云监控用户手册

——Version: 0.1

一、 概览

在概览页面中展示中系统默认提供的监控项或者用户创建的监控项、用户创建的监控点、云服务的实例数、用户设置的报警规则等。

1.1 名词解释

先介绍下云监控三个核心的概念。

【监控项】：用户设置或者系统默认的监控数据类型，例如站点监控的 Http 监控默认有两个监控项 http.responseTime & http.status。ECS 的监控项有 CPU 利用率、内存利用率等等。

【监控点】：某一实例绑定到具体的一个监控项即为一个监控点。如针对 www.aliyun.com 这个站点的 http 监控，实际包含两个监控点 http.response & http.status。对于 ECS 云主机有 11 个监控项，所以一台云主机默认有 11 个监控点

【报警规则】：用户在监控点上设置规则，当满足条件时会触发报警

1.2 短信使用情况

云监控默认为每位用户提供 1000 条免费的报警短信。在概览中，用户可以查看已经使用的短信数。

二、 站点监控

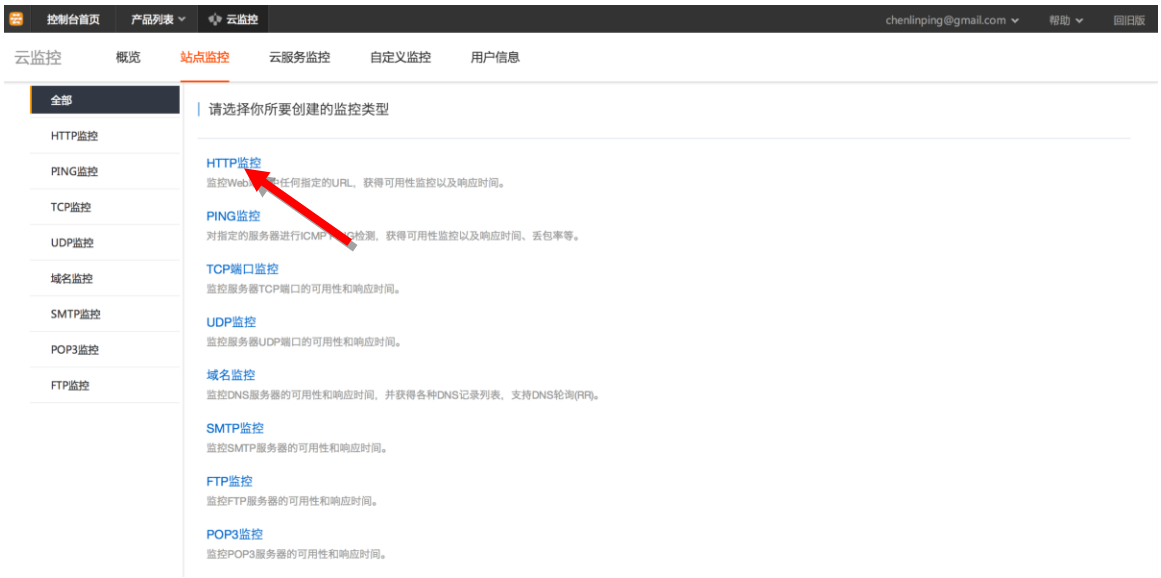
站点监控可以对目标站点服务的可用性以及响应时间进行监控。系统已经默认预置了 8 种监控类型，包括 http 监控、ping 监控、tcp 监控、udp 监控、DNS 监控、pop 监控、smtp 监控、ftp 监控。其中每种监控类型里面包含了两个监控项：status 和 responsetime。

监控类型	简介
HTTP 监控	监控 Web 站点中任何指定的 URL，获得可用性监控以及响应时间。
Ping 监控	对指定的服务器进行 ICMP Ping 检测，获得可用性监控以及响应时间、丢包率等。
TCP 端口监控	监控服务器 TCP 端口的可用性和响应时间。
UDP 端口监控	监控服务器 UDP 端口的可用性和响应时间。
DNS 监控	监控域名的可用性和响应时间，并获得各种域名记录列表，支持域名轮询(RR)。
POP3 监控	监控 POP3 服务器的可用性和响应时间。
SMTP 监控	监控 SMTP 服务器的可用性和响应时间。
FTP 监控	监控 FTP 服务器的可用性和响应时间。

1. 点击页面右上角的“创建监控点”按钮，进入“站点监控”类型选择页面；

单击列表页面的某一行，可以显示缩略图，可用性缩略表显示的是一天内的可用性展示，响应时间缩略图展示的是近 1 小时内的响应时间曲线，不代表当前状态。可用性和响应时间缩略图均是统计数据，不代表监控站点的最新状态。

2. 选择您要创建的“监控类型”，点击某一“监控类型”链接进入监控点创建页面；



3. 进入创建监控点的表单页面；

4. 创建监控点表单描述
    1) 监控点名称：为您的监控点输入个性化的名称
    2) 监控地址：您要监控的地址，对 http 来说，就是一个网站的地地址，对域名解析来说，就是某一个域名等等。
    3) 上报频率：站点监控探测引擎多长时间执行一次探测任务，并上报数据的频率。默认为 5 分钟，请谨慎选择 1 分钟，过于频繁的探测可能会导致对方服务屏蔽您的账号。
    4) 分页式监测点，目前我们部署了两个监测点，可以分别从杭州和青岛对您设置的目标服务进行监测，您也可以只选择从其中一个监测点进行探测。后续会支持更多监测点，包括海外的监测点。

