阿里云
专有云企业版

安全管理员指南（高级版）

产品版本：V3.5.2

文档版本：20180831

为了无法计算的价值 | 阿里云

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。

1. 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。
2. 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。
3. 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. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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、发行或公开发表本文档中的内容。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
	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。	**禁止**： 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	**注意**： 导出的数据中包含敏感信息，请妥善保存。
	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。	**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。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	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。	`swich` *`{stand | slave}`*

目录

1 概述

云盾高级版是适用于核心业务应用对外防护的互联网化防护体系，能够为用户提供DDoS检测/防御、Web层攻击检测/防御、Web漏洞发现/修复、主机漏洞发现/修复、主机防入侵的实时防护能力。通过现网获取的丰富本地泛安全数据与云端情报将统一在安全数据分析引擎集群里进行安全大数据分析，为安全管理员呈现整体安全态势、入侵事件回溯，包括针对性攻击发现、人员情报泄漏预警、入侵原因分析等。通过这些核心安全信息的分析展现，安全管理员不仅能够了解安全状况，还可以借助安全数据分析引擎开放的自定义分析界面对已有安全数据进行场景化分析，实现安全分析能力的灵活定制。

2 配置要求

本地PC需要满足如表 *2-1:* 配置要求表中要求才可以正常登录云盾安全中心。

表 2-1: 配置要求表

内容	要求
浏览器	• Internet Explorer浏览器：11及以上版本 • Chrome浏览器（推荐）：42.0.0及以上版本 • Firefox浏览器：30及以上版本 • Safari浏览器：9.0.2版本及以上版本
操作系统	• Windows XP/7 及以上版本 • Mac系统

3 登录和注销

3.1 用户权限说明

在登录云盾安全中心前，需要管理员已经创建云盾安全中心用户，并为该用户分配云盾安全中心相关的角色权限。

所有云盾安全中心角色均为默认角色，无法自定义添加。关于如何创建用户及授予角色权限，请参考《用户指南》中**创建用户**一节。

表 3-1: 云盾安全中心默认角色说明

角色名称	角色说明
云安全中心系统管理员	负责云盾安全中心系统管理设置，具备阿里云账号管理、云端同步、告警设置、及全局设置的权限。
云安全中心安全管理员	负责整个专有云平台的安全状态，管理云盾各功能模块的安全策略设置，包括态势感知、网络安全、应用安全、云主机安全、物理机安全、资产管理各目录下的所有功能节点权限。 **说明**： Web应用防火墙、云防火墙等功能的权限需要单独开通。
部门安全管理员	负责某个指定部门中各云产品资源的安全状态，管理针对该部门的云盾各功能模块的安全策略设置，包括态势感知、网络安全、应用安全、云主机安全、物理机安全、资产管理各目录下的所有功能节点权限。同时，部门管理员还可以设置该部门中安全事件告警的联系人及告警方式。 **说明**： Web应用防火墙、云防火墙等功能的权限需要单独开通。
云安全中心审计员	负责整个专有云平台安全审计工作，查看审计事件、原始日志并设置相关审计策略，具备安全审计目录下所有功能节点权限。

3.2 登录云盾安全中心

登录云盾安全中心两种方式：通过Apsara Stack控制台跳转到云盾安全中心和直接登录云盾安全中心。

- 登录Apsara Stack控制台，从Apsara Stack控制台页面上跳转到云盾安全中心页面。

a) 打开Chrome浏览器。

b) 在地址栏中，输入Apsara Stack控制台的网站地址（例如：http://*Apsara Stack*控制台网站地址），按**Enter**，进入Apsara Stack控制台登录页面。

c) 在Apsara Stack控制台登录页面，输入已创建的云盾安全中心用户的登录账号、密码及验证码。

d) 单击**登录**。

e) 登录Apsara Stack控制台后，选择**云管控中心** > **云基础产品** > **云盾控制台**。

f) 选择**区域**，单击**云盾控制台**，进入云盾安全中心页面，如图 *3-1:* 安全中心页面所示。

图 3-1: 安全中心页面

- 通过云盾安全中心的网站地址，直接登录。

说明：

从部署人员处获取相关网站地址信息，通过浏览器直接访问页面。

a) 打开Chrome浏览器。

b) 在地址栏中，输入云盾安全中心的网站地址（例如：http://*DTCSC*网站地址），按**Enter**。

c) 输入已创建的云盾安全中心用户的登录账号、密码及验证码。

d) 单击**登录**。

3.3 退出云盾安全中心

- 在**云盾安全中心**页面，单击页面右上角的**退出**，即可从云盾安全中心注销。

4 云盾高级版安全中心界面

云盾高级版云安全中心的界面主要可以分为三大区域，如图 *4-1:* 云盾高级版安全中心页面所示。

图 4-1: 云盾高级版安全中心页面

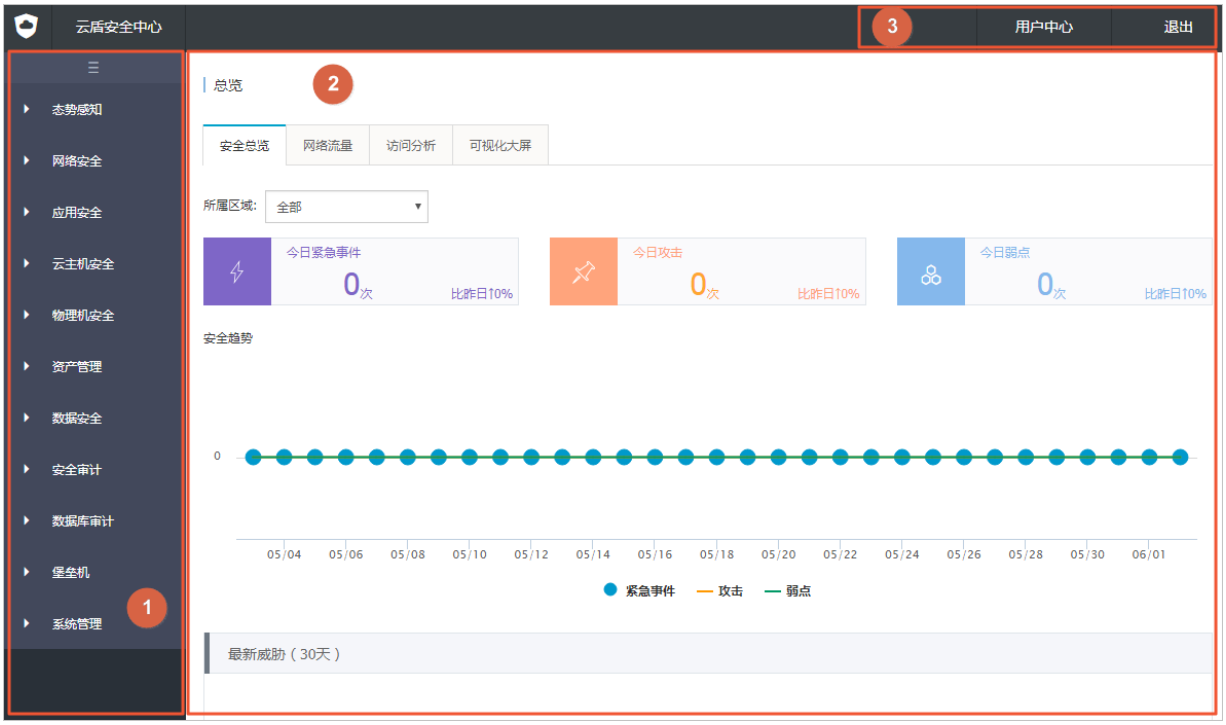


表 4-1: 云盾安全中心界面区域说明

序号	区域	说明
1	菜单导航区	云盾安全中心高级版主要功能如下： • **态势感知**：捕获和分析网络安全态势、对安全事件进行关联回溯和大数据分析，展示已发现的安全事件威胁风险。 • **网络安全**：包括DDoS攻击防护、云防火墙等功能，帮助安全管理员全面管理专有云平台内部、外部的网络安全状态。 • **应用安全**：包括Web应用防火墙功能，帮助安全管理员保障专有云平台应用层面安全。 • **云主机安全**：包括安全预防、入侵检测等功能，帮助安全管理员管理云主机安全。 • **物理机安全**：包括文件篡改、异常进程、异常网络连接、可以端口监听等功能。 • **资产管理**：帮助安全管理员管理专有云环境中的资产，包括主机资产、NAT IP资产。

序号	区域	说明
		• **数据安全**：通过数据发现和数据脱敏，保护用户数据安全，满足合规性遵从需求。 • **安全审计**：对云服务操作日志展示和审计，以便安全审计员及时发现并消除安全隐患。 • **数据库审计**：为专有云环境中的数据库提供安全诊断、维护、管理能力。 • **堡垒机**：为云服务器的运维提供完整的审计回放和权限控制服务。 • **系统管理**：包括阿里云账号管理、云端同步、告警设置、全局设置等功能。
2	操作视图区	选择某功能菜单项后，该菜单项的功能配置界面将显示在右侧的操作视图区中。
3	操作按钮区	• **用户中心**：单击此按钮进入个人信息页面，可查看当前登录用户的基本资料，或修改登录密码。 • **退出**：单击此按钮退出当前登录。

5 态势感知

态势感知全面集成了企业漏洞监控、黑客入侵监控、Web攻击监控、DDoS攻击监控、威胁情报监控、企业安全舆情监控等安全态势监控手段，通过建模分析方法，从流量特征、主机行为、主机操作日志等获取关键信息，识别无法单纯通过流量检测或文件查杀发现的入侵行为，借助云端分析模型输入并结合情报数据，发现攻击威胁来源和行为，并评估威胁程度。

态势感知主要包含：

- **总览**：展现安全的整体态势、网络流量情况和安全大屏相关信息。
- **事件分析**：展现业务系统中已经发生的安全事件和发展趋势。
- **威胁分析**：展现当前系统面临的安全风险。
- **安全报表**：配置专有云平台安全报表任务。
- **漏洞扫描**：展现系统中存在的漏洞和缺陷。

5.1 总览

总览页面展示了当前专有云环境的安全态势总览，对整体安全态势进行概要性展示，以便安全管理员快速了解和掌握当前安全态势。

总览主要包括以下方面：

- **安全总览**：对系统已经发生的安全事件、目前面临的安全威胁、系统自身存在的弱点缺陷进行概要性展示。
- **网络流量**：对网络的出口、入口、QPS 流量信息的分析，展示流量的高峰、低谷、速率和地域来源的分布规律。
- **访问分析**：分析前一天的访问情况，识别访问者身份，并向安全管理员展示访问者信息及访问页面信息。
- **可视化大屏**：为安全管理员提供最直观的安全形势和面临威胁的展示，作为安全决策的重要参考指标。

5.1.1 查看安全总览信息

背景信息

安全总览页面包括安全趋势、最新威胁和资产概览信息，帮助安全管理员全方位、整体性地把握自身系统的安全态势。

操作步骤

1. 登录云盾控制台。
2. 定位到**态势感知** > **总览**，单击**安全总览**，查看目前专有云平台安全的总览情况，如图 *5-1: 安全总览页面*所示。

图 5-1: 安全总览页面

表 5-1: 安全总览页面区域说明表

页面区域	说明
安全趋势	安全趋势展示了当前系统已经发生的安全事件和攻击、系统发现的弱点缺陷，并从时间维度展示了系统安全态势的变化。
最新威胁	最新威胁展示了当前系统存在的安全威胁，急需安全管理员积极关注。 **说明**： 这些安全威胁事件都是由云盾的核心扫描器扫描，并通过针对专有云平台的大数据分析模型分析所得。
资产概览	选取用户最关心的资产情况进行展示，使用户实时掌握资产状态。

3. 单击今日紧急事件、今日攻击、今日弱点，或查看最新威胁，可直接跳转至相应的页面查看详细信息。

   例如，单击今日紧急事件，即跳转至**事件分析**页面。

5.1.2 查看网络流量信息

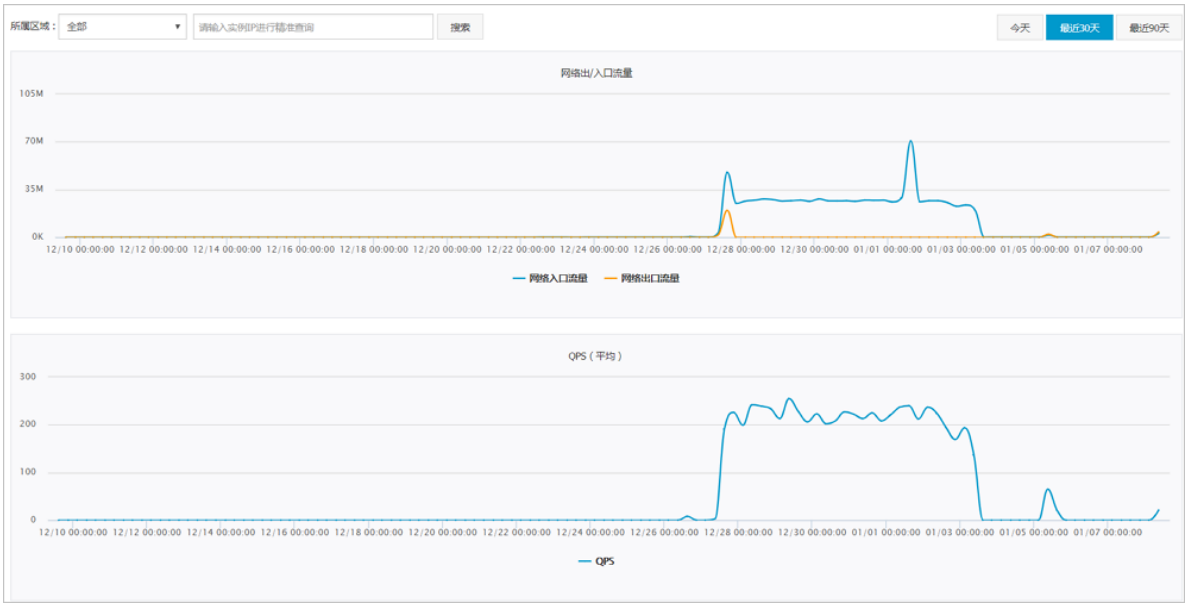
背景信息

网络流量页面通过折线图展示了过去一段时间的流量信息，通过查看不同时期、区域或单个IP的流量情况，可以定位流量的高峰和低谷时间、速率和地域等流量分布规律，同时通过展示TOP5流量的IP，帮助安全管理员有效甄别恶意的IP访问。

操作步骤

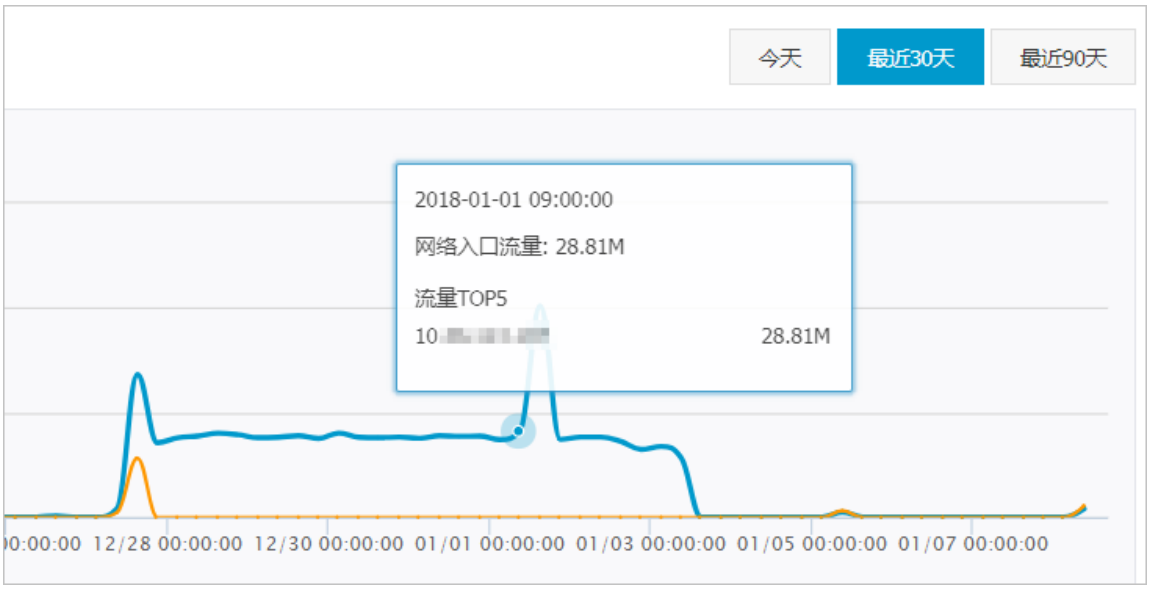
1. 登录云盾控制台。
2. 定位到**态势感知** > **总览**，单击**网络流量**进入网络流量页面，如图 *5-2: 总览页面*所示。

图 5-2: 总览页面



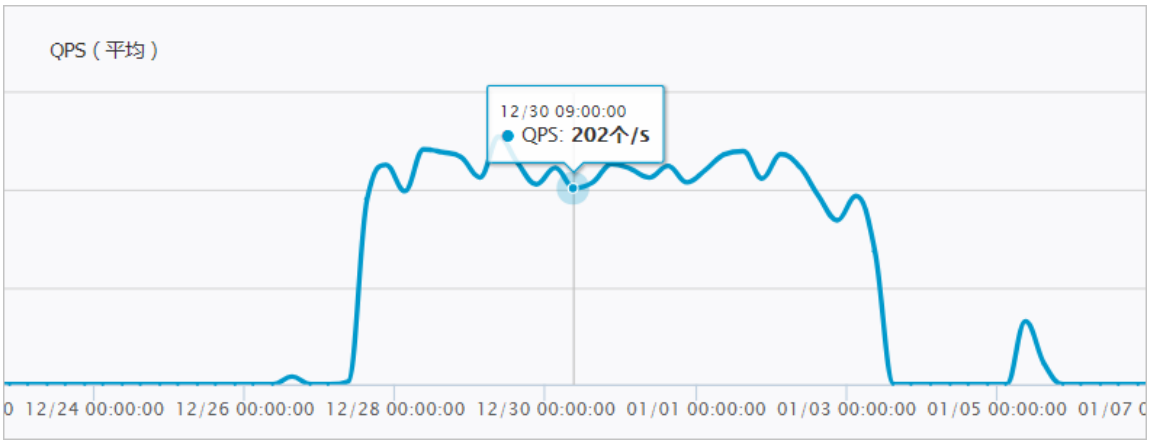
3. 查看不同时期、区域或单个IP的流量情况。
   - 在**总览**页面，单击**今天**、**最近30天**、**最近90天**可以切换查看不同时间段的流量信息。
   - 在**所属区域**中可以选择区域信息，或在搜索框中输入IP，可以分区域、分IP查询流量信息。
4. 查看某时间节点具体流量信息。
   - 在网络出/入口流量图中，将鼠标停留在流量折线上，可查看该时间点出口或入口流量的详细信息及流量TOP5的IP，如图 *5-3: 查看流量 TOP5 的 IP*所示。

图 5-3: 查看流量 TOP5 的 IP



- 在QPS（平均）图中，将鼠标停留在流量折线上，可查看该时间点的具体QPS信息，如图 *5-4: 查看QPS详细信息*所示。

图 5-4: 查看QPS详细信息



5.1.3 查看访问分析结果

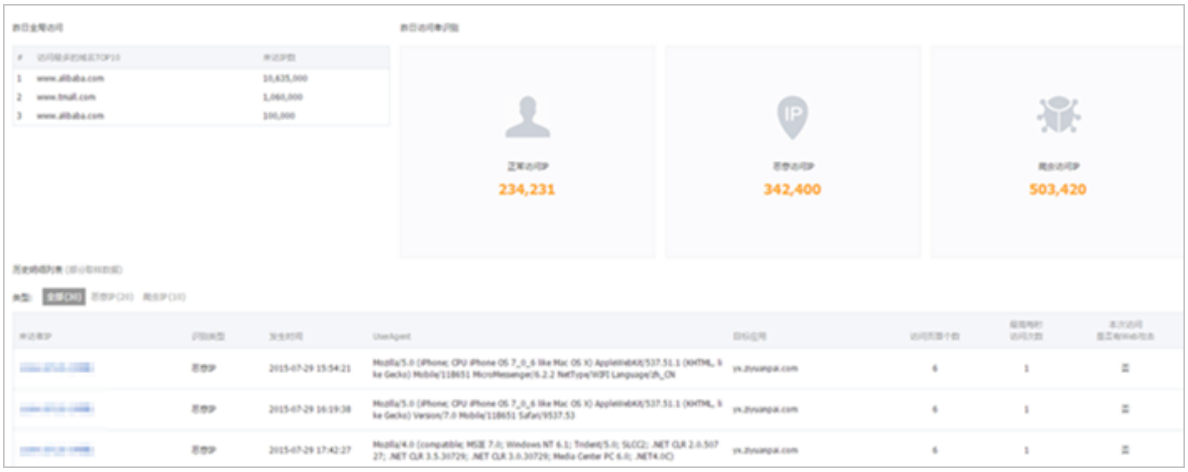
背景信息

访问分析页面是对不同来源的访问进行分析甄别，通过大数据分析，甄别出正常访问、恶意访问和爬虫访问者三种类型，安全管理员可以根据恶意访问和爬虫访问的行为动作有效了解自身系统可能面临的安全问题和来源。

操作步骤

1. 登录云盾控制台。
2. 定位到**态势感知** > **总览**，单击**访问分析**查看访问分析页面，如图 *5-5:* 访问分析页面所示。

图 5-5: 访问分析页面



3. 在历史明细列表中，可以查看详细访问信息。选择访问IP类型，查看指定类型的访问记录。

5.1.4 查看可视化大屏

背景信息

可视化大屏通过形象生动的动画效果展示了关键性的安全事件指标，使安全管理员一目了然地掌握当前的整体安全态势，为安全决策提供有效支持。

目前支持的可视化大屏有互联网边界流量安全监控大屏、业务安全态势和评分大屏。

操作步骤

1. 登录云盾控制台。
2. 定位到**态势感知** > **总览**，单击**可视化大屏**进入可视化大屏入口，如图 *5-6:* 可视化大屏页面所示。

图 5-6: 可视化大屏页面

单击页面上的**修改**，可以修改互联网边界流量安全监控大屏的显示标题。

3. 单击页面上显示的屏幕，进入大屏页面。

- **互联网边界流量安全监控**

  互联网边界流量安全监控大屏是依托云盾流量安全监控模块的访问和流量的监测上报能力，对目前的请求和攻击的来源地域、数量进行统计。同时，该大屏也展示系统目前流量的整体情况，通过列出的TOP5的请求和攻击地域，使安全管理员对请求的压力来源和攻击的地域分布有准确的了解，及时掌握攻击分布的地域规律，如图 *5-7:* 互联网边界流量安全监控所示。

图 5-7: 互联网边界流量安全监控

互联网边界流量安全监控大屏的流量来源和实现的机制参见表 *5-2:* 访问流量数据来源表。

表 5-2: 访问流量数据来源表

类型	实现的机制
请求分析	将用户关注的资产推送给流量安全监控模块，流量安全监控模块根据需要关注的资产上报这些资产被访问的情况。
攻击分析	由云盾流量安全监控模块检测，针对于类似Web攻击的事件进行上报和展示。
流量展示	由流量安全监控模块收集流量信息并上报给控制台记录。

- **业务安全态势和评分**

  业务安全态势和评分大屏是对当前系统面临的安全事件的详细呈现。通过对系统弱点缺陷、遭受攻击和黑客重点关注资产的分析，为系统的安全状况进行打分评价，提示目前系统的安全等级。

此大屏的数据主要是云盾流量安全监控、安骑士和弱点分析等模块进行扫描并上报。TOP5黑客最感兴趣资产由大数据引擎通过模型分析获得，如图 5-8: 业务安全态势和评分大屏所示。

图 5-8: 业务安全态势和评分大屏

5.2 事件分析

紧急事件是系统中已经或正在发生的安全事件。紧急事件被云盾的流量安全监控、安骑士、弱点分析等功能模块扫描发现并上报，需要安全管理员紧急关注并采取安全措施。

紧急事件中包括的事件类型和含义请参见表 5-3: 紧急事件类型表。

表 5-3: 紧急事件类型表

紧急事件类型	说明
后门	安骑士客户端检测用户系统中的Webshell后门，大数据分析模块通过对流量安全监控模块导入流量的分析，检测一句话木马和多功能木马。
暴力破解成功	当暴力破解行为发生和暴力破解成功时，安骑士客户端都会上报信息，暴力破解成功的事件会在紧急事件中显示，需要用户紧急处理。
未授权下载	从流量安全监控模块输出的流量中选择出较为特别的，数量在特定范围内（大于1小于20）的response进行筛选，通过大数据分析模型分析得出未授权下载的情况。

紧急事件类型	说明
肉鸡行为	用户的主机被黑客控制沦为肉鸡并对外进行攻击。
DDoS	流量安全监控模块检测到的DDoS攻击信息。
异常网络连接	基于各安全功能模块上报的信息，通过大数据分析模型，发现异常的向外连接、执行恶意程序下载、恶意文件下载等行为。
网络流量异常	基于流量安全监控模块及安骑士模块上报的信息，发现挖矿程序等。
黑客工具	基于安骑士模块上报的信息，发现主机上残留的黑客工具及黑客攻击行为。

5.2.1 查看紧急事件

操作步骤

1. 登录云盾控制台。
2. 定位到**态势感知** > **事件分析**，进入事件分析页面，如图 5-9: 事件分析页面所示。

图 5-9: 事件分析页面

3. 选择事件**类型**，查看指定类型的紧急事件。

5.3 安全报表

态势感知提供安全报表功能，支持定期将专有云平台的安全状况发送至指定邮箱，帮助安全管理员了解当前安全态势。

安全报表可选择发送以下内容：

- **态势感知**

- 安全统计：包括态势感知总览页面展示的安全总览信息，参见查看安全总览信息。
- 重点关注：包括态势感知事件分析页面展示的需要重点关注的紧急事件信息，参见事件分析。
- 威胁趋势：包括网络安全威胁感知页面展示的攻击趋势、攻击分析等信息，参见威胁分析。

- **安全防护**
  - DDoS：云盾安全中心发现的DDoS攻击事件信息，参见*DDoS事件*。
  - 主机安全：云盾安全中心发现的主机安全漏洞、异常登录、暴力破解攻击、配置风险项等信息，参见主机安全。
  - 防护资产：云盾安全中心已防护的资产信息，包括主机资产和NAT资产，参见资产总览。

5.3.1 添加报表任务

操作步骤

1. 登录云盾控制台。
2. 定位到**态势感知** > **安全报表**，进入**报表任务**页面，如图 *5-10:* 报表任务页面所示。

   图 5-10: 报表任务页面

3. 单击**新增任务**，添加报表任务。
4. 在**添加报表任务**对话框中，填写报表各项信息，如图 *5-11:* 添加报表任务所示。

图 5-11: 添加报表任务

说明：

单击**接收邮箱**右侧的**添加**可添加更多邮箱地址，最多支持输入10个邮箱地址。

5. 单击**确定**。

   报表任务添加成功后，指定的邮箱地址将根据设定的周期收到安全报表，如图 *5-12: 安全报表*所示。

图 5-12: 安全报表

5.3.2 管理报表任务

操作步骤

1. 登录云盾控制台。
2. 定位到**态势感知** > **安全报表**，进入**报表任务**页面。
3. 管理已添加的报表任务。
   - 选择报表任务，单击**详情**，查看该任务详情。
   - 选择报表任务，单击**编辑**，可修改该报表任务。
   - 选择报表任务，单击**删除**，可删除该报表任务。

5.4 威胁分析

威胁分析页面包括威胁分析和攻击两类。

威胁分析

通过对流量信息进行专有云特有的大数据模型的分析，发现攻击特征，并按攻击行为进行整合，展示当前系统面临的安全风险。

威胁分析主要包括以下几个方面：

- 展示普通攻击和针对性攻击的最近7日攻击趋势和最近30天攻击分析。
- TOP5黑客最感兴趣的资产：通过大数据模型分析处理，按照各个资产受到的威胁的得分大小，选择威胁得分最高的五个资产进行展示，以便安全管理员对这些资产进行重点关注和保护。
- 针对性攻击分析：通过大数据模型对流量安全监控模块提供的流量信息进行分析，分析和甄别出针对性攻击。

攻击

攻击主要包括应用攻击和暴力破解两类：

- **应用攻击**：访问Web服务器的流量都会经过云盾的流量安全监控模块，该模块将对流量进行监测，提取流量中的攻击信息。
- **暴力破解**：当黑客针对某个资产进行暴力破解的时候，安骑士客户端能够及时监测到暴力破解行为的发生并上报给控制台。

5.4.1 查看威胁分析结果

操作步骤

1. 登录云盾控制台。
2. 定位到**态势感知** > **威胁分析**，选择**威胁分析**页签，如图 *5-13: 威胁分析页面*所示。

图 5-13: 威胁分析页面

3. 查看最近7日攻击趋势、最近30日攻击分析。

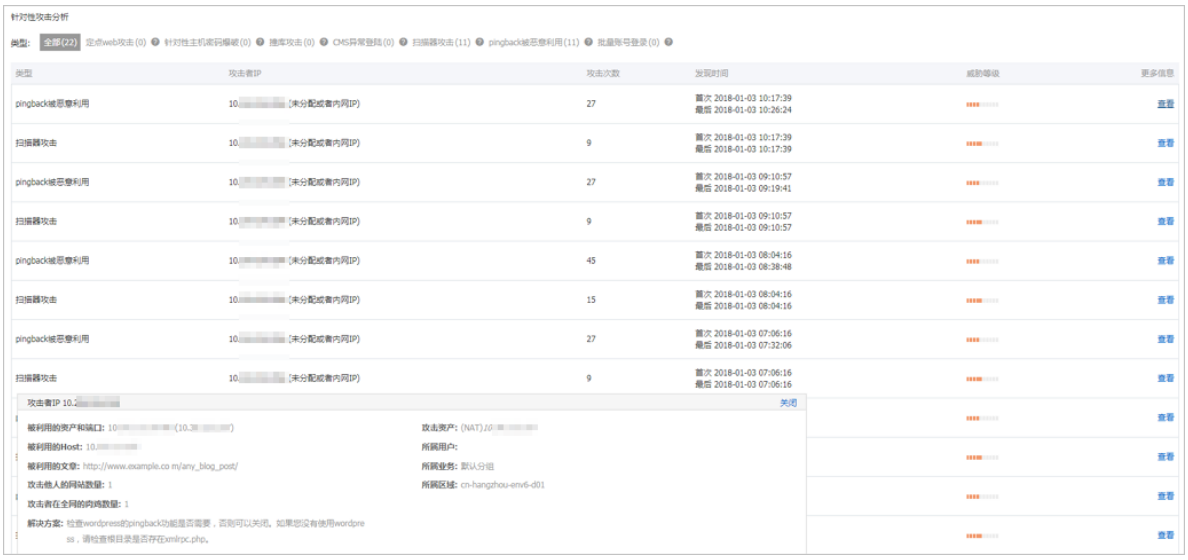
   通过此操作，了解专有云平台上的主机、应用近期遭受的攻击。

4. 查看TOP5黑客最感兴趣资产IP。

   这些资产IP是由云盾安全中心基于检测到的攻击、威胁信息通过大数据计算模型分析得出，建议安全管理员着重加固这些资产的安全防护。

5. 查看针对性攻击分析，如图 *5-14: 针对性攻击分析*所示。

图 5-14: 针对性攻击分析



a) 选择**类型**，可查看云盾安全中心检测到的指定类型的针对性攻击。各攻击类型参见表 *5-4: 针对性攻击类型*。

表 5-4: 针对性攻击类型

针对性攻击类型	说明
定点Web攻击	定点Web攻击是有明显针对性的Web攻击，这意味着相对于其他用户，黑客更关心特定的Web站点，对该Web站点进行SQL注入、命令执行、目录扫描等恶意操作。
针对性主机密码爆破	针对性主机密码爆破是明显针对用户的登录密码的暴力破解。通常黑客会无目标的破解主机密码，这种针对性的攻击往往暗示黑客想攻陷特定用户的资产。
撞库攻击	通过对异常登录分析，检测出类似撞库攻击的登录行为。黑客可能正在使用互联网上泄露的用户名密码组合尝试暴力登录用户的网站，一旦成功将会导致用户利益遭受损失。
CMS异常登录	检测到应用的管理后台存在的异地登录事件。如果本次登录不是用户本人操作，那么黑客可能已经窃取到后台密码，建议用户检查密码是否存在弱口令，并尽快修改现有密码。
扫描器攻击	检测黑客使用漏洞扫描工具扫描专有云平台中主机的行为，黑客发现漏洞后很可能对存在漏洞的主机发起针对性攻击。
pingback被恶意利用	检测攻击者利用pingback存在的漏洞发起的针对性攻击。
批量账号登录	检测攻击者使用大量的低质量账号登录的行为，而这批账号很可能是僵尸账号。

b) 选择已检测到的针对性攻击记录，单击**查看**，可查看该次攻击的详细信息及解决方案。

5.4.2 查看威胁攻击信息

操作步骤

1. 登录云盾控制台。
2. 定位到**态势感知** > **威胁分析**页面，选择**攻击**页签。
3. 查看应用攻击事件。

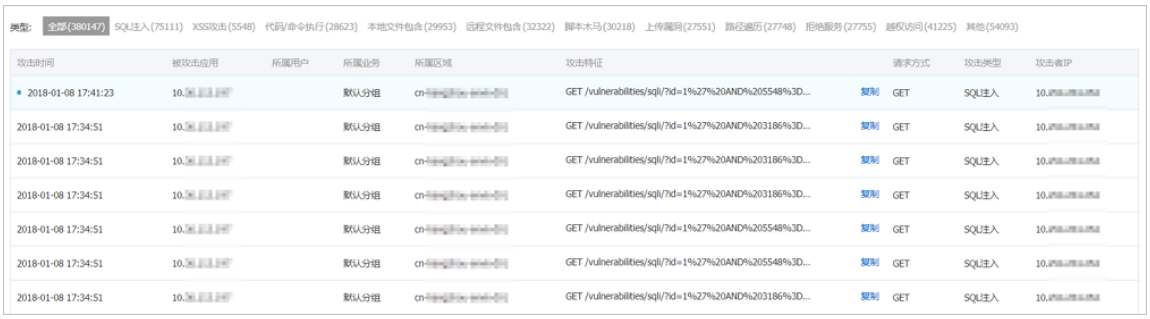
图 5-15: 最近7天攻击趋势及攻击类型

a) 单击**应用攻击**，并选择**所属区域**。

b) 查看最近7天检测到的攻击趋势、攻击类型信息。

c) 查看全部攻击事件的详细信息，如图 *5-16: 应用攻击事件记录*所示。

图 5-16: 应用攻击事件记录



在**类型**区域，单击具体攻击类型名称，可只展示对应攻击类型的攻击事件信息。各攻击类型说明参见表 *5-5: 应用攻击类型*。

表 5-5: 应用攻击类型

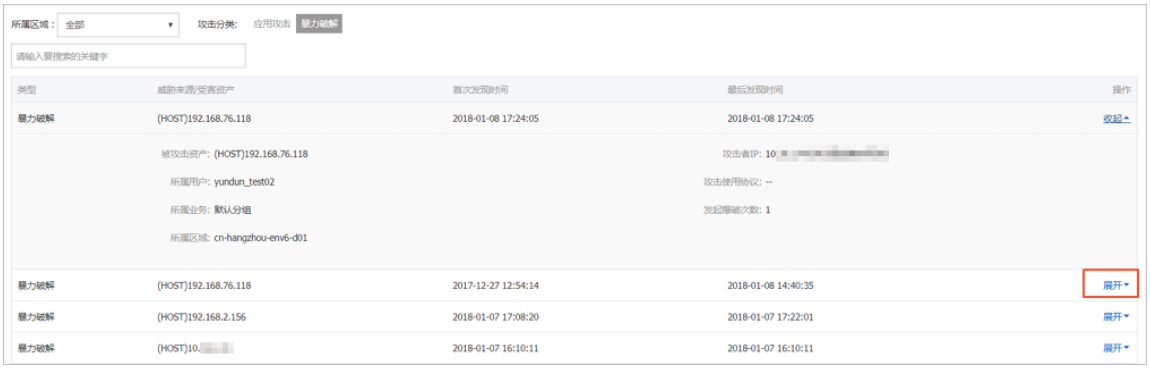
应用攻击类型	说明
SQL注入	Web应用程序没有对用户输入数据的合法性进行判断，攻击者通过Web页面的输入区域（如URL、表单等），用精心构造的SQL语句插入特殊字符和指令，通过和数据库交互获得私密信息或者篡改数据库信息。
XSS攻击	Web应用程序时没有对用户提交的语句和变量进行过滤或限制，攻击者通过Web页面的输入区域向数据库或HTML页面中提交恶意代码，当用户打开有恶意代码的链接或页面时，恶意代码通过浏览器自动执行，从而达到攻击的目的。
代码/命令执行	攻击者通过URL发起请求，在Web服务器端执行未授权的代码或命令，从而达到攻击的目的。
本地/远程文件包含	攻击者向Web服务器发送请求时，在URL添加非法参数，Web服务器端程序变量过滤不严，把非法的文件名作为参数处理。这些非法的文件名可以是服务器本地的某个文件，也可以是远端的某个恶意文件。由于这种漏洞是由PHP变量过滤不严导致的，所以只有基于PHP开发的Web应用程序才有可能存在文件包含漏洞。
脚本木马	webshell，以ASP、PHP、JSP等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。攻击者在入侵了一个网站后，通常会将ASP或PHP后门文件与网站服务器WEB目录下正常的网页文件混在一起，然后就可以使用浏览器来访问ASP或者PHP后门，得到一个命令执行环境，以达到控制网站服务器的目的。
上传漏洞	Web应用程序在处理用户上传的文件时，没有判断文件的扩展名是否在允许的范围内，或者没检测文件内容的合法性，就把文件保存在服务器上，甚至上传脚本木马到Web服务器上，直接控制Web服务器。
路径遍历	攻击者向Web服务器发送请求，通过在URL中或在有特殊意义的目录中附加`../`及其变形，导致攻击者能够访问未授权的目录，或者在Web服务器的根目录以外执行命令。
拒绝服务	其目的在于使目标主机的网络或系统资源耗尽，使服务暂时中断或停止，导致其正常用户无法访问。
越权访问	应用在检查授权时存在纰漏，使得攻击者可以利用一些方式绕过权限检查，访问或者操作到原本无权访问的代码。
其他	其他一些应用攻击类型。

4. 查看暴力破解事件。

   a) 单击**暴力破解**，并选择**所属区域**。

   b) 查看暴力破解事件记录，如图 *5-17: 暴力破解页面*所示。

   图 5-17: 暴力破解页面



   c) 选择暴力破解事件事件，单击**展开**，可查看该暴力破解事件的详细信息。

5.5 漏洞扫描

漏洞扫描页面主要展示系统中存在的漏洞和缺陷。这些弱点有可能被黑客利用，进行非法的操作，需要安全管理员及时消除弱点，提升系统的安全性。

漏洞扫描页面主要包括以下三类弱点：

- **漏洞**
  - 应用漏洞：弱点分析模块依赖扫描引擎具备的规则对云服务器上安装的应用程序进行扫描，并上报发现的缺陷信息。
  - 主机漏洞：扫描主机系统中自身存在的漏洞，由安骑士模块检测到并上报。
- **弱口令**：检测用户资产中简单的、容易被人猜测到或破解的口令，以便提醒安全管理员及时修改用户名和密码，提升用户密码的复杂度。

  弱口令对于用户系统来说是巨大的安全隐患，建议在对系统和应用设置账户的时候，尽可能的增加密码的复杂度（例如，密码中必须包含数字、字符、特殊字符，增加密码的长度等等），同时对密码进行分级管理；针对重要密码（例如SSH登录的用户名和密码），必须增加复杂度，同时定期进行更换。

  自定义弱口令：对于不同的用户，除了通用用户名和密码，还可能由于用户特点采用特定的用户名和密码，云盾支持用户自定义弱口令规则，可以将用户经常使用的用户名和密码添加到弱点分析模块的扫描规则中，实现对用户系统个性化的弱口令扫描。

- **配置项检测**：如果用户的系统配置文件或者敏感文件存放位置不当，攻击者可能在未授权的情况下获得这些文件，导致用户关键信息的泄露。弱点分析模块对用户系统中的配置文件进行扫描，并提示可能被未授权访问的配置项文件。

5.5.1 查看漏洞信息

背景信息

漏洞分为应用漏洞和主机漏洞：

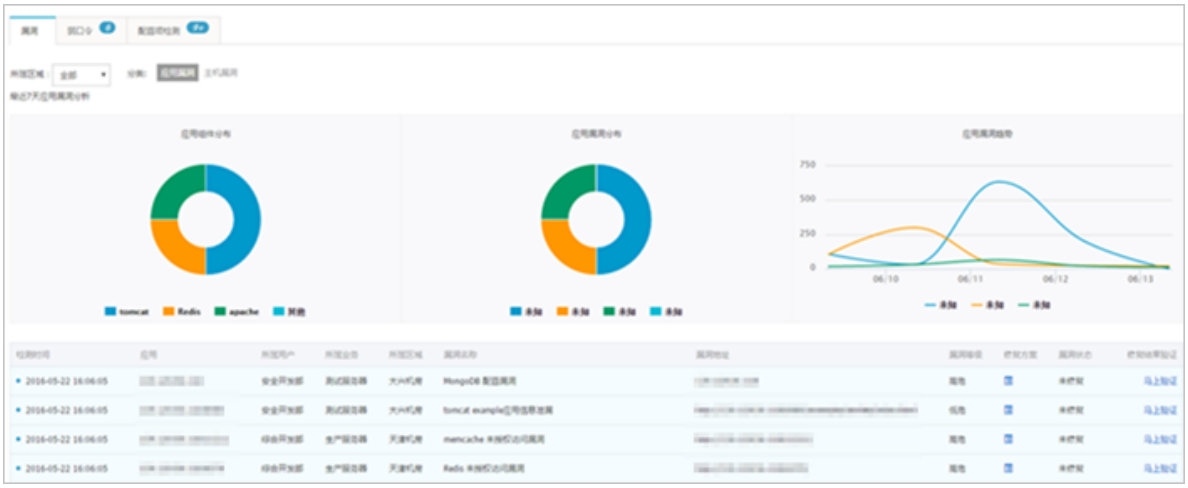
- 应用漏洞是指安装的应用程序存在的漏洞，由漏扫模块扫描并上报。
- 主机漏洞是主机本身存在的漏洞信息，由安骑士模块扫描并上报。

