



云监控 常见问题

文档版本: 20220512



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。

- 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。
- 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。
- 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
⚠ 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。	會学者 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。	大意 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 <i>,</i> 不是 用户必须了解的内容。	⑦ 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 cd /d C:/window 命令,进入 Windows系统文件夹。
斜体	表示参数、变量。	bae log listinstanceid
[] 或者 [alb]	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。	switch {active stand}

目录

1.	产品使用	05
	1.1. 签名算法: HMAC-SHA1	05
	1.2. 利用pssh批量安装云监控插件	06
	1.3. 云监控添加进程监控报错: Add Task Error	07
	1.4. 云监控控制台为什么CPU健康显示为0%	07
	1.5. 禁用ECS的内网后不能使用云监控	08
	1.6. 云监控610报警含义	08
	1.7. 云监控ECS的Windows主机CPU监控数值异常	08
2.	故障排查	10
	2.1. 如何排除云监控插件异常停止问题?	10
	2.2. 如何重启云监控C++版本插件?	11
	2.3. 如何通过云监控查看指定日期的监控数据?	11
	2.4. 非阿里云主机如何通过Nginx代理服务器上报监控数据?	12
	2.5. 如何卸载云监控插件?	16
	2.6. 如何处理云服务器ECS内网流量增高问题?	18
	2.7. 如何处理在阿里云主机上自动安装云监控插件失败问题?	20
	2.8. 站点监控任务到期后如何处理?	20
	2.9. 如何处理云监控插件心跳检查失败问题?	20
	2.10. 如何处理未收到报警电话的问题?	21
	2.11. 如何处理云监控识别多台相同镜像主机异常问题?	21

1.产品使用

1.1. 签名算法: HMAC-SHA1

目前,云监控只支持数字签名算法HMAC-SHA1。通过本文您可以了解数字签名算法HMAC-SHA1的操作方法。

操作步骤

1. 准备可用的阿里云访问密钥。

当HTTP请求生成签名时,需要使用一对访问密钥(AccessKey ID和AccessKey Secret)。

```
⑦ 说明 您可以使用已存在的访问密钥,也可以创建新的访问密钥,但需要保证该密钥处在启用
状态。
```

2. 生成请求的签名字符串。

HTTP签名字符串由HTTP请求中的Method、Header和Body信息共同生成。

```
SignString = VERB + "\n"
```

- + CONTENT-MD5 + "\n"
- + CONTENT-TYPE + "\n"
- + DATE + "\n"
- + CanonicalizedHeaders + "\n"
- + CanonicalizedResource

上述签名字符串中的 \n 表示换行转义字符, + 表示字符串连接操作, 其他部分定义如下表所示。

名称	描述	示例	
VERB	HTTP请求的方法名称。	PUT、GET、POST	
	HTTP请求中Body部分的MD5值。		
CONTENT-MD5	⑦ 说明 MD5必须为大写 字母和数字字符串。	0B9BE351E56C90FED853B325242 53E8B	
CONTENT-TYPE	HTTP请求中Body部分的类型。	application/json	
	HTTP请求中的标准时间戳头。		
DATE	⑦ 说明 遵循RFC 1123格式,使用GMT标准时间。	Mon, 3 Jan 2010 08:33:47 GMT	
CanonicalizedHeaders	由HTTP请求中以 x-cms 和 x- acs 为前缀的自定义头构造的字 符串。	 x-cms-api-version:0.1.0 x-cms-signature 	
CanonicalizedResource	由HTTP请求资源构造的字符串。	/event/custom/upload	

上表中CanonicalizedHeaders和CanonicalizedResource构造方式如下:

- CanonicalizedHeaders
 - a. 将所有以 x-cms 和 x-acs 为前缀的HTTP请求头的名字转换成小写字母。
 - b. 将所有CMS和ACS自定义请求头按照字典序的升序进行排序。
 - c. 删除请求头和内容之间分隔符两端出现的任何空格。
 - d. 将所有的请求头和内容用 \n 分隔符组合成最后的CanonicalizedHeaders。
- CanonicalizedResource
 - a. 将CanonicalizedResource设置为空字符串("")。
 - b. 将CanonicalizedResource中放入待访问的URI, 例如: /event/custom/upload 。
 - c. 如果请求包含查询字符串(QUERY_STRING),则在CanonicalizedResource字符串尾部添加
 ? 和查询字符串。