    5) 高级设置，不同的监控类型会有一些高级选项
        a. http 监控：
            i. 请求方法，http 标准的请求方法，get\post\head，其中 post 支持提交内容。
            ii. 提交内容，只对 post 请求方法有效，输入您的目标服务能够识别的内容。
            iii. 匹配响应内容，您期望探测目标网站返回什么样的内容。
            iv. 匹配方式：选择匹配，则如果网站返回内容匹配您期望的内容报警；选择不匹配，则如果网站返回内容不匹配您期望的内容报警。
            v. Cookie：您期望探测目标网站需要的 cookie，key:value 形式，多个 cookie 以半角分号分隔。
            vi. http 请求头信息：您期望探测目标网站需要的 http header 信息，key:value 形式，多个 header 以半角分号分隔。
                1. http 验证用户名：
                2. http 验证密码：
        b. ping 监控：您可以使用 ping 监控服务来检测目标服务的网络延迟。
        c. Tcp 监控：监控地址的端口是不是连通的。另外，您也可以配置请求内容和期望的响应内容。如果配置了这两项内容，则不匹配时会报警。内容支持 16 进制字节码和文本两种形式，
            i. 16 进制字节码。如：0xcf,0x0f,0x85,0x85
            ii. 文本。系统内容会对文本内容进行转换，请注意空格等容易出错的字符。

d. Udp 监控：监控某地址的 udp 服务，因为 udp 协议的特性，必须要为 udp 配置请求和响应内容，否则 udp 探测将永远成功。
    i. 16 进制字节码。如：0xcf,0x0f,0x85,0x85
    ii. 文本。系统内容会对文本内容进行转换，请注意空格、换行符等容易出错的字符。
e. DNS 监控：监控域名的可用性和响应时间，并获得各种域名记录列表，支持域名轮询(RR)。通常只需要默认选择查询类型 A.
f. POP 监控：监控 POP3 协议的接收邮件服务器，填写正确的地址、端口，如果配置用户名密码，则会验证用户名密码。请注意频率，如果频率太快，有可能会导致对方服务屏蔽您的账号。请依据对方服务选择是否使用完全连接。
g. Smtp 监控：监控 SMTP 协议的发送邮件服务器，填写正确的地址、端口，如果配置用户名密码，则会验证用户名密码。请注意频率，如果频率太快，有可能会导致对方服务屏蔽您的账号。请依据对方服务选择是否使用完全连接。
h. ftp 监控：验证 Ftp 服务是否正常以及延迟情况。

6) 约定：
a. 每个创建成功的监控点会形式两个监控指标，一个是状态，一个是响应时间。对所有的状态来说，我们约定，小于 400 的状态码为正常（对需要匹配内容的服务，如果服务状态正常，但内容不匹配，我们也认为是不正常。），大于等于 400 的状态为异常（有可能是服务响应内容不匹配您预置的期望值）。
b. 响应时间单位是毫秒。
c. 对于可用性图表，每小时计算一次。
d. 对于 ping 监控，目前没有可用性统计，我们展示的是某统计周期内的丢包率和响应时间的平均值统计。
e. 监控点创建成功后，站点监控后台会启动相应的探测任务， 按您指定的频率探测并上报数据给云监控后台，进行分析和报警服务。

7) 监控点创建成功会，会自动跳转到创建报警规则页面：

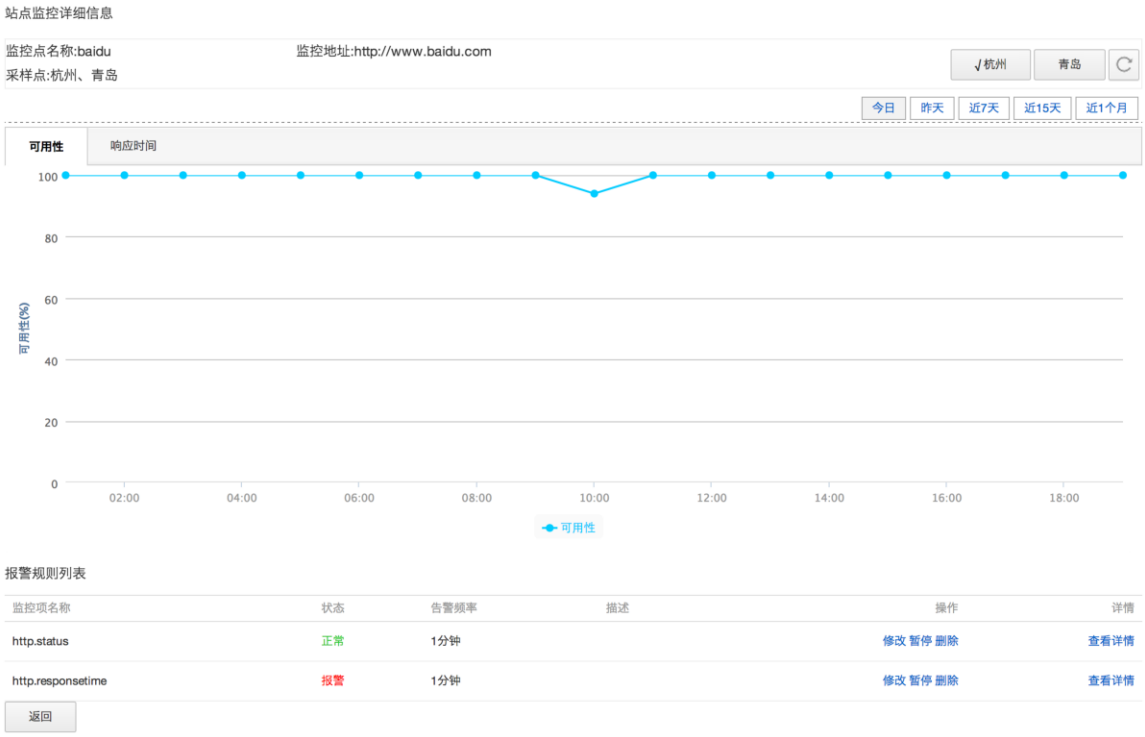
创建报警规则表单详细描述：

1) 统计周期：后台会依据统计周期形成统计报表，
2) 重试几次报警：您可以选择连续几次超过阀值报警，默认是三次，通常偶然因素会导致状态不对或者服务响应超时，连续三次以上更能代表服务工作不正常，减少误报的情况。
3) 响应时间的报警阀值：服务响应时间超过这个阀值，则会报警。
4) 报警的接收组（人）：参照报警管理部分的文档。

创建成功的监控点会进入列表页面

a. 查看详情：查看该监控点的当前的详情状态。
b. 报警规则修改：修改报警规则
c. 修改：修改监控点
d. 删除：会删除当前监控点以及监控点关联的报警规则。
e. 采样点:当前监控状态，列表页面的监控状态显示的是最新一条监控数据的状态。及时性很高。代表该目标服务的最新状态。

