行云管家 V4 产品指导性文档-管理员指南

深圳市傲冠软件股份有限公司

2018 年 6 月 14 日

文档控制

更改记录

日期	版本	更改人	审批人	更改条款及内容
2018/6/14	V1.0	卢龙成		

审阅

单位	职位	签字	日期
开发商			
用户方			
监理方			
其他方			

分发

拷贝号	姓名	单位/职务

目录

第1章 登录系统

以浏览器访问行云管家，打开行云管家的登录页面，输入用户名及密码，点击“登录”即可登录系统。

第2章 权限管理

2.1 团队管理

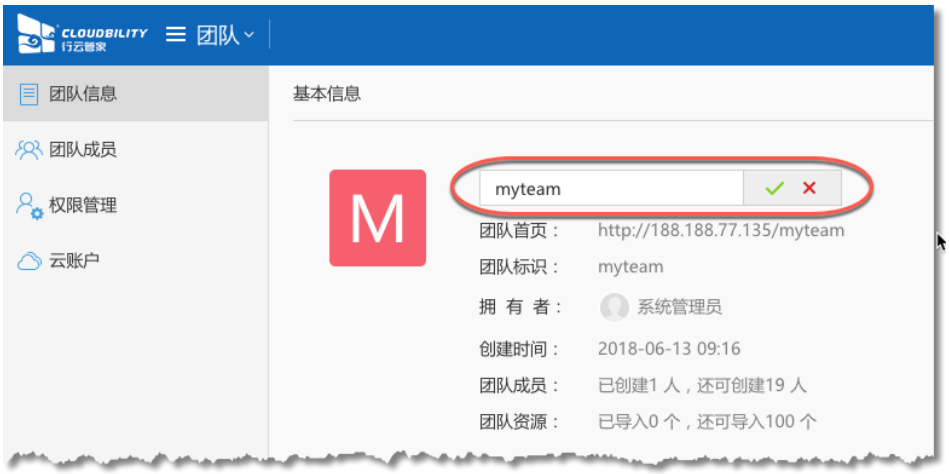
行云管家是一个基于团队协作的云资源管理平台，团队是行云管家中所有资源的载体，主机、文件、日志等数据资源依附于团队而存在，这些资源在团队范围内处于共享状态，团队中任何成员得到授权后均可以访问到这些资源。

管理员登录系统后，点击“开始”菜单，将弹出功能菜单，点击功能菜单中的“团队设置”，将进入团队管理页面。

2.1.1 设置团队信息

管理员可以对本团队的信息进行修改，目前仅支持修改团队名称；

在团队的工作空间进入“团队设置/团队信息”，将鼠标移入团队名称，将出现编辑图标，点击编辑图标，对团队名称进行修改；



2.1.2 查看团队成员

进入“团队设置/团队成员”，查看团队中所有的成员；

2.2 账号管理

2.2.1 添加团队成员（账号）

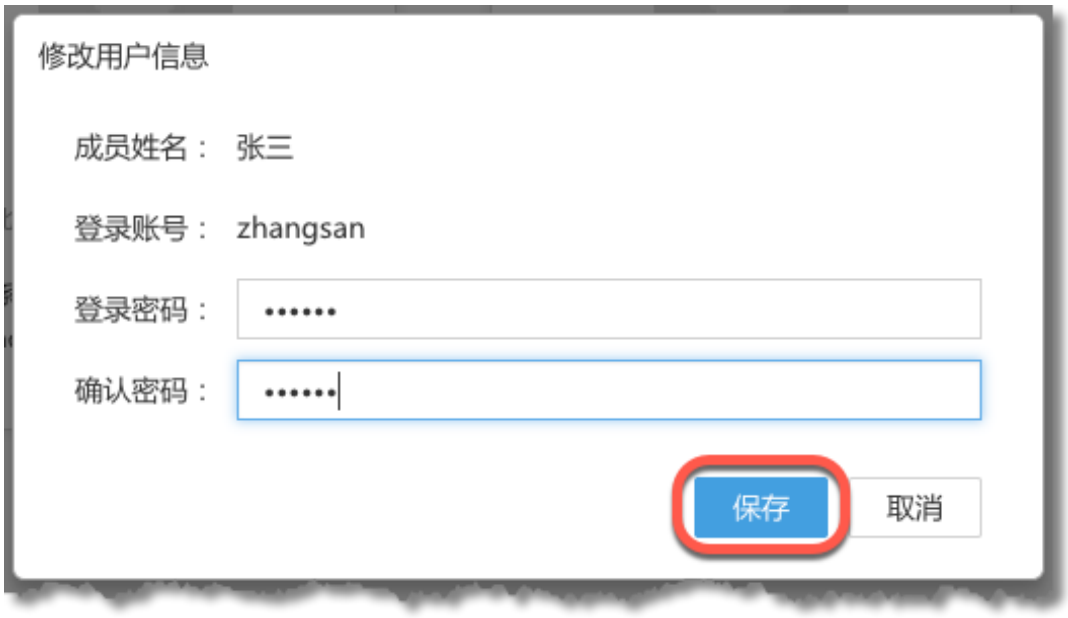
进入“团队设置/团队成员”，点击“添加成员”，将弹出添加成员对话框；

在添加成员对话框中，输入“成员姓名”、“登录账号”，并设置好密码，再点击“立即添加”，即可添加团队成员。

2.2.2 修改成员登录密码

将鼠标移入团队成员，将出现编辑图标，点击编辑图标，将弹出修改用户信息对话框

在修改用户信息对话框中，重新输入登录密码并确认，再点击“保存”即可修改成员的登录密码



2.2.3 删除团队成员

将鼠标移入团队成员，将出现删除图标，点击删除图标，将弹出踢出成员确认对话框

在踢出成员确认对话框中，点击“确定”即可删除团队成员

2.3 权限管理

行云管家是一种基于团队协作的工作模式，很自然的，我们需要通过权限控制来约束团队成员的行为，以实现安全运维的需要。行云管家采用基于角色的访问控制模型（Role-Based Access Control）来实现权限控制，具体来说，是将授权模型划分为功能授权和资源授权两个维度，而这两种授权都是针对角色的，角色是功能权限和资源权限的载体。当团队中的成员被添加到某一角色，该成员便自动拥有了该角色所被授予的各项权限。

2.3.1 功能权限原理

在基于角色的访问控制模型中，我们把功能权限赋予角色，再把角色赋予团队成员。团队成员和角色，角色和功能权限都是多对多的关系。团队成员拥有的功能权限等于他所有的角色持有功能权限之和。

2.3.2 资源权限原理

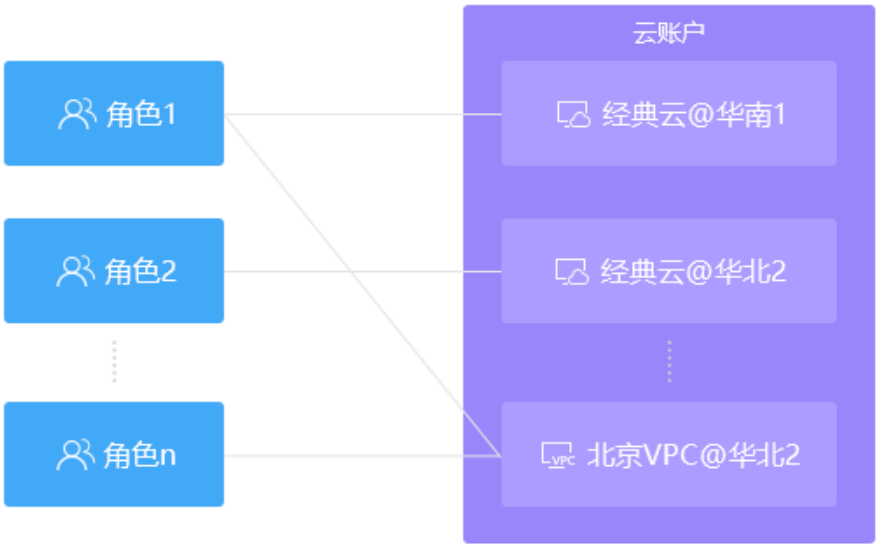
在行云管家中，资源授权中资源指的是导入到行云管家中的主机、对象存储 Bucket、CDN 加速域名等资源，在授权时，用户可以非常灵活的方式进行资源授权，既可以云账户为单位进行整体授权，也可以对云账户下某个区域/专有网络以物理网络的形态进行授权，甚至将云账户下的部分资源放到一个虚拟分组中，对该虚拟分组进行授权。和功能授权一样，我们把资源权限赋予角色，再把角色赋予团队成员。团队成员和角色，角色和资源权限都是多对多的关系。团队成员拥有的资源权限等于他所有的角色持有资源权限之和。

2.3.2.1 云账户授权

一个角色如果获得了某个云账户授权后，将默认拥有该云账户中所有资源的权限，在获得导入主机的功能权限前提下，可以向该云账户中导入主机，同时也能够查看该云账户的成本中心、网络等相关功能；

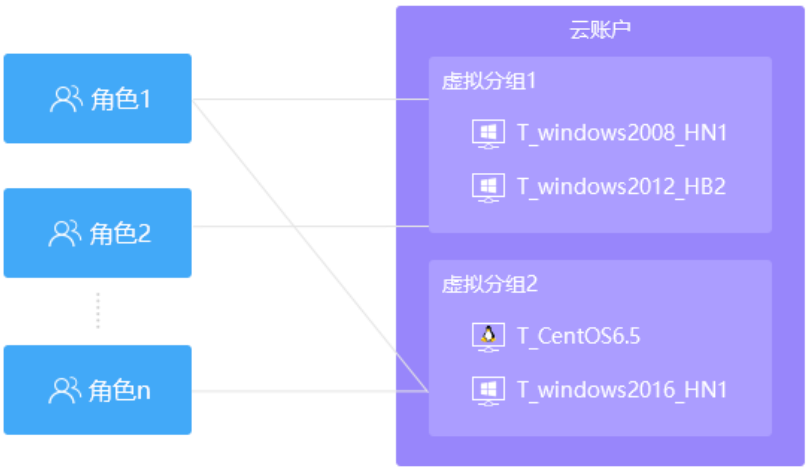
2.3.2.2 物理网络授权

物理网络授权只能获得云账户中某个区域/专有网络中的资源权限，如果网络中有新资源导入，可以动态的自动获得新资源的权限，不能查看该云账户网络等相关功能；



2.3.2.3 虚拟分组授权

虚拟分组由管理员手工创建，可以将云账户中部分资源添加到这个分组中，获得该资源权限的角色，对资源所属云账户并无权限，即便获得云账户相关功能权限，也无法管理云账户；



2.3.3 角色管理操作

在进行授权操作之前，您首先需要按照实际业务需求规划好相关角色，角色管理的入口位于团队设置中，进入“团队设置/权限管理”，即可查看“角色管理”。

2.3.3.1 了解系统内置角色

行云管家内置了“团队拥有者”和“管理员”两个基本角色，以及代表团队全部成员的“所有成员”这一特别角色，内置角色不可删除。

a）团队拥有者：团队拥有者默认拥有团队的完整管理权限，每个团队只允许拥有一个所有者。初始状态下，团队创建者即团队拥有者，但考虑到实际场景，团队拥有者可将此身份转移给其他团队成员。

b）管理员：管理员默认拥有大部分的业务管理权限，该角色可加入多名团队成员，用户可根据需要修改该角色的相关功能和资源授权。

c）所有成员：所有成员代表当前团队所有用户，无需再向该角色增添或删除任何用户，将某个权限项授给该角色，意味着团队内所有成员都会拥有此权限

2.3.3.2 查看角色成员

在角色列表中，我们可以看到每个角色均有“成员列表”，里面列出了该角色下的所有成员名单。

2.3.3.3 添加角色成员

一个成员可以同时拥有多个角色身份，如果要为某个成员指定某个角色，只需用鼠标点

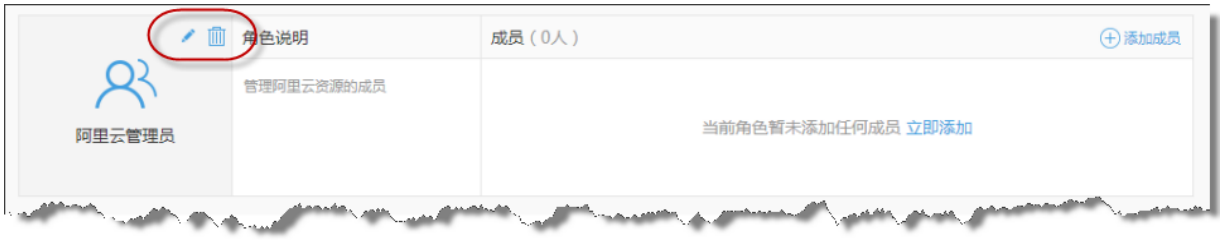
击该角色列表右上角的“添加成员”按钮，将该成员添加到该角色的成员列表中。

2.3.3.4 添加新的角色

除了系统内置的几个角色外，您可以根据实际需要自定义新的角色，在“角色管理”页面下方，点击“添加新的角色”，填写角色名称及说明后，点击“添加”即可。

2.3.3.5 修改和删除角色

对于用户自定义添加的角色，后期可对其进行修改和删除。将鼠标移动到角色名称所在表格的右上角，将出现修改角色名称和删除角色的图标，您可对角色进行修改或者删除操作。



2.3.4 功能授权操作

前文中已经介绍了行云管家授权模型原理和角色的管理操作，当您需要修改某功能项的授权时，只需在功能授权页面将相应角色添加到相应的功能权限项即可完成。

2.3.4.1 查看功能授权

进入“团队设置/权限管理”，点击“功能授权”页签。在这里列出了行云管家全部功能权限项，您可以通过设置操作对角色进行功能授权。

2.3.4.2 功能授权设置

除了“团队拥有者保留权限”之外，用户均可修改该权限项的授权。选择一个权限项，点击右侧的“设置”，打开功能授权对话框。

这里列出了团队拥有者、管理员、所有成员三个保留角色，以及全部的自定义角色，勾选您需要授权的角色，点击“确定”即可完成设置。需要注意的是，如果您勾选了“所有成员”，那么其他所有角色将自动选中，并处于 disable 状态。

2.3.5 资源授权操作

我们前面已经了解了资源授权可以分成云账户、物理网络、虚拟分组三层授权体系。因此，我们在进行资源授权前，需要对资源授权做一个规划，确保授权逻辑是准确的。

2.3.5.1 查看资源授权

进入“团队设置/权限管理”，点击“资源授权”即可查看所有的资源授权情况，默认情况下，系统会自动创建云账户及其下的物理网络（即区域或 VPC）授权，并对所有成员进行开放，您可以通过“授权”按钮修改云账户的授权情况。