操作步骤

1. 登录云盾控制台。
2. 定位到**态势感知 > 漏洞扫描**。
3. 选择**所属区域**，查看该区域的漏洞信息。
4. 选择**应用漏洞**分类，查看并修复应用漏洞。

   应用漏洞页面显示最近七天的应用漏洞分析和具体的应用漏洞信息，如*图 5-18: 应用漏洞页面*所示。

   图 5-18: 应用漏洞页面

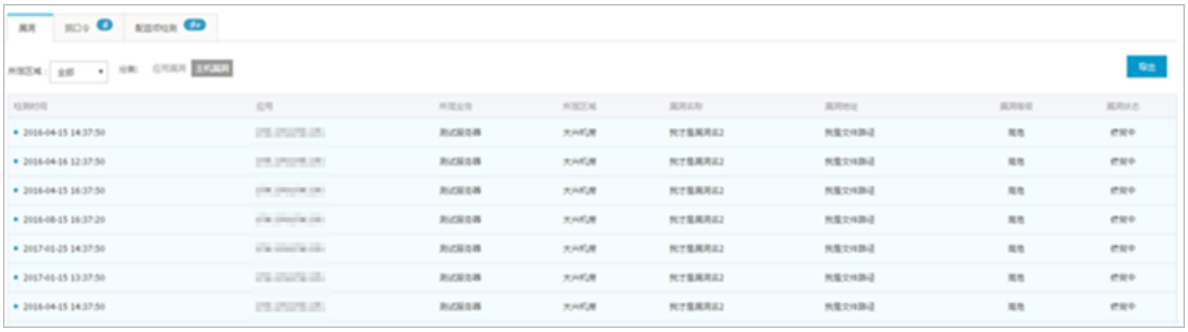


   a) 在应用漏洞记录区域，选择云盾检测到的应用漏洞记录，单击相应的修复方案按钮，可查看针对该漏洞的推荐修复方案。

   b) 漏洞修复完成后，单击**马上验证**，可以向弱点分析模块发出验证信息，立即校验当前漏洞的修复状态。

5. 选择**主机漏洞**分类，查看主机漏洞信息，如图 *5-19: 主机漏洞页面*所示。

图 5-19: 主机漏洞页面



在**主机漏洞**页面，单击右上方的**导出**，可将云盾检测到的主机漏洞记录导出到本地。

> **说明**：
> 此页面的主机漏洞信息由安骑士模块上报，对主机漏洞的具体操作请参见漏洞管理。

5.5.2 查看弱口令信息

操作步骤

1. 登录云盾控制台。
2. 定位到**态势感知** > **漏洞扫描**。
3. 选择**弱口令**，查看已检测到的弱口令信息，如。图 *5-20: 弱口令页面*所示。

图 5-20: 弱口令页面

4. 选择发现的弱口令记录，单击**展开**，查看详细信息，如图 *5-21: 弱口令详细信息*所示。

图 5-21: 弱口令详细信息

5. 单击**忽略**，可忽略该弱口令提示，且针对该弱口令将不再检测上报。

   选择查看已忽略的弱口令记录，单击**恢复**，即可恢复对该弱口令的检测。

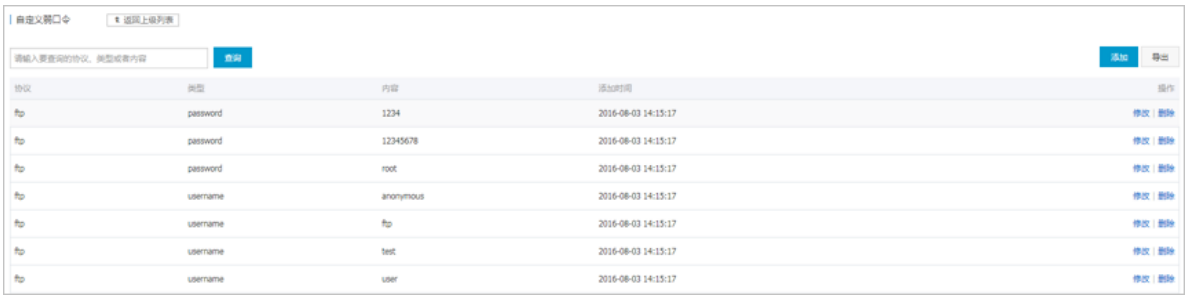
5.5.3 添加自定义弱口令

云盾支持自定义弱口令规则，可以将用户经常使用的用户名和密码添加到弱点分析模块的扫描规则中，发现特定的弱口令。

操作步骤

1. 登录云盾控制台。
2. 定位到**态势感知** > **漏洞扫描**，选择**弱口令**页签。
3. 单击**自定义弱口令**，可自定义针对性的弱口令规则，如图 *5-22: 自定义弱口令页面*所示。

   图 5-22: 自定义弱口令页面



   自定义弱口令页面显示目前弱点分析模块已经配置生效的弱用户名和弱密码。

4. 单击**添加**，在**添加弱口令**对话框中设置弱口令规则，如图 *5-23: 添加弱口令对话框*所示。

图 5-23: 添加弱口令对话框

5. 单击**确定**，并再次在**提示**弹窗中单击**确定**。
6. 检查已添加的弱口令规则。
   - 单击**修改**，修改弱口令或弱用户名内容。
   - 单击**删除**，删除不需要的弱口令规则。
7. 单击**导出**，生成并下载新的弱口令配置文件。

> **说明**：
> 一般情况下，文件保存路径为`C:\Users\`用户名`\Downloads`，下载的文件为zip格式的压缩包，无需进行解压。

8. 压缩包上传至弱点分析Cactus-keeper模块的master工程所在的系统，例如上传到`/root/war/`目录下，执行脚本`cactusConfig.sh`，如图 5-24: 执行脚本界面所示。

图 5-24: 执行脚本界面

```
[root@spark2 cactusConfig]# ./cactusConfig.sh
975550d3af6d
/root/war
Archive:  cactus_config_2016-10-28.zip
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_ftp_user.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_ftp_psw.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_mysql_user.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_mysql_psw.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_ssh_user.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_ssh_psw.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_mssql_user.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_mssql_psw.txt
65c5671c8259
cactus_config_2016-10-28.zip
Archive:  /home/datal/yundun/cactus-keeper/cactus_config.zip
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_ftp_user.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_ftp_psw.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_mysql_user.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_mysql_psw.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_ssh_user.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_ssh_psw.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_mssql_user.txt
  inflating: /home/datal/yundun/cactus-keeper/cactus_config/dic_mssql_psw.txt
commad.sh
done!
[root@spark2 cactusConfig]#
```

脚本执行完成后，新添加的弱口令规则即生效。

5.5.4 查看配置项检测结果

配置项检测页面显示弱点分析模块扫描到的配置项泄露的地址。

背景信息

黑客在未授权的情形下访问该地址，可能获取用户的敏感信息，造成信息泄露。安全管理员需要根据扫描检测结果，及时对存放有配置文件的目录添加权限或者将敏感文件转移至安全目录。

操作步骤

1. 登录云盾控制台。
2. 定位到**态势感知** > **漏洞扫描**。
3. 选择**配置项检测**页签，查看已检测到的配置项弱点，如图 *5-25:* 配置项检测页面所示。

图 5-25: 配置项检测页面

4. 选择发现的配置项弱点记录，单击**展开**，查看详细信息，如图 *5-26:* 配置项弱点详细信息所示。

图 5-26: 配置项弱点详细信息

5. 单击**忽略**，可忽略该配置项弱点提示，且针对该配置项将不再检测上报。

   选择查看已忽略的配置项记录，单击**恢复**，即可恢复对该配置项的检测。

6 网络安全

6.1 DDoS防护

DDoS（Distributed Denial of Service），即分布式拒绝服务。DDoS攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。

常见的DDoS攻击包括以下几类：

- **网络层攻击**：比较典型的攻击类型是UDP反射攻击，例如：NTP Flood攻击，这类攻击主要利用大流量拥塞被攻击者的网络带宽，导致被攻击者的业务无法正常响应客户访问。
- **传输层攻击**：比较典型的攻击类型包括SYN Flood攻击、连接数攻击等，这类攻击通过占用服务器的连接池资源从而达到拒绝服务的目的。
- **会话层攻击**：比较典型的攻击类型是SSL连接攻击，这类攻击占用服务器的SSL会话资源从而达到拒绝服务的目的。
- **应用层攻击**：比较典型的攻击类型包括DNS flood攻击、HTTP flood攻击、游戏假人攻击等，这类攻击占用服务器的应用处理资源极大的消耗服务器处理性能从而达到拒绝服务的目的。

云盾可以对攻击流量进行牵引、清洗和回注，提供对DDoS攻击的防御，保证业务正常进行。

6.1.1 查看DDoS事件

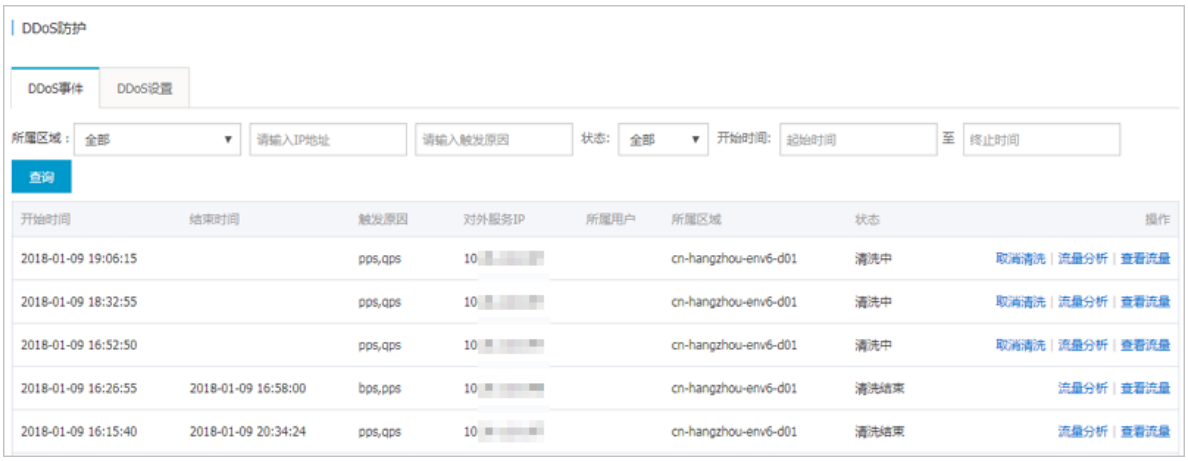
云盾在进行流量清洗或流量清洗结束，会上报安全事件到云盾安全中心。通过本章节可以查看到DDoS事件。

操作步骤

1. 登录云盾控制台。
2. 定位到**网络安全** > **网络防护**，选择**DDoS事件**页签。

   进入DDoS事件列表，如图 *6-1: DDoS事件页面*所示。

图 6-1: DDoS事件页面



3. 设置查询条件，单击**查询**。

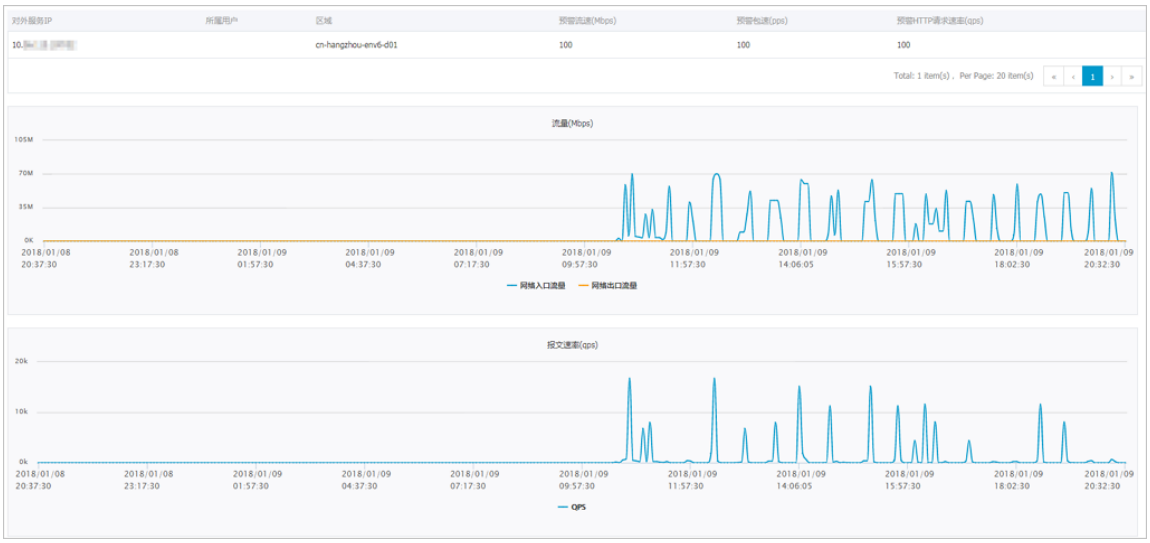
   可根据查询条件返回满足条件的DDoS事件信息。

信息列	说明
触发原因	表示DDoS攻击流量中哪一指标超过了设置的预警阈值。
对外服务IP	表示受到DDoS攻击的IP。
状态	• 清洗中：表示正在进行流量清洗。 • 清洗结束：表示流量清洗已经结束。
操作	• 取消清洗：手动停止流量清洗。 • 流量分析：查看DDoS事件中流量协议和Top10主机。 • 查看流量：查看预警阈值和流量图。

4. 查看和分析DDoS事件。

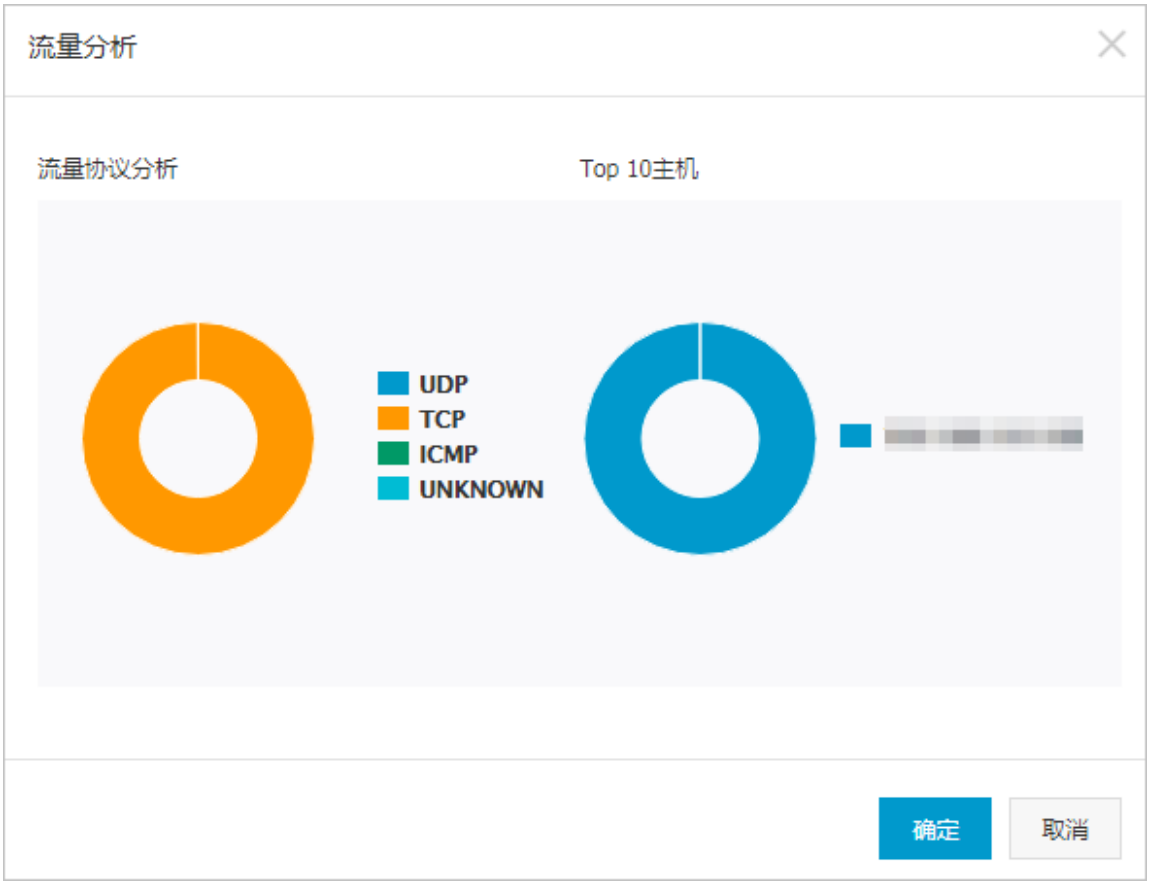
   - 单击**查看流量**，查看对应IP当前的设置阈值及流量图，如图 *6-2:* 流量视图所示。

图 6-2: 流量视图



- 单击**流量分析**，查看当前攻击事件的流量成分、Top10攻击机分析，如图 *6-3:* 流量分析页面所示。

图 6-3: 流量分析页面



6.1.2 DDoS防护策略

DDoS流量报警阈值即当访问该IP的流量达到阈值后触发流量报警。IP的阈值设置通常以流量作为依据，当流量过大时，表示可能受到DDoS攻击。

阈值一般建议设置为比流量的高峰期值稍大即可。

云盾支持全局阈值设置、网段阈值设置和单个IP地址阈值设置三种方式：

- **全局阈值**：全局阈值无法添加，默认值在服务初始化时通过导入实现。
- **网段阈值**：根据网段的流量，设置待设定网段的报警阈值。网段阈值设置方式相对全局阈值能更精准地设置对应网段的报警阈值。
- **单个IP地址阈值**：根据每个IP地址的流量，分别设置对应的报警阈值。单个IP地址阈值的设置方式相对网段阈值能更精准的设置每个IP的报警阈值。

6.1.2.1 设置预警阈值

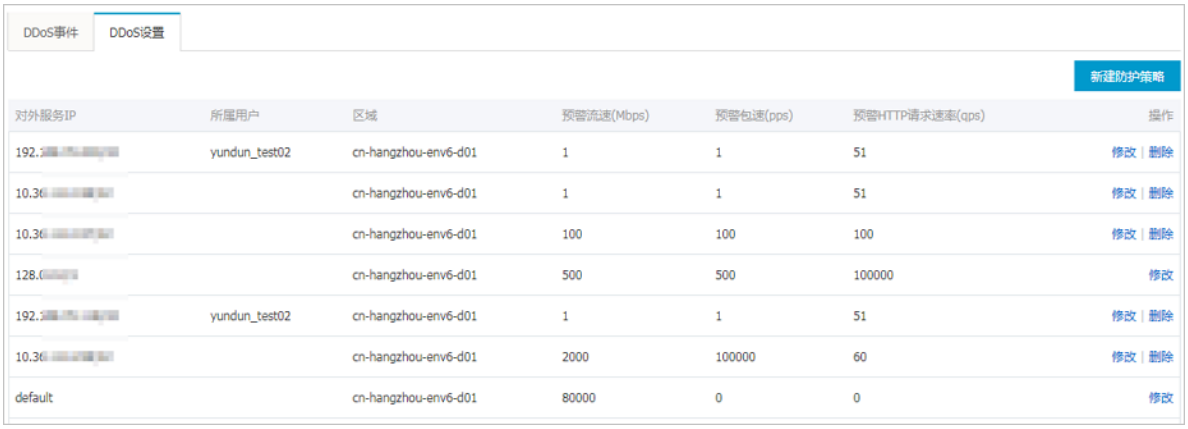
单独对一个网段或一个IP设置阈值时，以该阈值为准触发DDoS检测，否则按照全局阈值触发DDoS检测。

操作步骤

1. 登录云盾控制台。
2. 定位到**网络安全** > **网络防护**，单击**DDoS设置**。

   进入DDoS设置页面，如图 *6-4:* 阈值列表所示。

   图 6-4: 阈值列表



对外服务IP	所属用户	区域	预警流速(Mbps)	预警包速(pps)	预警HTTP请求速率(qps)	操作
192.[redacted]	yundun_test02	cn-hangzhou-env6-d01	1	1	51	修改 | 删除
10.3[redacted]		cn-hangzhou-env6-d01	1	1	51	修改 | 删除
10.3[redacted]		cn-hangzhou-env6-d01	100	100	100	修改 | 删除
128.[redacted]		cn-hangzhou-env6-d01	500	500	100000	修改
192.[redacted]	yundun_test02	cn-hangzhou-env6-d01	1	1	51	修改 | 删除
10.3[redacted]		cn-hangzhou-env6-d01	2000	100000	60	修改 | 删除
default		cn-hangzhou-env6-d01	80000	0	0	修改

3. 单击**新增防护策略**。
4. 在**新增防护策略**对话框中，设置预警参数，如图 *6-5:* 新增防护策略对话框所示。

图 6-5: 新增防护策略对话框

参数	说明
IP地址	设置预警的IP地址或网段。 **说明**： 添加阈值时，务必确认对应的网段已在流量采集网段设置中添加。
预警流速	设置机房中带宽报警阈值。当机房入+出流量速率达到该值时，即触发DDoS检测。一般根据业务实际使用带宽值设置，比峰值略大即可，建议阈值至少设置为100 Mbps以上。 带宽单位为：Mbps（兆比特 / 秒）
预警包速	设置机房包速率报警阈值。当机房入+出包速率达到该值时，即触发DDoS检测。一般根据业务实际使用包速率设置，比峰值略大即可，建议阈值至少设置为20000 pps以上。 包速率单位为： pps（包个数 / 秒）
预警HTTP请求速率	设置机房主机收到的HTTP请求速率报警阈值。当机房入+出HTTP请求速率达到该值时，即触发DDoS检测。一般根据业务实际情况设置，比峰值略大即可，建议阈值至少设置为100000 qps以上。 HTTP请求速率单位为：qps（请求个数 / 秒）

5. 单击**确定**。

6.1.2.2 管理预警阈值

操作步骤

1. 登录云盾控制台。
2. 定位到**网络安全** > **网络防护**，单击**DDoS设置**。
3. 管理已添加的防护策略。
   - 单击**修改**，在弹出的**修改防护策略**的对话框中，输入对应的阈值后单击**确定**，修改预警阈值。
   - 单击**删除**，删除该预警阈值。

> **说明**：
> 系统默认阈值无法删除。

6.2 启用网络安全阻断功能

操作步骤

1. 登录云盾控制台。
2. 定位到**网络安全** > **安全功能设置**。
3. 单击web攻击阻断、暴力破解阻断开关，开启或关闭相关功能，如图 *6-6:* 阻断开关设置所示。

> **说明**：
> 关闭阻断开关后，相应的拦截功能将被禁用，仅提供预警功能。

图 6-6: 阻断开关设置

6.3 云防火墙

云防火墙是一款针对云环境的防火墙安全产品，主要解决云上业务快速变化带来的安全边界模糊甚至无法定义的问题。云防火墙模块能够帮助安全管理员完成专有云环境中云服务器的业务分区和隔离策略的部署。

6.3.1 开始之前

当您需要配置云防火墙前，需要角色授权。

1. 创建云防火墙服务对应的Ram角色，具体请参见《用户指南》中**RAM管理**一节。
2. 定位到**云管控中心** > **云基础产品** > **云盾控制台**，单击**立即授权**，把用户所属部门添加到已授权部门中。

在进行云防火墙配置之前，安全管理员需要根据实际业务情况准备以下规划信息：

- 所需业务区，例如，测试区、开发区等。
- 每个业务区所需的服务器角色，例如，Web应用（Web）、数据库（DB）等。
- 确定ECS云服务器与业务区及服务器角色组之间的对应关系，即每台ECS云服务器需要被划分至哪个业务区以及角色分组中。

6.3.2 拓扑图图例说明

图例

在云防火墙拓扑图中，通过以下图形和颜色标识拓扑图中的各个要素信息。

说明：

在云防火墙拓扑图中，将鼠标移至流量线上可以通过观察虚线的流动情况来判断流量的访问方向，虚线的流动方向即是该流量的访问方向。

流量线筛选

云防火墙拓扑图提供多种筛选方式，通过隐藏/显示部分流量线的方式帮助您在拓扑图中找到您需要重点观察的流量线。

- **流量线类型筛选**：

  勾选或取消**业务区之间**、**业务区之内**、**外网入方向**和**出方向**，可设置是否在拓扑图中显示相应类型的流量线。

- **流量线颜色筛选**：

  单击**更多**，勾选或取消**绿色流量线**、**红色流量线**或**灰色流量线**，可设置是否在拓扑图中显示相应状态的流量线。

  在**端口**中输入端口号，单击**确定**，自定义设置在拓扑图中不显示与所输入端口相关的流量线。

  在**更多**下拉菜单中勾选**角色组名**，可在拓扑图中的业务分区内显示具体的角色组名称。

- **时间范围筛选**：

  单击时间范围筛选框，选择时间范围，在拓扑图中将显示指定时间范围内的流量线。

展现方式

云防火墙拓扑图提供多种展现方式，您可以根据实际情况自由切换展现方式。

- **业务区展现方式**：

单击相应的业务区展现方式按钮即可切换展现方式。

- **东西向**： 业务区以东西向的方式进行排列展示。在业务区较多的情况下，可以单击拓扑图左侧或右侧的箭头查看其它业务区；将鼠标移至业务区，单击业务区下方的左移、右移箭头可以调整业务区的排列顺序。

  通过东西向的展现方式，可以帮助您集中观察部分业务区的关联流量信息。
- **列表**： 在拓扑图中展示所有业务区。通过列表的展现方式，可以帮助您全局地了解所有业务区的关联流量信息。

- **流量线展现粒度**：

  单击相应的流量线展现粒度按钮即可切换流量线的展现粒度，包括**业务区**、**角色组**、**主机**三种粒度，您可以根据实际情况选择拓扑图中流量线的展现粒度。

6.3.3 建立业务区

在云防火墙控制台中新建业务区。

操作步骤

1. 登录云盾控制台。
2. 定位到**网络安全** > **云防火墙**，进入云防火墙控制台。
3. 选择需要管理的云服务器所属的区域和专有网络（VPC），如图 *6-7: 选择区域及网络*所示。

   图 6-7: 选择区域及网络

4. 单击**新建业务区**，如图 *6-8: 新建业务区*所示。

图 6-8: 新建业务区

说明：

如果在该VPC环境中已创建过业务分区，请在页面上方的菜单栏中单击**新建业务**。

5. 填写业务区名称，选择业务区标签。如图 *6-9: 创建业务区*所示。

图 6-9: 创建业务区

6. 单击**确定**。

6.3.4 导入ECS云服务器

在业务区中导入ECS云服务器。

操作步骤

1. 登录云盾控制台。
2. 定位到**网络安全** > **云防火墙**，进入云防火墙控制台。

3. 在**云防火墙拓扑图**页面，选择需要管理的业务区所属的区域，以及所属专有网络（VPC）的名称。
4. 将鼠标移至已创建的业务区，显示操作按钮，如图 *6-10: 操作按钮*所示。

图 6-10: 操作按钮

5. 单击添加资产按钮 ，打开**添加资产**窗口。
6. （可选）设置搜索条件，单击**搜索**。

   通过设置公网IP、实例名和标签搜索条件，可以快速搜索需要的服务器。
7. 选择需要添加的服务器，单击**立即添加**，如图 *6-11: 添加资产*所示。

图 6-11: 添加资产

6.3.5 建立角色组，将已导入的ECS云服务器分组

在云防火墙业务区中建立角色组，并将已导入的ECS云服务器进行角色分组。

6.3.5.1 将已明确角色的ECS云服务器进行分组

建立角色组，并将已导入的具有明确角色的ECS云服务器进行分组。

操作步骤

1. 登录云盾控制台。
2. 定位到**网络安全** > **云防火墙**，进入云防火墙控制台。
3. 在**云防火墙拓扑图**页面，选择需要管理的业务区所属的区域，以及所属专有网络（VPC）的名称。
4. 将鼠标移至已创建的业务区，显示操作按钮，如图 *6-12: 操作按钮*所示。

   图 6-12: 操作按钮

5. 单击用户管理按钮 ，打开**角色管理**页面。
6. 单击源角色组旁的添加角色组按钮（+），新建角色组，如图 *6-13: 新建角色组*所示。

   图 6-13: 新建角色组

7. 填写角色组名，单击**确定**。
8. 根据访问源中的ECS云服务器信息，为ECS云服务器选择已创建的源角色组，如图 *6-14: 分配角色组*所示。

图 6-14: 分配角色组

6.3.5.2 将未明确角色的ECS云服务器进行分组

对于未明确角色的ECS云服务器，参考以下操作步骤使用云防火墙提供的流量可视化功能，明确每一台ECS云服务器的角色。

操作步骤

1. 登录云盾控制台。
2. 定位到**网络安全** > **云防火墙**，进入云防火墙控制台。
3. 在**云防火墙拓扑图**页面，选择需要管理的云服务器所属的区域，以及所属专有网络（VPC）的名称。
4. 简化拓扑网络。
   - **流量线范围筛选**：

根据实际业务情况在拓扑图上方仅勾选需要显示的流量线，从而简化拓扑图。

您也可以单击**更多**，勾选是否显示特定类型的流量线，或者自定义不显示特定端口的流量线。

同时，您还可以单击时间维度选择所显示的流量线的时间范围。

- **智能搜索**：

通过设定搜索规则显示或不显示某个业务区或某个角色组的特定流量线。

说明：

智能搜索提供了强大的搜索规则功能，来实现过滤不相关流量信息的显示效果。智能搜索规则可以组合执行，采用自上而下的匹配顺序；每条规则都可单独设定是否显示符合规则条件的流量线。

1. 单击拓扑图右上方的**智能搜索**。
2. 单击**添加规则**，设置智能搜索规则，如图 *6-15:* 自定义搜索规则所示。

图 6-15: 自定义搜索规则

- 最多可以定义10条搜索规则，并且系统默认有一条缺省规则。
- 通过左侧的勾选框决定搜索规则是否生效，缺省规则无法取消勾选。

3. 勾选需要使用的智能搜索规则，单击**保存并执行**。

- **单服务器查看**：

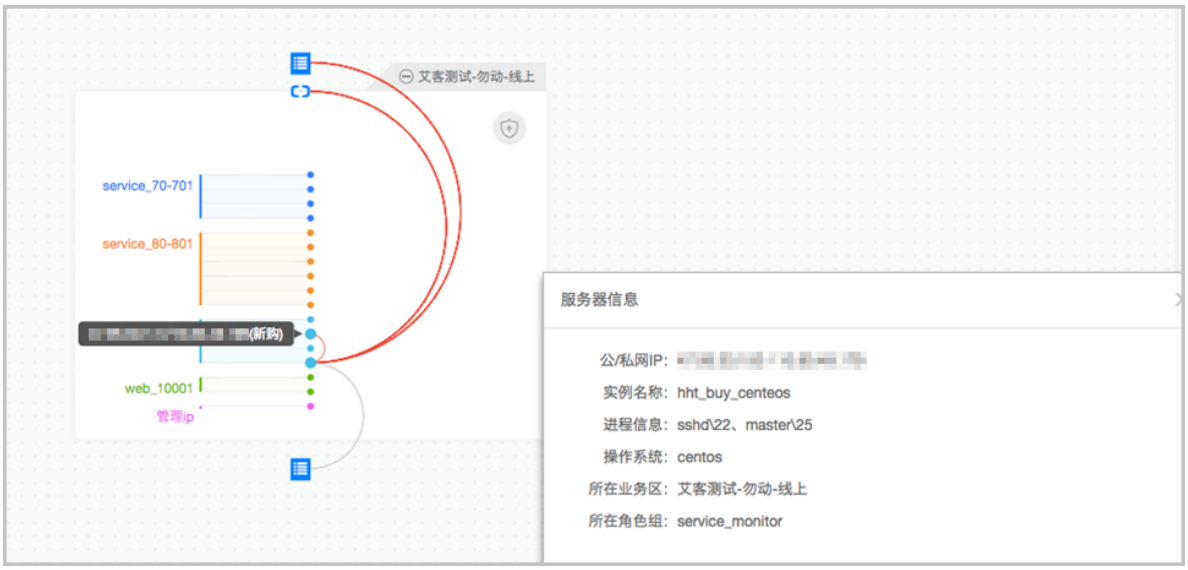
  在拓扑图中，单击某台服务器，可以查看该服务器的相关信息及与该服务器相关的流量线，其它的流量线信息将不显示。

5. 在业务区中，将鼠标悬停在ECS云服务器的节点上，查看该ECS云服务器的服务器信息，如图 *6-16:* 查看服务器信息所示。

图 6-16: 查看服务器信息

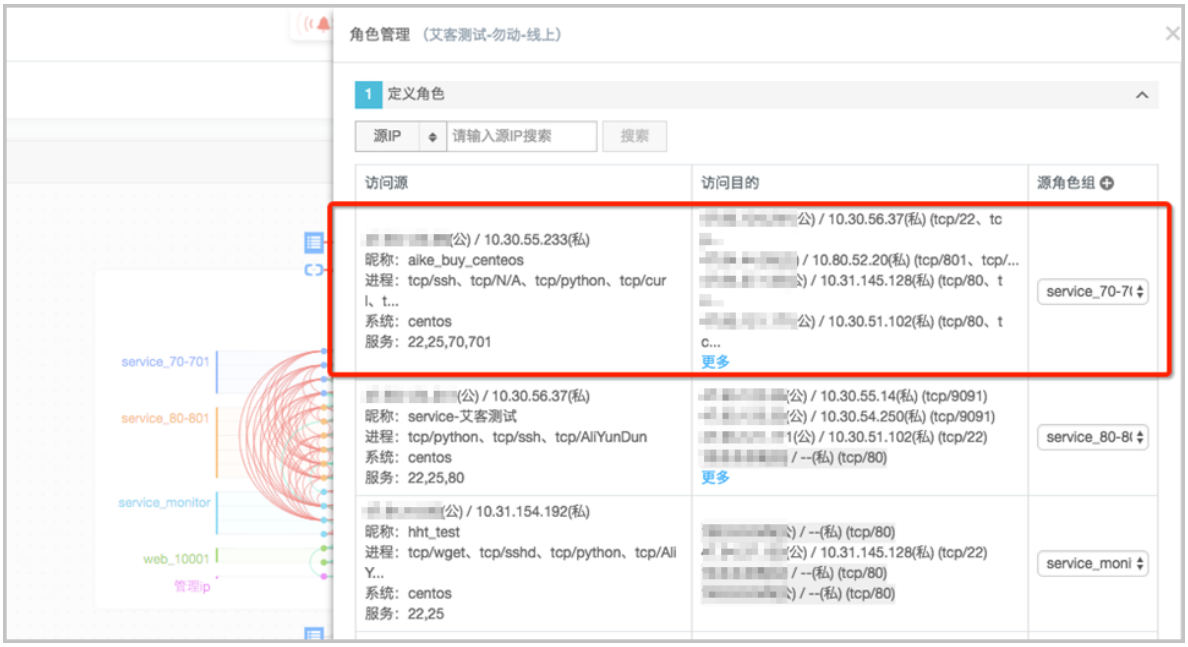
6. 单击ECS云服务器节点，查看该ECS云服务器与其他服务器之间的访问关系，如图 *6-17:* 查看服务器之间访问关系所示。

图 6-17: 查看服务器之间访问关系



7. 在**角色管理**页面中，通过查看本业务区所有ECS资产的服务器信息、及ECS资产与其他服务器的访问关系，判断该ECS资产的应属角色组，如图 *6-18: 通过角色管理查看服务器之间访问关系*所示。

图 6-18: 通过角色管理查看服务器之间访问关系



6.3.6 审核流量（部署访问控制策略）

在云防火墙控制台中，逐一审核流量的合法性、部署访问控制策略。

背景信息

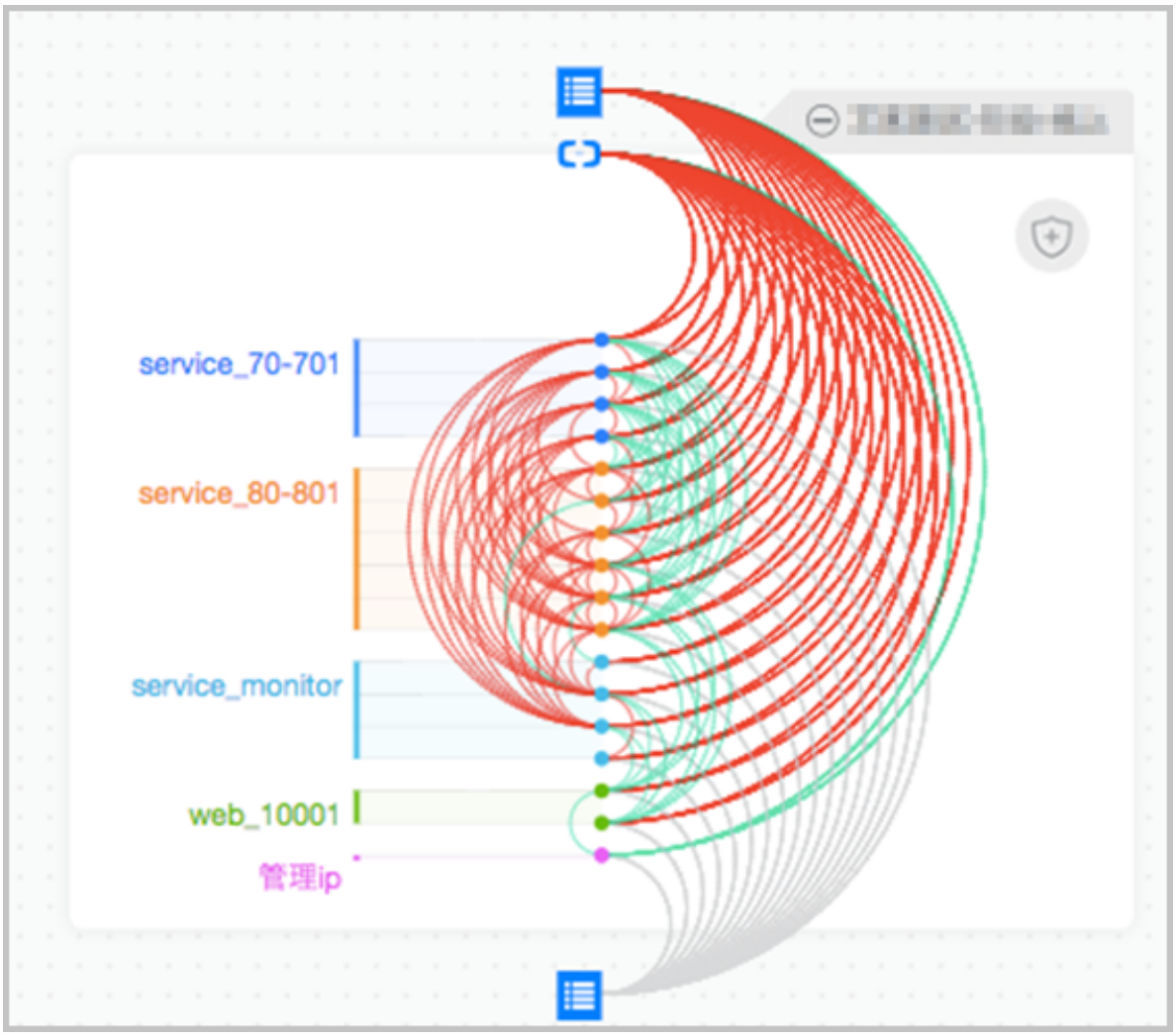
只要业务区没有发布，在该业务区上的所有操作、策略部署并不会真实发布，更不会影响实际业务。

操作步骤

1. 登录云盾控制台。
2. 定位到**网络安全** > **云防火墙**，进入云防火墙控制台。
3. 在**云防火墙拓扑图**页面，选择需要部署的业务区所属的区域，以及所属专有网络（VPC）的名称。
4. 在业务区中查看流量线条。

   未审核流量线默认都是红色线条，需要逐条确认该流量的合法性，如图 *6-19:* 审核流量线条所示。

图 6-19: 审核流量线条



5. （推荐）通过流量线审核，定义相应的白名单访问控制策略。

> **说明**：
> 审核通过后的流量将会显示为绿色。

a) 单击红色流量线。

b) 对该流量线进行放行或拒绝操作，如图 *6-20: 对流量线定义访问控制策略*所示。

图 6-20: 对流量线定义访问控制策略

6. 手动添加访问策略。

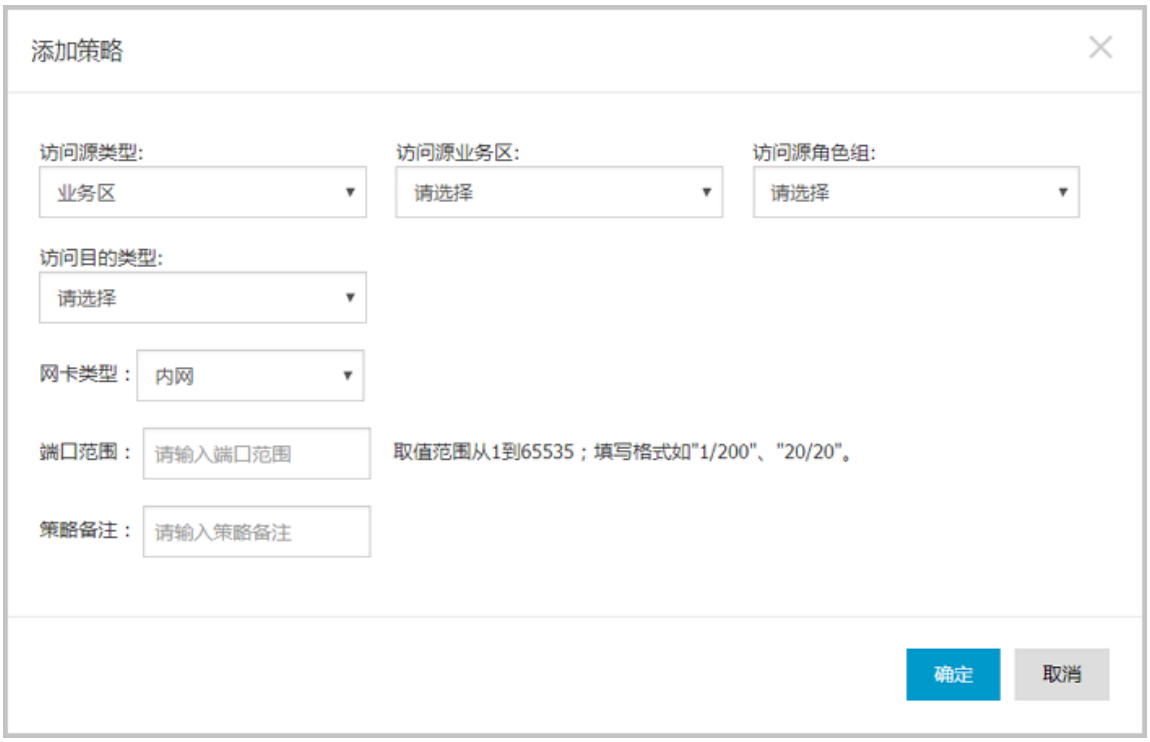
> **说明**：
> 建议通过对拓扑图中可视化的具体流量线操作的方式定义访问控制策略，参见步骤5。

