警，说明系统出现异常，需要调查原因。

处理方法

1. 根据报警信息，登录到对应的机器上。
2. 执行cd /apsara/ots_server/logs命令，打开ots_server日志所在目录。
3. 收集该目录下的所有日志，联系技术支持。

8.3 Alarm-02.310.0004.00001-表格存储前端机http连接数超限

当表格存储前端机检测到http连接数超过10000时，产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	表格存储	TableStore

可能原因

ots_server机器压力过大。

影响范围

ots_server不稳定，访问会出现超时、出错等问题。

处理方法

对ots_server机器组进行扩容。

8.4 Alarm-02.310.0010.00001-表格存储ots_server进程发生重启

当ots_server发生重启时，产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	表格存储	TableStore

可能原因

ots_server由于未知bug导致crash。

影响范围

访问该前端机的部分请求失败。

处理方法

1. 根据报警信息登录到对应的机器。
2. 执行cd /apsara/ots_server/logs命令，打开ots_server日志所在目录。
3. 收集该目录下的所有日志，联系技术支持。

8.5 Alarm-02.310.0010.00010-表格存储sqlonline_worker进程发生重启

当sqlonline_worker发生重启时，产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	表格存储	TableStore

可能原因

- sqlonline_worker所在机器有硬件故障，导致重启。
- 触发sqlonline_worker未知bug，导致重启。

影响范围

访问到该sqlonline_worker上分区的部分请求失败。

处理方法

1. 根据报警信息登录到对应机器上。
2. 执行ps aux | grep sqlonline_worker命令，查看sqlonline_worker进程。
3. 执行如下命令，打开sqlonline_worker所在的目录。

   cd /apsara/tubo/TempRoot/sys/sqlonline-OTS/SqlWorkerRole@*/sqlonline/
4. 收集该目录下的所有日志，联系技术支持。

8.6 Alarm-02.310.0020.00020-sqlonline_master coredump

当sqlonline_master发生coredump时，产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	表格存储	TableStore

可能原因

sqlonline_master由于未知原因导致coredump。

影响范围

- 在sqlonline_master重启期间，删建表以及修改、获取表meta操作会失败。
- 在sqlonline_master重启期间，数据读写可能出现失败。

处理方法

1. 登录到sqlonline_master所在机器。
2. 在OTS ag上执行r wl命令，找到*sys/sqlonline-OTS*对应replyAddress，登录到对应的机器。
3. 执行如下命令，打开sqlonline_master所在的目录，找到sqlonline_master binary。

   cd /apsara/tubo/TempRoot/sys/sqlonline-OTS/sqlonline/
4. 找到sqlonline_master生成的core文件。
5. 请收集sqlonline_master binary和对应的core文件，联系技术支持。

8.7 Alarm-02.310.0020.00010-sqlonline_worker coredump

当sqlonline_worker发生coredump时，产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	表格存储	TableStore

可能原因

sqlonline_worker由于未知原因导致coredump。

影响范围

访问到该sqlonline_worker上分区的部分请求失败。

处理方法

1. 根据报警信息登录到到对应机器上。
2. 执行ps aux | grep sqlonline_worker命令，查看sqlonline_worker进程。
3. 执行如下命令，打开sqlonline_worker所在的目录并找到sqlonline_worker binary。

   cd /apsara/tubo/TempRoot/sys/sqlonline-OTS/SqlWorkerRole@*/sqlonline/
4. 找到sqlonline_worker生成的core文件。
5. 请收集sqlonline_worker binary和对应的core文件，联系技术支持。

8.8 Alarm-02.310.0010.00002-ots_tengine进程发生重启

当ots_tengine进程发生重启时，发生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	表格存储	TableStore

可能原因

ots_tengine由于未知bug导致crash。

影响范围

访问该前端机的部分请求失败。

处理方法

1. 根据报警信息登录到对应的机器上。
2. 执行cd /apsara/ots_tengine/logs命令，打开ots_tengine日志所在目录。
3. 收集该目录下的所有日志，联系技术支持。

8.9 Alarm-02.310.0010.00004-表格存储replication_server进程发生重启

当replication_server发生重启时，产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	表格存储	TableStore

可能原因

- replication_server所在机器有硬件故障，导致重启。
- 触发replication_server未知bug，导致重启。

影响范围

数据同步到备集群可能出现不及时。

处理方法

1. 根据报警信息登录到对应的机器上。
2. 执行如下命令，打开replication_server日志所在目录。

   cd /apsara/sqlonline_replication_server/logs
3. 收集该目录下的所有日志，联系技术支持。

8.10 Alarm-02.310.0100.10000-表格存储出现warning日志

当表格存储出现warning日志时，发生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	表格存储	TableStore

可能原因

- worker_alert_log失败，sqlonline_worker出现alert日志。
- check_replicate_status失败，双集群数据同步速度过慢。
- ots_check_cgroup失败，机器或相关进程cpu使用超限。
- check_ots_server_health失败，有ots_server机器无法服务。
- ots_server_alert失败，ots_server出现alert日志。
- replication_server_alert_log失败，sqlonline_replication_server出现alert日志。
- check_sqlonline_master_process失败，sqlonline_master发生进程重启。
- master_alert_log失败，sqlonline_master出现alert日志。
- check_sqlservice失败，部分机器的sqlonline_worker进程没有启动。

影响范围

表格存储服务不稳定。

处理方法

- worker_alert_log失败，登录到对应机器，并打开sqlonline_worker目录，查看sqlonline_alert.LOG日志，联系技术支持。
- check_replicate_status失败，联系技术支持。
- ots_check_cgroup失败，联系技术支持。
- check_ots_server_health失败，登录到对应机器上，查看*/apsara/OTSAdmin/alert/warning/monitor_result*.log*文件，找到check_ots_server_health失败的机器并登录。

  查看ots_server、ots_tengine进程是否存在，*/var/www/html/ots_server.heartbeat*是否存在。
- ots_server_alert失败，登录到对应机器，并打开*/apsara/ots_server/logs*目录，查看sqlonline_alert.LOG日志，联系技术支持。
- replication_server_alert_log失败，登录到对应机器，并打开*/apsara/sqlonline_replication_server/logs*目录，查看sqlonline_alert.LOG日志，联系技术支持。
- check_sqlonline_master_process失败，登录到对应机器上，并打开sqlonline_master目录，查看sqlonline_alert.LOG日志，联系技术支持。
- master_alert_log失败，登录到对应机器上，并打开sqlonline_master目录，查看sqlonline_alert.LOG日志，联系技术支持。
- check_sqlservice失败，登录到对应机器上，查看*/apsara/OTSAdmin/alert/warning/monitor_result*.log*，找到check_sqlservice失败的日志，联系技术支持。

8.11 Alarm-02.310.0100.20000-表格存储出现critical日志

当表格存储出现critical日志时，发生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	表格存储	TableStore

可能原因

- check_cpls失败，partition load不起来。
- worker_alert_log失败，sqlonline_worker出现alert日志。
- check_replicate_status失败，双集群数据同步速度过慢。
- ots_check_cgroup失败，机器或相关进程cpu使用超限。
- check_ots_server_health失败，有ots_server机器无法服务。
- ots_server_alert失败，ots_server出现alert日志。
- replication_server_alert_log失败，sqlonline_replication_server出现alert日志。
- check_sqlonline_master_process失败，sqlonline_master发生进程重启。
- master_alert_log失败，sqlonline_master出现alert日志。
- check_sqlservice失败，部分机器的sqlonline_worker进程没有启动。

影响范围

表格存储服务出现严重异常，需要及时处理，否则服务受到严重影响。

处理方法

- check_cpls失败，在ots ag上执行`sql cpls`，并挑选一个partition登录到对应的worker上。

  打开sqlonline_worker所在目录，收集*sqlonline_alert.LOG**和*sqlonline_error.LOG**，联系技术支持。
- worker_alert_log失败，登录到对应机器，并打开sqlonline_worker目录，查看*sqlonline_alert.LOG*日志，联系技术支持。
- check_replicate_status失败，联系技术支持。
- ots_check_cgroup失败，联系技术支持。
- check_ots_server_health失败，登录到对应机器上，查看*/apsara/OTSAdmin/alert/warning/monitor_result*.log*日志，找到check_ots_server_health失败的机器并登录。

查看ots_server、ots_tengine进程是否存在，*/var/www/html/ots_server.heartbeat*是否存在。

- ots_server_alert失败，登录到对应机器，打开*/apsara/ots_server/logs*目录，查看*sqlonline_alert.LOG*日志，联系技术支持。
- replication_server_alert_log失败，登录到对应机器，打开*/apsara/sqlonline_replication_server/logs*目录，查看*sqlonline_alert.LOG*日志，联系技术支持。
- check_sqlonline_master_process失败，登录到对应机器上，打开*sqlonline_master*目录，查看*sqlonline_alert.LOG*日志，联系技术支持。
- master_alert_log失败，登录到对应机器上，打开*sqlonline_master*目录，查看*sqlonline_alert.LOG*日志，联系技术支持。
- check_sqlservice失败，登录到对应机器上，查看*/apsara/OTSAdmin/alert/warning/monitor_result*.log*日志，找到check_sqlservice失败的日志，联系技术支持。

8.12 Alarm-02.310.0001.00001-表格存储前端机cpu过高

当表格存储前端机所在cpu使用过高时，发生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警		表格存储	TableStore

可能原因

前端机所在机器压力过大。

影响范围

ots_server不稳定，长时间会出现访问超时、出错等问题。

处理方法

对ots_server机器组进行扩容。

8.13 Alarm-02.310.0001.00002-表格存储后端机cpu过高

当表格存储后端机所在cpu使用过高时，发生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	表格存储	TableStore

可能原因

后端机所在机器压力过大。

影响范围

sqlonline_worker服务不稳定，长时间会出现访问超时、出错等问题。

处理方法

查看所有ots后端机的CPU使用情况，如果所有机器都CPU使用率很高，需要对sqlonline_worker机器组进行扩容，如果不是请联系技术支持。

8.14 Alarm-02.310.0200.00001-PostCheck检查不通过

当对应的ServerRole运行异常时，发生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警		表格存储	TableStore

可能原因

ServerRole异常。

影响范围

TableStore无法正常工作。

处理方法

1. 通过天基查看对应的SR的PostCheck检查信息，如果信息中没有详细的错误信息，那么需要参见2。
2. 登录报错的机器，查看monitor的运行日志，日志路径为*/cloud/log/TableStore*/service-role#/{app}_monitor/*。

3. 基于日志判断修复方案或者联系技术支持。

8.15 Alarm-02.310.0200.00002-测试镜像运行不通过

当对应的Service运行异常时，发生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	表格存储	TableStore

可能原因

自身的ServerRole异常或者依赖的服务异常。

影响范围

TableStore无法正常工作。

处理方法

1. 查看错误报告。
2. 获取错误报告中的RequestID。
3. 登录OTS的大数据管家，域名一般是bigdata-ots.aliyun.com
4. 选择**监控中心** > **日志分析** > **请求日志搜索**，将RequestID填入搜索框中搜索。
5. 结果中有详细的错误信息，如果无法处理，请联系技术支持。

9 文件存储NAS

9.1 02.330.0111.00001-BillingService异常

billing_service_monitor会对billing_service进行监控，当其非健康状态时会告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	nas-billing	nas-billing.BillingService#

可能原因

billing_service服务异常。

影响范围

该billing_service服务不可用。

处理方法

1. 查看billing_servcie监控信息。
2. 查看billing_servcie日志，位于*/cloud/log/nas-billing/BillingService#/billing_service/*下，针对日志错误进行处理。
3. 请收集以上信息，并联系技术支持。

告警清除

自动清除

9.2 02.330.0121.00001-KVServer异常

kv_server_monitor会对kv_server进行监控，当其非健康状态时会告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	nas-kvengine	nas-kvengine.KVServer#

可能原因

kv_server服务异常。

影响范围

该kv_server服务不可用。

处理方法

1. 查看kv_server监控信息。
2. 查看kv_server日志，位于*/cloud/log/nas-kvengine/KVServer#/kv_server/*下，针对日志错误进行处理。
3. 请收集以上信息，并联系技术支持。

告警清除

自动清除

9.3 02.330.0122.00001-KVMaster异常

kv_server_monitor会对kv_master进行监控，当其非健康状态时会告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	nas-kvengine	nas-kvengine.KVMaster#

可能原因

kv_master服务异常。

影响范围

该kv_master服务不可用。

处理方法

1. 查看kv_server监控信息。
2. 查看kv_server日志，位于*/cloud/log/nas-kvengine/KVMaster#/kv_master/*下，针对日志错误进行处理。
3. 请收集以上信息，并联系技术支持。

告警清除

自动清除

9.4 02.330.0123.00001-KVSupervisor异常

kv_supervisor_monitor会对kv_supervisor进行监控，当其非健康状态时会告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	nas-kvengine	nas-kvengine. KVSupervisor#

可能原因

kv_supervisor服务异常。

影响范围

kvengine服务异常。

处理方法

1. 查看kv_supervisor监控信息。
2. 查看kv_supervisorr日志，位于*/cloud/log/nas-kvengine/KVSupervisor#/kv_supervisor/*下，针对日志错误进行处理。
3. 请收集以上信息，并联系技术支持。

告警清除

自动清除

9.5 02.330.0131.00001-NFSServer异常

nfs_server_monitor会对nfs_server进行监控，当其非健康状态时会告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	nas-nfs	nas-kvengine. KVSupervisor#

可能原因

nfs_server服务异常。

影响范围

nfs_server服务异常。

处理方法

1. 查看nfs_server监控信息。
2. 查看nfs_server日志，位于*/cloud/log/nas-nfs/NFSServer#/nfs_server/*下，针对日志错误进行处理。
3. 请收集以上信息，并联系技术支持。

告警清除

自动清除

9.6 02.330.0132.00001-NFSSupervisor异常

nfs_supervisor_monitor会对nfs_supervisor进行监控，当其非健康状态时会告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	nas-nfs	nas-nfs.NFSSupervisor#

可能原因

nfs_supervisor服务异常。

影响范围

supervisor服务异常。

处理方法

1. 查看nfs_supervisor监控信息。
2. 查看nfs_supervisor日志，位于*/cloud/log/nas-nfs/NFSSupervisor#/supervisor/*下，针对日志错误进行处理。
3. 请收集以上信息，并联系技术支持。

告警清除

自动清除

9.7 02.330.0141.00001-OcmServer异常

ocm_server_monitor会对ocm_server进行监控，当其非健康状态时会告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	nas-ocm	nas-nfs.NFSSupervisor#

可能原因

ocm_server服务异常。

影响范围

ocm_server服务不可用。

处理方法

1. 查看ocm_server监控信息。
2. 查看ocm_server日志，位于*/cloud/log/nas-ocm/OcmServer#/ocm_server/*下，针对日志错误进行处理。
3. 请收集以上信息，并联系技术支持。

告警清除

自动清除

9.8 02.330.0142.00001-Tengine异常

tengine_monitor会对tengine进行监控，当其非健康状态时会告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	nas-ocm	nas-ocm.Tengine#

可能原因

tengine服务异常。

影响范围

tengine服务不可用。

处理方法

1. 查看tengine监控信息。
2. 查看tengine日志，位于*/cloud/log/nas-ocm/Tengine#/tengine/*下，针对日志错误进行处理。
3. 请收集以上信息，并联系技术支持。

告警清除

自动清除

9.9 02.330.0151.00001-RecycleJob异常

recycle_job_monitor会对recycle_job进行监控，当其非健康状态时会告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	nas-ocm	nas-recycle. RecycleJob#

可能原因

recycle_job服务异常。

影响范围

recycle_job服务不可用。

处理方法

1. 查看recycle_job监控信息。
2. 查看recycle_job日志，位于*/cloud/log/nas-recycle/RecycleJob#/recycle_job/*下，针对日志错误进行处理。
3. 请收集以上信息，并联系技术支持。

告警清除

自动清除

10 云数据库RDS版

10.1 Alarm-02.003.0001.00001-数据库实例down

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS_MYSQL数据库	RDS

可能原因

- 实例异常crash。
- 预期中的实例维护。

影响范围

如果实例能正常切换，则可能会出现闪断，如果未能正常切换，则导致实例不可用。

处理方法

执行/usr/bin/mysqld_safe --defaults-file=/etc/my$端口.cnf命令，直接启动挂掉的实例。

10.2 Alarm-02.003.0001.00002-数据库实例延迟

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS_MYSQL数据库	RDS

可能原因

- 压力大。
- 数据库磁盘故障。
- 业务属性。

影响范围

可能导致主实例异常时，不能进行主备切换。

处理方法

1. 调整并发复制，执行set global slave_parallel_workers=8；命令，在mysql实例中设置。

2. 检查磁盘是否有坏盘或者介质错误。
3. 让业务进行错峰。

10.3 Alarm-02.003.0001.00003-复制io线程中断

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS_MYSQL数据库	RDS

可能原因

- 网络中断。
- 主库实例down掉。
- 复制账号异常。

影响范围

导致主从不一致，主库异常时不能进行切换，从而导致实例不可用。

处理方法

1. 执行telnet ping命令，查看主库是否正常。确认是否是网络以及主实例问题。
2. 打开mysql客户端用复制账号连接主库，查看是否是账号问题。

10.4 Alarm-02.003.0001.00004-复制sql线程中断

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS_MYSQL数据库	RDS

可能原因

- 跟备库数据发生冲突。
- 主备设置不一样。

影响范围

导致主从不一致，主库异常时不能进行切换，从而导致实例不可用。

处理方法

1. 执行show slave status \G命令，查看具体错误，根据不同情况进行具体分析。
2. 检查主备库my.cnf是否有不一样的地方，server_id不同是正常情况。

10.5 Alarm-02.003.0001.00005-cgroup挂载检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS_MYSQL数据库	RDS

可能原因

主机重启未自动加载。

影响范围

导致实例不受cgroup限制，可能会因为一个实例导致整机夯住。

处理方法

执行主机上的*/bin/loadcgroup_for_mysql.sh*脚本。

10.6 Alarm-02.003.0001.00006-内核模板检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS_MYSQL数据库	RDS

可能原因

主机重启未自动加载。

影响范围

可能会引起性能问题。

处理方法

在主机上执行lsmod |grep $模块命令，查看下模板是否加载，如果没有加载，执行modprobe $模块命令，进行加载。

10.7 Alarm-02.003.0001.00007-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS_MYSQL数据库	RDS

可能原因

- 主机重启未自动加载。
- 进程异常。

影响范围

可能会导致该台主机不能分配，并且服务异常。

处理方法

执行如下命令，重启异常进程。

/etc/init.d/rds-mcnode restart

/etc/init.d/rds-dbaas-agent-linux restart

11 云数据库Redis版

11.1 Alarm-02.003.0002.00001-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS茅台	RDS

可能原因

- 主机重启未自动加载。
- 进程异常退出。

影响范围

导致流量上报异常。

处理方法

执行/usr/local/rds/log/package/service.sh start命令，重启该服务进程。

11.2 Alarm-02.003.0002.00002-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS茅台	RDS

可能原因

- 主机重启未自动加载。
- 进程异常退出。

影响范围

SQL优化导致，用户不能得到sql优化报表。

处理方法

执行/usr/local/rds/tunning/package/service.sh start命令，重启该服务进程。

11.3 Alarm-02.003.0002.00003-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS茅台	RDS

可能原因

- 主机重启未自动加载。
- 进程异常退出。

影响范围

导致实例无法切换。

处理方法

执行/usr/local/rds/aurora/package/service.sh start命令，重启服务进程。

11.4 Alarm-02.003.0002.00004-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS茅台	RDS

可能原因

- 主机重启，未自动加载。
- 进程异常退出。

影响范围

实例没有性能数据，导致分配不出来资源。

处理方法

执行/usr/bin/redis-server /usr/local/rds/redis/conf/redis.conf$端口命令，重启服务进程。

11.5 Alarm-02.003.0002.00005-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS茅台	RDS

可能原因

- 主机重启，未自动加载。
- 进程异常退出。

影响范围

无法访问杜康系统。

处理方法

执行/usr/local/rds/dukang/package/service.sh start命令，重启服务进程。

11.6 Alarm-02.003.0002.00006-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS茅台	RDS

可能原因

- 主机重启，未自动加载。
- 进程异常退出。

影响范围

导致RDS API不能被调用。

处理方法

执行/usr/local/rds/rdsapi/package/service.sh start命令，重启服务进程。

11.7 Alarm-02.003.0002.00007-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS茅台	RDS

可能原因

- 主机重启，未自动加载。
- 进程异常退出。

影响范围

导致茅台异常，任务不能下发以及管控失效。

处理方法

执行如下命令，重启服务进程。

/etc/init.d/rds-dbaas-master restart

/etc/init.d/rds-dbaas-stat restart

/etc/init.d/rds-dbaas-bak restart

/etc/init.d/rds-dbaas-check restart

11.8 Alarm-02.003.0002.00008-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
监控检查	-	Redis节点	Redis

可能原因

- 主备关系断开。
- 进程异常退出。
- 管控机器不在管控白名单。

影响范围

实例同步异常，访问异常。

处理方法

1. 进入杜康实例详情页面。
2. 单击主库和备库的测试按钮测试实例是否保活。
3. 登录master机器。
4. 执行redis-cli -p port info repliation命令，查看是是否为master。