2.3.5.2 修改资源授权设置

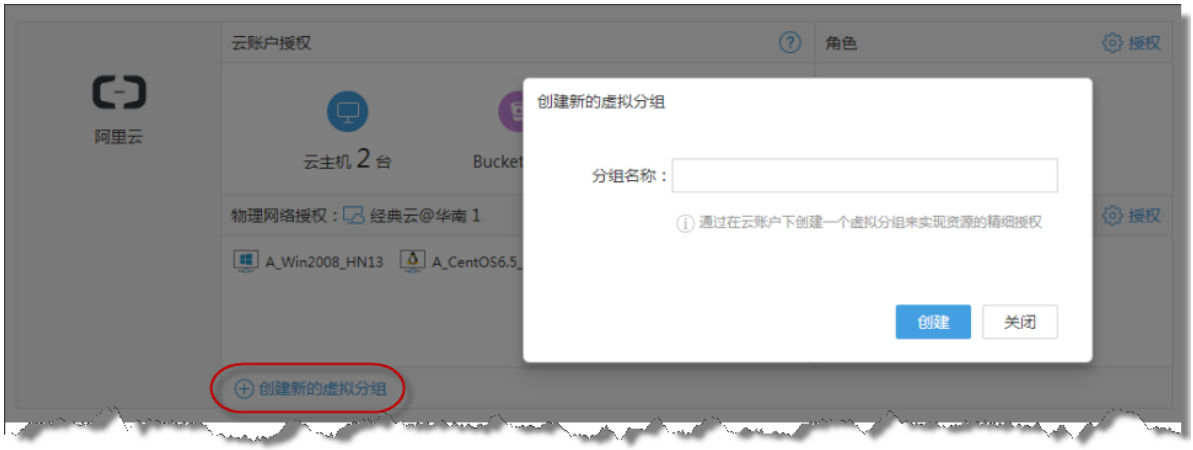
选择一个云账户或物理网络，点击右侧的“权限设置”，打开资源授权对话框，和功能授权一样，在对话框中选择对应的角色后点击“确定”即完成了该云账户的资源授权管理。

2.3.5.3 通过虚拟分组实现主机维度的权限管理模型

行云管家资源授权是以云账户为基本隔离单元，但是通常情况下，用户在导入主机时，一般是将一个云厂商账号或局域网中的所有主机都归到一个云账户中，那么在资源授权时，只能把该云账户下的所有主机都授权给某个角色，很显然这种方式是无法满足主机维度的精细化授权需求的，那么这种情况下，我们就需要通过创建虚拟分组来实现主机维度的权限管理模型。

2.3.5.3.1 创建新的虚拟分组

点击“创建新的虚拟分组”链接，在创建虚拟分组对话框中输入分组名称；

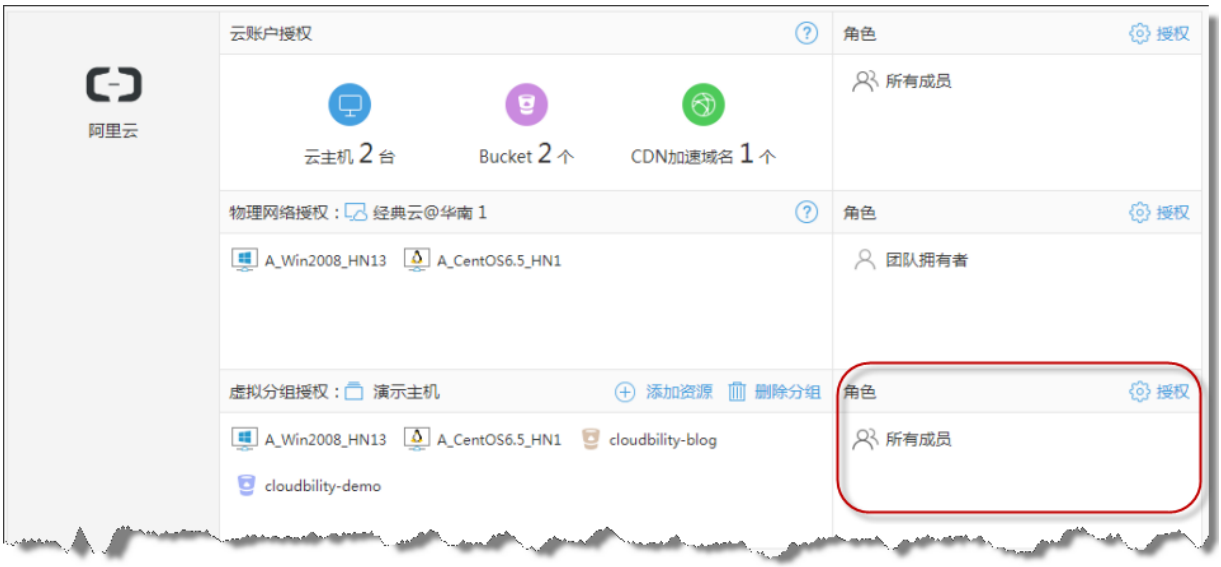


2.3.5.3.2 添加主机资源

在创建好的虚拟分组“演示主机”中，将需要进行精细化授权的主机（也支持云账户下的其它资源）添加进来；

2.3.5.3.3 修改虚拟分组授权角色

像云账户授权一样，修改该虚拟分组的授权策略，赋予相应的角色授权；



2.4 云账户

行云管家能够将各大云计算厂商中的云资源接入进来统一管理，出于云厂商隔离和业务划分的考虑，在行云管家中，以云账户作为云主机、对象存储、CDN 等云资源的容器及业务隔离单元。例如，用户张三在阿里云有一个账号，里面购买了云主机、CDN 等产品，那么这个账号体现在行云管家中，就是一个云账户。张三可能在腾讯云中也购买了一些云产品，那么他也可以将腾讯云的账户也导入到行云管家中，这样张三便拥有了两个云账户，分别管理他在阿里云和腾讯云的云资源。

2.4.1 云账户管理

1、云账户是属于团队的资产，因此首先需要进入“团队设置”；

2、点击左侧的“云账户”菜单，进入云账户管理。云账户无法单独创建，需要通过在导入相应的云资源过程中创建，如导入云主机、对象存储 Bucket、CDN 加速域名等，请继续阅读本文下面的内容来了解如何创建云账户。

2.4.2 创建云账户

本文以导入云主机为例，来演示如何创建云账户。一个云账户包含有用户在云厂商的 API 凭证、云主机资源等信息。因此，在新增云账户时，您需要准备好云厂商的 API 凭证和确定需要导入到行云管家的主机；

1、进入主机栏目；

2、点击“导入云主机”，打开向导；

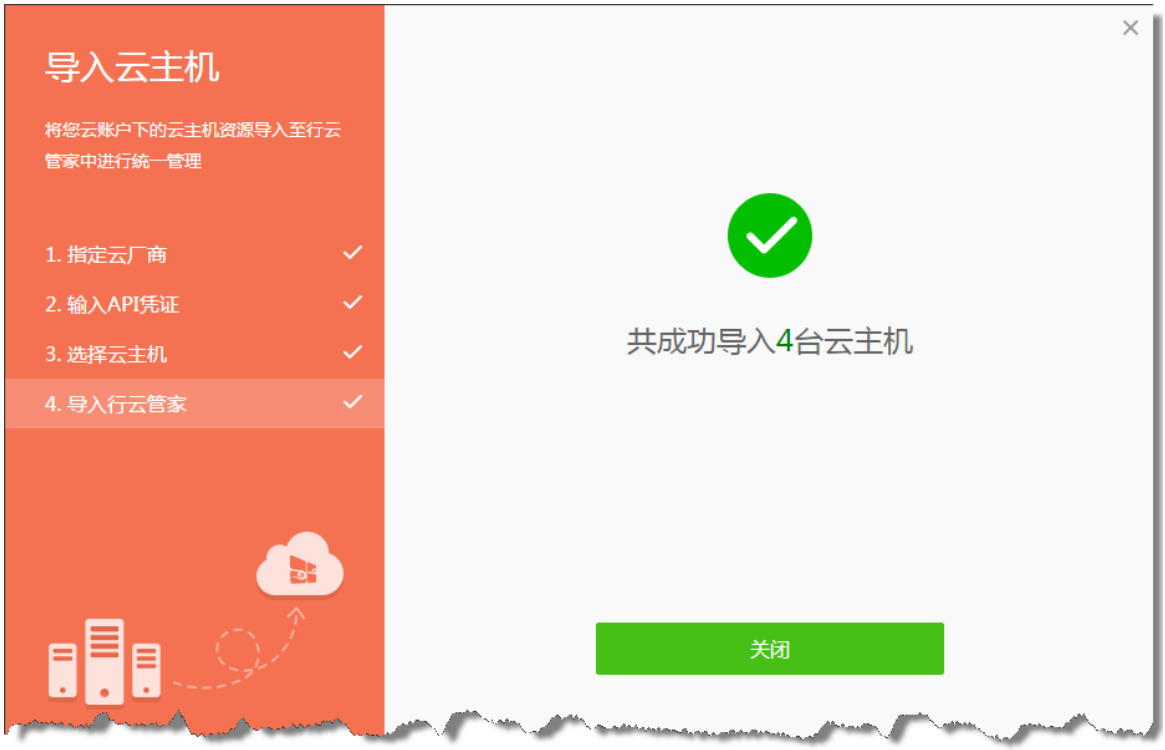
3、当前团队没有云账户时，会自动进入关联云厂商账户的向导，选择您需要导入的云厂商，点击“下一步”；

4、输入云厂商的 API 凭证（特别对于阿里云用户，我们提供了演示用的 Access Key），验证通过后点击“下一步”；

5、选择需要导入的云主机，点击“下一步”；

6、设置云账户名称，点击“下一步”；

7、在导入主机进度完成后，整个向导完成；

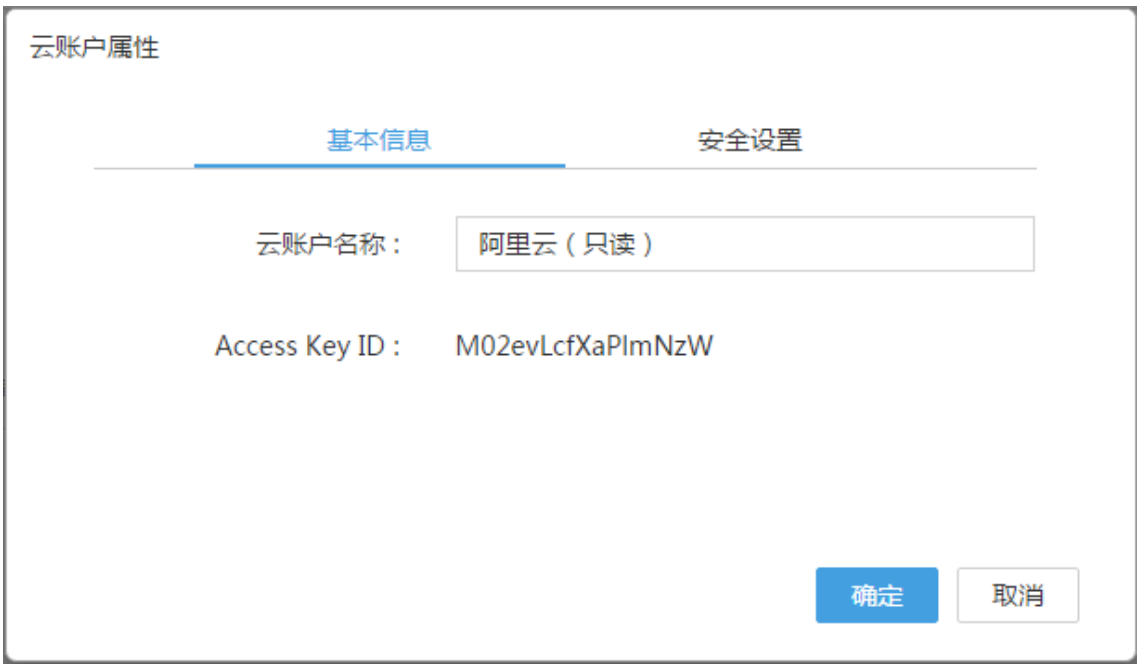


8、在云账户列表中，我们可以看到刚才创建的云账户；

2.4.3 云账户设置

云账户设置可以对云账户的名称和审计录像等进行设置，点击云账户设置图标，弹出云账户属性窗口；

云账户属性分为“基本信息”和“安全设置”两个标签页，基本信息可以修改云账户的名称；



安全设置用于对主机的操作录像进行相关设置；

第3章 设备管理

3.1 支持的云主机

截止目前，行云管家已经支持了阿里云、腾讯云、Ucloud、百度云、AWS 中国、Azure 中国几家云厂商，用户的云主机如果属于以上云厂商，皆可导入到行云管家中进行管理

3.2 导入云主机

如果这是您第一次导入云主机，您需要先创建云账户，在创建过程中，直接将云主机导入到行云管家。如果您已经拥有了云账户，想将未导入的云主机也添加进来，可以继续点击“导入云主机”，选择云账户；

行云管家将会把当前云账户下剩余主机全部列出，您可以根据需要选择需要导入的云主机；

3.3 导入局域网主机

3.3.1 局域网主机在行云管家中是什么概念

我们知道，行云管家是一个云计算管理平台，目前行云管家已经通过 API 的形式支持了业界主流的云厂商，但是，用户的主机资源并非只有公有云主机一类，OpenStack、VMware 等私有云平台应用也非常广泛，另外传统的 IDC 托管服务器也并未完全消亡，甚至还有相当数量的小公有云厂商由于诸如 API 等问题无法进行支持。

基于以上行业现状，行云管家为用户提供了局域网主机的解决方案，把这类无法通过 API 导入的主机，均以局域网主机的形式接入到行云管家上来。因此，行云管家中的局域网主机，并非我们传统意义上的“局域网络内的主机”，而是相对公有云 API 导入方式而言的另外一种主机导入方式。

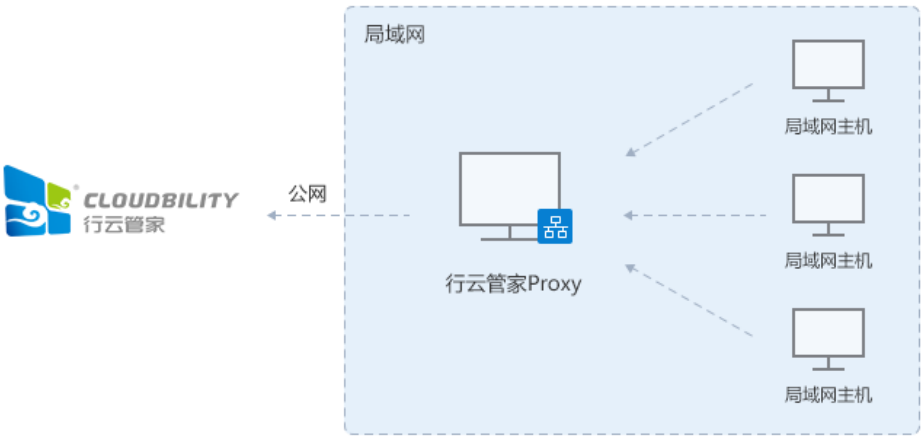
3.3.2 公有云主机和局域网主机在功能上有哪些差异

行云管家为用户提供了一站式的IT运维管理功能,其中即有主机监控、堡垒机安全审计、自动化运维等基础运维功能，也有成本等公有云特有的功能，因此，公有云主机和局域网主机在管理功能上来说，存在一些差异，主要体现在：