- 在角色管理页面中的建立策略区域，单击**添加**，直接添加相应的访问控制策略，如图 *6-21: 添加访问控制策略*所示。

图 6-21: 添加访问控制策略

- 单击拓扑图右上方的**添加策略**，手动添加访问控制策略，如图 *6-22: 手动添加访问控制策略*所示。

图 6-22: 手动添加访问控制策略



6.3.7 发布业务区（下发访问控制策略）

完成访问控制策略部署后，将该业务区进行发布。

操作步骤

1. 登录云盾控制台。
2. 定位到**网络安全** > **云防火墙**，进入云防火墙控制台。
3. 在**云防火墙拓扑图**页面，选择您想要发布的业务区所属的区域，以及所属专有网络（VPC）的名称。
4. 单击页面右上方的**发布/生效/回滚**。
5. 选择发布模式，选择需要发布的业务区，单击**发布**。

> **说明**：
> 存在流量线关联的业务区必须一起发布，无法单独发布。

- **发布观察模式**：

在尚不完全确定该业务区的策略配置是否合理时，建议选择**发布观察模式**。在观察模式下，云防火墙中仅模拟流量与访问控制策略，不会对流量进行真实阻断。

业务区发布为观察模式后，您可以在一段时间后继续观察拓扑图中是否出现其它未被放行的正常业务流量线，并配置相应的访问控制策略。

- **发布拦截模式**：

  选择**发布拦截模式**，云防火墙将根据业务区中所有基于流量线、服务器或角色组配置的访问控制策略自动生成安全组规则。拦截模式发布成功后，所有不在白名单策略定义的流量都会被拦截。

  > **说明**：
  > 为了避免ECS实例原先所属的安全组的规则影响云防火墙的访问控制规则的效果，在将所有业务区以拦截模式发布后，您需要将所有ECS实例从原先的安全组中移出，在云防火墙中配置访问规则才能真正生效。

后续操作

在业务区以拦截模式发布后，如果所配置的访问控制策略导致正常业务被中断，您可以使用一键全通功能实现在特殊情况下为某个业务区提供临时性放行策略，从而为您争取更多的排查时间。

关于一键全通功能的详细说明，请参见临时使用一键全通功能。

6.3.8 临时使用一键全通功能

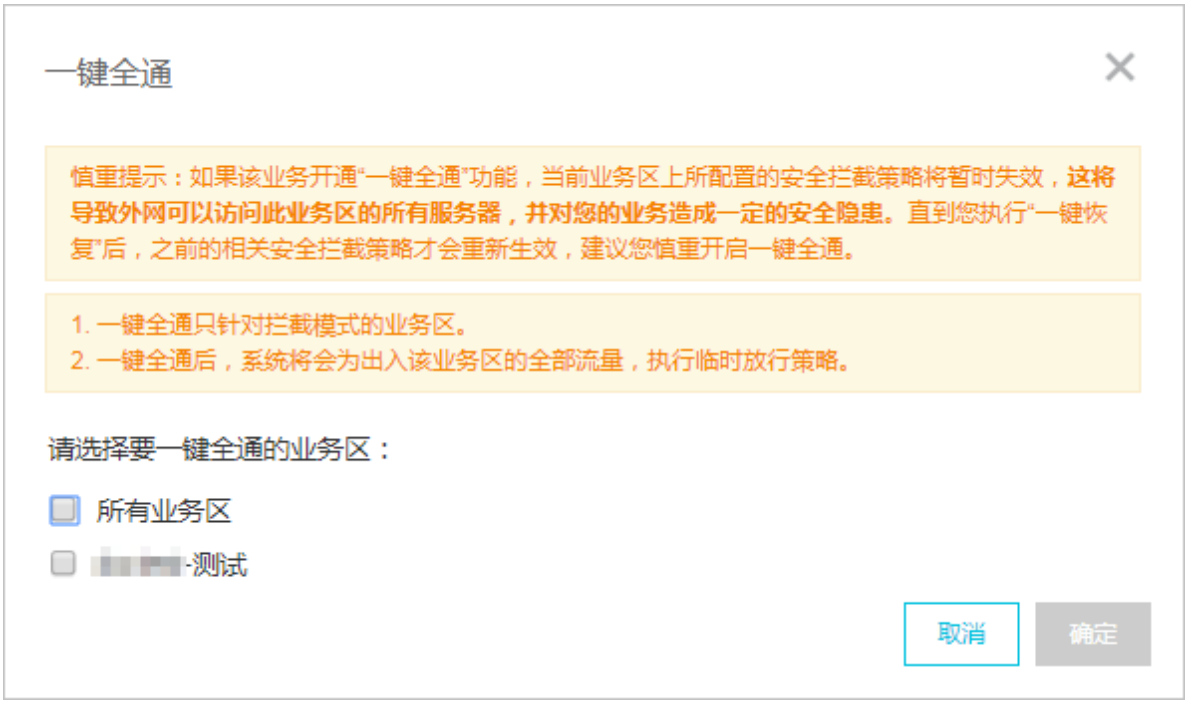
背景信息

业务区发布后，如果出现因防火墙策略配置导致的业务中断，可以参考以下操作步骤使用云防火墙的一键全通功能，为对应的业务区提供临时性放行策略的机制，从而争取更多的排查时间。

操作步骤

1. 登录云盾控制台。
2. 定位到**网络安全** > **云防火墙**，进入云防火墙控制台。
3. 在**云防火墙拓扑图**页面，选择相关业务区所属的区域，以及所属专有网络（VPC）的名称。
4. 单击页面右上方的**一键全通**。
5. 勾选需要一键全通的业务区，单击**确定**，如图 *6-23: 一键全通*所示。

图 6-23: 一键全通



6. 问题排查完成后，单击云防火墙拓扑图页面右上方的**一键恢复**，自动删除一键全通功能所增加的临时放行策略，恢复到业务区原有的策略配置。

6.3.9 管理云防火墙所有资源

安全管理员也可以在云防火墙控制台中的**资源列表**页面，对业务区、角色组、以及ECS云服务器资源进行管理。

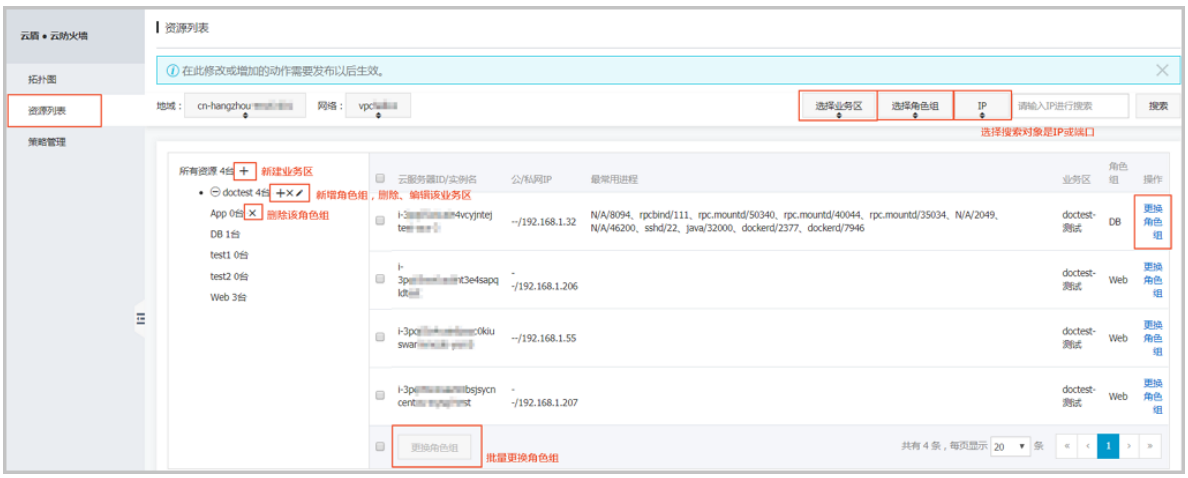
操作步骤

1. 登录云盾控制台。
2. 定位到**网络安全** > **云防火墙**，进入云防火墙控制台。
3. 在**云防火墙拓扑图**页面，单击左上方的**返回资源列表**，如图 *6-24: 返回资源列表*所示。

图 6-24: 返回资源列表

4. 选择需要管理的资源所属的区域，以及所属专有网络（VPC）的名称。
5. 在**资源列表**页面，管理云防火墙相关资源，如图 *6-25: 管理云防火墙资源*所示。

图 6-25: 管理云防火墙资源



说明：

在此页面进行的增加、修改的动作都需要发布相关业务区后才会生效。

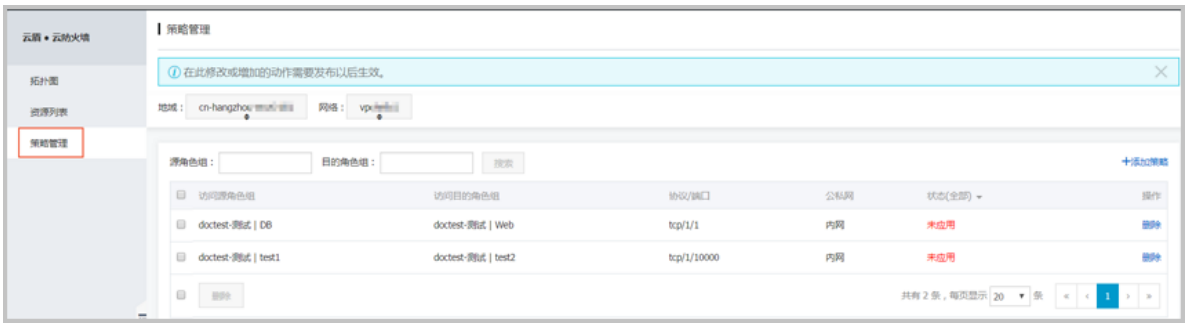
6.3.10 管理访问控制策略

业务区发布后，安全管理员可以在云防火墙控制台中的**策略管理**页面，查看并管理已创建的访问控制策略。

操作步骤

1. 登录云盾控制台。
2. 定位到**网络安全** > **云防火墙**，进入云防火墙控制台。
3. 在**云防火墙拓扑图**页面，单击左上方的**返回资源列表**。
4. 单击**策略管理**。
5. 在**策略管理**页面，选择想要查看或管理的策略所属的区域，以及所属专有网络（VPC）的名称。
6. 管理访问控制策略，如图 *6-26: 管理访问控制策略*所示。

图 6-26: 管理访问控制策略



说明：

在此页面进行的增加、修改的动作都需要发布相关业务区后才会生效。

- 查看或删除该网络区域内已配置的访问控制策略。
- 单击**添加策略**，手动添加访问控制策略。

说明：

建议通过对云防火墙拓扑图中可视化的具体流量线操作的方式定义访问控制策略。

策略项	说明
访问源	• 访问源类型为业务区：设置访问源业务区和角色组。 • 访问源类型为IP地址或网段：设置访问源IP段。
访问目的	• 访问目的类型为业务区：设置访问目的业务区和角色组。 • 访问目的类型为IP地址或网段：设置访问目的IP段。
网卡类型	设置网卡类型，即策略对哪个网卡的流量生效。
端口范围	设置端口范围，即策略对哪些端口的流量生效。
策略备注	设置策略备注。

7 应用安全

7.1 Web应用防火墙

Web应用防火墙 (简称WAF)，是阿里云自主研发的一款网站安全防护产品，它能够保护网站的应用程序避免遭受常见Web漏洞的攻击。这类攻击既有诸如SQL注入、XSS跨站脚本等常见 Web应用攻击，也有CC这种影响网站可用性的资源消耗型攻击。同时，它也允许根据网站实际业务制定精准的防护策略，用于过滤对您网站有恶意的Web请求。

专有云云盾WAF防护的流量定位在HTTP/HTTPS的网站业务上。支持用户在WAF的管理界面中自主导入证书与私钥，从而实现业务的全链路加密，避免数据在链路中被监听的可能。同时，也满足了对HTTPS业务的安全防护需求。

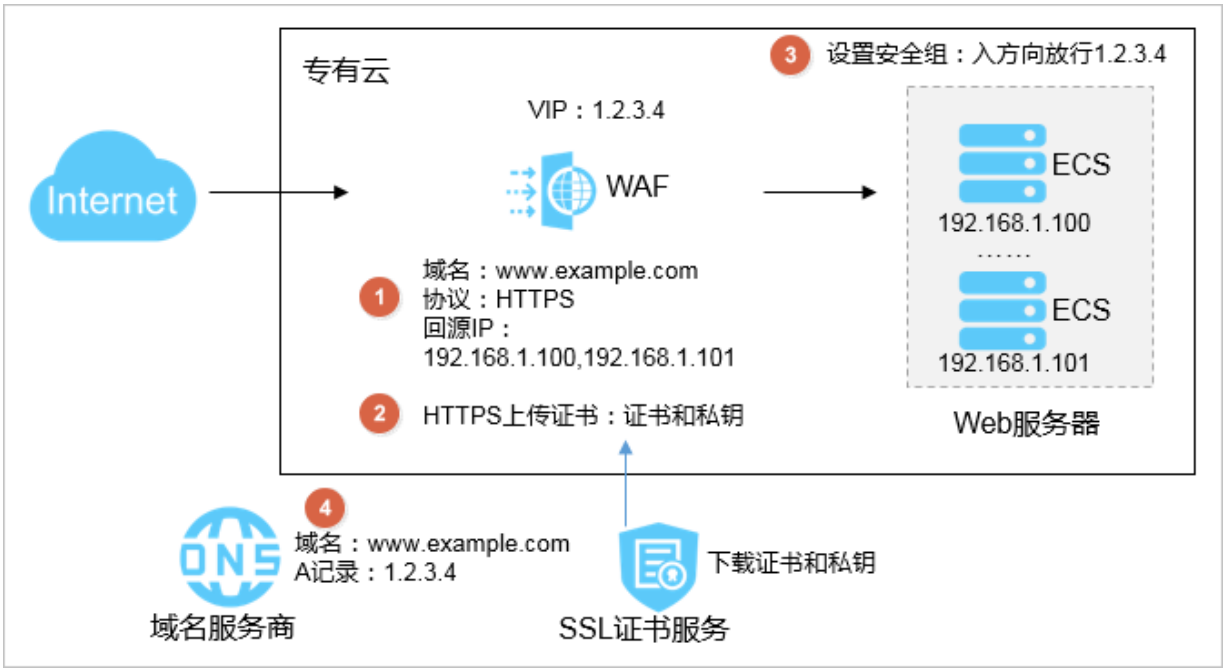
7.1.1 限制说明

Web应用防火墙存在以下使用限制：

- 支持最多100个域名的接入防护，支持泛域名，不限一二级域名。
- 仅支持HTTP 80端口、 HTTPS 443端口的域名防护。

7.1.2 配置域名接入

参考以下流程将需要防护的域名配置接入Web应用防火墙。



7.1.2.1 开始之前

在使用Web应用防火墙前，请准备以下信息：

- 需要防护的域名信息，不能直接使用IP。
- 源站IP，一般为真实服务器IP。

> **说明**：
> Web应用防火墙支持为同一域名配置多个源站IP，最多支持20个源站IP。

- 如果使用HTTPS，还需要准备服务器的证书和私钥。

7.1.2.2 添加防护域名

操作步骤

1. 登录云盾控制台。
2. 定位到**应用安全** > **域名配置**，如图 *7-1: Web应用防火墙域名配置页面*所示。

图 7-1: Web应用防火墙域名配置页面

3. 输入需要防护的**域名**，勾选**协议类型**，填写回源IP。

表 7-1: 域名配置项

配置项	说明
域名	支持配置泛域名，如*.aliyundemo.cn，可以匹配相关的二级域名。当同时配置泛域名和精确域名时，转发和防护策略匹配顺序以精确域名优先。

配置项	说明
协议	如果有HTTPS站点，务必勾选**HTTPS**协议类型。建议同时勾选**HTTP**协议类型，以应对HTTP跳转等问题，保证访问平滑。
回源设置	回源IP是指希望Web应用防火墙把请求转发到的地址，一般是真实服务器的地址（如ECS的IP），也可以是SLB的IP。 回源IP最多可以支持20个，Web应用防火墙支持负载均衡和健康检查功能。
WAF是否支持XFF？	X-Forwarded-For位于HTTP协议的请求头， 是一个 HTTP 扩展头部，用来表示 HTTP 请求端真实 IP。一般用于 HTTP 代理、负载均衡等转发服务。 如果WAF前使用了七层代理，为了保障WAF的安全策略能够针对真实源IP 生效，请务必选择**是**。

4. 单击**确定**。

7.1.2.3 上传HTTPS证书和私钥（仅针对HTTPS站点域名）

背景信息

如果需要防护HTTPS站点域名，必须将服务器的证书和私钥上传至Web应用防火墙，否则可能无法正常访问HTTPS站点。

如果需要防护的域名不支持HTTPS协议访问，请跳过此步骤。

操作步骤

1. 登录云盾控制台。
2. 定位到**应用安全** > **域名配置**。
3. 在**协议类型**中，勾选**HTTPS**。
4. 单击**HTTPS高级设置**可以选择HTTPS协议的回源方式及跳转设置，如*图 7-2: HTTPS高级设置选项*所示。

图 7-2: HTTPS高级设置选项

- 如果该站点不支持HTTPS回源，勾选**开启HTTP回源**，通过WAF实现HTTPS访问。使用该设置后，客户端可以通过HTTP和HTTPS方式访问站点。

  说明：
  使用HTTP回源，可以无需在源站服务器上做任何改动，也不需要配置HTTPS。但是，该配置的前提是在WAF上传正确的证书和私钥。

- 如果需要强制客户端使用HTTPS来访问，勾选**开启HTTPS的强制跳转**。

  说明：
  开启HTTPS强制跳转后，HTTP回源可以根据具体需求来开启或关闭。若同时开启HTTP回源，WAF会将客户端的HTTP请求重定向到HTTPS，并且设置客户端的HSTS属性（周期为一天）。支持HSTS的客户端后续会直接使用HTTPS访问，不支持的客户端则通过重定向方式访问。

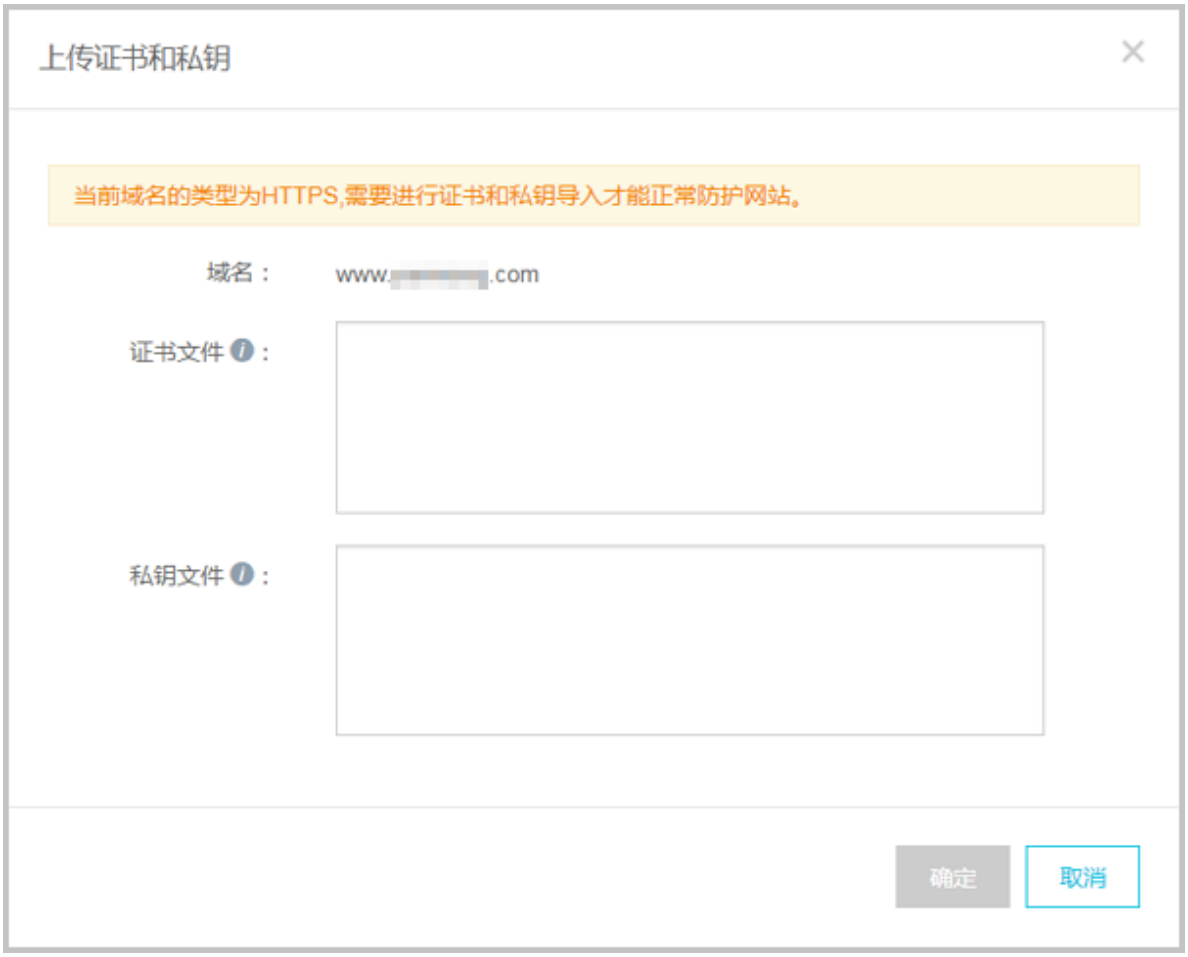
5. 添加HTTPS站点域名后，在已添加域名列表中找到该域名，单击**上传证书**，如图 *7-3: HTTPS站点域名证书更新*所示。

图 7-3: HTTPS站点域名证书更新

6. 上传服务器的证书文件和私钥文件，如图 *7-4:* 上传证书和私钥所示。

   复制证书和私钥文本内容粘贴至相应的文本框内。

图 7-4: 上传证书和私钥



一般如PEM、CER、CRT等证书格式，可用文本编辑器直接打开并复制内容；其它格式的证书（如PFX、P7B等）需要先转换成这些格式。如果有多个证书文件（如证书链），可拼接合并后一起上传。

- Web应用防火墙可识别的证书样例格式如下：

```
-----BEGIN CERTIFICATE----- 62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9f
mxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+j2kcubVpsE2 cgHdj4v8H6jUz9Ji4mr7
vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOkjgvhlqt9vc 65Cgb4mL+
n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKk
 vRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg== -----END
CERTIFICATE-----
```

- Web应用防火墙可识别的私钥样例格式如下：

```
-----BEGIN RSA PRIVATE KEY----- DADTPZoOHd9WtZ3UKHJTRgNQmioPQn
2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThLyvsmLQKBgQ Cr+ujntC1kN6pGBj2Fw2l
/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJaiygoIYo aMF2EjRwc0
qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o
4Vqf0YF8bv5UK5G04RtKadOw== -----END RSA PRIVATE KEY-----
```

7. 单击**确定**，完成配置。

7.1.2.4 放行Web应用防火墙VIP

背景信息

VIP是WAF用来代理客户端请求服务器时使用的源IP。在源站服务器看来，接入Web应用防火墙后所有访问源IP都会变成Web应用防火墙的VIP，而真实的客户端地址会被加在HTTP头部的XFF字段中。

域名接入Web应用防火墙后，需确保源站服务器的安全组已将Web应用防火墙的VIP放行，否则可能会出现网站无法访问或响应极其缓慢的情况。

操作步骤

1. 登录云盾控制台。
2. 定位到**应用安全** > **域名配置**。
3. 在页面上方查看Web应用防火墙VIP，如*图 7-5: Web应用防火墙VIP*所示。

图 7-5: Web应用防火墙VIP

4. 登录Apsara Stack控制台，在源站服务器的安全组中将Web应用防火墙的VIP放行（在入方向，允许VIP访问源站服务器）。

安全组具体设置，参见《用户指南》的**管理安全组**。

7.1.2.5 本地验证域名Web应用防火墙接入配置

在把业务流量切到Web应用防火墙之前，建议先通过本地验证的方式确保配置正常，Web应用防火墙转发正常。

操作步骤

1. 登录云盾控制台。
2. 在*hosts*文件中添加VIP和域名，使本地对于被防护站点的请求先经过Web应用防火墙。

   以Windows 7为例修改*hosts*文件，文件路径*C:\Windows\System32\drivers\etc\hosts*。

   a) 使用记事本等文本编辑器打开hosts文件。

   b) 在最后一行添加<*WAF*的*VIP*> <被防护域名>，如图 *7-6: Hosts文件添加内容示例*所示内容。

   图 7-6: Hosts文件添加内容示例

   ```
   # localhost name resolution is handled within DNS itself.
   #       127.0.0.1       localhost
   #       ::1             localhost

   [redacted] 58.255 www.aliyundemo.cn
   ```

   说明：
   域名前面的IP为对应的Web应用防火墙所分配的VIP。

3. 在本地Ping被防护的域名，解析到的IP应该为在hosts文件中绑定的Web应用防火墙VIP。

   说明：
   如果依然解析到源站地址，可尝试刷新本地的DNS缓存。

4. 在浏览器中输入该域名进行访问。

   如果Web应用防火墙的接入配置正确，则能够正常访问网站。

5. 验证Web应用防火墙保护功能。

   例如，在域名的URL后添加`/?alert(xss)`，即可模拟一个测试的Web攻击请求，如`www.aliyundemo.cn/?alert(xss)`。此时，Web应用防火墙应能弹出如图 *7-7: Web应用防火墙阻拦页面*所示的阻拦页面。

图 7-7: Web应用防火墙阻拦页面

7.1.2.6 修改DNS解析

通过修改DNS解析到Web应用防火墙，完成业务正式接入。

背景信息

如果防护的站点域名不是通过域名解析服务商进行解析，例如站点是通过负载均衡（SLB）实例连接公网，也可以参考以下步骤，将所对应的SLB实例的回源IP修改为WAF的VIP，实现Web应用防火墙防护接入。

操作步骤

1. 登录云盾控制台。
2. 定位到**应用安全** > **域名配置**。
3. 记录下Web应用防火墙为防护域名所分配的WAF的VIP。
4. 登录已防护站点的域名解析服务商所提供的控制台，定位到对应域名的域名解析设置，将A记录的值改为WAF的VIP。

> **说明**：
> 域名解析的TTL值一般建议设置为600秒。TTL值越大，DNS记录的同步和更新越慢。

7.1.3 配置防护功能

在将站点接入Web应用防火墙防护后，可对所防护的站点进行详细的防护规则配置。

7.1.3.1 配置Web应用攻击防护

启用Web应用攻击保护功能，并设置防护模式和防护规则。

背景信息

Web应用攻击防护功能可以防护SQL注入、XSS跨站脚本、文件上传、文件包含、常见目录遍历、常见CMS漏洞、代码执行注入、脚本后门攻击、扫描器攻击等常见Web应用攻击。

操作步骤

1. 登录云盾控制台。
2. 定位到**应用安全** > **域名配置**页面。
3. 选择已接入Web应用防火墙进行防护的站点域名，单击**防护配置**，如图 *7-8: 域名防护配置*所示。

图 7-8: 域名防护配置

4. 定位到**Web应用攻击防护**功能项，单击状态栏后的启用按钮并选择防护模式及防护规则策略，如图 *7-9: Web应用攻击防护功能项*所示。

图 7-9: Web应用攻击防护功能项

表 7-2: 防护模式和防护策略

防护设置		说明
防护模式	防护	Web应用防火墙自动对攻击行为进行阻断。
	预警	Web应用防火墙对可疑攻击告警但不立刻阻断，方便评估误报情况。
防护规则策略	正常	默认策略，一般情况下使用。
	宽松	当发现正常模式规则存在较多误拦截的情况，或业务存在较多不可控的用户输入（例如富文本编辑器、技术论坛）时，建议选择宽松模式。
	严格	需要更严格的防护规则来防护路径穿越、SQL注入、命令执行等攻击，建议选择严格模式。

7.1.3.2 配置恶意IP惩罚

当某个IP在短时间内进行多次Web攻击，可以设置自动封禁该IP一段时间。

背景信息

传统的Web应用防火墙产品，基本都是针对 IP-URL 维度的拦截。当判定一个请求是攻击行为后，仅仅把这个请求进行单次阻断。而实际上，恶意攻击者们日复一日地在对用户的网站进行扫描、攻击，黑客可能一个通宵都在挖掘网站的漏洞，研究防护策略并尝试绕过。

专有云云盾Web应用防火墙提供了恶意IP惩罚功能。利用阿里云平台积累的海量恶意IP库和机器学习功能，对发起攻击行为的 IP、攻击频率进行学习分析，自动生成判定规则。当发起攻击的IP的行为被判定为持续攻击行为，Web应用防火墙将直接阻断这个IP的所有访问请求。

操作步骤

1. 登录云盾控制台。
2. 定位到**应用安全** > **域名配置**页面。
3. 选择已接入Web应用防火墙进行防护的域名，单击**防护配置**。
4. 定位到**恶意IP惩罚**功能项，单击状态栏后的启用按钮即可启用恶意IP惩罚功能，如*图 7-10: 恶意IP惩罚功能项*所示。

图 7-10: 恶意IP惩罚功能项

7.1.3.3 配置CC安全防护

通过独家算法防护引擎并结合大数据，拦截CC攻击。

背景信息

CC（Challenge Collapsar）攻击，是一种专门针对于Web的应用层FLOOD攻击，是DDoS的一种。攻击者通过代理服务器或者肉鸡，对目标Web服务器进行海量http request攻击，造成对方服务器资源耗尽。

Web应用防火墙提供了正常、攻击紧急两种CC安全防护模式：

- **正常**：CC安全防护的默认模式，只会针对特别异常的请求进行拦截，误杀可能性较小。
- **攻击紧急**：攻击紧急模式拦截CC攻击效果较强，但可能存在误杀的情况。 当发现站点遭受CC攻击，且正常模式无法有效拦截时，可以启用攻击紧急模式。

> **说明**：
> 攻击紧急模式仅适用于普通网页及HTML5页面，对于API、Native APP的业务可能会造成大量误杀。如果需要为API、Native APP业务配置CC攻击防护，请使用CC自定义规则进行防护。

同时，Web应用防火墙提供了CC防护自定义规则，支持在控制台自定义对于特定URL路径的访问频率限制。

操作步骤

1. 登录云盾控制台。
2. 定位到**应用安全** > **域名配置**页面。
3. 选择已接入Web应用防火墙进行防护的域名，单击**防护配置**。
4. 定位到**CC安全防护**功能项，单击状态栏后的启用按钮，选择想要应用的CC安全防护模式，如*图7-11: CC安全防护功能项*所示。

图 7-11: CC安全防护功能项

5. 单击自定义规则栏后的启用按钮，可启用CC安全防护自定义规则。

   自定义规则设置如下：

   a) 单击**前去配置**，配置自定义防护规则，如图 *7-12: CC自定义安全防护规则*所示。

   图 7-12: CC自定义安全防护规则

   b) 单击**新增规则**，添加想要设置的自定义规则。

   例如，通过自定义防护规则可设置当单个访问源IP在10秒内访问www.abc.com/login.html超过20次，即封禁该IP一小时。

图 7-13: 新增自定义规则

表 7-3: 规则参数说明

规则参数	说明
URI	需要防护的具体URI地址，如`/register`。同时，支持输入参数，如`/user?action=login`。
匹配规则	• **完全匹配**：即精确匹配，请求必须跟所配置的URI完全一致才适用该规则。 • **前缀匹配**：指包含匹配，只要是请求的URI以配置的URI地址开头都适用该规则，如`/register.html`。
检测时长	访问次数的周期时长，与单一IP访问次数配置相配合。
单一IP访问次数	在统计周期内，单个源IP访问该URL的次数。
阻断类型	• **封禁**：触发规则条件后，直接断开连接。 • **人机识别**：触发规则条件后，通过重定向的方式进行客户端人机识别，成功通过验证的请求才可放行。

规则参数	说明
阻断时间	执行阻断动作的时间。

c) 单击**确定**。

7.1.3.4 配置精准访问控制

精准访问控制功能支持针对常见的HTTP字段（如IP、URL、Referer、UA、参数等）进行条件组合设置访问控制规则，支持业务场景的定制化防护策略，如盗链防护、网站管理后台保护等场景。

背景信息

配置精准访问控制规则之前，请注意以下事项：

- 每一条规则中最多允许由三个条件组合。
- 同一条规则中的多个条件之间都是“与”的逻辑关系，即必须同时满足多个条件才算匹配中规则。
- 匹配中规则后可设定的匹配动作有三种：
  - **阻断**：阻止访问。
  - **放行**：选择放行后，可选择后续是否继续执行Web应用攻击防护或CC攻击防护。
  - **告警**：只记录不阻断。
- 精准访问控制规则之间存在先后匹配顺序，可通过调整规则排序达到最优的防护效果。

操作步骤

1. 登录云盾控制台。
2. 定位到**应用安全** > **域名配置**页面。
3. 选择已接入Web应用防火墙进行防护的域名，单击**防护配置**。
4. 定位到**精准访问控制**功能项，单击状态栏后的启用按钮即启用精准访问控制功能，如*图 7-14: 精准访问控制功能项*所示。

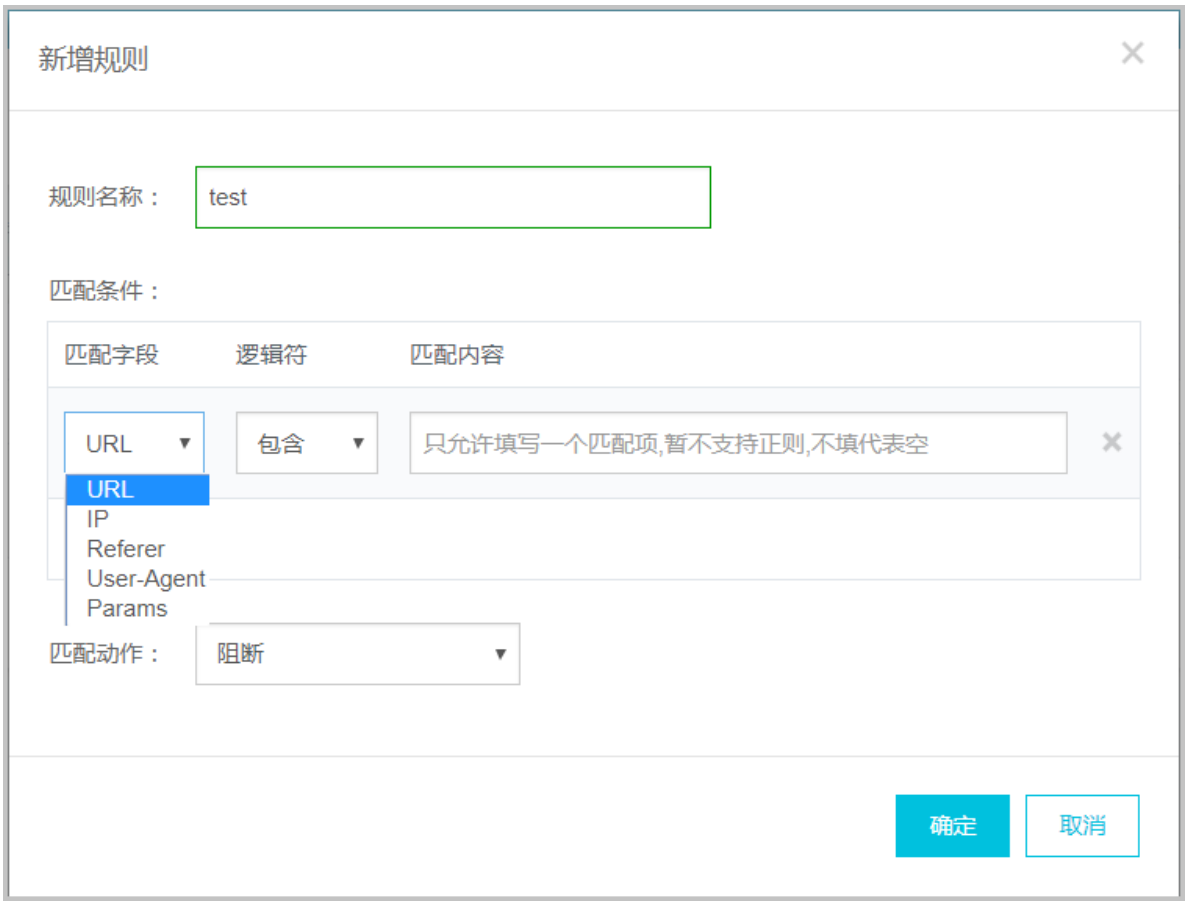
图 7-14: 精准访问控制功能项

5. 单击**前去配置**，配置精准访问控制规则，如图 *7-15:* 配置精准访问控制规则所示。

图 7-15: 配置精准访问控制规则

6. 单击**新增规则**，如图 *7-16:* 新增精准访问控制规则所示。

图 7-16: 新增精准访问控制规则



精准访问控制规则支持多种匹配字段及逻辑符，可根据实际业务需求进行规则设置，也可以参考如图 *7-17:* 精准访问控制规则样例所示的规则样例设置匹配规则。

图 7-17: 精准访问控制规则样例

精准访问控制　　您还可以添加 193 条　新增规则　规则排序

规则名称	规则条件	动作	后续安全策略	操作
只允许通过微信登录	请求URL 等于 /user 请求Params 包含 action=login 请求User-Agent 不包含 MicroMessenger	阻断		编辑 删除
只允许公司访问后台	请求IP 不属于 1.2.3.0/29 请求URL 包含 admin.php	阻断		编辑 删除
防WP攻击	请求User-Agent 包含 wordpress	阻断		编辑 删除
防盗链	请求URL 包含 photos 请求Referer 包含 blog.xxx.com	阻断		编辑 删除
黑名单1	请求IP 属于 4.4.4.0/24	阻断		编辑 删除
白名单2	请求IP 属于 3.3.3.0/24	放行	Web通用防护	编辑 删除
白名单1	请求IP 属于 2.2.2.0/24	放行		编辑 删除
默认规则	所有未命中以上规则的请求	放行	Web通用防护 CC防护	编辑

7. 在**精准访问控制**页面，单击**规则排序**可对已设定的精准访问控制规则进行排序，调整完成后单击**保存**即可。精准访问控制功能将按设置的规则顺序进行匹配。

7.1.3.5 配置封禁地区

Web应用防火墙可对特定地区的来源IP进行封禁。根据IP归属地信息库，封禁地区功能针对支持国内各省份和海外地区的IP封禁。

操作步骤

1. 登录云盾控制台。
2. 定位到**应用安全** > **域名配置**页面。
3. 选择已接入Web应用防火墙进行防护的域名，单击**防护配置**。
4. 定位到**封禁地区**功能项，单击状态栏后的启用按钮即启用封禁地区功能，如图 *7-18: 封禁地区功能项*所示。

图 7-18: 封禁地区功能项

5. 单击**设置**，可对封禁的地区进行设置，如图 *7-19:* 设置封禁地区所示。

图 7-19: 设置封禁地区

7.1.4 查看安全报表

Web应用防火墙提供了各种安全报表供安全管理员实时了解所防护的域名的安全状态。

7.1.4.1 查看安全总览

展示攻击防护报表和Web防护规则相关消息。

背景信息

WEB攻防总览页面展示了攻击防护报表和Web防护规则相关消息。

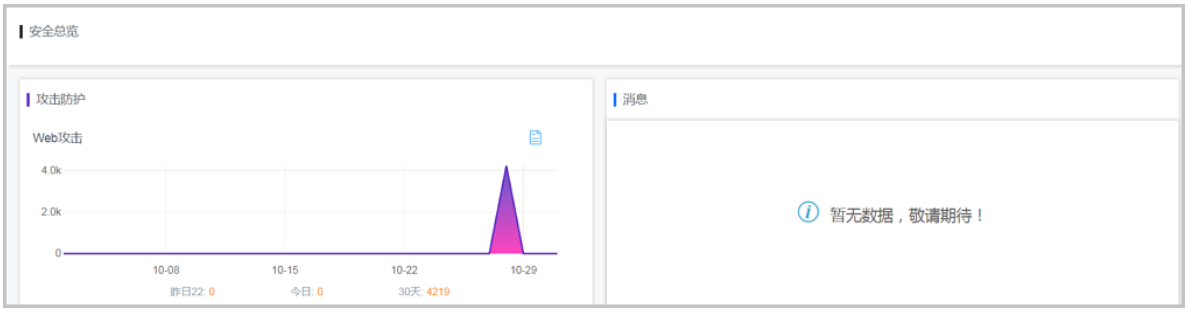
- 在攻击防护报表中，可以查看Web攻击、CC攻击的防护情况，并显示昨日、今日及30天内防护次数，帮助安全管理员快速了解所防护的域名的整体安全状态。
- 在消息区域中，可以查看阿里云实时发布的Web应用防火墙防护规则的更新消息。

