

安恒云使用手册

1. 概述

1.1 产品简介

安恒云是集多云管理和多云安全于一体的一站式平台级产品，旨在为用户打造一个安全、平等的多云管理和多云安全管理平台。安恒云可连接国内外主流公有云、私有云、传统 IDC 数据中心，帮助用户最优惠选云、便捷上云、安全用云、统一管云等。安恒云拥有丰富的多云管理能力和完善的云上安全能力，可以满足不同用户个性化的多云管理和多云安全需求。

1.2 主要业务流程

用户登录安恒云进行相关操作时，首先需要选择团队所在的工作空间。如果当前用户只加入了一个团队，系统将引导用户直接进入团队的工作空间。若当前用户加入了多个团队，则需要用户从团队列表选择一个团队进入。

进入之后可执行与团队相关操作，包括查看团队信息、管理团队成员权限/角色、查看操作日志、查看团队订单。

2. 多云管理

在多云场景下，不同云服务商的管理平台业务逻辑都有较大差异，且云服务商自身安全能力基本只能服务于其自身的云，导致用户被迫选择不同云服务商的安全能力，难以实现统一的安全分析、安全策略、安全运营等。

安恒云的多云管理功能允许用户同时管理来自于多家公有云厂商的资源（包括云主机、对象存储、CDN 等资源）以及 VMware、openstack 等常见私有云环境中的资源。通过多云管理的跨云管理能力，实现跨云厂商的资源调配，提升云资源的利用率，降低企业成本。

3.1 资源池

安恒云中的资源池指的是通过其云管功能所管理的 VMware vCenter Server (简称“vCenter”)以及 OpenStack 虚拟化环境中被管理资源的逻辑抽象。安恒云通过 API 接口与 vCenter 和 OpenStack 对接，实现与管理公有云资源同样方式管理上述虚拟化环境中的资源，即通过将资源池接入到安恒云中完成对云主机或虚拟机的全生命周期管理。

目前资源池管理支持以下虚拟化环境版本：

- ◆ vCenter V5.5、V6.0、V6.5 和 V6.7 版本
- ◆ 支持 keystone V3 版本身份认证的 OpenStack，以及 P、Q、R、S、T 版本

3.1.1 导入 VMware 资源池

在对云主机或虚拟机进行全生命周期管理之前，需要先导入资源池。

步骤1. 在菜单栏选择“多云管理 资源池”进入资源池页面，然后点击<添加资源池>，弹出添加资源池向导。

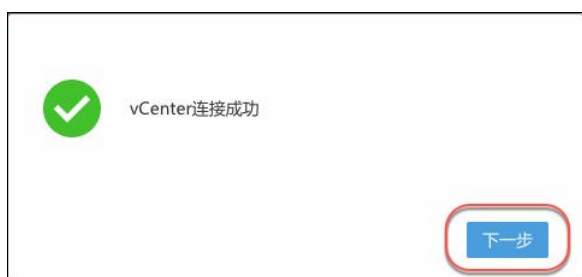
步骤2. 选择 VMware 资源池类型为 VMware，点击<下一步>。



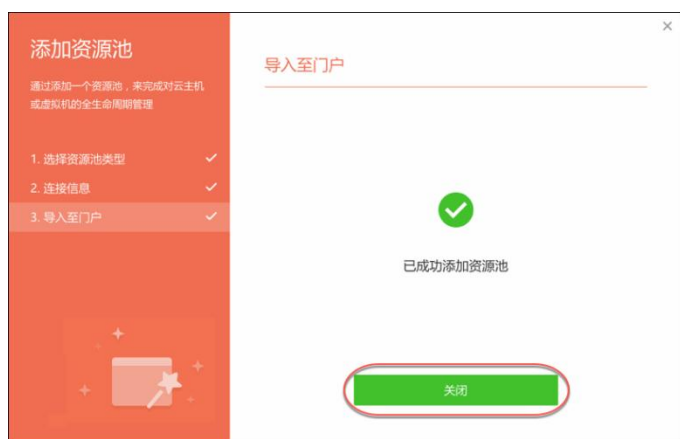
步骤3. 编辑连接信息。支持 vCenter 的 V5.5、V6.0、V6.5 以及 V6.7 版本，域名请填写 IP 或域名（不需要带 HTTP 格式）。点击<下一步>。



步骤4. 提示连接成功，点击<下一步>。如果连接不成功，请检查域名格式以及用户名和密码是否正确。



步骤5. 指定资源池名称，点击<确定>，即可添加资源池。



步骤6. 点击<关闭>，返回资源池页面。

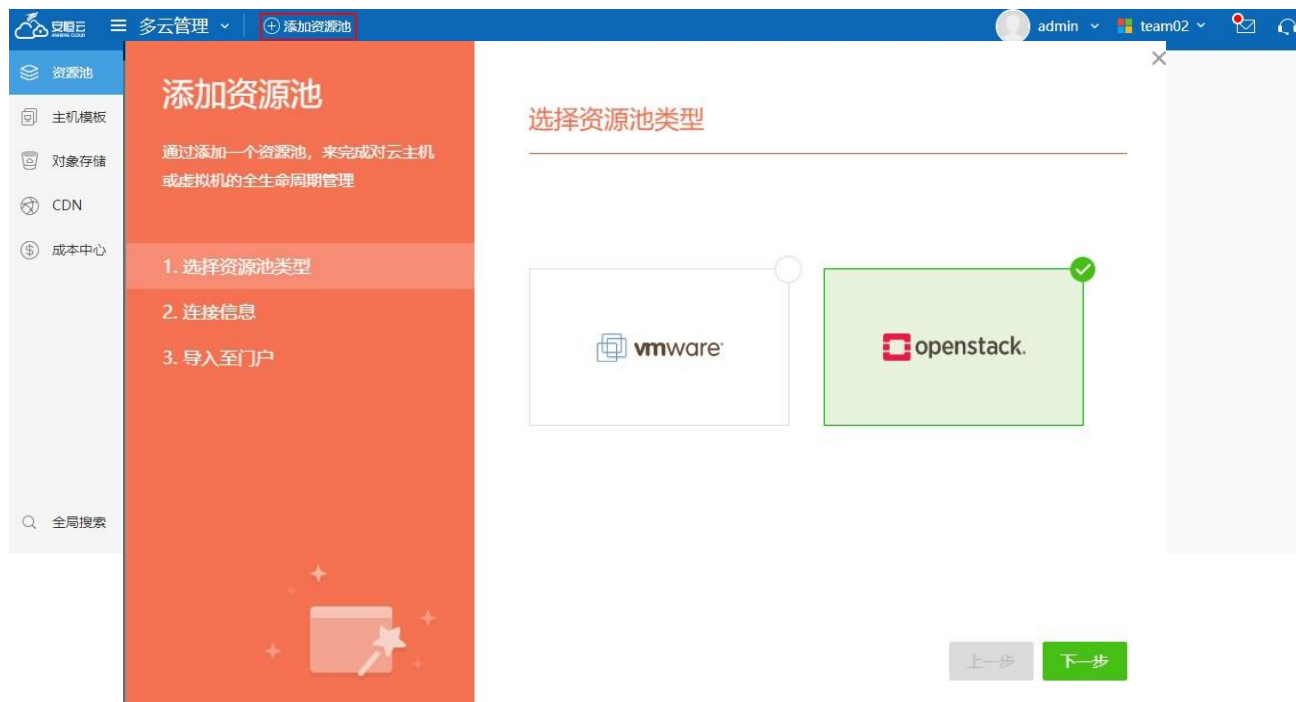
导入资源池后，您可以继续导入资源池主机进行主机访问等操作。更多信息请参考[导入资源池主机](#)。