功能对比	主机类型	
	公有云主机	局域网主机
主机访问	√	√
主机监控	√	√
安全审计（堡垒机）	√	√
主机会话文件传输	√	√
文件传输区域优化	√	×
磁盘快照	√	×
自动化运维	√	√
成本分析	√	×
主机体检	√	√

3.3.3 接入局域网

需要在行云管家中管理局域网主机，首先要建立一个局域网与行云管家之间的数据通讯链路。在行云管家中，我们通过在局域网中部署一个 Proxy 来实现这个连接，这个 Proxy 负责局域网主机和行云管家的通信代理，部署模型如下图所示：



了解了局域网主机管理原理后，我们接下来介绍如何将局域网接入到行云管家中。

3.3.3.1 接入流程

1、打开接入局域网向导

点击“导入局域网主机”，如果是第一次导入局域网主机，将出现“暂无可用的局域网Proxy，是否立即接入新的局域网”提示，点击“确定”按钮，打开“接入局域网”向导；

2、设置局域网信息

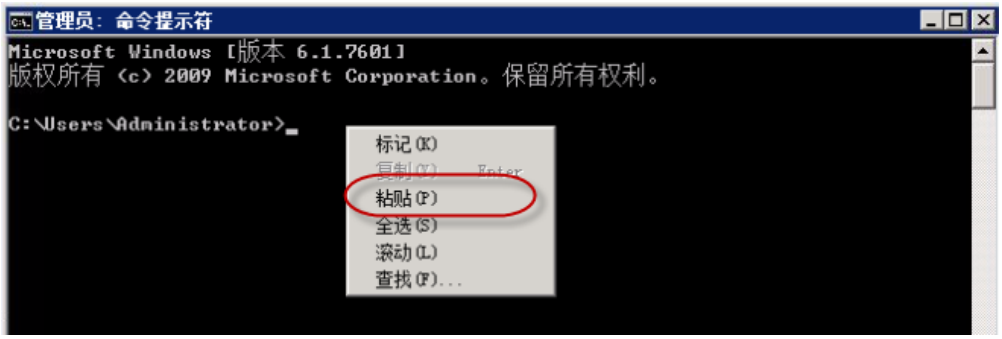
只需为您的局域网设置一个名称即可，点击“下一步”；

3、获取 Proxy 安装脚本

Proxy 负责局域网与行云管家之间的通讯，选择一台主机作为宿主机，无需逐台安装，请根据您的 Proxy 宿主机操作系统选择脚本类型，获得相应的 Proxy 的安装脚本，并将其复制；

4、安装 Proxy

将脚本粘贴到宿主机的 CMD 窗口上（Windows）或 SSH 终端中（Linux），再执行安装脚本（必须是管理员身份）；



请注意，Proxy 安装脚本是在您上一步选取的 Proxy 宿主机上执行的，而非您的个人终端，如果安装脚本无法执行，您可以尝试手动下载安装包。

5、关闭向导

不论您是否安装了 Proxy，您都可以直接点击“下一步”后直接关闭向导，但要想继续完成导入局域网主机的功能，您必须确保您的 Proxy 处于正常工作状态。

6、确认 Proxy 状态

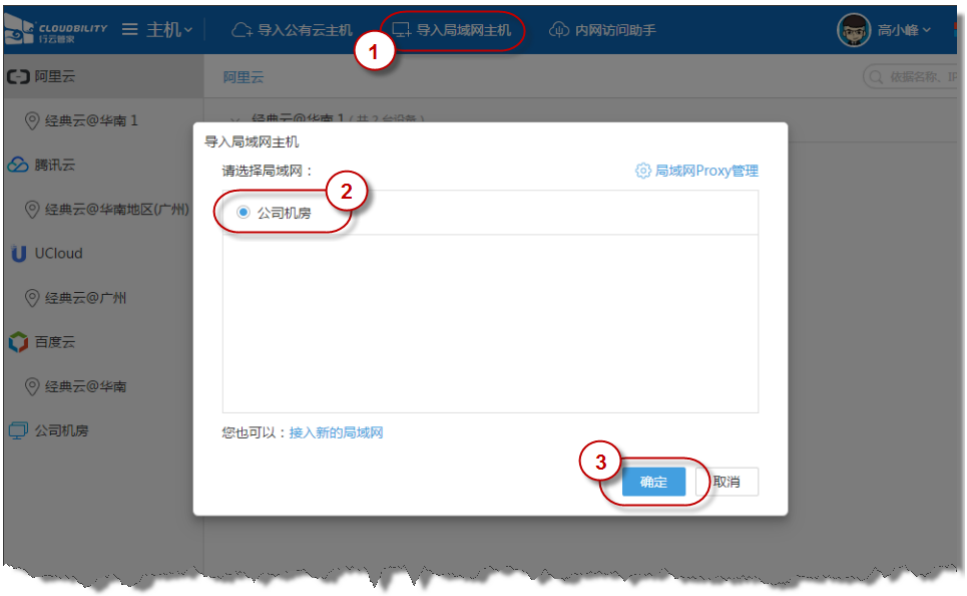
如果您已经正确安装了 Proxy，但界面上仍然提示“未检测到 Proxy，无法将局域网主机接入行云管家”，请点击“已经安装，立即刷新”。

3.3.4 导入主机

在 Proxy 正常运行之后，您可以将局域网中的主机导入到行云管家中进行管理。

1、打开导入局域网主机窗口

点击“导入局域网主机”，选择上一步所创建的局域网账户，点击“确定”按钮，打开“导入局域网主机”窗口；



2、输入主机搜索条件

输入您欲导入到行云管家的主机 IP 规则，点击“检索”，Proxy 将会自动将这些 IP 扫描

出来，目前 IP 规则支持以下格式：

a）单个 IP：当输入单 IP 时，不论该 IP 是否存在，都可以将其导入；

b）IP 网段：支持扫描 Proxy 宿主机所在 IP 段存在哪些主机，用户可自由决定要将哪些主机导入到行云管家；

3、将局域网主机导入

主机扫描完成后，选择相应的主机，点击“添加”，将所选主机全部导入到行云管家中进行管理；

3.3.5 为何通过 IP 段无法扫描出所有主机

在导入局域网主机时，用户可以通过 IP 段来将网段中的主机扫描出来，但有些情况下，部分主机却一直扫描不出来，这是为什么呢?

这其实和网段的扫描手段有关，行云管家是通过 Proxy 来对网段中的主机进行 Ping 来发现主机，如果主机设置了禁止 Ping，则会导致无法扫描出来；

如果碰到这种情况，用户可以通过以下手段来处理：

1、用户可以直接输入该主机的 IP，单独将主机导入，在输入单 IP 时，并不会扫描该主机是否存在，可以强制将其导入；

2、开启主机的 Ping 服务，让 Proxy 能够发现该主机的存在；

3.3.6 如何选择 Proxy 宿主机

在安装 Proxy 之前，我们需要先选择 Proxy 宿主机，Proxy 的宿主机选择需要遵循以下原则：

a）宿主机和其它主机处于同一个局域网内，且能够和其它主机通过局域网互通；

b）宿主机无需具备公网 IP，但必须要能够访问公网；

c）宿主机拥有大于 100M 的剩余空间，以及 64M 以上的可用内存。

3.3.7 如何在一个网络中部署多个 Proxy 进行负载

在网络中，如果 Proxy 发生了单点故障，将导致严重后果。行云管家支持在一个网络中部署多个 Proxy，以起到负载均衡的目的。

1、进入“网络”功能模块，查看当前团队所有网络；

2、找到您要部署多台 Proxy 的局域网，点击进入；

3、在局域网页面，左侧是当前所有的 Proxy，右侧是当前网络内所有主机，点击下方“可在同一个网络中部署多个 Proxy 以起到负载均衡的目的”；

4、打开安装 Proxy 界面，仍然是以脚本的形式进行安装，您可以将脚本复制到目标主机中进行执行；

3.3.8 Proxy 出现异常如何处理

3.3.8.1 异常原因

Proxy 通过心跳的方式与行云管家进行门户通信，当助手运行状况出现异常，能够实时向门户汇报，因此，我们可能会在门户中看到以下状态：

通常情况下，Proxy 运行异常可能由于以下原因导致：

1、升级失败：当行云管家对 Proxy 进行升级时，运行在用户主机上的 Proxy 均会自动升级，但如果用户日常将助手停用，会断开其与门户的正常通信，导致无法正常升级；

2、Proxy 文件损坏：可能由于文件误删除、助手被卸载等情况，导致 Proxy 本身无法正常启动；

3.3.8.2 修复方式

当 Proxy 出现异常时，建议先尝试重启解决，如果是 Linux，请直接输入以下命令进行重启：

```
/etc/init.d/CloudGateway restart
```

如果是 Windows，请进入安装目录（默认是：C:\Program Files (x86)\Cloudbility\CloudGateway\bin）执行以下命令：

```
stopCloudGateway.bat
startCloudGateway.bat
```

如果重启仍无法解决，您可以先删除 Proxy 再重新安装，删除 Proxy 操作步骤请见下文。

3.3.9 删除 Proxy

如果您要将网络中的某个 Proxy 删除，只需点击打开该 Proxy 的属性窗口，点击“卸载”即可。

一般情况下，主机中的 Proxy 程序会自动卸载，如果由于各种原因导致 Proxy 程序未自动卸载，请手工执行以下脚本：

Linux 版本

使用 root 权限执行以下脚本：

```
sudo uninstallCloudGateway.sh
```

Windows 版本

使用管理员身份打开 CMD 命令提示行，进入安装目录（默认是：C:\Program Files (x86)\Cloudbility\CloudGateway\bin），执行以下命令：

```
uninstallCloudGateway.bat
```

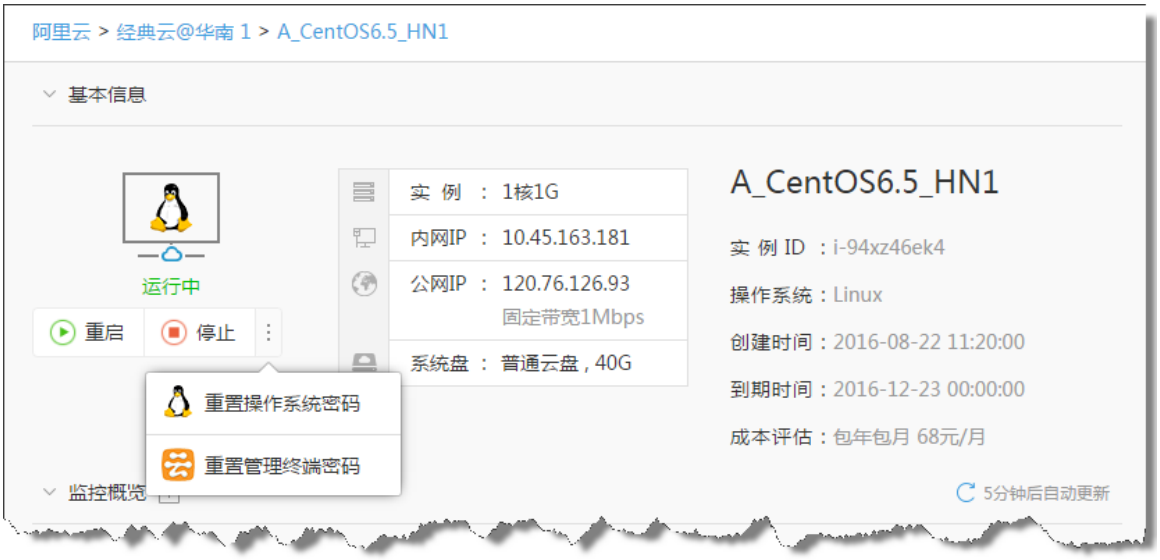
3.4 管理主机

3.4.1 查看主机详情

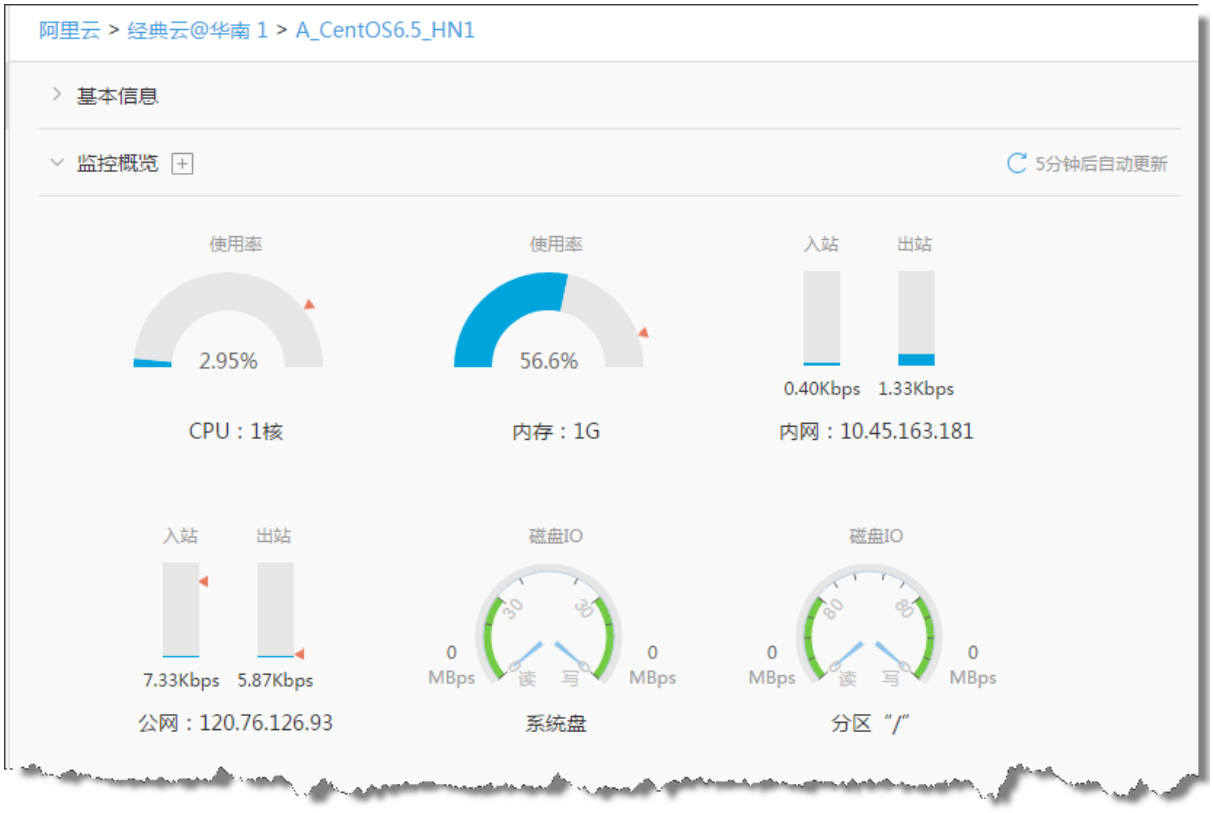
在云账户主机列表中，您可以点击任意的主机图标进入该主机的详情页面；

主机详情从主机基本信息、监控概览、接入方式等角度展示主机信息；

基本信息展示该云主机的实例配置情况、成本及到期时间等信息，并提供主机启动停止、重置密码等基本操作；



监控概览展示了 CPU、内存、网络和磁盘分区等配置的实时负载信息，并提供进一步的监控详情及告警设置入口，行云管家为用户提供了丰富的主机监控服务，包括云厂商监控（公有云）和行云管家 Agent 监控两种模式，详情请参见：主机监控；