   如果不是，则需要执行redis-cli -p port slaveof no one; redis-cli -p config rewrite命令修改。
5. 登录slave机器。
6. 执行redis-cli -p port info replication命令，查看是否为slave，是否连到正确的主库。
7. 执行redis-cli -p port slave of $master_ip $master_port; redis-cli -p port config rewrite命令连接。
8. 登录主库，执行redis-cli -p $port config get admin-whitelist命令，检查管控白名单。

   如果stat机器不在管控白名单，则执行redis-cli -p config set admin-whitelist ""命令加入。

12 云数据库MongoDB

12.1 Alarm-02.003.0001.00008-mongodb-mongo unavailable

告警信息

告警类型	告警级别	告警对象	告警模块
数据库实例不可用	阈值告警	副本集实例	MongoDB数据库

可能原因

- 节点发生故障。
- 节点的内部连接池打满。

影响范围

实例可用性。

处理方法

重启。

13 云数据库Memcache版

13.1 Alarm-02.003.0002.00001-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS茅台	RDS

可能原因

- 主机重启未自动加载。
- 进程异常退出。

影响范围

导致流量上报异常。

处理方法

执行/usr/local/rds/log/package/service.sh start命令，重启该服务进程。

13.2 Alarm-02.003.0002.00002-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS茅台	RDS

可能原因

- 主机重启未自动加载。
- 进程异常退出。

影响范围

SQL优化导致，用户不能得到sql优化报表。

处理方法

执行/usr/local/rds/tunning/package/service.sh start命令，重启该服务进程。

13.3 Alarm-02.003.0002.00003-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS茅台	RDS

可能原因

- 主机重启未自动加载。
- 进程异常退出。

影响范围

导致实例无法切换。

处理方法

执行/usr/local/rds/aurora/package/service.sh start命令，重启服务进程。

13.4 Alarm-02.003.0002.00004-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS茅台	RDS

可能原因

- 主机重启，未自动加载。
- 进程异常退出。

影响范围

实例没有性能数据，导致分配不出来资源。

处理方法

执行/usr/bin/redis-server /usr/local/rds/redis/conf/redis.conf$端口命令，重启服务进程。

13.5 Alarm-02.003.0002.00005-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS茅台	RDS

可能原因

- 主机重启，未自动加载。
- 进程异常退出。

影响范围

无法访问杜康系统。

处理方法

执行/usr/local/rds/dukang/package/service.sh start命令，重启服务进程。

13.6 Alarm-02.003.0002.00006-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS茅台	RDS

可能原因

- 主机重启，未自动加载。
- 进程异常退出。

影响范围

导致RDS API不能被调用。

处理方法

执行/usr/local/rds/rdsapi/package/service.sh start命令，重启服务进程。

13.7 Alarm-02.003.0002.00007-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	RDS茅台	RDS

可能原因

- 主机重启，未自动加载。
- 进程异常退出。

影响范围

导致茅台异常，任务不能下发以及管控失效。

处理方法

执行如下命令，重启服务进程。

`/etc/init.d/rds-dbaas-master restart`

`/etc/init.d/rds-dbaas-stat restart`

`/etc/init.d/rds-dbaas-bak restart`

`/etc/init.d/rds-dbaas-check restart`

13.8 Alarm-02.003.0002.00008-进程检查

告警信息

告警类型	告警级别	告警对象	告警模块
监控检查	-	Redis节点	Redis

可能原因

- 主备关系断开。
- 进程异常退出。
- 管控机器不在管控白名单。

影响范围

实例同步异常，访问异常。

处理方法

1. 进入杜康实例详情页面。
2. 单击主库和备库的测试按钮测试实例是否保活。
3. 登录master机器。
4. 执行redis-cli -p port info repliation命令，查看是是否为master。

   如果不是，则需要执行redis-cli -p port slaveof no one; redis-cli -p config rewrite命令修改。
5. 登录slave机器。
6. 执行redis-cli -p port info replication命令，查看是否为slave，是否连到正确的主库。
7. 执行redis-cli -p port slave of $master_ip $master_port; redis-cli -p port config rewrite命令连接。
8. 登录主库，执行redis-cli -p $port config get admin-whitelist命令，检查管控白名单。

   如果stat机器不在管控白名单，则执行redis-cli -p config set admin-whitelist ""命令加入。

14 HybridDB for MySQL

14.1 Alarm-01.001.0001.00001-数据库占用率过高

当维护工具检测（检测周期为5分钟）到数据库表空间占用率大于产生阈值95%时，产生该告警。当数据库表空间占用率小于清除阈值85%时，该告警会自动清除。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警，事件告警	重要（P2）	具体到产品，包括客户可见的产品和内部依赖的公共组件。	• 硬件：硬件对应服务器中的CPU、硬盘、内存、风扇等。 • 软件对应天基的service role或者service。 • 库存告警。

可能原因

数据库表空间占用率的产生阈值设置不合理。 对于Oracle数据库，数据被导出或转储后，数据库表空间未及时释放。

影响范围

数据库表空间占用率过高可能会导致数据库相关操作失败，如告警等信息入库可能会失败。

该告警发生时，若不及时处理，可能会导致系统运行异常。

处理方法

1. 检查数据库表空间占用率告警的产生阈值设置是否合理。

   Y：请重新设置阈值。

   N：请转至步骤2。
2. 确认是否是Oracle数据库数据被导出或转储后，数据库表空间未及时释放。

   Y：以管理员用户连接数据库后，执行如下命令释放数据库表空间。

   alter table <table_name> enable row movement

alter table <table_name> shrink space

N：请转至步骤3。

3. 请收集上述告警处理过程中的信息，联系技术支持。

14.2 Alarm-02.003.0001.00001-数据库实例down

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	HybridDB for MySQL 数据库	HybridDB for MySQL

可能原因

- 实例异常crash。
- 预期中的实例维护。

影响范围

如果实例能正常切换，则可能会出现闪断，如果未能正常切换，则导致实例不可用。

处理方法

执行/usr/bin/mysqld_safe --defaults-file=/etc/my$端口.cnf命令，直接启动挂掉的实例。

14.3 Alarm-02.003.0001.00002-数据库实例延迟

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	HybridDB for MySQL 数据库	HybridDB for MySQL

可能原因

- 压力大。
- 数据库磁盘故障。
- 业务属性。

影响范围

可能导致主实例异常时，不能进行主备切换。

处理方法

1. 调整并发复制，执行set global slave_parallel_workers=8；命令，在mysql实例中设置。
2. 检查磁盘是否有坏盘或者介质错误。
3. 让业务进行错峰。

14.4 Alarm-02.003.0001.00003-复制io线程中断

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	HybridDB for MySQL数据库	HybridDB for MySQL

可能原因

- 网络中断。
- 主库实例down掉。
- 复制账号异常。

影响范围

导致主从不一致，主库异常时不能进行切换，从而导致实例不可用。

处理方法

1. 执行telnet ping命令，查看主库是否正常。确认是否是网络以及主实例问题。
2. 打开mysql客户端用复制账号连接主库，查看是否是账号问题。

14.5 Alarm-02.003.0001.00004-复制sql线程中断

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	HybridDB for MySQL数据库	HybridDB for MySQL

可能原因

- 跟备库数据发生冲突。
- 主备设置不一样。

影响范围

导致主从不一致，主库异常时不能进行切换，从而导致实例不可用。

处理方法

1. 执行show slave status \G命令，查看具体错误，根据不同情况进行具体分析。
2. 检查主备库my.cnf是否有不一样的地方，server_id不同是正常情况。

14.6 Alarm-02.003.0001.00005-cgroup挂载检查

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	HybridDB for MySQL 数据库	HybridDB for MySQL

可能原因

主机重启未自动加载。

影响范围

导致实例不受cgroup限制，可能会因为一个实例导致整机停止响应。

处理方法

执行主机上的*/bin/loadcgroup_for_mysql.sh*脚本。

14.7 Alarm-02.003.0001.00006-petadata&kepler连接报警

该告警对应到杜康的异常信息页面，报警内容包括：活跃进程过多、磁盘使用过高、主备延迟过高、kepler内部报错等。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要（P2）	HybridDB for MySQL 实例	杜康

可能原因

进入杜康页面，会显示具体的告警信息。

影响范围

HybridDB for MySQL实例的可用性。

处理方法

进入杜康的报警信息页面，根据具体的报错信息进行处理。

14.8 Alarm-02.003.0001.00007- petadata&kepler错误报警

该告警对应到杜康的异常信息页面，报警内容包括：活跃进程过多、磁盘使用过高、主备延迟过高、kepler内部报错等。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要（P2）	HybridDB for MySQL实例	杜康

可能原因

进入杜康页面，会显示具体的告警信息。

影响范围

HybridDB for MySQL实例的可用性。

处理方法

进入杜康的报警信息页面，根据具体的报错信息进行处理。

14.9 Alarm-02.003.0001.00008-petadata&kepler其他报警

该告警对应到杜康的异常信息页面，报警内容包括：活跃进程过多、磁盘使用过高、主备延迟过高、kepler内部报错等。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要（P2）	HybridDB for MySQL实例	杜康

可能原因

进入杜康页面，会显示具体的告警信息。

影响范围

HybridDB for MySQL实例的可用性。

处理方法

进入杜康的报警信息页面，根据具体的报错信息进行处理。

15 HybridDB for PostgreSQL

15.1 Alarm-01.001.0001.00001-数据库占用率过高

当维护工具检测（检测周期为5分钟）到数据库表空间占用率大于产生阈值95%时，产生该告警。当数据库表空间占用率小于清除阈值85%时，该告警会自动清除。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警，事件告警	重要（P2）	具体到产品，包括客户可见的产品和内部依赖的公共组件。	• 硬件：硬件对应服务器中的CPU、硬盘、内存、风扇等。 • 软件对应天基的service role或者service。 • 库存告警。

可能原因

数据库表空间占用率的产生阈值设置不合理。 对于Oracle数据库，数据被导出或转储后，数据库表空间未及时释放。

影响范围

数据库表空间占用率过高可能会导致数据库相关操作失败，如告警等信息入库可能会失败。

该告警发生时，若不及时处理，可能会导致系统运行异常。

处理方法

1. 检查数据库表空间占用率告警的产生阈值设置是否合理。

   Y：请重新设置阈值。

   N：请转至步骤2。

2. 确认是否是Oracle数据库数据被导出或转储后，数据库表空间未及时释放。

   Y：以管理员用户连接数据库后，执行如下命令释放数据库表空间。

   alter table <table_name> enable row movement

alter table <table_name> shrink space

N：请转至步骤3。

3. 请收集上述告警处理过程中的信息，联系技术支持。

16 负载均衡SLB

16.1 Alarm-01.210.0001.00001-无日志生成

netframe LVS没有日志生成。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-lvs

可能原因

netframe配置异常或启动有问题。

影响范围

SLB业务可能出现异常。

处理方法

1. 检查LVS netfame配置是否正确和日志级别。
2. 检查磁盘是否太满，导致日志无法生成。

16.2 Alarm-01.210.0001.00002-base admin 绑定network失败

base admin 绑定network失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-lvs

可能原因

quagga启动异常，或重复绑定地址。

影响范围

SLB业务可能出现异常。

处理方法

1. 检查quagga是否正常启动。

2. 排查绑定路由是否有冲突。
3. 检查LVS日志，查看错误信息.

16.3 Alarm-01.210.0001.00003-同一个日志文件应用到互斥的logstore

同一个日志文件应用到互斥的logstore.

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-lvs

可能原因

ilogtail配置问题.

影响范围

SLB业务可能出现异常.

处理方法

检查ilogtail配置。

16.4 Alarm-01.210.0001.00004-分配内存失败

LVS分配内存失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-lvs

可能原因

LVS分配内存失败，可能内存不足。

影响范围

SLB业务可能出现异常。

处理方法

检查hugepage使用率。

16.5 Alarm-01.210.0001.00005-keepalived reload次数过多

keepalived reload次数过多。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	p2	ClusterOwner	软件，slb-lvs

可能原因

keepalived reload次数过多。

影响范围

SLB业务可能出现异常。

处理方法

检查keepalived agent的日志。

16.6 Alarm-01.210.0001.00006-keepalived died

keepalived 进程不在。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-lvs

可能原因

keepalive异常。

影响范围

SLB业务可能出现异常。

处理方法

检查keepalived agent slb_monitor的日志。

16.7 Alarm-01.210.0001.00007-zebra ospf状态异常

zebra ospf状态异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-lvs

可能原因

zebra ospf状态异常。

影响范围

slb业务可能出现异常。

处理方法

检查quagga zebra ospf slb_monitor的日志。

16.8 Alarm-01.210.0001.00008-进程磁盘占用率高

进程磁盘占用率高。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-lvs

可能原因

进程磁盘占用率高。

影响范围

SLB业务可能出现异常。

处理方法

检查磁盘情况，查看LVS日志中的异常。

16.9 Alarm-01.210.0001.00009-lvs入流量过大

LVS入流量过大。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	p2	ClusterOwner	软件，slb-lvs

可能原因

LVS入流量过大。

影响范围

SLB业务可能出现异常。

处理方法

tsar查看流量情况，确认当前是否有异常的流量。

16.10 Alarm-01.210.0001.00010-lvs新建连接过大

lvsVS新建连接过大。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	p2	ClusterOwner	软件，slb-lvs

可能原因

LVS新建连接过大，可能是突发流量，也可能是攻击流量。

影响范围

SLB业务可能出现异常。

处理方法

tsar查看流量情况，确认当前是否有异常的流量。

16.11 Alarm-01.210.0001.00011-agent进程挂了

agent进程挂了。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-lvs

可能原因

- agent有异常。
- slb_monitord重启了。

影响范围

SLB业务可能出现异常。

处理方法

查看agent，slb的日志，执行service slb-control-lvs start命令，重启agent。

16.12 Alarm-01.210.0001.00012-LVS 有coredump文件

LVS有coredump文件。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，SLB-LVS

可能原因

- LVS 有coredump文件，可能LVS发生过core。

影响范围

SLB业务可能出现异常。

处理方法

1. 检查当前各进程是否运行正常。
2. 保存core文件，交由阿里工程师分析处理。

16.13 Alarm-01.210.0001.00013- LVS到proxy后端健康检查失败

LVS到proxy后端健康检查失败

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，SLB-LVS

可能原因

LVS到proxy后端健康检查失败。

影响范围

SLB业务可能出现异常。

处理方法

检查LVS健康检查日志，检查proxy是否由异常。

16.14 Alarm-01.210.0001.00014-内存使用率过高

内存使用率过高。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	p2	ClusterOwner	软件，slb-lvs

可能原因

内存使用率过高。

影响范围

SLB业务可能出现异常。

处理方法

base_admin 查看内存占用情况。

16.15 Alarm-01.210.0001.00015-pidfile存在，LVSMonitor进程不存在

pidfile存在，LVSMonitor进程不存在。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，SLB-LVS

可能原因

pidfile存在，LVSMonitor进程不存在,monitor异常退出。

影响范围

SLB业务可能出现异常。

处理方法

查看SLB进程的当前的状态，LVSMonitor的状态，并重启。

16.16 Alarm-01.210.0001.00016-LVSMonitor进程的pidfile不存在

LVSMonitor进程的pidfile不存在。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，SLB-LVS

可能原因

LVSMonitor进程的pidfile不存在。

影响范围

SLB业务可能出现异常。

处理方法

查看SLB进程的当前的状态，LVSMonitor的状态，并重启。

16.17 Alarm-01.210.0001.00017-pidfile存在，SLB-Control-LVS进程不存在

pidfile存在，SLB-Control-LVS进程不存在。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，SLB-LVS

可能原因

pidfile存在，SLB-Control-LVS进程不存在。

影响范围

SLB业务可能出现异常。

处理方法

排查异常日志，重启SLB-Control-LVS。

16.18 Alarm-01.210.0001.00018-SLB-Control-LVS进程的pidfile都不存在

SLB-Control-LVS进程的pidfile都不存在。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，SLB-LVS

可能原因

- SLB-Control-LVS进程的pidfile都不存在

影响范围

- SLB业务可能出现异常

处理方法

排查异常日志，重启SLB-Control-LVS

16.19 Alarm-01.210.0001.00019-pidfile存在，keepalived进程不存在

pidfile存在，keepalived进程不存在。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，SLB-LVS

可能原因

pidfile存在，keepalived进程不存在。

影响范围

SLB业务可能出现异常。

处理方法

排查异常日志，重启keepalive。

16.20 Alarm-01.210.0001.00020-keepalived pidfile不存在

keepalived pidfile不存在。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，SLB-LVS

可能原因

keepalived pidfile不存在。

影响范围

SLB业务可能出现异常。

处理方法

排查异常日志，重启keepalive。

16.21 Alarm-01.210.0001.00021-组播消息异常

lsw交换机组播消息异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-lvs

可能原因

组播消息异常。

影响范围

SLB业务可能出现异常。

处理方法

1. 检查LVS上session同步是否正常。
2. 让网络同学排查交换机组播情况。

16.22 Alarm-01.210.0001.00022-slb_vxlan_addr没有绑定

slb_vxlan_addr没有绑定。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-lvs

可能原因

slb_vxlan_addr没有绑定。

影响范围

SLB业务可能出现异常。

处理方法

1. 检查agent有没有下发vxlan地址。
2. reload agent。

16.23 Alarm-01.210.0001.00023-没有配健康检查源地址到网卡上

没有配健康检查源地址到网卡上。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-lvs

可能原因

没有配健康检查源地址到网卡上。

影响范围

SLB业务可能出现异常。

处理方法

1. 检查agent有没有下发hc地址。
2. reload agent。

16.24 Alarm-01.210.0001.00024-vlan100口的ospf邻居状态不是ful

vlan100口的ospf邻居状态不是ful。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-lvs

可能原因

vlan100口的ospf邻居状态不是ful。

影响范围

SLB业务可能出现异常。

处理方法

检查ospf邻居状态信息，查看是否是网络抖动。

16.25 Alarm-01.210.0001.00025-vlan101口的ospf邻居状态不是ful

vlan101口的ospf邻居状态不是ful。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-lvs

可能原因

vlan101口的ospf邻居状态不是ful。

影响范围

SLB业务可能出现异常。

处理方法

检查ospf邻居状态信息，查看是否是网络抖动。

16.26 Alarm-01.210.0001.00026-ospf 邻居关系个数异常

ospf 邻居关系个数异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-lvs

可能原因

ospf 邻居关系个数异常。

影响范围

SLB业务可能出现异常。

处理方法

检查ospf邻居状态信息，查看是否是网络抖动。

16.27 Alarm-01.210.0001.00027-keepalive_process_has_no_the_-A_option

keepalive配置启动参数没有-A参数。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，SLB-LVS

可能原因

keepalive配置启动参数没有-A参数。

影响范围

SLB业务可能出现异常。

处理方法

检查keepalived配置文件，重新启动keepalive。

16.28 Alarm-01.210.0001.00028-Hugepage not enough

LVS hugepage不足。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，SLB-LVS

可能原因

LVS hugepage不足，内存占用过高。

影响范围

SLB业务可能出现异常。

处理方法

查看hugepage的占用情况。

16.29 Alarm-01.210.0001.00029-LVS(netframe) monitor 进程不存在

LVS(netframe) monitor 进程不存在。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，SLB-LVS

可能原因

LVS(netframe) monitor 进程不存在。

影响范围

SLB业务可能出现异常。

处理方法

检查monitord日志，如果进程没有run，重启monitord服务。

16.30 Alarm-01.210.0001.00030-LVS(netframe) 转发进程不存在

LVS(netframe) 转发进程不存在。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，SLB-LVS

可能原因

LVS(netframe) 转发进程不存在。

影响范围

SLB业务可能出现异常。

处理方法

检查monitord日志，如果进程没有run，重启monitord服务。

16.31 Alarm-01.210.0001.00031-LVS(netframe) 转发 core 负载过高

LVS(netframe) 转发 core 负载过高。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，SLB-LVS

可能原因

LVS(netframe) 转发 core 负载过高。

影响范围

SLB业务可能出现异常。

处理方法

查看netframe每个core的负载是否均匀，如果不均匀可能存在hash不均匀的情况。

16.32 Alarm-01.210.0001.00032-LVS（netframe）错误日志

LVS（netframe）存在错误日志。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，SLB-LVS

可能原因

LVS（netframe）存在错误日志。

影响范围

SLB业务可能出现异常。

处理方法

排查具体的错误日志。

16.33 Alarm-01.210.0001.00033-LVS（netframe）默认路由错误

LVS（netframe）默认路由错误。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，SLB-LVS

可能原因

LVS（netframe）默认路由错误。

影响范围

SLB业务可能出现异常。

处理方法

查看默认路由是否有两跳，端口是否正常。

16.34 Alarm-01.210.0001.00034-session_create_failed

session_create_failed,session创建时候有失败的情况。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	p1	ClusterOwner	软件，SLB-LVS