3.1.2 导入 OpenStack 资源池

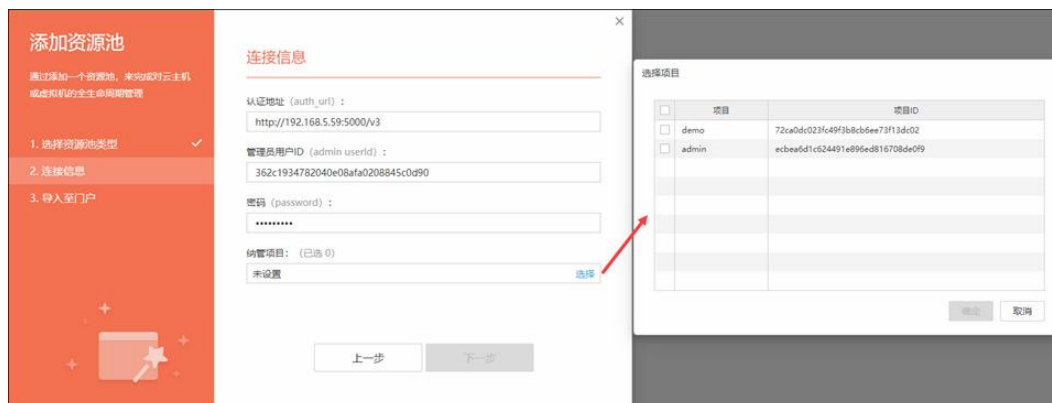
在对云主机或虚拟机进行全生命周期管理之前，需要先导入资源池。

步骤1. 在安恒云首页菜单栏选择“多云管理 资源池”进入资源池页面，然后点击<添加资源池>，弹出添加资源池向导。

步骤2. 选择 OpenStack 资源池类型为 OpenStack，点击<下一步>。



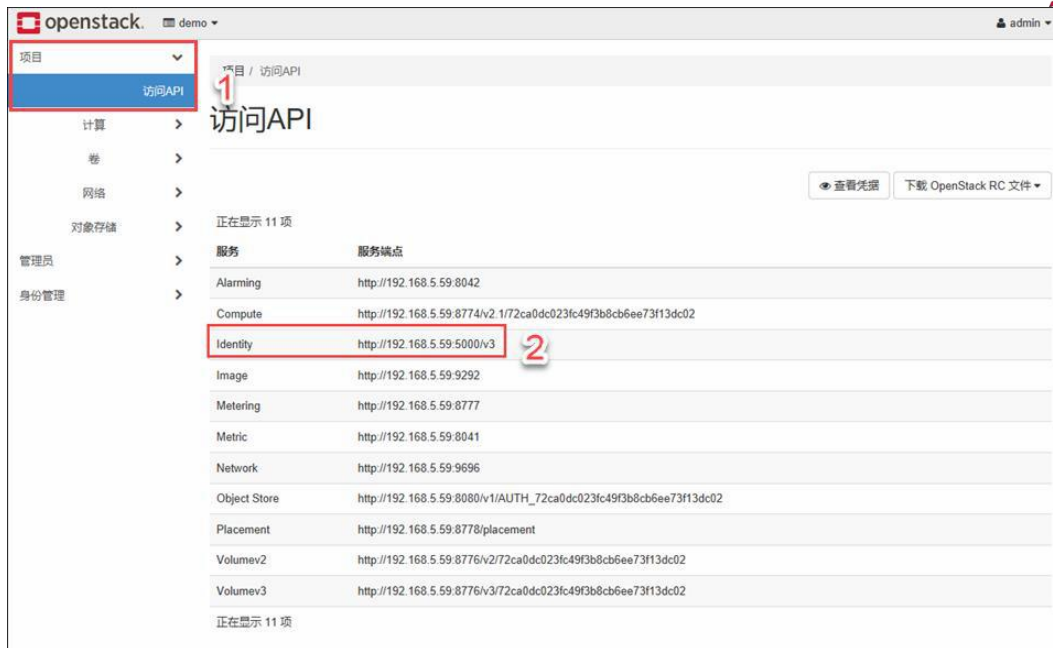
步骤3. 编辑连接信息，点击<下一步>。



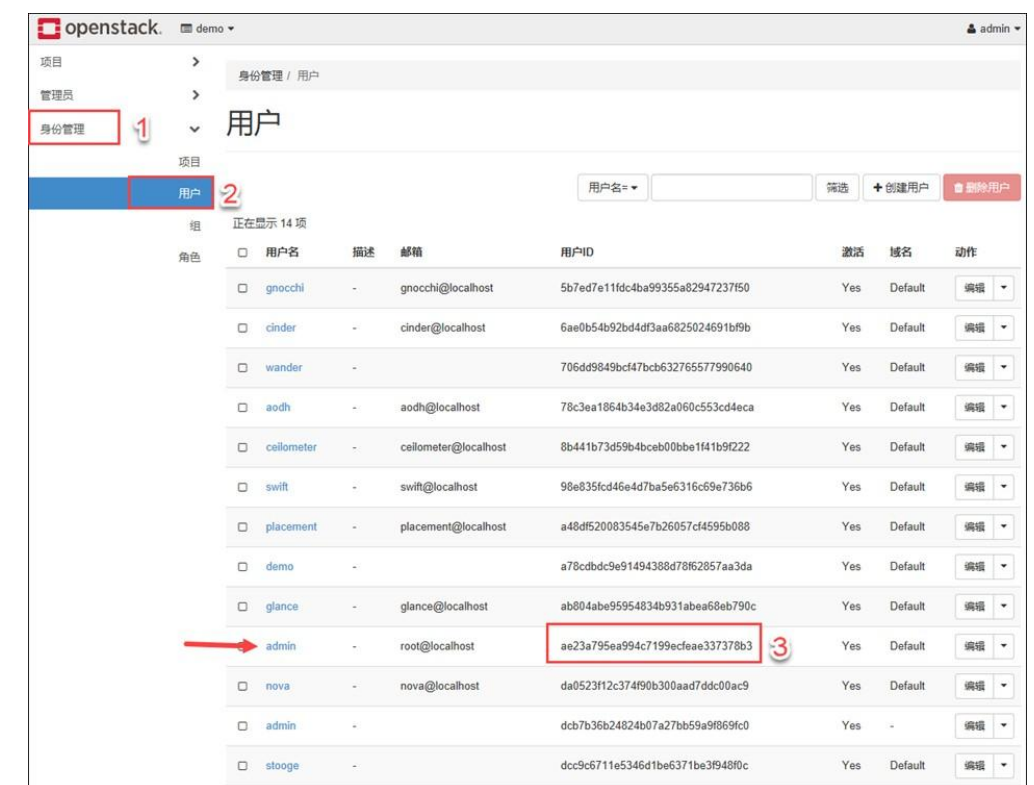
用户需登录到OpenStack 界面获取上述连接信息。

认证地址：可通过以下两种方式找到“认证地址”。**方法 1:** 登录 OpenStack 控制台，在菜单栏选择“项目 访问 API”，在该页面点击<查看凭据>，拷贝“认证URL”并填入到对应的“认证地址”即可。

方法 2: 在菜单栏选择“项目 访问 API”，找到“Identity”服务，拷贝“服务端点”并填入到对应的“认证地址”即可。



- ◆ 管理员用户 ID: 在菜单栏选择“身份管理 用户”，找到“admin”用户，将其对应的“用户名 ID”填入到对应的“管理员用户 ID”文本框中即可。



请勿填写用户名。

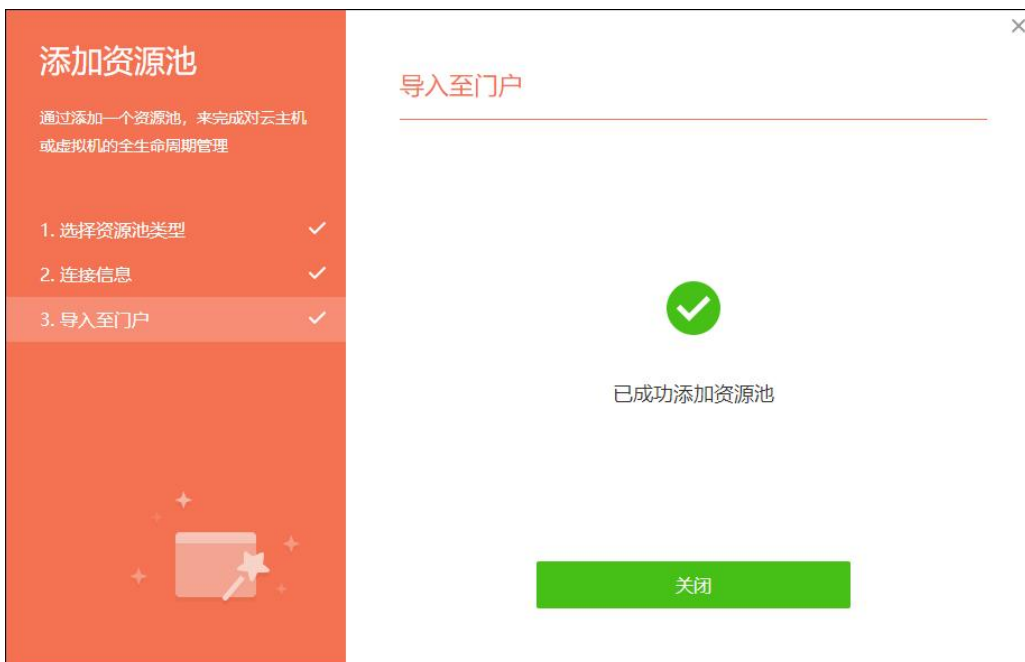
- ◆ 纳管项目：前三项填写完后，可继续选择“纳管项目”。选择希望导入的项目，即 OpenStack 中的“项目”，如下图所示。