操作步骤

1. 登录云盾控制台。

2. 定位到**应用安全** > **WEB攻防总览**。
3. 查看Web应用防火墙攻击防护信息，如图 *7-20: 安全总览页面*所示。

图 7-20: 安全总览页面



4. 单击攻击防护报表右上方的查看详情按钮，跳转至**WEB安全报表**页面，查看详细攻击防护情况。

7.1.4.2 查看安全报表

查看Web应用防火墙所防护的域名的详细防护情况。

背景信息

在**WEB安全报表**页面，可查看Web应用防火墙所防护的域名的详细防护情况。

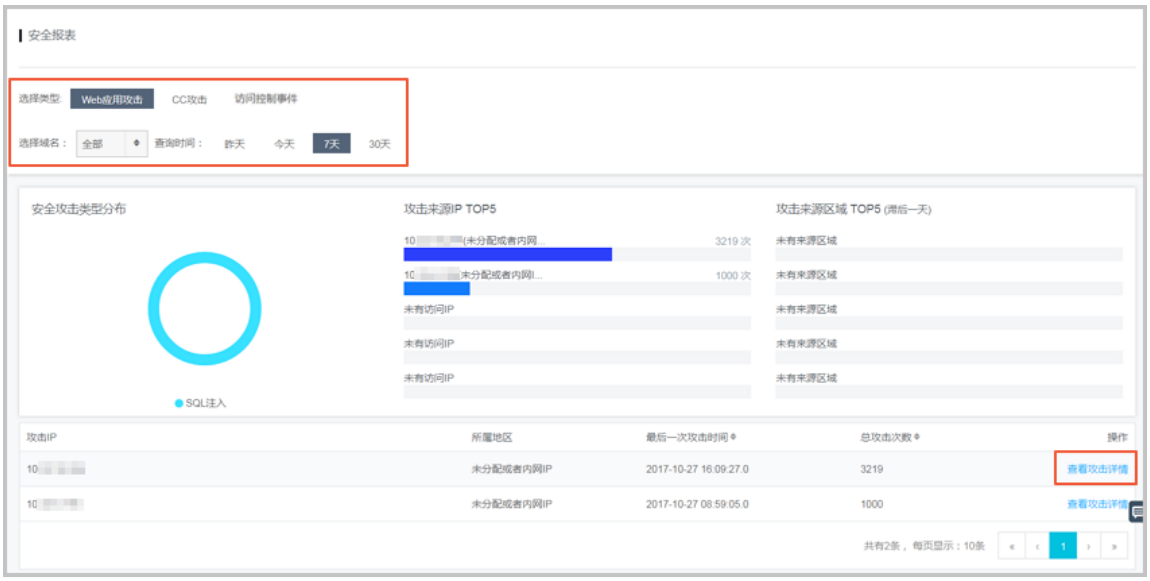
- 针对**Web应用攻击**，可以查看攻击类型分布、攻击来源IP、攻击来源区域及详细的攻击记录。
- 针对**CC攻击**，可以查看服务器每秒查询率（QPS），包括总QPS、攻击QPS信息及详细的恶意CC攻击事件记录。
- 针对**访问控制事件**，可以查看已配置的精准访问控制规则的匹配次数及对应的规则动作。

操作步骤

1. 登录云盾控制台。
2. 定位到**应用安全** > **WEB安全报表**页面。
3. 查看Web应用攻击安全报表。

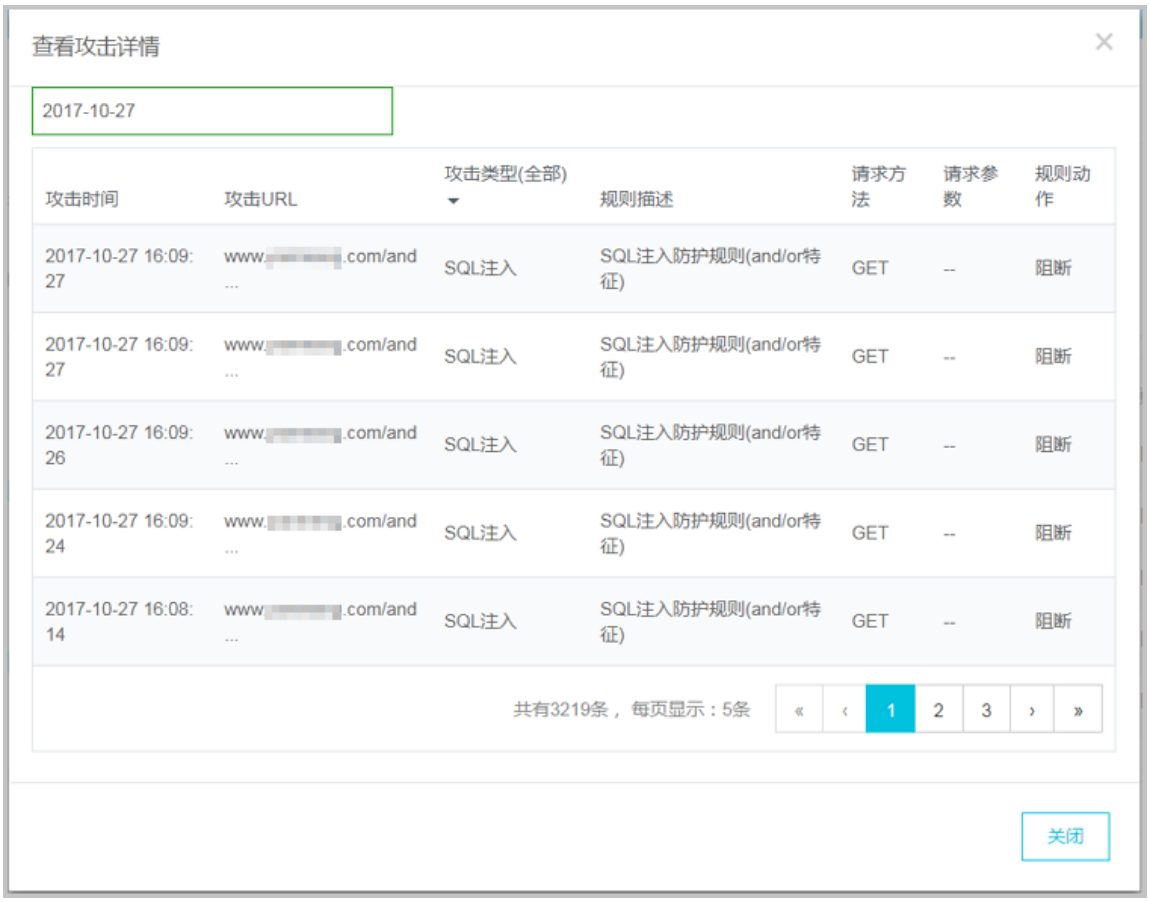
   a) 单击**Web应用攻击**，并设置域名和查询时间，如图 *7-21: Web应用攻击安全报表*所示。

图 7-21: Web应用攻击安全报表



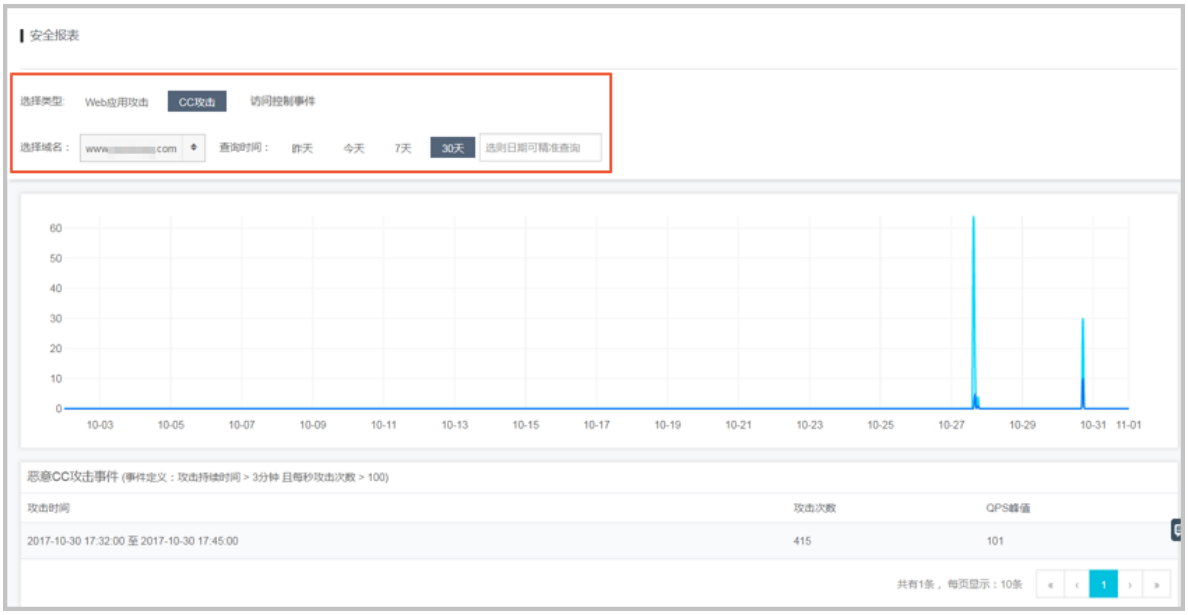
b) 单击**查看攻击详情**，可查看详细的攻击事件及所触发的拦截规则，如图 7-22: 查看攻击详情所示。

图 7-22: 查看攻击详情



4. 查看CC攻击安全报表，如图 *7-23: CC攻击安全报表*所示。

图 7-23: CC攻击安全报表



5. 查看访问控制事件安全报表，如图 *7-24: 访问控制事件安全报表*所示。

图 7-24: 访问控制事件安全报表

7.1.4.3 查看业务分析

业务分析功能结合Web应用防火墙的攻击拦截情况及访问流量，通过大数据引擎，对所防护域名的业务访问情况进行分析，帮助安全管理员及时发现业务漏洞，提升防御能力。

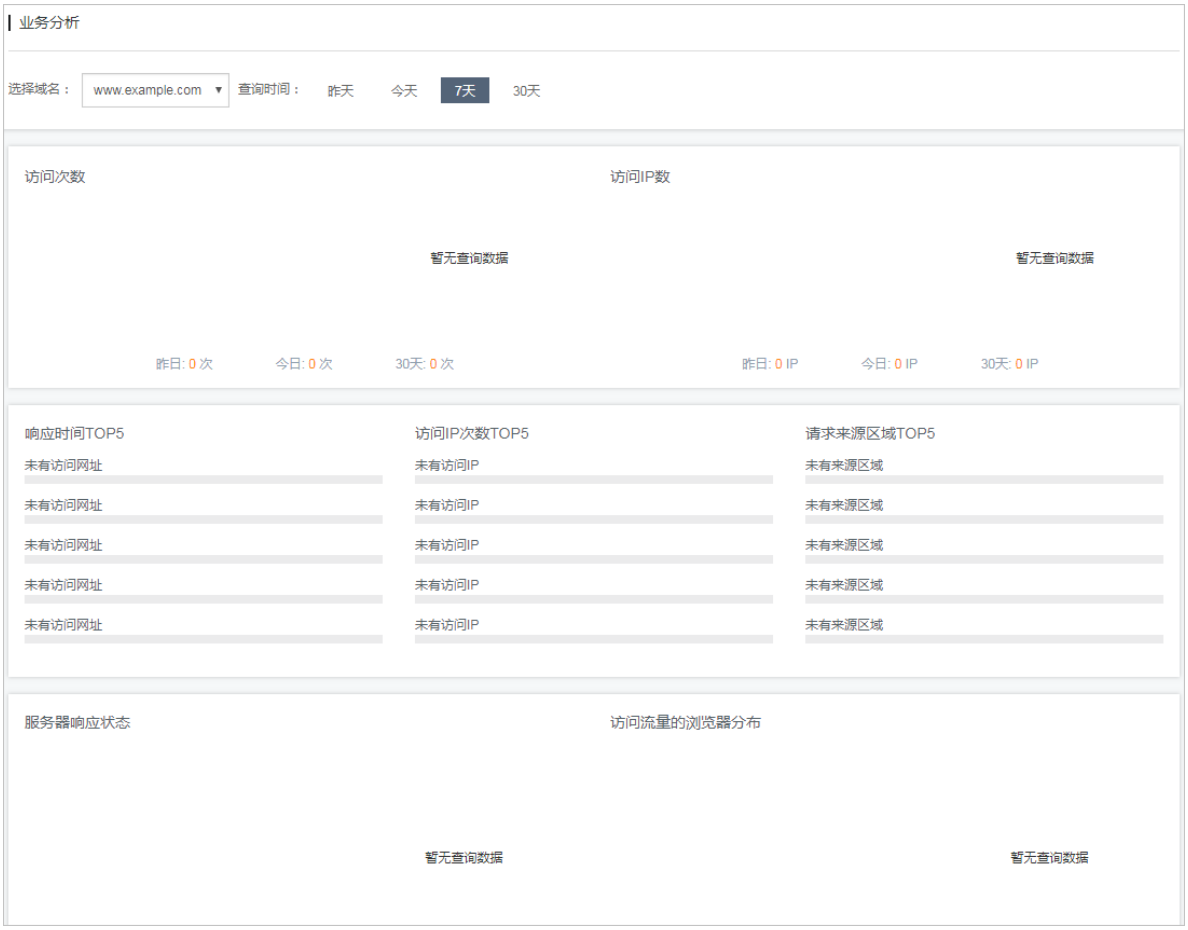
前提条件

Web应用防火墙的业务分析功能依赖于MaxCompute（原名 ODPS）服务进行数据分析。如果专有云环境中没有部署MaxCompute产品，将无法使用业务分析功能。

操作步骤

1. 登录云盾控制台。
2. 定位到**应用安全** > **业务分析**页面。
3. 选择域名及查询时间，查看业务分析结果，如图 *7-25:* 业务分析页面所示。

图 7-25: 业务分析页面



8 云主机安全

8.1 主机安全总览

主机安全总览对云主机整体安全情况进行概要性展示，以便安全管理员快速了解和掌握当前安全情况。

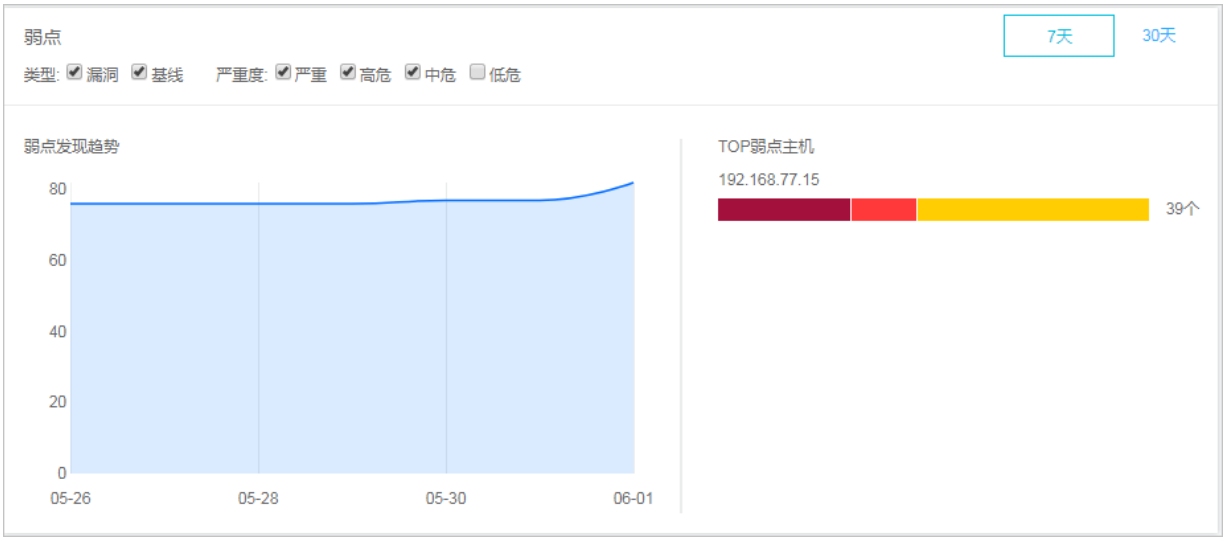
主机安全总览包括总览、弱点、事件、ECS保护状态、最近重要弱点和事件。

总览

整体展现云主机环境各类型的安全弱点（待处理漏洞、基线配置不当）和安全事件（异常登录、网站后门、主机异常）的数量。

弱点

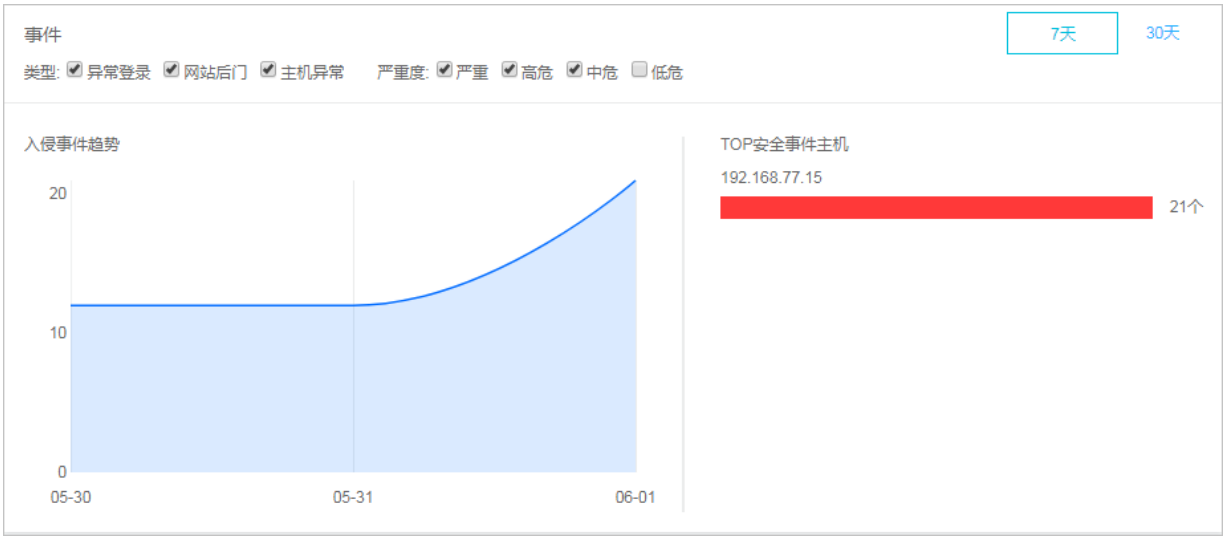
展示云主机存在的安全弱点趋势。安全弱点如果不修复，存在安全隐患，具体修复建议和操作可以参考安全预防。



- 上面为过滤条件，通过类型、严重程度和展示时间，生成展示结果。
- 左侧为弱点发现趋势，展示一段时间内云主机的弱点趋势。
- 右侧为TOP弱点主机，展示存在弱点数量最多的云主机。

事件

展示云主机存在的安全事件趋势。安全事件表明目前云主机已经发现的安全入侵行为，具体操作可以参考入侵检测。



- 上面为过滤条件，通过类型、严重程度和展示时间，生成展示结果。
- 左侧为入侵事件趋势，展示一段时间内云主机受到入侵的趋势。
- 右侧为TOP安全事件主机，展示受到入侵最多的云主机。

ECS保护

查看目前云主机中正在受到保护的主机数量和离线数量。

最近重要弱点和事件

展示最近重要的云主机安全弱点和安全事件，单击连接可以查看具体详细情况。

最近重要弱点和事件

【未修复】2018-06-02 05:11:49
【192.168.77.18（iZ5wf05ykw7minn5ge2ma9Z）】
漏洞: RHSA-2017:0252: ntp security update

【未修复】2018-06-02 05:11:49
【192.168.77.18（iZ5wf05ykw7minn5ge2ma9Z）】
漏洞: RHSA-2017:1574: sudo security update

【未修复】2018-06-02 05:11:49
【192.168.77.18（iZ5wf05ykw7minn5ge2ma9Z）】
漏洞: RHSA-2016:2824: expat security update

8.2 主机列表

以云主机维度，展示各主机的安全状况信息。

8.2.1 管理主机列表

在主机列表页面，可以查看安骑士已防护的服务器的状态。

背景信息

服务器保护状态分为在线、离线、暂停保护三种。

- **在线**：安骑士为该服务器提供全面的安全防护。
- **离线**：安骑士服务端无法与该服务器的客户端正常连通，无法提供安全防护功能。
- **暂停保护**：暂时关闭安骑士对该服务器的防护，具体参见暂停保护操作。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **主机列表**。
3. （可选）搜索服务器。

   如果想查看某台服务器的安全状态，也可以在搜索框中输入该服务器的IP，并单击**搜索**，即可快速查看该服务器的详细信息和安全信息。
4. 查看服务器的保护状态和具体安全信息。

   单击右上角的⚙，设置服务器具体显示哪些信息列。信息主要分为以下几类。

类别	信息
服务器基本信息	• 服务器IP/名称

类别	信息
	• 标签 • 操作系统 • 地域
保护状态	保护状态
安全预防	• 漏洞 • 基线
入侵检测	• 异常登录 • 网站后门 • 主机异常
主机指纹	• 进程数 • 端口数 • Root账号

5. 管理服务器。

功能	操作说明
更改分组	勾选服务器，单击**更改分组**，更改服务器所在的分组。分组具体说明参见管理分组。
设置标签	勾选服务器，单击**设置标签**，设置服务器标签信息。
一键安全检查	勾选服务器，单击**一键安全检查**，可以选择从多维度对服务器进行安全检查。
删除非阿里云机器	勾选**非阿里云**的服务器，单击**删除非阿里云机器**。
暂停保护	勾选**在线**状态的服务器，单击**更多操作** > **暂停保护**，暂时关闭安骑士对该服务器的防护，降低该服务器的资源消耗。
开启保护	勾选**暂停保护**状态的服务器，单击**更多操作** > **开启保护**，开启安骑士对该服务器的防护。

8.2.2 管理分组

为了方便对特定服务器进行安全管控，可以对服务器进行分组，通过分组的维度查看安全事件。

背景信息

未进行分组时，所有的服务器都在**未分组**中。当您删除某个分组时，该分组中的服务器也将默认移入**未分组**中。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **主机列表**。
3. 管理子分组。

- 新建子分组。

  单击**所有资源**或者子分组右侧的添加按钮，输入子分组名称并单击**确认**。

  > **说明**：
  > 最多支持三级子分组。

- 修改子分组。

  单击子分组右侧的修改按钮，输入子分组名称并单击**确认**。

- 删除子分组。

  单击子分组右侧的删除按钮，在弹出的确认框中单击**确认**。

  > **说明**：
  > 删除后该分组中的服务器默认移入**未分组**。

4. 给服务器进行分组。
   a) 在右侧的服务器列表中，勾选服务器。
   b) 单击**更换分组**。
   c) 在弹出窗口的下拉菜单中选择分组。
   d) 单击**确认**。
5. 切换分组排序。

单击**分组排序**，可以把优先级高的分组移动到上面。

8.3 安全预防

安全预防提供漏洞管理和基线检查功能，用于发现服务器中存在的漏洞和风险点，并提供修复建议。

8.3.1 漏洞管理

漏洞管理扫描出服务器中存在的漏洞，并提供漏洞修复方法。

8.3.1.1 管理Linux软件漏洞

比对CVE官方漏洞库，自动检测您服务器上安装的软件版本是否存在漏洞，并向您推送漏洞消息。针对检测到的漏洞，提供漏洞修复指令和验证功能。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **安全预防** > **漏洞管理**，选择**Linux软件漏洞**页签。
3. 查看所有漏洞。

   通过漏洞搜索和筛选功能，快速定位到具体漏洞，如*图 8-1: 过滤漏洞*所示。

   图 8-1: 过滤漏洞

4. 单击漏洞名称，进入漏洞详情页，查看漏洞详细信息和影响资产。

   通过搜索和筛选功能，快速展示影响资产，如*图 8-2: 筛选影响资产*所示。

图 8-2: 筛选影响资产

5. 根据漏洞影响情况，选择相应的处理方式，如表 *8-1: 漏洞操作方式*所示。

表 8-1: 漏洞操作方式

操作	说明
生成修复命令	自动生成修复漏洞的指令，然后登录服务器运行该指令来修复漏洞。
一键修复	直接修复漏洞。
已重启并验证	如果修复漏洞需要重启服务器才能生效，必须等待漏洞修复状态变为**修复成功待重启**后，重启该服务器，然后单击**已重启并验证**完成修复。
忽略	可忽略该漏洞，系统将不再上报并告警此服务器上被忽略的漏洞。
验证	修复漏洞后，单击**验证**，一键验证该漏洞是否已修复成功。 如果未进行手动验证，漏洞修复成功后 48 小时内系统会自动去验证。

对于影响资产，可以进行单个操作或多个批量操作。

- 单个操作：在**操作**列，对单个受影响的服务器进行处理。
- 批量操作：勾选一个或多个需要处理的服务器，使用列表下方的批量操作按钮进行批量处理。

8.3.1.2 管理Windows系统漏洞

比对微软官方补丁更新，自动检测您服务器上的补丁是否已更新，并向您推送漏洞消息。针对重大漏洞更新，提供自动检测和修复功能。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **安全预防** > **漏洞管理**，选择**Windows系统漏洞**页签。
3. 查看所有漏洞。

通过漏洞搜索和筛选功能，快速定位到具体漏洞，如图 *8-3: 过滤漏洞*所示。

图 8-3: 过滤漏洞

4. 单击漏洞名称，进入漏洞详情页，查看漏洞详细信息和影响资产。

   通过搜索和筛选功能，快速展示影响资产，如图 *8-4: 筛选影响资产*所示。

图 8-4: 筛选影响资产

5. 根据漏洞影响情况，选择相应的处理方式，如表 *8-2: 漏洞操作方式*所示。

表 8-2: 漏洞操作方式

操作	说明
立即修复	直接修复漏洞。系统会在云端缓存一份Windows官方补丁文件，您的Windows系统服务器会直接下载云端的补丁并完成自动更新。
忽略	可忽略该漏洞，系统将不再上报并告警此服务器上被忽略的漏洞。
验证	修复漏洞后，单击**验证**，一键验证该漏洞是否已修复成功。
已重启并验证	如果修复漏洞需要重启服务器才能生效，必须等待漏洞修复状态变为**修复成功待重启**后，重启该服务器，然后单击**已重启并验证**完成修复。

对于影响资产，可以进行单个操作或多个批量操作。

- 单个操作：在**操作**列，对单个受影响的服务器进行处理。
- 批量操作：勾选一个或多个需要处理的服务器，使用列表下方的批量操作按钮进行批量处理。

8.3.1.3 管理Web-CMS漏洞

Web-CMS 漏洞功能通过及时获取最新的漏洞预警和相关补丁，并通过云端下发补丁更新，实现漏洞快速发现、快速修复的功能。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **安全预防** > **漏洞管理**，选择**Web-CMS漏洞**页签。
3. 查看所有漏洞。

   通过漏洞搜索和筛选功能，快速定位到具体漏洞，如*图 8-5: 过滤漏洞*所示。

   图 8-5: 过滤漏洞

4. 单击漏洞名称，进入漏洞详情页，查看漏洞详细信息和影响资产。

   通过搜索和筛选功能，快速展示影响资产，如*图 8-6: 筛选影响资产*所示。

   图 8-6: 筛选影响资产

5. 根据漏洞影响情况，选择相应的处理方式，如*表 8-3: 漏洞操作方式*所示。

表 8-3: 漏洞操作方式

操作	说明
立即修复	系统将替换服务器上存在漏洞的Web文件以修复Web-CMS漏洞。 **说明**： 修复Web-CMS漏洞前，建议备份该漏洞相关的Web文件，Web文件的具体路径可参考漏洞处理说明栏中的路径。
忽略	可忽略该漏洞，系统将不再上报并告警此服务器上被忽略的漏洞。
验证	修复漏洞后，单击**验证**，一键验证该漏洞是否已修复成功。 如果未进行手动验证，漏洞修复成功后 48 小时内系统会自动去验证。
回滚	对于已修复完成的漏洞，单击**回滚**可进行漏洞回滚，还原修复前的Web文件。

对于影响资产，可以进行单个操作或多个批量操作。

- 单个操作：在**操作**列，对单个受影响的服务器进行处理。
- 批量操作：勾选一个或多个需要处理的服务器，使用列表下方的批量操作按钮进行批量处理。

8.3.1.4 管理其他漏洞

自动检测服务器上的Redis未授权访问漏洞、STRUTS-052命令执行漏洞等漏洞，并推送漏洞消息。同时，支持漏洞的修复验证操作。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **安全预防** > **漏洞管理**，选择**其他漏洞**页签。
3. 查看所有漏洞。

   通过漏洞搜索和筛选功能，快速定位到具体漏洞，如图 *8-7: 过滤漏洞*所示。

图 8-7: 过滤漏洞

4. 单击漏洞名称，进入漏洞详情页，查看漏洞详细信息和影响资产。

   通过搜索和筛选功能，快速展示影响资产，如*图 8-8: 筛选影响资产*所示。

图 8-8: 筛选影响资产

5. 根据漏洞影响情况，选择相应的处理方式，如*表 8-4: 漏洞操作方式*所示。

   其他漏洞需要按照修复说明手动修复。

表 8-4: 漏洞操作方式

操作	说明
忽略	可忽略该漏洞，系统将不再上报并告警此服务器上被忽略的漏洞。
验证	手动修复漏洞后，单击**验证**，一键验证该漏洞是否已修复成功。 如果未进行手动验证，漏洞修复成功后 48 小时内系统会自动去验证。

对于影响资产，可以进行单个操作或多个批量操作。

- 单个操作：在**操作**列，对单个受影响的服务器进行处理。
- 批量操作：勾选一个或多个需要处理的服务器，使用列表下方的批量操作按钮进行批量处理。

8.3.1.5 设置漏洞管理策略

漏洞管理设置允许您开启/关闭不同类型漏洞的自动检测，有选择性地对指定服务器应用漏洞检测，对已失效漏洞设置自动删除周期，和配置漏洞白名单。

背景信息

漏洞白名单用于彻底忽略某些漏洞，您可以在漏洞列表下批量添加漏洞至白名单。添加成功后，系统将不再去检测漏洞白名单中的漏洞。使用漏洞管理设置可以维护漏洞白名单。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全 > 安全预防 > 漏洞管理**。
3. 单击右上角的**漏洞管理设置**，配置相关策略，如图 *8-9:* 漏洞管理设置所示。

图 8-9: 漏洞管理设置

- 选择需要操作的漏洞类型，单击切换开关，开启/关闭该漏洞检测。

- 选择需要操作的漏洞类型，单击**管理**，配置应用该漏洞检测的服务器。
- 勾选需要扫描的漏洞等级：严重、高危、中危、低危。
- 选择失效漏洞自动删除周期：7天、30天、90天。

> **说明**：
> 对于检测出来的漏洞不做任何处理的话，默认该告警失效，并在指定周期后自动删除。

- 在漏洞白名单下勾选相应漏洞，单击**移除**，重新启用对该漏洞的检测和告警。

8.3.2 基线检查

检测服务器上的系统、数据库、账号配置存在的风险点，并针对所发现的问题项提供修复建议。

8.3.2.1 基线检查介绍

安骑士基线检查功能自动检测服务器上的系统、数据库、账号配置存在的风险点，并针对所发现的问题项提供修复建议。

检测原理

基线检查功能自动检测服务器上的系统、权限、账号、数据库等配置存在的风险点，并提供修复建议。

检测周期

默认每三天进行一次全面自动检测，自动检测在凌晨0到6点间完成。您可以在在安全设置页面设置检测周期和检测发生时间。

注意事项

某些检测项，例如：Mysql弱密码检测、sqlserver弱密码检测，会采用尝试登录方式进行检查，会占用一定的服务器资源以及生产较多的登录失败记录，这些项目是默认不开启的。如果需要这些功能，请确认上述风险后，在基线检查设置中勾选这些项目。

检测内容

表 8-5: 检测内容

分类	检测项	说明
系统	系统自启动项检测（Windows）	检测Windows系统服务器中的注册表项`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit`中的键值是否包含可疑的可执行文件。

分类	检测项	说明
	系统共享配置检测（Windows）	检测Windows系统服务器中的注册表`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous`中的键值，查看该键值控制是否允许远程操作注册表。
	组策略检测（Windows）	检测Windows系统服务器中以下账号相关的安全策略： • 账号密码长度最小值。 • 密码复杂度（数字、大小写字母、特殊字符组合）。 • 密码更新时必须与原密码不同。 • 登录框是否显示上次登录账号。 • 登录事件记录是否开启。 • 登录过程中事件记录是否开启。
	SSH登录基线检测	检测Linux系统服务器中以下SSH登录安全策略配置： • 登录端口是否为默认22端口。 • root账号是否允许直接登录。 • 是否使用不安全的SSH V1协议。 • 是否使用不安全的RSH协议。 • 是否运行基于主机身份验证的登录方式。
弱密码检测	Linux系统登录弱口令检测	检测Linux系统服务器的登录账号的密码是否为常见弱口令，及SSH登录的密码是否常见弱口令。
	SQLServer登录弱口令检测	检测服务器上SQLServer登录账号的密码是否为常见弱口令。
	Windows系统登录弱口令检测	检测Windows系统服务器中系统登录账号的密码是否为常见弱口令，及RDP登录的密码是否为常见弱口令。
	FTP匿名登录检测	检测服务器上的FTP服务是否开启匿名登录。
	MySQL弱口令检测	检测服务器上的MySQL服务的登录账户是否为常见弱口令。
	PostgreSQL登录弱口令检测	检测服务器中PostgreSQL登录账号的密码是否为常见弱口令。
账号	风险帐号扫描	检测服务器系统中可疑的隐藏账号、及克隆账号。
	密码策略合规检测	检测Linux系统服务器中的以下账户密码策略： • 账号密码最大使用期限。 • 密码修改最小间隔时间。 • 密码最小长度。

分类	检测项	说明
		• 密码到期开始通知时间。
	空密码账户检测	检测服务器中密码为空的账号。
	Linux账号完整性检测	检测Linux系统服务器中新增账号的完整性。
数据库	Redis配置漏洞被利用可疑文件检测	检测服务器上的Redis服务是否存在未授权访问漏洞被利用并向系统关键文件写入异常数据的情况。
	Redis配置漏洞检测	检测服务器上的Redis服务是否对公网开放。
CIS基线检测	Linux-Tomcat7基线检测	按照CIS-Tomcat7最新基线标准进行中间件层面基线检测。
	Linux-Centos7基线检测	按照CIS-Linux Centos7最新基线标准进行系统层面基线检测。

8.3.2.2 管理基线检查

通过基线检查功能，查看和修复服务器上的配置风险项。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **安全预防** > **基线检查**，进入基线检查页面。
3. 查看所有风险项。

   通过风险搜索和筛选功能，快速定位到具体风险。

4. 单击风险名称，可查看该风险详情及相关修复建议。

   加入白名单：如果发现风险对服务器没有影响，后续也不需要检查该风险，可以单击右上角的**加入白名单**。

5. 参考修复建议，在您的对应服务器上进行修复。

- 修复风险后，您可以单击**验证**，一键验证该风险是否已修复成功。如果您未进行手动验证，风险修复成功后 72 小时内安骑士会进行自动验证。
- 如果不需要修复，您可以单击**忽略**，忽略该风险，安骑士将不再上报并告警此服务器上的这个风险项。

8.3.2.3 设置基线检查策略

根据实际业务情况设置基线检测项，检测周期、检测风险等级。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **安全预防** > **基线检查**，进入基线检查页面。
3. 单击**基线检查设置**，可以新建或者修改策略。
4. 单击**添加**，配置策略。

   选择某一策略，单击**编辑**修改策略；单击**删除**删除策略。
5. 管理白名单。

8.4 入侵检测

入侵检测提供异常登录、网站后门和主机异常等功能，用于检测发现服务器受到的入侵行为。

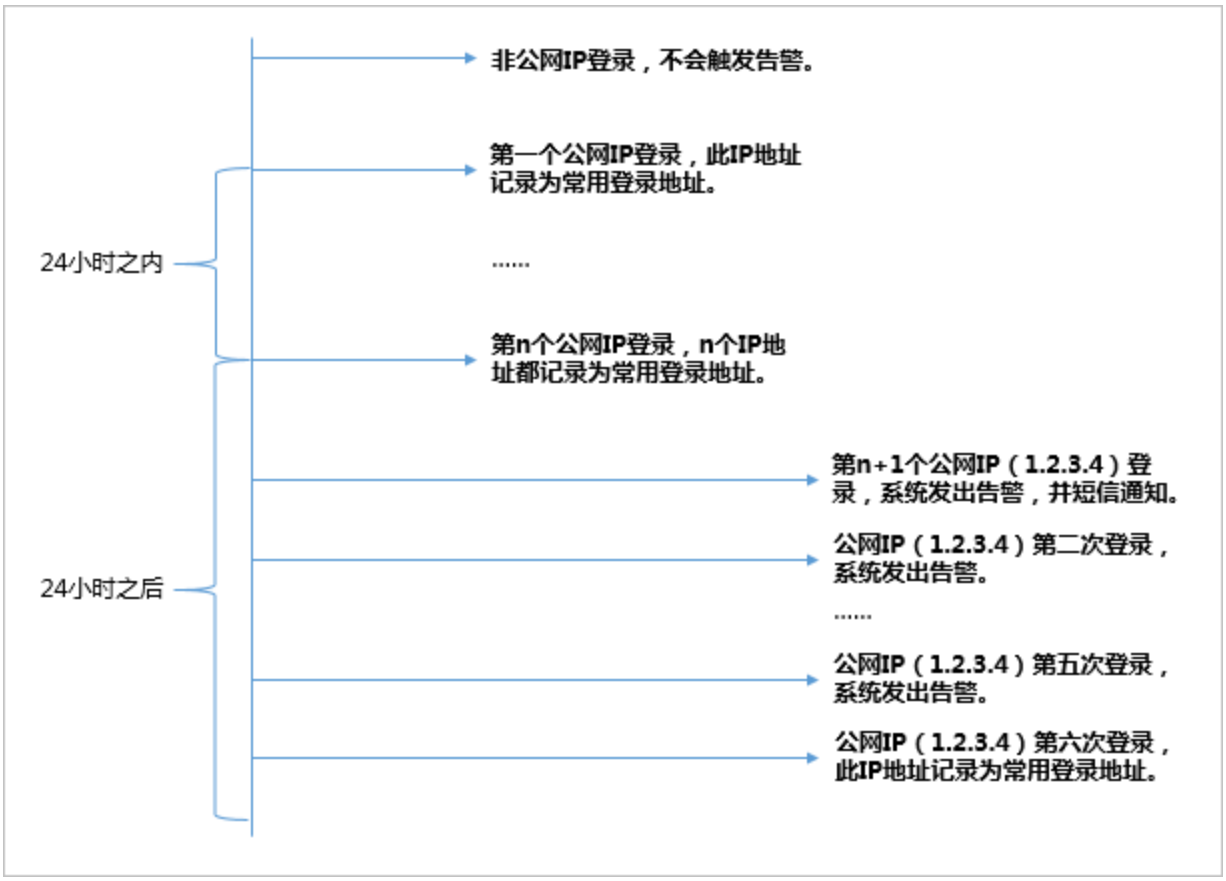
8.4.1 异常登录

在安骑士管理控制台中的**异常登录**页面，您可以查看服务器上每次登录行为有异常的登录IP、账号、时间，包括异地登录告警及非法登录IP、非法登录时间、非法登录账号的登录行为告警。

安骑士Agent通过定时收集您服务器上的登录日志并上传到安骑士服务器端，在安骑士服务器端进行分析和匹配。如果发现在非常用登录地或非法登录IP、非法登录时间、非法登录账号的登录成功事件，将会触发事件告警。

异地登录告警策略如图 *8-10:* 异地登录策略所示。

图 8-10: 异地登录策略



说明：

短信告警方式：可以在**设置** > **告警配置**中，选择**登录安全** > **异常登录**通知项目的告警方式（可配置为短信、邮件、及站内信方式，默认通过全部方式进行告警）。

针对机器设置合法登录IP、合法登录时间、合法登录账号，在上述合法登录IP、合法登录事件、合法登录账号之外的登录行为均提供告警，判断优先级高于异地登录判断。

8.4.1.1 查看异常登录

查看异常登录告警，包括异地登录、爆破登录、非法IP登录、非法账号登录和非法时间登录等告警。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **入侵检测** > **异常登录**。
3. 查看所有异常登录信息。

   通过搜索和筛选功能，快速定位到具体异常登录信息，如图 *8-11: 查找异常登录信息*所示。

图 8-11: 查找异常登录信息

4. 处理异常登录信息。

   选择异常登录信息，判断是否存在误报。

   - 如果是误报，直接单击**标记为已处理**。
   - 如果是非法入侵，对服务器进行安全加固（例如设置复杂密码，修复服务器漏洞，修复基线检查的风险点，设置黑/白名单等），完成后单击**标记为已处理**。

8.4.1.2 设置登录安全策略

设置登录安全策略，包括常用登录地、合法登录IP、合法登录时间和合法账号。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **入侵检测** > **异常登录**。
3. 在**异常登录**页面右上角，单击**登录安全设置**。
4. 设置常用登录地。
   a) 单击**添加**。
   b) 在下拉菜单中选择常用登录地。
   c) 设置常用登录地对哪些服务器生效。
      - **全部资源**中可以选择具体服务器。
      - **分组资产**中可以根据分组信息选择服务器。
   d) 单击**确定**，完成新增规则操作。
   e) 选择具体规则，单击**编辑**修改规则。
   f) 选择具体规则，单击**删除**删除规则。
5. 设置合法登录IP。
6. 设置合法登录时间。
7. 设置合法账号。

8.4.2 网站后门

安骑士采用本地查杀 + 云查杀体系，拥有定时查杀和实时防护扫描策略，支持检测常见的PHP、JSP等后门文件类型，并提供一键隔离功能。

安骑士通过检测您服务器上的Web目录中的文件，判断是否为Webshell木马文件。如果发现您的服务器存在网站后门文件，将会触发告警信息。

安骑士网站后门检测采用动态检测及静态检测两种方式：

- **动态检测**： 一旦 Web 目录中的文件发生变动，安骑士将会针对变动的内容进行动态检测。
- **静态检测**： 每天凌晨，安骑士将会扫描整个 Web 目录进行静态检测。

> **说明**：
> 默认情况下，安骑士防护的所有服务器均开启静态检测。如果需要设置特定服务器开启静态检测，可以在**设置** > **安全设置**中的**木马查杀**区域，单击**周期检查Web目录**右侧的**管理**设置需要进行静态检测的服务器。

8.4.2.1 管理网站后门

查看和隔离网站后门文件。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **入侵检测** > **网站后门**。
3. 选择资产，查看已发现的网站后门文件记录，如*图 8-12: 选择资产*所示。