可能原因

session_create_failed,session创建时候有失败的情况，可能是后端服务有异常。

影响范围

SLB业务可能出现异常。

处理方法

排查后端服务是否有异常。

16.35 Alarm-01.210.0001.00035-ilogtail进程没起

ilogtail进程没起。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-lvs

可能原因

ilogtail进程没起。

影响范围

SLB业务可能出现异常。

处理方法

重启ilogtail。

16.36 Alarm-01.210.0001.00036-网卡物理链路down

网卡物理链路down。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，SLB-LVS

可能原因

网卡物理链路down。

影响范围

SLB业务可能出现异常。

处理方法

排查物理网络是否有问题，LVS到LSW链路。

16.37 Alarm-01.210.0001.00037-有VPC RS健康检查全部失败

VPC RS健康检查全部失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-lvs

可能原因

VPC RS健康检查全部失败。

影响范围

SLB业务可能出现异常。

处理方法

查看keepalive健康检查结果，reload keepalived。

16.38 Alarm-01.210.0001.00038-健康检查失败个数突增

健康检查失败个数突增。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-lvs

可能原因

健康检查失败个数突增,有可能是业务迁移，也有可能是物理网络抖动。

影响范围

SLB业务可能出现异常。

处理方法

查看keepalive健康检查结果，reload keepalived。

16.39 Alarm-01.210.0001.00039-系统dstcache不足

系统dstcache不足。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-lvs

可能原因

系统dstcache不足。

影响范围

SLB业务可能出现异常。

处理方法

检查*/proc/slabinfo /proc/sys/net/ipv4/route/max_size*下关于dst cache的配置信息。

16.40 Alarm-01.210.0001.00040-agent offline了

agent offline了。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-lvs

可能原因

agent offline了，可能是网络抖动。

影响范围

SLB业务可能出现异常。

处理方法

观察是否可以恢复为online，重启agent进程。

16.41 Alarm-01.210.0001.00041-agent的管控状态service_enabled字段不为enabled

agent的管控状态service_enabled字段不为enabled。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-lvs

可能原因

agent的管控状态service_enabled字段不为enabled。

影响范围

SLB业务可能出现异常。

处理方法

调用管控接口enable lvs机器。

16.42 Alarm-01.210.0001.00042-同一个日志文件应用到互斥的logstore

同一个日志文件应用到互斥的logstore。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-proxy

可能原因

ilogtail配置问题。

影响范围

SLB业务可能出现异常。

处理方法

检查ilogtail配置。

16.43 Alarm-01.210.0001.00043-转发CPU利用率过高

转发CPU利用率过高。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	p2	ClusterOwner	软件，slb-proxy

可能原因

转发CPU利用率过高。

影响范围

SLB业务可能出现异常。

处理方法

检查各个core的利用率情况。

16.44 Alarm-01.210.0001.00044-内存占用率过高

内存占用率过高。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	p2	ClusterOwner	软件，slb-proxy

可能原因

内存占用率过高。

影响范围

SLB业务可能出现异常。

处理方法

检查内存的利用率情况。

16.45 Alarm-01.210.0001.00045-进程磁盘占用率高

进程磁盘占用率高。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-proxy

可能原因

进程磁盘占用率高。

影响范围

SLB业务可能出现异常。

处理方法

检查磁盘情况，查看proxy日志中的异常。

16.46 Alarm-01.210.0001.00046-proxy 有coredump文件

proxy有coredump文件。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

proxy有coredump文件，可能LVS发生过core。

影响范围

SLB业务可能出现异常。

处理方法

1. 检查当前各进程是否运行正常。
2. 保存core文件，请联系阿里工程师分析处理。

16.47 Alarm-01.210.0001.00047-network_card_of_bond0_is_down

bond0网卡down。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

bond0网卡down。

影响范围

SLB业务可能出现异常。

处理方法

查看bond0的接口状态，以及网络是否有异常。

16.48 Alarm-01.210.0001.00048-bond0的状态不是up

bond0的状态不是up。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

bond0网卡不是up。

影响范围

SLB业务可能出现异常。

处理方法

查看bond0的接口状态，网络是否有异常。

16.49 Alarm-01.210.0001.00049-出入方向有丢包

出入方向有丢包。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	p2	ClusterOwner	软件，slb-proxy

可能原因

出入方向有丢包。

影响范围

SLB业务可能出现异常。

处理方法

查看网卡的接口状态，网络是否有异常，流量是否过大。

16.50 Alarm-01.210.0001.00050-网卡使用率高

网卡使用率高。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-proxy

可能原因

网卡使用率高。

影响范围

SLB业务可能出现异常。

处理方法

查看网卡的接口状态，网络是否有异常，流量是否过大。

16.51 Alarm-01.210.0001.00051-软中断过高

软中断过高。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-proxy

可能原因

软中断过高。

影响范围

SLB业务可能出现异常。

处理方法

查看系统软中断。

16.52 Alarm-01.210.0001.00052-ilogtail进程没起

ilogtail进程没起。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-proxy

可能原因

ilogtail进程没起。

影响范围

SLB业务可能出现异常。

处理方法

重启ilogtail。

16.53 Alarm-01.210.0001.00053-ilogtail文件上传延迟或者一直失败

ilogtail文件上传延迟或者一直失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-proxy

可能原因

ilogtail文件上传延迟或者一直失败，可能是网络抖动。

影响范围

SLB业务可能出现异常。

处理方法

检查网络情况。

16.54 Alarm-01.210.0001.00054-proxy qps过高

proxy qps过高。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	p1	ClusterOwner	软件，slb-proxy

可能原因

proxy qps过高，可能有突发流量，也可能达到proxy的水位。

影响范围

SLB业务可能出现异常。

处理方法

tsar查看qps数量。

16.55 Alarm-01.210.0001.00055-健康检查波动

健康检查波动

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

健康检查波动。

影响范围

SLB业务可能出现异常。

处理方法

排查是否是网络抖动，是否是后端业务rs有问题。

16.56 Alarm-01.210.0001.00056-RS健康检查全部失败

proxy RS健康检查全部失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

proxy RS健康检查全部失败。

影响范围

SLB业务可能出现异常。

处理方法

排查是否是网络抖动，是否是后端业务rs有问题。

16.57 Alarm-01.210.0001.00057-没有TEngineMonitor进程

没有TEngineMonitor进程。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

没有TEngineMonitor进程。

影响范围

SLB业务可能出现异常。

处理方法

重启TEngineMonitor。

16.58 Alarm-01.210.0001.00058-proxy打开文件fd过多

proxy打开文件fd过多。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	p2	ClusterOwner	软件，slb-proxy

可能原因

proxy打开文件fd过多。

影响范围

SLB业务可能出现异常。

处理方法

查看worker进程打开文件的个数以及socket打开文件的个数。

16.59 Alarm-01.210.0001.00059-ospf 邻居关系个数异常

ospf 邻居关系个数异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

ospf 邻居关系个数异常。

影响范围

SLB业务可能出现异常。

处理方法

检查ospf邻居状态信息，查看是否是网络抖动。

16.60 Alarm-01.210.0001.00060-T2口的ospf邻居状态不是ful

T2口的ospf邻居状态不是ful。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

T2口的ospf邻居状态不是ful。

影响范围

SLB业务可能出现异常。

处理方法

检查ospf邻居状态信息，查看是否是网络抖动。

16.61 Alarm-01.210.0001.00061-T1口的ospf邻居状态不是ful

T1口的ospf邻居状态不是ful。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

T1口的ospf邻居状态不是ful。

影响范围

SLB业务可能出现异常。

处理方法

检查ospf邻居状态信息，查看是否是网络抖动。

16.62 Alarm-01.210.0001.00062-worker_process_greater_than_the_num_of_cpu

nginx worker的个数超过了cpu个数。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

nginx worker的个数超过了cpu个数。

影响范围

SLB业务可能出现异常。

处理方法

可能是shutingdown进程多，也可能是nginx reload。

16.63 Alarm-01.210.0001.00063-proxy default 路由缺失

SLB业务可能出现异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

proxy default 路由缺失。

影响范围

SLB业务可能出现异常。

处理方法

查看proxy 网口的状态，ospf邻居是否正常。

16.64 Alarm-01.210.0001.00064-zebra ospf状态异常

zebra ospf状态异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

zebra ospf状态异常。

影响范围

SLB业务可能出现异常。

处理方法

检查quagga zebra ospf日志。

16.65 Alarm-01.210.0001.00065-agent进程挂了

agent进程挂了。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

可能agent有异常。

影响范围

SLB业务可能出现异常。

处理方法

查看Agent，SLB的日志，尽快重启Agent。

16.66 Alarm-01.210.0001.00066-slb_vxlan_saddr没有绑定

slb_vxlan_saddr没有绑定。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

slb_vxlan_saddr没有绑定。

影响范围

SLB业务可能出现异常。

处理方法

1. 检查agent有没有下发vxlan地址。
2. reload agent。

16.67 Alarm-01.210.0001.00067-agent的管控状态enabled字段为disable

Agent的管控状态enabled字段为**disable**。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

Agent的管控状态enabled字段为**disable**。

影响范围

SLB业务可能出现异常。

处理方法

调用管控接口enable proxy机器。

16.68 Alarm-01.210.0001.00068-agent offline了

Agent offline了。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-proxy

可能原因

Agent offline了，可能是网络抖动。

影响范围

SLB业务可能出现异常。

处理方法

观察是否可以恢复为online，重启Agent进程。

16.69 Alarm-01.210.0001.00069-同一个日志文件应用到互斥的logstore

同一个日志文件应用到互斥的logstore。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-keyserver

可能原因

ilogtail配置问题。

影响范围

SLB业务可能出现异常。

处理方法

检查ilogtail配置。

16.70 Alarm-01.210.0001.00070-转发cpu 利用率过高

转发CPU利用率过高。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	p2	ClusterOwner	软件，slb-keyserver

可能原因

转发CPU利用率过高。

影响范围

SLB业务可能出现异常。

处理方法

检查各个core的利用率情况。

16.71 Alarm-01.210.0001.00071-内存占用率过高

内存占用率过高。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	p2	ClusterOwner	软件，slb-keyserver

可能原因

内存占用率过高。

影响范围

SLB业务可能出现异常。

处理方法

检查内存的利用率情况。

16.72 Alarm-01.210.0001.00072-进程磁盘占用率高

进程磁盘占用率高。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-keyserver

可能原因

进程磁盘占用率高。

影响范围

SLB业务可能出现异常。

处理方法

检查磁盘情况，查看proxy日志中的异常。

16.73 Alarm-01.210.0001.00073-keyserver 有coredump文件

keyserver 有coredump文件。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-keyserver

可能原因

keyserver有coredump文件，可能keyserver发生过core。

影响范围

SLB业务可能出现异常。

处理方法

1. 检查当前各进程是否运行正常。
2. 保存core文件，联系阿里工程师分析处理。

16.74 Alarm-01.210.0001.00074-network_card_of_bond0_is_down

bond0网卡down。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-keyserver

可能原因

bond0网卡down。

影响范围

SLB业务可能出现异常。

处理方法

查看bond0的接口状态，网络是否有异常。

16.75 Alarm-01.210.0001.00075-bond0的状态不是up

bond0的状态不是up。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-keyserver

可能原因

bond0网卡不是up。

影响范围

SLB业务可能出现异常。

处理方法

查看bond0的接口状态，网络是否有异常。

16.76 Alarm-01.210.0001.00076-出入方向有丢包

出入方向有丢包。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	p2	ClusterOwner	软件，slb-keyserver

可能原因

出入方向有丢包。

影响范围

SLB业务可能出现异常。

处理方法

查看网卡的接口状态，网络是否有异常，流量是否过大。

16.77 Alarm-01.210.0001.00077-网卡使用率高

网卡使用率高。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-keyserver

可能原因

网卡使用率高。

影响范围

SLB业务可能出现异常。

处理方法

查看网卡的接口状态，网络是否有异常，流量是否过大。

16.78 Alarm-01.210.0001.00078-软中断过高

软中断过高。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-keyserver

可能原因

软中断过高。

影响范围

SLB业务可能出现异常。

处理方法

查看系统软中断。

16.79 Alarm-01.210.0001.00079-ilogtail进程没起

ilogtail进程没起。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-keyserver

可能原因

ilogtail进程没起。

影响范围

SLB业务可能出现异常。

处理方法

重启ilogtail。

16.80 Alarm-01.210.0001.00080-ilogtail文件上传延迟或者一直失败

ilogtail文件上传延迟或者一直失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-keyserver

可能原因

ilogtail文件上传延迟或者一直失败，可能是网络抖动。

影响范围

SLB业务可能出现异常。

处理方法

检查网络情况。

16.81 Alarm-01.210.0001.00081-keyserver日志中有错误

keyserver日志中有错误。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p2	ClusterOwner	软件，slb-keyserver

可能原因

keyserver日志中有错误。

影响范围

SLB业务可能出现异常。

处理方法

排查错误日志。

16.82 Alarm-01.210.0001.00082-cert-central-agent_has_disappeared

cert-central-agent_has_disappeared。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，slb-keyserver

可能原因

cert agent进程不在或异常退出。

影响范围

SLB业务可能出现异常。

处理方法

重启cert-agent。

17 专有网络VPC

17.1 Alarm-01.205.0001.00001-XGW发生coredump

XGW进程在运行过程中发生coredump。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件,VPC-XGW

可能原因

XGW发生coredump。

影响范围

VPC业务可能出现异常。

处理方法

1. 重启VPC-XGW服务，将coredump文件保存下来。
2. 联系阿里云工程师，排查问题。

17.2 Alarm-02.205.0001.00002-XGW端口流量过高

XGW端口流量过高。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	p4	ClusterOwner	软件,VPC-XGW

可能原因

- 当前业务流量过高。
- 有攻击。

影响范围

导致VPC业务可能会有丢包。

处理方法

1. 查看是否被攻击。
2. 如果没有被攻击，需考虑扩容VPC-XGW物理机台数。

17.3 Alarm-01.205.0001.00003-XGW端口丢包

XGW端口丢包。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件,VPC-XGW

可能原因

- 当前业务流量过高。
- XGW机器网卡异常。

影响范围

VPC业务可能出现异常。

处理方法

在VPC-XGW物理机器上执行如下命令，查看当前XGW流量，每个端口的处理能力为10Gbps。

```
Telnet localhost; enable; show port 0 portspeed;show port 1 portspeed;show port 2 portspeed;
show port 3 portspeed;
```

- 如果是超过端口处理能力丢包，那么需要扩容XGW机器。
- 如果是因为网卡硬件问题丢包，那么需要在XGW可用台数大于2的情况下，下线当前丢包的XGW。

17.4 Alarm-01.205.0001.00004-XGW业务口mtu过小

XGW端口mtu错误。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件,VPC-XGW

可能原因

XGW网卡mtu设置错误，不是1982。

影响范围

VPC业务异常。

处理方法

在XGW上执行telnet localhost; enable; show running-config ; 命令，查看mtu配置，正确的mtu值应该为1982。

如果网卡mtu不是1982，执行vim /usr/local/etc/nf-startup-config命令，修改里面的值为1982，重启VPC-XGW服务。

17.5 Alarm-01.205.0001.00005-XGW日志中有critical日志

XGW日志中有critical日志。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件，VPC-XGW

可能原因

XGW进程运行异常。

影响范围

可能会让VPC业务异常。

处理方法

一般XGW运行日志里面的错误，多为配置下发出错，遇到这种情况，最好先联系阿里云VPC的同学，进行处理。

17.6 Alarm-01.205.0001.00006-XGW上默认路由不是4条

XGW正常运行有4条默认路由，如果不是，则异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p1	ClusterOwner	软件,VPC-XGW

可能原因

- XGW端口，或者XGW上联lsw端口状态异常。
- lsw ospf协议配置异常。
- XGW机器上ospf配置异常。

影响范围

可能会让VPC业务异常。

处理方法

1. 在XGW上执行telnet localhost; enable; show port all;命令，查看交换机和XGW端口状态。

   如果4个口都不是UP的，那么是因为交换机或者XGW网卡down了导致的，需检查硬件问题。
2. 在XGW上执行sudo vtysh; show ip ospf neighbor命令，检查XGW上联交换机lsw ospf路由协议配置。

   查看ospf令居情况，正常情况下会有4条邻居，如果没有，需要检查lsw ospf协议配置。
3. 如果以上都没有问题，重启当前机器的VPC-XGW服务，如果依然无法解决，请联系阿里云工程师。

17.7 Alarm-01.205.0002.00007-gwAgent中有错误日志

gwAgent发生异常，可能导致控制系统下发数据异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	p4	ClusterOwner	软件,VPC-gwAgent

可能原因

下发数据错误。

影响范围

可能会让控制台操作失败，openapi调用失败。

处理方法

重启该台机器的VPC-XGW服务。

17.8 Alarm-02.205.0001.00008-XGW上tunnel使用过多

当前region的VPC过多。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	p4	ClusterOwner	软件,VPC-XGW

可能原因

当前VPC过多。

影响范围

可能会让当前VPC集群负载过高，发生丢包等情况，影响其他VPC的业务。

处理方法

当前集群VPC 数据量过多，专有云一般不会出现，如果出现了，可考虑将改报警的阈值调大。

18 日志服务

18.1 Alarm-02.600.0001.0001-客户端logtail进程退出

当脚本检测到机器上logtail进程不存在时报警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	logtail	Agent

可能原因

logtail未启动或者未安装，也可能是超过内存、cpu使用阈值，进程自杀。

影响范围

该台机器上停止收集数据。

处理方法

1. 安装logtail，请联系技术支持。
2. 执行sudo /etc/init.d/ilogtaild start命令，启动logtail进程。

18.2 Alarm-02.600.0002.0001-机器上离线导入任务未运行

当脚本检测到机器上odps_cmd_server.jar进程不存在时报警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	离线导出模块	FuxiServic eShennongWorker

可能原因

未启动该进程。

影响范围

离线导入日志数据到ODPS会失败。

处理方法

此类问题一般原因比较复杂，调查头绪比较多，无法提供统一的处理方法，请直接联系技术支持。

18.3 Alarm-01.600.0002.0002-盘古数据副本数量<=1

当脚本检测到机器上盘古数据副本数量小于等于1时报警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	pangu	FuxiServic eShennongWorker

可能原因

盘古服务故障。

影响范围

可能会导致集群数据丢失。

处理方法

此类问题一般原因比较复杂，调查头绪比较多，无法提供统一的处理方法，请直接联系技术支持。

18.4 Alarm-02.600.0002.0003-shennong worker partitition未全部load

shennong worker fuxi service partition没有全部load起来。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	shennong worker	FuxiServic eShennongWorker

可能原因

原因复杂。

影响范围

数据写入报500错误，短时间内不会有影响，持续时间长可能会导致数据丢失。

处理方法

此类问题一般原因比较复杂，调查头绪比较多，无法提供统一的处理方法，请直接联系技术支持。

18.5 Alarm-02.600.0002.0004-shennong worker partitition未全部load

shennong worker fuxi service partition没有全部load起来，该报警支持未load的partition数量。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	shennong worker	FuxiServic eShennongWorker

可能原因

原因复杂。

影响范围

数据写入报500错误，短时间内不会有影响，持续时间长可能会导致数据丢失。

处理方法

此类问题一般原因比较复杂，调查头绪比较多，无法提供统一的处理方法，请直接联系技术支持。

18.6 Alarm-02.600.0002.0002-2小时内没有生成离线任务

系统检测到，部分离线任务执行失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	离线导出模块	ToolService

可能原因

可能的原因是用户odps endpoint配置错误。

影响范围

离线导入日志数据到ODPS会失败。

处理方法

此类问题一般原因比较复杂，调查头绪比较多，无法提供统一的处理方法，请直接联系技术支持。

18.7 Alarm-01.600.0002.0003-离线导入的fuxi作业堆积超过200

系统检测到，部分离线任务执行堆积。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	离线导出模块	ToolService

可能原因

ODPS执行quota不足。

影响范围

离线导入日志数据到ODPS会失败。

处理方法

此类问题一般原因比较复杂，调查头绪比较多，无法提供统一的处理方法，请直接联系技术支持。

18.8 Alarm-02.600.0003.0001-ots表创建失败

ots表创建失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	OTS建表模块	ToolService

可能原因

机器上定时任务被清理或者ots故障。

影响范围

索引数据写入OTS会失败，导致数据无法检索。

处理方法

此类问题一般原因比较复杂，调查头绪比较多，无法提供统一的处理方法，请直接联系技术支持。

18.9 Alarm-01.600.0004.0001-集群磁盘资源紧张

集群磁盘使用超过90%。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	pangu	FuxiServic eShennongWorker

可能原因

集群磁盘资源紧张。

影响范围

数据无法写入，服务退出。

处理方法

进行pangu磁盘扩容，并联系技术支持。

18.10 Alarm-02.600.0005.0001-index worker partition未全部load

index worker fuxi service partition没有全部load起来，该报警支持未load的partition数量。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	index worker	FuxiServiceSlsIndexW orker

可能原因

原因复杂。

影响范围

数据检索请求会失败。

处理方法

此类问题一般原因比较复杂，调查头绪比较多，无法提供统一的处理方法，请直接联系技术支持。

18.11 Alarm-02.600.0006.0001-configservice worker partition未全部load

configservice worker fuxi service partition没有全部load起来，该报警支持未load的partition数量。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	configservice worker	FuxiServiceSlsConfigservice

可能原因

原因复杂。

影响范围

机器相关的meta操作请求失败。

处理方法

此类问题一般原因比较复杂，调查头绪比较多，无法提供统一的处理方法，请直接联系技术支持。

18.12 Alarm-02.600.0007.0001-loghub master worker partition未全部load

loghub master worker fuxi service partition没有全部load起来，该报警支持未load的partition数量。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	loghub master worker	FuxiServiceSlsLoghubMaster

可能原因

原因复杂。

影响范围

logstore相关的meta操作请求失败。

处理方法

此类问题一般原因比较复杂，调查头绪比较多，无法提供统一的处理方法，请直接联系技术支持。

18.13 Alarm-02.600.0008.0001-quota service worker partition未全部load

quota service worker fuxi service partition没有全部load起来，该报警支持未load的partition数量。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	quota server worker	FuxiServiceSlsQuotaServer