其中 QUERY_STRING 是URI中请求参数按字典序排序后的字符串,其中参数名和值之间用 = 相隔组成字符串,并对参数名和值按照字典序升序排序,然后以 ④符号连接构成字符串。其公式化描述如下:

QUERY STRING = "KEY1=VALUE1" + "&" + "KEY2=VALUE2"

3. 生成请求的数字签名。

数字签名公式如下:

Signature=base16(hmac-sha1(UTF8-Encoding-Of(SignString), AccessKeySecret))

签名举例:

```
SignString="POST" + "\n"
+"0B9BE351E56C90FED853B32524253E8B" + "\n"
+"application/json" + "\n"
+"Tue, 11 Dec 2018 21:05:51 +0800" + "\n"
+"x-cms-api-version:1.0" + "\n"
+"x-cms-ip:127.0.0.1" + "\n"
+"x-cms-signature:hmac-shal" + "\n"
+"/metric/custom/upload"
accesskey="testkey"
accessSecret="testsecret" //签名密钥。
```

签名结果:

1DC19ED63F755ACDE203614C8A1157EB1097E922

1.2. 利用pssh批量安装云监控插件

本文为您介绍如何利用pssh批量安装云监控插件。

pssh介绍

pssh 是一个python写的批量执行工具,非常适合30台服务器以内的一些重复性的操作。例如安装一个软件,kill 一个进程,下载文件等。

单机安装云监控插件

bash -c "\$(curl http://cloudmonitor-agent.oss-cn-hangzhou.aliyuncs.com/release/install.sh)"

批量安装云监控插件

- 安装pssh
 - i. 安装 python 2.4 以上。
 - ii. 安装 pssh。

```
wget https://pypi.python.org/packages/source/p/pssh/pssh-2.3.1.tar.gz
tar zxf pssh-2.3.1.tar.gz
cd pssh-2.3.1
python setup.py install
```

- 配置IP列表,准备安装云监控插件的主机
 - i. 配置ip.txt文件。
 - ii. 格式为user@ip:port每行一个, port不填默认为22。
 - iii. 执行命令的用户需要有sudo权限。
 - iv. 批量安装的机器, 密码要相同, 也可以配置无密码互信。
- 批量执行

```
pssh -h ip.txt -A -i bash -c "$(curl http://cloudmonitor-agent.oss-cn-hangzhou.aliyuncs.co
m/release/install.sh)"
```

-h host列表文件

-A 手工输入密码,无密码互信不需要这个参数

-i执行的命令

查看云监控插件是否安装成功

pssh -h ip.txt -A -i"/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh status"

1.3. 云监控添加进程监控报错: Add Task Error

本文为您介绍云监控添加进程监控报错的原因及解决方法。

在云监控中添加进程监控的时候,遇到Add Task Error: add error的报错。

原因:是由于服务器上没有安装安骑士(云盾客户端)。

解决办法:请在服务器上安装安骑士(云盾客户端)。

1.4. 云监控控制台为什么CPU健康显示为0%

本文为您介绍云监控控制台CPU健康显示为0%的原因分析。

该问题通常主要是因为您的CPU使用率很低的缘故,从监控图上看CPU的使用基本在0.5%上下徘徊。

0	12.02.02.00	1 00 ¹ 05-00 12 00 ¹ 00-00	12.00 12.00	10.09.15.00	10.00 10.00

而ECS向云监控上报数据是一分钟一次,您在控制台上看到的数据是5分钟的平均值,如果5次上报的平均值都低于0.5就会显示0%的。

主机名/ID	插件版本	插件状态	所在区域	CPU/内存使用题	E 1 1	磁盘使用率	IP地址	操作
ecs i-2ze3jvsy7620gir	3.5.5	运行中	华北2 (北京)	CPU: 0%	内存: 13.2%	7.67%	47.94. 192.168.	と 报警規则
launch-advisor i-bp1ew0zfkjblsuw:	3.5.3	运行中	华东1 (杭州)	CPU: 1.3%	内存: 11.7%	• 20%	47.97. ,172.16.	レ 报警规则