图 8-12: 选择资产

4. 处理网站后门文件。
   - **隔离**：对发现的木马文件进行隔离操作，支持批量处理。
   - **恢复**： 如果错误隔离了某些文件，您可以单击**恢复**，将此文件恢复。
   - **忽略**： 忽略该木马文件后，安骑士将不再对此文件提示风险告警。

> **说明**：

安骑士不会将您服务器上的木马文件直接删除，只会将该文件转移到隔离区，在您确认该文件为信任文件后可通过恢复功能将该文件恢复，并且安骑士将不再对此文件进行告警。

8.4.3 主机异常

查看在服务器上检测到的异常进程行为、和恶意进程等。

8.4.3.1 管理主机异常

查看服务器上的主机异常告警，并修复相应问题。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **入侵检测** > **主机异常**。
3. 选择资产，查看已发现的主机异常事件。
4. 根据主机异常事件影响情况，选择相应的处理方式，如*表 8-6: 处理主机异常事件*所示。

表 8-6: 处理主机异常事件

操作	说明
一键修复	直接修复漏洞。
忽略本次	如果该事件不影响服务器安全，可以选择忽略本次告警。
确认事件	确认该事件。
标记为误报	如果本次告警为误报，可以标记为误报。
查看	查看本次告警详细信息。

8.5 主机指纹

主机指纹功能定期收集并记录服务器上的运行进程、系统账号、开放端口和软件版本，帮助您全面了解资产的运行状态和进行回溯分析。

8.5.1 管理监听端口

定期收集服务器的对外端口监听信息，用于清点端口。

背景信息

监听端口应用场景包括：清点一个端口被哪些服务器监听；清点一台服务器开通了哪些端口。

操作步骤

1. 登录云盾控制台。

2. 定位到**云主机安全** > **主机指纹**，选择**监听端口**页签。
3. 查看所有已开放端口、端口对应的网络协议、和开放这些端口的主机数。

   您可以通过端口号或进程名搜索，快速查找端口。
4. 单击端口号，查看对应的资产、协议等详细信息。

8.5.2 管理运行进程

定期收集服务器的进程信息，用于清点进程。

背景信息

运行进程应用场景包括：清点一个进程被哪些服务器运行；清点一台服务器运行了哪些进程。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **主机指纹**，选择**运行进程**页签。
3. 查看所有运行中进程和运行这些进程的主机数。

   您可以使用进程名或运行用户进行搜索。
4. 单击进程名，查看进程对应资产、路径、启动参数等详细信息。

8.5.3 管理账号信息

定期收集服务器的账号信息，用于清点账号。

背景信息

账号信息应用场景包括：清点一个账号被哪些服务器创建；清点一台服务器创建了哪些账号。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **主机指纹**，选择**账号信息**页签。
3. 查看所有已登录的系统账号和使用这些账号的主机数。

   您可以使用账号名进行搜索。
4. 单击账号名，查看对应资产、ROOT权限、用户组等详细信息。

8.5.4 管理软件版本

定期收集服务器的软件版本信息，用于清点软件资产。

背景信息

软件版本应用场景包括：清点非法软件资产（非法安装）；清点版本过低软件资产；漏洞爆发时快速定位受影响资产范围。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **主机指纹**，选择**软件版本**页签。
3. 查看所有使用中的软件和使用这些软件的主机数。

   您可以使用软件名、版本名或软件安装目录进行搜索。
4. 单击软件名，查看其对应资产、软件版本等信息。

8.5.5 设置主机指纹刷新频率

通过主机指纹设置功能，选择运行进程、系统账号、开放端口、软件版本数据的收集刷新频率。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **主机指纹**，单击**主机指纹设置**。
3. 在相应项目的下拉菜单中，选择刷新频率。
4. 单击**确认**，完成配置。

8.6 日志检索

全面支持主机的进程启动、网络连接、系统登录流水等日志查询和导出，便于您进行安全事件分析、操作日志审计。

8.6.1 日志检索介绍

云主机安全提供主机日志检索功能，将散落在阿里云各系统中的日志集中管理，便于您在出现主机问题时一站式搜索定位问题根源。

支持180天以内的日志存储，并提供30天以内的日志查询。

功能特性

日志检索功能具备以下特性：

- **一站式日志检索平台**，集中查询专有云各产品日志，单一接口，便于问题溯源。
- **日志功能的SaaS化**，无需进行额外安装部署，即可查询所有云环境中的服务器日志。

- 支持TB级数据检索，以及50个维度的数据逻辑（布尔表达式）组合，可以秒级展示日志全文检索结果。
- 支持丰富的主机日志源。
- 支持日志投递，允许您将安全日志导入到日志服务做进一步分析。

应用场景

日志检索帮助您实现以下需求：

- **安全事件分析**：主机发生安全事件后，通过日志功能进行调查，评估资产受损范围和影响。
- **操作审计**：对主机的操作日志进行审计，对高危操作和严重问题进行细粒度排查。

可检索日志类型

表 8-7: 日志源

日志源	说明
登录流水	系统登录成功的日志记录。
暴力破解	系统登录失败的日志记录。
进程快照	某一时刻主机上的进程运行信息。
端口监听快照	某一时刻主机上的监听端口信息。
账号快照	某一时刻主机上的账号登录信息。
进程启动日志	主机上进程启动的相关信息。
网络连接日志	主机对外主动连接的日志。

8.6.2 查询日志

搜索和查看主机日志。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **日志检索**。
3. 设置搜索条件。

表 8-8: 搜索条件说明

搜索项	说明
请选择日志源	支持的日志源，具体内容参考*表 8-9: 日志源*。
请选择字段	各日志源支持的字段，具体内容参考*表 8-9: 日志源*。
关键字	需要搜索的字段具体关键字。
语法逻辑	语法逻辑包括and、or、not，具体说明参考*表 8-17: 语法逻辑说明*。
+	在一个搜索条件（一个日志源）下增加多个逻辑判断。
增加一组	增加多个搜索条件（不同的日志源）。

4. 单击**搜索**，查看搜索结果。
   - **重置**：如果不需要原来设置的搜索条件，单击**重置**，搜索条件回到初始状态。
   - **保存搜索逻辑**：如果以后需要重用这个搜索条件，单击**保存搜索逻辑**进行保存。
   - **已保存的搜索**：如果需要执行以前保存的搜索条件，单击**已保存的搜索**，选择已有的搜索条件执行。

8.6.3 各日志源字段说明

本文介绍了日志检索功能可以采集并供检索的原始日志类型和字段说明。

日志检索功能支持您查询下表列述的日志源。您可以单击一个日志源查看其支持的字段信息。

表 8-9: 日志源

日志源	说明
登录流水	系统登录成功的日志记录。
暴力破解	系统登录失败的日志记录。
进程快照	某一时刻主机上的进程运行信息。
端口监听快照	某一时刻主机上的监听端口信息。
账号快照	某一时刻主机上的账号登录信息。
进程启动日志	主机上进程启动的相关信息。
网络连接日志	主机对外主动连接的日志。

登录流水

登录流水查询支持以下字段：

表 8-10: 登录流水支持字段

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
warn_ip	string	登录来源IP
warn_port	string	登录端口
warn_user	string	登录用户名
warn_type	string	登录类型
warn_count	string	登录次数
time	datetime	登录时间

暴力破解

暴力破解查询支持以下字段：

表 8-11: 暴力破解支持字段

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
warn_ip	string	攻击来源IP
warn_port	string	破解端口
warn_user	string	破解用户名
warn_type	string	类型
warn_count	string	破解次数
time	datetime	破解时间

进程启动日志

进程启动日志查询支持以下字段：

表 8-12: 进程启动日志支持字段

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
pid	string	进程ID
groupname	string	用户组
ppid	string	父进程ID
uid	string	用户ID
username	string	用户名
filename	string	文件名
pfilename	string	父进程文件名
cmdline	string	命令行
filepath	string	进程路径
pfilepath	string	父进程路径
time	datetime	启动时间

端口监听快照

端口监听快照查询支持以下字段：

表 8-13: 端口监听快照支持字段

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
src_port	string	监听端口
src_ip	string	监听IP
proc_path	string	进程路径
PID	string	进程ID
proc_name	string	进程名
proto	string	协议

字段	数据类型	说明
time	datetime	数据获取时间

账号快照

账号快照查询支持以下字段：

表 8-14: 账号快照支持字段

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
perm	string	是否拥有root权限
home_dir	string	home目录
warn_time	string	密码到期提醒时间
groups	string	用户属于的组
login_ip	string	最后一次登录的IP地址
last_chg	string	密码最后修改时间
shell	string	Linux的shell命令
domain	string	Windows域
tty	string	登录的终端
account_expire	string	账号超期时间
passwd_expire	string	密码超期时间
last_logon	string	最后登录时间
user	string	用户
status	string	用户状态： • 0表示禁用 • 1表示正常
time	datetime	数据获取时间

进程快照

进程快照查询支持以下字段：

表 8-15: 进程快照支持字段

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
path	string	进程路径
start_time	string	进程启动时间
uid	string	用户ID
cmdline	string	命令行
pname	string	父进程名
name	string	进程名
pid	string	进程ID
user	string	用户名
md5	string	进程文件MD5值，超过1MB不计算
time	datetime	数据获取时间

网络连接日志

网络连接日志查询支持以下字段：

表 8-16: 网络连接日志支持字段

字段	数据类型	说明
uuid	string	客户端编号
IP	string	IP地址
src_ip	string	源IP
src_port	string	源端口
proc_path	string	进程路径
dst_port	string	目标端口
proc_name	string	进程名
dst_ip	string	目标IP

字段	数据类型	说明
status	string	状态
proto	string	协议
time	datetime	连接时间

8.6.4 语法逻辑说明

日志检索支持多条件逻辑检索，您可以在一个搜索条件（一个日志源）下增加多个判断逻辑，也可以对多个搜索条件（不同的日志源）进行逻辑组合。本文介绍了日志检索支持的语法逻辑，也列举了部分用例，帮助您理解和使用。

日志检索支持下表中列举的语法逻辑。

表 8-17: 语法逻辑说明

逻辑名称	描述
and	双目运算符。 形式为`query1 and query2`，搜索结果展示`query1`和`query2`查询结果的交集。 **说明**： 如果多个单词间没有语法关键词，默认是and的关系。
or	双目运算符。 形式为`query1 or query2`，搜索结果展示`query1`和`query2`查询结果的并集。
not	双目运算符。 形式为`query1 not query2`，搜索结果展示符合`query1`并且不符合`query2`的结果，相当于`query1 - query2`。 **说明**： 如果只有`not query1`，那么表示从全部日志中选取不包含`query1`的结果。

8.7 设置

本章主要说明安全配置、告警配置、安装和卸载安骑士Agent插件。

8.7.1 管理安全配置

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **设置**。
3. 配置对服务器进行周期性木马查杀。
   a) 单击**管理**。
   b) 选择哪些服务器需要进行周期性的木马查杀。
   c) 单击**确认**，完成配置。
4. 配置安骑士Agent资源占用模式。
   - **业务优先模式**：CPU占用峰值小于10%，内存占用峰值小于50 MB。
   - **防护优先模式**：CPU占用峰值小于20%，内存占用峰值小于80 MB。

   a) 单击**管理**。
   b) 设置服务器的安骑士Agent工作模式。
   c) 单击**确认**，完成配置。

8.7.2 安装安骑士Agent插件

在Windows服务器或Linux服务器上手动安装安骑士Agent插件。

前提条件

如果您已在服务器上安装了安全软件（如安全狗、云锁等），可能会导致安骑士Agent插件无法正常安装，建议您暂时关闭或卸载该安全软件，然后再安装安骑士Agent插件。

背景信息

安骑士Agent插件已集成于公共镜像中。如果您在创建 ECS 实例时选择公共镜像，安骑士Agent插件将自动集成到ECS实例中。

非阿里云服务器必须通过安装程序（Windows）或脚本命令（Linux）方式安装安骑士Agent 插件。

如果您的非阿里云服务器通过以下方式安装安骑士Agent 插件，需要删除安骑士Agent插件目录后，按照上述手动安装步骤重新安装安骑士Agent 插件。

- 通过已安装安骑士Agent插件的镜像批量安装服务器。
- 从已安装安骑士Agent插件的服务器上直接复制安骑士Agent插件文件。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **设置** > **安装 / 卸载**。

   进入安骑士Agent插件安装页面，如图 *8-13: Agent安装*所示。

   图 8-13: Agent安装

3. 根据您的服务器操作系统，获取并安装安骑士Agent插件。
   - **Windows系统**
     1. 在左侧区域，单击**点击下载**，下载安装文件到本地计算机。
     2. 将安装文件上传至您的Windows服务器。例如，您可以通过FTP工具，将安装文件上传到服务器。
     3. 在Windows服务器上，以管理员权限运行安装文件，完成安装。

     > **说明**：
     > 在非阿里云服务器上安装Agent插件的过程中，您会收到提示，要求您输入安装验证Key。您可在安骑士Agent插件安装页面找到您的安装验证Key。

   - **Linux系统**
     1. 在右侧区域，根据您的实际情况，选择**阿里云服务器**或**非阿里云服务器**。

2. 根据您的操作系统类型，选择32位或64位的安装命令，单击**复制**。
3. 以管理员身份登录您的Linux服务器。
4. 在Linux服务器上执行安装命令，下载和安装安骑士Agent插件。

4. 查看服务器在线情况。

   安骑士Agent 插件安装完成约五分钟后，可以在云盾服务器安全（安骑士）管理控制台中查看您服务器的在线情况：

   - 阿里云服务器将会从离线变成在线。
   - 非阿里云服务器将会被添加至您的服务器列表中。

8.7.3 卸载安骑士Agent插件

如果云主机不再使用安骑士服务的所有功能，可以选择以下方式进行卸载安骑士Agent插件。

背景信息

通过控制台卸载指定主机安骑士Agent，请务必确保当前机器安骑士Agent处于在线状态，否则无法接收到卸载指令。

如果卸载后重新安装安骑士Agent，请手工进行安装，忽略期间的报错，重复操作3次以上（安骑士Agent卸载会有一段保护期24小时或重复执行3次以上安装命令）。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **设置** > **安装 / 卸载**。
3. 单击右上角的**卸载安骑士**。
4. 在**卸载提示**对话框中，选择要卸载安骑士Agent插件的服务器。
5. 单击**确认卸载**，系统将自动卸载安骑士Agent插件。

9 物理机防护

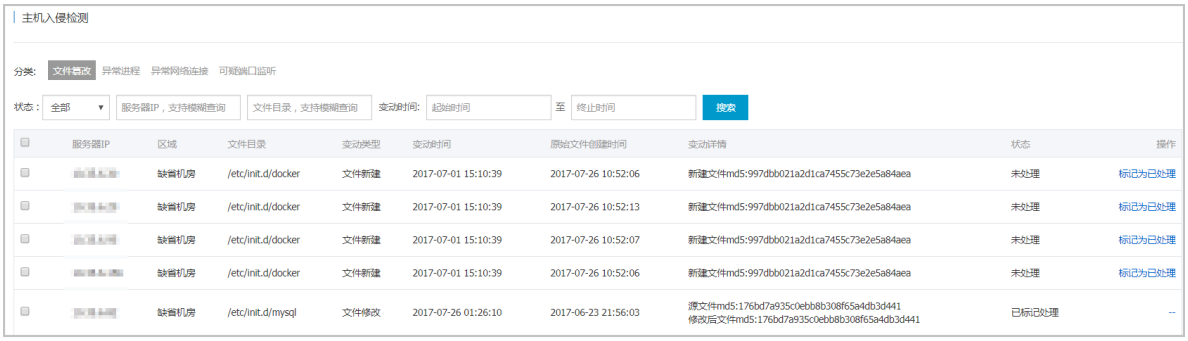
9.1 查看并处理文件篡改事件记录

监控主机系统特定目录中文件的完整性，及时发现篡改行为并进行告警。

操作步骤

1. 登录云盾控制台。
2. 定位到**物理机安全** > **物理机防护**页面，选择**文件篡改**。
3. 查看文件篡改事件记录，如图 *9-1: 文件篡改事件记录*所示。

图 9-1: 文件篡改事件记录



4. 进一步排查该文件篡改事件。
   - 如确认该事件为异常事件，请立即对该服务器采取安全加固措施，并建议进一步检查、分析被入侵的原因。
   - 如确认该事件为正常事件或已处理完该入侵事件，单击**标记为已处理**，在弹出的对话框中单击**确定**，将该事件标记为已处理。

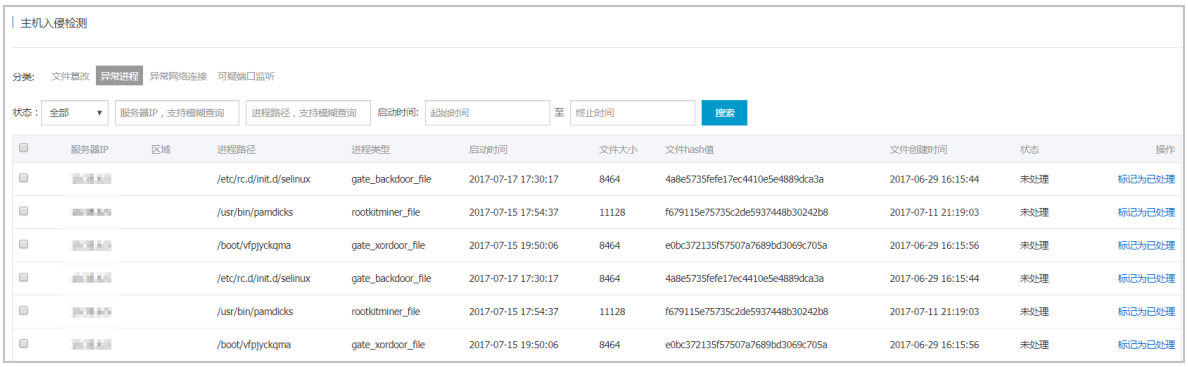
9.2 查看并处理异常进程记录

及时发现异常进程启动，并进行告警。

操作步骤

1. 登录云盾控制台。
2. 定位到**物理机安全** > **物理机防护**页面，选择**异常进程**。
3. 查看异常进程记录，如图 *9-2: 异常进程记录*所示。

图 9-2: 异常进程记录



4. 进一步排查该异常进程。
   - 如确认该进程为异常进程，请立即对该服务器采取安全加固措施，并进一步检查、分析被入侵的原因。
   - 如确认该进程为正常进程或已处理完该异常进程事件，单击**标记为已处理**，在弹出的对话框中单击**确定**，将该事件标记为已处理。

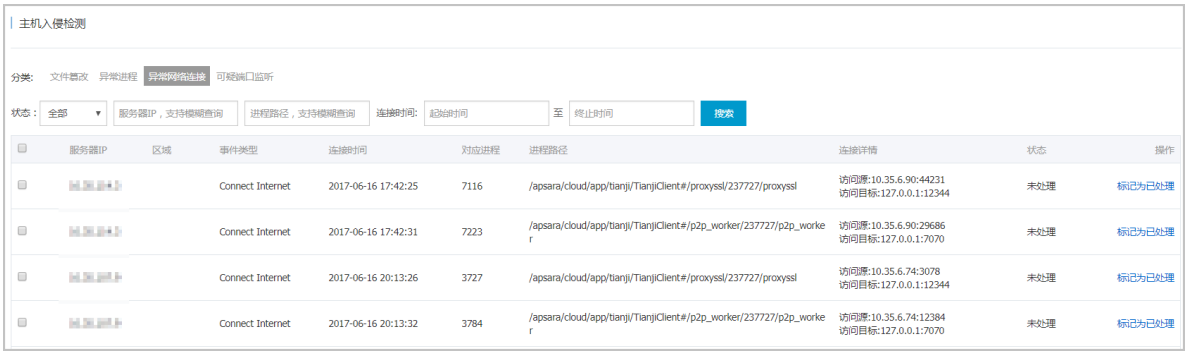
9.3 查看并处理异常网络连接记录

及时发现主动外连公网的网络连接，并进行告警。

操作步骤

1. 登录云盾控制台。
2. 定位到**物理机安全** > **物理机防护**页面，选择**异常网络连接**。
3. 查看异常网络连接记录，如图 *9-3:* 异常网络连接所示。

图 9-3: 异常网络连接



4. 进一步排查该异常网络连接。

- 如确认该进程为异常连接，请立即对该服务器采取安全加固措施，并进一步检查、分析被入侵的原因。
- 如确认该进程为正常连接或已处理完该异常网络连接事件，单击**标记为已处理**，在弹出的对话框中单击**确定**，将该事件标记为已处理。

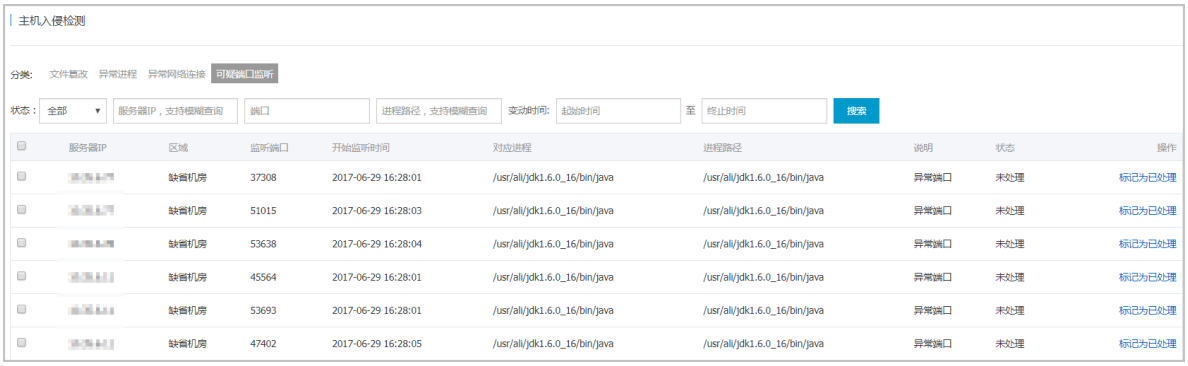
9.4 查看并处理异常端口监听记录

及时发现异常的端口监听，并进行告警。

操作步骤

1. 登录云盾控制台。
2. 定位到**物理机安全** > **物理机防护**页面，选择**可疑端口监听**。
3. 查看异常端口监听记录，如图 *9-4:* 异常端口监听记录所示。

图 9-4: 异常端口监听记录



4. 进一步排查该异常端口监听。
   - 如确认该进程为异常监听事件，请立即对该服务器采取安全加固措施，并进一步检查、分析被入侵的原因。
   - 如确认该进程为正常端口监听或已处理完该异常监听事件，单击**标记为已处理**，在弹出的对话框中单击**确定**，将该事件标记为已处理。

10 资产总览

云盾安全中心通过图表方式展现当前用户资产的总数（分为主机资产、NAT资产）、增减频率、以及区域分布等统计信息，并按分组、类型供安全管理员查询资产的相关信息，帮助安全管理员从整体了解资产情况，以便更好地管理资产。

安全管理员可以在**资产管理** > **资产总览**页面，直观了解到资产概览信息，包括资产总数、本月新增资产数、分组数目、区域数目、资产上报时间分布图、资产所属分组分布图、资产所属区域分布图，帮助用户更好地管理资产，如图 *10-1:* 资产总览页面所示。

图 10-1: 资产总览页面

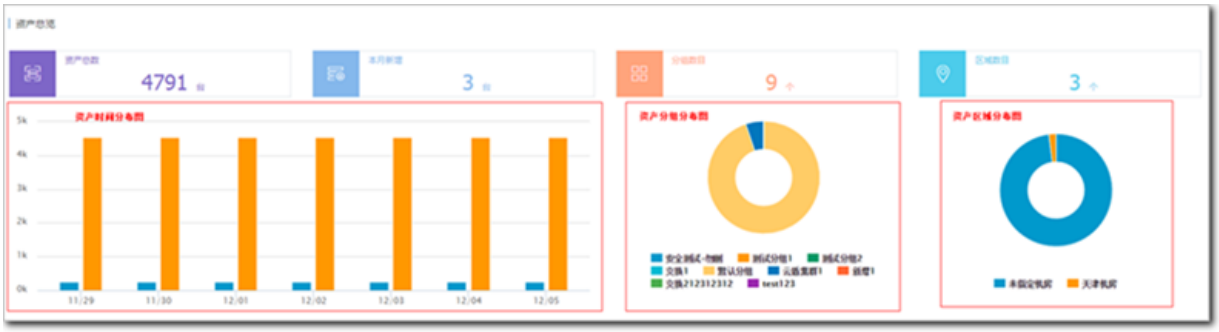


表 10-1: 资产总览页面参数说明表

参数	说明
资产总数	安骑士客户端上报的资产总数，包含主机资产和NAT资产。
本月新增资产数	本月新增的资产总数，包含主机资产和NAT资产。
资产时间分布图	七天内资产数量的变化情况，分主机资产、NAT资产进行统计。
分组数目	当前已有的分组数目。
资产分组分布图	资产分组比例图是按每个分组内的资产数占总资产数目的比例计算的。
区域数目	当前配置的区域数目。
资产区域分布图	资产区域分布图是按每个区域内的资产数占总资产数目的比例计算的。

10.1 分组管理

分组管理主要用于对资产分组的增加、删除、重新排序。将资产分组，用于区分不同资产的特定作用，便于查询资产信息并对资产信息进行修改。

说明：

- 资产分组最多只支持10个分组。
- 默认分组不可被删除且不可更改名称。
- 资产分组中存在资产时不可被删除。

10.1.1 添加分组

操作步骤

1. 登录云盾控制台。
2. 定位到**资产管理** > **资产总览**页面，单击**分组管理**。

   图 10-2: 分组管理

3. 在弹出**业务分组**对话框，单击**添加分组**，如图 *10-3:* 业务分组对话框所示。

图 10-3: 业务分组对话框

4. 填写分组名称。
5. 单击**确认**，添加资产分组。

10.1.2 删除分组

操作步骤

1. 登录云盾控制台。
2. 定位到**资产管理** > **资产总览**页面，单击**分组管理**。
3. 在**业务分组**对话框内，单击对应分组条目后的**删除**，如图 *10-4: 删除业务分组*所示。

图 10-4: 删除业务分组

4. 单击**确认**，删除该资产分组。

10.1.3 调整分组排序

操作步骤

1. 登录云盾控制台。
2. 定位到**资产管理** > **资产总览**页面，单击**分组管理**。
3. 通过单击**业务分组**对话框内各个条目后的**上移**、**下移**进行排序调整。
4. 单击**确认**，完成资产分组的排序调整。

10.2 资产信息

资产分为主机资产和 NAT 资产，两种资产的信息和管理方式略有差异，可以通过切换查看不同类型的资产信息。

表 10-2: 资产类型表

资产类型	说明
主机资产	安骑士客户端防护的服务器资产。
NAT资产	内网地址经过NAT转换，暴露给外网的IP资产。

10.2.1 管理主机资产

主机资产主要是指服务器资产，安装安骑士客户端并连接到服务器后，将会上报为资产。

背景信息

通过查询主机资产，安全管理员可以掌握各资产的大致情况，例如操作系统、开放端口、已安装的常用软件，也可以对资产的区域和分组进行调整。

操作步骤

1. 登录云盾控制台。
2. 定位到**资产管理** > **资产总览**页面，选择**主机资产**。

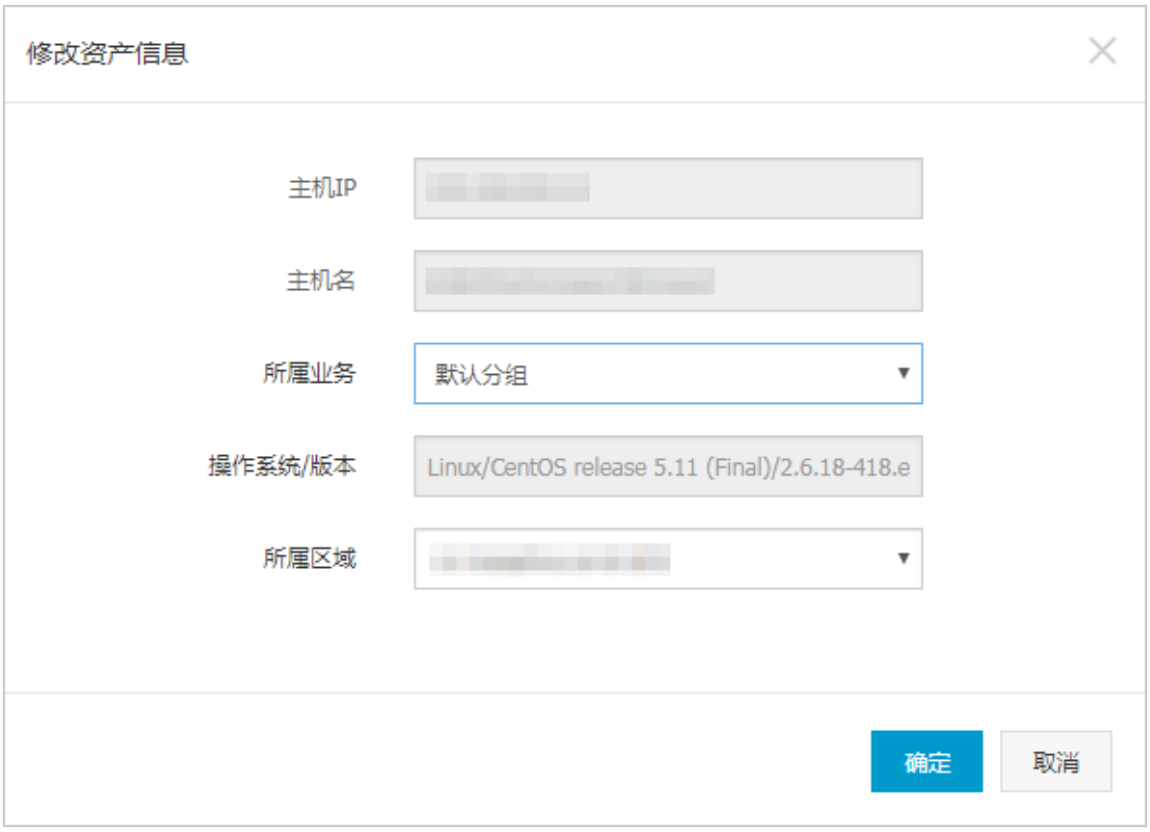
3. 设置查询条件，单击**查询**，查看主机资产信息，如图 *10-5: 主机资产页面*所示。

> **说明**：
> 主机资产的查询支持根据操作系统、区域、分组进行筛选，并支持通过主机IP及主机名进行模糊查询。默认情况下，主机资产页面展示全部区域，并按照IP排序。

图 10-5: 主机资产页面

4. 选择主机，查看详细信息。
   - 单击**详情**，可以查看主机端口开放情况。
   - 单击**展开应用信息**，可以查看主机已有的可监测应用信息。
5. 维护主机资产信息。
   - 单击**修改**，在**修改资产信息**对话框修改所属资产分组及所属区域，单击**确定**，如图 *10-6: 修改资产信息对话框*所示。

图 10-6: 修改资产信息对话框



- 单击**删除**，在**资产信息删除**对话框中单击**确定**进行删除。

> **说明**：
> 如果在云服务器中卸载了安骑士客户端，或者在专有云平台中删除了一台ECS云服务器，这些主机对应的资产需要手动删除。

10.2.2 管理NAT资产

NAT资产，也可以理解为IP资产，是指内网地址经过NAT转换来访问互联网的IP资产，即暴露给外网的IP地址资产。该IP可能会被很多主机使用，不同端口可以指向不同主机。当IP被设置为NAT资产后，态势感知模块会对其进行分析，从而发现一些攻击事件。

背景信息

通过查询NAT资产，安全管理员可以了解当前云盾防护的NAT资产的基本信息，也可以对资产进行分组和区域的修改，NAT资产支持单个资产添加以及按网段批量添加。

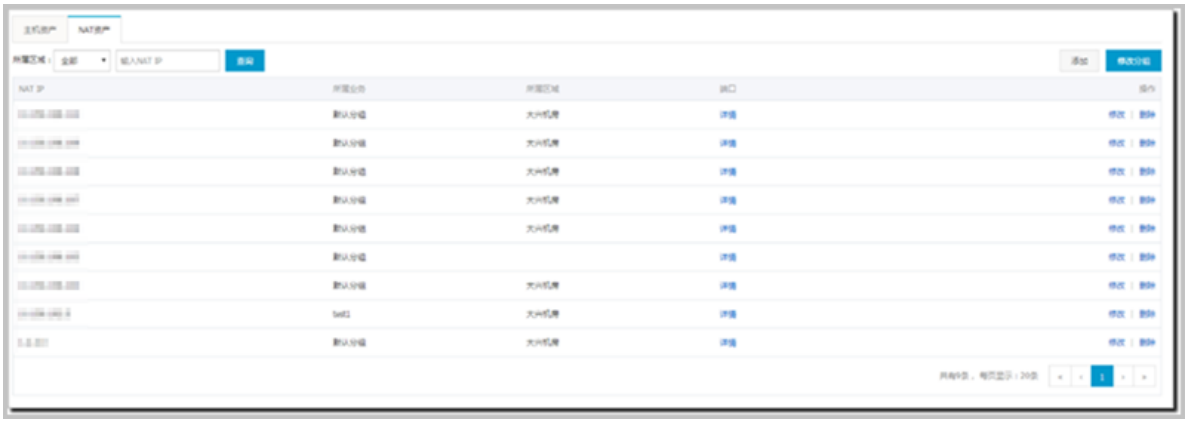
操作步骤

1. 登录云盾控制台。

2. 定位到**资产管理** > **资产总览**页面，选择**NAT资产**。
3. 设置查询条件，单击**查询**，查看NAT资产信息，如图 *10-7: NAT资产页面*所示。

> **说明**：
> NAT资产的查询支持通过区域、分组进行筛选，支持根据IP进行模糊查询。默认情况下，NAT资产页面展示全部区域，并按照IP排序。

图 10-7: NAT资产页面



4. 添加新的NAT资产。

   添加的资产IP不能与当前已有IP冲突。NAT IP字段必须为合法IP或者为合法网段。

   a) 在**NAT资产页面**，单击列表右上方的**添加**。
   b) 在**添加资产信息**对话框中，输入IP地址或者IP表达式，选择所属业务和所属区域。
   c) 单击**确定**。

5. 维护NAT资产信息。

   - 单击**详情**，可以查看该NAT资产的端口开放情况。
   - 单击**修改**，在修改资产信息对话框中，修改该资产所属业务分组和所属区域，单击**确定**，如图 *10-8: 修改资产信息对话框*所示。

图 10-8: 修改资产信息对话框

- 单击**删除**，在**资产信息删除**对话框中单击**确定**，可删除该NAT资产。

10.2.3 批量修改资产所属分组或区域

背景信息

资产管理功能支持通过两种方式来修改资产的所属分组和所属区域：单个修改和批量修改。

- 单个修改适用于需要修改信息的资产数量只有一台；或者，需要修改的资产既不在同一网段，主机名也没有任何规律。单个资产的修改方法，参见管理主机资产和管理*NAT*资产。
- 批量修改适用于对多台资产进行修改并且这些资产属于同一个网段或拥有相似的主机名。

说明：

主机IP、主机名和操作系统/版本是资产的固有信息不能修改。

操作步骤

1. 登录云盾控制台。
2. 定位到**资产管理** > **资产总览**页面。
3. 修改资产所属分组或所属区域。
   - 单击**修改分组**，批量修改资产分组。
   - 单击**修改区域**，批量修改资产区域。

4. 在**修改分组**或**修改区域**对话框中，根据实际情况设置批量修改范围，选择这些资产需要分配到的资产分组或区域，单击**确定**。
   - 选择**网段**类型，输入所需批量修改的主机资产或NAT资产的所属网段。
   - 选择**主机名**类型，输入所需批量修改的主机资产主机名所共有的部分。

说明：

- 使用网段类型进行批量修改，符合所设置的网段范围的主机资产和NAT资产都会被修改。
- 使用主机名类型进行批量修改，只有符合所设置的主机名范围的主机资产被修改。

11 数据发现与脱敏

11.1 登录专有云数据安全控制台

专有云数据安全控制台面向专有云平台租户开放，可供租户为自己部门中的数据库进行数据抽取、数据脱敏和数据隐藏等的数据处理操作。

前提条件

确认您所使用的账号已具备相应部门的云资源权限，例如具备部门管理员角色权限。

操作步骤

1. 登录云盾控制台。
2. 定位到**数据安全** > **数据发现与脱敏**，单击**DDM**，如图 *11-1:* 登录数据发现与脱敏控制台所示。

图 11-1: 登录数据发现与脱敏控制台

11.2 专有云数据安全控制台界面

专有云数据安全控制台的界面主要分为三大区域，功能菜单、数据统计、任务信息，如图 *11-2:* 专有云数据安全控制台界面所示。

图 11-2: 专有云数据安全控制台界面

各区域详细说明如表 *11-1:* 专有云数据安全控制台区域说明所示。

表 11-1: 专有云数据安全控制台区域说明

区域	说明
功能菜单	单击不同的功能菜单时，将进入相应功能的界面。
数据统计	展示已发现的敏感数据的统计和分布信息。
任务信息	展示最近发生的数据发现及脱敏任务数据。

11.3 使用指南

11.3.1 数据源管理

登录专有云数据安全控制台之后，您可以连接生产数据库、文件源等数据源，并对数据源进行管理。

11.3.1.1 数据库

11.3.1.1.1 添加数据库

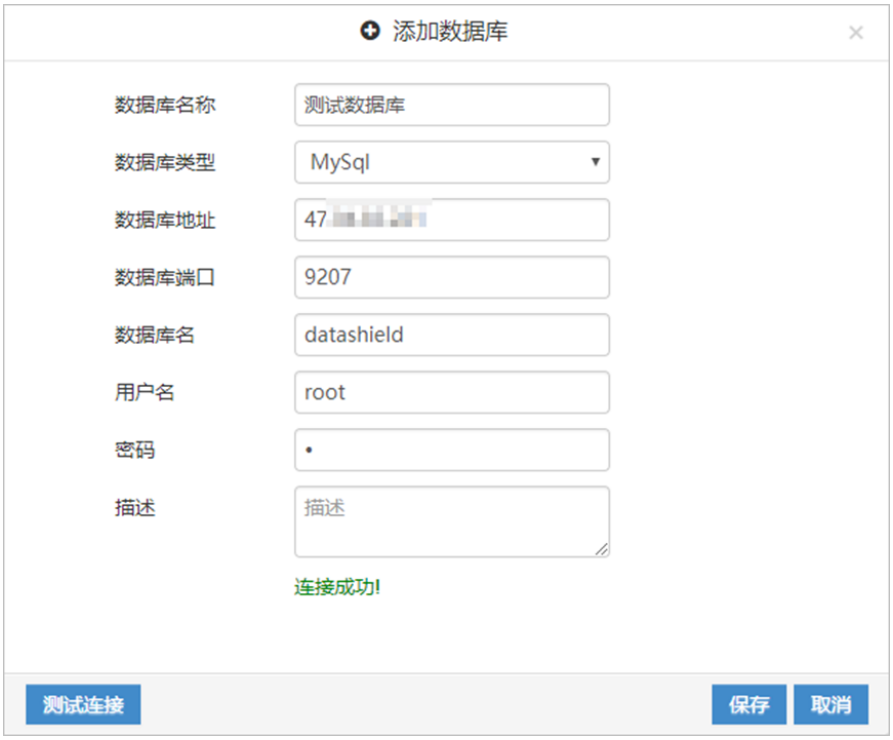
操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据源管理** > **数据库列表**页面，单击**添加数据库**，如图 *11-3:* 数据库列表页面所示。

图 11-3: 数据库列表页面

3. 在**添加数据库**对话框中，输入数据库名称，选择数据库类型，输入数据库地址、数据库端口、数据库名、用户名、密码、描述等信息，如*图 11-4: 添加数据库*所示。

图 11-4: 添加数据库



4. 单击**测试连接**。

> **说明**：
> 如果测试连接失败，请检查输入的数据库信息是否正确，建议仅在测试连接成功时保存数据库信息。

5. 连接测试成功后，单击**保存**，即完成数据库的添加。

> **说明**：

- 数据库名称不允许重复。
- 数据库信息记录不允许重复。
- 对于Oracle类型的数据库，通过“数据库主机IP + 数据库主机端口 + 数据库实例名”的方式确定唯一的数据库信息记录。

11.3.1.1.2 修改数据库

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据源管理** > **数据库列表**页面，选择需要修改的数据库信息记录，单击右侧的编辑按钮，如图 *11-5: 编辑数据库*所示。

图 11-5: 编辑数据库

3. 在**编辑数据库**对话框中，修改数据库信息，单击**保存**。

说明：
数据库类型无法修改。

11.3.1.1.3 删除数据库

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据源管理** > **数据库列表**页面，选择需要删除的数据库信息记录，单击右侧的删除按钮，如图 *11-6: 删除数据库*所示。

图 11-6: 删除数据库

3. 在**信息提示**对话框中，单击**确定**，删除该数据库信息记录，如图 *11-7: 确认删除提示*所示。

图 11-7: 确认删除提示

说明：

删除数据库信息记录时，如果该数据库信息与专有云数据安全系统内其他数据存在关联，将无法删除该数据库信息记录，如图 *11-8: 删除数据库信息提示*所示。这种情况下，您需要先完成该数据库关联信息的清理，才可删除该数据库信息记录。

图 11-8: 删除数据库信息提示

11.3.1.1.4 查询数据库

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据源管理** > **数据库列表**页面，输入数据库名称或IP地址，单击**搜索**，如图 *11-9: 搜索数据库信息记录*所示，即可查询包含所输入信息的数据库信息记录。

说明：

数据库搜索功能支持模糊查询。

图 11-9: 搜索数据库信息记录

3. 选择数据库信息记录，单击右侧的查看按钮，可查看该数据库的详细信息，如图 *11-10: 查看数据库*所示。

图 11-10: 查看数据库

11.3.1.2 文件源

专有云数据安全支持将数据库导出的数据文件作为数据源进行脱敏处理，支持csv和txt格式的平面文件。

从数据库导出的平面文件相当于一张数据库表，若干个平面文件的集合则相当于一个数据库。因此，专有云数据安全定义了**文件源**的概念，在同一个文件源中的平面文件，具有相同的存储位置和管理方式，且这些文件内部具有逻辑关系。