可能原因

原因复杂。

影响范围

Project级别的写入、读取等流量限制失效。

处理方法

此类问题一般原因比较复杂，调查头绪比较多，无法提供统一的处理方法，请直接联系技术支持。

18.14 Alarm-02.600.0009.0001-metering service worker partition未全部load

metering service worker fuxi service partition没有全部load起来，该报警支持未load的partition数量。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	metering service worker	FuxiServiceSlsMeteringService

可能原因

原因复杂。

影响范围

用户计量数据丢失。

处理方法

此类问题一般原因比较复杂，调查头绪比较多，无法提供统一的处理方法，请直接联系技术支持。

18.15 Alarm-01.600.0010.0001-sls到ots replay数据太多

当文件数量大于300000，文件总长度大于1PB时报警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	replay worker	ToolService

可能原因

OTS故障。

影响范围

系统恢复后数据短时间内无法完全导入OTS，导致部分数据检索不到。

处理方法

此类问题一般原因比较复杂，调查头绪比较多，无法提供统一的处理方法，请直接联系技术支持。

18.16 Alarm-02.600.0011.0001-sls_web进程不存在

sls web进程未启动或者异常退出。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	sls web	WebServer

可能原因

异常退出或者未启动。

影响范围

给使用日志服务带来不便。

处理方法

此类问题一般原因比较复杂，调查头绪比较多，无法提供统一的处理方法，请直接联系技术支持。

18.17 Alarm-01.600.0011.0002-fastcgi 进程数量小于5

FastcgiAgent进程数量小于5。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	Fastcgi	WebServer

可能原因

异常退出或者未启动。

影响范围

落到该台机器上的用户请求会失败。

处理方法

1. 执行rm -f /var/www/html/heartbeat命令，摘掉机器心跳。
2. 执行sudo /etc/init.d/sls-fastcgid stop命令，停掉前端进程。
3. 执行sudo /etc/init.d/sls-fastcgid start命令，重新启动进程。
4. 执行sudo touch /var/www/html/heartbeat命令，touch心跳。
5. 联系技术支持。

18.18 Alarm-01.600.0011.0003-operation log中500请求数量超过阈值

http status是500的请求数量一分钟内大于1000个。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	Fastcgi	WebServer

可能原因

后端模块内部错误或者异常退出。

影响范围

部分用户请求返回非200。

处理方法

此类问题一般是后端系统能够故障引起，原因多样，请直接联系技术支持。

18.19 Alarm-02.600.0011.0004-nginx toa模块未加载

系统检测到toa模块未加载。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	nginx	WebServer

可能原因

未安装toa。

影响范围

无法正确解析用户请求的IP来源。

处理方法

安装toa模块，重启机器，并联系技术支持。

18.20 Alarm-02.600.0011.0005-机器上产生core文件

系统检测到机器上有core文件产生。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	OS	OS

可能原因

某模块异常退出。

影响范围

模块不可服务，如果是前端进程将会导致用户请求失败，后端进程可能会丢用户数据。

处理方法

产生core的可能是系统中的任意组件，无法提供统一的处理方法，因此需要详细调查，请直接联系技术支持。

19 云盾

19.1 beaver高级版和基础版

19.1.1 Alarm-01.401.0002.00001-内存使用率过高

超过内存使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	beaver_basic	yundun-beaver-basic

可能原因

存在内存泄漏或者请求数据大量增加。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到beaver basic所在机器：执行top命令，查看各进程内存占用情况。
2. 登录到beaver basic所在机器：查看*/var/log/messages*中的异常错误信息。
3. 联系技术支持。

19.1.2 Alarm-01.401.0002.00002-机器load过高

超过机器load阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	beaver_basic	yundun-beaver-basic

可能原因

存在请求数据大量增加或者CPU/IO使用过高的情况。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到beaver basic所在机器：执行top命令，查看各进程CPU占用情况，各进程信息。
2. 登录到beaver basic所在机器：查看*/var/log/messages*中的异常错误信息。
3. 联系技术支持。

19.1.3 Alarm-01.401.0002.00003-网络流量过高

超过网络流量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	beaver_basic	yundun-beaver-basic

可能原因

网络流量超过设计规格。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到beaver basic所在机器：执行cat /proc/ixgbe_debug_info命令，查看各业务网口的速率。
2. 如果速率确实超过阈值，考虑扩容beaver。

19.1.4 Alarm-01.401.0002.00004-CPU使用率过高

超过cput使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	beaver_basic	yundun-beaver-basic

可能原因

网络流量过大或者是进程异常。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到beaver basic所在机器：执行top命令，查看各进程CPU占用情况，各进程信息。
2. 登录到beaver basic所在机器：查看*/var/log/messages*中的异常错误信息。
3. 联系技术支持。

19.1.5 Alarm-01.402.0002.00001-内存使用率过高

超过内存使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	beaver_advance	yundun-beaver-advance

可能原因

存在内存泄漏或者请求数据大量增加。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到beaver advance所在机器：执行top命令，查看各进程内存占用情况。
2. 登录到beaver advance所在机器：查看*/var/log/messages*中的异常错误信息。
3. 联系技术支持。

19.1.6 Alarm-01.402.0002.00002-机器load过高

超过机器load阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	beaver_advance	yundun-beaver-advance

可能原因

存在请求数据大量增加或者CPU/IO使用过高的情况。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到beaver advance所在机器：执行topt命令，查看各进程CPU占用情况，各进程信息。
2. 登录到beaver advance所在机器：查看*/var/log/messages*中的异常错误信息。
3. 联系技术支持。

19.1.7 Alarm-01.402.0002.00003-网络流量过高

超过网络流量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	beaver_advance	yundun-beaver-advance

可能原因

网络流量超过设计规格。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到beaver advance所在机器：执行cat /proc/ixgbe_debug_info命令，查看各业务网口的速率。
2. 如果速率确实超过阈值，考虑扩容beaver。

19.1.8 Alarm-01.402.0002.00004-CPU使用率过高

超过CPU使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	beaver_advance	yundun-beaver-advance

可能原因

网络流量过大或者进程异常。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到beaver advance所在机器：执行top命令，查看各进程CPU占用情况，各进程信息。
2. 登录到beaver advance所在机器：查看*/var/log/messages*中的异常错误信息
3. 联系技术支持。

19.2 OPS-Console告警参考

19.2.1 Alarm-01.401.0003.00001-内存使用率过高

超过内存使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	opsconsole	yundun-opsconsole. BanffEmbassy

可能原因

存在内存泄漏或者请求数据大量增加。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到banff-embassy docker所在机器：通过jmap导出jvm堆信息。
2. 登录到banff-embassy docker所在机器：查看*/home/admin/banff-embassy/logs/banff.log*中的异常信息。
3. 收集*/home/admin/banff-embassy/logs/*目录下的所有日志，联系技术支持。

19.2.2 Alarm-01.401.0003.00002-机器load过高

超过机器load阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	opsconsole	yundun-opsconsole.BanffEmbassy

可能原因

存在请求数据大量增加或者CPU/IO使用过高的情况。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到banff-embassy docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，执行top命令后，按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到banff-embassy docker所在机器：查看*/home/admin/banff-embassy/logs/banff.log*中的异常信息。
3. 收集*/home/admin/banff-embassy/logs/*目录下的所有日志，联系技术支持。

19.2.3 Alarm-01.401.0003.00003-网络流量过高

超过网络流量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	opsconsole	yundun-opsconsole.BanffEmbassy

可能原因

存在请求数据大量增加或者docker非banff-embassy应用占用过高带宽。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到banff-embassy docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，执行top命令后，按shift -H将cpu、内存、io使用大的线程ID记录下来，通过iostat记录io消耗情况。
2. 登录到banff-embassy docker所在机器：查看*/home/admin/banff-embassy/logs/common-error.log*中的异常信息。
3. 收集*/home/admin/sas/logs/*目录下的所有日志，联系技术支持。

19.2.4 Alarm-01.401.0003.00004-CPU使用率过高

超过CPU使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	opsconsole	yundun-opsconsole.BanffEmbassy

可能原因

存在请求数据大量增加或者gc频繁或者死循环。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到banff-embassy docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，执行top命令后，按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到banff-embassy docker所在机器：查看*/home/admin/banff-embassy/logs/banff.log*中的异常信息。
3. 收集*/home/admin/banff-embassy/logs/*目录下的所有日志，联系技术支持。

19.2.5 Alarm-02.401.0003.00005-端口探测失败

检查docker中7001端口失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	opsconsole	yundun-opsconsole.BanffEmbassy

可能原因

应用异常退出或者应用启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到banff-embassy docker所在机器：查看*/home/admin/banff-embassy/logs/banff.log*中的异常信息。
2. 收集*/home/admin/banff-embassy/logs/*目录下的所有日志，联系技术支持。

19.2.6 Alarm-02.401.0003.00006-VIP探测失败

检查应用VIP 80端口失败，VIP不通。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	opsconsole	yundun-opsconsole.BanffEmbassy

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到banff-embassy docker所在机器：查看*/home/admin/banff-embassy/logs/common-error.log*中的异常信息。
2. 登录到banff-embassy docker所在机器： 执行`ps -ef | grep -i nginx`命令，是否存在。
3. 登录到banff-embassy docker所在机器：执行`curl 127.0.0.1/checkpreload.htm`命令，是否返回success。
4. 收集*/home/admin/banff-embassy/logs/*目录下的所有日志，联系技术支持。

19.2.7 Alarm-02.401.0003.00007-HTTP探测无响应

请求*/checkpreload.htm*地址未正常返回。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	opsconsole	yundun-opsconsole.BanffEmbassy

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到banff-embassy docker所在机器：查看*/home/admin/banff-embassy/logs/common-error.log*中的异常信息。
2. 登录到banff-embassy docker所在机器： 执行`ps -ef | grep -i nginx`命令，查看是否存在。
3. 登录到banff-embassy docker所在机器： 执行`curl 127.0.0.1/checkpreload.htm`命令，是否返回success。
4. 收集*/home/admin/banff-embassy/logs/*目录下的所有日志，联系技术支持。

19.2.8 Alarm-02.401.0003.00008-Url检查失败

请求*/checkpreload.htm*地址未返回Success。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	opsconsole	yundun-opsconsole.BanffEmbassy

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到banff-embassy docker所在机器：查看*/home/admin/banff-embassy/logs/common-error.log*中的异常信息。
2. 登录到banff-embassy docker所在机器：执行`ps -ef | grep -i nginx`命令，是否存在。
3. 登陆到banff-embassy docker所在机器：执行`curl 127.0.0.1/checkpreload.htm`命令，查看是否返回SUCCESS。
4. 收集*/home/admin/banff-embassy/logs/*目录下的所有日志，联系技术支持。

19.3 service-aegis告警参考

19.3.1 Alarm-01.401.0001.00001-内存使用率过高

超过内存使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士基础版	yundun-aegis.Aegiserverlite

可能原因

存在内存泄漏或者请求数据大量增加。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegiserverlite docker所在机器：通过jmap导出jvm堆信息。
2. 登录到aegiserverlite docker所在机器：查看*/home/admin/aegiserverlite/logs/aegis-default.log*中的异常信息。
3. 收集*/home/admin/aegiserverlite/logs/*目录下的所有日志，联系技术支持。

19.3.2 Alarm-01.401.0001.00002-机器load过高

超过机器load阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士基础版	yundun-aegis. Aegiserverlite

可能原因

存在请求数据大量增加或者CPU/IO使用过高的情况。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegiserverlite docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到aegiserverlite docker所在机器：查看*/home/admin/aegiserverlite/logs/aegis-default.log*中的异常信息。
3. 登录到aegiserverlite docker所在机器：查看*/home/admin/logs/AEGIS_MESSAGE.log*中协议上报数据量。
4. 收集*/home/admin/aegiserverlite/logs/*和*/home/admin/logs/*目录下的所有日志，联系技术支持。

19.3.3 Alarm-01.401.0001.00003-网络流量过高

超过网络流量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士基础版	yundun-aegis. Aegiserverlite

可能原因

存在请求数据大量增加或者docker非sas应用占用过高带宽。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegiserverlite docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到aegiserverlite docker所在机器：查看*/home/admin/aegiserverlite/logs/aegis-default.log*中的异常信息。
3. 登录到aegiserverlite docker所在机器：查看*/home/admin/logs/AEGIS_MESSAGE.log*中协议上报数据量。
4. 收集*/home/admin/aegiserverlite/logs/*和*/home/admin/logs/*目录下的所有日志，联系技术支持。

19.3.4 Alarm-01.401.0001.00004-CPU使用率过高

超过cput使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士基础版	yundun-aegis. Aegiserverlite

可能原因

存在请求数据大量增加或者gc频繁或者死循环。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegiserverlite docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后，按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到aegiserverlite docker所在机器：查看*/home/admin/aegiserverlite/logs/aegis-default.log*中的异常信息。
3. 登录到aegiserverlite docker所在机器：查看*/home/admin/logs/AEGIS_MESSAGE.log*中协议上报数据量。
4. 收集*/home/admin/aegiserverlite/logs/*和*/home/admin/logs/*目录下的所有日志，联系技术支持。

19.3.5 Alarm-02.401.0001.00005-端口探测失败

检查Docker中7001端口失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士基础版	yundun-aegis. Aegiserverlite

可能原因

应用异常退出或者应用启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录aegiserverlite docker所在机器：查看*/home/admin/aegiserverlite/logs/aegis-default.log*中的异常信息。
2. 收集*/home/admin/aegiserverlite/logs/*、*/home/admin/logs/*和*/home/admin/aegiserverlite/.default/logs/*目录下的所有日志，联系技术支持。

19.3.6 Alarm-02.401.0001.00006-vip探测失败

检查应用vip 80端口失败，VIP不通。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士基础版	yundun-aegis. Aegiserverlite

可能原因

应用异常退出或者应用启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegiserverlite docker所在机器：查看*/home/admin/aegiserverlite/logs/aegis-default.log*中的异常信息。
2. 登录到aegiserverlite docker所在机器：执行ps -ef | grep aegis 命令，查看是否存在。
3. 登录到aegiserverlite docker所在机器：执行telnet localhost 80命令，查看是否能连接通。
4. 收集*/home/admin/aegiserverlite/logs/*、*/home/admin/logs/*和*/home/admin/aegiserverlite/.default/logs/*目录下的所有日志，联系技术支持。

19.3.7 Alarm-02.401.0001.00007-HTTP探测无响应

请求/checkpreload.htm地址未正常返回。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士基础版	yundun-aegis. Aegiserverlite

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegiserverlite docker所在机器：查看*/home/admin/aegiserverlite/logs/aegis-default.log*中的异常信息。
2. 登录到aegiserverlite docker所在机器：执行`ps -ef | grep -i nginx`命令，查看是否存在。
3. 登录到aegiserverlite docker所在机器：执行`curl 127.0.0.1:8080/checkpreload.htm`命令，查看是否返回**success**。
4. 收集*/home/admin/aegiserverlite/logs/*、*/home/admin/logs/*和*/home/admin/aegiserverlite/.default/logs/*目录下的所有日志，联系技术支持。

19.3.8 Alarm-02.401.0001.00008-URL检查失败

请求/checkpreload.htm地址，未返回success。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士基础版	yundun-aegis.Aegiserverlite

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegiserverlite docker所在机器：查看*/home/admin/aegiserverlite/logs/aegis-default.log*中的异常信息。
2. 登录到aegiserverlite docker所在机器：执行`ps -ef | grep -i nginx`命令，查看是否存在。
3. 登录到aegiserverlite docker所在机器：执行`curl 127.0.0.1:8080/checkpreload.htm`命令，查看是否返回success。

4. 收集*/home/admin/aegiserverlite/logs/*、*/home/admin/logs/*和*/home/admin/aegiserverlite/.default/logs/*目录下的所有日志，联系技术支持。

19.3.9 Alarm-01.401.0001.00101-内存使用率过高

超过内存使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士基础版	yundun-aegis.Aegisupdatelite

可能原因

存在内存泄漏或者请求数据大量增加。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegisupdatelite docker所在机器：通过jmap导出jvm堆信息。
2. 登录到aegisupdatelite docker所在机器：查看*/home/admin/aegisupdatelite/logs/aegis-default.log*中的异常信息。
3. 收集*/home/admin/aegisupdatelite/logs/*目录下的所有日志，联系技术支持。

19.3.10 Alarm-01.401.0001.00102-机器load过高

超过机器load阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士基础版	yundun-aegis.Aegisupdatelite

可能原因

存在请求数据大量增加或者CPU/IO使用过高的情况。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegisupdatelite docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top后，按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到aegisupdatelite docker所在机器：查看*/home/admin/aegisupdatelite/logs/aegis-default.log*中的异常信息。
3. 登录到aegisupdatelite docker所在机器：查看*/home/admin/aegisupdatelite/logs/aegis-web-api-debug.log*中协议上报数据量。
4. 收集*/home/admin/aegisupdatelite/logs*目录下的所有日志，联系技术支持。

19.3.11 Alarm-01.401.0001.00103-网络流量过高

超过网络流量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士基础版	yundun-aegis.Aegisupdatelite

可能原因

存在请求数据大量增加或者docker非sas应用占用过高带宽。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegisupdatelite docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到aegisupdatelite docker所在机器：查看*/home/admin/aegisupdatelite/logs/aegis-default.log*中的异常信息。
3. 登录到aegisupdatelite docker所在机器：查看*/home/admin/aegisupdatelite/logs/aegis-web-api-debug.log*中协议上报数据量。
4. 收集*/home/admin/aegisupdatelite/logs*目录下的所有日志，联系技术支持。

19.3.12 Alarm-01.401.0001.00104-CPU使用率过高

超过cpu使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士基础版	yundun-aegis.Aegisupdatelite

可能原因

存在请求数据大量增加、gc频繁或者死循环。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegisupdatelite docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top后，按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到aegisupdatelite docker所在机器：查看*/home/admin/aegisupdatelite/logs/aegis-default.log*中的异常信息。
3. 登录到aegisupdatelite docker所在机器：查看*/home/admin/aegisupdatelite/logs/aegis-web-api-debug.log*中协议上报数据量。
4. 收集*/home/admin/aegisupdatelite/logs*目录下的所有日志，联系技术支持。

19.3.13 Alarm-02.401.0001.00105-端口探测失败

检查docker中7001端口失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士基础版	yundun-aegis.Aegisupdatelite

可能原因

应用异常退出或者应用启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录aegisupdatelite docker所在机器：查看*/home/admin/aegisupdatelite/logs/aegis-default.log*中的异常信息。
2. 收集*/home/admin/aegisupdatelite/logs/*和*/home/admin/aegisupdatelite/.default/logs/*目录下的所有日志，联系技术支持。

19.3.14 Alarm-02.401.0001.00106-VIP探测失败

检查应用VIP 80端口失败，VIP不通。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警		安骑士基础版	yundun-aegis. Aegisupdatelite

可能原因

应用异常退出或者应用启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegisupdatelite docker所在机器：查看*/home/admin/aegisupdatelite/logs/aegis-default.log*中的异常信息。
2. 登录到aegisupdatelite docker所在机器：执行`ps -ef | grep nginx`命令，查看是否存在。
3. 收集*/home/admin/aegisupdatelite/logs/*和*/home/admin/aegisupdatelite/.default/logs/*目录下的所有日志，联系技术支持。

19.3.15 Alarm-02.401.0001.00107-HTTP探测无响应

请求 /checkpreload.htm地址未正常返回。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士基础版	yundun-aegis. Aegisupdatelite

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegisupdatelite docker所在机器：查看*/home/admin/aegisupdatelite/logs/aegis-default.log*中的异常信息。
2. 登录到aegisupdatelite docker所在机器：执行`ps -ef | grep -i nginx`命令，查看是否存在。
3. 登录到aegisupdatelite docker所在机器：执行`curl 127.0.0.1/checkpreload.htm`命令，查看是否返回**success**。
4. 收集*/home/admin/aegisupdatelite/logs/*和*/home/admin/aegisupdatelite/.default/logs/*目录下的所有日志，联系技术支持。

19.3.16 Alarm-02.401.0001.00108-URL检查失败

请求/checkpreload.htm地址未返回success。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士基础版	yundun-aegis. Aegisupdatelite

可能原因

- 应用异常退出或者应用启动失败。

- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegisupdatelite docker所在机器：查看*/home/admin/aegisupdatelite/logs/aegis-default.log*中的异常信息。
2. 登录到aegisupdatelite docker所在机器：执行`ps -ef | grep -i nginx`命令，查看是否存在。
3. 登录到aegisupdatelite docker所在机器：执行`curl 127.0.0.1/checkpreload.htm`命令，查看是否返回success。
4. 收集*/home/admin/aegisupdatelite/logs/*和*/home/admin/aegisupdatelite/.default/logs/*目录下的所有日志，联系技术支持。

19.4 service-aegis-advance告警参考

19.4.1 Alarm-01.402.0006.00001-内存使用率过高

超过内存使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士高级版	yundun-aegisadvance.Aegiserver

可能原因

存在内存泄漏或者请求数据大量增加。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegiserver docker所在机器：通过jmap导出jvm堆信息。
2. 登录到aegiserver docker所在机器：查看*/home/admin/aegiserver/logs/common-error.log*中的异常信息。
3. 收集*/home/admin/aegiserver/logs/*目录下的所有日志，联系技术支持。