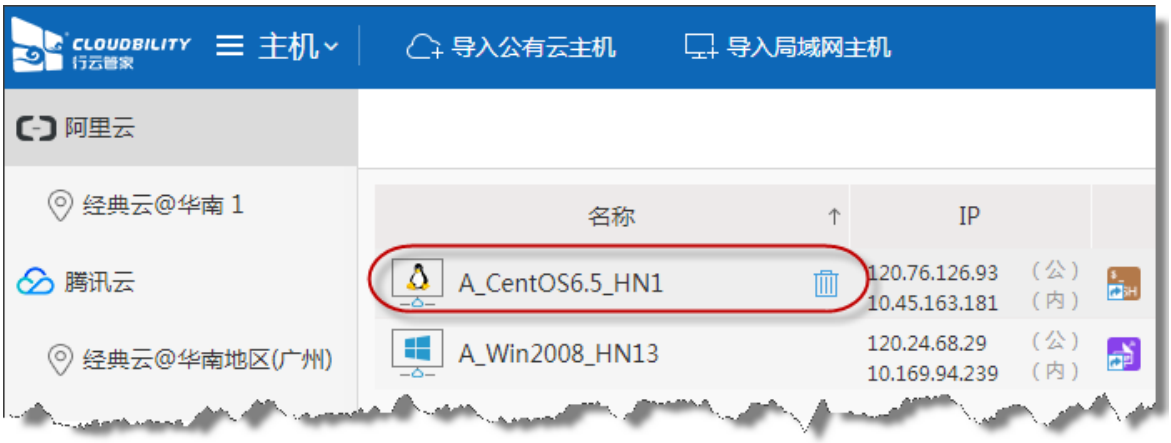


接入方式是主机的访问入口，用户在此处访问主机的远程桌面/终端，主机访问详情请参见：访问主机；

3.4.2 重置主机操作系统密码

每台主机在系统初始状态时，都有默认创建的管理员账号，如 root、Administrator（对于云主机而言，默认管理员随着云厂商不同而存在差异，如 Azure 不允许设置 Administrator 为默认管理员）。当用户遗忘了默认管理员密码，可以通过行云管家提供的“重置主机操作系统密码”功能，找回默认管理员密码。

1、找到目标云主机，进入主机详情页面；



2、展开主机功能菜单；

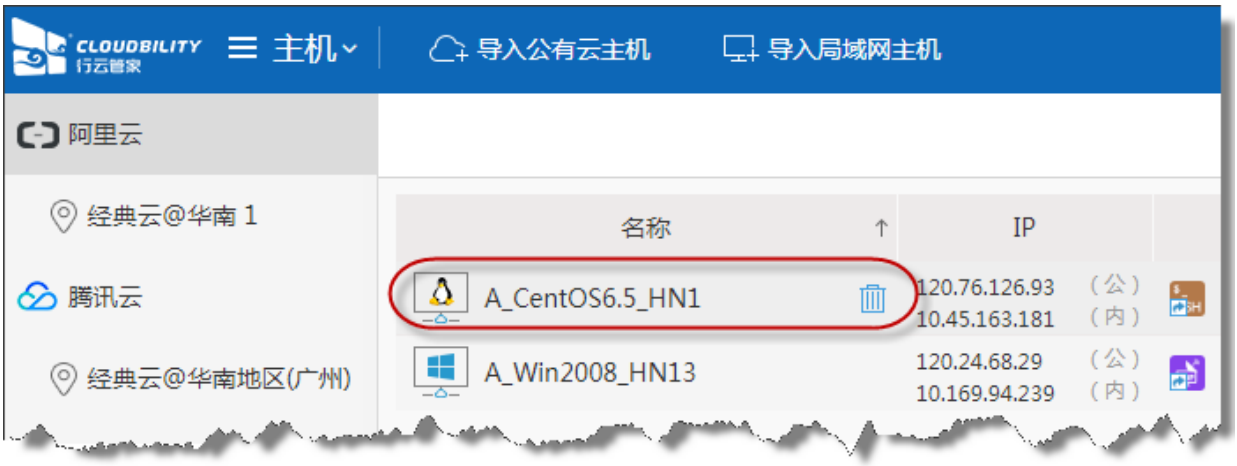
3、点击“重置操作系统密码”，在弹出的界面中输入新密码（目前 Azure 中国和局域网主机暂不支持）；

4、部分厂商的部分系列云主机产品，修改操作系统密码只有在云主机重启后才能生效，因此建议您在不影响服务的情况下重启您的主机。

3.4.3 移除主机

用户可随时移除已导入到行云管家中的主机，在云账户主机列表中，将鼠标移入主机图

标，出现“移除”按钮，点击后在弹出的提示框中选择“确定”。移除后，您还可以通过“添加云主机”的方式再次导入该主机。



3.4.4 主机监控

3.4.4.1 行云管家如何提供主机监控服务

在行云管家中，我们为用户提供了两种模式的监控服务：云厂商监控和行云管家 Agent 监控（需要在主机上安装行云管家 Agent）；

对于公有云主机而言，行云管家通过 API 集成了各大云厂商监控服务，用户可直接在行云管家中查看云厂商的监控数据。同时，如果云主机上已经安装了行云管家 Agent，也可采用行云管家 Agent 监控；

而对于局域网主机，只能通过安装行云管家 Agent 来获得监控服务。

3.4.4.1.1 监控模式对比

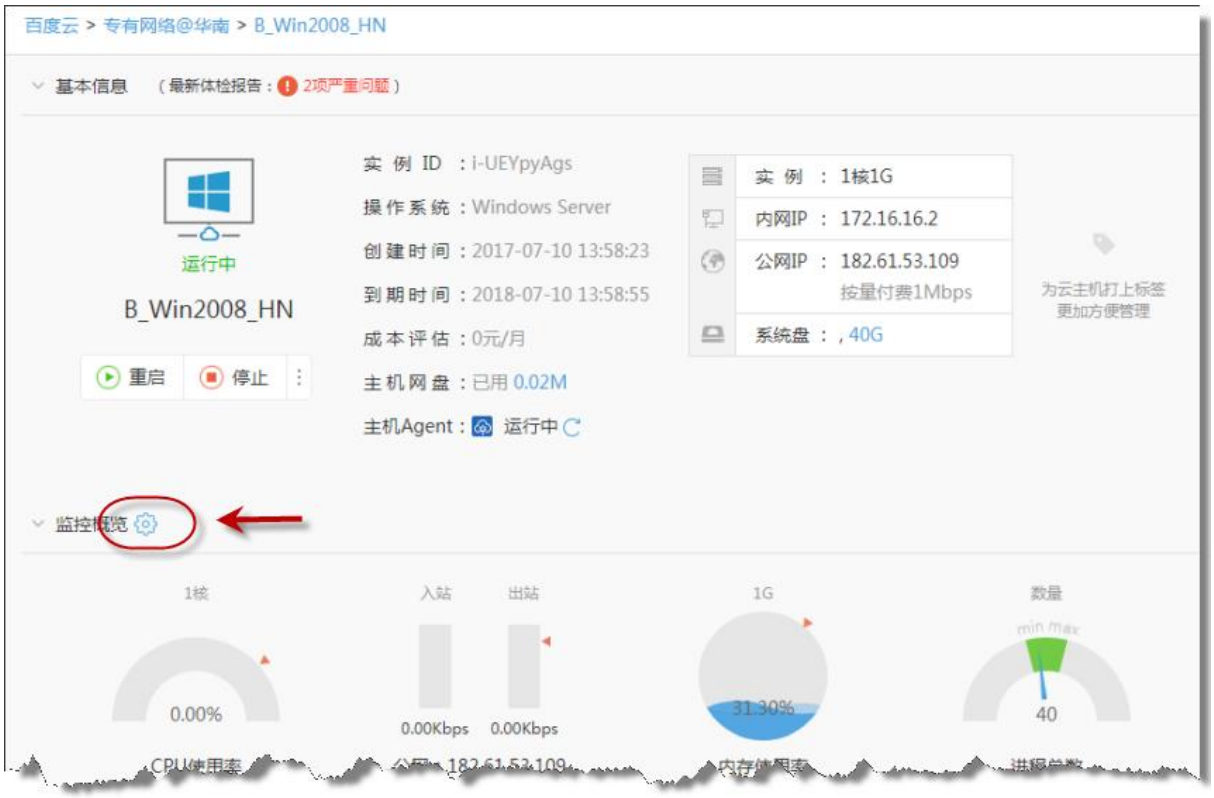
受限于公有云厂商 API 的限制，云厂商监控模式存在诸如监控项过少、监控数据丢失、监控频率过低等问题。行云管家 Agent 监控模式，由安装在主机上的行云管家 Agent 插件直接向服务器汇报监控数据，有着稳定性高、频率高的优点，下面表格展示了两种监控模式的差异：

对比项	云厂商监控	行云管家 Agent 监控
数据来源	云厂商监控 Agent	行云管家 Agent
监控项数量	不同云厂商，监控项数量不一致	10 项
监控频率	5 分钟/次（收费版团队阿里云主机 2 分钟/次）	1 分钟/次
稳定性和准确性	依赖于云厂商 Agent 和 API	高

3.4.4.1.2 监控模式切换

所谓监控模式的切换，是指公有云主机监控可在公有云厂商监控和行云管家 Agent 监控模式之间进行切换。

在主机详情的监控概览中，点击“监控模式设置”图标，打开“设置主机监控模式”窗口。



根据您的需求，选择您要采用的监控模式，点击“确定”后保存设置。

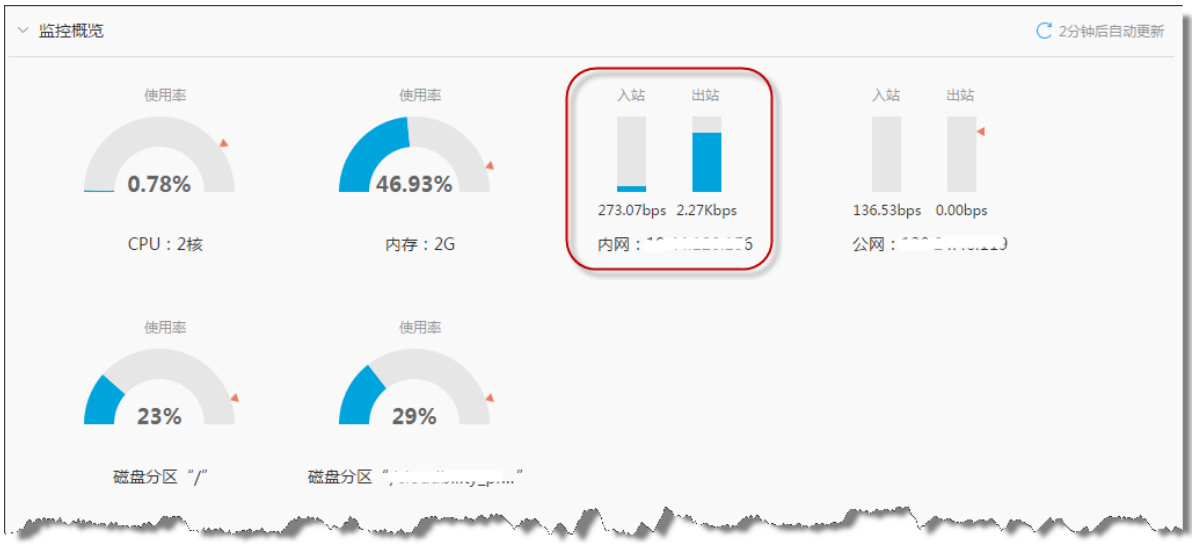
3.4.4.2 自定义监控项

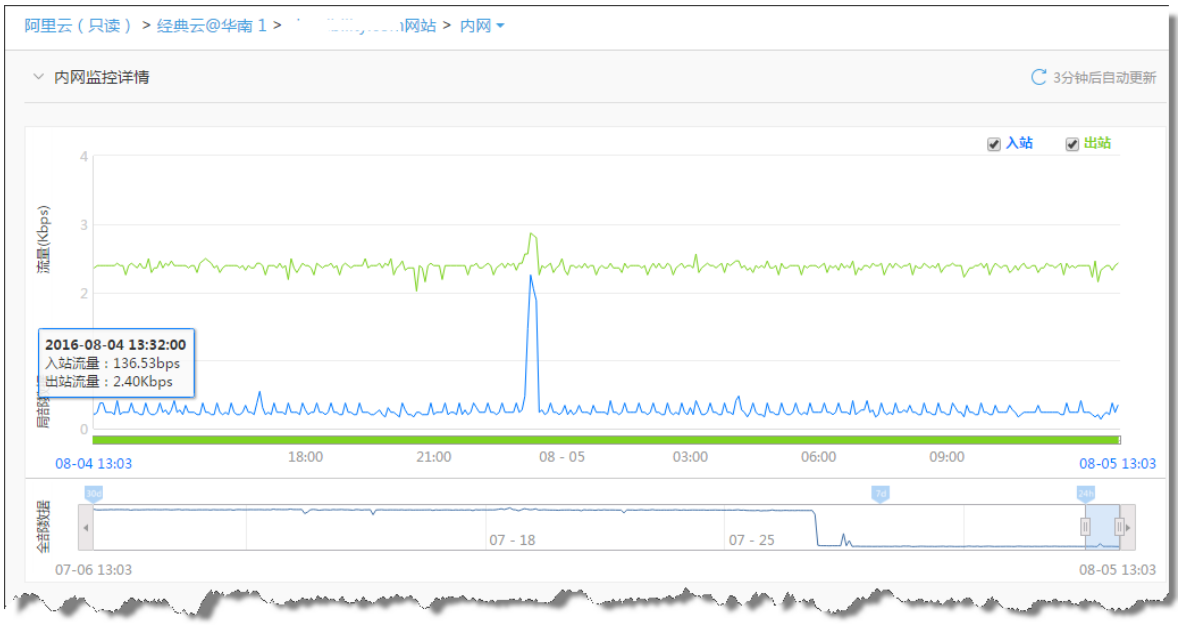
不论用户采用何种监控模式，行云管家都将默认提供一些基础监控项（如 CPU），若用户需要更丰富的监控项，请进入主机详情页面，点击添加按钮增加监控项。需要注意的是，云主机某些监控项依赖于云厂商的监控 Agent，否则将无法获取监控数据；