1.5. 禁用ECS的内网后不能使用云监控

本文为您介绍为何禁用ECS的内网后不能使用云监控。

ECS服务器使用云监控服务,是不能禁用内网的。

因为云监控的通讯地址open.cms.aliyun.com是解析在内网上的,通过内网来进行通讯获取数据,如果禁用 了内网,云监控服务会出现无法正常使用,所以为了能够正常的使用云监控服务,必须要确保在服务器上能 连通open.cms.aliyun.com的80端口。



1.6. 云监控610报警含义

本文为您介绍云监控返回610状态码的报警含义。

报警规则 610 表示HTTP链接超时。

监测点探测您的网站时出现连接超时现象,云监控发出HTTP请求后5秒内没有回包,会返回610状态码。

建议您设置报警规则时增加重试次数、采用组合报警等,以便优化以及提高报警准确率。

1.7. 云监控ECS的Windows主机CPU监控数值异常

本文为您介绍云监控ECS的Windows主机CPU监控数值异常的原因及解决办法。

云监控中的ECS CPU监控数值如果出现为0或者负数(实际CPU使用率不是0),其他监控值都正常。这个问题主要出现在Windows的机器上,一般原因是Windows内部的性能计数器损坏了。

可以通过typeperf "\Processor(_Total)\% Processor Time"查看计数器是否正常。如果提示"错误:没有有效计数器",则说明计数器已损坏,可通过lodctr /r命令进行修复。

相关截图如下:

管理员: C:\Tindows\system32\cmd.exe	_ 🗆 X
C:\Users\Administrator>typeperf "\Processor(_Total)\% Processor Time"	_
错误:没有有效计数器。	
C:\Users\Administrator>lodctr /r	
信息: 成功地从系统备份存储中重建性能计数器设置 C:\Users\Administrator>typeperf "\Processor(_Total>\% Processor Time"	
"(PDH-CSU 4.0)","\\AY140122152254Z\Processor(_Total)\% Processor Time" "09/23/2015 09:15:30.964","4.681400" "09/23/2015 09:15:31.964","3.900100" "09/23/2015 09:15:32.964","3.118800" "09/23/2015 09:15:33.963","4.681400"	
命令成功结束。	
C: Wsers Administrator>_	
	-

2.故障排查

2.1. 如何排除云监控插件异常停止问题?

本文为您介绍云监控插件异常停止问题的排查和处理方法。

背景信息

云监控插件默认每3分钟一次心跳联网。如果15分钟没有心跳联网,则主机判断插件已经停止运行。 云监控插件自动停止的可能原因如下:

- 云监控插件无法与云监控服务器通信。
- 云监控插件进程已退出。

插件无法与云监控服务器通信

如果云监控插件之前运行正常,您可以通过重新安装云监控插件来恢复其运行状态。

• 自动安装插件

操作方法请参见自动安装插件(推荐)。

• 手动安装插件

操作方法请参见为阿里云主机手动安装插件或为非阿里云主机手动安装插件。

插件进程已退出

您可以通过查看云监控插件的运行状态和日志来判断停止原因。如果出现云监控插件进程已退出的情况,则可能是云监控自身缺陷导致,建议您直接提工单,并保留问题。

- 查看插件日志
 - Windows
 - a. 以Administrator用户登录待安装云监控插件的主机。
 - b. 进入云监控插件日志所在目录C:\Program Files\Alibaba\cloudmonitor\local_data\logs。
 - c. 选中日志文件argusagent.log或argusagentd.log,通过记事本或写字板打开。
 - *argusagent d.log*: 云监控C++版本插件运行时为了守护进程而记录的日志。日志主要包括监控 进程的启动、停止等信息。
 - argusagent.log: 云监控C++版本插件的运行日志。
 - Linux
 - a. 以root用户登录待安装云监控插件的主机。
 - b. 执行以下命令, 查看云监控插件日志。

cd /usr/local/cloudmonitor/local_data/logs

cat argusagent.log

cat argusagentd.log

- argusagent d.log: 云监控C++版本插件运行时为了守护进程而记录的日志。日志主要包括监控 进程的启动、停止等信息。
- argusagent.log: 云监控C++版本插件的运行日志。