19.4.2 Alarm-01.402.0006.00002-机器load过高

超过机器load阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士高级版	yundun-aegisadvance.Aegiserver

可能原因

存在请求数据大量增加或者cpu/io使用过高的情况。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegiserver docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到aegiserver docker所在机器：查看*/home/admin/aegiserver/logs/common-error.log*中的异常信息。
3. 收集*/home/admin/sas/logs/*目录下的所有日志，联系技术支持。

19.4.3 Alarm-01.402.0006.00003-网络流量过高

超过网络流量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士高级版	yundun-aegisadvance.Aegiserver

可能原因

存在请求数据大量增加或者docker非sas应用占用过高带宽。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegiserver docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来，通过iostat记录io消耗情况。
2. 登录到aegiserver docker所在机器：查看*/home/admin/aegiserver/logs/common-error.log*中的异常信息。
3. 收集*/home/admin/aegiserver/logs/*目录下的所有日志，联系技术支持。

19.4.4 Alarm-01.402.0006.00004-CPU使用率过高

超过CPU使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士高级版	yundun-aegisadvance.Aegiserver

可能原因

存在请求数据大量增加或者gc频繁或者死循环。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegiserver docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top后，按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到aegiserver docker所在机器：查看*/home/admin/sas/logs/common-error.log*中的异常信息。
3. 收集*/home/admin/aegiserver/logs/*目录下的所有日志，联系技术支持。

19.4.5 Alarm-02.402.0006.00005-端口探测失败

检查docker中7001端口失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士高级版	yundun-aegisadvance.Aegiserver

可能原因

应用异常退出或者应用启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegiserver docker所在机器：查看*/home/admin/aegiserver/logs/common-error.log*中的异常信息。
2. 收集*/home/admin/aegiserver/logs/*目录下的所有日志，联系技术支持。

19.4.6 Alarm-02.402.0006.00006-VIP探测失败

检查应用VIP 80端口失败，VIP不通。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士高级版	yundun-aegisadvance.Aegiserver

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegiserver docker所在机器：查看*/home/admin/aegiserver/logs/common-error.log*中的异常信息。
2. 登录到aegiserver docker所在机器：执行`ps -ef | grep -i nginx`命令，查看是否存在。
3. 登录到aegiserver docker所在机器：执行`curl 127.0.0.1:8080/checkpreload.htm`命令，查看是否返回success。
4. 收集*/home/admin/aegiserver/logs/*目录下的所有日志，联系技术支持。

19.4.7 Alarm-02.402.0006.00007-HTTP探测无响应

请求 127.0.0.1:8080/checkpreload.htm地址未正常返回。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士高级版	yundun-aegisadvance.Aegiserver

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegiserver docker所在机器：查看*/home/admin/sas/logs/common-error.log*中的异常信息。
2. 登录到aegiserver docker所在机器：执行`ps -ef | grep -i nginx`命令，是否存在。
3. 登录到aegiserver docker所在机器：执行`curl 127.0.0.1:8080/checkpreload.htm`命令，查看是否返回success。
4. 收集*/home/admin/sas/logs/*目录下的所有日志，联系技术支持。

19.4.8 Alarm-02.402.0006.00008-URL检查失败

请求127.0.0.1:8080/checkpreload.htm地址未返回success。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士高级版	yundun-aegisadvance.Aegiserver

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegiserver docker所在机器：查看*/home/admin/aegiserver/logs/common-error.log*中的异常信息。
2. 登录到aegiserver docker所在机器：执行`ps -ef | grep -i nginx`命令，查看是否存在。
3. 登录到aegiserver docker所在机器：执行`127.0.0.1:8080/checkpreload.htm`命令，查看是否返回success。
4. 收集*/home/admin/sas/logs/*目录下的所有日志，联系技术支持。

19.4.9 Alarm-01.402.0006.00009-内存使用率过高

超过内存使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士高级版	yundun-aegisadvance.Defender

可能原因

存在内存泄漏或者请求数据大量增加。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到defender docker所在机器：通过jmap导出jvm堆信息。
2. 登录到defender docker所在机器：查看*/home/admin/defender/logs/defender-error.log*中的异常信息。
3. 收集*/home/admin/defender/logs/*目录下的所有日志，联系技术支持。

19.4.10 Alarm-01.402.0006.00010-机器load过高

超过机器load阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士高级版	yundun-aegisadvance.Defender

可能原因

存在请求数据大量增加或者CPU/IO使用过高的情况。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到defender docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到defender docker所在机器：查看*/home/admin/defender/logs/defender-error.log*中的异常信息。
3. 收集*/home/admin/defender/logs/*目录下的所有日志，联系技术支持。

19.4.11 Alarm-01.402.0006.00011-网络流量过高

超过网络流量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士高级版	yundun-aegisadvance.Defender

可能原因

存在请求数据大量增加或者docker非sas应用占用过高带宽。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到defender docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来，通过iostat记录io消耗情况。
2. 登录到defender docker所在机器：查看*/home/admin/defender/logs/defender-error.log*中的异常信息。
3. 收集*/home/admin/defender/logs/*目录下的所有日志，联系技术支持。

19.4.12 Alarm-01.402.0006.00012-CPU使用率过高

超过CPU使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士高级版	yundun-aegisadvance.Defender

可能原因

存在请求数据大量增加或者gc频繁或者死循环。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到defender docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来，通过iostat记录io消耗情况。
2. 登录到defender docker所在机器：查看*/home/admin/defender/logs/defender-error.log*中的异常信息。
3. 收集*/home/admin/defender/logs/*目录下的所有日志，联系技术支持。

19.4.13 Alarm-02.402.0006.00013-端口探测失败

检查docker中7001端口失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士高级版	yundun-aegisadvance.Defender

可能原因

应用异常退出或者应用启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到defender docker所在机器：查看*/home/admin/defender/logs/defender-error.log*中的异常信息。
2. 收集*/home/admin/defender/logs/*目录下的所有日志，联系技术支持。

19.4.14 Alarm-02.402.0006.00014-VIP探测失败

检查应用VIP 80端口失败，VIP不通。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士高级版	yundun-aegisadvance.Defender

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到defender docker所在机器：查看*/home/admin/defender/logs/defender-error.log*中的异常信息。
2. 登录到defender docker所在机器：执行ps -ef | grep -i nginx命令，查看是否存在。
3. 登录到defender docker所在机器：执行curl 127.0.0.1/securedefender/checkpreload.htm命令，查看是否返回success。
4. 收集*/home/admin/defender/logs/*目录下的所有日志，联系技术支持。

19.4.15 Alarm-02.402.0006.00015-HTTP探测无响应

请求127.0.0.1/securedefender/checkpreload.htm地址未正常返回。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士高级版	yundun-aegisadvance.Defender

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到defender docker所在机器：查看*/home/admin/defender/logs/defender-error.log*中的异常信息。
2. 登录到defender docker所在机器：执行ps -ef | grep -i nginx命令，查看是否存在。

3. 登录到defender docker所在机器：执行curl 127.0.0.1/securedefender/checkpreload.htm是否返回success。
4. 收集*/home/admin/defender/logs/*目录下的所有日志，联系技术支持。

19.4.16 Alarm-02.402.0006.00016-URL检查失败

请求/checkpreload.htm地址未返回success。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士高级版	yundun-aegisadvance.Defender

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到defender docker所在机器：查看*/home/admin/defender/logs/defender-error.log*中的异常信息。
2. 登录到defender docker所在机器：执行ps -ef | grep -i nginx 命令，查看是否存在。
3. 登录到defender docker所在机器：执行curl 127.0.0.1/securedefender/checkpreload.htm命令，查看是否返回success。
4. 收集*/home/admin/defender/logs/*目录下的所有日志，联系技术支持。

19.4.17 Alarm-01.402.0006.00017-内存使用率过高

超过内存使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士高级版	yundun-aegisadvance.AegisHealthCheck

可能原因

存在内存泄漏或者请求数据大量增加。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegis-health-check docker所在机器：通过jmap导出jvm堆信息。
2. 登录到sasapp docker所在机器：查看*/home/admin/aegis-health-check/logs/health-check-error.log*中的异常信息。
3. 收集*/home/admin/aegis-health-check/logs/*目录下的所有日志，联系技术支持。

19.4.18 Alarm-01.402.0006.00018-机器load过高

超过机器load阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士高级版	yundun-aegisadvance.AegisHealthCheck

可能原因

存在请求数据大量增加或者CPU/IO使用过高的情况。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegis-health-check docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到aegis-health-check docker所在机器：查看*/home/admin/aegis-health-check/logs/health-check-error.log*中的异常信息。
3. 收集*/home/admin/aegis-health-check/logs/*目录下的所有日志，联系技术支持。

19.4.19 Alarm-01.402.0006.00019-网络流量过高

超过网络流量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士高级版	yundun-aegisadvance.AegisHealthCheck

可能原因

存在请求数据大量增加或者docker非sas应用占用过高带宽。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到sasapp docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来，通过iostat记录io消耗情况。
2. 登录到sasapp docker所在机器：查看*/home/admin/sas/logs/common-error.log*中的异常信息。
3. 收集*/home/admin/sas/logs/*目录下的所有日志，联系技术支持。

19.4.20 Alarm-01.402.0006.00020-CPU使用率过高

超过CPU使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安骑士高级版	yundun-aegisadvance.AegisHealthCheck

可能原因

存在请求数据大量增加或者gc频繁或者死循环。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegis-health-check docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到aegis-health-check docker所在机器：查看*/home/admin/aegis-health-check/logs/health-check-error.log*中的异常信息。
3. 收集*/home/admin/aegis-health-check/logs/*目录下的所有日志，联系技术支持。

19.4.21 Alarm-02.402.0006.00021-端口探测失败

检查docker中7001端口失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士高级版	yundun-aegisadvance.AegisHealthCheck

可能原因

应用异常退出或者应用启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegis-health-check docker所在机器：查看*/home/admin/aegis-health-check/logs/health-check-error.log*中的异常信息。
2. 收集*/home/admin/aegis-health-check/logs/*目录下的所有日志，联系技术支持。

19.4.22 Alarm-02.402.0006.00022-VIP探测失败

检查应用VIP 80端口失败，VIP不通。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士高级版	yundun-aegisadvance.AegisHealthCheck

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegis-health-check docker所在机器：查看*/home/admin/aegis-health-check/logs/common-error.log*中的异常信息。
2. 登陆到aegis-health-check docker所在机器： ps -ef | grep -i nginx 是否存在；
3. 登录到aegis-health-check docker所在机器：执行curl 127.0.0.1/aegis-health-check/check_health命令，查看是否返回ok。
4. 收集*/home/admin/aegis-health-check/logs/*目录下的所有日志，联系技术支持。

19.4.23 Alarm-02.402.0006.00023-HTTP探测无响应

请求 curl 127.0.0.1/aegis-health-check/check_health地址未正常返回。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士高级版	yundun-aegisadvance.AegisHealthCheck

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegis-health-check docker所在机器：查看*/home/admin/aegis-health-check/logs/common-error.log*中的异常信息。
2. 登录到aegis-health-check docker所在机器：执行ps -ef | grep -i nginx命令，查看是否存在。

3. 登录到aegis-health-check docker所在机器：执行curl 127.0.0.1/aegis-health-check/check_health命令，查看是否返回ok。
4. 收集*/home/admin/aegis-health-check/logs/*目录下的所有日志，联系技术支持。

19.4.24 Alarm-02.402.0006.00024-URL检查失败

请求 curl 127.0.0.1/aegis-health-check/check_health地址未返回ok

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安骑士高级版	yundun-aegisadvance.AegisHealthCheck

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到aegis-health-check docker所在机器：查看*/home/admin/aegis-health-check/logs/common-error.log*中的异常信息。
2. 登录到aegis-health-check docker所在机器：执行ps -ef | grep -i nginx命令，查看是否存在。
3. 登录到aegis-health-check docker所在机器：执行curl 127.0.0.1/aegis-health-check/check_health命令，查看是否返回ok。
4. 收集*/home/admin/aegis-health-check/logs/*目录下的所有日志，联系技术支持。

19.5 advance_service-aliguard告警参考

19.5.1 Alarm-02.402.0007.00001-aliguard defender processes is running error, please check

aligaurd清洗进程出错。

告警信息

告警类型	告警级别	告警对象	告警模块
事件	P2	aliguard-defender	tianji-AligaurdDefender

可能原因

aliguard清洗进程down了。

影响范围

清洗服务不可用。

处理方法

执行如下命令，重启进程。

/home/admin/aliguard/target/AliguardDefender/bin/aliguard stop

/home/admin/aliguard/target/AliguardDefender/bin/aliguard start

如果无法解决，请联系专有云接口人或者参考问题排查文档。

19.5.2 Alarm-02.402.0007.00002-aliguard defender bgp config is error

aligaurd 清洗bgp出错。

告警信息

告警类型	告警级别	告警对象	告警模块
事件	P2	aliguard-defender	tianji-AligaurdDefender

可能原因

bgp网络问题。

影响范围

bgp牵引不可用。

处理方法

执行如下命令，重启进程 。

/home/admin/aliguard/target/AliguardDefender/bin/aliguard stop

/home/admin/aliguard/target/AliguardDefender/bin/aliguard start

如果无法解决，请联系专有云接口人或者参考问题排查文档。

19.5.3 Alarm-02.402.0007.00003-aliguard route config is error, please check

aliguard回注路由出错。

告警信息

告警类型	告警级别	告警对象	告警模块
事件	P2	aliguard-defender	tianji-AligaurdDefender

可能原因

回注网络问题。

影响范围

回注路由不可用。

处理方法

执行如下命令，重启进程。

/home/admin/aliguard/target/AliguardDefender/bin/aliguard stop

/home/admin/aliguard/target/AliguardDefender/bin/aliguard start

如果无法解决，请联系专有云接口人或者参考问题排查文档。

19.5.4 Alarm-02.402.0007.00004-aliguard monitor alarm

aligaurd监控脚本报警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件	P3	aliguard-defender	tianji-AligaurdDefender

可能原因

监控脚本down了。

影响范围

监控脚本不可用。

处理方法

执行如下命令，重启进程。

/home/admin/aliguard/target/AliguardDefender/bin/aliguard stop

/home/admin/aliguard/target/AliguardDefender/bin/aliguard start

如果无法解决，请联系专有云接口人或者参考问题排查文档。

19.5.5 Alarm-01.402.0007.00005-aliguardhost-cpu usage too high alarm

aliguard 利用率>90。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值	P3	aliguard-defender	tianji-AligaurdDefender

可能原因

CPU利用率太高。

影响范围

正常，无影响。

处理方法

不需要处理。

19.5.6 Alarm-02.402.0007.00006-aliguard console core process is running error, please check

aliguard console核心进程出错。

告警信息

告警类型	告警级别	告警对象	告警模块
事件	P2	aliguard-console	tianji-AligaurdConsole

可能原因

aligaurd console核心进程出错。

影响范围

aliguard console不可用。

处理方法

执行/home/admin/aliguard/target/AliguardConsole/bin/aligaurd_webconsole restart命令，重启进程。

19.5.7 Alarm-02.402.0007.00007-aliguard console tcp port is error, please check

aliguard console tcp 端口出错。

告警信息

告警类型	告警级别	告警对象	告警模块
事件	P2	aliguard-console	tianji-AligaurdConsole

可能原因

aliguard console tcp 端口出错。

影响范围

aliguard console不可用。

处理方法

执行/home/admin/aliguard/target/AliguardConsole/bin/aligaurd_webconsole restart命令，重启进程。

19.5.8 Alarm-02.402.0007.00008-subject|aliguard console monitor please check

aligaurd console监控脚本报警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件	P2	aliguard-console	tianji-AligaurdConsole

可能原因

aligaurd console监控脚本报警。

影响范围

监控脚本不可用。

处理方法

执行/home/admin/aliguard/target/AliguardConsole/bin/aligaurd_webconsole restart命令，重启进程。

19.5.9 Alarm-01.402.0007.00009-subject|aliguardhost-disk is too high

cpu 过高报警>90。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值	P3	aliguard-defender	tianji-AligaurdDefender

可能原因

CPU过高报警。

影响范围

正常，无影响。

19.5.10 Alarm-01.402.0007.00010-aliguardmaster-disk is too high

CPU过高报警>90。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值	P3	aliguard-console	tianji-AligaurdConsole

可能原因

CPU过高报警。

影响范围

正常，无影响。

19.5.11 Alarm-02.402.0007.00011-aliguardmaster-alarm

aliguardmaster-alarm。

告警信息

告警类型	告警级别	告警对象	告警模块
事件	P4	aliguard-console	tianji-AligaurdConsole

可能原因

aliguardmaster-alarm。

影响范围

正常，无影响。

19.6 advance_service-cactus告警参考

19.6.1 Alarm-01.402.0003.00001-内存使用率过高

超过内存使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	cactus	yundun-cactus. CactusKeeper

可能原因

存在内存泄漏或者请求数据大量增加。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到 cactus-batch docker所在机器：通过jmap导出jvm堆信息。
2. 登录到 cactus-batch docker所在机器：查看*/home/admin/logs/cactus-batch.log*中的异常信息。
3. 收集*/home/admin/logs/*目录下的所有日志，联系技术支持。

19.6.2 Alarm-01.402.0003.00002-机器load过高

超过机器load阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	cactus	yundun-cactus. CactusKeeper

可能原因

存在请求数据大量增加或者CPU/IO使用过高的情况。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到 cactus-batch docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到 cactus-batch docker所在机器：查看*/home/admin/logs/cactus-batch.log*中的异常信息。
3. 收集*/home/admin/logs/*目录下的所有日志，联系技术支持。

19.6.3 Alarm-01.402.0003.00003-网络流量过高

超过网络流量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	cactus	yundun-cactus.CactusKeeper

可能原因

存在请求数据大量增加或者docker非sas应用占用过高带宽。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到 cactus-batch docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来，通过iostat记录io消耗情况。
2. 登录到 cactus-batch docker所在机器：查看*/home/admin/logs/cactus-batch.log*中的异常信息。
3. 收集*/home/admin/logs/*目录下的所有日志，联系技术支持。

19.6.4 Alarm-01.402.0003.00004-CPU使用率过高

超过CPU使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	cactus	yundun-cactus.CactusKeeper

可能原因

存在请求数据大量增加或者gc频繁或者死循环。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到cactus-batch docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到 cactus-batch docker所在机器：查看*/home/admin/logs/cactus-batch.log*中的异常信息。
3. 收集*/home/admin/logs/*目录下的所有日志，联系技术支持。

19.6.5 Alarm-02.402.0003.00005-端口探测失败

检查docker中7001端口失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	cactus	yundun-cactus.CactusKeeper

可能原因

应用异常退出或者应用启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到 cactus-batch docker所在机器：查看*/home/admin/logs/cactus-batch.log*中的异常信息。
2. 收集*/home/admin/logs/*目录下的所有日志，联系技术支持。

19.6.6 Alarm-02.402.0003.00006-VIP探测失败

检查应用VIP 80端口失败，VIP不通。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	cactus	yundun-cactus.CactusKeeper

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到cactus-batch docker所在机器：查看*/home/admin/logs/cactus-batch.log*中的异常信息。
2. 登录到 cactus-batch docker所在机器：执行ps -ef | grep -i nginx命令，查看是否存在。
3. 登录到cactus-batch docker所在机器：执行curl 127.0.0.1/checkpreload.htm命令，查看是否返回success。
4. 收集*/home/admin/logs/*目录下的所有日志，联系技术支持。

19.6.7 Alarm-02.402.0003.00007-HTTP探测无响应

请求/checkpreload.htm地址未正常返回。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	cactus	yundun-cactus.CactusKeeper

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到 cactus-batch docker所在机器：查看*/home/admin/logs/cactus-batch.log*中的异常信息。
2. 登录到 cactus-batch docker所在机器：执行ps -ef | grep -i nginx命令，查看是否存在。
3. 登录到cactus-batch docker所在机器：执行curl 127.0.0.1/checkpreload.htm命令，查看是否返回success。
4. 收集*/home/admin/logs/*目录下的所有日志，联系技术支持。

19.6.8 Alarm-02.402.0003.00008-URL检查失败

请求/checkpreload.htm地址未返回success。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	cactus	yundun-cactus.CactusKeeper

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到 cactus-batch docker所在机器：查看*/home/admin/logs/cactus-batch.log*中的异常信息。
2. 登录到 cactus-batch docker所在机器：执行`ps -ef | grep -i nginx`命令，查看是否存在。
3. 登录到 cactus-batch docker所在机器：执行`curl 127.0.0.1/checkpreload.htm`命令，查看是否返回success。
4. 收集*/home/admin/logs/*目录下的所有日志，联系技术支持。

19.7 yundun-advance_service-sas告警参考

19.7.1 Alarm-01.402.0001.00001-内存使用率过高

超过内存使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	态势感知	yundun-sas.SasApp

可能原因

存在内存泄漏或者请求数据大量增加。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到sasapp docker所在机器：通过jmap导出jvm堆信息。
2. 登录到sasapp docker所在机器：查看*/home/admin/sas/logs/common-error.log*中的异常信息。
3. 收集*/home/admin/sas/logs/*目录下的所有日志，联系技术支持。

19.7.2 Alarm-01.402.0001.00002-机器load过高

超过机器load阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	态势感知	yundun-sas.SasApp

