

SOFAStack

云产品中台
运维指南

产品版本：AntStack Plus 1.11.0

文档版本：20220929



法律声明

蚂蚁集团版权所有©2022，并保留一切权利。

未经蚂蚁集团事先书面许可，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。

商标声明

 蚂蚁集团 ANT GROUP 及其他蚂蚁集团相关的商标均为蚂蚁集团所有。本文档涉及的第三方的注册商标，依法由权利人所有。

免责声明

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。蚂蚁集团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，并在蚂蚁集团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蚂蚁集团授权渠道下载、获取最新版的用户文档。如因文档使用不当造成的直接或间接损失，本公司不承担任何责任。

通用约定

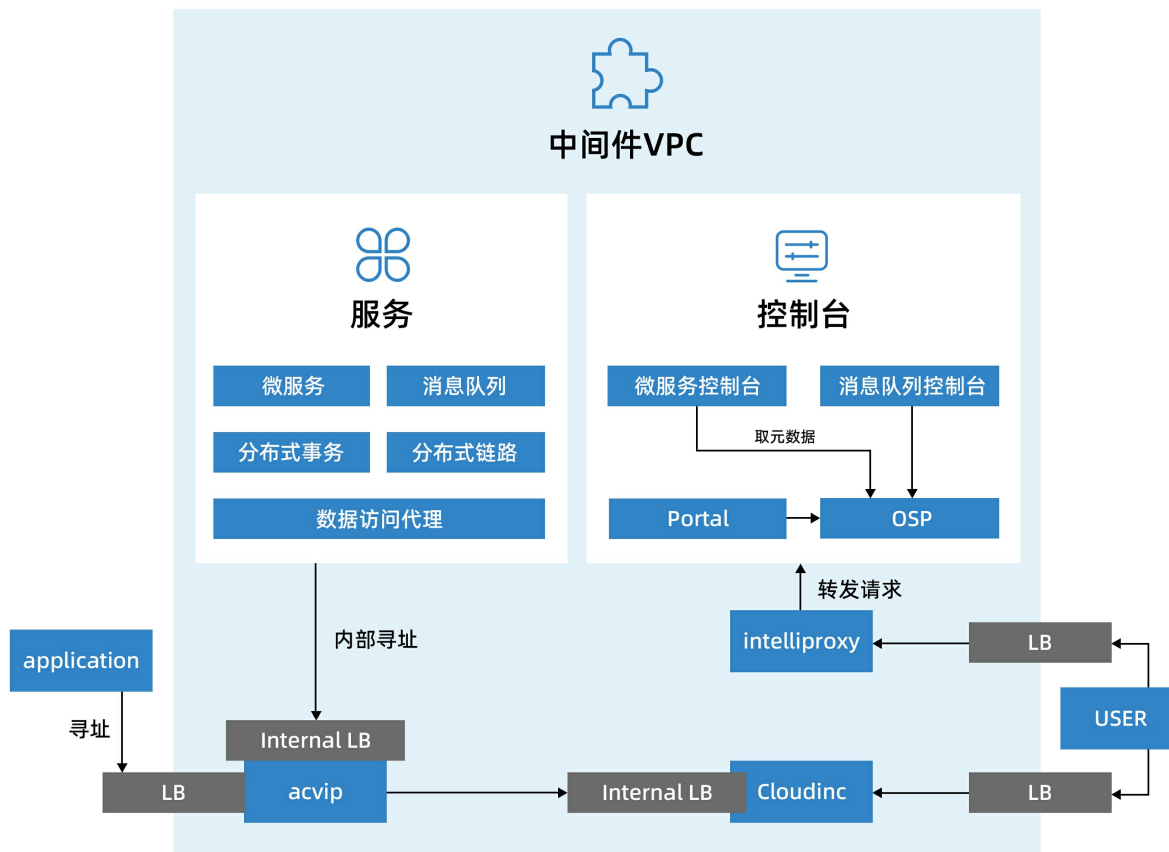
格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1.系统组件	05
2.ACVIP 高可用	07
3.同城容灾	08
3.1. ACVIP	08
3.1.1. 容灾架构	08
3.1.2. 热切换方案	09
3.1.3. 容灾场景处理	10
3.2. OSP + Intelliproxy	10
3.2.1. 容灾架构	10
3.2.2. 热切换方案	12
3.2.3. 容灾处理场景	13
4.日常运维	14
4.1. 监控和预警	14
4.2. 系统日志	20
4.3. 服务巡检	21
4.3.1. 系统组件监控检查	21
4.3.2. 业务功能检查	23
5.中间件细粒度权限管控方案	25
6.常见故障处理	27
6.1. 常见问题	27
6.2. 普通用户登录 SOFA 控制台后拥有管理员权限	32

1. 系统组件

组件拓扑



中间件门户产品包括以下组件：

- **Intelliproxy**：全局微服务代理层，主要提供用户认证和权限校验功能。
- **Portal**：中间件平台的门户。
- **OSP**：支撑中台系统，提供租户实例信息。
- **ACVIP**：负责域名 IP 的健康检查（health check），提供域名可用 IP 节点。

中间件注册地址的逻辑

1. 中间件通过后置任务将需要注册到 ACVIP 的地址写入到 OSP。
2. 在 OSP 控制台的 domain 页签单击 **刷新**，将中间件地址写入 ACVIP 中。
 - AntStack 底座环境：Pod IP 固定，写入 ACVIP 的地址为 Pod IP 列表。
 - AntStack Plus 底座公有云环境：Pod IP 不固定，写入 ACVIP 的地址为 SLB 内网 IP。
 - AntStack Plus 底座物理机环境：Pod IP 固定，写入 ACVIP 的地址为 Pod IP 列表。

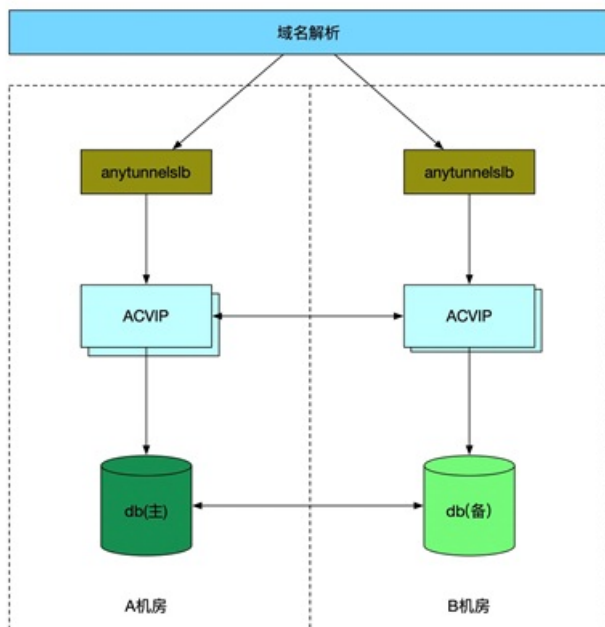
资源清单说明

组件	资源依赖	服务端口
Intelliporxy	N/A	80
Portal	N/A	80
OSP	N/A	80、8341
ACVIP	2 * 服务器 (4 CPU、8 GB 内存、100 GB 磁盘)	9003

2.ACVIP 高可用

本文介绍 ACVIP（Ant Cloud Vip）的高可用原理。

ACVIP 高可用



ACVIP 在 VPC 网络下的高可用方案说明如下：

- 域名解析：通过域名解析完成主备机房的 ACVIP 寻址。
- Anytunnel SLB：每个机房通过 Anytunnel SLB 下挂 ACVIP Server 提供服务。
- ACVIP：每个机房的 ACVIP Server 冗余部署，一般是 2 台。
- DB：主备机房的 DB 是主备关系。