11.3.1.2.1 添加文件源

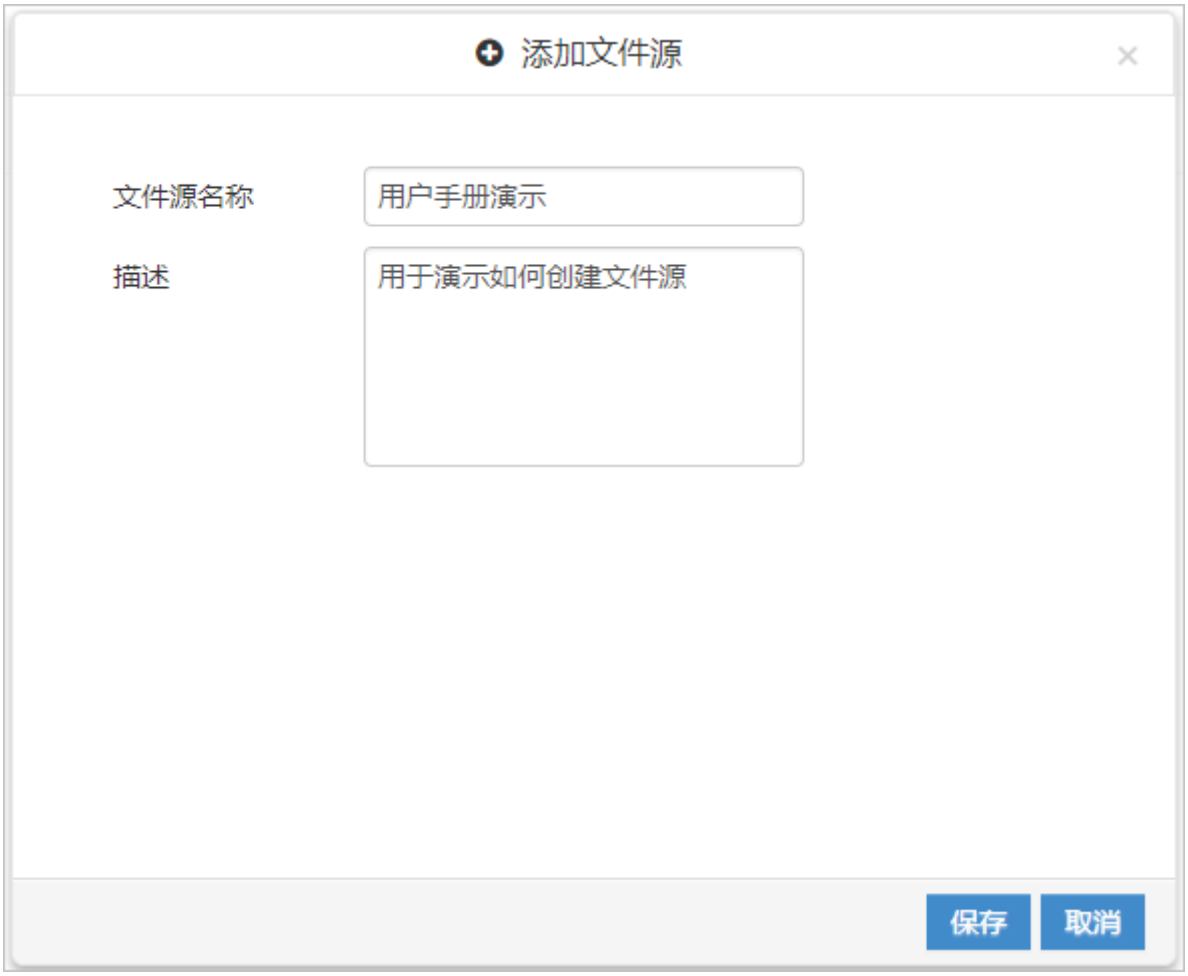
操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据源管理** > **文件源列表**页面，单击**添加**，如图 *11-11: 文件源列表页面*所示。

图 11-11: 文件源列表页面

3. 在**添加文件源**对话框中，输入文件源名称、描述，单击**保存**，如图 *11-12: 添加文件源*所示。

图 11-12: 添加文件源



说明：

文件源名称不允许重复。

11.3.1.2.2 添加文件

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据源管理** > **文件源列表**页面，选择文件源信息记录，单击右侧的文件列表按钮，如图 *11-13: 打开文件列表*所示。

   图 11-13: 打开文件列表

3. 在**文件列表**对话框中，单击**添加**，如图 *11-14: 文件列表对话框*所示。

   图 11-14: 文件列表对话框

4. 在**添加文件**对话框中，单击**选择文件**，选择一个数据文件。

5. 选择该文件的字符集、行分隔符、列包围符、列分隔符、日期格式、日期分隔符、时间分隔符、小数点符、日期时间排序、是否有表头，单击**保存**，如图 *11-15: 添加文件*所示，将该文件添加到文件源中。

图 11-15: 添加文件

说明：

- 添加文件时，文件源名称无法修改。
- 同一文件源中，无法添加重复文件。

11.3.1.2.3 修改文件

操作步骤

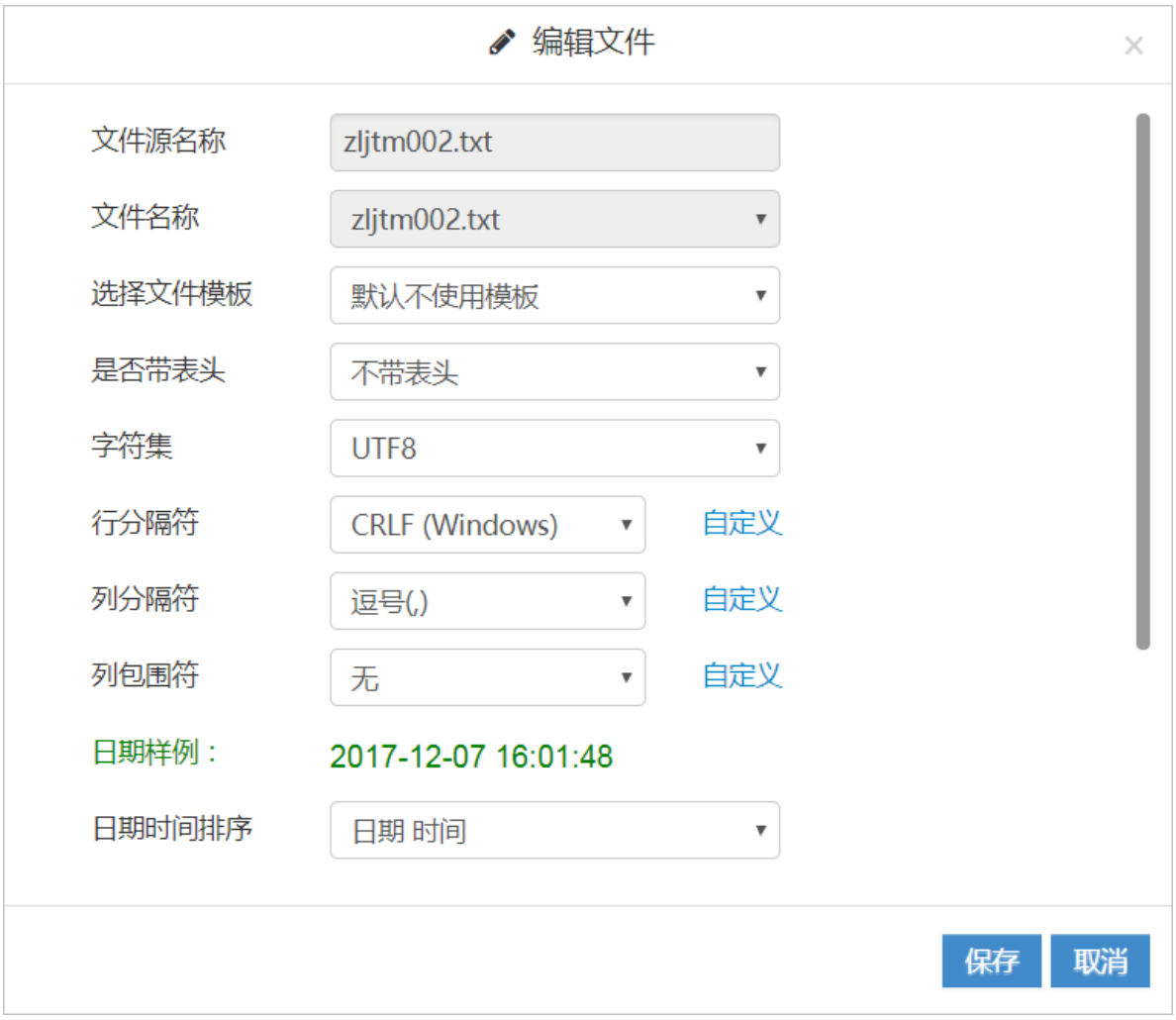
1. 登录专有云数据安全控制台。
2. 定位到**数据源管理** > **文件源列表**页面，选择文件源信息记录，单击右侧的文件列表按钮。

3. 在**文件列表**对话框中，选择已添加的文件，单击右侧的编辑按钮，如图 *11-16:* 文件列表所示。

图 11-16: 文件列表

4. 在**编辑文件**对话框中，修改该文件的相关设置信息，单击**保存**，如图 *11-17:* 编辑文件所示。

图 11-17: 编辑文件



说明：

在**编辑文件**对话框中，文件源名称及文件名称无法修改。

11.3.1.2.4 删除文件

前提条件

删除文件前，请确认该文件与专有云数据安全系统中其它数据已无关联。

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据源管理** > **文件源列表**页面，选择文件源信息记录，单击右侧的文件列表按钮。
3. 在**文件列表**对话框中，选择已添加的文件，单击右侧的删除按钮，如图 *11-18: 文件列表*所示。

图 11-18: 文件列表

4. 在**信息提示**对话框中，单击**确定**，如图 *11-19: 删除文件提示*所示，删除该文件。

图 11-19: 删除文件提示

11.3.1.2.5 修改文件源

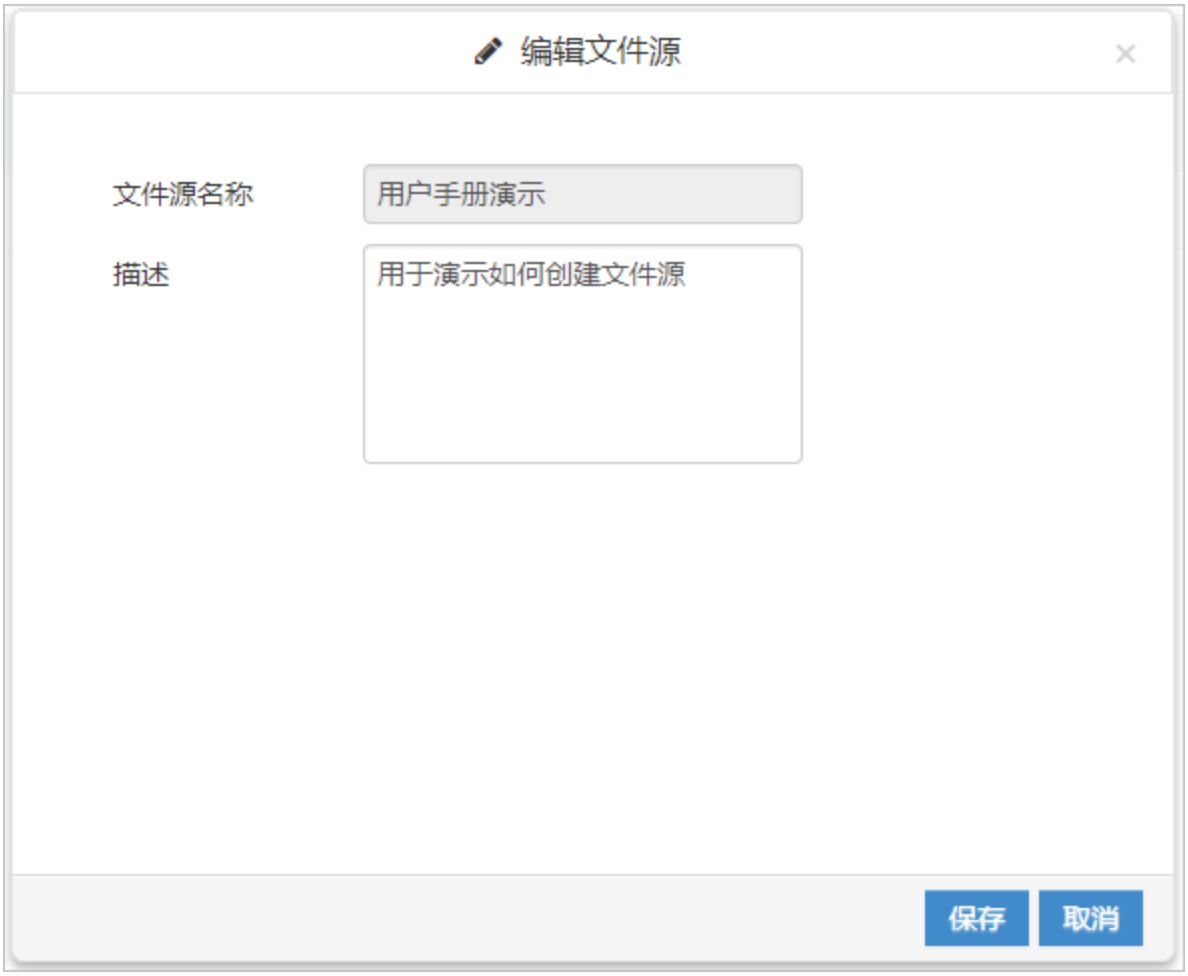
操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据源管理** > **文件源列表**页面，选择文件源信息记录，单击右侧的编辑文件源按钮，如图 *11-20: 文件源列表*所示。

图 11-20: 文件源列表

3. 在**编辑文件源**对话框中，修改文件源描述，如图 *11-21:* 编辑文件源所示。

图 11-21: 编辑文件源



说明：

文件源名称无法修改。

11.3.1.2.6 删除文件源

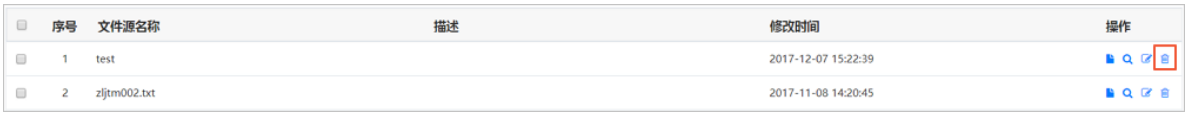
前提条件

删除文件源前，请确认该文件源记录与专有云数据安全系统内其他数据已无关联。

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据源管理** > **文件源列表**页面，选择文件源信息记录，单击右侧的删除文件源按钮，如图 *11-22: 文件源列表*所示。

图 11-22: 文件源列表



3. 在**信息提示**对话框中，单击**确定**，如图 *11-23: 删除文件源提示*所示，删除该文件源。

图 11-23: 删除文件源提示

11.3.1.2.7 查询文件源

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据源管理** > **文件源列表**页面，输入文件源名称，单击**搜索**，如图 *11-24: 搜索文件源*所示，即可查询包含所输入信息的文件源信息记录。

> **说明**：
> 文件源搜索功能支持模糊查询。

图 11-24: 搜索文件源

3. 选择文件源信息记录，单击右侧的查看按钮，如图 *11-25: 查看文件源*所示，可查看该文件源的详细信息。

图 11-25: 查看文件源

11.3.2 数据发现

专有云数据安全支持按照所选的发现规则，对数据库和文件源中的数据库表和文件进行敏感数据识别，并展示识别结果。

11.3.2.1 发现任务

11.3.2.1.1 数据库发现任务

11.3.2.1.1.1 添加数据库发现任务

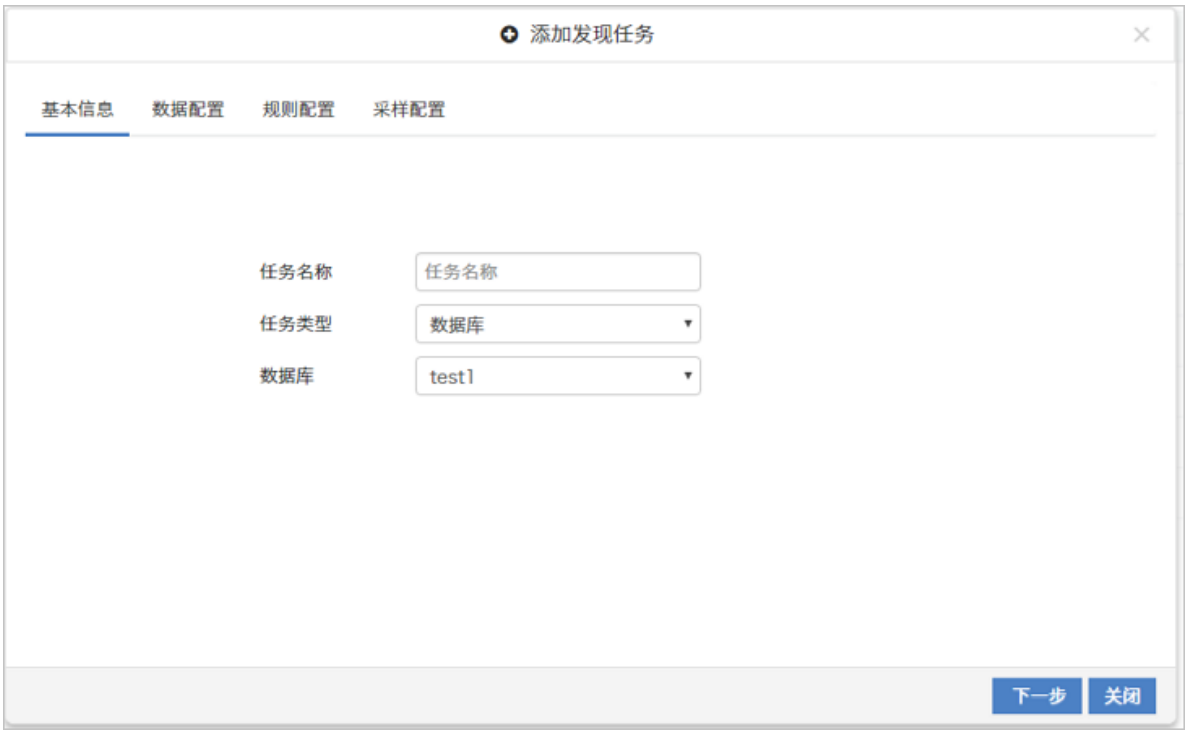
操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现任务**页面，单击**添加**，如图 *11-26: 发现任务列表*所示。

图 11-26: 发现任务列表

3. 在**添加发现任务**对话框的**基本信息**页签中，输入任务名称，选择数据库任务类型，选择数据库，单击**下一步**，如图 *11-27: 添加发现任务基本信息页签*所示。

图 11-27: 添加发现任务基本信息页签

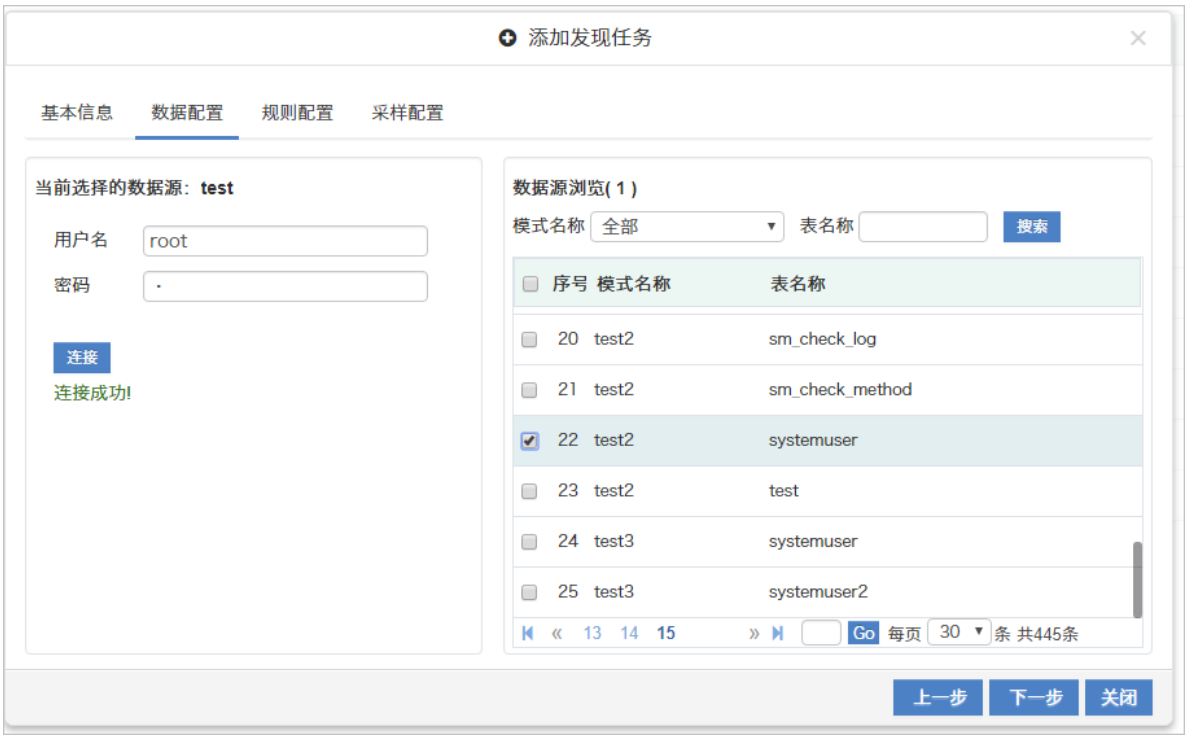


说明：

任务名称不可重复。

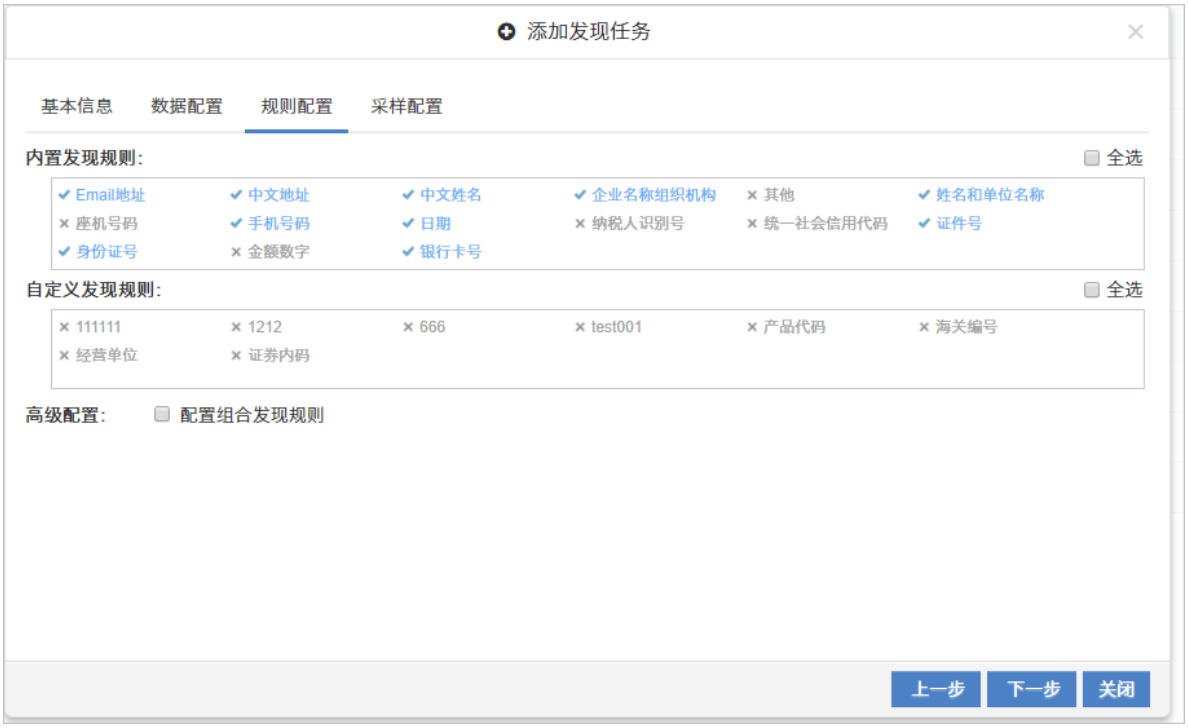
4. 在**添加发现任务**对话框的**数据配置**页签中，输入用户名、密码，单击**连接**。
5. 测试连接成功后，在右侧显示的模式及数据库表信息中，勾选您想要执行发现任务的数据库表，单击**下一步**，如图 *11-28:* 添加发现任务数据配置页签所示。

图 11-28: 添加发现任务数据配置页签



6. 在**规则配置**页签中，选择发现规则，单击**下一步**，如图 *11-29:* 添加发现任务规则配置页签所示。

图 11-29: 添加发现任务规则配置页签



说明：

关于发现规则的具体介绍参见发现规则。

7. 在**采样配置**页签中，设置采样规则，单击**保存**，如图 *11-30: 添加发现任务采样配置页签*所示，即可完成数据库发现任务的添加。

图 11-30: 添加发现任务采样配置页签

采样规则举例：

- 假设数据库表中有10000行数据，采样前1000行，再抽取数据的1‰进行分析，则一共会抽取1000+(10000-1000)*1‰=1009行数据根据发现规则进行数据发现。
- 假设数据库表中有800行数据，采样前1000行，再抽取数据的1‰进行分析，则一共会抽取800行数据进行发现规则验证。

11.3.2.1.1.2 执行数据库发现任务

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现任务**页面，选择已添加的数据库发现任务，单击任务记录右侧的操作列表，单击**运行任务**，如图 *11-31: 发现任务列表*所示。

图 11-31: 发现任务列表

3. 在**运行发现任务**对话框中，输入用户名、密码，选择是否启用发现关系，单击**检测**，如图 *11-32: 运行发现任务*所示。

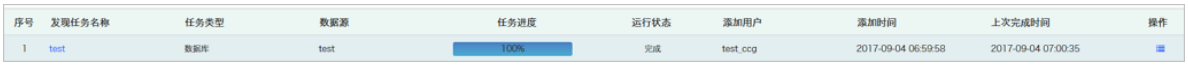
> **说明**：
> 启用发现关系后，在运行数据库发现任务时可发现数据库中数据表之间的关系。关于数据关系发现的具体介绍参见数据关系。

图 11-32: 运行发现任务

4. 检测通过后，单击**运行**，该数据库发现任务即开始执行。

等待数据库发现任务执行完毕，如图 *11-33: 数据库发现任务执行完成*所示。

图 11-33: 数据库发现任务执行完成



11.3.2.1.1.3 停止数据库发现任务

背景信息

当数据库发现任务运行时，可以参考以下操作步骤停止该发现任务：

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现任务**页面，选择正在执行的数据库发现任务，单击任务记录右侧的操作列表，单击**停止任务**，如图 *11-34: 发现任务列表*所示，即可终止正在执行的发现任务。

图 11-34: 发现任务列表

11.3.2.1.1.4 查看数据库发现任务的历史记录

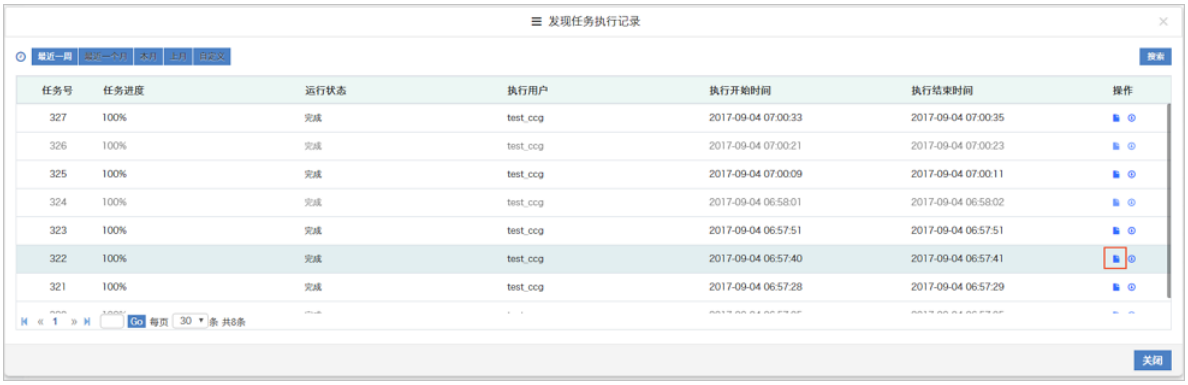
操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现任务**页面，选择已执行的数据库发现任务，单击任务记录右侧的操作列表，单击**历史任务**，如图 *11-35: 发现任务列表*所示。

图 11-35: 发现任务列表

3. 在**发现任务执行记录**对话框中，选择任务记录，单击右侧的执行报告按钮，如图 *11-36:* 发现任务执行记录所示。

图 11-36: 发现任务执行记录

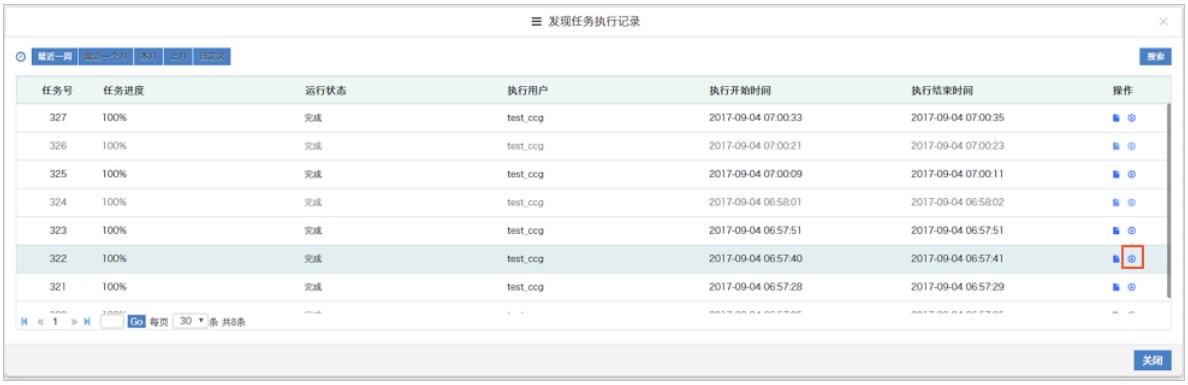


4. 在**发现任务执行报告**页面中，查看该发现任务的执行信息，如图 *11-37:* 发现任务执行报告所示。

图 11-37: 发现任务执行报告

5. 在**发现任务执行记录**对话框中，选择任务记录，单击右侧的下载执行日志按钮，如图 *11-38: 下载执行日志*所示，可将该发现任务的执行日志下载到本地。

图 11-38: 下载执行日志



11.3.2.1.1.5 编辑数据库发现任务

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现任务**页面，选择已添加的数据库发现任务，单击任务记录右侧的操作列表，单击**编辑任务**，如图 *11-39: 发现任务列表*所示。

图 11-39: 发现任务列表

3. 在**编辑发现任务**对话框中，可变更需要被发现的数据库表、发现规则、采样规则，修改完成后，单击**保存**，如图 *11-40: 编辑发现任务*所示。

图 11-40: 编辑发现任务

说明：

任务名称、任务类型、和数据库无法修改。

11.3.2.1.1.6 查看数据库发现任务

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现任务**页面，选择已添加的数据库发现任务，单击任务发现名称。
3. 在**发现任务详情**页面，查看该数据库发现任务的详细信息，如图 *11-41:* 发现任务详情页面所示。

图 11-41: 发现任务详情页面

11.3.2.1.1.7 删除数据库发现任务

前提条件

删除数据库发现任务前，请确认该发现任务与专有云数据安全系统中其它数据已无关联。

操作步骤

1. 登录专有云数据安全控制台。

2. 定位到**数据发现** > **发现任务**页面，选择已添加的数据库发现任务，单击任务记录右侧的操作列表，单击**删除任务**，如图 *11-42: 发现任务列表*所示。

图 11-42: 发现任务列表

3. 在**信息提示**对话框中，单击**确定**，删除该数据库发现任务。

11.3.2.1.2 文件发现任务

11.3.2.1.2.1 添加文件发现任务

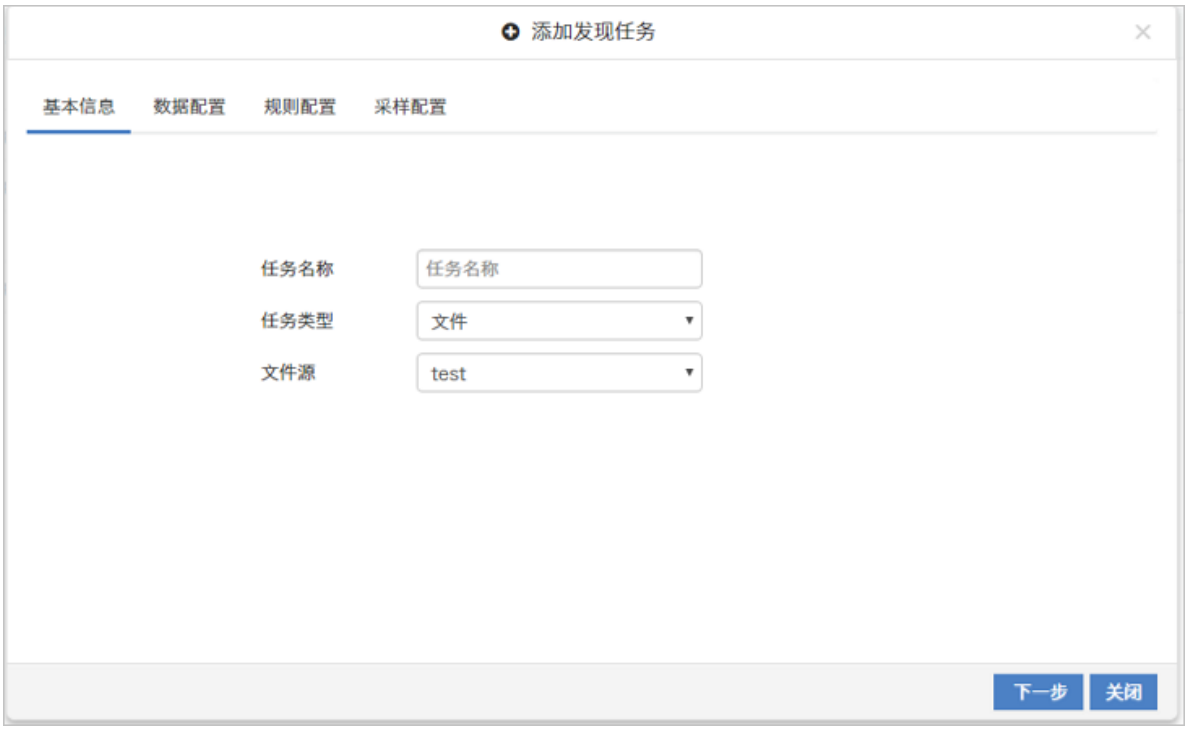
操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现任务**页面，单击**添加**，如图 *11-43: 发现任务列表*所示。

图 11-43: 发现任务列表

3. 在**添加发现任务**对话框的**基本信息**页签中，输入任务名称，选择文件任务类型，选择文件源，单击**下一步**，如图 *11-44: 添加发现任务基本信息页签*所示。

图 11-44: 添加发现任务基本信息页签

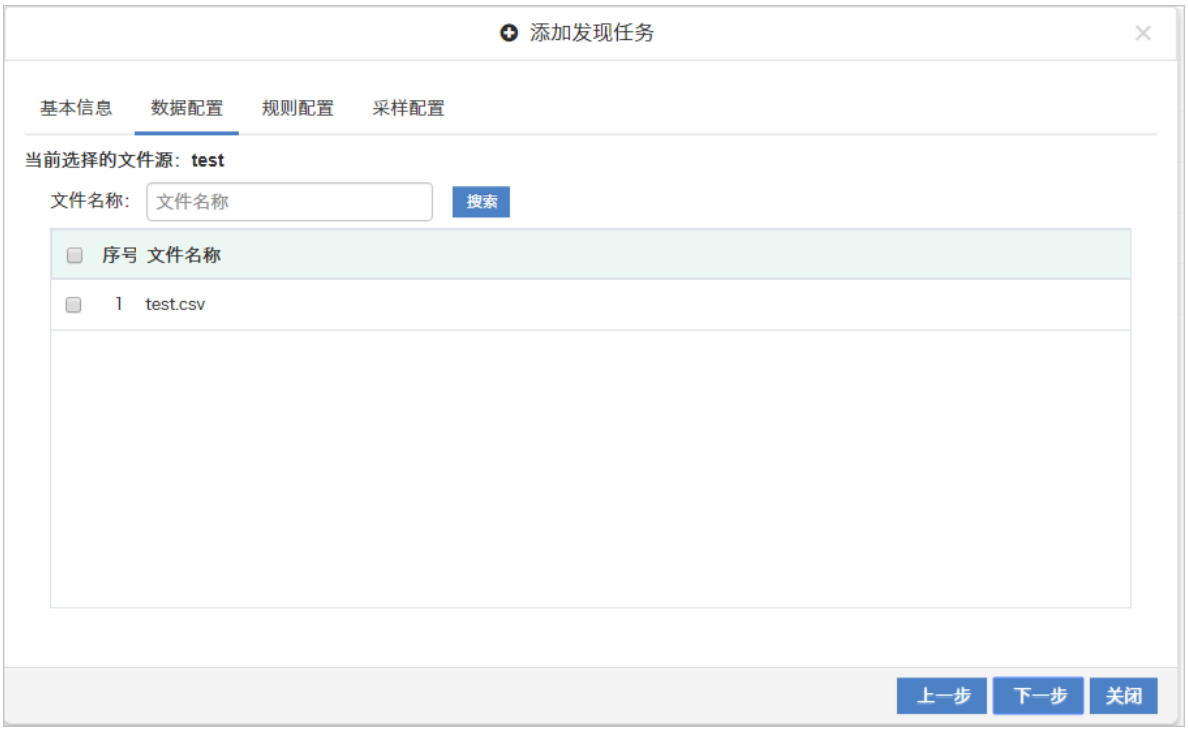


说明：

任务名称不可重复。

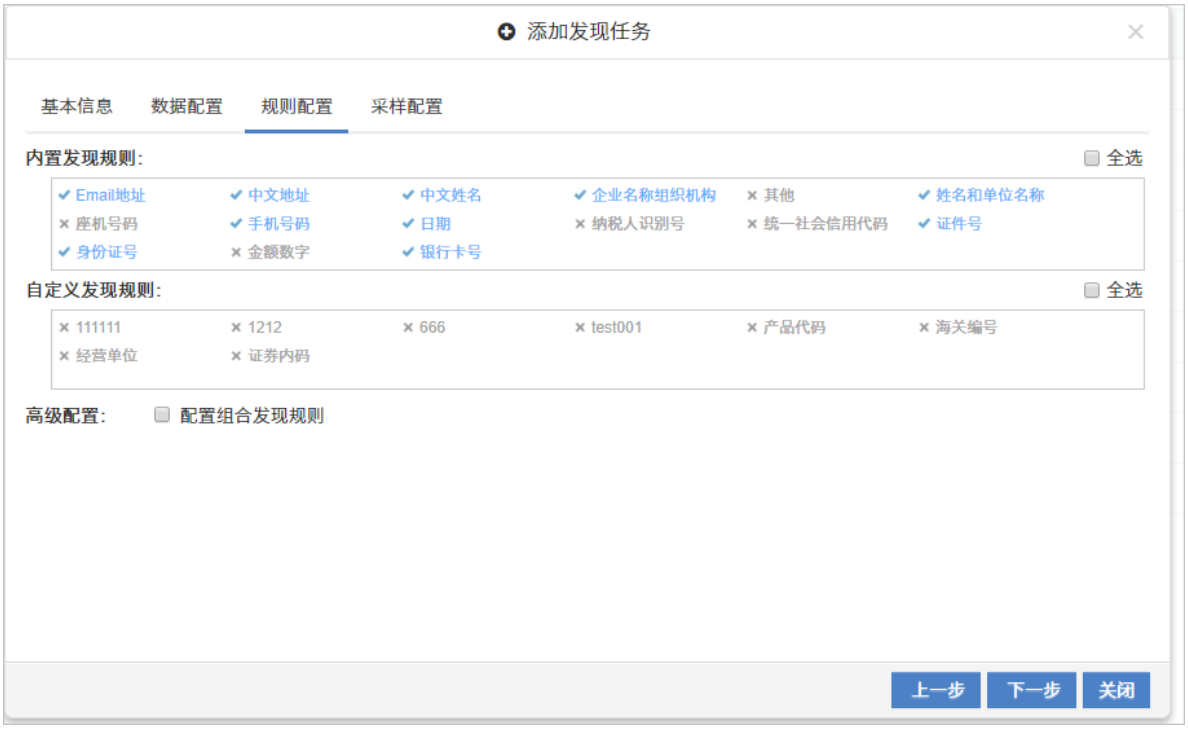
4. 在**添加发现任务**对话框的**数据配置**页签中，勾选您想要执行发现任务的文件，单击**下一步**，如*图 11-45: 添加发现任务数据配置页签*所示。

图 11-45: 添加发现任务数据配置页签



5. 在**规则配置**页签中，选择发现规则，单击**下一步**，如图 *11-46: 添加发现任务规则配置页签*所示。

图 11-46: 添加发现任务规则配置页签



6. 在**采样配置**页签中，设置采样规则，单击**保存**，如图 *11-47:* 添加发现任务采样配置页签所示，即可完成文件发现任务的添加。

图 11-47: 添加发现任务采样配置页签

说明：

关于发现规则的具体介绍参见发现规则。

采样规则举例：

- 假设数据库表中有10000行数据，采样前1000行，再抽取数据的1‰进行分析，则一共会抽取1000+(10000-1000)*1‰=1009行数据根据发现规则进行数据发现。
- 假设数据库表中有800行数据，采样前1000行，再抽取数据的1‰进行分析，则一共会抽取800行数据进行发现规则验证。

11.3.2.1.2.2 执行文件发现任务

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现任务**页面，选择已添加的文件发现任务，单击任务记录右侧的操作列表，单击**运行任务**，如图 *11-48:* 发现任务列表所示。