同样，您也可以删除不关心的监控项。

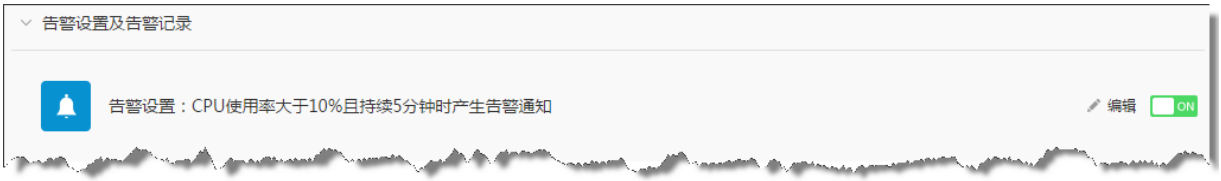
3.4.4.3 查看监控数据及告警设置

您可以通过点击云主机任意一个监控项的图形界面进入到该监控项的监控详情，下图以内网流量监控为例；





根据监控项的不同，行云管家提供了相应的告警设置，您可以依据真实情况修改告警的阈值或停用部分告警，下图以 CPU 监控的告警项设置为例；



当云主机某项负载达到告警阈值时，将产生告警记录；

同时，在主机图标中，将标记告警状态，提示用户当前云主机的异常状态；


经典云@华南 1（共 5 台设备）
网站
centos_sz
windows_sz

第4章 凭证管理

4.1 SSH 密钥对管理

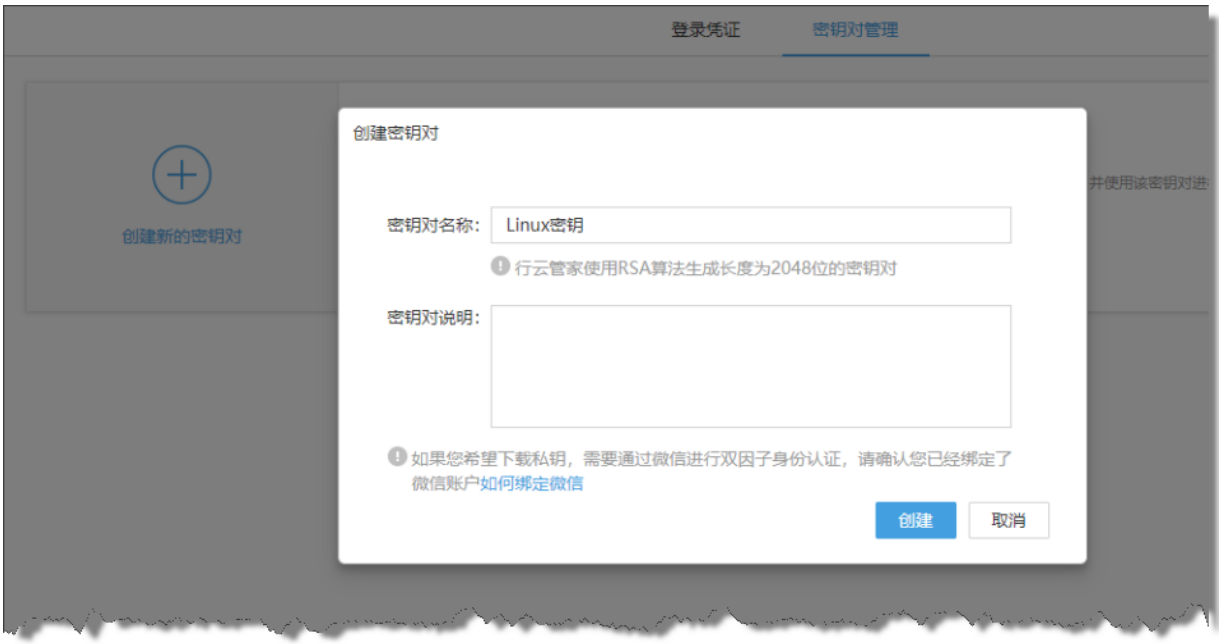
我们知道，访问 Linux 服务器通常使用 SSH 协议，而 SSH 协议支持密码和密钥两种身份认证机制，但是基于安全性考虑，我们建议用户在使用 SSH 时，尽量使用密钥的方式，避免攻击者使用暴力破解来猜测 Linux 主机密码；

对于 Linux 入门用户来说，启用 SSH 密钥登录配置过程繁琐，即便是对 Linux 熟悉的用户，也需要定期更换 SSH 密钥，以确保安全。针对这一需求，行云管家提供了 SSH 密钥对管理的功能，为用户提供傻瓜化的 SSH 密钥配置和一系列的管理能力。

4.1.1 在行云管家中将 SSH 公钥下发至主机

启用 Linux 主机的 SSH 密钥登录，其本质是将 SSH 公钥下发至主机，私钥保存在客户端用于登录。首先，我们需要创建一个 SSH 密钥对，进入“安全审计\登录凭证管理\密钥对管理”；

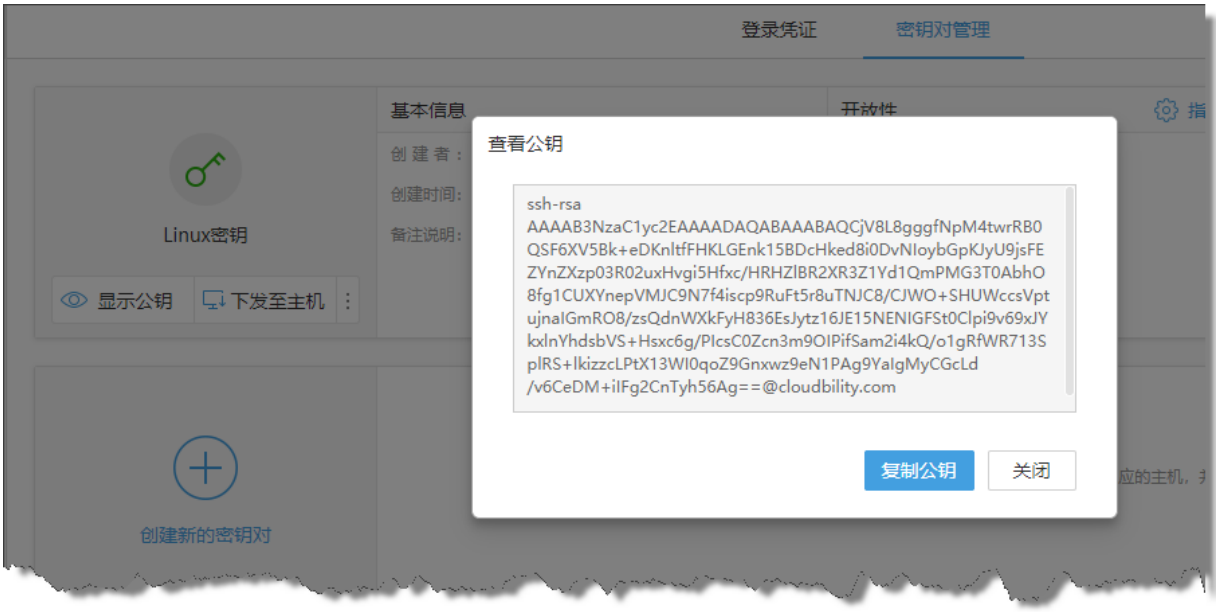
点击“创建新的密钥对”，在创建密钥对窗口中输入密钥对名称和说明，行云管家使用的是 RSA 算法，生成长度为 2048 位的密钥对；



在创建好的 SSH 密钥对中，我们需要关注到以下几个操作：

4.1.1.1 显示公钥

用于查看该密钥对的公钥内容，方便用户查验相应主机上关联的公钥内容；



4.1.1.2 下发至主机

将公钥批量下发至需要使用该密钥对的主机上，请根据向导的指引，选择相应的主机完成公钥下发操作；

4.1.1.3 下载私钥

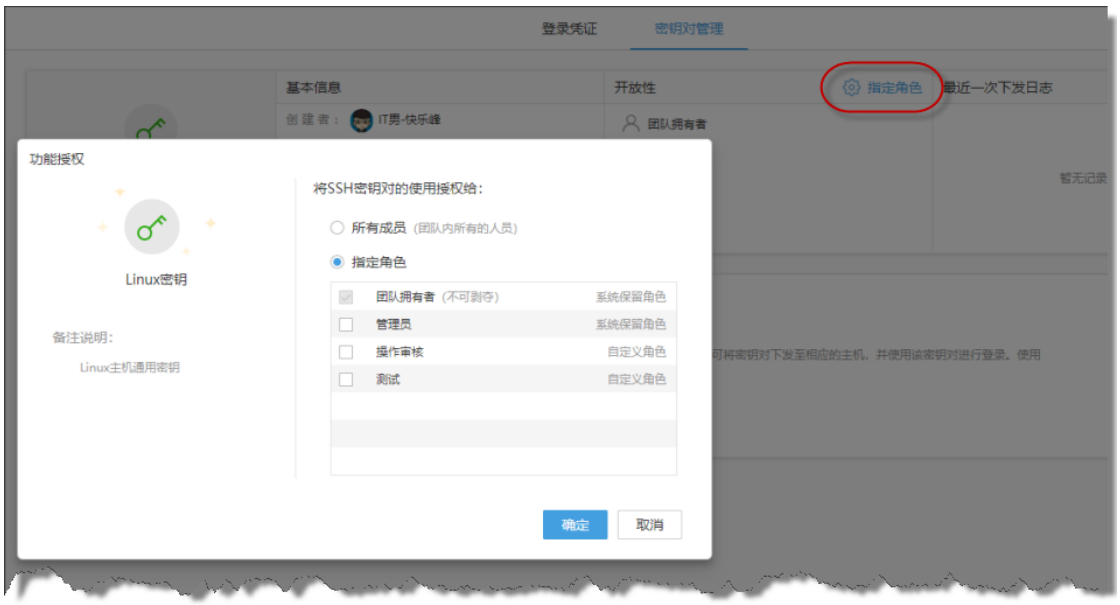
如果用户需要在其它 SSH 终端上使用该密钥访问主机，可以下载私钥文件，但为了避免

私钥泄露，系统要求对下载者进行基于微信的二次身份认证；

温馨提示：基于安全性考虑，请不要将私钥文件进行传播；

4.1.1.4 设置开放性

密钥对一旦下发到目标主机之后，默认情况下，团队管理员可以使用该密钥对来访问目标主机的 SSH，如果您希望其他成员可以使用该密钥，可以将相应的角色加入到开放性列表中；



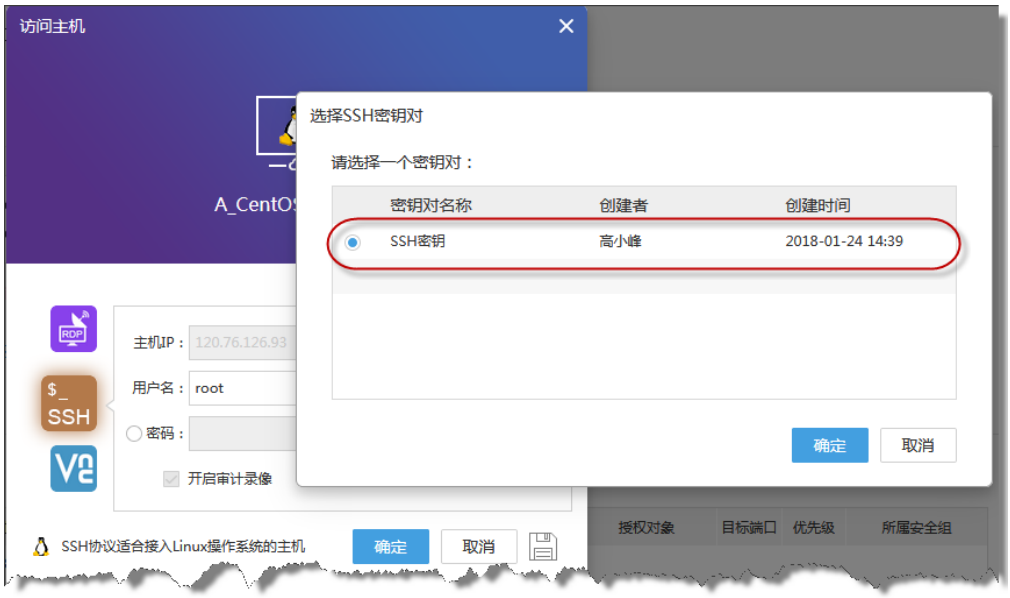
4.1.2 如何在行云管家中使用 SSH 密钥登录

在行云管家中，用户可以上传已有的 SSH 密钥，也可以使用行云管家创建的 SSH 密钥（前提是已将密钥下发至该主机）；

使用 SSH 协议访问主机，登录凭证选择“密钥”，点击展开按钮，可以看到“上传新密钥”和“使用密钥对”；

如果选择“上传新密钥”，您需要从本地上传已有的 SSH 密钥进；

如果选择“使用密钥对”，可以选择行云管家中创建好的 SSH 密钥；



只要该 SSH 密钥已经下发至主机，即可使用该 SSH 密钥进行登录。温馨提示：目前行云管家 SSH 密钥仅供本平台使用，暂不向其它 SSH 客户端开放私钥下载；

4.2 登录凭证

在主机数量较多时，为了方便管理，一般我们会为主机设置相同的用户名密码。这种场景下，我们就需要一种批量为主机设置访问凭证的方法。

在行云管家中，我们把这种方法称为“登录凭证”，只要创建一个登录凭证，设置好主机的访问协议、用户名、密码、默认端口等信息，再将相关的主机加入到这个凭证中，这些主机便自然能够使用这个登录凭证来访问。

1、进入“安全审计”功能模块，默认看到“登录凭证管理”；

2、点击“创建新的主机登录凭证”；

3、输入凭证名称、安全性及主机的登录信息后，点击“确定”进行保存；

4、我们把使用这套登录凭证的主机称为关联主机，在刚创建好的登录凭证中，点击“添加主机”，将它们添加到登录凭证的关联主机中；

5、考虑到安全性因素，如果该登录凭证使用的账户权限过高，您应该将该登录凭证限制为只允许部分成员使用，如：root 用户分配给管理员使用，welcome 用户分配给普通成员使用，要使用该特性，请在开放性列表中指定相应的角色；