步骤4. 指定资源池名称，点击<确定>。



步骤5. 点击<关闭>完成资源池导入，返回资源池页面。



导入资源池后，您可以继续导入资源池主机进行主机访问等操作。更多信息请参考[导入资源池主机](#)。

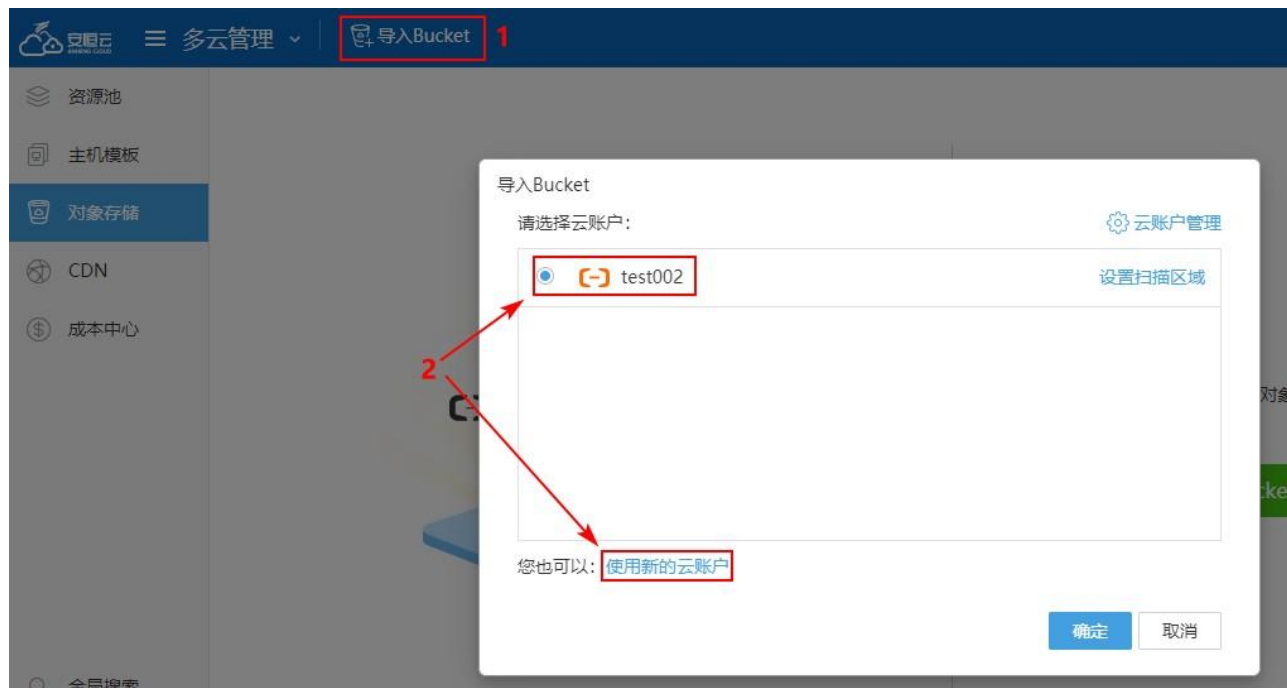
3.2 导入对象存储资源

对象存储是由云厂商提供的云存储服务，用户可通过调用 API 的方式，在任何应用、任何时间、任何地点上传和下载数据，实现数据的管理和处理。目前各大云服务厂商均有此类产品，例如阿里云的OSS、腾讯云COS、亚马逊S3等。

对象存储服务的基本存储空间是 Bucket，它是存储对象的容器，所有的对象都必须隶属于某个 Bucket。您可以设置和修改 Bucket 属性用来控制地域、访问权限、生命周期等。这些属性设置直接作用于该 Bucket 内所有对象，因此可以通过创建不同的Bucket 来实现不同的管理功能。

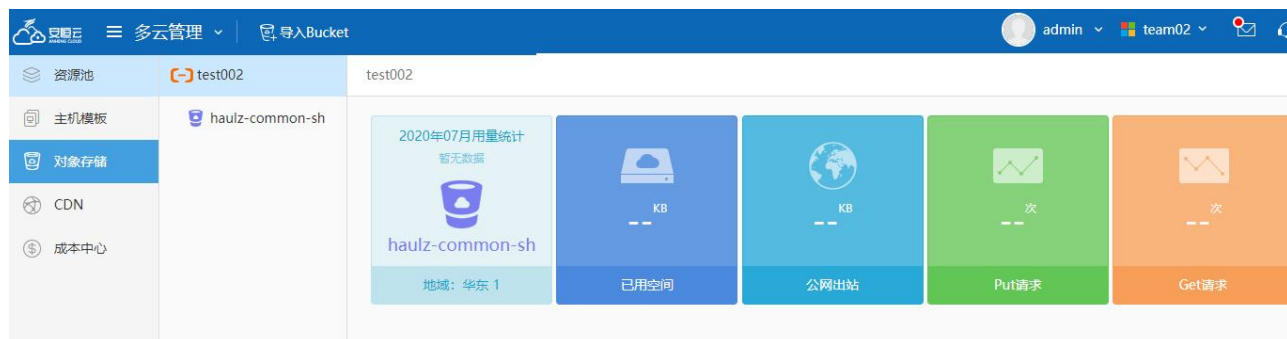
导入Bucket 时需要拥有云账户，该云账户可与云主机共用同一云账户，也可新建另一云账户。创建过程请参考[导入公有云主机](#)。目前只支持阿里云、腾讯云、AWS 的对象存储。

步骤1. 在安恒云主界面选择“多云管理 对象存储”，点击<导入 Bucket>开始导入。



步骤2. 导入成功后，当用户在对象存储页面左侧树结构中选择某个云账户节点时，右侧将显示该云账户中所管理的 Bucket 当月用量统计，统计指标包括：已用空间、公网出站流量、请求数(Put 及 Get)。并可对 object 进行管理。

3.3 导入CDN 资源



CDN 是安恒云支持的一种重要云资源，在菜单栏选择“多云管理 CDN”，点击导入 CDN 并选择已有的云账号即可从该账号导入 CND 资源。有关云账号的更多信息，请参考[导入公有云主机](#)。目前支持导入阿里云以及腾讯云 CDN。

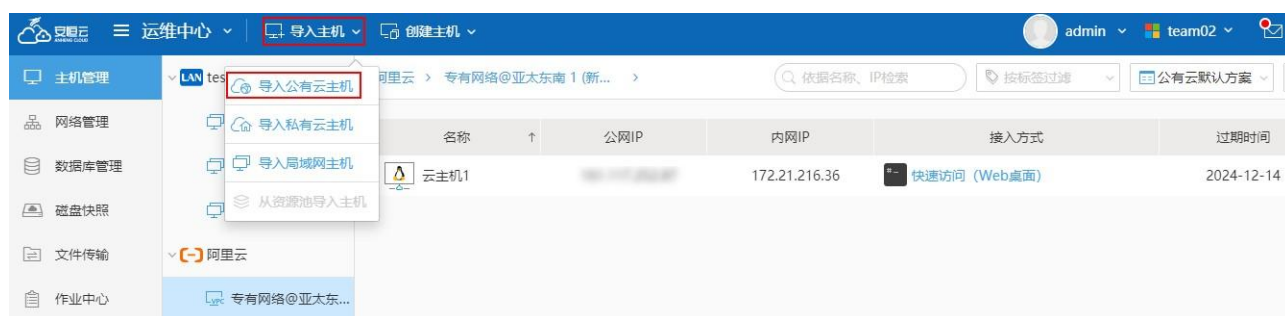
3. 导入主机与数据库

在安恒云的运维中心可对云主机和数据库等资源统一进行管理。为方便对云主机、对象存储、CDN 等云资源的容器及业务进行隔离，安恒云中引入了“云账号”概念。例如，用户A 在阿里云有一个账号，里面购买了云主机、CDN 等产品，则这个账号体现在安恒云中就是一个云账户；同时用户 A 可能在腾讯云中购买了云产品，且也将腾讯云的账户也导入到安恒云中。这样用户 A 在安恒云上便拥有了两个云账户，分别管理其在阿里云和腾讯云上的云资源。

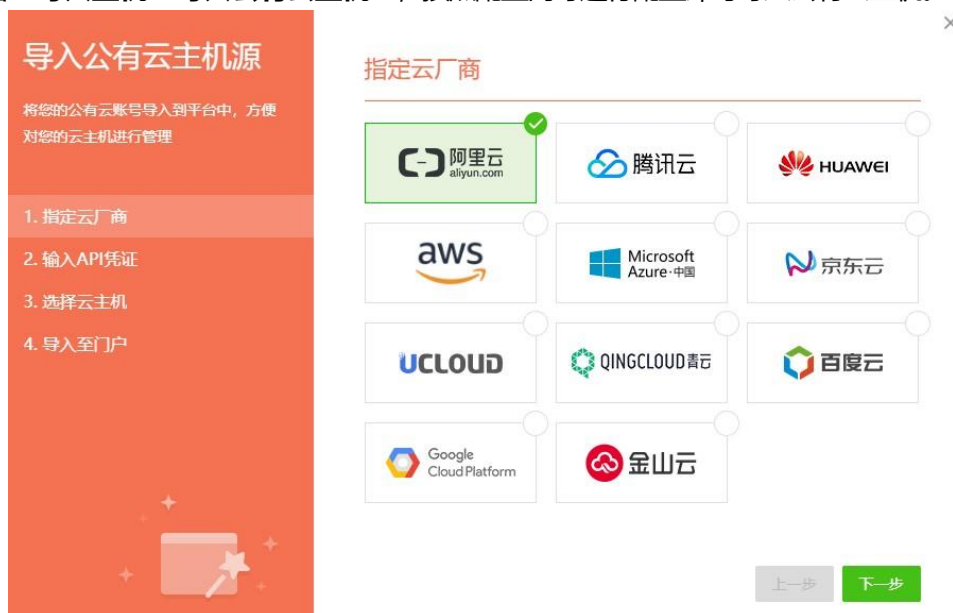
4.1 导入公有云主机

安恒云支持阿里云、腾讯云、华为云、AWS、Azure（仅中国区）、京东云、Ucloud、青云、百度云、谷歌云、金山云等云厂商。用户的云主机如果属于以上云厂商，可通过云厂商API 方式导入到安恒云中进行管理；如果非以上公有云主机，可以通过导入局域网主机的方式导入到安恒云中进行管理。

步骤1. 在菜单栏选择“**运维中心 主机管理**”进入主机管理页面。



步骤2. 点击“**导入主机 导入公有云主机**”，按照配置向导进行配置即可导入公有云主机。



4.2 导入私有云主机

安恒云支持通过 OpenStack 和 Zstack 私有云厂商的云主机导入。后续将支持更多的私有云厂商，其他暂未支持的私有云主机，可以通过导入局域网主机的方式导入到安恒云中。

步骤1. 在主机管理页面点击“导入主机 导入私有云主机”。



步骤2. 按照配置向导配置相关信息，导入 OpenStack 或 Zstack 私有云主机。



4.3 导入局域网主机

安恒云是一个云计算管理平台，目前安恒云已经通过 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，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，安恒云为用户提供了局域网主机的解决方案。安恒云中的局域网主机，并非传统意义上的“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。