图 11-48: 发现任务列表

3. 在**运行发现任务**对话框中，单击**检测**，如图 *11-49:* 运行发现任务所示。

图 11-49: 运行发现任务

4. 检测通过后，单击**运行**，该文件发现任务即开始执行。

11.3.2.1.2.3 停止文件发现任务

背景信息

当文件发现任务运行时，可以参考以下操作步骤停止该发现任务：

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现任务**页面，选择正在执行的文件发现任务，单击任务记录右侧的操作列表，单击**停止任务**，如图 *11-50: 停止文件发现任务*所示，即可终止正在执行的发现任务。

图 11-50: 停止文件发现任务

11.3.2.1.2.4 查看文件发现任务的历史记录

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现任务**页面，选择已执行的文件发现任务，单击任务记录右侧的操作列表，单击**历史任务**，如图 *11-51: 发现任务列表*所示。

图 11-51: 发现任务列表

3. 在**发现任务执行记录**对话框中，选择任务记录，单击右侧的执行报告按钮，如图 *11-52: 发现任务执行记录*所示。

图 11-52: 发现任务执行记录

4. 在**发现任务执行报告**页面中，查看该发现任务的执行信息，如图 *11-53:* 发现任务执行报告所示。

图 11-53: 发现任务执行报告

5. 在**发现任务执行记录**对话框中，选择任务记录，单击右侧的下载执行日志按钮，如图 *11-54: 下载执行日志*所示，可将该发现任务的执行日志下载到本地。

图 11-54: 下载执行日志

11.3.2.1.2.5 编辑文件发现任务

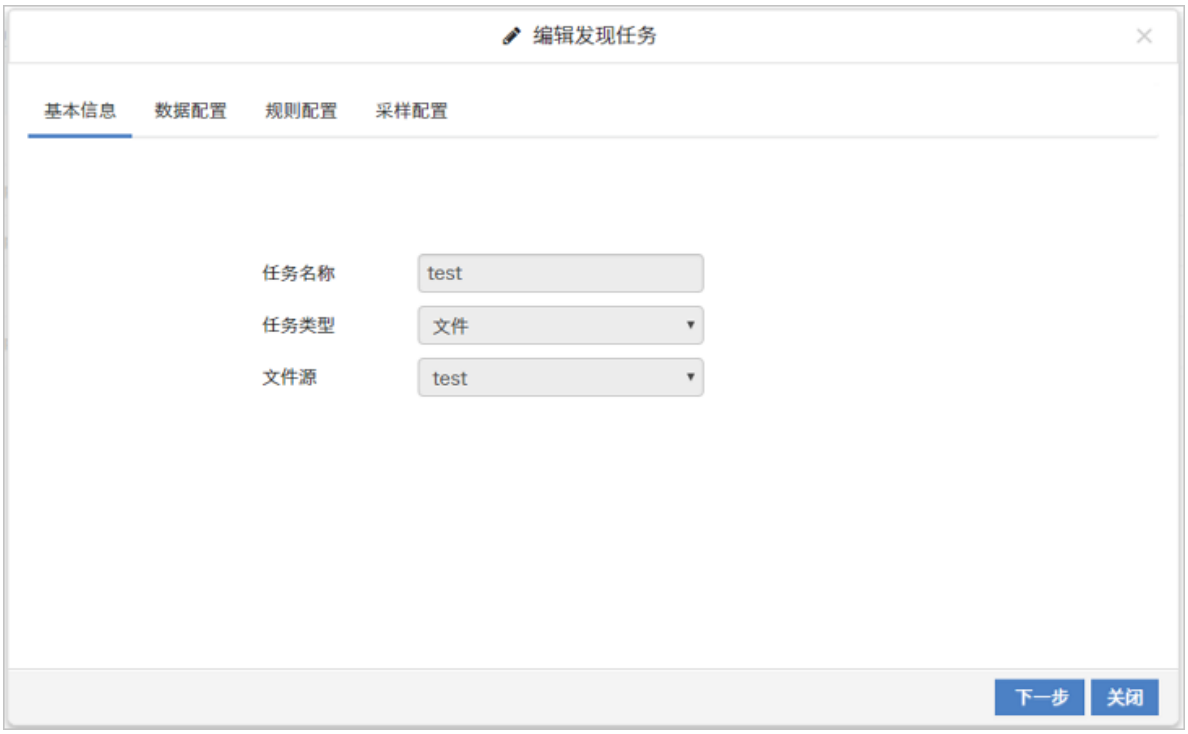
操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现任务**页面，选择已添加的文件发现任务，单击任务记录右侧的操作列表，单击**编辑任务**，如图 *11-55: 发现任务列表*所示。

图 11-55: 发现任务列表

3. 在**编辑发现任务**对话框中，可变更需要被发现的文件、发现规则、采样规则，修改完成后，单击**保存**，如图 *11-56: 编辑发现任务*所示。

图 11-56: 编辑发现任务



说明：

任务名称、任务类型、和文件源无法修改。

11.3.2.1.2.6 查看文件发现任务

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现任务**页面，选择已添加的文件发现任务，单击任务发现名称。
3. 在**发现任务详情**页面，查看该文件发现任务的详细信息，如图 *11-57: 发现任务详情页面*所示。

图 11-57: 发现任务详情页面

11.3.2.1.2.7 删除文件发现任务

前提条件

删除文件发现任务前，请确认该发现任务与专有云数据安全系统中其它数据已无关联。

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现任务**页面，选择已添加的文件发现任务，单击任务记录右侧的操作列表，单击**删除任务**，如图 *11-58: 删除发现任务*所示。

图 11-58: 删除发现任务

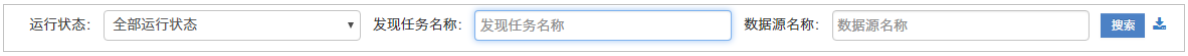
3. 在**信息提示**对话框中，单击**确定**，删除该文件发现任务。

11.3.2.1.3 查询发现任务

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现任务**页面，选择运行状态，输入发现任务名称，单击**搜索**，如图 *11-59: 查询发现任务*所示，查询包含所设定条件的发现任务。

图 11-59: 查询发现任务



11.3.2.2 敏感字段梳理

执行数据库发现任务后，专有云数据安全系统会将数据库表所有的字段和匹配的敏感数据发现规则等信息展示在**敏感字段梳理**页面。

11.3.2.2.1 添加敏感数据源

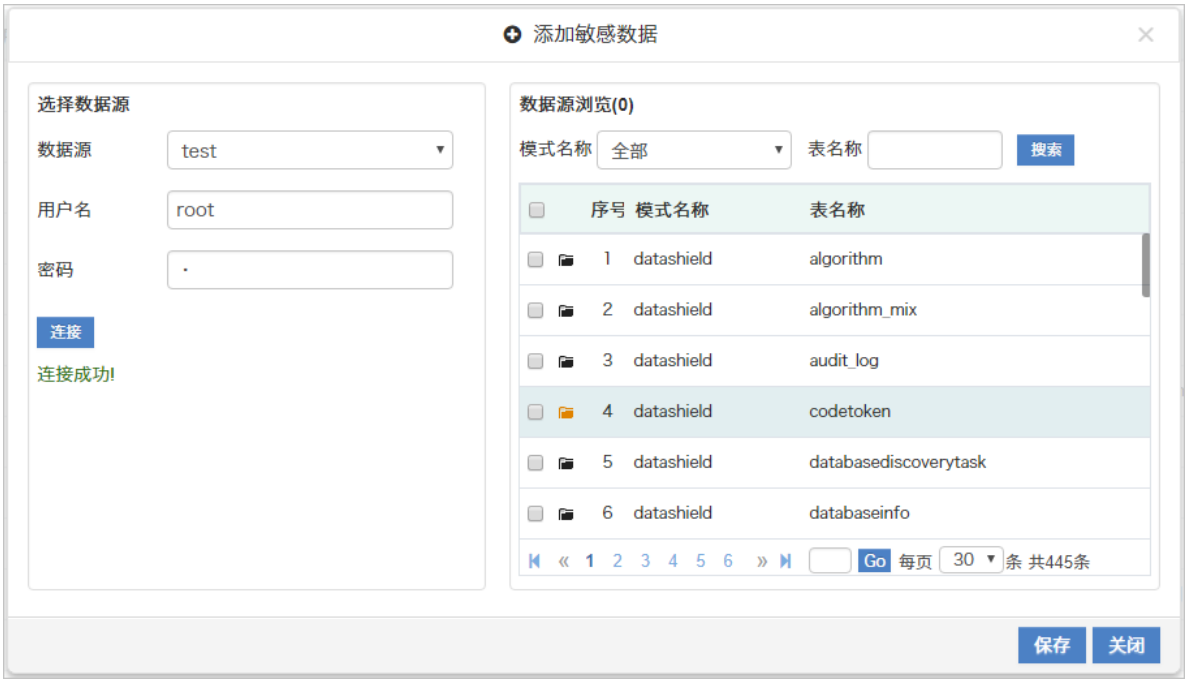
操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **敏感字段梳理**页面，在数据源列表区域，单击**添加**，如图 *11-60: 数据源列表*所示。

图 11-60: 数据源列表

3. 在**新增敏感数据**对话框中，选择数据源，输入用户名、密码，单击**连接**，如图 *11-61: 新增敏感数据*所示。

图 11-61: 新增敏感数据



说明：

连接成功后，数据源浏览区域会显示数据库表名称及模式名称。

4. 勾选需要被发现的数据库表，单击**保存**，新增的敏感字段将显示在敏感字段梳理页面的敏感数据列表中。

11.3.2.2.2 核实敏感数据

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **敏感字段梳理**页面，在敏感数据列表区域，核实已发现的敏感数据字段。
   - 选择敏感数据记录，单击右侧的核实此敏感数据按钮，如图 *11-62: 核实敏感数据记录*所示，核实该敏感数据。

图 11-62: 核实敏感数据记录

- 单击敏感数据列表区域上方的核实当前页按钮，如图 *11-63: 核实当前页敏感数据记录*所示，核实当前页面所有敏感数据记录。

图 11-63: 核实当前页敏感数据记录

11.3.2.2.3 设置为非敏感数据

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **敏感字段梳理**页面，在敏感数据列表区域，选择已发现的敏感数据记录，单击右侧的设置为非敏感数据按钮，如图 *11-64: 设置为非敏感数据*所示。

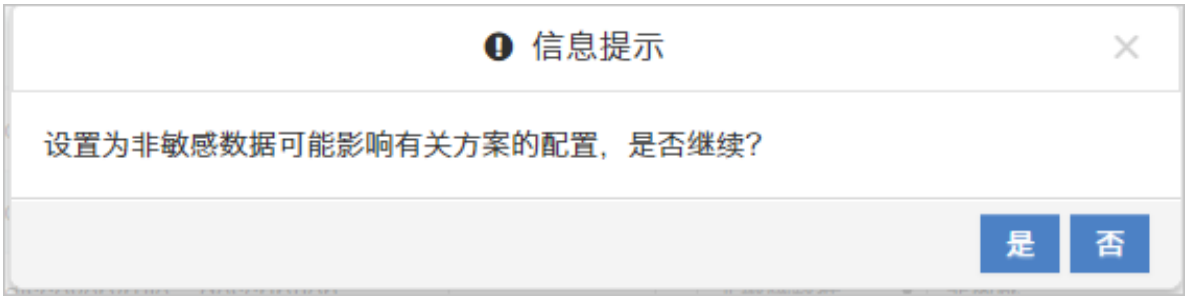
> **说明**：
> 在敏感级别栏中已标识为非敏感的数据记录无法设置为非敏感数据。

图 11-64: 设置为非敏感数据

序号	状态	模式	表	字段	字段备注	发现规则	敏感级别	样本	数据类型	约束类型	是否核实	操作
1		dbsec	jctm001	email地址		非敏感数	非敏感	gong_1043...	STRING	----	已核实	
2		dbsec	jctm001	money		金额数字	低	-121.33	DOUBLE(0,0)	----	未核实	
3		dbsec	jctm001	中文地址		中文地址	高	上海市海淀...	STRING	----	未核实	

3. 在**信息提示**对话框中，单击**是**，如图 *11-65: 设置非敏感数据信息提示*所示。

图 11-65: 设置非敏感数据信息提示



说明：

设置为非敏感数据的数据记录的敏感级别将变成非敏感，其发现规则也将变更为非敏感数据。

11.3.2.2.4 修正敏感数据

背景信息

数据库发现任务可以多次执行，当第一次发现任务的结果被人为修改或者被发现的数据库表发生变化时，第二次发现任务的结果可能和第一次的不同。这种情况下，需要安全管理人员修正敏感数据。

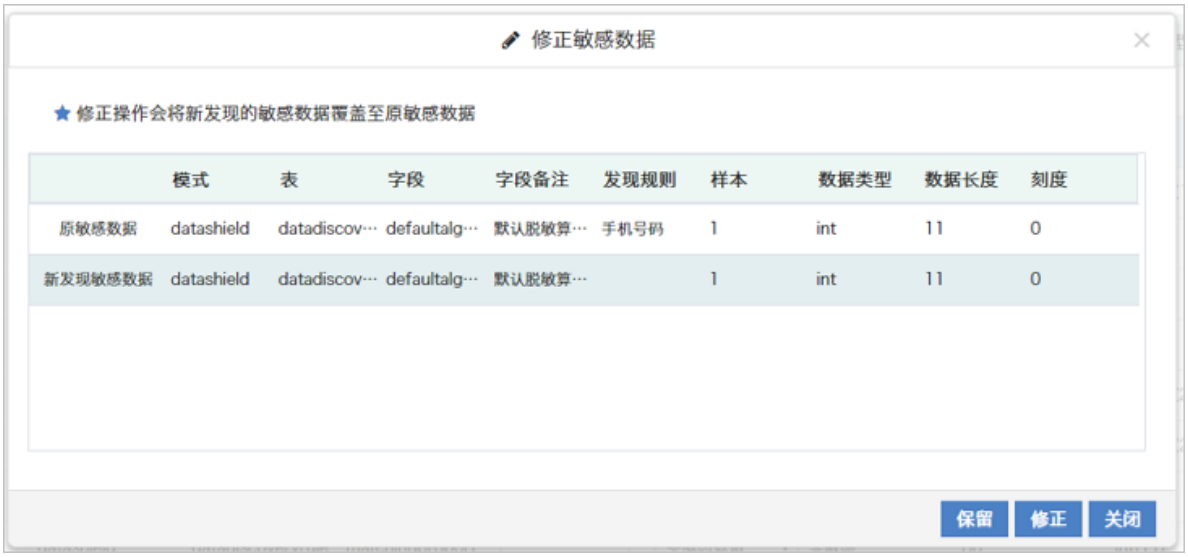
操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **敏感字段梳理**页面，在敏感数据列表区域，选择状态为**新增**、**已变更**或**已删除**的敏感数据记录，单击右侧的修正此敏感数据按钮，如图 *11-66: 敏感数据列表*所示。

图 11-66: 敏感数据列表

3. 在**修正敏感数据**对话框中，修正该敏感数据记录，如图 *11-67: 修正敏感数据*所示。
   - 单击**修正**，新发现的敏感数据将会覆盖原敏感数据记录。
   - 单击**保留**、或**关闭**，放弃本次修正操作。

图 11-67: 修正敏感数据



11.3.2.2.5 查询敏感数据

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **敏感字段梳理**页面，单击**展开更多条件**，如图 *11-68: 搜索敏感数据记录*所示。

- 输入模式、表名、字段名、字段备注等信息，单击**搜索**，查询包含所设定条件的敏感数据记录。
- 选择发现规则，单击**搜索**，查询相应发现规则的发现的敏感数据。
- 选择显示未核实字段、显示敏感数据字段、当前变更字段，单击**搜索**，显示相应敏感数据。

图 11-68: 搜索敏感数据记录

11.3.2.3 敏感文件梳理

执行文件发现任务后，专有云数据安全系统会将文件源中所有的字段和匹配的敏感数据发现规则等信息展示在**敏感文件梳理**页面。

11.3.2.3.1 核实敏感数据

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **敏感文件梳理**页面，在敏感文件列表区域，核实已发现的敏感数据字段。
   - 选择敏感数据记录，单击右侧的核实此敏感数据按钮，如*图 11-69: 核实敏感数据记录*所示，核实该敏感数据。

     图 11-69: 核实敏感数据记录

   - 单击敏感文件列表区域上方的核实当前页按钮，如*图 11-70: 核实当前页敏感数据记录*所示，核实当前页面所有敏感数据记录。

图 11-70: 核实当前页敏感数据记录

11.3.2.3.2 设置为非敏感数据

操作步骤

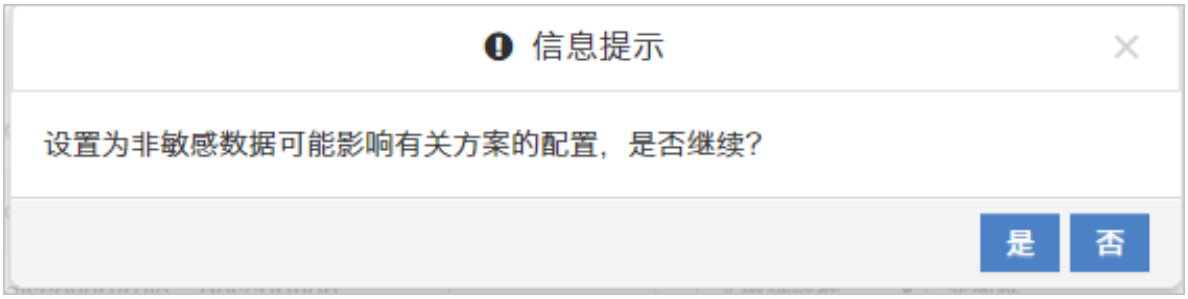
1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **敏感文件梳理**页面，在敏感文件列表区域，选择已发现的敏感数据记录，单击右侧的设置为非敏感数据按钮，如图 *11-71:* 设置为非敏感数据所示。

> **说明**：
> 在敏感级别栏中已标识为非敏感的数据记录无法设置为非敏感数据。

图 11-71: 设置为非敏感数据

3. 在**信息提示**对话框中，单击**是**，如图 *11-72:* 设置为非敏感数据信息提示所示。

图 11-72: 设置为非敏感数据信息提示



说明：

设置为非敏感数据的数据记录的敏感级别将变成非敏感，其发现规则也将变更为非敏感数据。

11.3.2.3.3 修正敏感数据

背景信息

文件发现任务可以多次执行，当第一次发现任务的结果被人为修改或者被发现的文件发生变化时，第二次发现任务的结果可能和第一次的不同。这种情况下，需要安全管理人员修正敏感数据。

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **敏感文件梳理**页面，在敏感文件列表区域，选择状态为**新增**、**已变更**或**已删除**的敏感数据记录，单击右侧的修正此敏感数据按钮，如图 *11-73: 敏感文件列表*所示。

图 11-73: 敏感文件列表

3. 在**修正敏感数据**对话框中，修正该敏感数据记录，如图 *11-74: 修正敏感数据*所示。
   - 单击**修正**，新发现的敏感数据将会覆盖原敏感数据记录。
   - 单击**保留**或**关闭**，放弃本次修正操作。

图 11-74: 修正敏感数据

11.3.2.3.4 查询敏感数据

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **敏感文件梳理**页面，单击**展开更多条件**，如图 *11-75:* 搜索敏感数据记录所示。
   - 输入文件名，单击**搜索**，查询包含所设定条件的敏感数据记录。
   - 选择发现规则，单击**搜索**，查询相应发现规则的发现的敏感数据。
   - 选择显示未核实字段、显示敏感数据字段、当前变更字段，单击**搜索**，显示相应敏感数据。

图 11-75: 搜索敏感数据记录

11.3.2.4 发现规则

专有云数据安全系统内置了15种发现规则，用于发现用户数据中的敏感数据。

11.3.2.4.1 查看发现规则

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现规则**页面，在发现规则列表区域选择发现规则记录，右侧的规则基本信息区域将展示该发现规则的规则信息，如图 *11-76: 查看发现规则*所示。

图 11-76: 查看发现规则

3. 在规则基本信息区域的**测试样本**框中，输入测试数据，单击**测试**可对发现规则进行测试。符合该发现规则的数据，提示通过；不符合的测试数据，则提示不通过。

11.3.2.4.2 添加自定义发现规则

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据发现** > **发现规则**页面，可以在发现规则列表区域单击**添加**，并在规则基本信息区域设置自定义规则的相关信息，单击**保存**，如图 *11-77: 添加发现规则*所示。

图 11-77: 添加发现规则

11.3.3 数据脱敏

专有云数据安全为了便于对数据库表的数据进行抽取，定义了“数据子集”的概念。通过定义数据子集，您可以对符合一定条件的数据进行脱敏。

11.3.3.1 数据子集

11.3.3.1.1 添加数据子集

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **数据子集**页面，单击左侧数据子集区域的**添加**，如图 *11-78:* 数据子集列表所示。

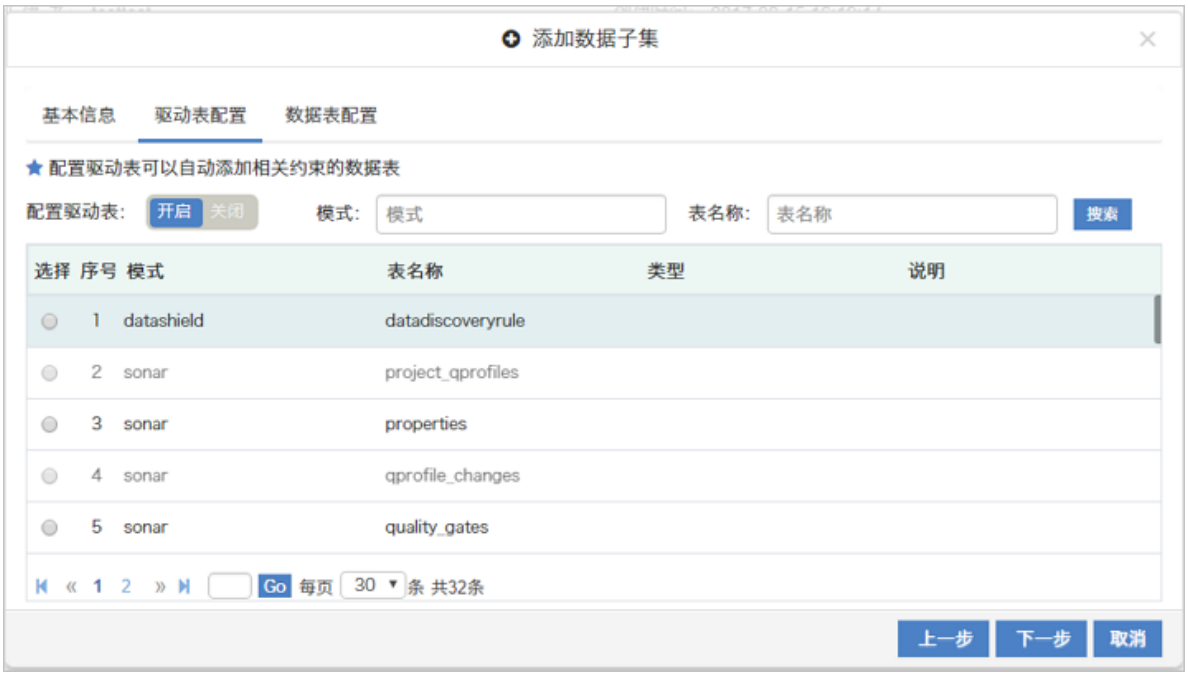
图 11-78: 数据子集列表

3. 在**添加数据子集**对话框的**基本信息**页签，输入子集名称、数据源、描述，单击**下一步**，如图 *11-79: 添加数据子集基本信息*所示。

图 11-79: 添加数据子集基本信息

4. 在**添加数据子集**对话框的**驱动表配置**页签，选择是否开启驱动配置表，单击**下一步**，如图 *11-80: 添加数据子集驱动表配置*所示。

图 11-80: 添加数据子集驱动表配置

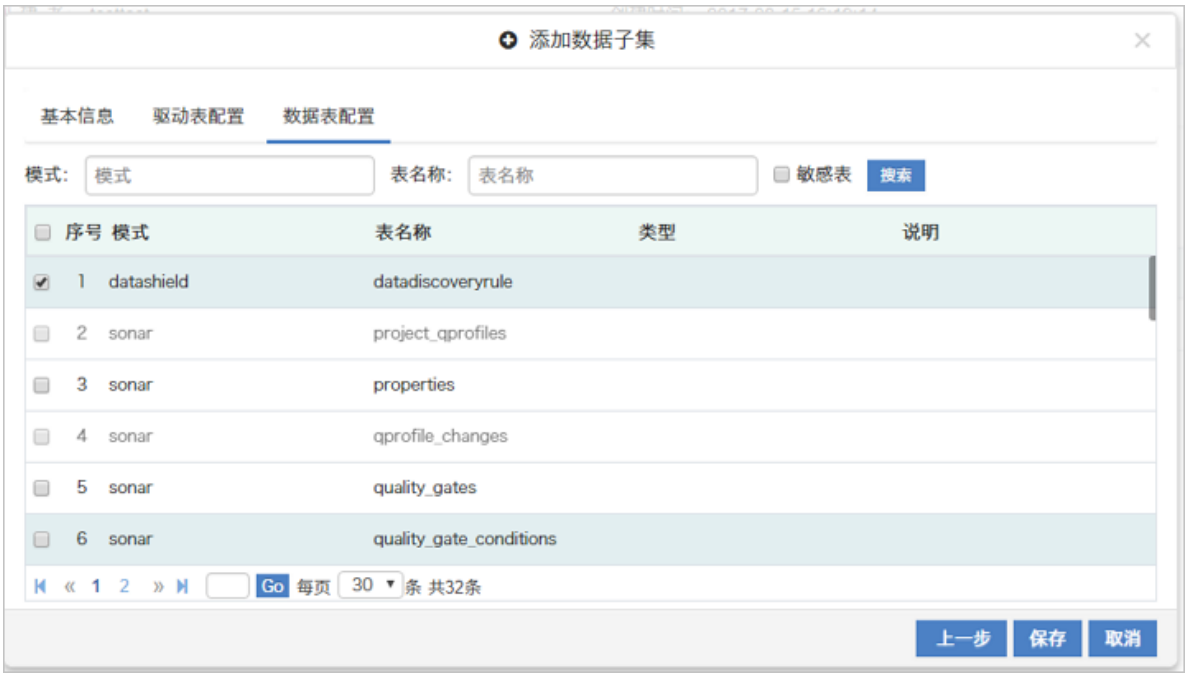


说明：

开启配置驱动表后，可以选择所需要的驱动表。

5. 在**添加数据子集**对话框的**数据表配置**页签，勾选该子集所需要的表，单击**保存**，如图 *11-81: 添加数据子集数据表配置*所示。

图 11-81: 添加数据子集数据表配置

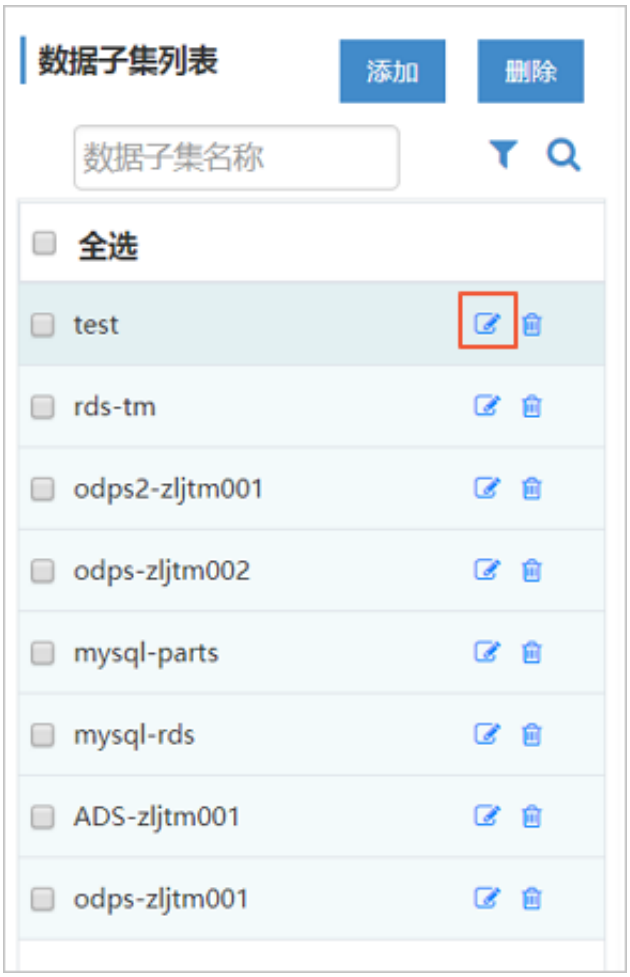


11.3.3.1.2 编辑数据子集

操作步骤

1. 定位到**数据脱敏** > **数据子集**页面，选择已添加的数据子集，单击右侧的编辑按钮，如图 *11-82: 数据子集列表*所示。

图 11-82: 数据子集列表



2. 在编辑数据子集信息对话框中，修改该数据子集的基本信息、驱动表、及数据表配置等信息，如图 *11-83:* 编辑数据子集信息所示。

图 11-83: 编辑数据子集信息

说明：

数据子集的数据源无法修改。

11.3.3.1.3 删除数据子集

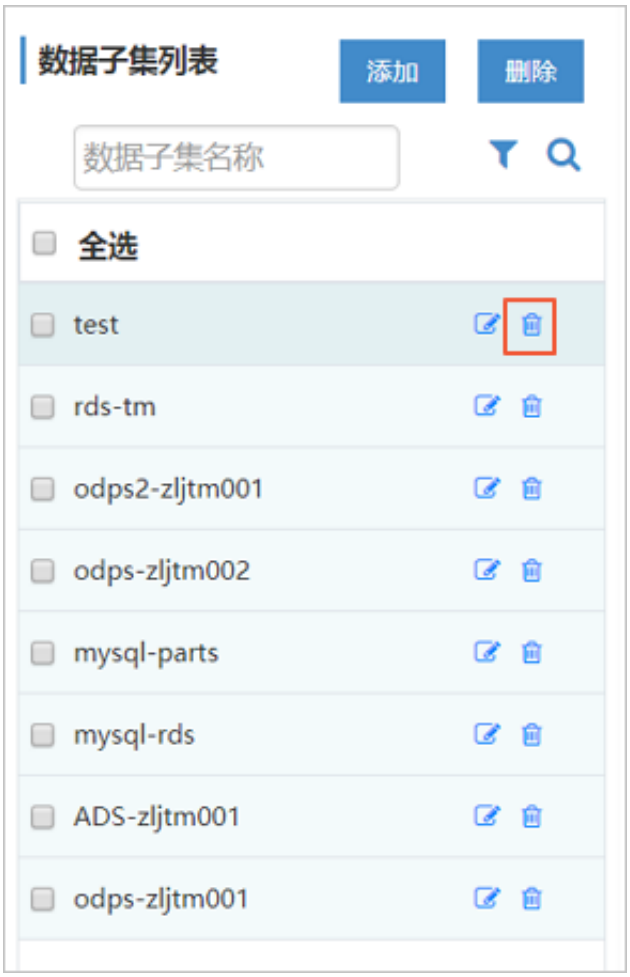
前提条件

删除数据子集前，请确认该数据子集与专有云数据安全系统中其它数据已无关联。

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **数据子集**页面，选择已添加的数据子集，单击右侧的删除按钮，如图 *11-84: 数据子集列表*所示。

图 11-84: 数据子集列表



3. 在**信息提示**对话框中，单击**确定**删除该数据子集。

11.3.3.2 数据关系

在执行数据发现任务时，如果启用了发现关系功能，发现任务执行完成后，具有主外键关联关系的表将会在**数据关系**页面中展示相关约束及关系拓扑图。

11.3.3.2.1 查看数据关系

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **数据关系**页面，单击数据表，查看该数据表的相关约束及关系拓扑图，如*图 11-85: 数据关系*所示。

图 11-85: 数据关系

11.3.3.3 脱敏方案

11.3.3.3.1 添加数据库脱敏方案

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏方案**页面，单击方案列表区域的**添加**，如图 *11-86: 方案列表*所示。

图 11-86: 方案列表

3. 在**添加方案**对话框的**基本信息**页签中，输入方案名称、方案描述，选择数据类型为数据库，选择数据源，单击**下一步**，如图 *11-87: 添加方案基本信息*所示。

图 11-87: 添加方案基本信息

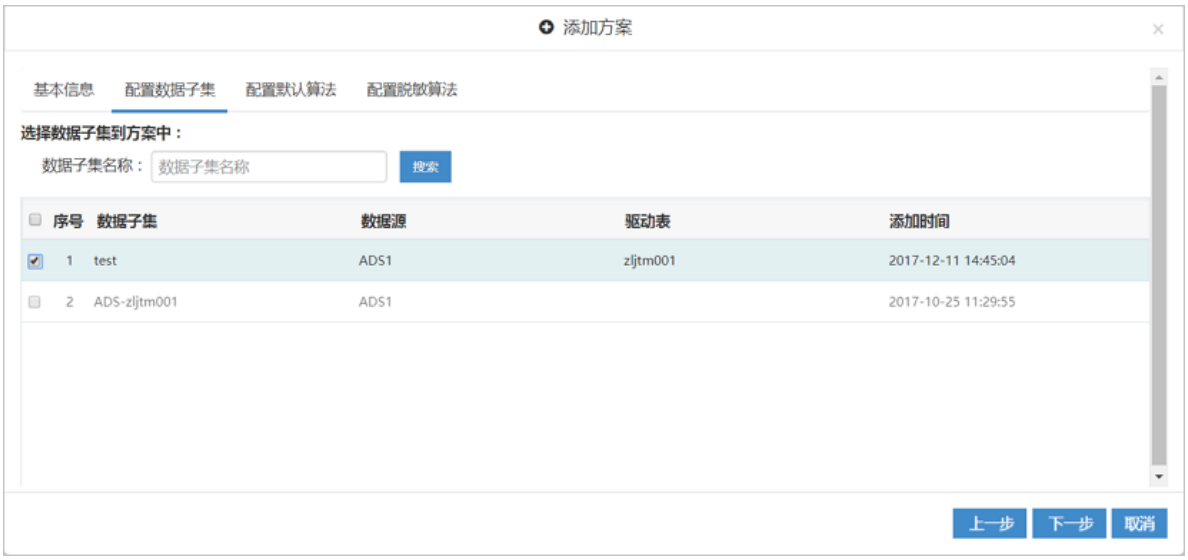
说明：

脱敏方案名称不可重复。

4. 在**添加方案**对话框的**配置数据子集**页签中，选择数据子集，单击**下一步**，如图 *11-88: 添加方案配置数据子集*所示。

> **说明**：
> 输入数据子集名称，单击**搜索**，可查询相应的数据子集。

图 11-88: 添加方案配置数据子集



5. 在**添加方案**对话框的**配置默认算法**页签中，对敏感数据类型进行统一算法配置，单击**下一步**，如图 *11-89: 添加方案配置默认算法*所示。

> **说明**：
> 您可以单击**推荐算法**，或手动选择脱敏算法并设置算法参数。

图 11-89: 添加方案配置默认算法

6. 在**添加方案**对话框的**配置脱敏算法**页签中，选择需要脱敏的数据表字段并配置脱敏算法，单击**保存**，如图 *11-90: 添加方案配置脱敏算法*所示，完成添加脱敏方案。

图 11-90: 添加方案配置脱敏算法

11.3.3.3.2 添加文件脱敏方案

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏方案**页面，单击方案列表区域的**添加**，如图 *11-91: 方案列表*所示。

图 11-91: 方案列表

3. 在**添加方案**对话框的**基本信息**页签中，输入方案名称、方案描述，选择数据类型为文件源，选择数据源，单击**下一步**，如图 *11-92: 添加方案基本信息*所示。

图 11-92: 添加方案基本信息

说明：

脱敏方案名称不可重复。

4. 在**添加方案**对话框的**配置默认算法**页签中，对敏感数据类型进行统一算法配置，单击**下一步**，如图 *11-93: 添加方案配置默认算法*所示。

> **说明**：
> 您可以单击**推荐算法**，或手动选择脱敏算法并设置算法参数。

图 11-93: 添加方案配置默认算法

5. 在**添加方案**对话框的**配置脱敏算法**页签中，选择需要脱敏的文件数据列并配置脱敏算法，单击**保存**，如图 *11-94: 添加方案配置脱敏算法*所示，完成添加脱敏方案。

图 11-94: 添加方案配置脱敏算法

11.3.3.3.3 修改脱敏方案

背景信息

> **说明**：
> 脱敏方案的方案名称、数据源类型、及数据源无法修改。

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏方案**页面。
3. 在**方案列表**区域中选择脱敏方案，单击右侧的编辑此方案信息按钮，如图 *11-95: 方案列表*所示。

   图 11-95: 方案列表

4. 在**编辑方案**对话框中，修改默认算法和脱敏算法，单击**保存**，如图 *11-96: 编辑脱敏方案*所示。

图 11-96: 编辑脱敏方案

11.3.3.3.4 删除脱敏方案

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏方案**页面。
3. 在**方案列表**区域中选择脱敏方案，单击右侧的删除此方案信息按钮，如图 *11-97:* 删除脱敏方案所示。

图 11-97: 删除脱敏方案

4. 在**信息提示**中，单击**确定**。

11.3.3.4 脱敏任务

专有云数据安全系统可以按照所选的脱敏算法，对已核实的数据库和文件源中的敏感数据进行脱敏，并将脱敏结果存储到脱敏任务所指定的目的位置。

11.3.3.4.1 数据库脱敏任务

11.3.3.4.1.1 添加数据库脱敏任务

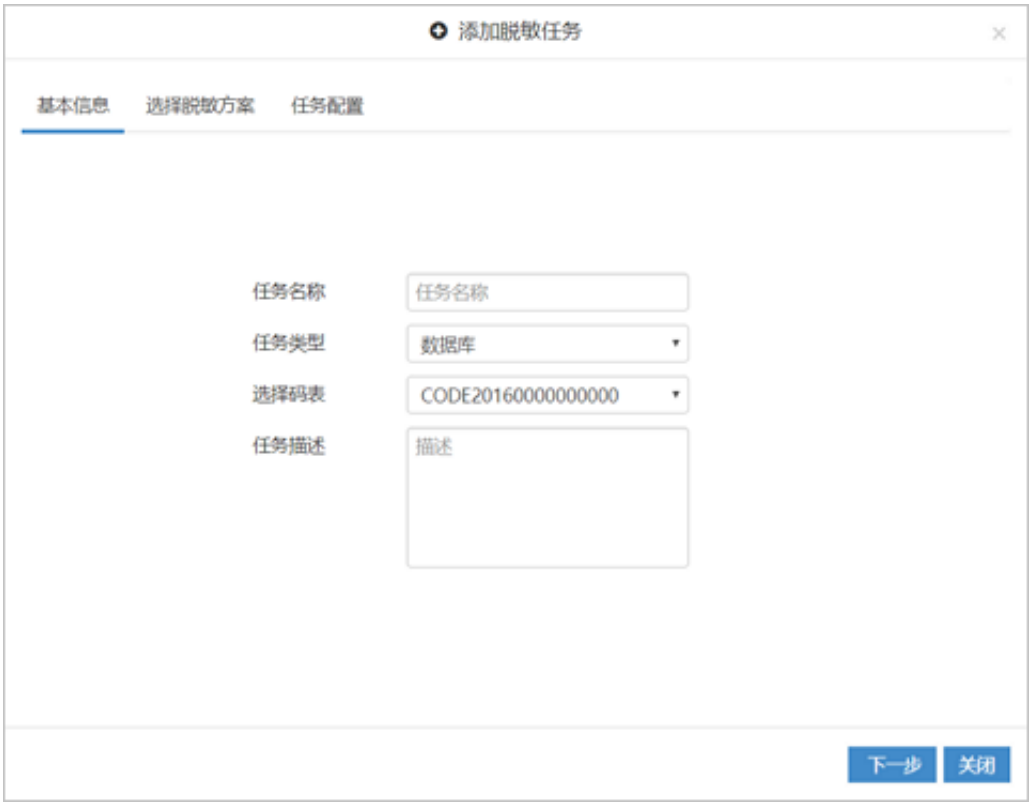
操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏任务**页面，单击右上角的**添加**，如图 *11-98:* 脱敏任务列表所示。

图 11-98: 脱敏任务列表

3. 在**添加脱敏任务**对话框的**基本信息**页签，输入任务名称、任务描述，选择任务类型为数据库，选择码表，单击**下一步**，如图 *11-99: 添加脱敏任务基本信息*所示。

图 11-99: 添加脱敏任务基本信息

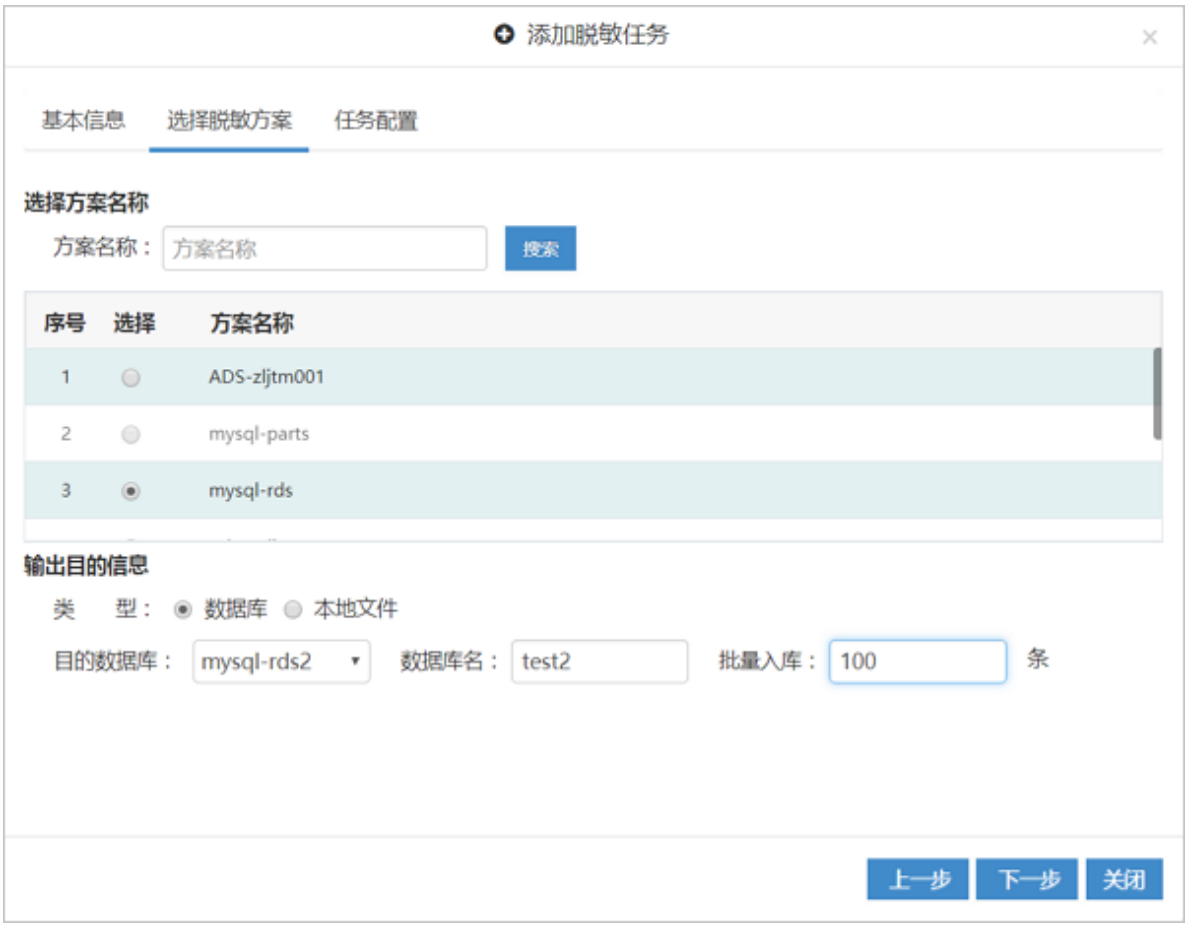


4. 在**添加脱敏任务**对话框的**选择脱敏方案**页签，勾选脱敏方案，在输出目的信息区域选择数据库类型，并选择目的数据库，填写数据库名及批量入库条数，单击**下一步**，如图 *11-100: 选择脱敏方案*所示。