● 查看插件运行状态

- Windows
 - a. 以Administrator用户登录云监控插件所在主机。
 - b. 打开**服务**页面。

通过键盘快捷键Win+R打开运行对话框,输入命令services.msc,单击确定。

- c. 查看服务argusagent service的状态。
- Linux
 - a. 以root用户登录云监控插件所在主机。
 - b. 执行以下命令, 查看云监控插件状态。

ps aux | grep argusagent | grep -v grep

2.2. 如何重启云监控C++版本插件?

当您安装或配置云监控C++版本插件时,为了使其生效,需要重启插件。本文为您介绍在Windows和Linux操 作系统中,重启云监控C++版本插件的操作方法。

Windows

- 1. 以Administrator用户登录云监控插件所在服务器。
- 2. 进入云监控插件所在目录 C:\Program Files\Alibaba\cloudmonitor。
- 3. 双击stop.bat,停止云监控插件。
- 4. 双击start.bat, 启动云监控插件。

Linux

- 1. 以root用户登录云监控插件所在服务器。
- 2. 执行以下命令,进入云监控插件所在目录。

cd /usr/local/cloudmonitor

执行以下命令,重启云监控插件。
 ./cloudmonit orCtl.sh rest art

2.3. 如何通过云监控查看指定日期的监控数据?

本文为您介绍如何通过云监控控制台查看指定日期的监控数据。

操作步骤

- 1. 登录云监控控制台。
- 2. 在左侧导航栏,单击主机监控。
- 3. 在主机监控页面,单击目标主机对应操作列的一图标。
- 4. 您可以选择指定日期查看监控数据。

← launch- ~	(i-m5e2	2w4o6/192.168) 实例详情	的建板等规则
操作系统监控 ◎ 基础监控 进程监控 网络监控 云盘 ◎	报警规则	则	
1 小时 6 小时 12 小时 1天 3 天 7 天 14 天 2022年2月11日 04:39		2022年2月11日 10:39 箇	
CPU,内存,负载监控指标			
CPU使用率(%)	¢ /	内存使用率(%)	
切绕描标 平均值 V (周期:15秒)		切換描示 平均値 ~ (周期:15秒)	平均值 ~ (周期:15 秒)
100.00		100.00	0.56
80.00		80.00	0.40
40.00		40.00	0.20
20.00		20.00	0.10
0.00 04:39 05:53 07:16 08:40 10:03	10:39	0.00 04:39 05:53 07:16 08:40 10:03 10	0.00 A A A A A A A A A A A A A A A A A A
 (Agent)cpu.total 		(Agent)memory.used.utilization	● (Agenti/oad.1m ● (Agenti/oad.5m ● (Agenti/oad.15m

⑦ 说明 目前云监控只支持查看最近30天内的监控数据。

2.4. 非阿里云主机如何通过Nginx代理服务器上 报监控数据?

本文为您介绍非阿里云主机通过Nginx代理服务器上报监控数据至云监控的操作方法。

步骤一: 部署Nginx代理服务器

⑦ 说明 由于云监控部署在Linux服务器上,因此建议您的代理服务器选用Linux服务器。本文以 Cent OS操作系统为例。

- 1. 下载Nginx最新安装包,例如: nginx-1.19.6。
 - i. 登录Nginx下载中心。
 - ii. 单击nginx-1.19.6,下载Nginx安装包nginx-1.19.6.tar.gz。
- 2. 下载Nginx补丁包至代理服务器的指定目录,例如: /opt。