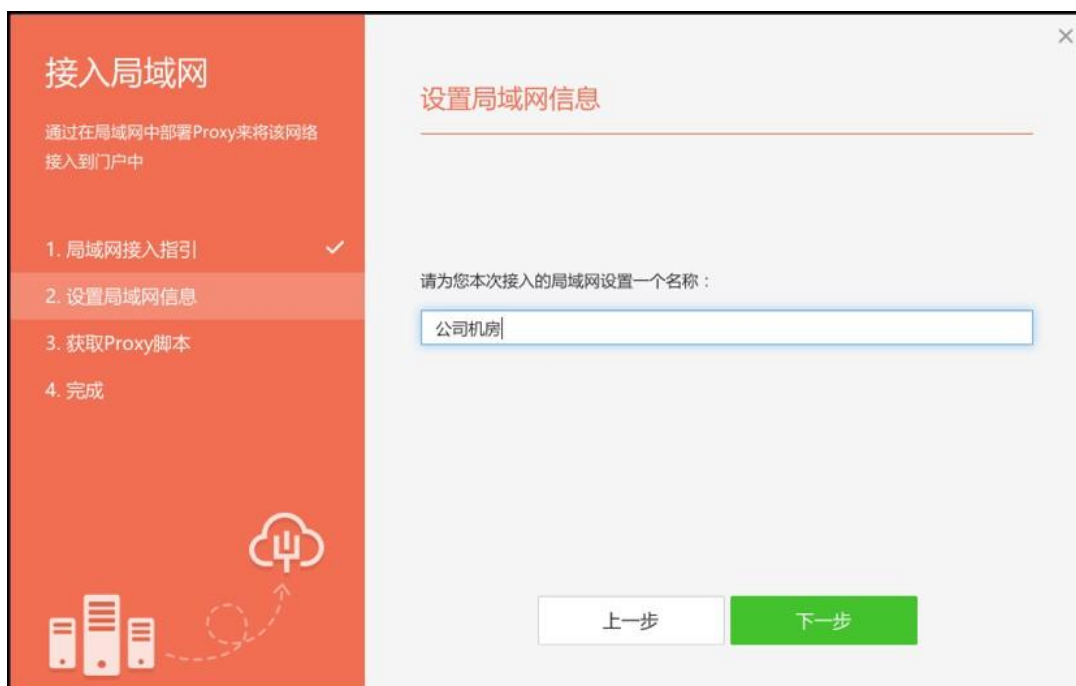
步骤1. 在菜单栏中选择“运维中心 主机管理”进入主机管理页面，点击“导入主机 导入局域网主机”



步骤2. 查看局域网接入指引，点击<下一步>。



步骤3. 设置局域网名称，点击<下一步>。

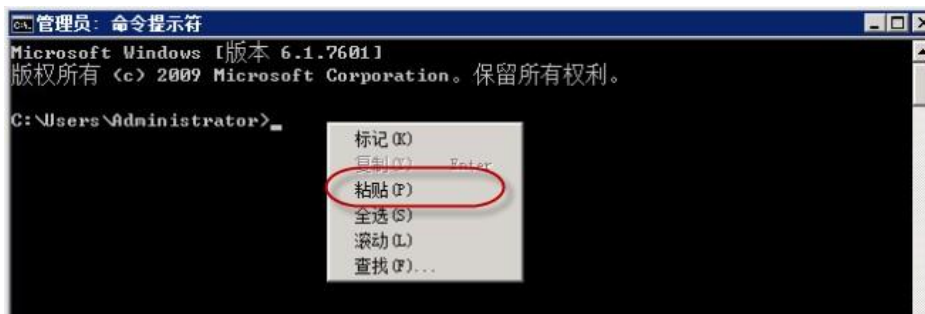


步骤4. Proxy 负责局域网与安恒云之间的通讯，选择一台主机作为宿主机，无需逐台安装，请根据您的Proxy 宿主机操作系统选择脚本类型，获得相应的 Proxy 的安装脚本，点击<复制脚本内容>。



步骤5. 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)。

步骤6. 无论您是否安装了 Proxy，都可以直接点击<下一步>，直接关闭向导，但要想继续完



成导入局域网主机的功能，必须确保 Proxy 处于正常工作状态。



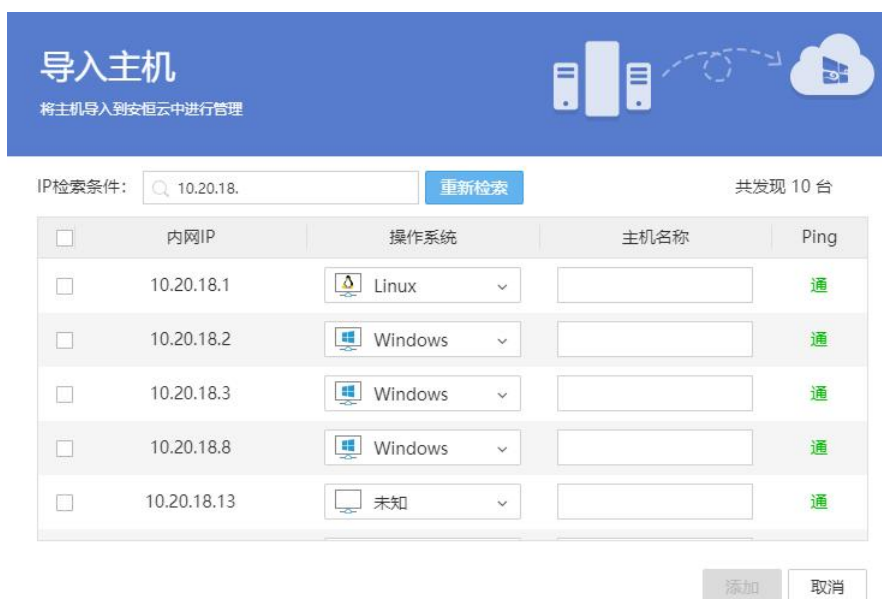
步骤7. 点击“**导入主机**”，选择之前创建的局域网，点击<确定>。



步骤8. 局域网主机有三种导入方式：手工输入主机 IP、IP 网段自动扫描、模板文件批量导入，这里以选择“IP 网段自动扫描”为例。



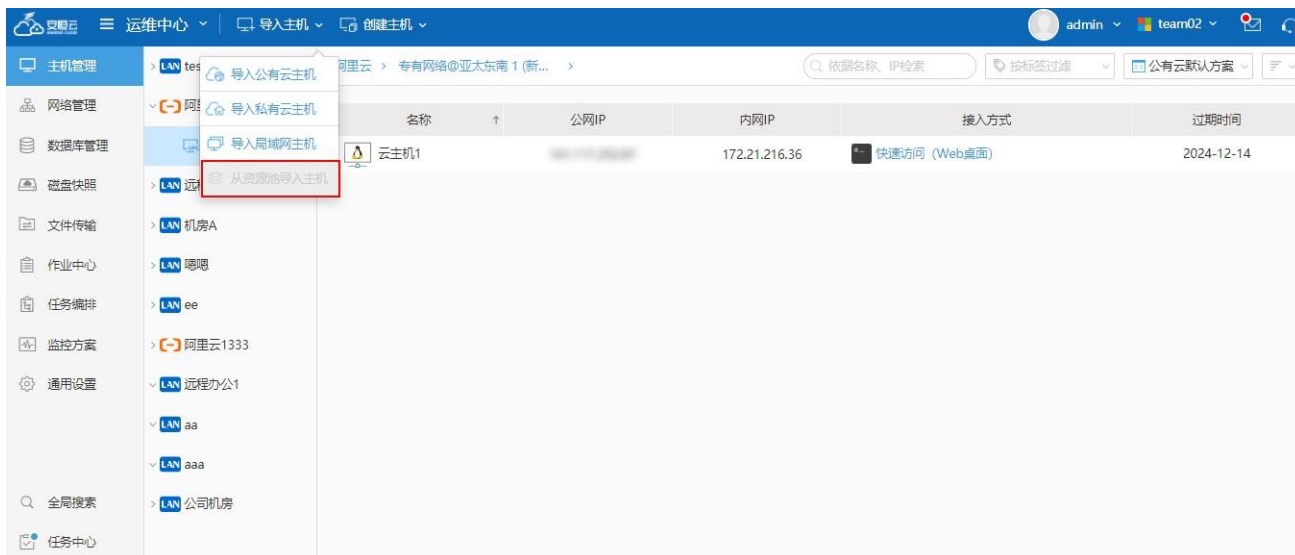
步骤9. 主机扫描完成后，勾选相应的主机，点击<添加>，将所选主机全部导入到安恒云中进行管理。



4.4 导入资源池主机

导入 vCenter、OpenStack 资源池后，可以将资源池中的虚拟机导入安恒云，实现对 vCenter、OpenStack 虚拟机的访问、安装 Agent 乃至监控等操作。安恒云以 API 接口形式来导入和管理 vCenter 以及 OpenStack 的主机。