ACVIP 原理说明如下：

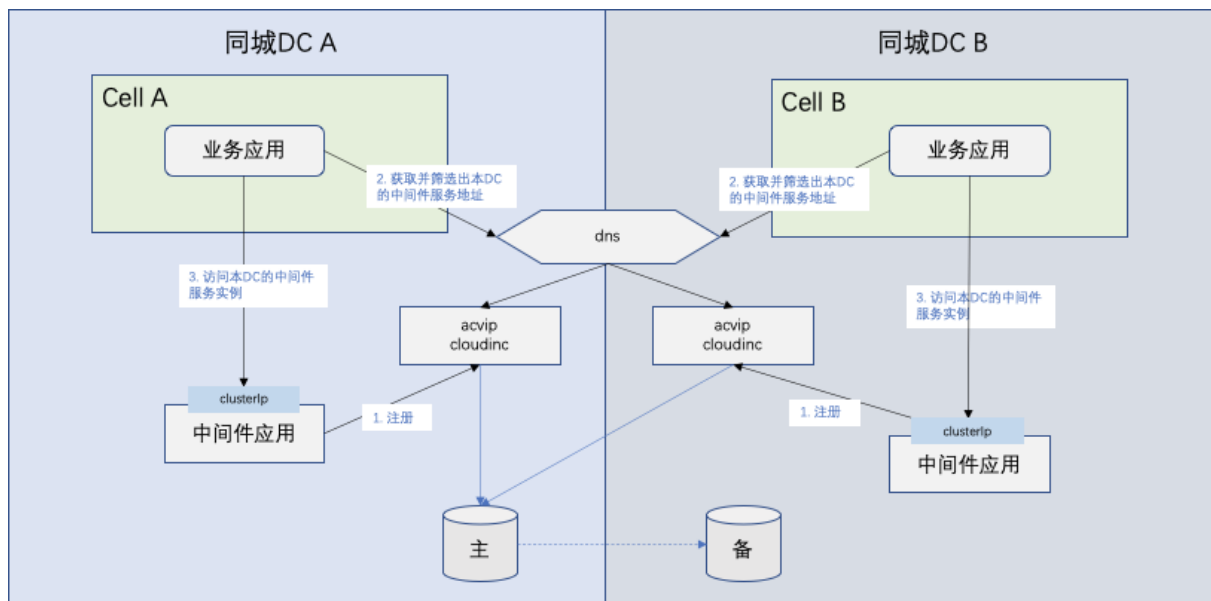
1. ACVIP 服务端启动时，将所有域名加载到内存，并进行健康检查，成功加载后，服务端启动完成。
2. ACVIP 服务端周期性检查 DB 配置，将添加或者修改的配置同步到内存。
3. ACVIP 服务端周期性检查每个域名下挂节点状态，并同步到内存。
4. 客户端启动后从服务端拉取 domains 列表，并拉取订阅的 domains 详情，同时将 domain 详情数据保存到客户端的本地磁盘。客户端周期性和服务端对比数据变化，如果有数据变化，从服务端拉取数据，进行更新。

3.同城容灾

3.1. ACVIP

3.1.1. 容灾架构

架构图



容灾架构说明如下：

- ACVIP 主备机房需同等部署，数据库共库。
- DNS 主备机房双挂，提供给业务应用使用。
- 客户端通过自带的 DATACENTER 属性来完成正常情况单机房流量收敛。

高可用说明

- 单机房 ACVIP 组件不可用时，ACVIP Client 会缓存所有中间件地址，依然可以使用本地的缓存来访问中间件服务。
- 机房宕机导致 ACVIP 及所有中间件都不可用时，无法提供高可用，必须依赖容灾整体切换。

产品依赖

外部产品依赖

无

底座产品依赖

- 元集群：元集群主备机房独立部署，无容灾要求。
- 内网 DNS：
 - i. ACVIP 通过内网 DNS 提供的域名访问数据库。容灾时，需将数据库域名切换至备机房的数据库。所以依赖内网 DNS 的容灾能力。

ii. ACVIP 通过内网 DNS 提供的域名，双挂主备机房的内网负载均衡，对外提供服务。

- 内网负载均衡：主备机房各自通过内网负载均衡进行负载。

内网 DNS 和 内网负载均衡 在不同底座下，有不同的选择。具体如下表所示：

底座	内网 DNS	内网负载均衡
AntStack	AntDNS	ALB
AntStack Plus 公有云	privatezone	SLB
AntStack Plus 物理机	AntDNS	-
AntStack Plus 物理机 + 飞天	AntDNS (forward opsdns)	-

注意

物理机底座下，AntStack Plus 目前没有内网负载均衡，实际部署时用客户环境选用的负载均衡设备。

数据库依赖

OB/RDS：主备机房共库，依赖 OB/RDS 的容灾能力。

数据同步

主备机房共库，依赖数据库的同步能力。

网络链路

- 用户应用通过 ACVIP 域名访问 ACVIP 服务。
- 中枢应用，通过 ACVIP 内网 LB 访问 ACVIP 服务。

容灾能力

支持机房级/组件级容灾，容灾切换后无功能降级。

3.1.2. 热切换方案

容灾切换说明

- 容灾切换时需要切换域名，摘除故障机房的流量。
- 数据库容灾切换依赖数据库容灾能力。

切换逻辑

1. 切换元数据库 DB、内网 DNS。
2. 切换 ACVIP 内网域名，摘除故障机房的流量。
3. 切换完毕后，验证备机房 ACVIP 状态。

切换原则

保证数据不丢失，业务断开后可以立即恢复。

3.1.3. 容灾场景处理

常见容灾场景及处理方式如下：

容灾场景	容灾切换	容灾恢复	容灾回切
主机房断电 或网络孤岛	<ol style="list-style-type: none">1. 切换元数据库 DB、内网 DNS。2. 切换内网域名，摘除主机房的流量3. 切换完毕后，验证备机房 ACVIP 状态。	自动恢复，无需人工干预。	<ol style="list-style-type: none">1. 切换元数据库 DB、内网 DNS。2. 切换内网域名，挂载主机房流量。3. 切换完毕后，验证主机房 ACVIP 状态。
备机房断电、网络孤岛、脑裂	<ol style="list-style-type: none">1. 切换元数据库 DB、内网 DNS。2. 切换内网域名，摘除备机房流量。3. 切换完毕后，验证主机房 ACVIP 状态。	自动恢复，无需人工干预。	<ol style="list-style-type: none">1. 切换元数据库 DB、内网 DNS。2. 切换内网域名，挂载备机房流量3. 切换完毕后，验证备机房 ACVIP 状态。