可能原因

存在请求数据大量增加或者CPU/IO使用过高的情况。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到sasapp docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到sasapp docker所在机器：查看*/home/admin/sas/logs/common-error.log*中的异常信息。
3. 收集*/home/admin/sas/logs/*目录下的所有日志，联系技术支持。

19.7.3 Alarm-01.402.0001.00003-网络流量过高

超过网络流量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	态势感知	yundun-sas.SasApp

可能原因

存在请求数据大量增加或者Docker非sas应用占用过高带宽。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到sasapp docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来，通过iostat记录io消耗情况。
2. 登录到sasapp docker所在机器：查看*/home/admin/sas/logs/common-error.log*中的异常信息。
3. 收集*/home/admin/sas/logs/*目录下的所有日志，联系技术支持。

19.7.4 Alarm-01.402.0001.00004-CPU使用率过高

超过CPU使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	态势感知	yundun-sas.SasApp

可能原因

存在请求数据大量增加或者gc频繁或者死循环。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到sasapp docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到sasapp docker所在机器：查看*/home/admin/sas/logs/common-error.log*中的异常信息。
3. 收集*/home/admin/sas/logs/*目录下的所有日志，联系技术支持。

19.7.5 Alarm-02.402.0001.00005-端口探测失败

检查Docker中7001端口失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	态势感知	yundun-sas.SasApp

可能原因

应用异常退出或者应用启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到sasapp docker所在机器：查看*/home/admin/sas/logs/common-error.log*中的异常信息。
2. 收集*/home/admin/sas/logs/*目录下的所有日志，联系技术支持。

19.7.6 Alarm-02.402.0001.00006-VIP探测失败

检查应用VIP 80端口失败，VIP不通。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	态势感知	yundun-sas.SasApp

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到sasapp docker所在机器：查看*/home/admin/sas/logs/common-error.log*中的异常信息。
2. 登录到sasapp docker所在机器：执行`ps -ef | grep -i nginx`，查看进程是否存在。

3. 登录到sasapp docker所在机器：执行curl 127.0.0.1/checkpreload.htm命令，查看是否返回success。
4. 收集*/home/admin/sas/logs/*目录下的所有日志，联系技术支持。

19.7.7 Alarm-02.402.0001.00007-HTTP探测无响应

请求 /checkpreload.htm地址未正常返回。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	态势感知	yundun-sas.SasApp

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到sasapp docker所在机器：查看*/home/admin/sas/logs/common-error.log*中的异常信息。
2. 登录到sasapp docker所在机器：执行ps -ef | grep -i nginx命令，查看进程是否存在。
3. 登录到sasapp docker所在机器：执行curl 127.0.0.1/checkpreload.htm命令，查看是否返回success。
4. 收集*/home/admin/sas/logs/*目录下的所有日志，联系技术支持。

19.7.8 Alarm-02.402.0001.00008-URL检查失败

请求 /checkpreload.htm地址未返回success。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	态势感知	yundun-sas.SasApp

可能原因

- 应用异常退出或者应用启动失败。

- tengine启动失败。

影响范围

- 对整个服务的所有功能都会有影响，建议立即排查

处理方法

1. 登录到sasapp docker所在机器：查看*/home/admin/sas/logs/common-error.log*中的异常信息。
2. 登录到sasapp docker所在机器：执行`ps -ef | grep -i nginx`命令，查看进程是否存在。
3. 登录到sasapp docker所在机器：执行`curl 127.0.0.1/checkpreload.htm`命令，查看是否返回success。
4. 收集*/home/admin/sas/logs/*目录下的所有日志，联系技术支持。

19.8 advance_service-secure-console告警参考

19.8.1 Alarm-01.402.0004.00001-内存使用率过高

超过内存使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	云盾高级版控制台	yundun-secureconsole.SecureConsoleApp

可能原因

存在内存泄漏或者请求数据大量增加。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到secureconsoleapp docker所在机器：通过jmap导出jvm堆信息。
2. 登录到secureconsoleapp docker所在机器：查看*/home/admin/console/logs/applog/yundun-error.log*中的异常信息。
3. 收集*/home/admin/console/logs/*目录下的所有日志，联系技术支持。

19.8.2 Alarm-01.402.0004.00002-机器load过高

超过机器load阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	云盾高级版控制台	yundun-secureconsole .SecureConsoleApp

可能原因

存在请求数据大量增加或者CPU/IO使用过高的情况。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到secureconsoleapp docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到secureconsoleapp docker所在机器：查看*/home/admin/console/logs/applog/yundun-error.log*中的异常信息。
3. 收集*/home/admin/console/logs/*目录下的所有日志，联系技术支持。

19.8.3 Alarm-01.402.0004.00003-网络流量过高

超过网络流量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	云盾高级版控制台	yundun-secureconsole .SecureConsoleApp

可能原因

存在请求数据大量增加或者Docker非secureconsole应用占用过高带宽。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到secureconsoleapp docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来，通过iostat记录io消耗情况。
2. 登录到secureconsoleapp docker所在机器：查看*/home/admin/console/logs/applog/yundun-error.log*中的异常信息。
3. 收集*/home/admin/console/logs/*目录下的所有日志，联系技术支持。

19.8.4 Alarm-01.402.0004.00004-CPU使用率过高

超过CPU使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	云盾高级版控制台	yundun-secureconsole.SecureConsoleApp

可能原因

存在请求数据大量增加或者gc频繁或者死循环。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到sasapp docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到secureconsoleapp docker所在机器：查看*/home/admin/console/logs/applog/yundun-error.log*中的异常信息。
3. 收集*/home/admin/console/logs/*目录下的所有日志，联系技术支持。

19.8.5 Alarm-02.402.0004.00005-端口探测失败

检查Docker中7001端口失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	云盾高级版控制台	yundun-secureconsole .SecureConsoleApp

可能原因

应用异常退出或者应用启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到secureconsoleapp docker所在机器：查看*/home/admin/console/logs/applog/yundun-error.log*中的异常信息。
2. 收集*/home/admin/console/logs/*目录下的所有日志，联系技术支持。

19.8.6 Alarm-02.402.0004.00006-VIP探测失败

检查应用VIP 80端口失败，VIP不通。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	云盾高级版控制台	yundun-secureconsole .SecureConsoleApp

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到secureconsoleapp docker所在机器：查看*/home/admin/console/logs/applog/yundun-error.log*中的异常信息。
2. 登录到secureconsoleapp docker所在机器：执行`ps -ef | grep -i nginx`命令，查看进程是否存在。
3. 登录到secureconsoleapp docker所在机器：执行`curl 127.0.0.1/check.htm`命令，查看是否返回OK。
4. 收集*/home/admin/console/logs/*目录下的所有日志，联系技术支持。

19.8.7 Alarm-02.402.0004.00007-HTTP探测无响应

请求 /check.htm地址未正常返回。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	云盾高级版控制台	yundun-secureconsole.SecureConsoleApp

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到secureconsoleapp docker所在机器：查看*/home/admin/console/logs/applog/yundun-error.log*中的异常信息。
2. 登录到secureconsoleapp docker所在机器：执行`ps -ef | grep -i nginx`命令，查看进程是否存在。
3. 登录到secureconsoleapp docker所在机器：执行`curl 127.0.0.1/check.htm`命令，查看是否返回success。
4. 收集*/home/admin/console/logs/*目录下的所有日志，联系技术支持。

19.8.8 Alarm-02.402.0004.00008-URL检查失败

请求 /check.htm地址未返回OK。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	云盾高级版控制台	yundun-secureconsole.SecureConsoleApp

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到secureconsoleapp docker所在机器：查看*/home/admin/console/logs/applog/yundun-error.log*中的异常信息。
2. 登录到secureconsoleapp docker所在机器：执行`ps -ef | grep -i nginx`命令，查看进程是否存在。
3. 登录到secureconsoleapp docker所在机器：执行`curl 127.0.0.1/check.htm`命令，查看是否返回OK。
4. 收集*/home/admin/console/logs/*目录下的所有日志，联系技术支持。

19.9 advance_service-secure-service告警参考

19.9.1 Alarm-01.402.0005.00001-内存使用率过高

超过内存使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	云盾高级版SecureService	yundun-secureservice.SecureServiceApp

可能原因

存在内存泄漏或者请求数据大量增加。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到secureserviceapp docker所在机器：通过jmap导出jvm堆信息。
2. 登录到secureserviceapp docker所在机器：查看*/home/admin/secureservice/logs/ERROR*中的异常信息。
3. 收集*/home/admin/secureservice/logs/*目录下的所有日志，联系技术支持。

19.9.2 Alarm-01.402.0005.00002-机器load过高

超过机器load阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	云盾高级版 SecureService	yundun-secureservice. SecureServiceApp

可能原因

存在请求数据大量增加或者CPU/IO使用过高的情况。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到secureserviceapp docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到secureserviceapp docker所在机器：查看*/home/admin/secureservice/logs/ERROR*中的异常信息。
3. 收集*/home/admin/secureservice/logs/*目录下的所有日志，联系技术支持。

19.9.3 Alarm-01.402.0005.00003-网络流量过高

超过网络流量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	云盾高级版 SecureService	yundun-secureservice.SecureServiceApp

可能原因

存在请求数据大量增加或者Docker非secureservice应用占用过高带宽。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到secureserviceapp docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来，通过iostat记录io消耗情况。
2. 登录到secureserviceapp docker所在机器：查看*/home/admin/secureservice/logs/ERROR*中的异常信息。
3. 收集*/home/admin/secureservice/logs/*目录下的所有日志，联系技术支持。

19.9.4 Alarm-01.402.0005.00004-CPU使用率过高

超过CPU使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	云盾高级版 SecureService	yundun-secureservice.SecureServiceApp

可能原因

存在请求数据大量增加或者GC频繁或者死循环。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到secureserviceapp docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 登录到secureserviceapp docker所在机器：查看*/home/admin/secureservice/logs/ERROR*中的异常信息。
3. 收集*/home/admin/secureservice/logs/*目录下的所有日志，联系技术支持。

19.9.5 Alarm-02.402.0005.00005-端口探测失败

检查docker中7001端口失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	云盾高级版 SecureService	yundun-secureservice. SecureServiceApp

可能原因

应用异常退出或者应用启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到secureserviceapp docker所在机器：查看*/home/admin/secureservice/logs/ERROR*中的异常信息。
2. 收集*/home/admin/secureservice/logs/*目录下的所有日志，联系技术支持。

19.9.6 Alarm-02.402.0005.00006-VIP探测失败

检查应用VIP 80端口失败，VIP不通。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	云盾高级版 SecureService	yundun-secureservice. SecureServiceApp

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到secureserviceapp docker所在机器：查看*/home/admin/secureservice/logs/ERROR*中的异常信息。
2. 登录到secureserviceapp docker所在机器：执行ps -ef | grep -i nginx命令，查看进程是否存在。
3. 登录到secureserviceapp docker所在机器：执行curl 127.0.0.1命令，查看是否返回OK。
4. 收集*/home/admin/secureservice/logs/*目录下的所有日志，联系技术支持。

19.9.7 Alarm-02.402.0005.00007-HTTP探测无响应

请求 /index.jsp地址未正常返回。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	云盾高级版 SecureService	yundun-secureservice. SecureServiceApp

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到secureserviceapp docker所在机器：查看*/home/admin/secureservice/logs/ERROR*中的异常信息。
2. 登录到secureserviceapp docker所在机器：执行ps -ef | grep -i nginx命令，查看进程是否存在。

3. 登录到secureserviceapp docker所在机器：执行curl 127.0.0.1/index.jsp命令，查看是否返回OK。
4. 收集*/home/admin/secureservice/logs/*目录下的所有日志，联系技术支持。

19.9.8 Alarm-02.402.0005.00008-URL检查失败

请求 /index.jsp地址未返回OK。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	云盾高级版 SecureService	yundun-secureservice. SecureServiceApp

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到secureserviceapp docker所在机器：查看*/home/admin/secureservice/logs/ERROR*中的异常信息。
2. 登录到secureserviceapp docker所在机器：执行ps -ef | grep -i nginx命令，查看进程是否存在。
3. 登录到secureserviceapp docker所在机器：执行curl 127.0.0.1/index.jsp命令，查看是否返回OK。
4. 收集*/home/admin/secureservice/logs/*目录下的所有日志，联系技术支持。

19.10 common_service-security-auditlog告警参考

19.10.1 Alarm-01.400.0001.00001-内存使用率过高

超过内存使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安全审计	yundun-security-auditlog.security-auditlog-app

可能原因

存在内存泄漏或者请求数据大量增加。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到security-auditlog-app docker所在机器：通过jmap导出jvm堆信息。
2. 查看*/home/admin/security-auditlog/logs/*目录下的异常信息：
   - main.log：默认日志。
   - system-error.log：系统错误日志。
   - biz-error.log：业务错误日志。
   - check-error.log：校验错误日志。
   - remote-exec.log：远程调用日志。
   - service-exec.log：OpenApi调用和错误日志。
   - job-exec.log：定时任务执行和错误日志。
   - task-exec.log：异步任务执行和错误日志，包括下载任务。
   - audit-exec.log：审计日志。
3. 收集*/home/admin/security-auditlog/logs/*目录下的所有日志，联系技术支持。

19.10.2 Alarm-01.400.0001.00002-机器Load过高

超过机器Load阈值

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安全审计	yundun-security-auditlog.security-auditlog-app

可能原因

存在请求数据大量增加或者cpu/io使用过高的情况。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到security-auditlog-app docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 查看*/home/admin/security-auditlog/logs/*目录下的异常信息：
   - main.log：默认日志。
   - system-error.log：系统错误日志。
   - biz-error.log：业务错误日志。
   - check-error.log：校验错误日志。
   - remote-exec.log：远程调用日志。
   - service-exec.log：OpenApi调用和错误日志。
   - job-exec.log：定时任务执行和错误日志。
   - task-exec.log：异步任务执行和错误日志，包括下载任务。
   - audit-exec.log：审计日志。
3. 收集*/home/admin/security-auditlog/logs/*目录下的所有日志，联系技术支持。

19.10.3 Alarm-01.400.0001.00003-网络流量过高

超过网络流量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安全审计	yundun-security-auditlog.security-auditlog-app

可能原因

存在请求数据大量增加或者Docker非security-auditlog应用占用过高带宽。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到security-auditlog-app docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来，通过iostat记录io消耗情况。
2. 查看*/home/admin/security-auditlog/logs/*目录下的异常信息：
   - main.log：默认日志。
   - system-error.log：系统错误日志。
   - biz-error.log：业务错误日志。
   - check-error.log：校验错误日志。
   - remote-exec.log：远程调用日志。
   - service-exec.log：OpenApi调用和错误日志。
   - job-exec.log：定时任务执行和错误日志。
   - task-exec.log：异步任务执行和错误日志，包括下载任务。
   - audit-exec.log：审计日志。
3. 收集*/home/admin/security-auditlog/logs/*目录下的所有日志，联系技术支持。

19.10.4 Alarm-01.400.0001.00004-CPU使用率过高

超过CPU使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安全审计	yundun-security-auditlog.security-auditlog-app

可能原因

存在请求数据大量增加或者GC频繁或者死循环。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到security-auditlog-app docker所在机器：查看内存、cpu、io使用情况，通过jstack导出线程运行栈信息，top 后按shift -H将cpu、内存、io使用大的线程ID记录下来。
2. 查看/home/admin/security-auditlog/logs/目录下的异常信息：
   - main.log：默认日志。
   - system-error.log：系统错误日志。
   - biz-error.log：业务错误日志。
   - check-error.log：校验错误日志。
   - remote-exec.log：远程调用日志。
   - service-exec.log：OpenApi调用和错误日志。
   - job-exec.log：定时任务执行和错误日志。
   - task-exec.log：异步任务执行和错误日志，包括下载任务。
   - audit-exec.log：审计日志。
3. 收集*/home/admin/security-auditlog/logs/*目录下的所有日志，联系技术支持。

19.10.5 Alarm-02.400.0001.00005-端口探测失败

检查docker中7001端口失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安全审计	yundun-security-auditlog.security-auditlog-app

可能原因

应用异常退出或者应用启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到security-auditlog-app docker所在机器：查看/home/admin/security-auditlog/logs/目录下的异常信息：
   - main.log：默认日志。
   - system-error.log：系统错误日志。
   - biz-error.log：业务错误日志。
   - check-error.log：校验错误日志。
   - remote-exec.log：远程调用日志。
   - service-exec.log：OpenApi调用和错误日志。
   - job-exec.log：定时任务执行和错误日志。
   - task-exec.log：异步任务执行和错误日志，包括下载任务。
   - audit-exec.log：审计日志。
2. 收集*/home/admin/security-auditlog/logs/*目录下的所有日志，联系技术支持。

19.10.6 Alarm-02.400.0001.00006-VIP探测失败

检查应用VIP 80端口失败，VIP不通。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安全审计	yundun-security-auditlog.security-auditlog-app

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到security-auditlog-app docker所在机器：执行`ps -ef | grep -i nginx`命令，查看进程是否存在。
2. 执行`curl 127.0.0.1/checkpreload.htm`命令，查看是否返回success。
3. 查看*/home/admin/security-auditlog/logs/*目录下的异常信息：
   - main.log：默认日志。
   - system-error.log：系统错误日志。
   - biz-error.log：业务错误日志。
   - check-error.log：校验错误日志。
   - remote-exec.log：远程调用日志。
   - service-exec.log：OpenApi调用和错误日志。
   - job-exec.log：定时任务执行和错误日志。
   - task-exec.log：异步任务执行和错误日志，包括下载任务。
   - audit-exec.log：审计日志。
4. 收集*/home/admin/security-auditlog/logs/*目录下的所有日志，联系技术支持。

19.10.7 Alarm-02.400.0001.00007-HTTP探测无响应

请求/checkpreload.htm地址未正常返回。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安全审计	yundun-security-auditlog.security-auditlog-app

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到security-auditlog-app docker所在机器：执行`ps -ef | grep -i nginx`命令，查看进程是否存在。
2. 执行`curl 127.0.0.1/checkpreload.htm`命令，查看是否返回success。
3. 查看*/home/admin/security-auditlog/logs/*目录下的异常信息：
   - main.log：默认日志。
   - system-error.log：系统错误日志。
   - biz-error.log：业务错误日志。
   - check-error.log：校验错误日志。
   - remote-exec.log：远程调用日志。
   - service-exec.log：OpenApi调用和错误日志。
   - job-exec.log：定时任务执行和错误日志。
   - task-exec.log：异步任务执行和错误日志，包括下载任务。
   - audit-exec.log：审计日志。
4. 收集*/home/admin/security-auditlog/logs/*目录下的所有日志，联系技术支持。

19.10.8 Alarm-02.400.0001.00008-URL检查失败

请求 /checkpreload.htm地址未返回Success。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安全审计	yundun-security-auditlog.security-auditlog-app

可能原因

- 应用异常退出或者应用启动失败。
- tengine启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到security-auditlog-app docker所在机器：执行`ps -ef | grep -i nginx`命令，查看进程是否存在。
2. 执行`curl 127.0.0.1/checkpreload.htm`命令，查看是否返回success。
3. 查看*/home/admin/security-auditlog/logs/*目录下的异常信息：
   - main.log：默认日志。
   - system-error.log：系统错误日志。
   - biz-error.log：业务错误日志。
   - check-error.log：校验错误日志。
   - remote-exec.log：远程调用日志。
   - service-exec.log：OpenApi调用和错误日志。
   - job-exec.log：定时任务执行和错误日志。
   - task-exec.log：异步任务执行和错误日志，包括下载任务。
   - audit-exec.log：审计日志。
4. 收集*/home/admin/security-auditlog/logs/*目录下的所有日志，联系技术支持。

19.10.9 Alarm-01.400.0001.00101-内存使用率过高

超过内存使用量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安全审计	yundun-security-auditlog.security-auditlog-syslog

可能原因

存在内存泄漏或者写入日志量过大。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到security-auditlog-syslog docker所在机器。
2. 查看*/home/log-store*目录下的日志文件，查看日志文件大小，联系技术支持。

19.10.10 Alarm-01.400.0001.00102-机器Load过高

超过机器Load阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安全审计	yundun-security-auditlog.security-auditlog-syslog

可能原因

写入日志量过大或者cpu/io使用过高的情况。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到security-auditlog-syslog docker所在机器。

2. 查看*/home/log-store*目录下的日志文件，查看日志文件大小，联系技术支持。

19.10.11 Alarm-01.400.0001.00103-网络流量过高

超过网络流量阈值。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安全审计	yundun-security-auditlog.security-auditlog-syslog

可能原因

写入日志量过大或者Docker非security-auditlog应用占用过高带宽。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到security-auditlog-syslog docker所在机器。
2. 查看*/home/log-store*目录下的日志文件，查看日志文件大小，联系技术支持。

19.10.12 Alarm-01.400.0001.00104-CPU使用率过高

超过CPU使用量阈值

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	-	安全审计	yundun-security-auditlog.security-auditlog-syslog

可能原因

写入日志量过大。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到security-auditlog-syslog docker所在机器。
2. 登录到security-auditlog-syslog docker所在机器：查看*/home/log-store*目录下的日志文件，查看日志文件大小，联系技术支持。

19.10.13 Alarm-02.400.0001.00105-端口探测失败

检查docker中514、2514端口失败。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安全审计	yundun-security-auditlog.security-auditlog-syslog

可能原因

syslog-ng程序异常退出或者启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到security-auditlog-syslog docker所在机器。
2. 执行ps -ef | grep syslog-ng命令，查看syslog-ng进程是否存在。
3. 执行如下命令，查看514、2514两个端口是否存在。