步骤1. 在菜单栏中选择“**运维中心 主机管理**”进入主机管理页面，点击“**导入主机 从资源池导入主机**”。



步骤2. 点击**使用新的云账户**，本文以第一次导入资源池里的主机为例（如果您已经从目标资源池里导入



过主机，直接选该云账户导入即可)。

步骤3. 选择要导入其主机的资源池，点击<下一步>。



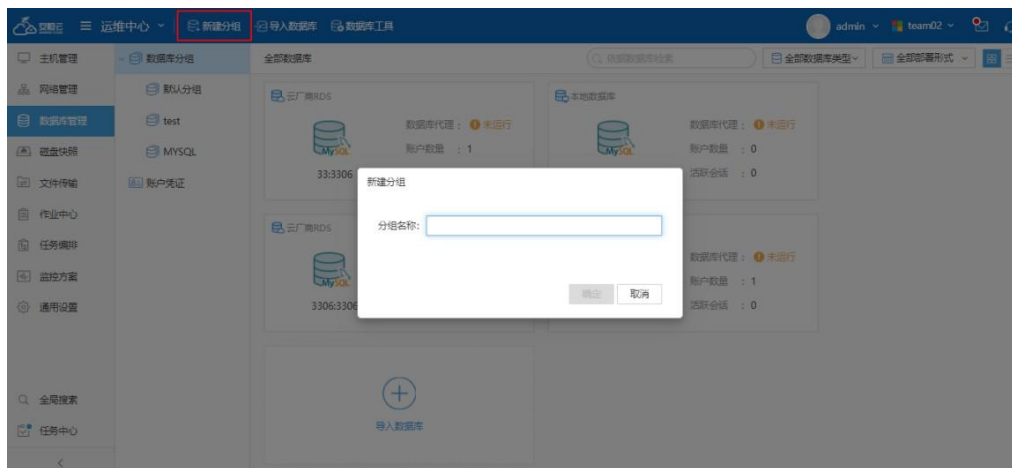
步骤4. 之后按照配置向导完成导入资源池主机操作。

4.5 导入数据库

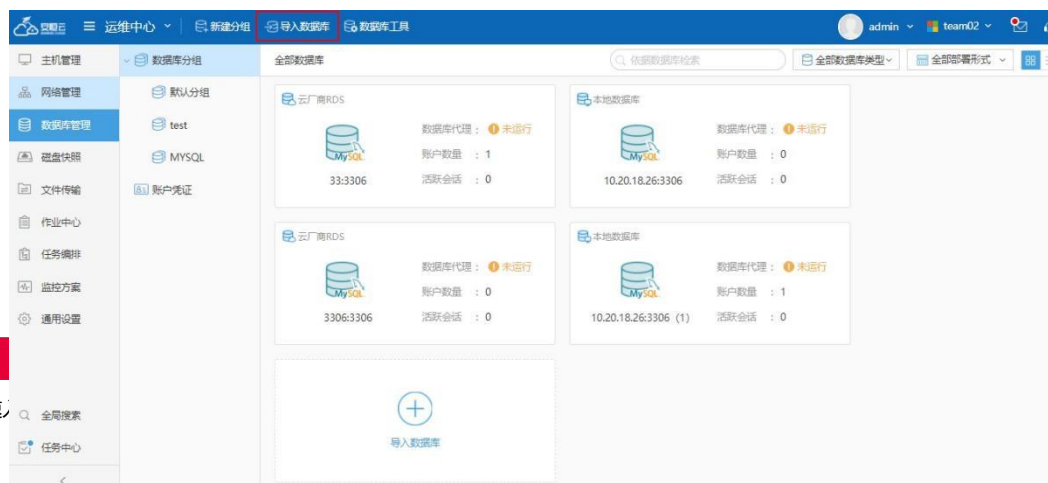
安恒云为用户提供了数据库访问的跳板机代理，用户通过跳板机访问数据库时，所有的 SQL 语句将被记录下来。同时，还可将敏感数据设置为脱敏字段，在查询相关的字段数据时，将进行脱敏处理，保护数据不被泄露。

导入数据库的操作方法如下：

步骤1. 在菜单栏中选择“**运维中心** **数据库管理**”进入**数据库管理**页面。点击**新建分组**，填写分组名称 点击<**确定**>。



步骤2. 新建分组后，即可在对应的分组里导入数据库，选择分组，点击**导入数据库**。





步骤3. 选择要导入的数据库部署形式，可以选择本地数据库或云厂商 RDS，然后选择要添加的数据库分组，点击<下一步>。



步骤4. 如果针对本地数据库的管理，需要事先将本地数据库所在主机导入到安恒云主机列表里，选择数据库所在主机

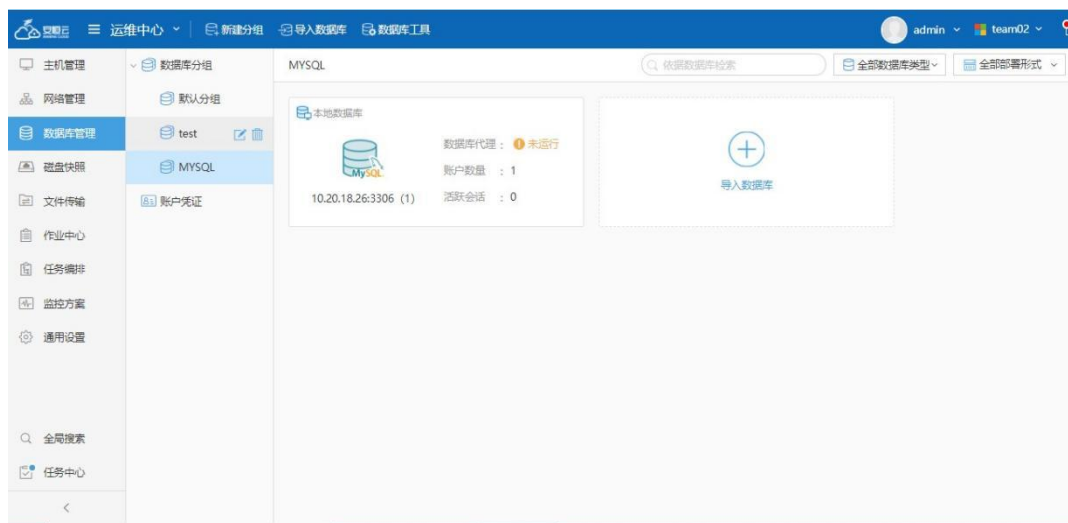
步骤5. 选择数据库代理并选择数据库类型及填写数据库端口，用户在安恒云中通过数据库代理访问目标数据库，并由数据库代理承担 SQL 指令的拦截、审计、敏感指令告警等职责。

- ◆ Proxy 代理
- ◆ 默认中转服务器

步骤6. 导入数据库完成，点击<前往设置>设置账户凭证或数据库访问方案。



步骤7. 导入成功后，可在数据库分组中查看该数据库。



导入云厂商 RDS 与导入本地数据库操作类似，不再赘述。

4.6 云账号管理

导入上述主机或数据库成功后，选择“**运维中心 通用设置**”，进入**云账户管理**页签进行查看和管理。



4. 开启安全防护

在安恒云中导入云资源后，可开通安全产品对云资源进行安全防护。安全产品主要包括主机安全体检、Web 应用防火墙、漏洞扫描、网站监测、堡垒机、数据库运维网关、数据库审计、主机安全、防火墙、日志审计等。

安全产品分为两类：

- ◆ 服务类产品：平台自带产品，开通后即可使用，不需要部署在用户的云环境中。包括 Web 应用防火墙、漏洞扫描、网站监测、堡垒机和数据库运维网关。
- ◆ 镜像类产品：平台仅提供安全产品的镜像文件，开通后需要部署在用户的云环境中（目前仅支持阿里云、腾讯云和华为云）。包括数据库审计、主机安全、防火墙和日志审计。

5.1 开通服务类产品

5.2 开通镜像类产品

本文以开通数据库审计举例说明，其他镜像类产品开通步骤大致相同。

5.2.1 开通数据库审计

步骤1. 购买数据库审计服务。

- 1) 在菜单栏选择“**云安全中心 数据库审计**”，进入如下页面。



- 2) 点击<**正式开通使用**>，选择服务版本，设置配额详情、购买时长，勾选**我已阅读和同意《安恒云用户使用协议》**，点击<**去结算**>。



- 3) 在**订单结算**页面支付费用后，完成开通。

步骤2. 部署数据库审计服务实例。

购买数据库审计服务成功后，在**数据库审计**页面会显示该服务实例，并且状态为**待部署**。需要将该服务实例部署到用户的云环境。

在不同的公有云上部署数据库审计服务实例，操作可能会有部分差别，本文以阿里云为例进行说明：

- 1) 点击待部署的数据库审计服务实例对应的**<立即部署>**。



- 2) 指定主机源。进入部署服务实例页面，选择部署服务实例的**主机源**和云厂商**账号 id**，点击**<下一步>**。如果当前没有云账号，可以点击**<添加云账户>**根据添加向导导入公有云主机源。更多信息请参考导入公有云主机。



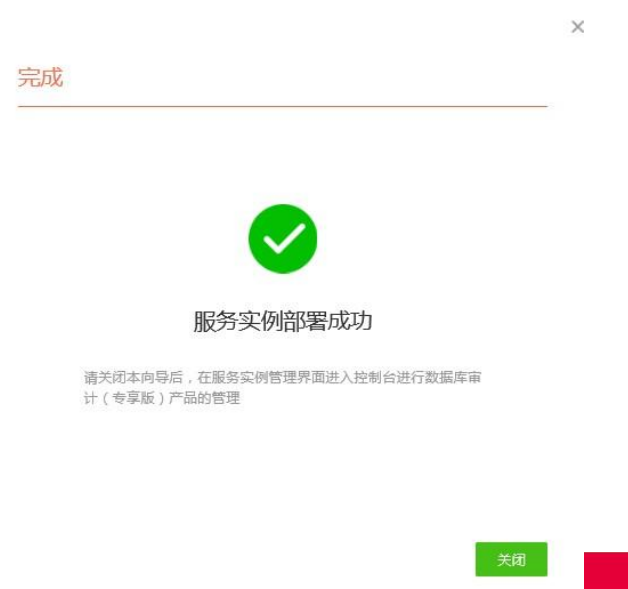
- 3) 选择VPC网络。点击**选择**下拉框，选择计划部署服务实例的地域，然后添加对应的VPC网络，点击**<下一步>**。