⑦ 说明 本文以安装Nginx补丁包proxy_connect_1014.patch为例。

- i. 以root用户登录代理服务器。
- ii. 执行以下命令, 下载Nginx补丁包。

cd /opt

yum inst all -y git

git clone https://github.com/chobits/ngx_http_proxy_connect_module.git

得到的补丁包如下:

```
proxy_connect.patch
proxy_connect_1014.patch
proxy_connect_rewrite.patch
proxy_connect_rewrite_1014.patch
```

proxy_connect_rewrite_1015.patch
proxy_connect_rewrite_101504.patch
proxy_connect_rewrite_1018.patch

3. 安装Nginx补丁包。

yum install -y patch pcre pcre-devel

patch -p1 < ngx_http_proxy_connect_module/patch/proxy_connect_1014.patch</pre>

- 4. 安装Nginx。
 - i. 上传Nginx安装包nginx-1.19.6.tar.gz至代理服务器的指定目录,例如:/usr/local。
 - ii. 以root用户登录代理服务器。
 - iii. 执行以下命令, 解压Nginx安装包nginx-1.19.6.tar.gz至目录nginx-1.19.6。

cd /usr/local

tar zxvf nginx-1.19.6.tar.gz

iv. 执行以下命令,初始化Nginx。

cd nginx-1.19.6

./configure --prefix=/usr/local/nginx-1.19.6 --with-http_stub_status_module -with-http_ssl_module --add-module=ngx_http_proxy_connect_module

v. 执行以下命令, 安装Nginx。

make install

make && make install

vi. 执行以下命令, 启动Nginx。

./nginx

vii. 查看Nginx安装结果。

在浏览器的地址栏输入代理服务器的IP地址:80,显示如下,说明安装成功。

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to <u>nginx.org</u>. Commercial support is available at <u>nginx.com</u>.

Thank you for using nginx.

- 5. 配置Nginx。
 - i. 执行以下命令, 新建目录conf.d。

cd /usr/local/nginx-1.19.6/conf

mkdir conf.d

ii. 执行以下命令,在目录conf.d中新建文件forward.conf。

cd conf.d

vi nginx.conf

iii. 在文件forward.conf中设置正向代理或反向代理。

■ 正向代理

如果把局域网外的Internet想象成一个巨大的资源库,则局域网中的客户端要访问Internet,则需要通过代理服务器来访问,这种代理服务就称为正向代理。

将如下信息拷贝到文件*forward.conf*中,其中参数 resolver 设置为代理服务器的IP地址,其 他参数均保持默认值。

```
server {
   listen
                               80:
   # dns resolver used by forward proxying
    resolver
                              192.168.XX.XX; #设置代理服务器的IP地址。
    # forward proxy for CONNECT request
   proxy connect;
                         443;
   proxy connect allow
   proxy_connect_connect_timeout 10s;
   proxy_connect_read_timeout 10s;
   proxy connect send timeout
                              10s;
    # forward proxy for non-CONNECT request
    location / {
       proxy_pass http://$http_host$request_uri #设定代理服务器的协议和地址,均使
用默认值。
       proxy_set_header Host $host;
    }
}
```

⑦ 说明 Nginx的正向代理不支持HTTPS协议。

■ 反向代理

请。

如果局域网向Internet提供资源服务,让Internet上的其他客户端来访问局域网内的资源,使他们 必须通过一个代理服务器进行访问,这种服务就称为反向代理。

将如下信息拷贝到文件forward.conf中,其中参数 server_name 设置为代理服务器的IP地址, 参数 proxy_pass 设置为代理服务器访问的URL地址,参数 ssl_certificate 设置为SSL证 书,参数 ssl certificate key 设置为SSL证书的密码,其他参数均保持默认值。

- iv. 按Esc键, 输入:wq, 再按Enter键, 保存并退出文件forward.conf。
- v. 执行以下命令, 打开文件nginx.conf。

cd ..