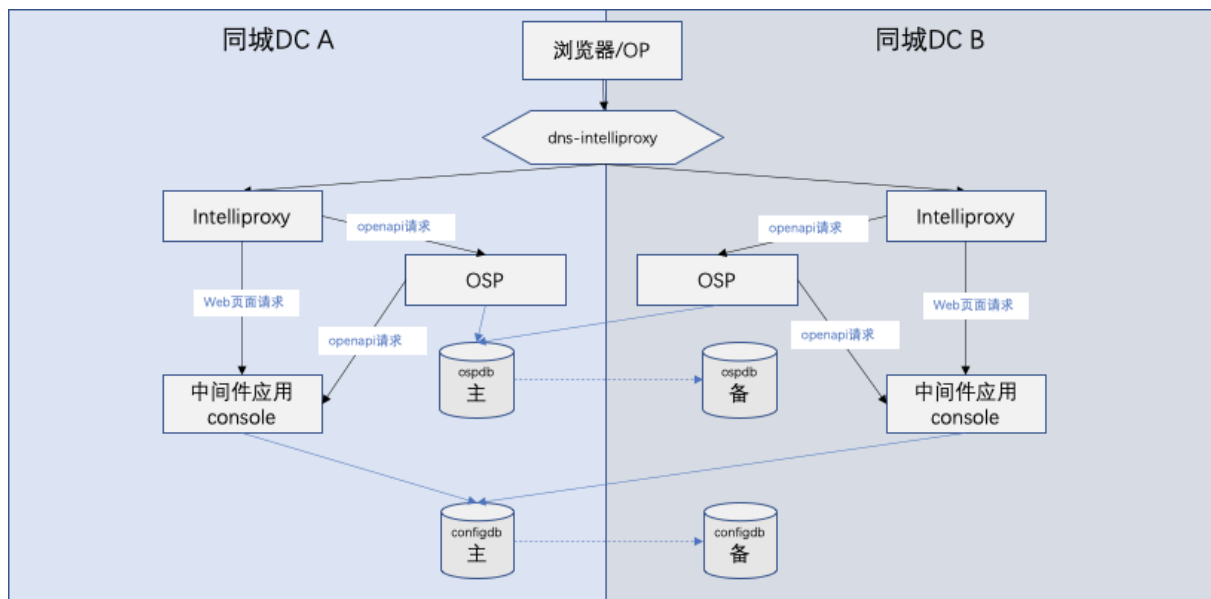
② 说明

网络恢复后会自动重连，在网络中断期间，Dsrconsole、ACVIP、OSP 及其他和管控台有关联的组件均无法使用。

3.2. OSP + Intelliproxy

3.2.1. 容灾架构

架构图



说明

- Intelliproxy 为中间件管控页面入口，各中间件管控页面所有 API 调用均为 OpenAPI，通过 OSP 代理。
- 图中“Web 页面请求”主要为静态资源请求。

容灾架构说明如下：

- Intelliproxy + OSP 主备机房需对等部署，数据库共库。
- Intelliproxy + OSP 只承载中间件控制层流量（Web 控制台页面和 OpenAPI），数据流则全部直连中间件各个应用。Intelliproxy 只能通过域名访问，通过域名解析对应的中间件服务。
- 客户端通过 DATACENTER 和 cell 属性来完成正常情况单机房流量收敛。

产品依赖

外部产品依赖

- ACVIP：Intelliproxy 通过 ACVIP 找到 SOFARegistry 地址。
- SOFARegistry：Intelliproxy、OSP、中间件应用 console 都会将自己注册到 SOFARegistry，以便发现彼此的 IP 来进行正确路由和转发。其中客户端 SDK 为 sensor，是一个 SOFARegistry SDK 的简化版本，会注册 IP 和 Cell 信息。Cell 信息使服务发现本机房收敛。
- IAM：OSP 依赖 IAM 做统一认证。
- acmetaservice/apconsole：用于获取 workspace。该配置通过后置任务写入数据库。

底座产品依赖

- 元集群：元集群主备机房独立部署，无容灾要求。
- 内网 DNS：
 - ACVIP 通过内网 DNS 提供的域名访问数据库。容灾时，需将数据库域名切换至备机房的数据库。所以依赖内网 DNS 的容灾能力。
 - Intelliproxy 通过内网 DNS 提供的域名，双挂主备机房的内网负载均衡，对外提供服务。

- **内网负载均衡**：主备机房各自通过内网负载均衡进行负载。

内网 DNS 和 内网负载均衡 在不同底座下，有不同的选择。具体如下表所示：

底座	内网 DNS	内网负载均衡
AntStack	AntDNS	ALB
AntStack Plus 公有云	privatezone	SLB
AntStack Plus 物理机	AntDNS	-
AntStack Plus 物理机 + 飞天	AntDNS (forward opsdns)	-



注意

物理机底座下，AntStack Plus 目前没有内网负载均衡，实际部署时用客户环境选用的负载均衡设备。

数据库依赖

OB/RDS：主备机房共库，依赖 OB/RDS 的容灾能力。

数据同步

主备机房共库，依赖数据库的同步能力。

网络链路

- 用户应用通过 Intelliproxy 域名调用 OpenAPI。
- 用户通过 Intelliproxy 域名访问中间件控制台。

容灾能力

支持机房级/组件级容灾，容灾切换后无功能降级。

3.2.2. 热切换方案

容灾切换说明

- 容灾切换时需要切换域名，摘除故障机房的流量。
- 数据库容灾切换依赖数据库容灾能力。

切换逻辑

1. 切换元数据库 DB 和 内网 DNS。
2. 切换 Intelliproxy 内网域名，摘除故障机房的流量。
3. 切换完毕后，验证机房 OSP 状态。

切换原则

保证数据不丢失，业务断开后可以立即恢复。

3.2.3. 容灾处理场景

常见容灾场景及处理方式如下：

容灾场景	容灾切换	容灾恢复	容灾回切
主机房断电 或网络孤岛	<ol style="list-style-type: none">1. 切换元数据库 DB 和内网 DNS。2. 切换 Intelliproxy 域名，摘除主机房的流量3. 切换完毕后，验证备机房 Intelliproxy + OSP 状态。	无需人工干预，自动恢复。	<ol style="list-style-type: none">1. 切换元数据库 DB 和内网 DNS。2. 切换内网域名，挂载主机房流量。3. 切换完毕后，验证主机房 Intelliproxy + OSP 状态。
备机房断电、网络孤岛、脑裂	<ol style="list-style-type: none">1. 切换元数据库 DB 和内网 DNS。2. 切换内网域名，摘除备机房流量。3. 切换完毕后，验证主机房 Intelliproxy + OSP 状态。	无需人工干预，自动恢复。	<ol style="list-style-type: none">1. 切换元数据库 DB 和内网 DNS。2. 切换内网域名，挂载备机房流量3. 切换完毕后，验证备机房 Intelliproxy + OSP 状态。

② 说明

网络恢复后会自动重连，在网络中断期间，Dsrconsole、ACVIP、OSP 及其他和管控台有关联的组件均无法使用。

4. 日常运维

4.1. 监控和预警

系统监控指标和预警项清单

监控指标	监控指标说明	预警触发条件
Intelliproxy 磁盘空间监控	磁盘空间占用率监控	大于 80%
Intelliproxy 端口监控	端口是否可以访问	端口 80 无法访问
Intelliproxy 内存监控	内存占用率	大于 80%
Intelliproxy CPU 利用率	CPU 利用率	大于 80%
Portal 磁盘空间监控	磁盘空间占用率监控	大于 80%
Portal 端口监控	端口是否可以访问	端口 80、8080 无法访问
Portal 内存监控	内存占用率	大于 80%
Portal CPU 利用率	CPU 利用率	大于 80%
OSP 磁盘空间监控	磁盘空间占用率监控	大于 80%
OSP 端口监控	端口是否可以访问	端口号：80、8080 无法访问
OSP 内存监控	内存占用率	大于 80%
OSP CPU 利用率	CPU 利用率	大于 80%
ACVIP 磁盘空间监控	磁盘空间占用率监控	大于 85%
ACVIP 端口监控	端口是否可以访问	端口 9003 无法访问

监控指标	监控指标说明	预警触发条件
ACVIP 内存监控	内存占用率	大于 90%

自定义监控信息

ACVIP IP 挂载数量

挂载数量之和小于配置的挂载数量阈值（例如：公有云参考值 1700）时，通过短信或者钉钉进行告警。可用于评估 ACVIP 的负载情况、功能大概是否正常、是否挂载了所有的 IP。

acvip_ip挂载数量 17

类型: 分钟统计无 Key 创建人: antCloudAdmin 创建时间: 2021-03-27 18:22:15 最后修改人: antCloudAdmin 最后修改时间: 2021-03-27 18:22:15