1）点击查看详情，进入详情页面：



可以查看到今日、昨日、近 7 天、近 15 天、近 1 月的监控数据情况。

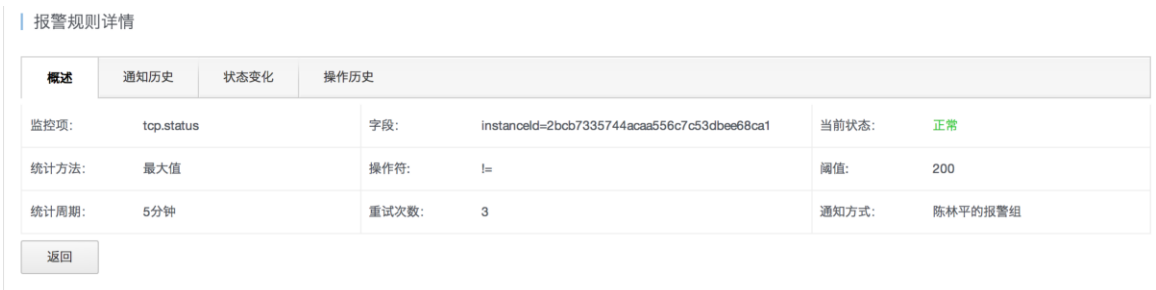
描述：站点监控的详情页面共有两个 tab 页面， 分别是显示可用性图表和响应时间的变化曲线。

可用性展示的是按小时统计的可用性比例。计算规则如下：成功状态的数据总数/上报数据总数=可用性比率。假定用户设定的上报频率为 1 分钟，则每小时共有 60 次数据上报，其中 2 条不成功，则在当前的这一小时内的可用性为 58/60=96.7。

响应时间展示的数据统计周期，随查询的时间段不同而不同，今天和昨天两个时间段，查询的是 5 分钟内的平均值。7 天及以上，查询的是 1 小时内的平均值。

所以，图表展示的监控状态会有延迟，有可能和监控点列表页面的状态不一致，该图表仅作统计展示用，不代表监控点的当前状态。

2) 点击报警详情，可以查看报警的详情，包括概述，通知历史，报警的状态变化，操作历史。



报警规则详情

概述 | **通知历史** | 状态变化 | 操作历史

开始时间: 2014-03-17 00:00:00 结束时间: 2014-03-24 14:10:31 搜索

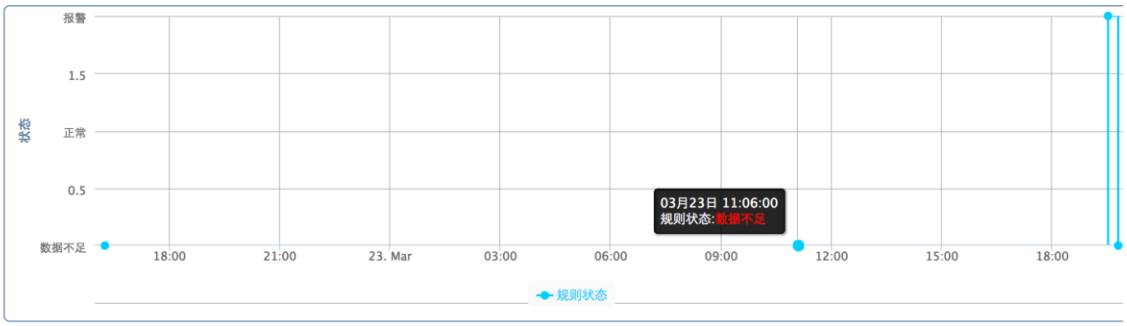
时间	触发状态	报警值	通知方式	接收人	结果
2014-03-23 19:31:03	报警	530	陈林平的报警组	邮件:linping.chenlp@taobao.com;	发送

返回

报警规则详情

概述 | 通知历史 | **状态变化** | 操作历史

开始时间: 2014-03-17 00:00:00 结束时间: 2014-03-24 14:10:31 搜索



时间	描述	状态值
2014-03-22 16:14:35	恢复正常 -> 数据不足	None
2014-03-23 19:47:38	恢复正常 -> 数据不足	None
2014-03-23 19:31:03	恢复正常 -> 发生告警	530
2014-03-23 11:06:00	恢复正常 -> 数据不足	None

返回

报警规则详情

概述 | 通知历史 | 状态变化 | **操作历史**

开始时间: 2014-03-17 00:00:00 结束时间: 2014-03-24 14:10:31 搜索

时间	描述
2014-03-22 15:54:35	IF tcp.status 连续3次 != 200 THEN 通知[石叟的报警组]
2014-03-23 17:47:38	IF tcp.status 最大值 连续3次 != 200 THEN 通知[陈林平的报警组]
2014-03-23 10:46:00	IF tcp.status 连续3次 != 200 THEN 通知[陈林平的报警组]
2014-03-24 12:39:12	IF tcp.status 最大值 连续3次 != 200 THEN 通知[陈林平的报警组]

返回

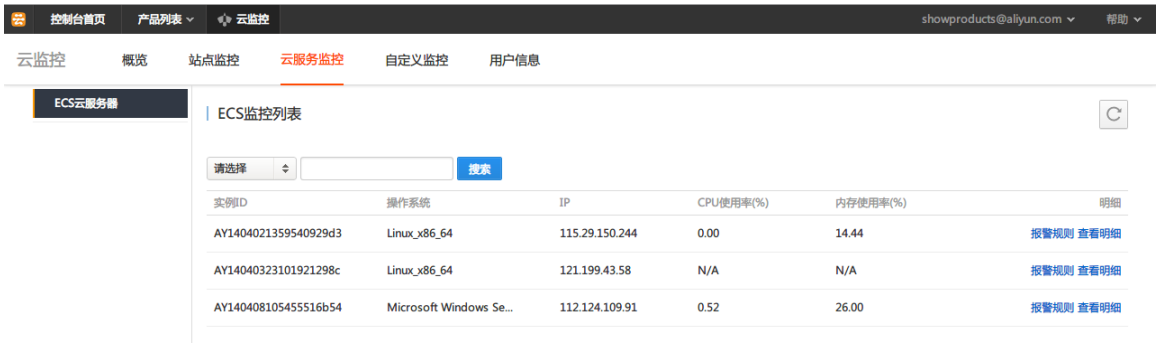
三、 云服务监控

云服务监控是阿里云为用户提供的各种云产品的监控，包括 ECS, RDS, OCS, OTS, OSS 等，当前对用户开放的只有 ECS 云主机的监控，其它云产品的监控会陆续加入进来，尽请期待。