确认实例信息，确认无误后点击<下一步>



4) 等待服务实例部署完成，点击<关闭>，完成部署。



某些场景需要登录客户的公有云控制台接受共享镜像才能完成部署，请根据界面提示操作。

步骤3. 确认数据库审计服务部署实例状态正常。

数据库审计服务部署成功后，在**数据库审计**页面会显示该服务实例，并且状态为**运行中**。



5.2.2 使用数据库审计

数据库审计服务部署成功后，点击**<控制台>**登录到 Web 管理界面。确认许可正常后，可以添加数据库资产并配置安全规则和过滤规则对数据库资产进行保护。

镜像类产品详细使用方法请登录安恒社区，[下载并查看对应版本的用户手册等资料](#)。

下载路径：**文档中心** **网络信息安全防护** **镜像类产品名称（如明御数据库审计与风险控制系統产品手册）**。

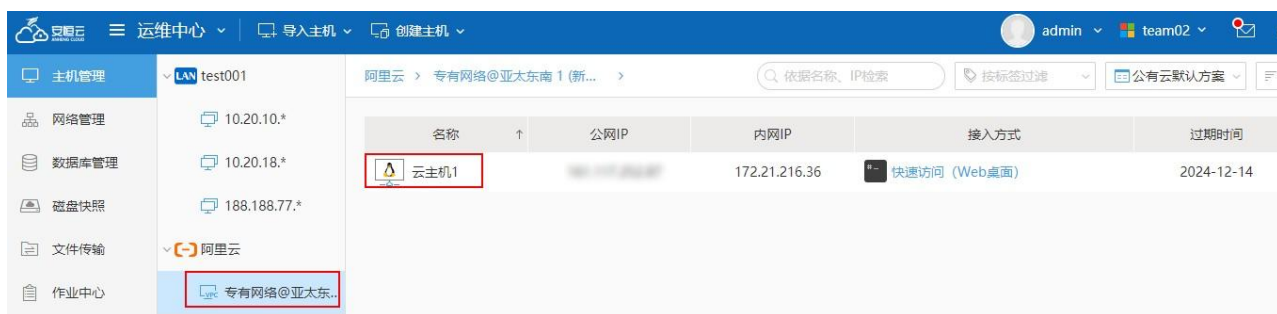
5. 日常运维

日常运维是指对导入到安恒云的云资源的运行维护，主要包括主机管理、磁盘快照、成本优化等。

6.1 主机管理

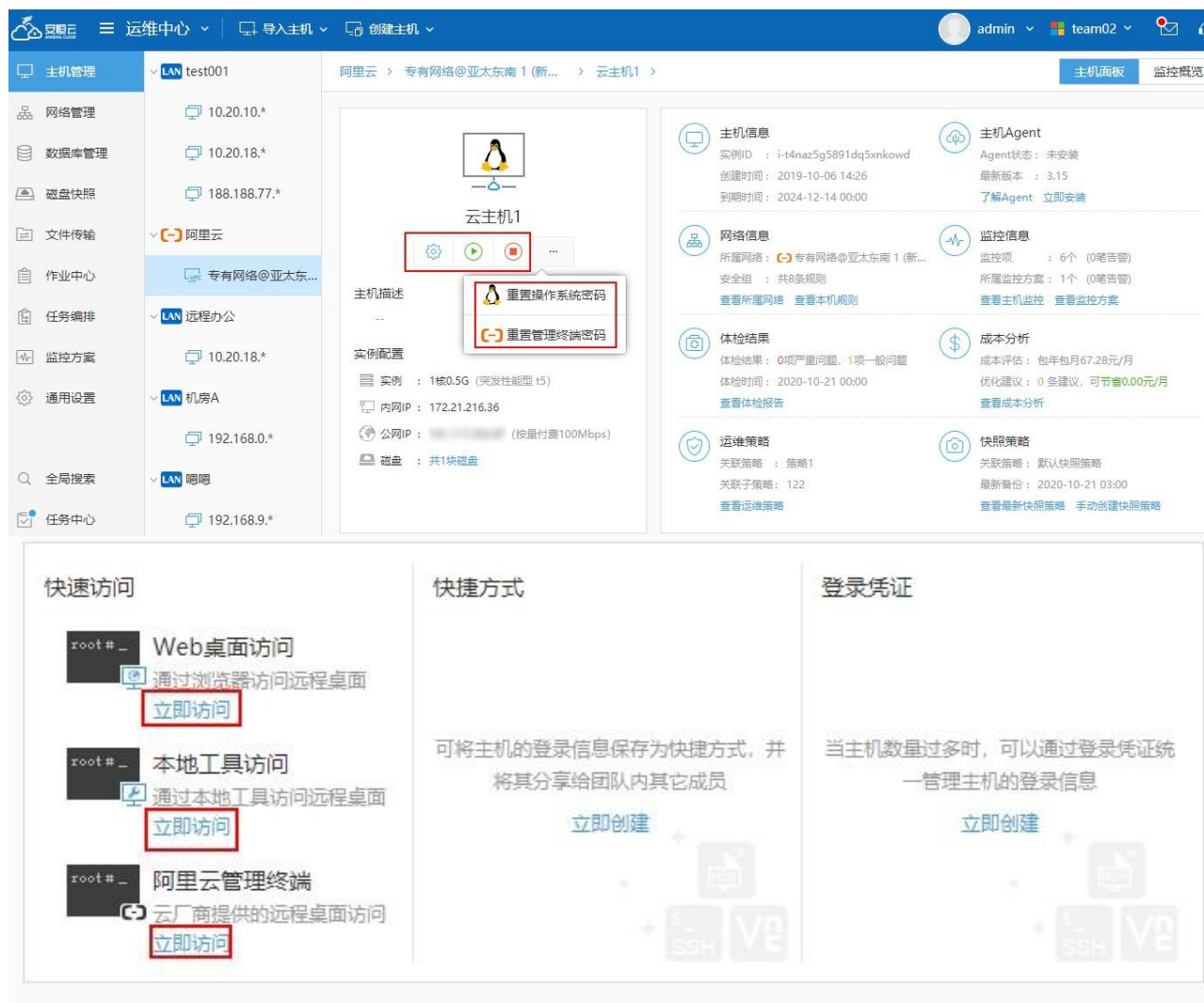
主机管理主要包括重启主机、停止主机、访问主机等。操作方法如下：

步骤1. 在菜单栏选择**“运维中心 主机管理”**进入主机管理页面，点击目标主机。



步骤2. 进入主机详情页面，可查看主机运行状态，设置主机信息、重启主机、停止主机、重置操作系统密码、重置管理终端密码等。

步骤3. 在快速访问区域点击**立即访问**可远程访问主机。



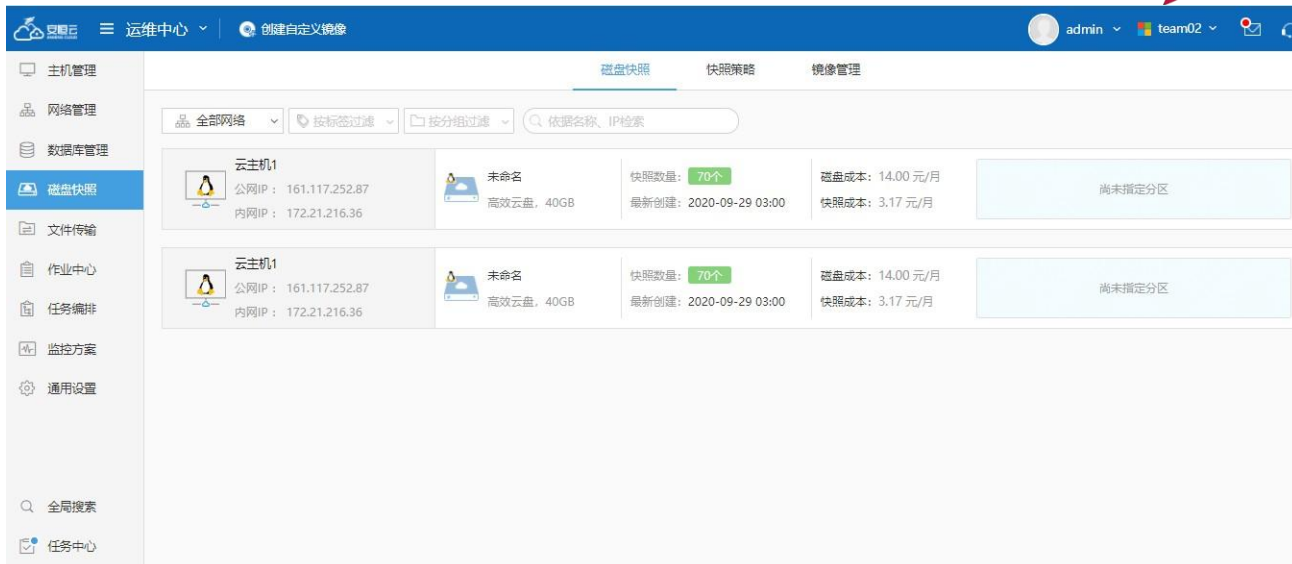
6.2 磁盘快照

磁盘资源是作为云主机的一种附属资源而存在的，因此在安恒云中，磁盘是以云主机为维度来查看。快照是磁盘的一种备份方式，是某一个时间点上某一个磁盘的数据备份，用户可以将快照作为数据的备份。也可以是创建新磁盘时的镜像文件，快速克隆出多块磁盘，以达到快速部署的目的。通常来说，快照由云厂商负责存储，不会占据用户的存储空间。