* 所属应用: ACVIP-acvip x 手动填写应用

* 采集日志文件: /home/admin/logs/acvip/StatusMonitor.log 扫描选取 手动填写日志路径

生成开关: ☒

描述: 记录配置描述, 最长不超过100个字

高级选项

采集筛选

采集元数据选择过滤(高级配置)

日志筛选

日志请日志筛选

+ 新增黑名单筛选 + 新增黑名单筛选

提示: 如果填入多个值, 如A,B, 白名单筛选需要A或B, 黑名单筛选需要A和B

* 白名单选择: HealthCheckController * 黑名单: HealthCheckController

统计方式

* 求值方式: 对列值求和

* 求和列: ipcount

告警配置

第1个告警配置

复制告警名称 删除告警名称

* 告警名称: 第1个告警配置

日志文件为: /home/admin/logs/acvip/StatusMonitor.log , 示例如下:

```
2021-04-20 17:07:41.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size:5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps: [10.126.13.53, 10.126.13.67]
2021-04-20 17:08:42.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size:5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps: [10.126.13.53, 10.126.13.67]
2021-04-20 17:09:43.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size:5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):94ms, [ERROR] failureIps: [10.126.13.53, 10.126.13.67]
2021-04-20 17:10:44.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size:5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps: [10.126.13.53, 10.126.13.67]
2021-04-20 17:11:45.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size:5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):94ms, [ERROR] failureIps: [10.126.13.53, 10.126.13.67]
2021-04-20 17:12:46.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size:5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps: [10.126.13.53, 10.126.13.67]
2021-04-20 17:13:47.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size:5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):94ms, [ERROR] failureIps: [10.126.13.53, 10.126.13.67]
2021-04-20 17:14:48.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size:5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps: [10.126.13.53, 10.126.13.67]
2021-04-20 17:15:49.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size:5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps: [10.126.13.53, 10.126.13.67]
2021-04-20 17:16:50.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size:5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps: [10.126.13.53, 10.126.13.67]
2021-04-20 17:17:51.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size:5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):94ms, [ERROR] failureIps: [10.126.13.53, 10.126.13.67]
```

ACVIP 健康检测

对健康检测值求和，小于配置的健康值阈值（例如 1900）时，通过短信或钉钉进行告警。用来评估 ACVIP 的负载情况。

自定义名称 / 编辑

acvip健康检测

类型: 分钟统计无 Key | 创建人: antCloudAdmin | 创建时间: 2021-03-27 18:22:15 | 最后修改人: antCloudAdmin | 最后修改时间: 2021-03-27 18:22:15

所属应用: ACVIP-acvip

采集日志文件: /home/admin/logs/acvip/StatusMonitor.log

生成开关: ☒

描述: 记录配置描述, 最长不超过100个字

采集筛选

采集元数据筛选通过(高级配置)

日志筛选

新增白名单筛选 新增黑名单筛选

白名单选择: HealthCheckController 黑名单: HealthCheckController

统计方式

求值方式: 列求和

求和列: HealthCheckController

告警配置

第1个告警配置

告警配置名称: 第1个告警配置

日志文件为: /home/admin/logs/acvip/StatusMonitor.log , 日志示例如下:

```
root@zjknoifn-acvip-acvip-0 /home/admin/logs/acvip# tail -n 50 StatusMonitor.log | grep HealthCheckController
021-04-20 17:16:50.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:17:51.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):94ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:18:52.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:19:53.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):113, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:20:54.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:21:55.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):112, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:22:56.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:23:57.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:24:58.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:25:59.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):94ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:27:00.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:28:01.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):94ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:29:02.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:30:03.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):94ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:31:04.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):115, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:32:05.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
root@zjknoifn-acvip-acvip-0 /home/admin/logs/acvip#
```

ACVIP 域名个数

对域名个数进行求和, 小于配置的域名个数阈值(例如 500)时, 通过短信或者钉钉进行告警。用来评估 ACVIP 的负载情况, 以及健康检查的机器是否正常。

您可以登录 ACVIP 后台查看配置个数。

类型: 分钟级访问 Key | 创建人: antCloudAdmin | 创建时间: 2021-03-27 18:22:15 | 最后修改人: antCloudAdmin | 最后修改时间: 2021-03-27 18:22:15

* 所属应用: ACVIP-acvip x 手动填写应用

* 采集日志文件: /home/admin/logs/acvip/StatusMonitor.log 扫描获取 手动填写日志路径

生效开关: ☒

描述: 记录配置描述, 最长不超过100个字

高级选项

采集筛选

采集元数据选择过滤(高级配置)

日志筛选

新增白名单筛选 新增黑名单筛选

* 白名单选择: HealthCheckController * 黑名单: HealthCheckController

统计方式

* 求值方式: 对列求和

* 求配: domain size

告警配置

第1个告警配置

* 告警配置名称: 第1个告警配置

日志文件为: /home/admin/logs/acvip/StatusMonitor.log , 日志示例如下:

```
root@zjknofin-acvip-acvip-0 /home/admin/logs/acvip#
tail -n 50 StatusMonitor.log | grep HealthCheckController
021-04-20 17:16:50.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:17:51.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):94ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:18:52.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:19:53.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):113, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:20:54.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:21:55.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):112, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:22:56.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:23:57.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:24:58.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:25:59.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):94ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:27:00.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:28:01.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):94ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:29:02.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:30:03.553 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):94ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:31:04.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):115, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
021-04-20 17:32:05.554 [AntVip-Monitor] INFO com.antcloud.antvip.common.log.StatusMonitorLogger - [HealthCheckController] responsibleDomainNames'size:5, schedulingDomainNames'size
5, ipCount:10, healthCheckCount(lastInterval):116, averageDelay(lastInterval):93ms, [ERROR] failureIps:[10.126.13.53, 10.126.13.67]
root@zjknofin-acvip-acvip-0 /home/admin/logs/acvip#
```

ACVIP 检测耗时

检测耗时超过配置的耗时阈值（例如 900ms）时，通过短信或者钉钉进行告警。

类型: 分钟统计/无 Key | 创建人: antCloudAdmin | 创建时间: 2021-03-27 18:22:15 | 最后修改人: antCloudAdmin | 最后修改时间: 2021-03-27 18:22:15

* 采集日志文件: /home/admin/logs/acvip/acvip-default.log [扫描选取] [手动填写日志路径]

生效开关: ☒

描述: 记录配置描述, 最长不超过100个字

高级选项

采集筛选

采集元数据选择过滤(高级配置)

日志筛选 [取消清除日志筛选]

+ 新增白名单筛选 + 新增黑名单筛选

提示: 如果填入多个值, 如A,B, 白名单筛选是要A或B, 黑名单筛选是不要A和B

* 白名单筛选: 租户 * 黑名单: instanceid

统计方式

* 求值方式: 求行数

告警配置

第1个告警配置 [复制告警配置] [删除告警配置]

* 告警名称: 第1个告警配置

* 规则: 是否开启: ☒

日志文件为: /home/admin/logs/acvip/acvip-default.log。

CommonError 监控

报错行数大于配置的报错行数阈值（例如 100）时，通过钉钉进行告警，大于 200 时，通过短信进行告警。

自定义监控 / 编辑

commonerror ☆ [查看数据] [更多]