vi nginx.conf

vi. 配置文件nginx.conf。

将如下信息拷贝到文件nginx.conf中,其中参数 include 设置为文件forward.conf所在路径。

```
http {
.....
include /usr/local/nginx-1.19.6/conf/conf.d/forward.conf;
.....
}
```

vii. 按Esc键, 输入:wq, 再按Enter键, 保存并退出文件 nginx.conf。

viii. 执行以下命令, 重启Nginx代理服务器。

nginx -s reload

- ix. 测试Nginx安装结果
 - 正向代理

执行以下命令,能访问任意网址,表示安装成功。

curl -x192.168.XX.XX(代理服务器的IP地址) http://example.aliyundoc.com(任意网址)

■ 反向代理

执行以下命令,无论输入任何网址,均只能访问文件*nginx.conf*中指定的网址,表示安装成功。 **curl -x** *192.168.XX.XX(代理服务器的IP地址)https://example.aliyundoc.com(任意网址)*

步骤二:安装和配置云监控插件

- 在非阿里云主机上安装云监控插件。
 具体操作,请参见安装和卸载C++版本插件。
- 2. 在云监控插件中配置Nginx代理服务器。
 - i. 以root用户登录云监控插件所在的非阿里云主机。
 - ii. 执行以下命令, 打开文件agent.properties。
 - cd /usr/local/cloudmonitor/conf
 - vi agent.properties
 - iii. 在云监控插件中配置Nginx代理服务器的相关信息。

配置方法如下:

```
http.proxy.auto=false
#手动配置代理
http.proxy.host=192.168.XX.XX #Nginx代理服务器的IP地址。
http.proxy.port=8080 #Nginx代理服务器的端口。
#http.proxy.user=user #Nginx代理服务器的HTTP服务无用户名。
#http.proxy.password=password #Nginx代理服务器的HTTP服务无用户密码。
```

iv. 按Esc键, 输入:wq, 再按Enter键, 保存并退出文件 agent.properties。

- v. 执行以下命令, 重启云监控插件。
 - ./cloudmonitorCtl.sh restart

步骤三:查看非阿里云主机的监控数据

- 1. 登录云监控控制台。
- 2. 在左侧导航栏,单击主机监控。
- 在主机监控页面,单击目标主机的实例名称链接,或单击目标主机对应操作列的应图标。
 查看非阿里云主机的监控数据。

2.5. 如何卸载云监控插件?

您可以通过本操作卸载云监控Java、Go或C++版本插件。

Windows

- 1. 以Administrator用户登录云监控插件所在主机。
- 2. 创建.ps1格式文件,例如: test.ps1。
- 3. 将以下内容拷贝到文件test.ps1中。

```
云监控
```

```
if([System.Environment]::Is64BitOperatingSystem -eq $true)
{
   $CMS ARCH="amd64"
   $ARGUS ARCH="win64"
}else
{
    $CMS ARCH="386"
   $ARGUS ARCH="win32"
}
$dest path prefix="C:\Program Files\Alibaba"
$dest path="$dest path prefix\cloudmonitor"
echo "the current arch is $CMS ARCH"
$go dest file="CmsGoAgent.windows-$CMS ARCH.exe"
$argus dest file="cloudmonitor $ARGUS ARCH.zip"
$downloadpath="Argus/$CMS VERSION/$argus dest file"
if (Test-Path "$dest_path\wrapper\bin\AppCommand.bat")
{
  echo "old java cloudmonitor already installed - remove it..."
  & "$dest path\wrapper\bin\AppCommand.bat" remove
  rm -Force -Recurse "$dest path"
}
if (Test-Path "C:\Program Files (x86)\Alibaba\cloudmonitor\wrapper\bin\AppCommand.bat"
)
{
   echo "old java cloudmonitor already installed - remove it..."
    & "C:\Program Files (x86)\Alibaba\cloudmonitor\wrapper\bin\AppCommand.bat" remove
   rm -Force -Recurse "C:\Program Files (x86)\Alibaba\cloudmonitor"
if (Test-Path "$dest path\$go dest file")
{
   "echo remove go-agent"
   & "$dest_path\$go_dest_file" stop
    & "$dest path\$go dest file" uninstall
}
```