3.1 云服务器监控

ECS 监控主要涵盖的指标有 CPU 利用率、内存利用率、磁盘利用率、磁盘读写、网络速率，系统平均负载（仅限 Linux 主机）、进程数、TCP 连接数等。

进入云监控的控制台后，点击【云服务监控】标签，即可进入 ECS 云服务器监控。如下图所示：

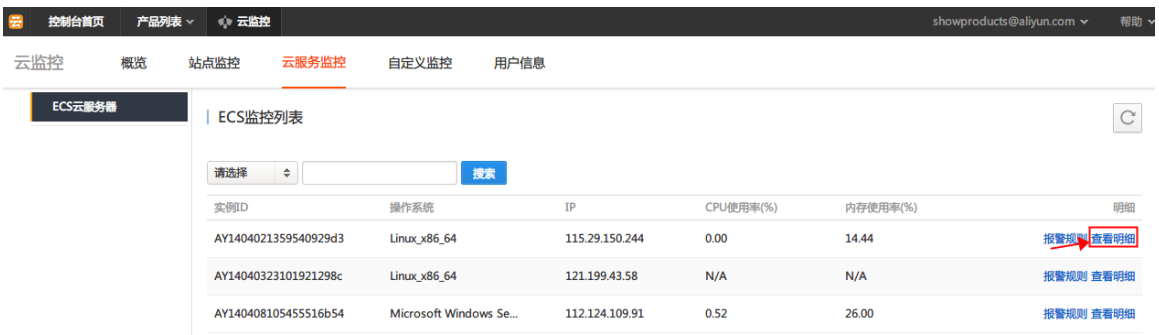


首页中，罗列出用户的机器列表。对于每一台云主机，默认展示的有**实例 ID、操作系统类型、机器 IP、CPU 利用率、内存利用率、操作**等。这里 CPU 利用率与内存利用率是最新的监控数据展示。

3.1.1 查看明细

【ECS 云服务器】→【查看明细】，可看到此云主机所有的监控指标情况。

点击查看明细：



明细指标页面：

可以查看到今日、昨日、近 7 天、近 15 天、近 1 月的监控数据情况。

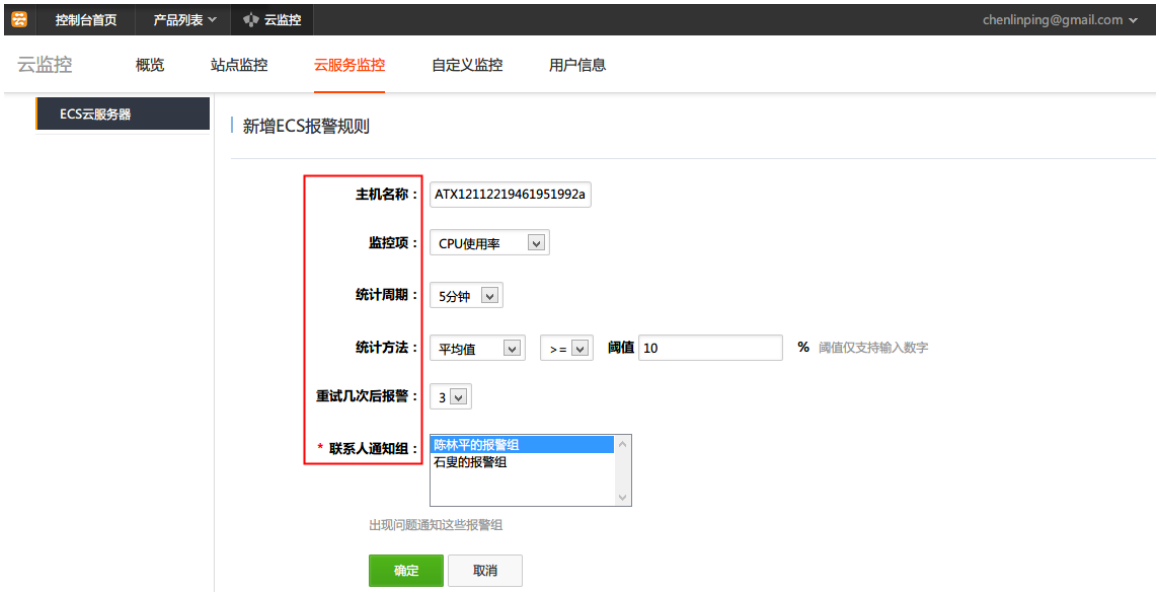
说明：对于系统为 linux 的主机，磁盘 IO 的监控数据获取是通过 iostat 进行的；若您发现 Linux 主机无磁盘 IO 数据，请确认您的机器是否安装了 iostat 指令。Redhat 与 CentOS 用户可以使用 yum 进行安装；Ubuntu 与 Debian 用户可以使用 apt-get 进行安装。

3.1.2 ECS 云主机报警管理

在【查看明细】的页面的下端，有针对这台云主机报警规则的管理页面，如下图：

用户可以在这里新增报警、修改报警、暂停报警、删除报警、查看报警历史详情。

3.1.2.1 新增报警



名词解释：

【监控项】：云主机采集的监控数据指标，如 CPU 利用率、内存利用率等

【统计周期】：监控数据的聚合周期，如采集周期是 1 分钟一次，统计周期可以是 5 分钟、1 小时等，ECS 的统计周期是固定的，不需要用户设置，但在报警设置这里，用户可以选择对采集的原始数据（1 分钟 1 次）进行报警设置，也可以选择对统计的结果进行报警设置

【统计方法】：默认有五种统计方式，**最大值、最小值、平均值、求和值、采样计数值**。特别说明下，采样计数值，是指在统计周期内，上报的监控数据条数。阈值目前数值型。