第5章 运维策略

5.1 运维策略介绍

从安全运维的角度来看，资源授权满足了主机层面的安全管理需求，但是一旦登录到主机后，团队成员便可对该台主机进行任何的操作，如果出现问题，只能通过事后审计来回溯追责。所以我们还需要一种手段，对于一些安全要求更高的主机来讲，即使登录了主机，成员在其中执行的操作，依然处于安全监管之下，对其所执行的高危指令进行拦截，提前防范运维风险。

在行云管家中，我们把这些安全性更高的主机叫做关键设备，而将在这些主机上所执行的高危指令的定义以及相应的处理方式叫做关键设备运维策略。

5.2 运维策略设置

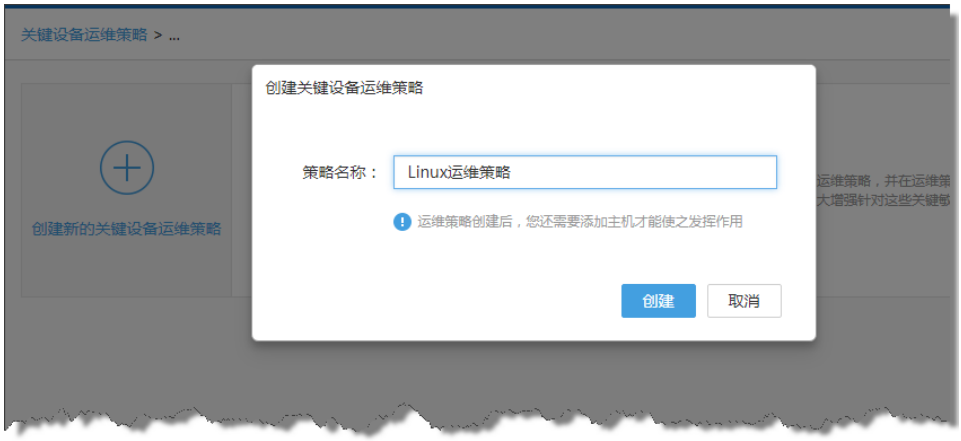
展开功能模块菜单，选择“安全审计/关键设备运维策略”，进入相应的策略功能设置。

5.2.1 新增关键设备运维策略

5.2.1.1 创建运维策略

点击“创建新的关键设备运维策略”，在弹出的窗口中，输入了策略名称后，点击“创建”即成功创建一条关键设备运维策略，但要生效，您还需要添加关键设备，只有在关键设备列

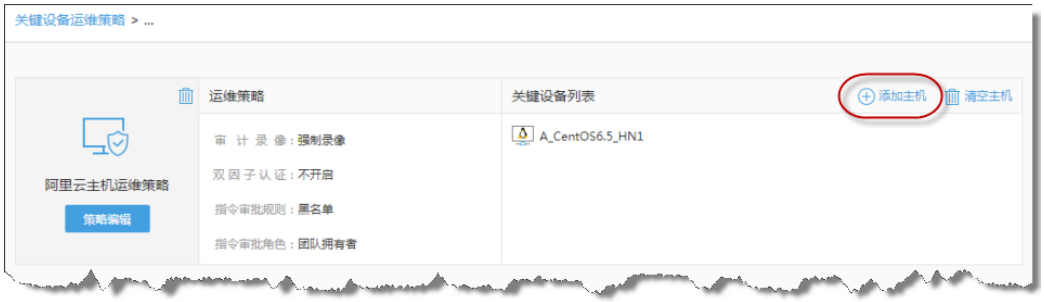
表中的主机，才会受该条运维的影响。



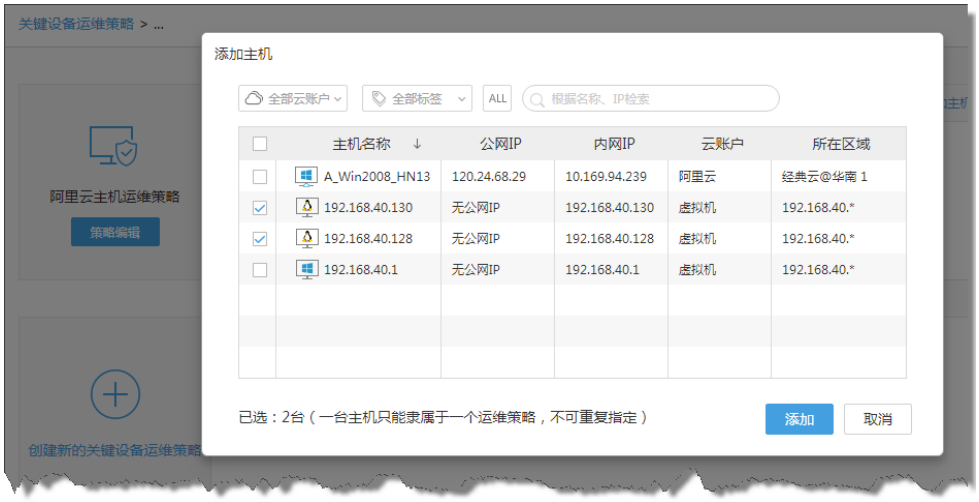
5.2.1.2 添加关键设备

首先您需要根据业务情况定义好哪些设备主机属于关键设备，关键设备允许跨云账户添加，但每台主机只允许添加到一个运维策略中，不能重复添加；

点击相应策略里的“添加主机”链接，弹出对话框；

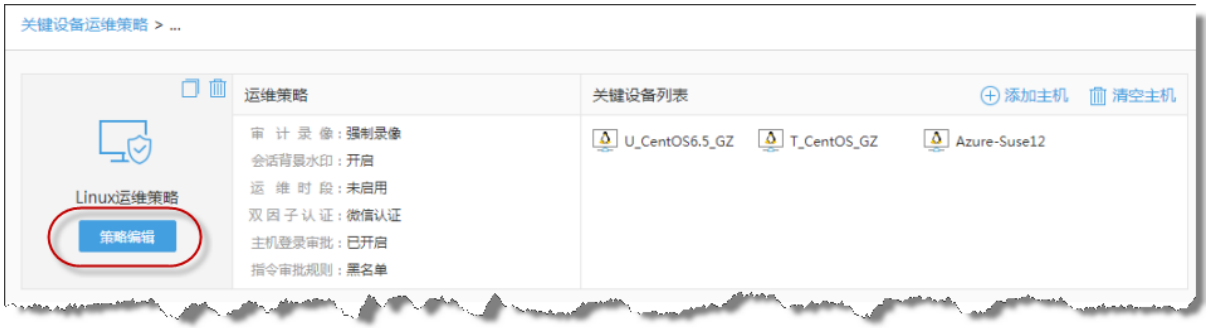


在添加主机对话框中选择要加入的主机，已经关联过运维策略的主机将不会再显示，选择完成后点击“添加”即可；



5.2.2 设置运维策略

运维策略是安全审计的核心功能，在您成功创建了一个运维策略之后，您需要对这个策略进行配置，让运维操作真正的按照您的业务要求规范起来。点击对应运维策略的“策略编辑”按钮，进入运维策略的配置界面。策略配置主要包含两部分：基础运维策略设置和审批策略设置；

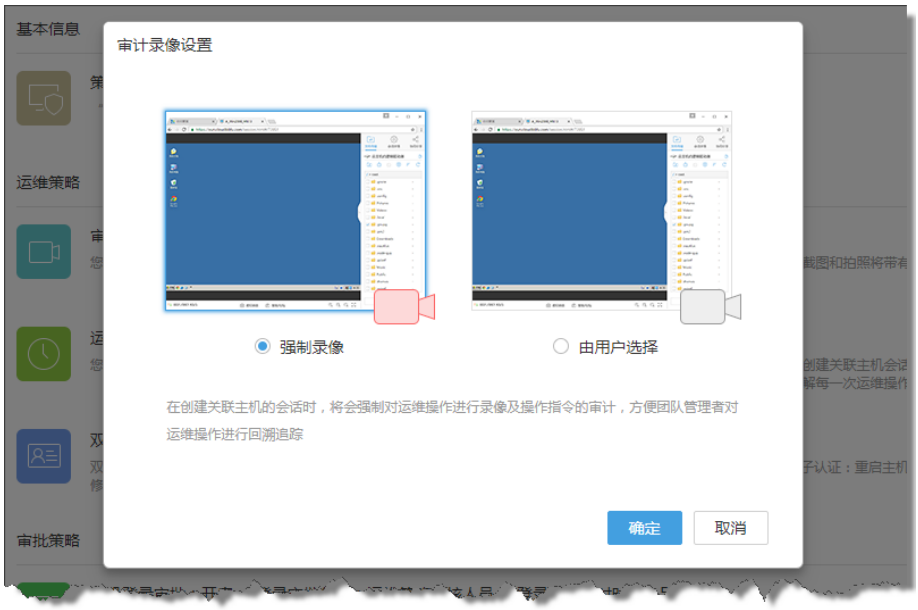


5.2.2.1 基础运维策略设置

我们可以看到，基础运维策略设置主要有以下几项内容，下面分别介绍每一个设置项：

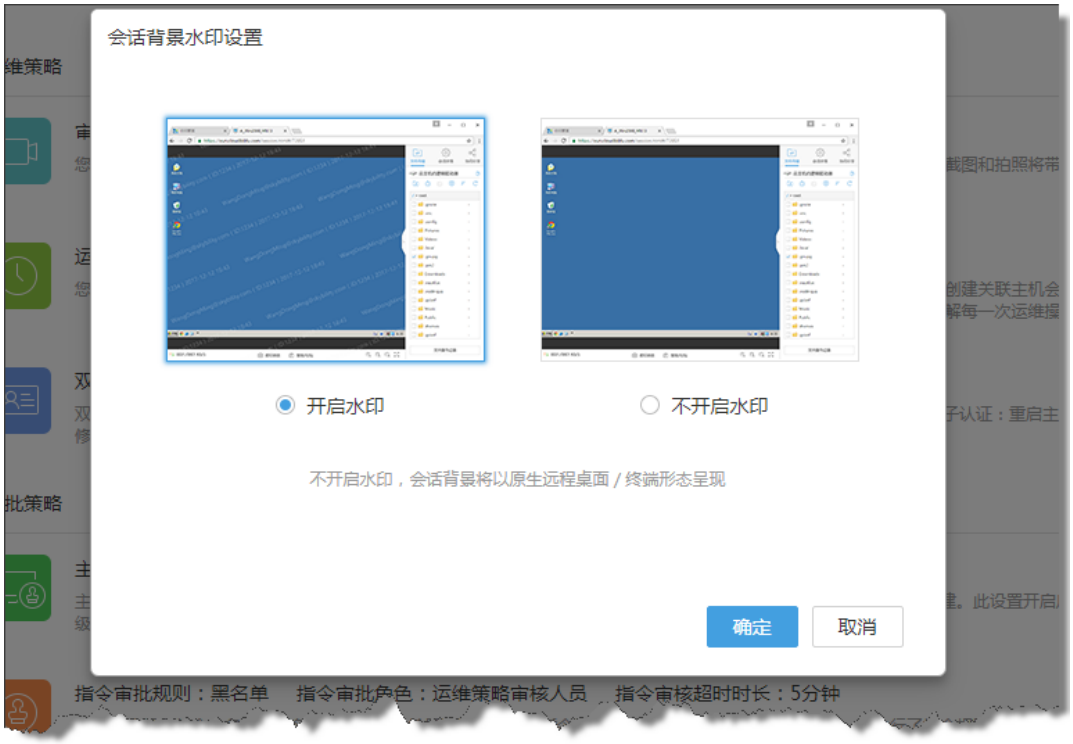
5.2.2.1.1 审计录像

访问运维策略里的关键设备时，是否强制进行审计录像。这里需要注意，在云账户中也存在该项设置，而一台主机访问时是否强制录像，同时受到它所在的云账户和运维策略的设置影响，只要其中有一个设置为“强制录像”，那么访问时即会进行强制录像；



5.2.2.1.2 会话背景水印

开启会话背景水印后，会话的背景将带有密密麻麻的会话创建者的用户昵称（不唯一、可修改）和用户 ID（唯一、不可修改）信息，适用于安全保密等级较高的主机，禁止团队成员擅自将主机上的任何数据外泄。当管理者发现了外界出现了相关主机的截图或对屏幕的拍照，可以通过图片上遗留的会话创建者信息查找泄露源头；

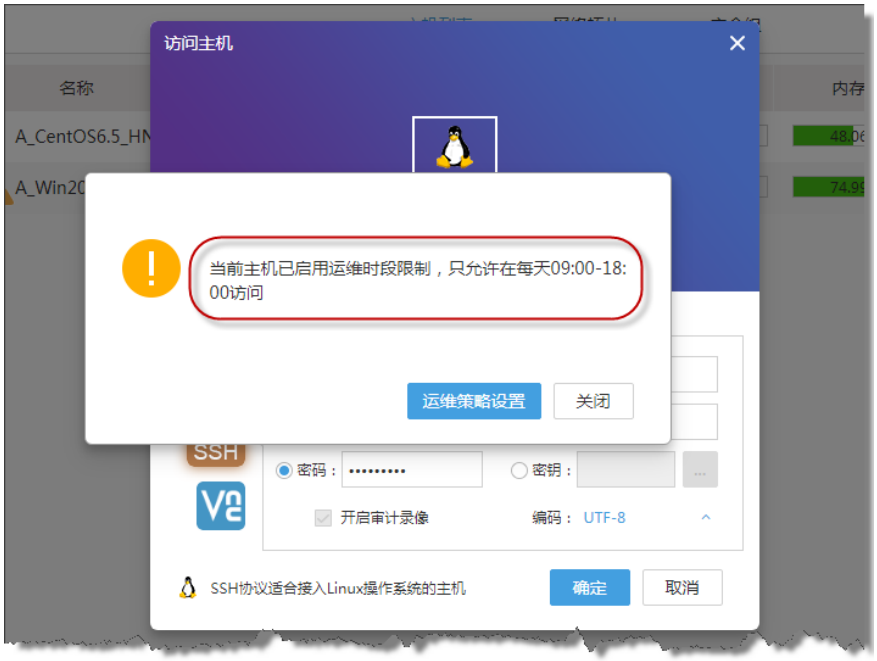


5.2.2.1.3 运维时段设置

在某些特定的场景下，我们需要对主机可访问的时间段进行控制，例如：只有在工作时段才允许登录行云管家访问主机，因此需要将运维时段设置为 09:00 到 18:00，那么可以按照以下指引进行设置；