类型: 分钟统计/无 Key | 创建人: antCloudAdmin | 创建时间: 2021-03-27 18:22:16 | 最后修改人: antCloudAdmin | 最后修改时间: 2021-03-27 18:22:16

* 所属应用: ACVIP-acvip X [手动填写应用]

* 采集日志文件: /home/admin/logs/acvip/common-error.log [扫描选取] [手动填写日志路径]

生效开关: ☒

描述: 记录配置描述, 最长不超过100个字

高级选项

采集筛选

采集元数据选择过滤(高级配置)

日志筛选 [取消清除日志筛选]

+ 新增白名单筛选 + 新增黑名单筛选

提示: 如果填入多个值, 如A,B, 白名单筛选是要A或B, 黑名单筛选是不不要A和B

* 白名单筛选: ERROR * 黑名单: ERROR

统计方式

* 求值方式: 求行数

告警配置

告警名称: 1 [复制告警配置] [删除告警配置]

日志文件为: /home/admin/logs/acvip/common-error.log。

预警项运维动作说明

ACVIP 磁盘空间预警

预警项说明

ACVIP 服务节点磁盘空间预警。

运维动作说明

登录对应的服务器，进入 `/home/admin/logs/acvip` 目录，对大文件进行清除。一般是 `common-default.log` 文件。

4.2. 系统日志

产品	日志路径	说明
Portal	系统运行日志： <code>/home/admin/logs/node-stdout.log</code>	记录应用启动和运行过程中的全部日志。
	系统错误日志： <code>/home/admin/logs/node-stderr.log</code>	记录应用运行过程中抛出的错误信息，主要包括代理转发过程中的错误信息。
OSP	系统运行日志： <code>/home/admin/logs/</code>	记录应用启动和运行过程中的全部日志。其中， <code>/osp</code> 子目录是 OSP 系统主要运行日志，包含如下日志： <ul style="list-style-type: none"><code>/home/admin/logs/osp/user-façade.log</code> 是跟用户鉴权相关的日志。<code>/home/admin/logs/osp/openapi.log</code> 是跟 OpenAPI 请求转发相关的日志。<code>/home/admin/logs/osp/operation-product-instance.log</code> 是跟产品启动相关的日志。
	系统错误日志： <code>/home/admin/logs/osp/common-error.log</code>	记录应用启动和运行过程中抛出的错误信息。

产品	日志路径	说明
	系统默认日志： /home/admin/logs/osp/common-default.log	记录应用启动和运行过程中所有的 info 级别日志。
Intelliproxy	系统运行日志： /home/admin/logs/	记录应用启动和运行过程中的全部日志。其中， /home/admin/logs/access.log 日志记录所有经过 Intelliproxy 代理转发的 REST 服务 API 的流量，不会记录静态资源或者非符合标准规范的 API 请求。遇到转发问题时，可以通过 Intelliproxy /home/admin/logs/access.log 查看 转发是否存在异常情况。若异常，确认 OSP 或业务方应用是否存在异常。
	系统错误日志： /home/admin/logs/common-error.log	记录应用启动和运行过程中抛出的错误信息。
ACVIP	系统运行日志： /home/admin/logs/	记录应用启动和运行过程中的全部日志。其中， /acvip 子目录是 ACVIP 系统主要运行日志，包含如下日志： <ul style="list-style-type: none">• /home/admin/logs/acvip/acvip-default.log 是用户请求访问与响应，以及其他运行过程相关的日志。• /home/admin/logs/acvip/Startup.log 是系统启动和状态检查相关的日志。
	系统错误日志： /home/admin/logs/acvip/common-error.log	记录应用启动和运行过程中抛出的错误信息。

4.3. 服务巡检

4.3.1. 系统组件监控检查

基础监控检查

登录 RMS 监控系统，查看系统中台组件相关系统组件有无异常告警，需要关注的监控项内容如下表所示。

应用	分类	指标（关键字）	告警阈值
INTELLIPROXY-intelliproxyOSP-ospPORTAL-portal	基础监控-CPU 使用率监控	cpu_usage	>80%
	基础监控-内存使用率监控	mem_usage	>80%
	基础监控-磁盘使用率监控	disk_usage	>80%
	基础监控-load5	load5	>3
INTELLIPROXY-intelliproxy	基础监控-端口监控	80、2022	不通
OSP-osp	基础监控-端口监控	2022、8341	不通
PORTAL-portal	基础监控-端口监控	80、2022	不通
ACVIP-acvip ACVIP-cloudinc	基础监控-CPU 使用率监控	cpu_usage	>80%
	基础监控-内存使用率监控	mem_usage	>90%
	基础监控-磁盘使用率监控	disk_usage	>85%
	基础监控-load5	load5	参考值为：CPU 2.5 倍
ACVIP-acvip	基础监控-端口监控	9003、2022、12200	不通

自定义业务监控检查

通过 RMS 控制台查看云中台产品各项系统监控指标。访问方式：

1. 登录 RMS 控制台。
2. 在左侧导航栏单击 **应用监控**，然后单击 **全部应用** 页签。
3. 在 **搜索应用** 文本框输入中台产品（例如 ACVIP），然后单击 **🔍** 按钮。

4. 单击目标应用名称，即可查看系统监控详情。

如果有异常告警产生，联系技术支持进行排查。

4.3.2. 业务功能检查

OSP 服务验证

说明

`netstat -an | grep PORT` 判断监听端口是否正常，有端口进程说明是正常的，无端口进程说明是不正常的。

- 执行以下命令，判断监听端口是否正常。

```
netstat -an | grep 80
```

- 执行以下命令，判断业务端口是否存活。

```
netstat -an | grep 8341
```

- 执行以下命令，判断 acvip 连接。

```
netstat -an | grep 9003
```

- 执行以下命令，判断注册中心连接。

```
netstat -an | grep 9600
```

- 访问 `sofa-osp.{domain}/admin/index.html` 页面，判断是否能正常访问。

- 访问 `http://sofa-osp.{domain}/api/admin/services/{ms/mq/dds/...}/addresses` 页面，查看 OSP 上订阅的地址。地址不应为空，且每个服务都至少有两个以上地址返回，否则就存在单点问题。

Intelliproxy 服务验证

- 执行以下命令，判断业务端口是否正常。如果端口没有启动，那通常是程序启动失败，需要通过排查 `common-error.log` 日志解决。

```
netstat -an | grep 80
```

- 执行以下命令，判断 acvip 连接。

```
netstat -an | grep 9003
```

- 执行以下命令，判断注册中心连接。

```
netstat -an | grep 9600
```

Portal 服务验证

- 访问 `http://sofa-portal.{domain}` 页面，查看各页面功能是否正常。

ACVIP 服务验证

- 执行以下命令，检查 9003 端口是否有监听。

```
netstat -an | grep 9003
```

- 检查 ACVIP 域名是否创建成功。

其他中间件部署之后，需确认 ACVIP 域名创建成功以及 IP 挂载正常。

ACVIP 域名可以在 ACVIP 控制台查看，acvip 控制台的访问地址是：public-lb vip 或 ip。

- 检查 antvip server 节点存活状态，可以通过以下任一方式查看。

- 直接登录对应的服务器查看进程和端口是否存在。

```
ps -ef | grep acvip-web
```

- 登录 ACVIP 控制台，查看 antvip server 信息。

5. 中间件细粒度权限管控方案

目前中间件只有 `middleware_root`、`middleware_master`、`middleware_developer`、`middleware_observer` 四种角色，权限管控粒度比较粗，本文介绍如何通过 IAM 实现中间件更灵活、可配的权限管控能力。