【重试几次后报警】：是指当监控数据连续几次满足用户设置的规则后，才进行报警。主要目的是避免监控数据的抖动。

【联系人通知组】：满足报警条件后，通知给哪些联系人。具体的概念介绍请参考第一部分，用户信息管理

3.1.2.2 暂停报警

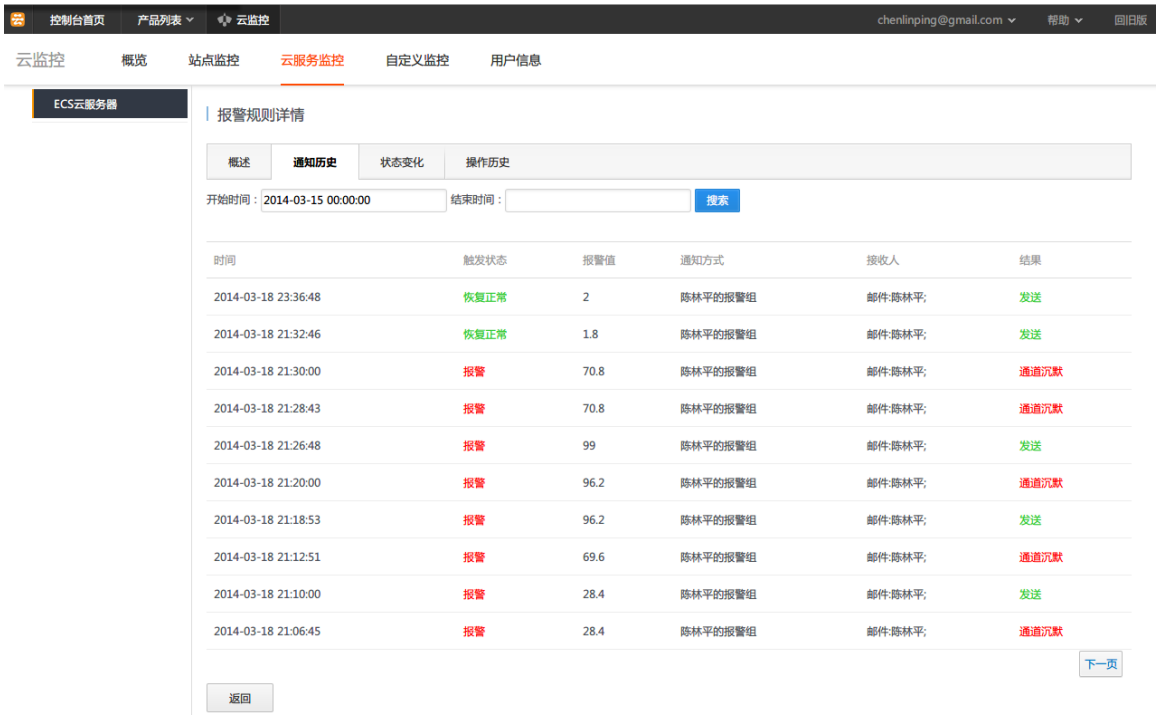
用户可以选择关闭或者打开报警

3.1.2.3 报警详情

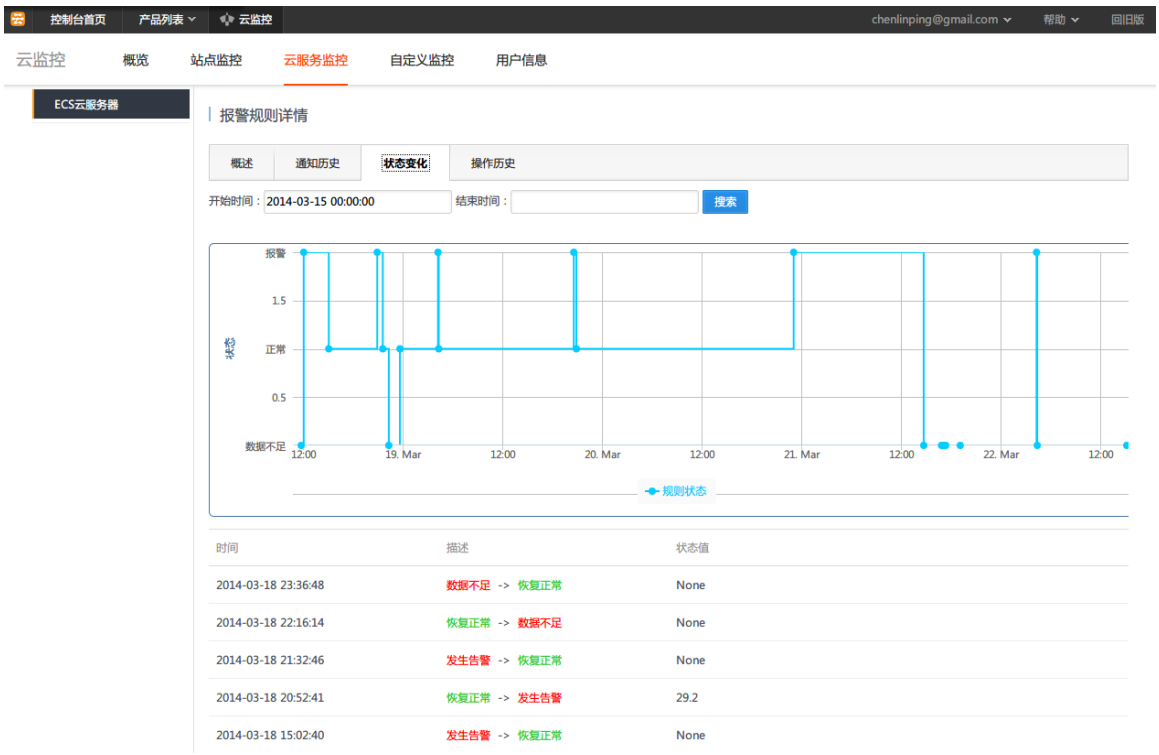
点击详情按钮进入下图展示的页面，包含概述、通知历史、状态变化、操作历史。

概述：用户针对当前实例某一监控项设置的报警规则

通知历史：在满足用户设置的报警规则时，会进行报警；当恢复正常后，亦会通知用户。这里需要介绍下通道沉默这一概念，当某一条报警发出后，在 1 天内若再次触发报警，不会通知，恢复正常的通知不会受沉默期的影响。当前系统默认的沉默期是 1 天，在后面的版本会将沉默期的设置开放给用户。