- 4. 保存并关闭文件test.ps1。
- 5. 选中文件test.ps1, 单击鼠标右键, 选择使用PowerShell运行。

Linux

- 1. 以root用户登录云监控插件所在主机。
- 2. 执行以下命令, 创建文件, 例如: test.sh。

touch test.sh

3. 执行以下命令,编辑文件test.sh。

vi test.sh

4. 将以下内容拷贝到文件test.sh中。

```
#!/bin/bash
if [ -z "${CMS HOME}" ]; then
CMS HOME PREFIX="/usr/local"
if [ -f /etc/os-release -a ! -z "`egrep -i coreos /etc/os-release`" ];then
   CMS HOME PREFIX="/opt"
 fi
fi
CMS HOME="${CMS HOME PREFIX}/cloudmonitor"
if [ `uname -m` = "x86_64" ]; then
   ARCH="amd64"
  ARGUS ARCH="64"
else
   ARCH="386"
  ARGUS ARCH="32"
fi
case `uname -s` in
 Linux)
  CMS_OS="linux"
   ;;
  *)
   echo "Unsupported OS: $(uname -s)"
   exit 1
   ;;
esac
DEST START FILE=${CMS HOME}/cloudmonitorCtl.sh
#卸载Java和Go插件
GOAGENT ELF NAME=${CMS HOME}/CmsGoAgent.${CMS OS}-${ARCH}
if [ -d  (CMS_HOME ) ; then
 if [ -f ${DEST START FILE} ];then
   ${DEST START FILE} stop
 fi
 if [ -f ${CMS_HOME}/wrapper/bin/cloudmonitor.sh ] ; then
   ${CMS HOME}/wrapper/bin/cloudmonitor.sh remove;
   rm -rf ${CMS_HOME};
 fi
 if [ -f ${GOAGENT ELF NAME} ]; then
   ${GOAGENT ELF NAME} stop
   rm -rf ${CMS HOME}
 fi
fi
```

- 5. 按Esc键, 输入:wq, 再按Enter键, 保存并退出文件test.sh。
- 6. 执行以下命令,执行文件*test.sh*。

sh test.sh

2.6. 如何处理云服务器ECS内网流量增高问题?

本文为您介绍如何处理云服务器ECS内网流量增高问题。

问题描述

在云监控控制台的主机监控中,看到云服务器ECS的内网流量增高,如下图所示。



问题分析

云服务器ECS通过外网网卡对外提供服务,内网的使用率通常比较低。当其他ECS服务器向某个ECS服务器拷 贝数据时,会导致当前服务器内网流量增高。

⑦ 说明 负载均衡SLB除外,因为负载均衡SLB通过内网与云服务器ECS通信。

如果非数据拷贝问题,则可能是云服务器ECS中毒,对外大量发包导致内网流量增高。此时,处理方法请参 见<mark>处理方法</mark>。

处理方法

云服务器ECS部署在Linux和Windows上的处理方法如下:

• Linux

⑦ 说明 NetHogs是一个开源的命令行工具(类似于Linux的top命令),用来按进程或程序实时统 计网络带宽使用率。

- i. 下载NetHogs。
- ii. 执行以下命令, 安装NetHogs。

yum inst all net hogs

iii. 执行以下命令, 查看占用内网带宽的进程。

nethogs eth0

NetHogs version 0.8.0

PID	USER	PROGRAM	DEV	SENT	RECEIVED
23701	root	/usr/sbin/sshd	eth0	0.667	26.321 KB/sec
23696	sshd	sshd: [net]	eth0	0.000	0.000 KB/sec
?	root	unknown TCP		0.000	0.000 KB/sec

• Windows

⑦ 说明 Windows Server 2008及以上的操作系统,您可以通过资源监视器查看占用内网带宽的进程。

i. 在云服务器ECS的任务栏上,单击鼠标右键,选择任务管理器。

ii. 在任务管理器的进程页签, 查看占用内网带宽的进程。

如果问题仍未能解决,请您提交工单。

2.7. 如何处理在阿里云主机上自动安装云监控插件失败问题?