1、编辑策略中的“运维时段”，打开“运维时段设置”窗口，设置运维时段为：指定以下时段 09 时 00 分至 18 时 00 分，点击“确定”保存；

2、在非运维时段访问主机，如果出现以下提示，则表示配置生效；



5.2.2.1.4 主机登录事由

如果您了解团队成员的每一次会话访问操作的原因和目的，您可以这是主机登录事由为“强制填写”；

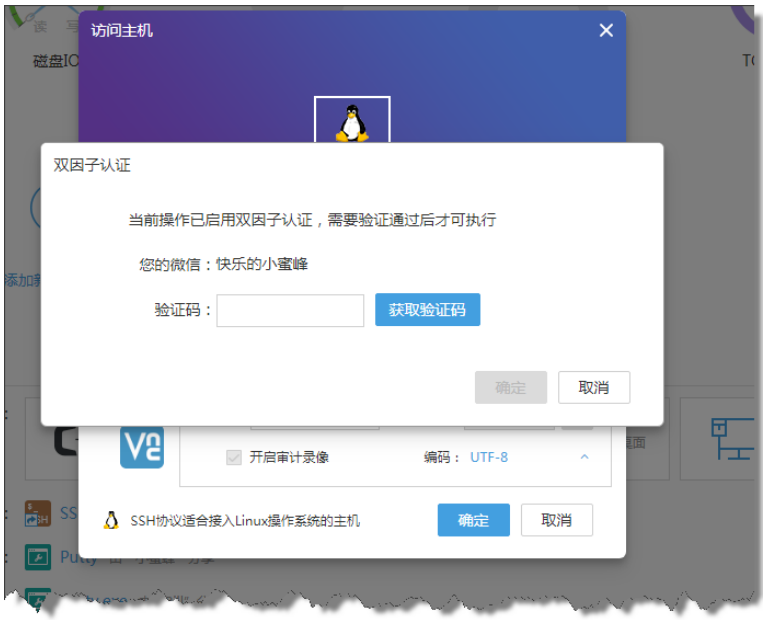
5.2.2.1.5 双因子认证

也叫多重身份认证，开启后，在执行重启主机、停止主机、修改主机操作系统密码、修改管理终端密码、创建主机会话、快照回滚、更换系统盘、初始化磁盘、卸载数据盘、挂载数据盘等操作时，会要求以微信或短信接收验证码的方式进行二次身份确认，确保访问者的身份合法性；

一旦某个运维策略设置了开启双因子认证，那么该策略中的所有关键设备在访问时，均会要求进行二次身份认证，目前支持微信和短信两种认证方式，这也意味着开启双因子认证后，需要团队成员在个人资料中绑定微信或手机；

点击“双因子认证”的编辑图标，打开“修改双因子认证”对话框，并选择对应的双因子策略；

访问关键设备时，将会弹出双因子认证对话框，需要输入“验证码”，点击“立即获取”；



您的微信或短信将收到一个四位数字验证码，将验证码回填至访问凭证中即可访问该设备；

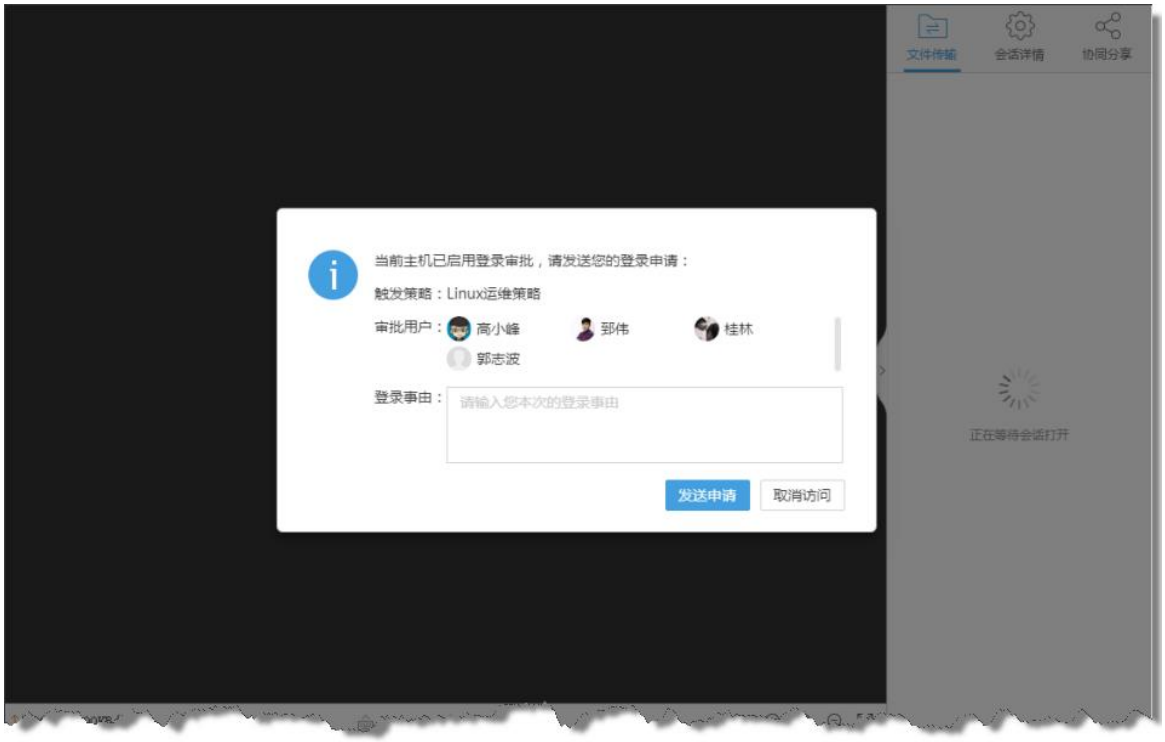
5.2.2.2 审批策略设置

目前，审批策略设置支持主机登录审批和指令审批规则两个设置项：

5.2.2.2.1 主机登录审批

主机登录审批开启后，团队成员在创建关联主机会话时，将需要获得相关角色成员的审批，审批通过后，会话才能被创建。此设置开启后一定程度上将影响运维效率，适用于安全级别较高的主机，默认情况下不开启。

团队成员在访问该运维策略关联的主机时，需要输入主机登录事由，等待审核人员的审核。



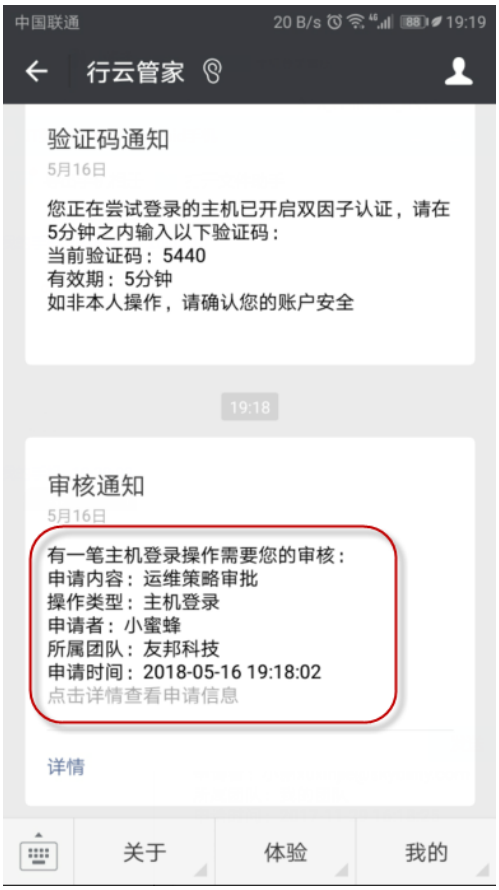
提示：审核角色中的成员在访问相关主机时，无需通过审核，可直接登录。

5.2.2.2.2 主机登录申请的审核

团队成员在发送了主机登录申请后，相关的审核角色成员有两种方式接收审核消息：

a）站内审核消息：审核角色成员将收到站内消息，点击查看后进入“安全审计/运维策略审批”，在“待审批”标签页里将列出当前所有待审批的申请，只需按照实际情况选择同意执行或拒绝执行即可。查询审批历史请切换到“已完成”标签页；

b）微信审核消息：审核角色成员账号如果绑定了微信，其微信将收到指令审批信息，可直接点击进入进行审批操作；



5.2.2.2.3 指令审批规则

您可以为当前运维策略开启指令审批，包含白名单和黑名单两种，如果是白名单，那么将只允许指令规则中的指令执行。如果是黑名单，团队成员在操作中执行的指令只要被敏感指令规则匹配，即执行相应的响应动作。

指令审计角色：敏感指令如果触发的是审核操作，那么将推送审核消息给指令审计角色成员，由他们审核通过后，敏感指令才能在主机上执行；

指令审核超时时长：敏感指令触发审核操作时，如果在超时时长内未处理，指令将因超时被取消执行。

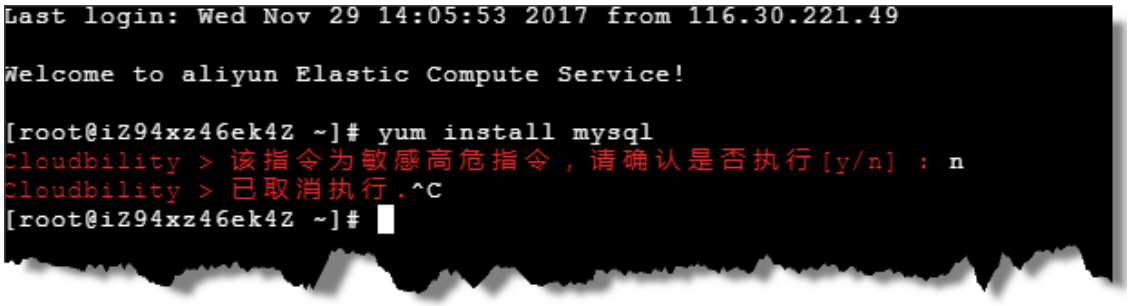
指令审批规则是安全审计的重要特性，可以有效避免团队成员进行违规操作。为了达到对敏感指令的拦截，我们首先需要有效的定义指令规则；

默认情况下，指令规则列表为空，用户可按照业务情况，添加相应的规则；

在定义敏感指令时，还需要指定指令匹配规则及相应的响应动作，只要在关键设备中执行的指令被匹配，既会触发指令审计策略，按照用户设定的响应动作进行处理；

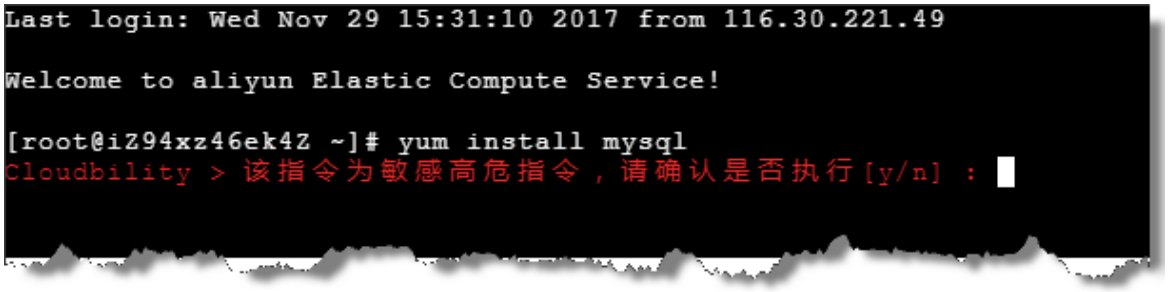
目前支持以下三种指令匹配方式：

完全匹配：适合匹配某条指令的全部操作，该指令所有形式的执行都会被匹配，如指令规则是 yum，使用完全匹配规则，那么用户输入 yum、yum install、yum remove 等相关指令都会被匹配；



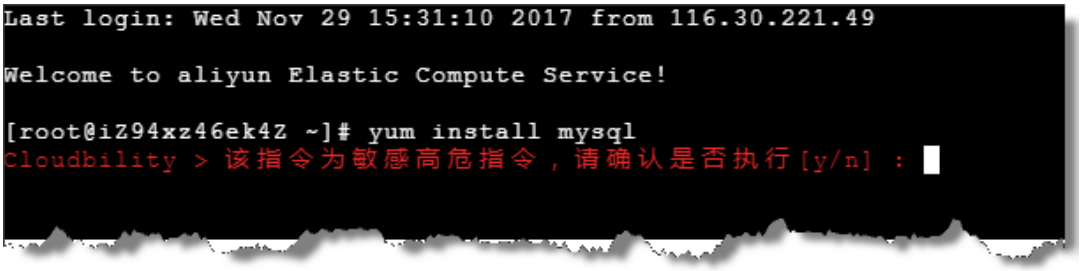
正则表达式：支持正则表达式模糊匹配，适合匹配某个指令的部分参数，如只需要匹配 yum 安装和卸载操作，指令规则为 yum (install|remove)，那么用户输入 yum search 不会被匹配，但是输入 yum install、yum remove 会被匹配；

通配符：支持通配符模糊匹配，使用场景和正则表达式类似，但语法有些许差别，如同样匹配 yum 安装和卸载操作，指令规则为 yum {install,remove}；



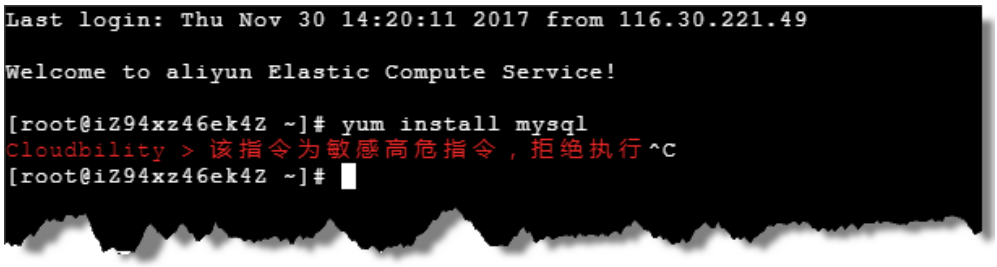
目前支持以下四种响应动作：

指令提醒：对于团队管理者希望团队成员谨慎执行却时效性较高的一般敏感指令，可设置为“指令提醒”，在执行时，需要由成员自行确认后执行；



指令审核：对于团队管理者认为会带来一定风险的敏感指令，可以设置为“指令审核”，这类指令执行时，会被临时阻塞，待指令审核后才能执行；

指令阻断：对于团队管理者认为风险较高不希望成员执行的敏感指令，会被直接阻断，不允许执行；



中断会话：对于团队管理者认为会带来极大危险性的的恶意指令，建议设置为“中断会话”。

5.2.2.2.4 敏感指令审核

团队成员在触发了指令审核响应动作时，相关的审核角色成员有两种方式接收审核消息：

a）站内审核消息：审核角色成员将收到站内消息，点击查看后进入“安全审计/运维策略审批”，在“待审批”标签页里将列出当前所有待审批的敏感指令申请，只需按照实际情况选择同意执行或拒绝执行即可。查询审批历史请切换到“已完成”标签页；