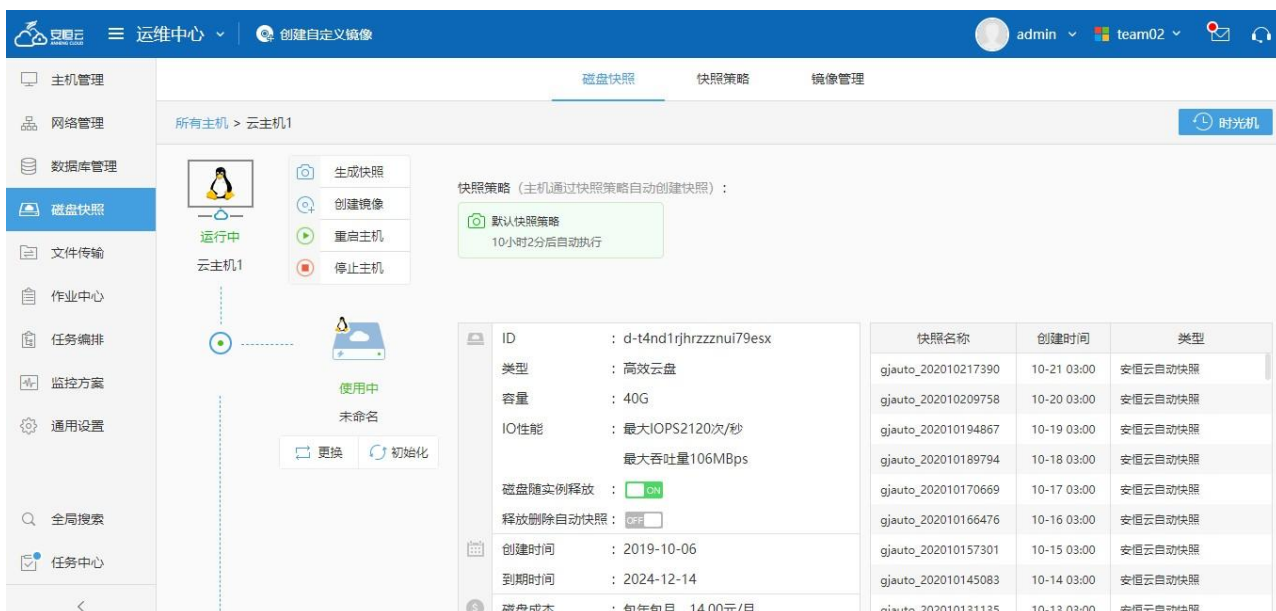
快照的生成方式分手动和自动两种，用户可以在任意一个时间点手动创建快照，也可以通过设置快照策略来自动创建快照（腾讯云没有提供自动快照策略）。

安恒云作为第三方的云资源管理平台，通过调用云厂商相关的 API 查询用户的快照资源，安恒云自身并不提供独立的快照功能。

步骤1. 在菜单栏中选择“**运维中心 磁盘快照**”进入**磁盘快照**页面。在磁盘列表中，可以查看磁盘类型容量、快照信息和成本信息。



步骤2. 点击目标主机, 进入该主机的磁盘详情页面, 可进行磁盘管理, 快照策略管理和镜像管理等操作。



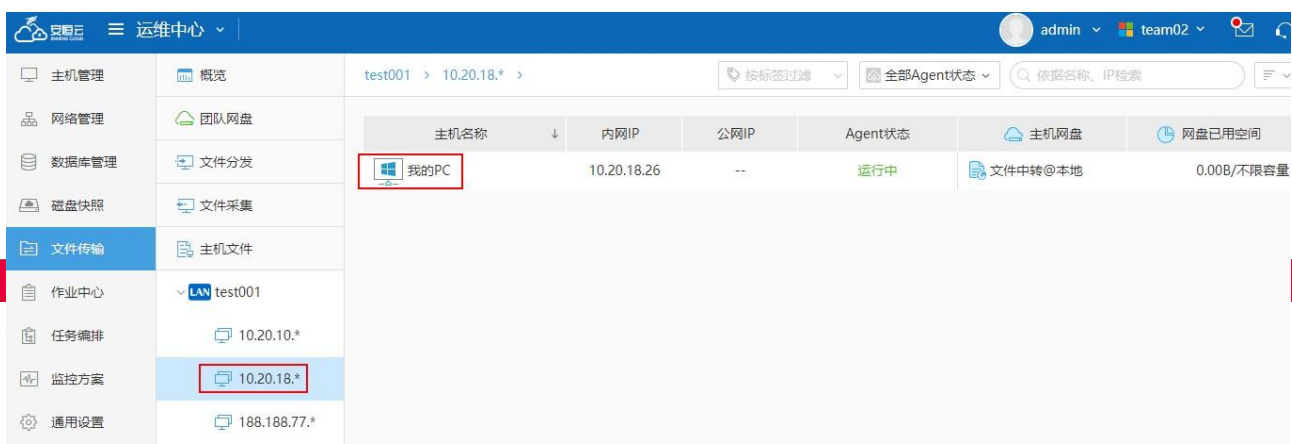
6.3 文件传输

安恒云可对云主机的文件进行管理, 包括主机文件管理、文件分发、文件采集等。

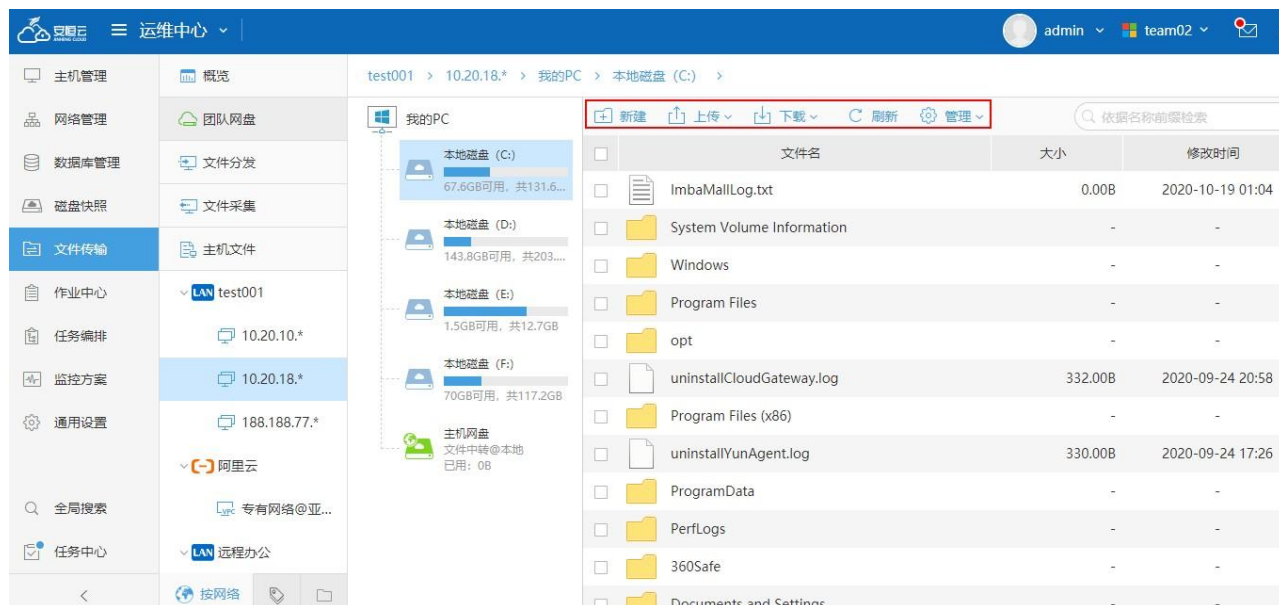
Agent 的更多信息, 请参考《安恒云用户手册》。

6.3.1 主机文件管理

步骤1. 在菜单栏选择“运维中心 文件传输”进入文件传输管理页面, 点击目标主机。



步骤2. 进入主机文件详情页面，可对主机文件进行管理，包括上传文件至主机，或从主机下载文件等。

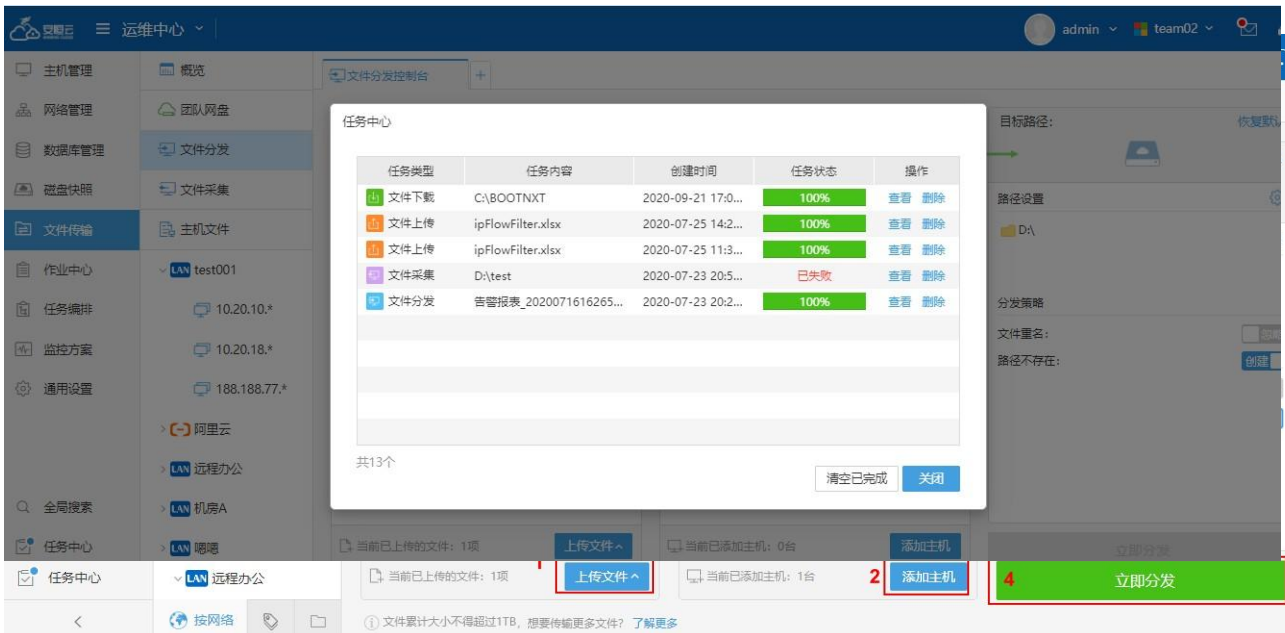


6.3.2 文件分发

安恒云网盘资源是在现有主机资源管理平台基础上提供的能够支持批量文件分发、采集的多云运维工具。

步骤1. 在菜单栏中选择“**运维中心 文件传输 文件分发**”进入**文件分发**页面，点击<上传文件>添加要分发的文件，点击<添加主机>添加文件分发的目标主机，设置目标路径，点击<立即分发>进行文件分发。