状态变化：共三种状态，发生报警、恢复正常、数据不足



数据不足，是指无监控数据上报到服务器端。

3.1.3 如何开通云主机监控

请注意，当前只云盾阿里云 ECS 云主机

1. 若用户发现自己的主机并未显示在云监控的云服务器的监控列表中，请从云监控控制台下载新版云盾，安装或者升级云盾
2. 若用户发现自己的主机已经显示在云监控的机器列表中，但无监控数据，请重新下载安装新版云盾进行安装
3. 云盾安装过后，请等待 10 分钟，监控数据方可展示在云监控控制台。

具体操作请参考 http://jiankong.aliyun.com/readme.htm

四、 自定义监控

自定义监控是提供给用户自由定义监控项及报警规则的一项功能。通过此功能，用户可以针对自己关心的业务进行监控，将采集到监控数据上报至云监控，由云监控来进行数据的处理，并根据结果进行报警。

登录云监控后，点击标签页【自定义监控】，即可进入以下页面：

左侧分别有三个选项，分别为【自定义监控项管理】、【自定义监控数据查询】、【自定义报警管理】

4.1 自定义监控项管理

云监控当前允许至多 10 个自定义监控项，且上报监控数据的服务必须在阿里云的云服务器上。

4.1.1 创建监控项

用户点击创建监控项按钮，即可进行自定义监控项设置页面：

名词解释

【监控项名称】：用户上报的监控数据指标名称，如 cpuUtilization, memoryUtilization 等。

【单位】：监控数据的单位，在上报数据时不会做校验，只是为了便于展示数据，或者便于数据信息的沟通，希望用户根据自己的实际情况填写。

【上报频率】：监控数据上报的周期，只允许 1 分钟，5 分钟，15 分钟三种上报频率

【字段信息】：一条监控数据肯定需要附属到某一实体才有意义。如 ECS 的 cpu 监控项，需要映射到某台机器才有意义。因此，字段信息可以填写 vmIP，在用户上报监控数据时，需要在上报的数据中填写如 vmIp=xxx.xxx.xxx.xxx。**字段信息最多允许五项**。

【统计周期】：用户可以告知云监控，上报的监控数据需要以何种频率进行聚合。

【统计方法】：参考 2.1.2.3 报警详情

若用户设置的自定义监控项已经达到 10 个，再进行创建时，会显示如下异常：

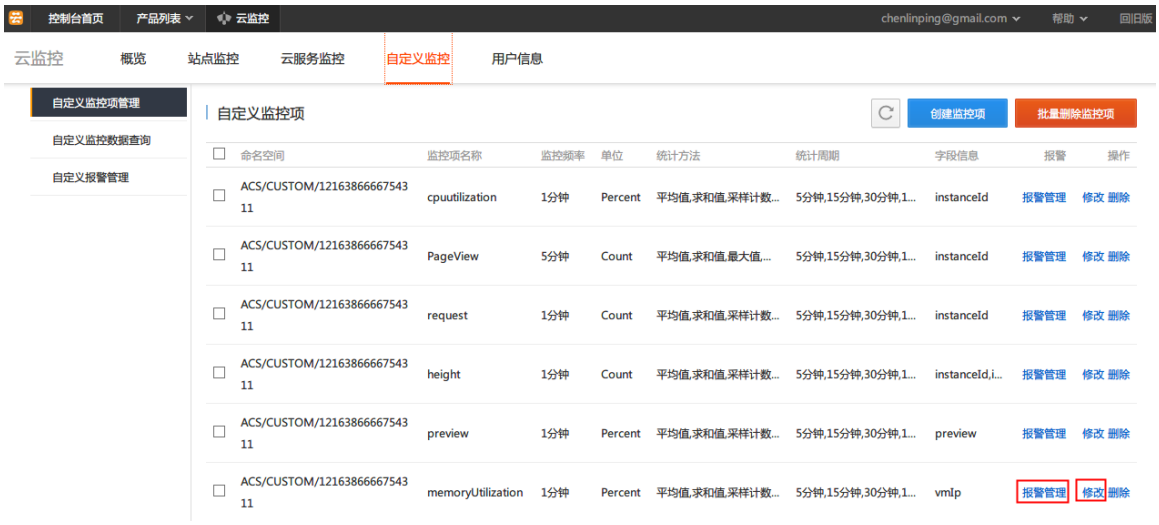
例如，创建一个监控项名称为 memoryUtilization，字段信息亦为 vmIp，点击确认后进入报警规则设置页面；若此时用户不想创建报警规则可以先点击页面上的取消按钮

用户可以在字段信息中填写某一机器的 IP，如 192.168.1.1；填写【规则名称】、【阈值】、选择【联系人通知组】，点击【确认】后即创建了 192.168.1.1 这台机器 memoryUtilization 的报警。