当前鉴权流程

1. 各个中间件控制台通过引入 OSP 的 JAR 包，引入了 `UserInfoFetcherJaxrsFilter`，并通过 RPC 调用 OSP 的 `UserFacade`。`UserFacade` 会通过调用 IAM 的 WebAPI 获取用户信息以及用户和用户下的所有租户的角色，最后会把信息写入 `resteasy` 的 `context` 上下文。
2. 在引入 OSP 的 JAR 包的同时，也会引入一个 `OSPRoleBasedSecurityFilter`，该 Filter 通过一个对应的 Feature 去提取各个中间件控制台代码上打的注解（`RolesAllowed`），来提取调用该方法需要具有的角色，再调用上面写入的 `context` 的 `hasAnyRoles` 进行鉴权。
3. `hasAnyRoles` 会调用 OSP 的 `UserFacade` 的 `judge` 方法，`judge` 方法会调用 IAM 的 OpenAPI 进行鉴权。
OpenAPI 的请求参数里除了必带的 `tenant` 参数，剩余参数中：
 - `action` 用于添加角色。
 - `conditions` 在 mock 掉 `apconsole` 的情况下传入 `instanceId`；不 mock 的情况下传入 `workspace`。

细粒度管控方案

IAM 除了支持 `condition` 这种自定义条件，还支持通过 `resource` 进行资源级别的鉴权。方法如下：

- 各个中间件控制台代码，以 `dsrcconsole` 为例，需要在 IAM 控制台配置多个角色，角色里包含若干个 `action`，`action` 可以定位为 OpenAPI 的 API 名称（例如 `ms.ddcs.attribute.add`）。
- 在接口上增加注解：

```
@RolesAllowed(MS.DDCS_DEVELOPER)
String getConfig();

@MiddlewareAuth(MS_DDCS_ATTRIBUTE_ADD, method=POST)
String addAttribute(String attribute);
```

以上注解是 IAM 会用到的 `action`，并搭配类似 HTTP 的 `Method`。

- 将 OSP 的 SDK 升级到 1.2.19 版本。

以上操作完成后，您可以参考以下配置示例将中间件产品接入 IAM。

配置示例

以 `dsrcconsole` 接入 IAM 鉴权为例，操作如下：

1. 在云游中发布微服务前，修改以下应用启动参数：

- o `osp.canUseJudge=true`（必选）：鉴权是否远程调用 OSP 接口。false 为不使用；true 为使用。

- o `osp.auth.fine.grain=true`（必选）：是否使用 OSP 细粒度鉴权。true 为启用；false 为不启用。

默认不启用，使用旧的共享中间件管理员、共享中间件观察者、共享中间件开发者鉴权。

- o `osp.auth.strict.mode=false`（可选）：是否使用 OSP 细粒度鉴权严格模式。true 为使用；false 为不使用。

默认不启用，严格模式下，查看的请求也会报 403 错误。

2. 在 IAM 控制台录入权限。

i. 下载 [MS 操作点](#)。

ii. 登录 IAM 控制台。

iii. 选择租户为 ROC。



iv. 在左侧导航栏选择 **系统管理 > 权限元数据**。

v. 单击 **权限录入**，然后将步骤 1 下载的文件上传。

vi. 单击 **提交**。

6. 常见故障处理

6.1. 常见问题

中间件门户首页页面无法访问

1. 确认 OSP 系统已经部署成功。
2. 使用中间件租户账号登录 OSP 管理员后台，检查 Portal 是否正常上报机器 IP 地址。

查看路径为：`\${OSP域名}/api/admin/services/osp/addresses`。

3. 如果 IP 未上报，则查看 Portal docker 镜像的日志信息。

OSP 管理控制台页面白屏

确认右上角所选的租户为共享中间件（ALIPAYCN），工作空间为 middleware。

如何查看 OSP 是否为 mock 状态

检查数据库里的 `t_admin_config` 表的 `auth.disabled` 配置，true 表示 mock 状态；false 表示非 mock 状态。

OSP 管理控制台无法访问，按 F12 进入调试模式发现 groupByRegion 接口报错

1. 检查当前环境是否部署了 apconsole。
通常只有经典 PaaS 环境才需要部署 apconsole。
2. 如果没有部署 apconsole，则确认 OSP 数据库里 `t_admin_config` 表的 `core.apconsole.url` 为 OSP 自身的 SLB 地址。
如果不是，需修改为 OSP 的 SLB 地址。

中间件门户首页可以访问，但首页监控视图部分数据显示不正确或无数据

可能是 监控预警 产品的问题和异常，可以查看监控预警的控制台和日志排查问题。

首页可以访问，但页面显示（或加载时）有错误提示

1. 进入 监控预警 控制台，选择 应用视图。
2. 选择 000001 实例 ID（只有中间件租户账号可以看见实例 ID 并进行此操作）。
3. 搜索应用 OSP，查看其 JVM 监控视图。
4. 如果 JVM 从某个时刻开始有跌 0，则 OSP 应用可能非正常退出。
5. 此时，可通过 发布部署服务，查询定位到具体的应用，选择异常的服务实例点击 重启应用。

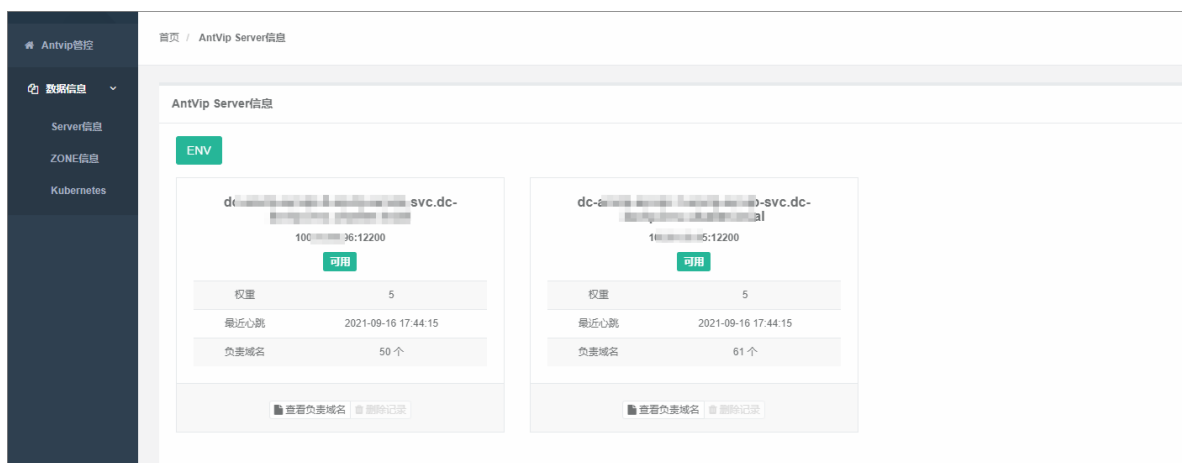
如何确认 ACVIP server 节点存活状态

通过以下任一方式，确认 ACVIP server 节点存活状态。

- 登录对应的服务器，执行以下命令，查看进程和端口是否存在。

```
ps -ef | grep AntVipServerBootstrap
```

- 登录 ACVIP 控制台查看，如下图所示。



ACVIP 拉取不到域名列表

在应用端日志里面出现 Domain Not Found，但该域名在 ACVIP 上存在。登录 ACVIP 控制台，可查看到 ACVIP 节点显示不可用，但进程和端口都存在，且心跳时间也在变化，如下图所示。