b）微信审核消息：审核角色成员账号如果绑定了微信，其微信将收到指令审批信息，可直接点击进入进行审批操作；

注意:团队中的指令审批角色可能有多个成员，每个成员均会收到审批消息，审批操作以时间为顺序，一个申请只能被审批一次，其他成员将不再允许对该笔申请进行审批。

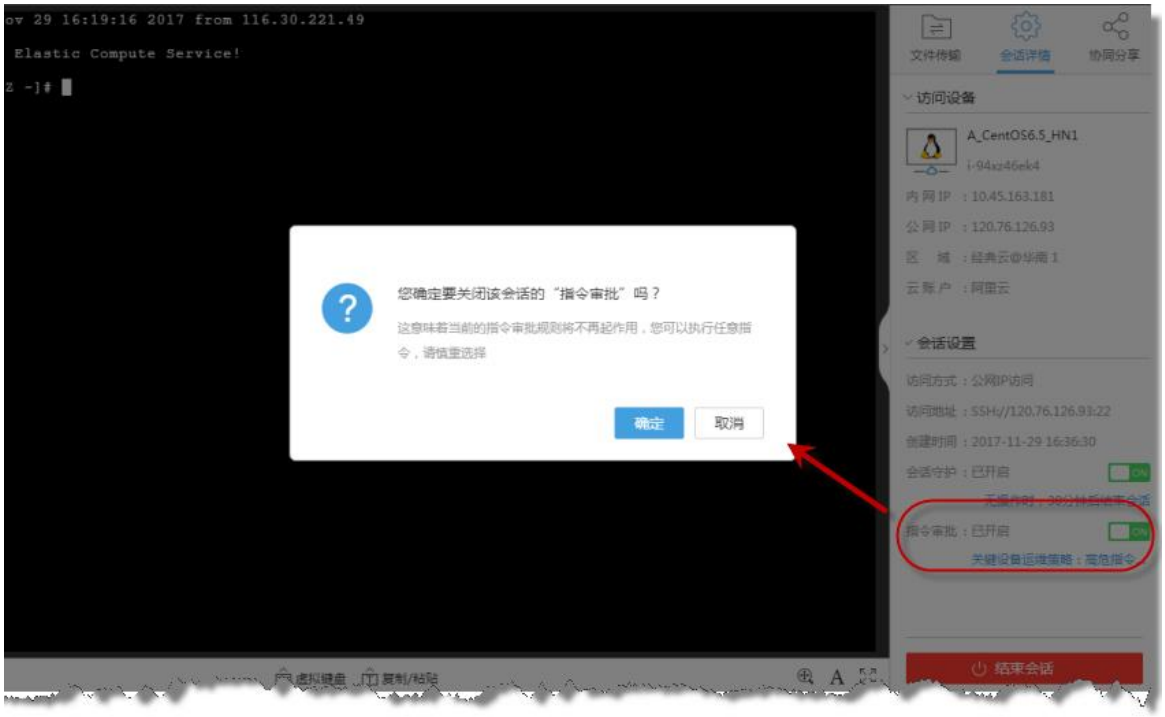
5.2.2.2.5 特殊场景下如何绕开指令黑名单拦截

指令黑名单一旦设置，所有团队成员执行的指令被认定为敏感指令时，均会执行相应的响应动作。但在某些特殊场景下，如果需要给个别成员较高的权限，在操作时不受指令黑名单的影响，可以为其赋予临时禁用指令审批规则的权限；

进入“团队/权限管理/角色管理”，为这类成员创建一个专门的角色，如“禁用指令审批角色”，将相应成员加入到角色中；

进入“团队/权限管理/功能授权”，找到“安全审计/禁用指令审批规则”，将上一步创建的角色“禁用指令审批角色”加入到该功能权限中；

该角色中的成员在访问会话时，在会话详情中，可以看到“指令审批”，只要当前主机属于关键设备且开启了指令黑白名单，均可将指令审批设置为关闭，这样在当前会话中，所执行的指令将不受运维策略的影响。



5.2.2.3 运维策略指令规则设置参考

行云管家在会话中对敏感指令的拦截，并非是匹配用户输入的完整内容，而是对用户输入的内容进行分析，找到这条内容的核心指令，再将这条指令与运维策略中设置的指令规则进行匹配。因此在设定指令规则时，只需填写指令本身即可，无需考虑指令所在目录等元素，下面列举几个指令规则设置场景；

5.2.2.3.1 彻底拒绝某个指令的执行

如果需要彻底阻断某个指令，建议使用指令+完全匹配的方式，不论用户在会话中是否带有参数，都将被拦截。例如，为了避免有人通过 shutdown 重启服务器，管理员可以按以下规则进行设置：

- ✓ 指令规则：shutdown；
- ✓ 匹配规则：完全匹配；

那么当用户尝试在会话中以 shutdown、shutdown -r now、./shutdown.sh 等任何形式执行，此条命令会被自动阻断；

5.2.2.3.2 拒绝某个指令的部分参数

如果仅需要拦截某个指令部分参数，例如，不允许通过 yum 来安装和卸载，但允许执行 yum 其它操作，可以按以下规则进行设置：

- ✓ 指令规则：yum (install|remove)；
- ✓ 匹配规则：正则表达式；

那么当用户尝试在会话中以 yum install 和 yum remove 时，此条命令会被自动阻断，但用户执行 yum search 时将被允许；

5.2.2.3.3 阻断对某个文件的操作

要阻断对某个特定文件的操作，例如，不允许删除 root 目录下的 aaa.txt，文件，可以按以下规则进行设置：

- ✓ 指令规则：rm\s.*/root/aaa\.txt；
- ✓ 匹配规则：正则表达式；

那么当用户尝试在会话中以 rm /root/aaa.txt 时，此条命令会被自动阻断，但用户执行 rm /aaa.txt 时将被允许；

第6章 安全（运维）审计

6.1 什么是运维审计日志

运维安全是 IT 管理中不可或缺的一环，行云管家在安全层面除了通过事前权限授权、事中敏感指令拦截外，还为用户提供了事后运维审计的特性，用户在行云管家中所进行的运维操作均会以日志的形式记录下来。目前支持审计的运维操作有：主机访问（会话）、批量作业、任务编排三种，此类操作执行后均会产生审计日志，团队管理者可通过日志对成员的运维操作进行审计，以此来达到安全、可控、合规的团队协作目的；

审计日志分为我的审计日志和团队审计日志两个维度，每个团队成员均可查看自己创建的运维操所产生的审计日志，但是从团队管理的角度考虑，查看团队运维审计日志需要获得相应的权限，相关权限是位于“安全审计”中的三项：团队会话审计、团队作业审计、团队任务审计，只要拥有相应的权限，便可查看团队成员的运维审计日志，下面分别从三种运维操作的角度来介绍如何查看审计日志。

6.2 会话审计

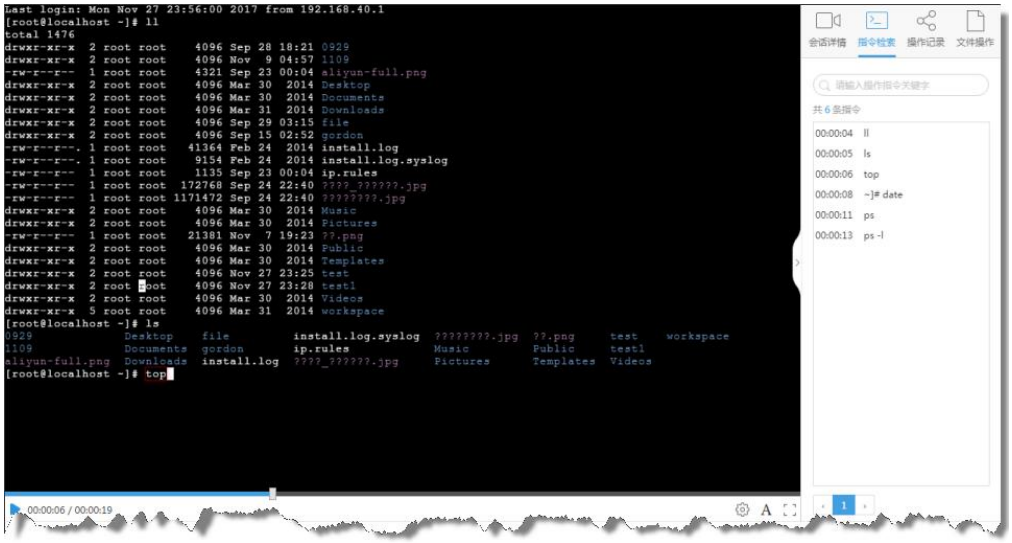
进入“安全审计”栏目，选择“团队审计日志/会话日志”，如果没有团队审计权限，则只能查看“我的审计日志”；

运维审计包含“会话记录”、“指令查询”和“文件操作”三个标签页；

“会话审计”从会话的维度展示最近的主机访问日志，点击该条记录，展开日志详情，用户可以点击录像截图查看运维审计录像；

“指令查询”为用户提供了一个按照指令来检索操作行为的入口，用户可以输入相关指令，并配合其它搜索条件，准确的查找出相关操作。在结果中点击“指令定位”将打开审计录像，并自动定位到该指令产生的时间点；

在审计录像中，“指令检索”将展示当前会话产生的所有指令，用户可以根据指令关键字、指令类型进行检索，并可快速的将录像定位到相应的时间点；



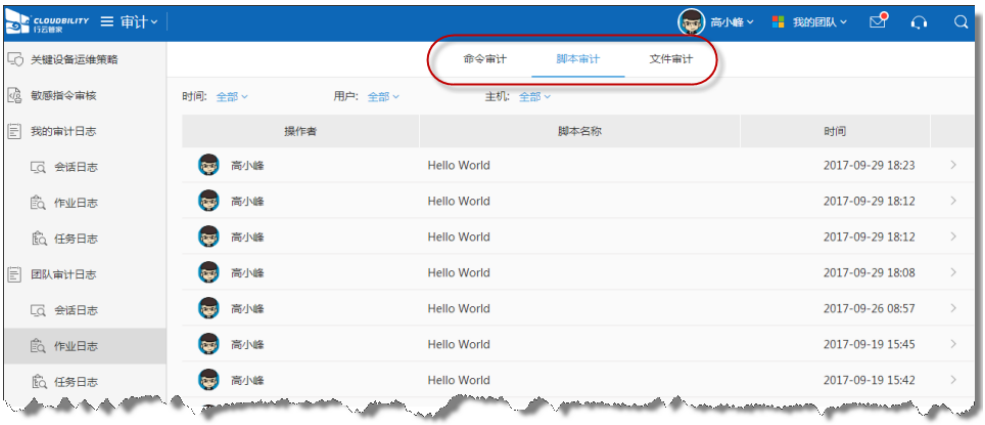
“文件操作”记录了用户在会话的文件操作面板中对文件所做的全部操作：新建文件夹、上传文件、下载文件、文件重命名、移动文件、复制文件、删除文件共七种类型；

如要查询用户通过命令执行的文件操作，请通过会话记录或指令查询进行检索；

6.3 作业审计

作业中心里的操作都是直接作用于主机上的操作，从运维管控的角度上考虑，所有在行云管家上执行的作业，都会进行审计记录，以此来达到安全、可控、合规的团队协作目的；

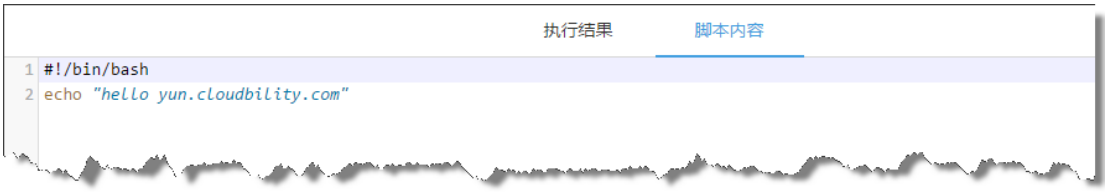
进入“安全审计”栏目，选择“团队审计日志/作业日志”，里面分别提供了“命令执行”、“脚本执行”、“文件分发”、“文件采集”。我们以“脚本审计”为例，可以看到所有执行过的脚本执行记录，也可以根据执行时间、操作者、执行的主机等进行过滤；



对每一条脚本执行记录，可以展开了解脚本执行的细节信息，当需要查看每一台主机的执行结果时，可以点击“查看详情”链接，打开脚本执行审计详情页面；

在脚本执行审计详情页面中可以查看每台主机的脚本执行状态和结果；

也可以查看脚本执行时的脚本内容，避免脚本修改后无法追溯以前的脚本内容。



6.4 任务审计

在任务编排中，每个用户只能看到自己创建的运维任务，为了便于团队管理，我们提供了任务审计功能，团队所有执行过的任务都会在任务审计中展示；

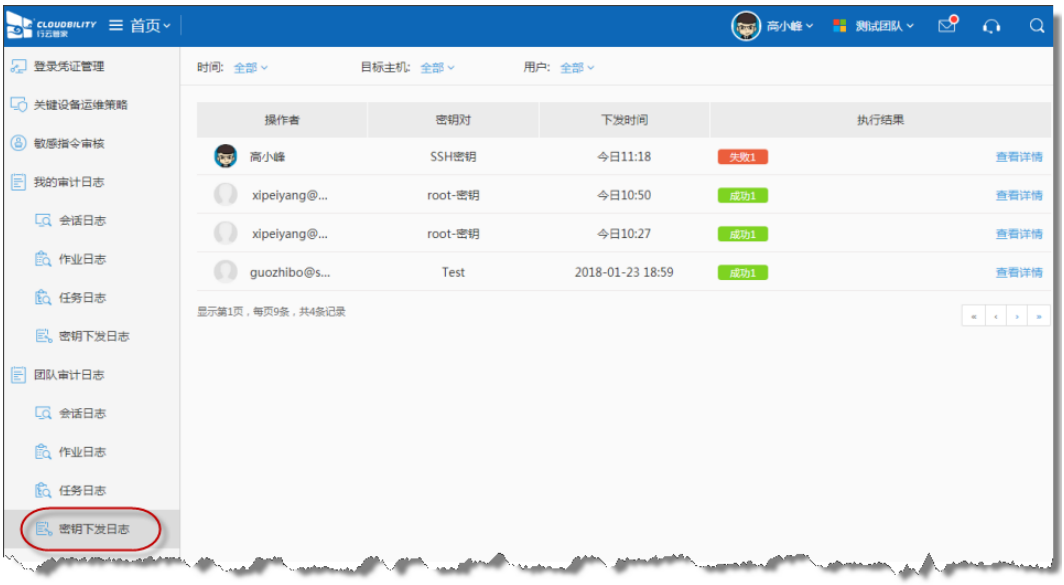
进入“安全审计”栏目，选择“团队审计日志/任务日志”，可以看到所有执行过的任务执行记录，也可以根据执行时间、操作者等进行过滤；

点击查看任意一笔记录，可以打开该笔任务的执行详情，便于管理员进行审计；

6.5 SSH 密钥对下发审计

在“安全审计/登录凭证管理/密钥对管理”中，所进行的每一笔 SSH 密钥对下发操作，都将形成审计日志；

进入“安全审计”栏目，选择“团队审计日志/密钥下发日志”，支持执行时间、目标主机等进行过滤；



点击查看任意一笔记录，可以打开该笔下发操作的执行详情，便于管理员进行审计；