如果您在阿里云主机上自动安装云监控插件失败,则请按照以下方法逐步排查。

操作步骤

- 1. 以root用户登录云监控插件所在的阿里云主机。
- 2. 执行以下命令,检查是否能获取到阿里云主机的地域ID。

curl http://100.100.100.200/latest/meta-data/region-id

- 是: 执行。
- 否:请手动为阿里云主机安装插件。具体操作,请参见为阿里云主机手动安装插件。
- 3. 执行以下命令, 检查阿里云主机与对象存储OSS之前的网络是否正常。

ping cms-agent-\${region-id}.oss-\${region-id}.aliyuncs.com

{region-id} 是阿里云主机的地域ID,例如: {region-id} 为 cn-shenzhen , 命令为ping cmsagent-cn-shenzhen.oss-cn-shenzhen.aliyuncs.com。

- 是:网络正常,可能是云监控的问题。请给云监控提交工单。
- 否:网络异常,可能是对象存储OSS的网络问题。请给对象存储OSS<mark>提交工单</mark>。

2.8. 站点监控任务到期后如何处理?

本文为您介绍站点监控任务到期后的处理方法。

对于未开通包年包月或按量付费的阿里云账号,站点监控任务的免费额度为10个,有效期为30天。当您的站 点监控任务状态为**已过期**时,处理方法如下:

• 方法一:删除到期站点监控任务,重新创建站点监控任务,该任务的有效期仍然为30天。

具体操作,请参见删除站点监控任务和创建站点监控任务。

 方法二:开通按量付费或包年包月后,到期站点监控任务自动恢复,免费额度仍然为10个,且付费周期内 不会过期。

更多信息,请参见计费标准或套餐。

2.9. 如何处理云监控插件心跳检查失败问题?

当主机宕机、网络异常或插件停止服务时,云监控都会为您上报系统事件"心跳检查失败"。本文以阿里云 主机为例,为您介绍云监控插件心跳检查失败的处理方法。

操作步骤

- 1. 检查主机的运行状态是否正常。具体操作,请参见查看实例信息。
 - 是: 执行。
 - 否: 请启动或重启主机。具体操作, 请参见启动实例或重启实例。

⑦ 说明 如果启动或重启主机仍然不能解决问题,请根据云服务器ECS的相关文档进行排查。 更多信息,请参见实例FAQ。

- 2. 检查主机的云监控插件是否正常运行。具体操作,请参见安装和卸载C++版本插件。
 - 是: 执行。
 - 否:请重启云监控插件。具体操作,请参见如何重启云监控C++版本插件?。
- 3. 在主机上ping云监控的心跳IP地址,检查主机的网络是否正常。

关于如何获取云监控的心跳IP地址,请参见配置网络。

- 是: 执行。
- 否:请为主机设置网络。具体操作,请参见配置网络。
- 4. 收集云监控插件目录/usr/local/cloudmonitor/local_data/logs中的日志信息,并给云监控提交工单。

2.10. 如何处理未收到报警电话的问题?

当您创建报警规则时,设置的报警通知方式包括电话和短信,但报警联系人仅收到报警短信,未收到报警电 话。

因为您使用的是免费版云监控,其中仅包括免费报警短信(1000条/月),不包括免费报警电话,所以您无 法收到报警电话。处理方式如下:

● 方法一:开通按量付费。

云监控按量付费的购买页和价格说明,请参见按量付费。

• 方法二: 购买报警电话包。

云监控报警电话包的购买页和价格说明,请参见报警电话包。

2.11. 如何处理云监控识别多台相同镜像主机异 常问题?

当您的非阿里云主机采用镜像方式部署时,在安装云监控插件后,将自动生成序列号相关信息,会导致云监 控识别多台相同镜像的非阿里云主机时出现异常。

不同操作系统主机的处理方法如下:

• Windows

在注册表中删除目录*计算机\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\cloudmonitor*中的键 值对*serial_number*。

• Linux

删除目录/etc/cloudmonitor中的文件serial_number.properties。