此时，需要确认 ACVIP 服务器上的时间和数据库的时间是否一致。如果不一致，则要对数据库所在主机的时间以及应用所在主机的时间进行调整同步，保持一致。

ACVIP 部署问题

前置条件

解决 ACVIP 部署问题时，请先按照以下内容确认您的环境：

- 数据库时间和 ACVIP 机器时间需要一致，否则无法部署完成。

- 查看机器时间

命令如下：

```
date -R
```

- 查看数据库时间

- a. 获取 DB 连接。

```
env | grep data
```

- b. 连接数据库。

```
mysql -h<hostname> -u<username> -p<passwd> -P <port> -D <DB 链接>
```

- c. 查看数据库时间。

```
select now()
```

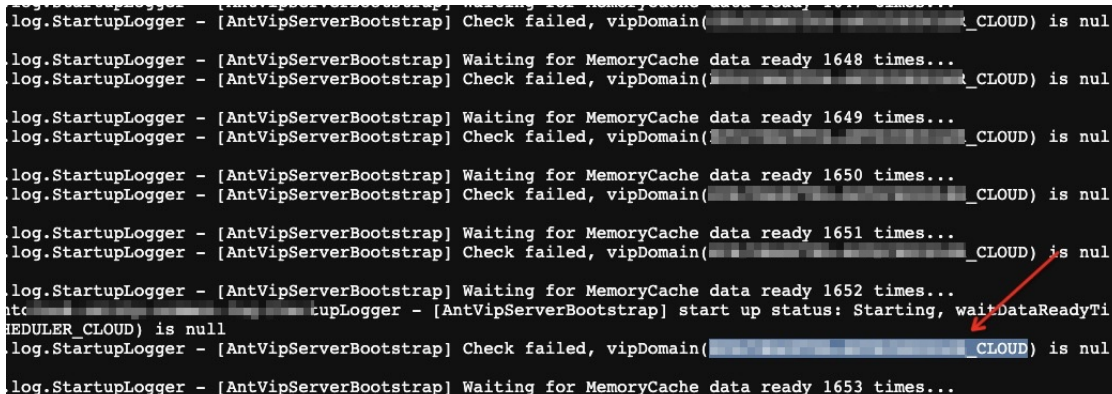
- 数据库版本不能为 MySQL 8。

- `/etc/hosts` 文件中需要有 IPv4 地址和 hostname 的映射配置。

ACVIP 部署不到终态

排查步骤如下：

1. 查看启动日志 `/home/admin/logs/acvip/Startup.log`。



```
log.StartupLogger - [AntVipServerBootstrap] Check failed, vipDomain( ) is null
log.StartupLogger - [AntVipServerBootstrap] Waiting for MemoryCache data ready 1648 times...
log.StartupLogger - [AntVipServerBootstrap] Check failed, vipDomain( ) is null
log.StartupLogger - [AntVipServerBootstrap] Waiting for MemoryCache data ready 1649 times...
log.StartupLogger - [AntVipServerBootstrap] Check failed, vipDomain( ) is null
log.StartupLogger - [AntVipServerBootstrap] Waiting for MemoryCache data ready 1650 times...
log.StartupLogger - [AntVipServerBootstrap] Check failed, vipDomain( ) is null
log.StartupLogger - [AntVipServerBootstrap] Waiting for MemoryCache data ready 1651 times...
log.StartupLogger - [AntVipServerBootstrap] Check failed, vipDomain( ) is null
log.StartupLogger - [AntVipServerBootstrap] Waiting for MemoryCache data ready 1652 times...
log.StartupLogger - [AntVipServerBootstrap] start up status: Starting, waitDataReadyTi
log.StartupLogger - [AntVipServerBootstrap] Check failed, vipDomain( ) is null
log.StartupLogger - [AntVipServerBootstrap] Waiting for MemoryCache data ready 1653 times...
```

图中日志说明 domain 加载失败，需要确认发布失败的原因。

2. 查询 `antvip_vip_domain`。

查询命令如下：

```
select * from antvip_vip_domain
```

```

domain_type: NORMAL
***** 4. row *****
      id: 4
      name: DSR_HTTP_CLOUD
      app: NULL
      env: PROD
      station: MAIN_SITE
      zone: NULL
      protect_threshold: 50
      enable: 1
      health_check_type: TCP
health_check_default_port: 9600
      health_check_timeout: 2000
      health_check_interval: 5000
      health_check_raise: 1
      health_check_fall: 3
      health_check_payload:
      version: 13
      gmt_create: 2020-11-13 11:00:58
      gmt_modified: 2021-02-24 15:05:44
      owner: osp
      health_check_enable: 1
      domain_type: NORMAL
***** 5. row *****
      id: 5

```

查找是否有步骤 1 中加载失败的域名，且 enable 是否为 1，为 1 则继续下面的步骤。

3. 查询是否存在有效节点。

查询命令如下：

```
select * from antvip_real_node where domain_id=4
```

```

MySQL [cloudinc]> select * from antvip_real_node where domain_id=4;
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id | domain_name | ip | fqdn | env | zone | weight | health_check_port | enable | gmt_create | gmt_modified | domain_id | data_center |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 13001 | NULL | 10.128.0.111 | DSR_HTTP_CLOUD | PROD | ENV | 1 | 9600 | 0 | 2020-12-25 17:36:38 | 2021-02-24 15:05:44 | 4 | NULL |
| 13002 | NULL | 10.128.0.40 | DSR_HTTP_CLOUD | PROD | ENV | 1 | 9600 | 0 | 2020-12-25 17:36:49 | 2021-02-24 15:05:44 | 4 | NULL |
| 13005 | NULL | 10.186.112.216 | DSR_HTTP_CLOUD | PROD | ENV | 1 | 9600 | 1 | 2021-02-24 14:58:15 | 2021-02-24 15:05:16 | 4 | NULL |
| 13006 | NULL | 10.186.112.217 | DSR_HTTP_CLOUD | PROD | ENV | 1 | 9600 | 1 | 2021-02-24 15:05:34 | 2021-02-24 15:05:34 | 4 | NULL |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

确认节点是否存活，如果有不正常的节点，进行处理。如果都正常，继续进行下面的步骤。因为 ACVIP 有多个节点时，会有数据分组，这个 domain 可能是其他的 ACVIP 在进行加载。

4. 查询其他 ACVIP 节点。

查询命令如下：

```
select * from antvip_vip_server
```

```
mysql [cloudinc]> select * from antvip_vip_server;
```

id	host	weight	last_heartbeat	env	zone	gmt_create	gmt_modified	hostname
40	10.100.0.176:12200	5	2021-04-18 03:18:10	PROD	ENV	2020-11-10 20:36:27	2021-04-18 03:18:10	acvip-acvip-0-acvip-acvip-service.default.svc.cluster.local
41	10.100.0.226:12200	5	2021-04-18 03:18:10	PROD	ENV	2020-11-10 20:36:27	2021-04-18 03:18:10	acvip-acvip-1-acvip-acvip-service.default.svc.cluster.local
42	10.100.0.235:12200	5	2021-05-13 21:31:01	PROD	ENV	2020-12-11 11:12:37	2021-05-13 21:31:01	zjknofin-acvip-acvip-0-acvip-acvip-svc.zjknofin-acvip.svc.cluster.local
43	10.100.0.193:12200	5	2021-05-13 21:31:02	PROD	ENV	2020-12-11 11:14:50	2021-05-13 21:31:02	zjknofin-acvip-acvip-1-acvip-acvip-svc.zjknofin-acvip.svc.cluster.local

心跳时间 (last_heartbeat) 和当前时间相近的是活跃节点，需要测试当前服务器和这些服务器是否建立连接。

5. 确认网络连通性。

命令如下：