若前面取消了创建报警规则，可以在【自定义报警管理】监控项下拉框中选择您所希望创

建报警的监控项，然后点击创建报警规则。

4.1.2 修改监控项



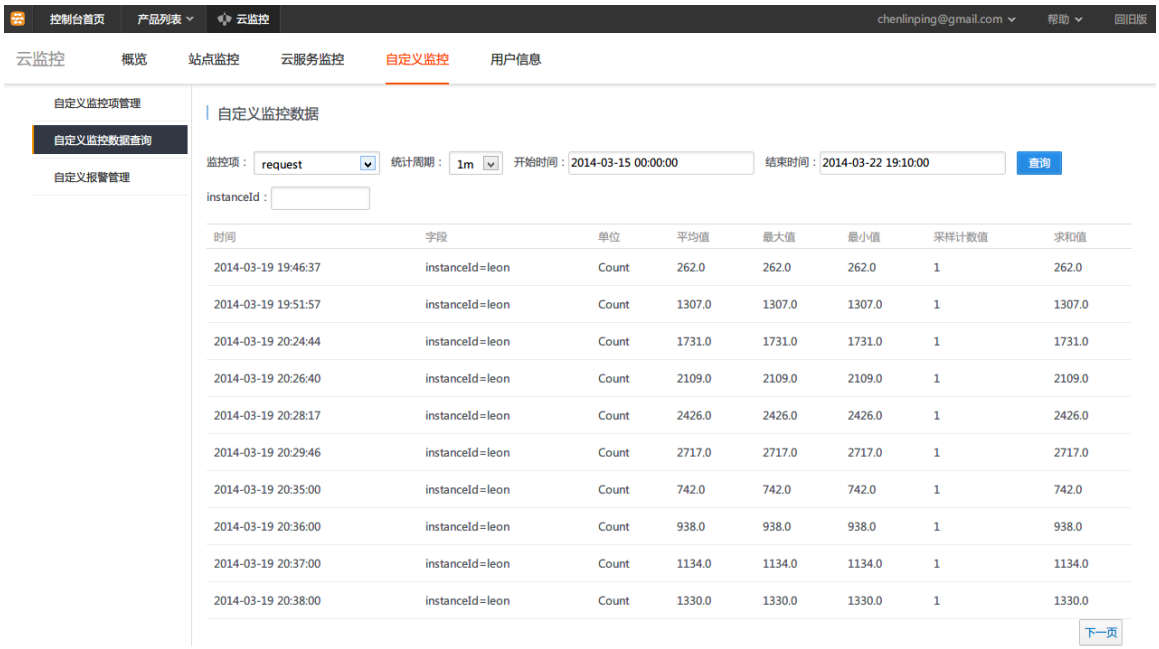
点击【修改】按钮，可以进入监控项修改页面

点击【报警管理】按钮，可以查看在些监控项上设置的所有报警

4.2 自定义监控数据查询

用户选择监控项名称，填写字段信息，选择统计周期进行监控数据查询

自定义监控暂时只支持数据在页面上的展示，尚不支持按照时间倒序排列，所以若用户关心最近的监控数据是多少，请选择最近的开始时间与结束时间。自定义监控暂时也不支持图表展示。请见下图：



4.3 自定义报警管理

进入自定义报警管理页面后，展示在用户面前的是所有用户配置过的报警规则。用户可以在监控项栏，选择在某一监控项，查询在此监控项上设置的报警规则。

4.4 监控数据上报

自定义监控操作分为两部分，一部分操作是在云监控 Portal 上配置自定义监控项与报警规则，如 3.1，3.3 节所示；另一部分操作是用户编写代码上报监控数据。

4.4.1 监控数据上报规范

用户可以使用云监控接口 http://open.cms.aliyun.com/metrics/put 上报监控数据

Post 方式

用户可以一次提交多条统计数据，统计数据放在消息体中，遵循 JSON 格式。如消息体内容：

```
userId=123456&namespace=acs/custom/123456&metrics =
[{"metricName":"vm.cpu","timestamp":"1395556197448","value":80.0,"unit":"Percen
t","dimensions":{"instanceId":"vm_001"}}]
```

GET 方式

用户可以一次提交多条统计数据，统计数据存放在 metrics 字段中，遵循 JSON 格式。

```
http://open.cms.aliyun.com
/metrics/put?userId=123456&namespace=acs/custom/123456&metrics=[{"metricName":
"vm.cpu","timestamp":"1395556197448","value":80.0,"unit":"Percent","dimensions"
:{"instanceId":"vm_001"}},{"metricName":"vm.mem","timestamp":"1395556197448","v
alue":1280.0,"unit":"Megabytes","dimensions":{"instanceId":"vm_002"}}]
```

字段说明

字段名称	字段说明	字段类型	是否必须
userId	用户唯一标识，对非系统内部默认账号，该字段必填	long	必选
namespace	名字空间，表明监控数据所属产品	String	必选
metricName	监控指标名称	String	必选
value	监控指标值	数值型	必选
timestamp	时间	String	必选
unit	统计项单位	String	必选
dimensions	即字段信息，用于标识资源或服务的唯一 ID，可以多个	String	必选

用户在云监控 portal 上创建自定义监控项

metricName：portal 创建时填写的【监控项名称】

unit：用户选择的【单位】
dimensions：用户填写的【字段信息】，允许多个，使用半角逗号分隔

点击确认过后，进行【自定义监控项管理】，这里用户可以看见 userId, namespace

namespace： 红色方框中的字符串
userId：红色方框字符串最后的数字串
timestamp：数据上传的时间，支持两种表示方式：一种方式取时间的长整型表示方式 1395556197448，另一种方式按照 ISO8601 标准表示，并使用 UTC 时间，例如 2014-9-11T10:00:00Z，注意它对应的北京时间是 2014-09-11 18:00:00

响应消息

云监控收到 http 请求后，若处理成功，则直接返回状态码为 200 的 Http 响应，消息体中不携带内容，用户也不需要处理响应消息。若处理失败，返回 JSON 格式的消息体，同时 Http 响应的状态码不为 200

错误	错误描述	HTTP Status Code
InternalServerError	由于内部错误或不确定的异常导致的请求失败	500
InvalidParameterCombination	参数组合错误	400
InvalidParameterValue	参数无效或超出范围	400
MissingRequiredParameter	缺少必须的参数	400

例如：`{"code":"InvalidParameterValue","msg":"the metricName is empty."}`

4.4.2 监控数据上报方式

云监控为用户提供了方便的定时任务调度程序，若用户安装了云盾，可以在云盾的目录下找到 aegis_quartz 程序。若没有发现，请升级云盾至最新版本。

操作系统类型	Quartz 路径
Windows 32bit	C:\" program files" \alibaba\aegis\aegis_quartz\aegis_quartz.exe
Windows 64bit	C:\" program files(x86)" \alibaba\aegis\aegis_quartz\aegis_quartz.exe
linux	/usr/local/aegis/aegis_quartz/aegis_quartz