   `netstat -ano | grep 514`

   `netstat -ano | grep 2514`

19.10.14 Alarm-02.400.0001.00106-VIP探测失败

检查应用VIP 514、2514端口失败，VIP不通。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	安全审计	yundun-security-auditlog.security-auditlog-syslog

可能原因

syslog-ng程序异常退出或者启动失败。

影响范围

对整个服务的所有功能都会有影响，建议立即排查。

处理方法

1. 登录到security-auditlog-syslog docker所在机器。
2. 执行ps -ef | grep syslog-ng命令，查看syslog-ng进程是否存在。
3. 执行如下命令，查看514、2514两个端口是否存在。

   `netstat -ano | grep 514`

   `netstat -ano | grep 2514`

20 密钥管理服务KMS

20.1 Alarm-02.495.0004.00001-数据同步监控错误

主备部署状态下，当备集群没有及时同步主集群数据时，触发报警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	kms	kms.Rotator#

可能原因

- 主、备集群网络不通。
- 备集群 ETCD 出现异常。

处理方法

- 如果是网络原因，待主、备网络恢复后，观察一段时间，如果不再报警，则说明已经自动恢复。
- 如果非网络原因，请联系技术支持人员。

20.2 Alarm-02.495.0004.00002-数据同步出现错误

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P1	kms	kms.Rotator#

可能原因

- 主、备集群网络不通。
- 主集群HSA 或 ETCD 出现异常。
- 备集群Rotator 或 ETCD出现异常。

处理方法

- 如果是网络原因，待主、备网络恢复后，观察一段时间，如果不再报警，则说明已经自动恢复。
- 如果非网络原因，请联系技术支持人员。

20.3 Alarm-02.495.0002.00001-HSA出现Panic错误

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	kms	kms.HSA#

可能原因

运行时的BUG。

处理方法

保存*/cloud/log/kms/HSA#/hsa/*路径下的log后，联系技术支持人员。

20.4 Alarm-02.495.0001.00001-KMS出现Panic错误

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	kms	kms.KmsHost#

可能原因

运行时的BUG。

处理方法

保存/cloud/log/kms/KmsHost#/kms_host/路径下的log后，联系技术支持人员。

20.5 Alarm-02.495.0003.00001-ETCD发生严重错误

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	kms	kms.Etcd#

可能原因

TPM相关出现异常。

处理方法

情况较复杂，请保留机器现场，联系技术支持人员。

20.6 Alarm-02.495.0002.00002-HSA发生严重警告错误

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P2	kms	kms.HSA#

可能原因

- KMS 数据库数据受到篡改。
- 来自非KMS的 HSA API访问。
- ETCD中数据出现异常。

处理方法

情况较复杂，请保留机器现场，联系技术支持人员。

20.7 Alarm-02.495.0001.00002-KMS响应出现500错误

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P3	kms	kms.KmsHost#

可能原因

- KMS 处理请求时，依赖的服务出现了预期以外的异常。
- KMS 处理请求时，产生了预期之外的BUG。

处理方法

记录报警中的**request_id**，并联系技术支持人员。

20.8 Alarm-02.495.0004.00003-Rotator删除Key时发生错误

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P4	kms	kms.Rotator#

可能原因

Rotator访问数据出现异常。

处理方法

确认kms的数据库访问是否正常：

- 如果数据库不正常，先恢复数据库。
- 如果数据库正常，请联系技术支持人员。

20.9 Alarm-02.495.0005.00001-kms server role出现异常

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	P3	kms	kms.ServerroleMonitor#

可能原因

KMS服务的ServerRole有节点处于异常状态。

处理方法

1. 确认kms服务是否存在rolling情况。

   如果是，请确认rolling时间是否过长，或rolling的新版本是否已经失败。

   如果是rolling导致的报警，先中断rolling任务，再使用之前正常的版本进行回滚。

2. 重启异常的serverrole。

   如果重启以后依然存在报警，请联系技术支持人员。

3. 如果收到 kms server role 恢复正常的报警，说明异常情况已经恢复。

21 大数据开发套件

21.1 01.505.0003.00003-port_7001

nc检查tomcat服务端口7001，如果端口服务异常，则出现告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(p2)	base产品下列模块： • BaseBizBaseapi • BaseBizCdp • BaseBizCommonbase • BaseBizConsole • BaseBizDfs • BaseBizDmc • BaseBizDqcexecutor • BaseBizDqcsupervisor • BaseBizMetaservice • BaseBizPhoenix • BaseBizSso • BaseBizTenant • BaseBizWkbench	软件对应天基的service role或者service

可能原因

- 应用服务异常或主机异常。

影响范围

服务单点，若同一个模块两个服务均异常，则base服务不可用。

处理方法

到大数据管家base分站重启异常应用进程。

21.2 01.505.0002.00002-http_80

nc检查nginx服务端口80，如果端口服务异常，则出现告警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(p2)	base产品下列模块： • BaseBizBaseapi • BaseBizCdp • BaseBizCommonbase • BaseBizConsole • BaseBizDfs • BaseBizDmc • BaseBizDqcexecutor • BaseBizDqcsupervisor • BaseBizMetaservice • BaseBizPhoenix • BaseBizSso • BaseBizTenant • BaseBizWkbench	软件对应天基的service role或者service

可能原因

应用服务异常，或主机异常。

影响范围

服务单点，若同一个模块两个服务均异常，则base服务不可用。

处理方法

到大数据管家base分站重启异常应用进程。

21.3 02.505.0001.00001-df_home

检查磁盘home目录使用率，当磁盘使用率大于85%，则预警出来，若磁盘使用率大于90%，则告警出来。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(p2)	base产品下列模块： • BaseBizBaseapi • BaseBizCdp • BaseBizCommonbase • BaseBizConsole • BaseBizDfs • BaseBizDmc • BaseBizDqcexecutor • BaseBizDqcsupervisor • BaseBizMetaservice • BaseBizPhoenix • BaseBizSso • BaseBizTenant • BaseBizWkbench	软件对应天基的service role或者service

可能原因

应用服务异常引起应用日志异常增大，导致日志打满磁盘，或其它临时文件打满磁盘。

影响范围

若不及时清理，则会导致应用服务不可用，若Gateway磁盘报警，则导致执行任务失败。

处理方法

到大数据管家base分站清理相关应用日志，或者登陆到机器上清理相关应用日志或无效文件。

21.4 01.215.0006.00006-ssh

探测主机22端口，若端口不通，则ssh服务异常，并告警出来。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(p2)	base产品下列模块： • BaseBizBaseapi • BaseBizCdp • BaseBizCommonbase • BaseBizConsole • BaseBizDfs • BaseBizDmc • BaseBizDqcexecutor • BaseBizDqcsupervisor • BaseBizMetaservice • BaseBizPhoenix • BaseBizSso • BaseBizTenant • BaseBizWkbench	软件对应天基的service role或者service。

可能原因

主机（容器）异常或者应用异常打挂主机，导致ssh服务异常。

影响范围

服务单点，若同一个模块两个服务均异常，则base服务不可用。

处理方法

重启主机或容器。

21.5 01.215.0005.00005-s_ntpd_130605_1

检查ntp服务，若ntp服务异常，则告警出来。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(p2)	base产品下列模块： • BaseBizBaseapi • BaseBizCdp • BaseBizCommonbase • BaseBizConsole • BaseBizDfs • BaseBizDmc • BaseBizDqcexecutor • BaseBizDqcsupervisor • BaseBizMetaservice • BaseBizPhoenix • BaseBizSso • BaseBizTenant • BaseBizWkbench	软件对应天基的service role或者service

可能原因

ntp服务不存在或者服务异常。

影响范围

若应用时间与Gateway时间不一致，则导致base执行任务失败。

处理方法

检查ntp主机服务是否正常。

21.6 01.505.0004.00004-alisa_alert

nc检查gateway服务端口8000，如果端口服务异常，则告警出来。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(p2)	base产品下列模块：BaseBizGateway	软件对应天基的service role或者service

可能原因

Gateway进程挂掉。

影响范围

任务积压，或一直等待资源。

处理方法

到大数据管家上重启Gateway服务。

22 分析型数据库

22.1 Alarm-02.510.1002.00001-build进程死亡

当无法连接build进程的端口时，产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
2	P2	ADS的build模块	BUILD

可能原因

- build进程OOM、机器宕机、网络不通。

影响范围

- 当两个build全部死亡时，用户build失败。

处理方法

执行/home/admin/garuda/bin/garuda.sh start命令。

22.2 Alarm-02.510.1001.00002-rm进程死亡

当无法连接rm进程的端口时，产生该告警。

告警信息

告警类型	告警级别	告警对象	告警模块
2	P3	ADS的rm模块	RM

可能原因

rm进程OOM、机器宕机、网络不通。

影响范围

当两个rm全部死亡时，用户无法发起ddl。

处理方法

执行/home/admin/garuda/bin/garuda.sh start命令。

22.3 Alarm-02.510.1001.00003-rm gc严重

rm gc严重。

告警信息

告警类型	告警级别	告警对象	告警模块
2	P3	ADS的rm模块	RM

可能原因

- rm gc严重。

影响范围

- 当两个rm全部死亡时，用户无法发起ddl。

处理方法

执行/home/admin/garuda/bin/garuda.sh stop; /home/admin/garuda/bin/garuda.sh start命令。

22.4 Alarm-02.510.1003.00004-节点gc超过10s

集群有节点GC超过10s。

告警信息

告警类型	告警级别	告警对象	告警模块
2	P4	ADS的instance节点	tubo

可能原因

负载过高。

影响范围

节点不工作，用户查询慢。

处理方法

重启该节点。

22.5 Alarm-01.510.1008.00005-用户数据盘满

机器用户数据所在盘满。

告警信息

告警类型	告警级别	告警对象	告警模块
1	P3	ADS的instance节点	tubo

可能原因

日志过多、用户数据过多。

影响范围

用户无法上线数据。

处理方法

清理机器日志，联系用户清理无效数据。

22.6 Alarm-01.510.1009.00006-网络队列超过100w

mn节点的网络队列超过100w。

告警信息

告警类型	告警级别	告警对象	告警模块
1	P3	ADS的mergenode节点	tubo

可能原因

网络拥塞。

影响范围

查询慢。

处理方法

重启该mn节点。

23 流计算

23.1 Alarm-02.515.0001.0001-rm_restart

Galaxy调度RM服务重启。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	-	Gallardo调度

影响范围

Galaxy作业受影响。

处理方法

重启gallardo容器。

23.2 Alarm-02.515.0001.0002-rm_status_checker

Galaxy调度RM服务异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	-	Gallardo调度

影响范围

Galaxy作业受影响。

处理方法

重启gallardo容器。

23.3 Alarm-02.515.0001.0003-rm_slot_event_checker

有资源请求未分配。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	-	Gallardo调度

影响范围

新作业无法提交。

处理方法

参考运维手册扩容步骤。

23.4 Alarm-02.515.0002.0001-galaxy_service_checker

Galaxy Service服务异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	-	Galaxy服务层

影响范围

新作业无法提交。

处理方法

重启Galaxy容器。

23.5 Alarm-02.515.0002.0002-galaxy_ops_checker

Galaxy Ops服务异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	-	Galaxy服务层

影响范围

新作业无法提交。

处理方法

重启Galaxy容器。

23.6 Alarm-02.515.0002.0003-galaxy_pool_status_checker

Galaxy某个组服务异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	-	Galaxy服务层

影响范围

报警的组作业影响。

处理方法

重启Galaxy容器。

24 大数据应用加速器

24.1 Alarm-01.520.0001.00001-cpu内存占用率过高

当dtboost server占用CPU达到90%，或者内存达到90%，会产生该告警，当CPU，内存占用率小于70%，该告警清除。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	dtboost server	DtboostServer

可能原因

系统处理出现异常，导致cpu，内存占用过高。

影响范围

cpu、内存占用率过高可能会导致系统处理异常，后续请求处理过慢或无法完成。

处理方法

1. 检查dtboost server的日志是否异常。
   - 如果是，请跳转至*3*。
   - 如果否，请跳转至*2*。
2. 检查所在机器的cpu和内存配置是否符合要求。
   - 如果是，请跳转至*3*。
   - 如果否，联系相关负责人员调整机器配置，并重启服务。
3. 请搜集上述告警处理过程中的日志和消息，包括*/home/admin/dtboost/logs*目录下日志，联系开发。

24.2 Alarm-01.520.0001.00002-磁盘使用率过高

当dtboost server所在机器对应磁盘使用率达到90%。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	dtboost server	DtboostServer

可能原因

磁盘使用率过高会导致系统无法继续写日志，处理异常。

影响范围

磁盘使用过高，会导致系统后续日志等操作无法继续，系统处理异常。

处理方法

1. 检查dtboost server日志是否异常。
   - 如果是，请跳转至*3*。
   - 如果否，请跳转至*2*。
2. 检查对应磁盘容量大小是否符合要求。
   - 如果是，请跳转至*3*。
   - 如果否，联系相关负责人员调整机器配置，并重启服务。
3. 请搜集上述告警处理过程中的日志和消息，包括*/home/admin/dtboost/logs* 目录下日志，联系开发。

24.3 Alarm-01.520.0003.00002-磁盘使用过高

当dtboost smartmove所在机器磁盘使用率超过90%会产生该告警，当磁盘使用率小于60%，该告警消除。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	smart move	DtboostSmartm

可能原因

smartmove处理异常，导致系统持续写日志，会导致在短时间迅速写满磁盘。

影响范围

磁盘使用率过高，会导致系统处理异常，无法完成后续的写日志等操作。

处理方法

1. 检查smart move日志是否异常。
   - 如果是，请跳转至*3*。
   - 如果否，请跳转至*2*。

2. 检查对应磁盘容量大小是否符合要求。
   - 如果是，请跳转至*3*。
   - 如果否，联系相关负责人员调整机器配置，并重启服务。
3. 请搜集上述告警处理过程中的日志和消息，包括*/home/admin/smart-move/logs* 目录下日志，联系开发。

24.4 Alarm-01.520.0002.00001-cpu使用率过高

当dtboost smartview所在机器cpu的占用率超过90%，该告警产生，当cpu使用率小于70%，该告警消除。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	smart view	DtboostSmartv

可能原因

系统处理出现异常，导致cpu，内存占用过高。

影响范围

cpu、内存占用率过高可能会导致系统处理异常，后续请求处理过慢或无法完成。

处理方法

1. 检查dtboost smartview的日志是否异常。
   - 如果是，请跳转至*3*。
   - 如果否，请跳转至*2*。
2. 检查所在机器的cpu和内存配置是否符合要求。
   - 如果是，请跳转至*3*。
   - 如果否，联系相关负责人员调整机器配置，并重启服务。
3. 请搜集上述告警处理过程中的日志和消息，包括/home/admin/smart-view/logs 目录下日志，联系开发。

24.5 Alarm-01.520.0003.00001-cpu使用率过高

当dtboost smartmove所在机器cpu的占用率超过90%，该告警产生，当cpu使用率小于70%，该告警消除。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	smart move	DtboostSmartm

可能原因

系统处理出现异常，导致cpu，内存占用过高。

影响范围

cpu、内存占用率过高可能会导致系统处理异常，后续请求处理过慢或无法完成。

处理方法

1. 检查dtboost smartmove的日志是否异常。
   - 如果是，请跳转至*3*。
   - 如果否，请跳转至*2*。
2. 检查所在机器的cpu和内存配置是否符合要求。
   - 如果是，请跳转至*3*。
   - 如果否，联系相关负责人员调整机器配置，并重启服务。
3. 请搜集上述告警处理过程中的日志和消息，包括*/home/admin/smart-move/logs*目录下日志，联系开发。

25 大数据管家

25.1 02.535.0001.00001-check_bcc_api_alve

bcc api的80 http服务无法正常服务。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	紧急(P1)	bcc	bcc.bcc-api

可能原因

BCC API异常。

影响范围

BCC API不可用。

处理方法

1. 自动处理方法：重新部署BCC API。
2. 手工处理方法：
   1. 执行cd /home/admin/bigdata-cloudconsole/sbin;bash start_server_supervisor_mode.sh命令，重启BCC API。
   2. 执行cd /home/admin/cai/bin/; bash nginxctl.sh start命令，重启NGINX。

25.2 02.535.0002.00002-check_bcc_web_alive

BCC WEB的80 http服务不能正常使用。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	紧急(P1)	bcc	bcc.bcc-web

可能原因

BCC WEB的nginx异常。

影响范围

BCC WEB不可用。

处理方法

1. 自动处理方法：重新部署bcc web
2. 手工处理方法：执行cd /home/admin/cai/bin/; bash nginxctl.sh start命令，重启NGINX。

26 关系网络分析

26.1 Alarm-01.013.0080.0002-iplus_memo_cluster_service

内存使用率过高，内存已满。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	紧急(P1)	iplus-iplus_biz	iplus-iplus_biz

可能原因

并发过高或者数据量过大。

影响范围

可能会导致服务响应很慢，甚至服务不可用，丢失数据。

处理方法

降低用户并发量，并且降低请求数量级。

26.2 Alarm-01.013.0080.0001-iplus_load_cluster_service

CPU负载过高。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	iplus-iplus_biz	iplus-iplus_biz

可能原因

并发过高或者数据量过大。

影响范围

服务响应变慢。

处理方法

降低用户并发量，并且降低请求数量级。

26.3 Alarm-01.013.0080.0003-iplus_disk_cluster_service

日志或临时文件把磁盘写满。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	次要(P3)	iplus-iplus_biz	iplus-iplus_biz

可能原因

磁盘使用率过高会导致系统无法继续写日志，处理异常。

影响范围

磁盘使用过高，会导致系统后续日志等操作无法继续，系统处理异常。

处理方法

清除容器内部*/home/admin/logs /root/logs* 两个过期的日志。

26.4 Alarm-01.013.0080.0102-iplus_testimage_monitor_alarm

测试镜像异常。

告警信息

告警类型	告警级别	告警对象	告警模块
测试镜像报警	通知(P4)	iplus-iplus_biz	iplus-iplus_biz

可能原因

测试镜像数据冲突。

影响范围

可能服务不可用。

处理方法

重启。

26.5 Alarm-01.013.0080.0101-iplus_postcheck_monitor_alarm

PostCheck检查不通过，服务不可用。

告警信息

告警类型	告警级别	告警对象	告警模块
PostCheck检查不通过	紧急(P1)	iplus-iplus_biz	iplus-iplus_biz

可能原因

应用出现异常。

影响范围

服务不可用。

处理方法

重启。

27 机器学习PAI

27.1 02.525.0001.00001-DNS连接异常

CAP的DNS域名ping不通时，会触发报警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	pai_cap	pai_dmscloud

可能原因

- 网络原因。
- VIP挂掉。

影响范围

用户不能登录。

处理方法

1. 确认网络是否有异常。
   - 如果异常，联系驻场网工处理。
   - 如果无异常，请跳转至2。
2. 确认vip是否异常。

27.2 02.525.0001.00002-DNS连接异常

PAI的DNS域名ping不通时，会触发报警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	pai_dmscloud	pai_dmscloud

可能原因

- 网络原因。
- VIP挂掉。

影响范围

PAI页面不能正常展现。

处理方法

1. 确认网络是否有异常。
   - 如果异常，联系驻场网工处理。
   - 如果正常，请跳转至2。
2. 确认vip是否异常。

27.3 02.525.0001.00003-DNS连接异常

JCS的DNS域名ping不通时，会触发报警。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	pai_jcs	pai_dmscloud

可能原因

- 网络原因。
- VIP挂掉。

影响范围

实验任务无法提交。

处理方法

1. 确认网络是否有异常。
   - 如果异常，联系驻场网工处理。
   - 如果正常，请跳转至2。
2. 确认VIP是否异常。

27.4 02.525.0002.00001-VIP 端口异常

CAP的VIP异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	pai_cap	pai_dmscloud

可能原因

- 网络原因。
- CAP服务挂掉。

影响范围

用户不能登录。

处理方法

1. 登录CAP容器： 查看java以及nginx 进程是否存在，不存在退出容器，重启容器。
2. 若进程存在，进入*/home/admin/logs/cap/commom-error.log*目录，查看有无明显异常日志，请联系技术支持。

27.5 02.525.0002.00002-VIP 端口异常

PAI的VIP异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	pai_dmscloud	pai_dmscloud

可能原因

- 网络原因。
- dms服务挂掉。

影响范围

PAI页面不能正常展现。

处理方法

登录dms 容器： 查看java以及nginx 进程是否存在。

1. 如果不存在，退出容器，重启容器。
2. 如果存在，进入*/home/admin/logs/dmscloud/commom-error.log*查看有无明显异常日志，请联系技术支持。

27.6 02.525.0002.00003-VIP 端口异常

jcs的。VIP异常

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	pai_jcs	pai_dmscloud

可能原因

- 网络原因。
- jcs服务挂掉。

影响范围

实验任务无法提交。

处理方法

登录jcs 容器：查看java以及nginx 进程是否存在。

- 如果不存在，退出容器，重启容器。
- 如果存在，进入*/home/admin/logs/jcs/commom-error.log* 目录，查看有无明显异常日志，请联系技术支持。