步骤2. 在菜单栏中选择“**运维中心 任务中心**”，进入**任务中心**页面，可以查看文件分发情况。



步骤3. 点击<查看>，选择**分发情况**页签，查看文件分发详情。



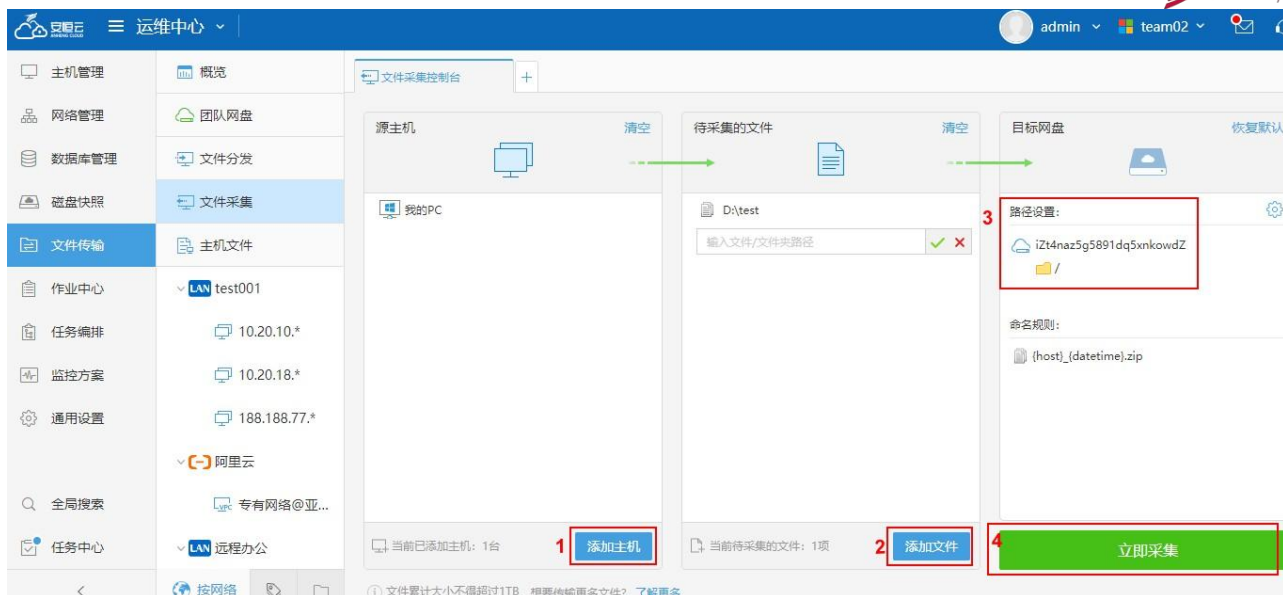
步骤4. 选择**文件信息**页签，查看具体文件信息。



6.3.3 文件采集

在文件批量操作场景中，除文件分发外，还存在从多台主机中批量采集某些共同特征文件的情况，如：定期收集多台主机上的日志文件。在安恒云中，可以通过文件采集控制台来实现这个需求。

步骤1. 在菜单栏中选择“**运维中心** **文件传输** **文件采集**”进入**文件采集**页面。点击<添加主机>添加目标主机，点击<添加文件>设置文件采集的路径，设置目标网盘路径（采集后的文件存放位置），点击<立即采集>即可采集文件。



步骤2. 在菜单栏中选择“**运维中心** **任务中心**”，进入**任务中心**页面，可以查看文件采集情况。

任务中心

任务类型	任务内容	创建时间	任务状态	操作
文件采集	D:\test	2020-09-30 14:46:38	100%	查看 删除
文件采集	D:\test	2020-09-30 14:45:46	已失败	查看 删除
文件分发	告警报表_20200716162656.xl...	2020-09-30 14:38:59	100%	查看 删除
文件下载	C:\BOOTNXT	2020-09-21 17:01:16	100%	查看 删除
文件上传	ipFlowFilter.xlsx	2020-07-25 14:28:08	100%	查看 删除
文件上传	ipFlowFilter.xlsx	2020-07-25 11:32:43	100%	查看 删除
文件采集	D:\test	2020-07-23 20:50:53	已失败	查看 删除
文件分发	告警报表_20200716162656.xl...	2020-07-23 20:27:29	100%	查看 删除

共16个

[清空已完成](#) [关闭](#)

步骤3. 点击<查看>，可以看到文件采集详情。



6.4 成本优化

6.4.1 概述

弹性是云计算的一大特性。在云计算使用过程中，允许用户对云资源计算能力进行动态的调整，使用户可以根据业务需求调整云资源的配置。但是在拥有大量云资源的情况下，用户可能没有能力跟踪每个云资源的变配需求，导致无法及时对云资源的配置进行调整。

针对上述问题，安恒云提供成本优化功能，主要包含两部分内容：

- ◆ **成本优化建议：**为用户提供云资源变配建议，系统会对云资源最近 10 天的负载数据进行分析，为用户做出调整建议；用户可以根据系统建议以及利用[优化仿真工具](#)来模拟变配后的负载情况，最终做出是否升降级的决策。
- ◆ **闲置资源清理：**用户购买后未绑定的弹性公网 IP、未挂载的磁盘和磁盘释放后留存的快照等资源，如果长期闲置下去，将导致不必要的成本支出。安恒云能够为用户罗列出所有的闲置资源，用户可根据实际情况决定是保留或者及时释放。

6.4.2 查看成本优化

选择“多云管理 成本中心”，在各个云账户的成本总览中可查看当前云资源的优化建议和闲置资源情况。



优化建议包含云主机和CDN 的优化建议：

- ◆ 云主机优化建议可提供实例、带宽的规格调整方案。
- ◆ CDN 优化建议可提供计费方式变更、流量包购买的调整方案。

点击<导出优化建议>查看系统提供的优化建议。

闲置资源罗列出用户名下云账户的所有闲置资源（包括未导入安恒云的云资源），用户可直接将闲置资源释放。

资源类型	资源名称	闲置原因	资源规格	成本评估 (元/月)	查看
快照链	源磁盘【d-rj93vbx1xdoky2wis5o】的快照 sl-rj9216ctez1mfjxsek5l	源磁盘已释放	14.90GB	1.63	查看详情
快照链	源磁盘【d-94ko5cdwn】的快照 d-94ko5cdwn	源磁盘已释放	26.35GB	3.90	查看详情
快照链	源磁盘【d-94g1gwcal】的快照 d-94g1gwcal	源磁盘已释放	64.16GB	9.50	查看详情
快照链	源磁盘【d-94rpgqbcc】的快照 d-94rpgqbcc	源磁盘已释放	66.44GB	9.83	查看详情

6.4.3 优化仿真工具

优化仿真工具是安恒云对主机在不同配置下的负载情况进行模拟的工具，以便为用户是否需要将主机进行变配提供决策支撑。

6.4.3.1 概述

在菜单栏选择“多云管理 成本中心”，点击页面上方的<优化仿真工具>选择相关工具。



按照模拟的对象不同，优化仿真工具分为实例仿真工具和网络带宽仿真工具两种。



6.4.3.2 实例仿真工具

点击<实例优化>进入实例仿真工具，对主机的CPU 和内存进行变配模拟，形成变配前后的CPU 及内存负载及成本支出对比。



通过可视化的负载曲线和热力图, 用户可以更直观的了解变配前后的负载变化情况。



6.4.3.3 网络带宽仿真工具

点击<带宽优化>进入实例仿真工具, 对主机的网络带宽进行变配模拟。

支持带宽计费类型和带宽峰值的调整, 将变配前后的负载情况对比以曲线图展示。用户通过仿真工具, 可以更好的调整带宽配置, 将带宽成本支出控制在合理的范围。



评估周期: 最近10天	公网出站真实流量负载	按量付费, 100Mbps	公网出站仿真流量负载	按量付费, 50Mbps	
 iZt4naz5g5891dq... (i-14naz5g5891dq5xmkow... 网络类型: 经典网络 公网IP: 161.117.252.87 区域: 亚太东南1(新加坡)	带宽负载	 公网出站负载极低, 建议缩减带宽限额		 仿真后公网出站负载极低, 建议缩减带宽限额	
	出站负载指数: 6			出站负载指数: 2	
	平均出站速率: 360.14Kbps			平均出站速率: 354.61Kbps	
	出站总流量: 36.49GB			出站总流量: 36.52GB	
	95分位数: 2.53Mbps			95分位数: 2.52Mbps	
	峰值速率时长: 0分钟			峰值速率时长: 0分钟	
峰值时长占比: 0.00%			峰值时长占比: 0.00%		
成本	¥58.02元/月		¥58.07元/月		