各操作系统平台下 aegis_quartz 使用方式相同。下面我们以 linux 为例，说明 quartz 的使用方式。

查看帮助

```
[root@monitorZc77aa57fZf8d6Z445dZ8eZ aegis_quartz]# /usr/local/aegis/aegis_quartz/aegis_quartz -h
Usage:/usr/local/aegis/aegis_quartz/aegis_quartz
   -f  configFile            (default:conf/staragent.conf)
   -c  configFile            (only check configFile)
   -e "opType value"         (get or set some inner info)
   -v                        (show agent version)
   -h                        (show help)
about opType and value:
   SetLogLevel [error|warn|info|debug] (set agent log level)
   GetLogLevel            (show agent log level)
   GetConfig              (show config)
   GetTasks               (show tasks)
   GetTasksJson           (show tasks)
   GetTaskStatus          (show task status)
   AddTask "xxx"          (add task)
   RemoveTask "xxx"       (remove task)
   RemoveAllTasks         (remove all tasks)
```

查看当前任务

```
[root@monitorZc77aa57fZf8d6Z445dZ8eZ aegis_quartz]# /usr/local/aegis/aegis_quartz/aegis_quartz -e "GetTasks"
Task Num : 2
  QuartzStr : [0 0/1 * * * ?]
     CmdStr : /usr/local/aegis/aegis_quartz/libexec/default/sampler.py


  QuartzStr : [0 0/5 * * * ?]
     CmdStr : /usr/local/aegis/aegis_quartz/libexec/user/sampler.py
```

添加任务

```
[root@monitorZc77aa57fZf8d6Z445dZ8eZ ~]# /usr/local/aegis/aegis_quartz/aegis_quartz -e "AddTask [0 0/1 * * * ?] user/sampler.py"
{"code":0,"msg":"add task ok"}
```

删除任务

```
[root@monitorZc77aa57fZf8d6Z445dZ8eZ ~]# /usr/local/aegis/aegis_quartz/aegis_quartz -e "RemoveTask [0 0/1 * * * ?] user/sampler.py"
{"code":0,"msg":"remove task ok"}
```

需要用户注意的一些事情：

1. aegis_quartz 进程请勿停止，系统的监控数据采集也是通过 aegis_quartz 完成
2. aegis_quartz 程序的调用请使用绝对路径，如 linux 环境下 /usr/local/aegis/aegis_quartz/aegis_quartz
3. aegis_quartz libexec/default 下面的脚本是内置的监控数据采集脚本，请用户勿使用与修改
4. 用户的监控数据程序只能放在 libexec/user 目录下面；上面添加任务与删除任务的示例中，脚本程序的路径写的即是相对路径。因此，用户在命令行中的脚本路径只需要填写成 user/xxx 即可（其中 xxx，是用户的脚本）
5. 关于任务的执行频率，是基于标准的 quartz 表达式，用户按照规范填写即可。用户的执行频率请与 portal 中设置监控项上报频率保持一致（portal 支持的频率是 1 分钟，5 分钟，15 分钟），若修改上报频率请保持 portal 与脚本一致，否则监控数据处理可能会不准确。关于如何创建自定义监控项请参考 3.1 节
6. aegis_quartz 只允许用户创建 10 个定时任务
7. 若用户的脚本被调度后，没有成功上报监控数据，可以将 log level 设置为 debug 模式，通过 aegis_quart/log 查看出错的原因；log 位置在 aegis_quartz/log 下

```
[root@monitorZc77aa57fZf8d6Z445dZ8eZ ~]# /usr/local/aegis/aegis_quartz/aegis_quartz -e "SetLogLevel debug"
SetLogLevel to debug successful
```

五、 用户信息管理

5.1 名词解释

【报警联系人】：报警消息的接收人，包含手机、旺旺（淘宝）、邮件。

【报警组】：一组报警联系人，可以包含一个或多个“报警联系人”。在报警设置中，均通过“报警组”发送报警通知。对应每一个监控点，根据预先设定的报警方式在到达报警阈值时采取不同的报警方式向报警组成员发送报警消息。

【报警方式】：异常通知用户的手段。包括短信、旺旺、邮件等。

5.2 功能说明

报警联系人管理，所属标签位置：【用户信息】 -> 【报警联系人管理】

5.2.1 新增报警联系人

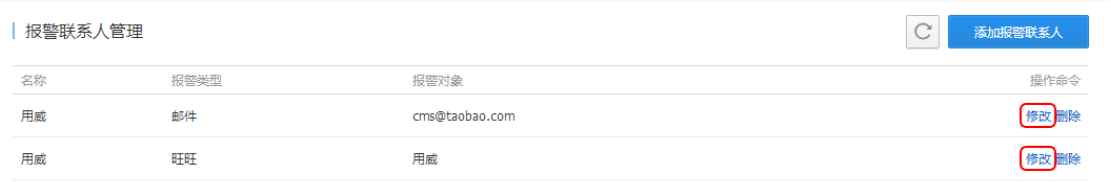
点击【添加报警联系人按钮】，如下图红框标识，出现添加报警联系人页面

下图为添加报警联系人表单页面。其中【姓名】为必填项目，且不能重复。余下【手机号码】、【邮箱地址】、【阿里旺旺】三个通知方式中，选择其中一个。目前单个联系人不支持多个手机号或者多个邮箱，多个旺旺。如有需要，可以通过新建多个联系人解决。

填写【手机号码】时，需要进行校验。点击【发送校验码】，系统会向输入的手机号发送校验码，请收到校验码后，输入到校验框中。校验码 1 分钟内有效，若 1 分钟内未使用将失效，请重新点击【发送校验码】。

5.2.2 修改报警联系人

在报警联系人列表中，点击【修改】按钮，进行联系人修改：



在修改联系人的界面，除姓名无法修改，手机号码、邮箱地址、阿里旺旺均可修改。

删除报警联系人时，目前删除的是单项，而不是整个联系人的所有信息。

5.3 报警组管理

添加报警组时，名称不可重复。一组报警联系人，可以包含一个或多个“报警联系人”。在报警设置中，均通过“报警组”发送报警通知。对应每一个监控点，根据预先设定的报警方式在到达报警阈值时采取不同的报警方式向报警组成员发送报警消息。

5.4 报警统计

【报警统计】功能展示的是每天发送的邮件次数、短信条数、旺旺次数，该统计会有几分钟（不超过 10 分钟）的统计滞后。手机校验码的发送量，也统计在短信发送条数中。每个用户总共拥有 1000 条短信/月的免费使用配额。