27.7 02.525.0003.00001-RDS 端口异常

cap的数据库端口异常

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	pai_cap	pai_dmscloud

可能原因

- 网络原因。
- 数据库挂掉。

影响范围

用户不能登录，获取不到用户数据。

处理方法

，

- 如果网络问题，请联系网工处理。
- 如果RDS服务挂掉，请联系RDS技术支持。

27.8 02.525.0003.00002-RDS 端口异常

dmscloud的数据库端口异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	pai_dmscloud	pai_dmscloud

可能原因

- 网络原因。
- 数据库挂掉。

影响范围

用户不能访问页面，无法查看实验。

处理方法

- 如果网络问题，请联系网工处理。
- 如果RDS服务挂掉，请联系RDS技术支持。

27.9 02.525.0003.00003-RDS 端口异常

jcs的数据库端口异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	-	pai_jcs	pai_dmscloud

可能原因

- 网络原因。
- 数据库挂掉。

影响范围

实验任务无法提交。

处理方法

- 如果是网络问题，联系网工处理。
- 如果是RDS服务挂掉，联系RDS技术支持。

28 MiniLVS

28.1 Alarm-01.211.0001.00001-VIP库存

可分配 VIP 资源过少 (默认20) 时告警。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	miniLVS	minilvs.API#

可能原因

该环境VIP消耗过多。

影响范围

如果库存耗尽时影响新 VIP 申请，不影响在用 VIP。

处理方法

1. 评估业务是否有新增 VIP 需求。
   - 如果否，请调整阈值。
   - 如果是，请跳转至2.
2. 网络工程师分配新的 VIP 资源段，扩容到 minilvs。

28.2 Alarm-02.211.0002.00001-LVSNode KVM连通性

LVSNode KVM 连不通。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	miniLVS	minilvs.LVSNode#

可能原因

KVM 异常。

影响范围

KVM 网络或者负载异常。

处理方法

在 minilvs 所在 ops 两台宿主机上: 执行`virsh list --all`，获取 kvm Name: minilvsNNN。

执行`virsh destroy $name; virsh start $name`命令重启。

28.3 Alarm-02.211.0001.00002-API 可用性

miniLVS 管控API 异常。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	紧急(P1)	miniLVS	minilvs.API#

可能原因

miniLVS 管控API 异常, 返回值不合预期.可能原因: DNS 异常、LVSNode 异常、DB 长时间连接失败。

影响范围

影响新 VIP 的生产，及已有 VIP 的变配，不影响已有 VIP 的流量转发。

处理方法

1. 执行`dig minilvs-api.${intranet-domain}`命令，确认解析正常。
2. 执行`ping minilvs-api.${intranet-domain}`命令，确认 VIP 可以ping 通。
3. 执行`curl minilvs-api.${intranet-domain}/slb/api?list_lvs_node`命令，确认是否返回正常。

   如果还是无法定位问题，请收集上述处理过程的输出，联系 minilvs 开发排查。

29 MiniRDS

29.1 Alarm-02.301.0001.0001-check slave(sql thread down)

当slave sql 线程 down。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	minirds	minirds.db

可能原因

主从同步失败。

影响范围

如果不及时处理导致 master slave 数据不一致。

处理方法

执行curl "http://${api}/action=recover&url=${url}&port=${port}"命令，重搭备库。

29.2 Alarm-02.301.0001.0002-check alive

当mysql实例 down。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	紧急(P1)	minirds	minirds.db

可能原因

mysql实例故障。

影响范围

不及时处理可能服务不能保证。

处理方法

执行curl "http://${api}/action=recover&url=${url}&port=${port}"命令重搭。

29.3 Alarm-02.301.0001.0003-chk_thread_connected above 8000

mysql 连接数过高。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	minirds	minirds.db

可能原因

mysql 连接数过高。

影响范围

导致后续服务中断。

处理方法

执行kill process kill -9 ${mysqld_pid}命令。

29.4 Alarm-02.301.0001.0004-chk_slavelag behind 36000

slave 。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	minirds	minirds.db

可能原因

网络原因。

影响范围

可能导致数据不一致。

处理方法

执行tcpdump –i any命令，抓包检验，是否网络问题。

29.5 Alarm-02.301.0001.0005-chk_mysql_aborted_conn above 10

Aborted 连接数过多。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	minirds	minirds.db

可能原因

网络原因。

影响范围

服务不稳定。

处理方法

执行tcpdump –i any命令，抓包检验，是否网络问题。

29.6 Alarm-02.301.0001.0006-chk_slaveio

当slave io 线程 down。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	minirds	minirds.db

可能原因

主从同步失败。

影响范围

如果不及时处理导致 master slave 数据不一致。

处理方法

执行curl "http://${api}/action=recover&url=${url}&port=${port}"命令，重搭备库。

30 ODPS

30.1 Testalert-send title-odps-service-controller_serviceNametestalert

Debug使用，无实际业务作用。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

无。

影响范围

无。

处理方法

无。

30.2 Odpsworkerruntimealert-send title-odps-service-controller_serviceNameodpsworkerruntimealert

判断odpsWorker是否连续重启。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

OdpsWorker连续重启。

影响范围

严重。

处理方法

无。

30.3 Cpustatusalert-send title-odps-service-controller _serviceNamecpustatusalert

判断单台机器cpu使用率是否达到某个阈值。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

Cpu使用率过高。

影响范围

无。

处理方法

无。

30.4 Executorruntimealert-send title-odps-service-controller _serviceNameexecutorruntimealert

判断executor是否连续重启。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

Executor连续重启。

影响范围

严重。

处理方法

无。

30.5 Hiveserverruntimealert-send title-odps-service-controller _serviceNamehiveserverruntimealert

判断hiveserver是否连续重启。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

Hiveserver连续重启。

影响范围

严重。

处理方法

无。

30.6 Hivegclogalert-send title-odps-service-controller _serviceNamehivegclogalert

统计hive heap内存是否泄漏。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

Hive heap内存泄漏。

影响范围

严重。

处理方法

重启hive server进程。

30.7 Schedulerpoolsizaalert-send title-odps-service-controller _serviceNameschedulerpoolsizaalert

Schedulepoolsize totalSize的值超过阈值。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

Odps各类任务堆积。

影响范围

严重。

处理方法

1. 可能是正常现场，任务本身就多，此时无需处理，等待即可。
2. 如果是某个组件挂了，导致其他任务在排队，则需要检查并修复该组件。

30.8 Hivechildprocessexistalert-send title-odps-service-controller_serviceNamehivechildprocessexistalert

判断hive子进程是否存在。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

Hive子进程不存在。

影响范围

严重。

处理方法

重启hive server进程。

30.9 Diskdriveralert-send title-odps-service-controller _serviceNamediskdriveralert

判断diskdriver是否正常。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

Diskdriver不正常。

影响范围

严重。

处理方法

无。

30.10 Alarm-01.000.0001.00004-check_pangu_diskfull

查看集群盘古磁盘空余空间。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	pangu

可能原因

临时数据过多。

影响范围

影响集群作业数据保存。

处理方法

清理回收站、作业临时文件。

30.11 Alarm-02.000.0001.00005-check_pangu_file_replicate

查看文件副本数。

告警信息

告警类型	告警级别	告警模块
事件告警	重要(P4,P1)	文件

可能原因

文件副本所在机器宕机。

影响范围

影响对应文件副本数。

处理方法

执行相关命令增加副本或者重启副本存放服务器。

30.12 Pangudiskcreachalert-send title-odps-service-controller _serviceNamepangudiskcreachalert

判断pangu磁盘是否有损坏。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

盘古磁盘损坏。

影响范围

严重。

处理方法

无。

30.13 Nuwaaddressalert-send title- odps-service-controller _serviceNamenuwaaddressalert

判断女娲是否会丢失odps某些节点。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

Nvwa关联的odps节点有丢失。

影响范围

严重。

处理方法

无。

30.14 Pangumastermemoryalert-send title-odps-service-controller_serviceNamepangumastermemoryalert

判断pangumaster内存是否超过阈值。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

PanguMaster内存超出阈值。

影响范围

严重。

处理方法

合并小文件或删除无用文件。

30.15 Alarm-02.005.0001.00000-check_nuwa_zk

查看nuwa状态。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P1)	nuwa	nuwa

可能原因

心跳丢失、对应服务器状态不正常。

影响范围

影响集群稳定。

处理方法

1. 执行/apsara/deploy/nuwa_console --address=nuwa://localcluster/ --console --admin=true命令，确定nuwa服务是否正常。
2. 登录报警机器确定nuwa进程是否存在。
3. 联系nuwa开发排查问题。

30.16 Pidmaxalert-send title-odps-service-controller_serviceNamepidmaxalert

系统pid最大检查。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps-service-controller

可能原因

pid设置过小，可能是克隆模板的问题。

影响范围

严重。

处理方法

1. 手动调节pid数量。

2. 更换克隆模板。

30.17 Alarm-02.010.0001.00004-check_fuxi_master_alive

查看集群fuxi master是否alive。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P1)	fuxi master	fuxi

可能原因

程序异常退出、服务器宕机。

影响范围

影响集群稳定。

处理方法

1. 登录报警fuxi master，查看进程是否存在，存在进行下一步调查。
2. 确定*/apsara/cloud/data/corefile*是否有coredump出现。
3. 如果1和2检查都正常，该错误应该是误报，联系fuxi开发排查。

30.18 Alarm-01.010.0002.00001-check_package_manager_alive

查看集群pangu master进程是否alive。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	package manager	package manager

可能原因

程序异常退出、服务器宕机。

影响范围

影响集群包管理。

处理方法

1. 登录报警pacakge manager，查看进程是否存在。

- 不存在，联系package 开发进行处理。
- 存在，执行下一步。

2. 确定*/apsara/cloud/data/corefile*是否有coredump出现。
3. 如果1和2都正常，应该是误报，联系package开发排查问题。

30.19 Alarm-02.005.0001.00001-check_nuwa_config

查看nuwa config。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P1)	nuwa	nuwa

可能原因

配置文件丢失。

影响范围

影响集群服务。

处理方法

联系nuwa开发排查问题。

30.20 Alarm-01.000.0001.00006-check_pangu_free_size

集群盘古空闲空间。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	集群

可能原因

数据量过多。

影响范围

影响集群正常存储服务。

处理方法

扩容或者清理数据。

30.21 Alarm-01.000.0001.00007-盘古工作模式告警

维护工具检测到集群中盘古工作模式不对的时候，产生该告警，检测周期为三分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P1	盘古	盘古整体

可能原因

大于一半的master机器挂了。

影响范围

影响盘古的可用性。

处理方法

修复没有运行的pangu master所在机器。

30.22 Alarm-01.000.0001.00008-盘古总文件数量过多告警

维护工具检测到集群中盘古文件数目过多时，产生该告警，检测周期为一分钟。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古整体

可能原因

盘古中文件数量过大。

影响范围

影响盘古的可用性。

处理方法

删除一些不需要的文件，或者扩大盘古master，cs的内存。

30.23 Alarm-01.000.0001.00009-盘古空间使用超限告警

维护工具检测到集群中盘古使用量超限的时候，产生该告警，检测周期为一天。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古整体

可能原因

盘古中的文件容量过大。

影响范围

影响盘古的可用性。

处理方法

删除不需要使用的文件，或者扩容一些CS。

30.24 Alarm-01.000.0001.00010-盘古SECONDARY master数量不对告警

维护工具检测到集群中盘古SECONDARY master数量不足时，产生该告警，检测周期为半小时。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古整体

可能原因

存在master机器挂了。

影响范围

影响盘古的可用性。

处理方法

修复没有运行的pangu master所在机器。

30.25 Alarm-01.000.0001.00011-盘古binary文件不一致告警

维护工具检测到集群中盘古binary文件版本不一致时，产生该告警，检测周期为一小时。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	P2	盘古	盘古整体

可能原因

所有master的二进制文件md5不一致。

影响范围

影响盘古的可用性。

处理方法

将所有的second master 进程修复为一致。

如果是primary master不一致，先切换再修复。

30.26 Alarm-01.005.0001.00002-check_nw_zk_queue

zk请求队列。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	nuwa	nuwa

可能原因

nuwa进程处理变慢。

影响范围

影响集群飞天服务。

处理方法

该监控出现可能会影响现有整个集群服务，需要联系nuwa开发上线排查。

30.27 Alarm-01.010.0001.00005-check_FuxiMaster_queue_size

fuxi master请求处理队列。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	fuxi master	fuxi

可能原因

请求过多或者fuxi进程处理变慢。

影响范围

整个集群fuxi处理能力。

处理方法

fuximaster连接数过多，可能是作业导致，也可能是fuxi master本身处理变慢引起，联系fuxi开发进行排查。

30.28 Alarm-01.000.0002.00000-check_cs_sendbuffer

查看cs sendbuffer是否打满。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	chunkserver	chunkserver

可能原因

对端cpu打满或者网络丢包。

影响范围

影响cs服务能力。

处理方法

联系pangu开发查看sendbuffer打满机器，查看网络是否正常、服务器正常服务。

30.29 Alarm-02.500.0001.00002-check_status_file

Status.html是否存在。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	tunnel/frontend

可能原因

Tunnel/frontend进程异常。

影响范围

单台服务器无法服务。

处理方法

查看相关log以及服务器状态。

30.30 Alarm-02.500.0001.00001-check_coredump

进程是否发生core文件。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	tunnel/frontend	tunnel/frontend

可能原因

对应进程出现异常。

影响范围

单台服务器可能无法正常服务。

处理方法

判断是frontend还是tunnel，联系对应开发进行排查，查看服务是否正常。

30.31 Alarm-02.500.0001.00002-check_status_file

status.html是否存在。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	tunnel/frontend	tunnel/frontend

可能原因

tunnel/frontend进程异常。

影响范围

单台服务器无法服务。

处理方法

- 如果是升级过程，请忽略。
- 如果是机器重装,联系frontend/tunnel开发部署服务。

如果不是上述两种情况，联系frontend或者tunnel开发排查。

30.32 Alarm-02.500.0002.00000-check_frontend_process_exists

Frontend进程是否存在。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	frontend

可能原因

服务器异常、进程异常。

影响范围

单台服务器无法服务。

处理方法

查看相关log以及服务器状态。

30.33 Alarm-02.500.0001.00003-check_toa_odps

查看toa模块是否加载。

告警信息

告警类型	告警级别	告警对象	告警模块
事件告警	重要(P2)	单台服务器	单机报警

可能原因

没有insmod toa。

影响范围

无法查看真实IP。

处理方法

执行如下命令：

sudo modprobe toa

lsmod | grep toa

30.34 Alarm-02.500.0003.00000-check_tunnel_service

Tunnel进程是否存在。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	tunnel

可能原因

服务器异常、进程异常。

影响范围

单台服务器无法服务。

处理方法

查看相关log以及服务器状态。

30.35 Alarm-01.500.0004.00000-Check_ExecutorWorker_sql_relative_task_default_QPS

sql_relative总请求QPS。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	executorworker	executorworker

可能原因

sql_relative类型请求数过多。

影响范围

影响sql_relative类型作业正常运行。

处理方法

联系executor work开发进行排查。

30.36 Alarm-01.500.0004.00001-Check_ExecutorWorker_sql_relative_task_default_Latency

tryrun的latency。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	executorworker	executorworker

可能原因

sql_relative类型操作重跑延迟增加负载过高，延迟增加。

影响范围

影响sql_relative类型作业正常运行。

处理方法

联系executor work开发进行排查。

30.37 Alarm-01.500.0004.00002-Check_ExecutorWorker_aggregate_task_default_QPS

aggregate总请求QPS。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	executorworker	executorworker

可能原因

aggregate类型请求数过多。

影响范围

影响aggregate类型作业运行。

处理方法

联系executor work开发进行排查。

30.38 Alarm-01.500.0004.00003-Check_ExecutorWorker_aggregate_task_default_Latency

aggregate tryrun的latency。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	executorworker	executorworker

可能原因

aggregate类型操作重跑延迟增加。

影响范围

影响aggregate类型作业正常运行。

处理方法

联系executor work开发进行排查。

30.39 Alarm-01.500.0004.00004-Check_ExecutorWorker_RunningTaskCount

executorwork运行的线程数。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	executor	executor

可能原因

job数过多。

影响范围

影响整个服务单位时间运行job的能力。

处理方法

如果报警时间超过报警间隔3-5倍，也就是联系收到3-5次报警。

联系executor work排查是否需要扩容，如果偶尔在业务高峰期出现一次，属于压力过大，符合预期。

30.40 Alarm-01.500.0004.00005-Check_ExecutorWorker_EasyRPC_Latency

executor父进程网络耗时。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	executor	executor

可能原因

服务器负载过高、网络不稳定。

影响范围

影响executor正常服务。

处理方法

联系executor work开发进行排查。

30.41 Alarm-01.500.0005.00000-check_odpsworker_requestpoolsize

odps worker 请求队列长度。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	odpswork	odpswork

可能原因

job数过多，odpswork数量不足。

影响范围

影响odps服务正常运行。

处理方法

联系odpswork开发排查odpswork是否正常工作。

- 如果是，则减少提交的job数或者增加odpswork数。
- 如果不是，则需要开发进一步排查。

30.42 Alarm-01.500.0005.00001-check_OdpsWorker_StoreEventLatecy

odpswork storeEvent方法的latency。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	odpswork	odpswork

可能原因

进程繁忙、ots延迟过大。

影响范围

影响storeEvent进程运行。

处理方法

查看对应机房网络流量打满和ots服务是否正常，联系scheduler worker开发上线排查，否则处理机房网络流量打满问题或者ots服务异常问题。

30.43 Alarm-01.500.0006.00000-check_SchedulerWorker_CreateInstanceQPS

异步instance请求的qps。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	schedulerwork	schedulerwork

可能原因

instance数增加、schedulerwork处理能力下降。

影响范围

影响schedulerwork正常运行。

处理方法

联系scheduler worker开发排查。

30.44 Alarm-01.500.0006.00001-Check_SchedulerWorker_RunningTaskCount

集群总的executorwork处理线程总数。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	schedulerwork	schedulerwork

可能原因

job数增加。

影响范围

影响整个odps服务处理能力。

处理方法

降低提交的job数或者联系odps executor work开发增加executor work线程数。

30.45 Alarm-01.500.0007.00000-check_QuotaWorkerRole_CPUUsage

quotaworker cpu使用率。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	quotawork	quotawork

可能原因

quotawork请求数过多、进程夯。

影响范围

影响tunnel服务的quota设置。

处理方法

联系quotawork开发上线排查，紧急情况可以对对应进程gcore $pid(对应进程pid）。

30.46 Alarm-01.500.0007.00001-check_QuotaWorkerRole_MEMUsage

quotaworker mem使用率。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	quotawork	quotawork

可能原因

quotawork请求数过多、进程夯。

影响范围

影响tunnel 服务的quota设置。

处理方法

联系quotawork开发上线排查，紧急情况可以对对应进程执行gcore $pid命令，pid对应进程pid。

30.47 Alarm-01.500.0008.00000-check_MessageServerRole_CPUUsage

messagework CPU使用率。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	messagework	messagework

可能原因

message过多、进程异常。

影响范围

影响ODPS各角色间消息传送。

处理方法

联系messagework开发上线排查,紧急情况可以对对应进程gcore $pid，pid表示对应进程pid。

30.48 Alarm-01.500.0008.00001-check_MessageServerRole_MEMUsage

messagework mem使用率。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	messagework	messagework

可能原因

message过多、进程异常。

影响范围

影响ODPS各角色间消息传送。

处理方法

联系messagework开发上线排查，紧急情况可以对对应进程执行gcore $pid，pid表示对应进程pid。

30.49 Alarm-01.500.0009.00000-check_hiveserver_fn_createPartition_latency

create partition的latency。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	hiveserver	hiveserver

可能原因

OTS异常。

影响范围

影响ODPS服务创建partition。

处理方法

查看对应机房网络流量是否打满和OTS服务是否正常，联系hiveserver开发上线排查，否则处理机房网络流量打满问题或者ots服务异常问题。

30.50 Alarm-01.500.0010.00000-check_ddl_server_thread_pool_state

正在运行的ddltask个数。

告警信息

告警类型	告警级别	告警对象	告警模块
阈值告警	重要(P2)	hiveserver	hiveserver

可能原因

有ddl hang，ddlserver数量不够。

影响范围

影响ddl操作。

处理方法

联系hiverserver开发上线排查。

30.51 BCC监控-checkdiskusage

监控磁盘使用率 。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	pangu

可能原因

磁盘空间被占满。

影响范围

影响集群作业数据保存。

处理方法

手工干预清理。

30.52 BCC监控-checkass

Ping aas是否正常。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps依赖

可能原因

Ass出现问题。

影响范围

影响odps服务。

处理方法

通知相关模块联系人。

30.53 BCC监控-checkumm

Ping umm是否正常。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps依赖

可能原因

Umm出现问题。

影响范围

影响odps服务。

处理方法

通知相关模块联系人。

30.54 BCC监控-checkots

Otsmeta工具检查 。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps依赖

可能原因

Ots出现问题。

影响范围

影响odps服务。

处理方法

通知相关模块联系人。

30.55 BCC监控-checknuwa

执行nuwa命令检查nuwa。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odps依赖

可能原因

Nuwa出现问题。

影响范围

影响odps服务。

处理方法

通知相关模块联系人。

30.56 BCC监控-checkchlildprocessruntime

检查executor的子进程是否存在和重启。

告警信息

告警类型	告警级别	告警模块
阈值告警	重要(P4,P1)	odpsexecutor子进程

可能原因

Odps框架问题。

影响范围

影响odps服务。

处理方法

通知odps值班人员。