```
netstat -anlp | grep 12200
```

```
root@zjknofin-acvip-acvip-0 /home/admin/logs/acvip]# netstat -anlp | grep 12200
```

tcp	0	0	0.0.0.0:12200	0.0.0.0:*	LISTEN	-
tcp	0	0	10.100.0.235:58536	10.100.0.226:12200	ESTABLISHED	-
tcp	0	0	10.100.0.235:12200	10.100.0.176:42242	ESTABLISHED	-
tcp	0	0	10.100.0.235:12200	10.100.0.226:38892	ESTABLISHED	-
tcp	0	0	10.100.0.235:58202	10.100.0.193:12200	ESTABLISHED	-
tcp	0	0	10.100.0.235:34950	10.100.0.176:12200	ESTABLISHED	-
tcp	0	0	10.100.0.235:12200	10.100.0.193:41464	ESTABLISHED	-

查看 ACVIP 的 12200 端口是否有正常的通讯，有则表示网络正常，建议联系售后技术支持进行排查；如果没有通讯，则说明网络出现故障，建议检查网络问题。

使用问题

获取不到域名信息如何处理？

使用 `curl` 命令尝试获取域名信息，获取命令如下：

```
curl -i -XPOST {acvip地址}:9003/antcloud/antvip/instances/get -d '{"vipDomainName2ChecksumMap":{"000001-DSR_CLOUD":"N"}}'
```

长连接 Long Polling 命令示例如下：

```
curl -i -XPOST localhost:9003/antcloud/antvip/instances/get -d '{"vipDomainName2ChecksumMap":{"000001-DSR_CLOUD":"N"},"allowPolling":true}'
```

```
# curl -i -XPOST localhost:9003/antcloud/antvip/instances/get -d '{"vipDomainName2ChecksumMap":{"000001-DSR_CLOUD":"N"}}'
```

```
HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 982
```

```
{
  "acceptTime": 0,
  "errorCode": 0,
  "prettyErrorMsg": "null(errorCode:0)",
  "startTime": 1620913902122,
  "success": true,
  "transmissionTime": -1620913902122,
  "vipDomains": [
    {
      "healthCheckDefaultPort": 9600,
      "healthCheckEnable": false,
      "healthCheckFall": 3,
      "healthCheckInterval": 5000,
      "healthCheckPayload": {},
      "healthCheckRaise": 1,
      "healthCheckTimeout": 2000,
      "healthCheckType": "TCP",
      "name": "000001-DSR_CLOUD",
      "protectThreshold": 50,
      "realNodes": [
        {
          "available": true,
          "effectiveHealthCheckHost": "10.100.112.216:9600",
          "effectiveHealthCheckPort": 9600,
          "falling": false,
          "healthCheckPort": 9600,
          "ip": "10.100.112.216",
          "lastHealthCheckTime": 1618498212285,
          "raising": false,
          "reason": "Success",
          "roundTripTime": 1,
          "weight": 1,
          "zone": "ENV",
          "available": true,
          "effectiveHealthCheckHost": "10.100.112.217:9600",
          "effectiveHealthCheckPort": 9600,
          "falling": false,
          "healthCheckPort": 9600,
          "ip": "10.100.112.217",
          "lastHealthCheckTime": 1618498215385,
          "raising": false,
          "reason": "Success",
          "roundTripTime": 1,
          "weight": 1,
          "zone": "ENV"
        }
      ],
      "version": 14
    }
  ]
}
```

- 查询到结果，说明 ACVIP 服务正常，请检查本地 ACVIP 配置。

i. 执行 `cd /home/admin/conf/acvip-java-client-cache/domains/` 命令，查看本地缓存中是否有目标域名信息，并查看获取的时间信息。

ii. 如果获取信息失败，查看 `api-stat.log` 是否有报错。

```
cd /home/admin/logs/acvip-java-client
cat api-stat.log
```

iii. 根据查询的报错信息进行处理。

您可以查询指定时段的 JAVA 客户端拉取记录，命令如下：

```
tail -n 500 acvip-default.log.2021-05-12 | grep java
```

```
root@zjknofin-acvip-acvip-0 /home/admin/logs/acvip]
# tail -n 500 acvip-default.log.2021-05-12 | grep java
2021-05-13 22:00:30.294 [AntVip-PollingWorker-Executor-4] INFO com.antcloud.acvip.server.log.ServerAccessLogger - [Access][Polling][java-client-1.0.7,/10.100.112.209:64714,acpr
sdapigw] reqDomains:2, rspDomains:0, rspNameList:0, requestTransmitTime:0, responseProcessTime:50398
2021-05-13 22:00:30.894 [AntVip-PollingWorker-Executor-5] INFO com.antcloud.acvip.server.log.ServerAccessLogger - [Access][Polling][java-client-1.0.4,/100.121.113.56:35937,AntV
ipDefaultAppName] reqDomains:2, rspDomains:0, rspNameList:0, requestTransmitTime:1, responseProcessTime:50389
2021-05-13 22:01:10.694 [AntVip-PollingWorker-Executor-7] INFO com.antcloud.acvip.server.log.ServerAccessLogger - [Access][Polling][java-client-1.0.4,/100.121.113.61:5377,AntVi
pDefaultAppName] reqDomains:3, rspDomains:0, rspNameList:0, requestTransmitTime:1, responseProcessTime:50379
2021-05-13 22:01:21.694 [AntVip-PollingWorker-Executor-4] INFO com.antcloud.acvip.server.log.ServerAccessLogger - [Access][Polling][java-client-1.0.7,/10.100.112.209:64714,acpr
sdapigw] reqDomains:2, rspDomains:0, rspNameList:0, requestTransmitTime:0, responseProcessTime:50399
```

日志格式如下：

```
this.info(
    msgFormat: "[Access][Polling][%s,%s,%s] reqDomains:%s, rspDomains:%s, rspNameList:%s, requestTransmitTime:%s, responseProcessTime:%s",
    from, address, appName, reqDomains, rspDomains, rspNameList, transmitTime, processTime);
}
```

- 如果查询到的结果是空，需要到 ACVIP 服务端增加域名配置。
- 如果网络报错，确认 ACVIP 服务器地址配置是否正确。

如何查看客户端的请求内容？

您可以在 ACVIP 上执行如下命令查看：

```
tcpdump port 9003 and host <对端 IP> -nnvvXS
```

6.2. 普通用户登录 SOFA 控制台后拥有管理员权限

问题现象

某专有云环境，普通用户登录到 SOFA 控制台之后也有管理员权限。例如一个普通的用户拥有开发者（不是中间件开发者）和中间件观察者的权限，却能禁用微服务里面的任何服务。

排查过程

1. 查看 OSP 的 /home/admin/logs/osp/user-facade.log 日志。

```
2020-04-23 09:33:17.342 INFO - 用户信息 0000015527/005...Y...BAX
authorization-bmac%20000001...-1%3Ad0JntGtMumpYQWV622t0fZk0fRM1p1d11KbWDRUP10D~0
{"roles":["middleware_master"],"tenantInfo":{"instanceIds":["4...f...PBS","...TYQUM...INS5","BfTPDRME...5...P","BLJ57CRCQP/K
...SE...L...JW","KETA2...E3D65","3QCELV...UBAK","...330F0YMKTN","SHAFREYGT..."],"tenantId":"ANTCLOUD","workspaceIds":["
BOTJDEV","B...RT","BOTJSSI","BOTJTEST","BOTJIA","BOTJWS","BOTJWS2","BOTJWS3","BOTJWS4","BOTJWS5","BOTJWS6","LiAutom
{"$ref":"$.tenantInfo"},"useJudge":false,"user":{"id":"000...25...","loginName":"test@test.com","realName":"test"}}
```

从日志中可以看出，该用户的 role 是 middleware_master。