说明：

输出目的数据库的schema不能与数据库源的schema相同。

图 11-100: 选择脱敏方案



5. 在**添加脱敏任务**对话框的**任务配置**页签，选择对象处理方式和异常处理方式，如图 *11-101: 脱敏任务配置*所示，单击**保存**，完成该脱敏任务的添加。

图 11-101: 脱敏任务配置

11.3.3.4.1.2 执行数据库脱敏任务

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏任务**页面，在**脱敏任务列表**中选择已添加的数据库脱敏任务，单击任务记录右侧的操作列表，单击**运行任务**，如图 *11-102: 脱敏任务列表*所示。

图 11-102: 脱敏任务列表

3. 在**运行脱敏任务**对话框中，输入数据源的用户名、密码，输入输出源的用户名、密码，单击**检测**。
4. 检测通过后，单击**运行**，执行该脱敏任务，如图 *11-103: 运行脱敏任务*所示。

图 11-103: 运行脱敏任务

等待该数据库脱敏任务执行完毕，如图 *11-104: 脱敏任务运行完成*所示。

图 11-104: 脱敏任务运行完成

11.3.3.4.1.3 停止数据库脱敏任务

背景信息

当数据库脱敏任务正在运行时，可以参考以下操作步骤，停止该脱敏任务：

操作步骤

1. 登录专有云数据安全控制台。

2. 定位到**数据脱敏** > **脱敏任务**页面，在**脱敏任务列表**中选择正在运行的数据库脱敏任务，单击任务记录右侧的操作列表，单击**停止任务**，如图 *11-105: 停止脱敏任务*所示。

图 11-105: 停止脱敏任务

3. 在**信息提示**对话框中，单击**确定**。

11.3.3.4.1.4 查看数据库脱敏任务的历史任务

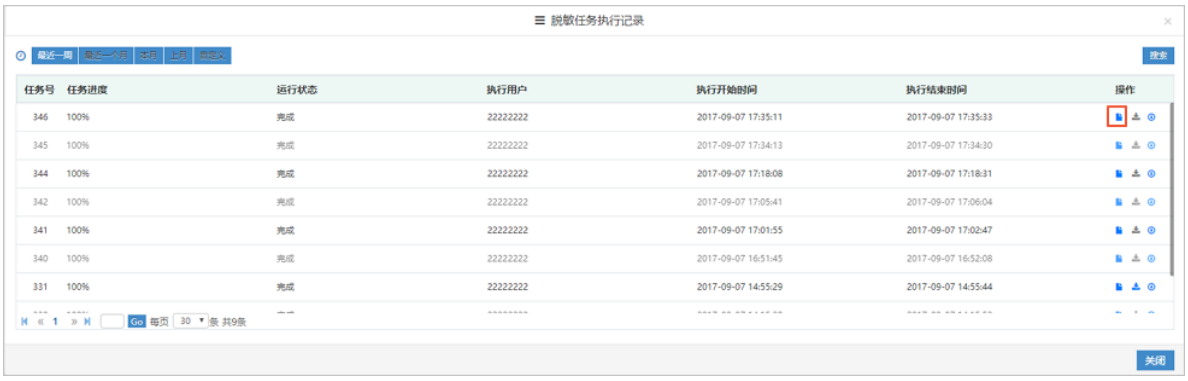
操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏任务**页面，在**脱敏任务列表**中选择已完成的数据库脱敏任务，单击任务记录右侧的操作列表，单击**历史任务**，如图 *11-106: 脱敏任务列表*所示。

图 11-106: 脱敏任务列表

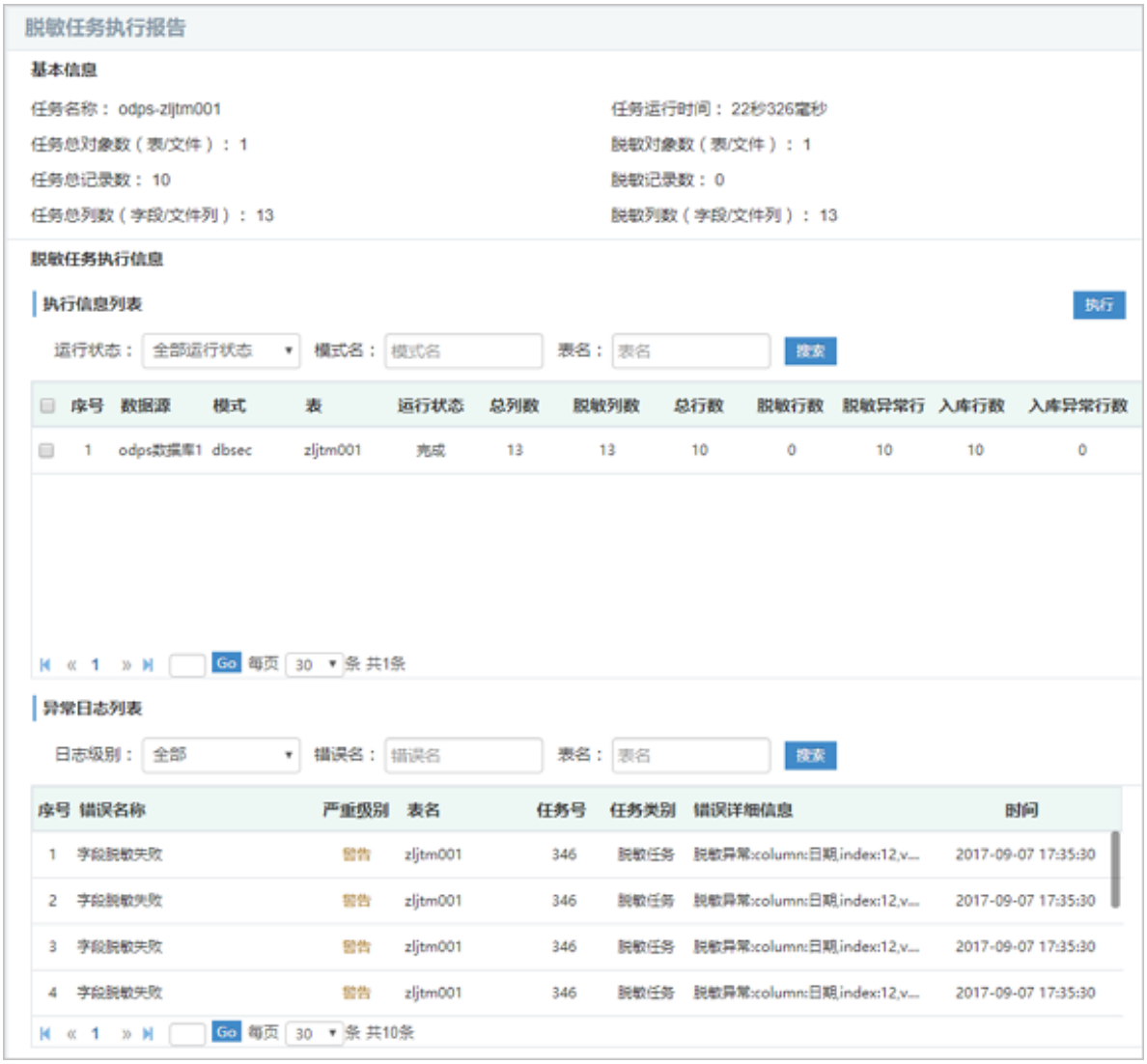
3. 在**脱敏任务执行记录**对话框中，选择已执行的任务记录，单击执行报告按钮，如图 *11-107: 脱敏任务执行记录*所示。

图 11-107: 脱敏任务执行记录



4. 在**脱敏任务执行报告**页面，查看该脱敏任务的执行报告，如图 *11-108:* 脱敏任务执行报告所示。

图 11-108: 脱敏任务执行报告



11.3.3.4.1.5 编辑数据库脱敏任务

操作步骤

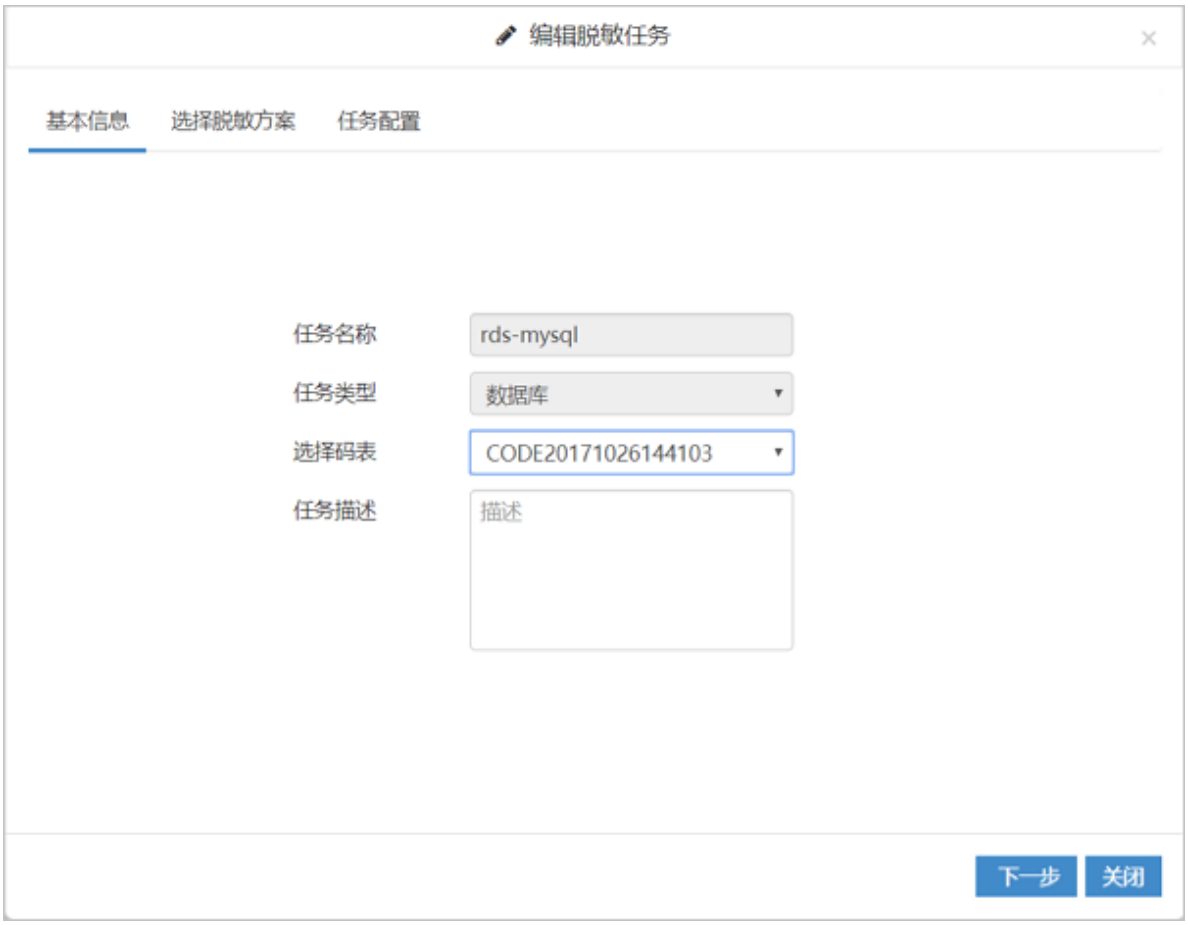
1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏任务**页面，在**脱敏任务列表**中选择数据库脱敏任务，单击任务记录右侧的操作列表，单击**编辑任务**，如图 *11-109: 脱敏任务列表*所示。

图 11-109: 脱敏任务列表

3. 在**编辑脱敏任务**对话框中，变更码表、任务描述、输出目的数据库信息、对象处理方式、异常处理方式，单击**保存**，如图 *11-110: 编辑脱敏任务*所示。

> **说明**：
> 任务名称、任务类型无法修改。

图 11-110: 编辑脱敏任务



11.3.3.4.1.6 删除数据库脱敏任务

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏任务**页面，在**脱敏任务列表**中选择数据库脱敏任务，单击任务记录右侧的操作列表，单击**删除任务**，如图 *11-111: 删除脱敏任务*所示。

图 11-111: 删除脱敏任务

3. 在**信息提示**对话框中，单击**确定**，删除该脱敏任务。

11.3.3.4.2 文件脱敏任务

11.3.3.4.2.1 添加文件脱敏任务

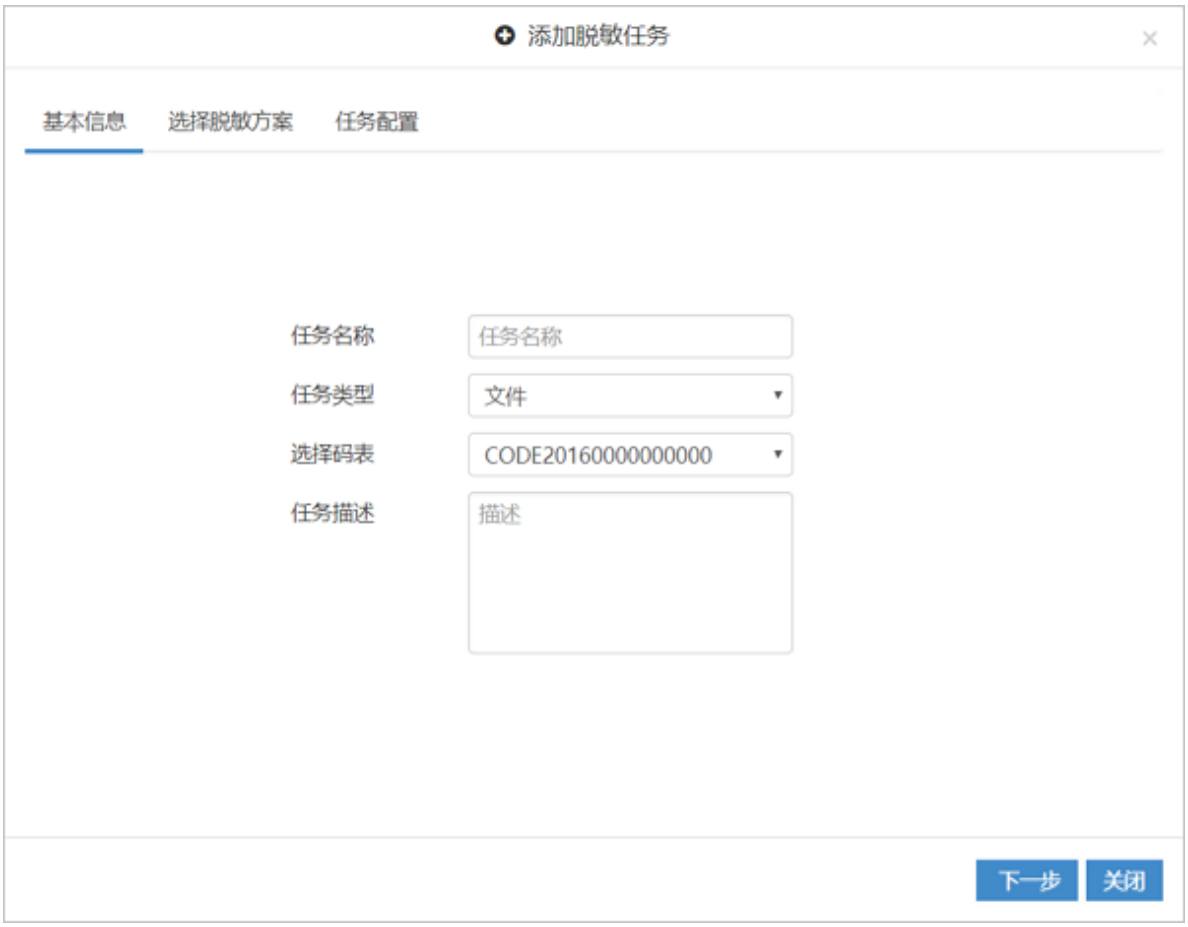
操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏任务**页面，单击右上角的**添加**，如图 *11-112:* 脱敏任务列表所示。

图 11-112: 脱敏任务列表

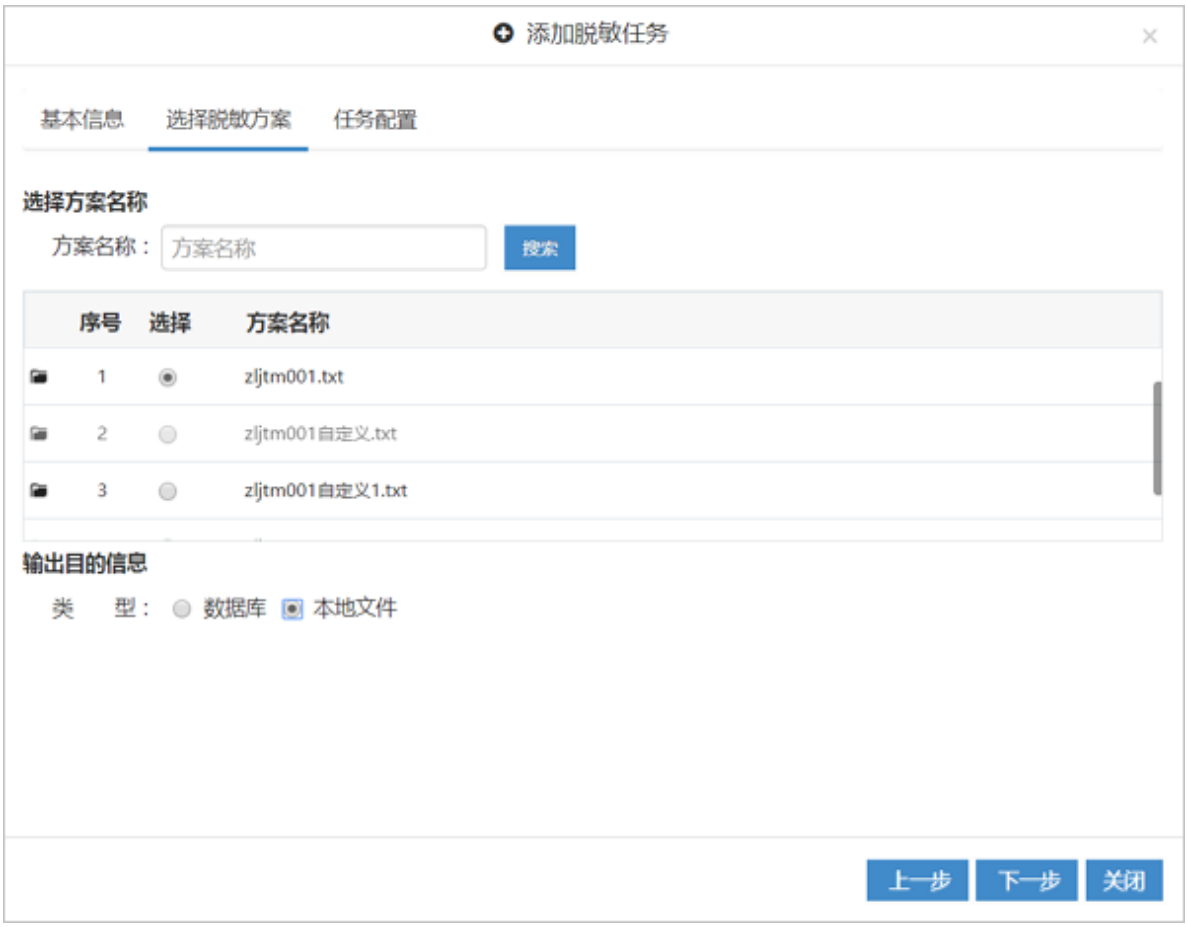
3. 在**添加脱敏任务**对话框的基本信息页签，输入任务名称、任务描述，选择任务类型为文件，选择码表，单击**下一步**，如图 *11-113:* 添加脱敏任务基本信息所示。

图 11-113: 添加脱敏任务基本信息



4. 在**添加脱敏任务**对话框的选择脱敏方案页签，勾选脱敏方案，在输出目的信息区域选择本地文件类型，单击**下一步**，如图 *11-114:* 选择脱敏方案所示。

图 11-114: 选择脱敏方案



5. 在**添加脱敏任务**对话框的**任务配置**页签，选择异常处理方式，如图 *11-115:* 添加脱敏任务任务配置所示，单击**保存**，完成该脱敏任务的添加。

图 11-115: 添加脱敏任务任务配置

11.3.3.4.2.2 执行文件脱敏任务

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏任务**页面，在**脱敏任务列表**中选择已添加的文件脱敏任务，单击任务记录右侧的操作列表，单击**运行任务**，如图 *11-116: 脱敏任务列表*所示。

图 11-116: 脱敏任务列表

3. 在**运行脱敏任务**对话框中，单击**检测**。
4. 检测通过后，单击**运行**，如图 *11-117: 运行脱敏任务*所示，执行该脱敏任务。

图 11-117: 运行脱敏任务

11.3.3.4.2.3 停止文件脱敏任务

背景信息

当文件脱敏任务正在运行时，可以参考以下操作步骤，停止该脱敏任务：

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏任务**页面，在**脱敏任务列表**中选择正在运行的文件脱敏任务，单击任务记录右侧的操作列表，单击**停止任务**，如图 *11-118: 停止脱敏任务*所示。

图 11-118: 停止脱敏任务

3. 在**信息提示**对话框中，单击**确定**。

11.3.3.4.2.4 查看文件脱敏任务的历史任务

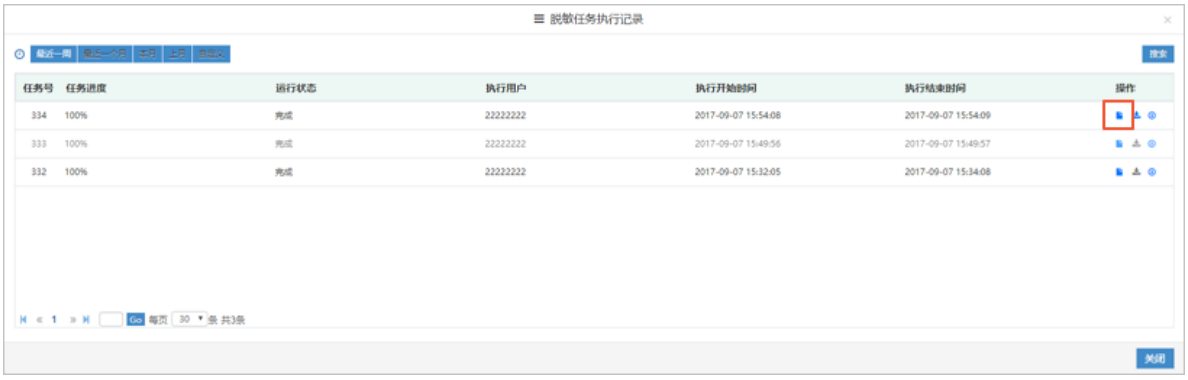
操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏任务**页面，在**脱敏任务列表**中选择已完成的文件脱敏任务，单击任务记录右侧的操作列表，单击**历史任务**，如图 *11-119:* 脱敏任务列表所示。

图 11-119: 脱敏任务列表

3. 在**脱敏任务执行记录**对话框中，选择已执行的任务记录，单击执行报告按钮，如图 *11-120:* 脱敏任务执行记录所示。

图 11-120: 脱敏任务执行记录



4. 在**脱敏任务执行报告**页面，查看该脱敏任务的执行报告，如图 *11-121:* 脱敏任务执行报告所示。

图 11-121: 脱敏任务执行报告

5. 在**脱敏任务执行记录**对话框中，选择已执行的任务记录，单击FTP下载按钮，如图 *11-122: 下载脱敏后的文件*所示，可下载脱敏后的文件。

图 11-122: 下载脱敏后的文件

11.3.3.4.2.5 编辑文件脱敏任务

操作步骤

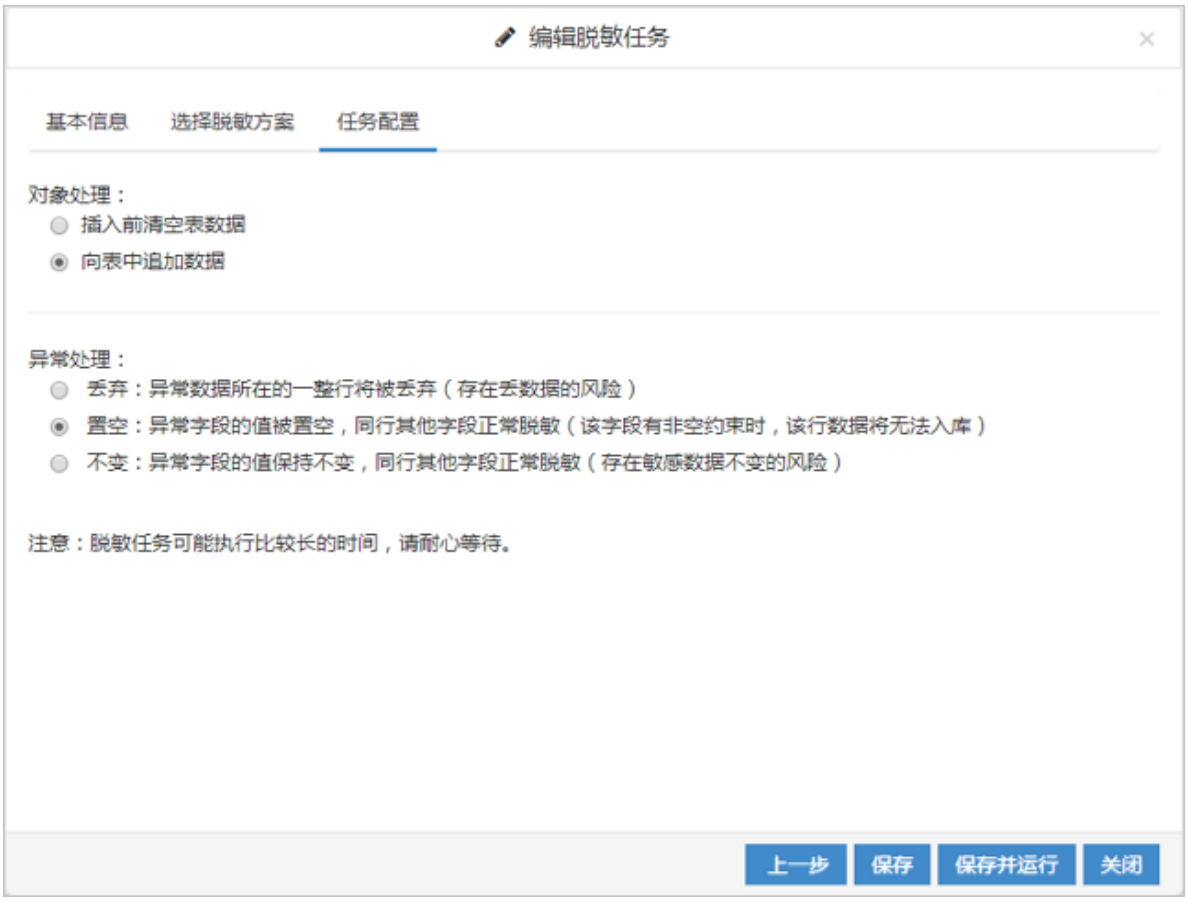
1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏任务**页面，在**脱敏任务列表**中选择文件脱敏任务，单击任务记录右侧的操作列表，单击**编辑任务**，如图 *11-123:* 脱敏任务列表所示。

图 11-123: 脱敏任务列表

3. 在**编辑脱敏任务**对话框中，变更码表、任务描述、输出目的、对象处理方式、异常处理方式，单击**保存**，如图 *11-124:* 编辑脱敏任务所示。

> **说明**：
> 任务名称、任务类型无法修改。

图 11-124: 编辑脱敏任务



11.3.3.4.2.6 删除文件脱敏任务

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏任务**页面，在**脱敏任务列表**中选择文件脱敏任务，单击任务记录右侧的操作列表，单击**删除任务**，如图 *11-125: 删除脱敏任务*所示。

图 11-125: 删除脱敏任务

3. 在**信息提示**对话框中，单击**确定**，删除该脱敏任务。

11.3.3.4.3 查询脱敏任务

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏任务**页面，选择运行状态、输入脱敏任务名称，单击**搜索**，如图 *11-126: 搜索脱敏任务*所示，查询符合相应条件的所有脱敏任务。

图 11-126: 搜索脱敏任务

11.3.3.5 脱敏算法

专有云数据安全内置了53种脱敏算法，用于对已核实的数据库和文件源中的敏感数据进行脱敏。

11.3.3.5.1 查看脱敏算法

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏算法**页面，在脱敏算法列表区域选择脱敏算法记录，右侧的脱敏算法信息区域将展示该脱敏算法的详细信息，如图 *11-127: 查看脱敏算法*所示。

图 11-127: 查看脱敏算法

3. 在脱敏算法测试区域，选择码表文件，输入测试数据，单击**脱敏测试**，在输出脱敏数据框中可显示测试样本脱敏后的数据。

11.3.3.5.2 添加自定义脱敏算法

操作步骤

1. 登录专有云数据安全控制台。
2. 定位到**数据脱敏** > **脱敏算法**页面，在脱敏算法列表区域单击**添加**，如图 *11-128: 添加脱敏算法*所示。

图 11-128: 添加脱敏算法

3. 在脱敏算法信息、脱敏参数、脱敏算法测试区域设置自定义算法的相关信息，单击**保存**。

12 安全审计

安全审计是指由专业审计人员根据有关法律法规、财产所有者的委托和管理当局的授权，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并作出相应评价。在管理员需要对系统过往的操作做回溯时，可以进行安全审计。

安全审计是一项长期的安全管理活动，贯穿云服务使用的生命周期。云盾的安全审计能够收集系统安全相关的数据，分析系统运行情况中的薄弱环节，上报审计事件，并将审计事件分为高、中、低三种风险等级，安全管理员关注和分析审计事件，从而持续改进系统，保证云服务的安全可靠。

12.1 查看审计一览

审计一览页面提供原始日志趋势、审计事件趋势、审计风险分布、危险事件分布四种报表。报表以趋势图或饼图的方式直观地呈现给安全管理员，便于分析云服务面临的风险趋势。

背景信息

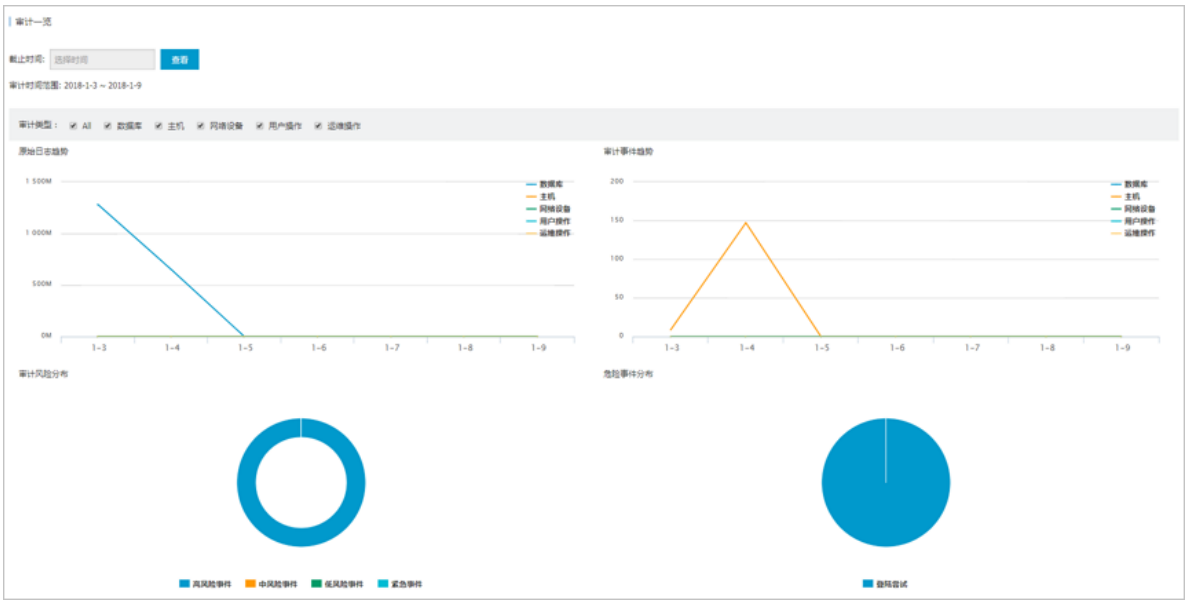
- **原始日志趋势**的数据是物理服务器、网络设备、RDS、ECS、OpenAPI一周内产生的日志个数。通过云平台日志趋势，安全管理员可以了解系统产生的日志数量是否正常。
- **审计事件趋势**的数据是物理服务器、网络设备、RDS、ECS、OpenAPI一周内产生的审计事件个数。通过审计事件趋势，安全管理员可以了解系统产生的审计事件数量是否正常。
- **审计风险分布**的数据是一周内高风险、中风险、低风险事件的个数。通过审计风险分布，安全管理员可以了解系统产生的审计事件级别是否正常。
- **危险事件分布**的数据是一周内不同事件类型占总事件的比例。通过危险事件分布，安全管理员可以了解什么类型的审计事件占比较多，识别高风险问题，做好预防措施。

同时，在**审计一览**页面，安全管理员还可以了解指定时间范围内所有审计类型的日志量信息及存储用量情况。

操作步骤

1. 登录云盾控制台。
2. 定位到**安全审计** > **审计一览**，进入**审计一览**页面，如图 *12-1:* 审计一览页面所示。

图 12-1: 审计一览页面



3. 选择**截止时间**，单击**查看**，即可查看截止至该时间一周内的审计一览信息。

> **说明**：
> 在**审计时间范围**可以查看当前显示的审计日志信息的具体时间范围。

4. 勾选**审计类型**，可以选择是否显示该类型的审计日志信息。

12.2 查询审计事件

审计查询页面可查看日志创建时间、审计类型、审计对象、操作类型、风险级别、日志内容等审计事件的详细信息。

背景信息

审计事件生成的过程：将安全审计模块收集到的日志匹配审计规则，如果日志内容能匹配任意一条审计规则的正则表达式，就会上报审计事件。关于审计策略规则，参见管理审计策略。

操作步骤

1. 登录云盾控制台。
2. 定位到**安全审计** > **审计查询**，进入**审计查询**页面。
3. 选择**审计类型**、**审计对象**、**操作类型**、**操作风险级别**等查询条件，设置查询时间，单击**查询**，查看该时间段内发现的审计事件。

> **说明：**
> 单击**高级查询**，可设置更详细的审计事件过滤条件。

4. 单击**导出**，可将本次查询到的审计事件信息进行导出，参见管理导出任务。

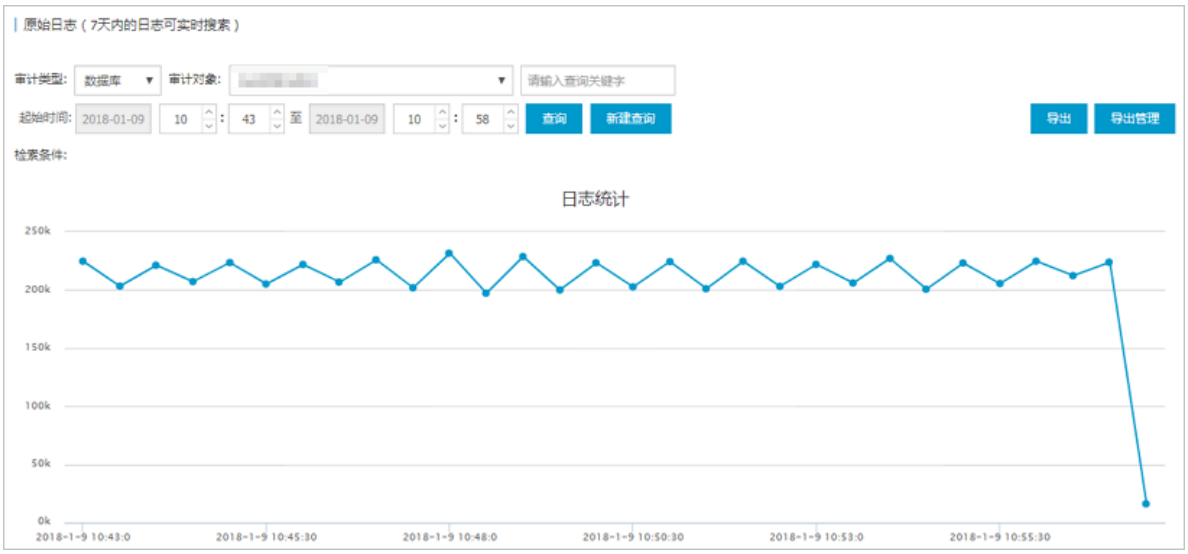
12.3 查看原始日志

在**原始日志**页面中，可查看审计对象在运行时产生的原始日志。原始日志作为必要的调试信息，安全管理员可以根据这些日志信息定位系统出现的故障。

操作步骤

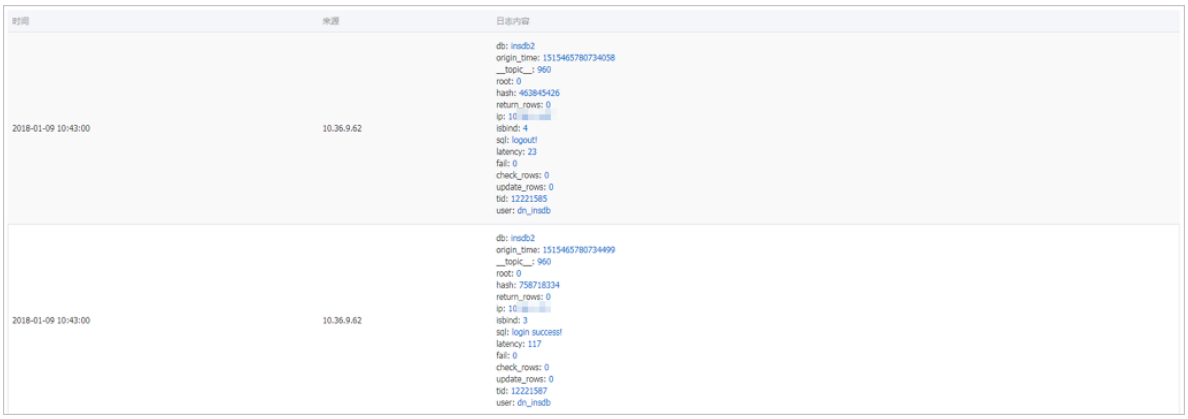
1. 登录云盾控制台。
2. 定位到**安全审计** > **原始日志**，进入**原始日志**页面，如图 *12-2:* 原始日志页面所示。

图 12-2: 原始日志页面



3. 选择**审计类型**、**审计对象**，设置查询时间，单击**查询**，查看该时间段内指定审计对象的原始日志信息，如图 *12-3:* 原始日志信息所示。

图 12-3: 原始日志信息



4. 单击**导出**，可将本次查询到的原始日志信息进行导出，参见管理导出任务。

12.4 策略设置

12.4.1 管理审计策略

审计策略是正则表达式规则，当日志记录中的某个字符串匹配审计规则的正则表达式，就会上报审计事件。

背景信息

正则表达式描述了一种字符串匹配的模式，可以用来检查一个串是否含有某种子串。例如：

正则表达式	说明
`^\d{5,12}$`	表示匹配第5到第12位的连续数字
`load_file\(`	表示匹配“load_file(”字符串

安全审计模块根据发生审计事件时日志中输出的字符串，定义了默认的审计策略。安全管理员也可以根据受到攻击时日志输出的字符串自定义审计策略。

操作步骤

1. 登录云盾控制台。
2. 定位到**安全审计** > **策略设置**，选择**审计策略**页签，如图 *12-4:* 审计策略页面所示。

图 12-4: 审计策略页面

3. 选择**审计类型**和**审计对象**，单击**查询**，查看当前已设置的审计策略。

> **说明**：
>
> 在**审计对象**中选择全局，即显示对该审计类型的所有审计对象均适用的审计策略。

4. 管理审计策略。

   - 单击**新增**，在**新增规则**对话框中输入相关信息并单击**添加**，可添加审计策略，如图 *12-5: 新增规则对话框*所示。

图 12-5: 新增规则对话框

说明：

添加审计策略后，在指定的审计类型、审计对象、风险级别的审计日志中，如果出现匹配正则表达式的内容，会发送一封告警邮件给已设置的报警接收人。例如，添加设置了正则表达式`hi|hello`，并设置了ECS日志类型、登录尝试事件、高风险事件的审计策略。那么在ECS日志中，如果出现**hi**或者**hello**，会上报一个尝试登录高风险的审计事件，并发送告警邮件给告警接收人。

- 单击**删除**，可删除该审计策略。

说明：

系统默认的审计策略无法删除。

- 单击**启用**或**禁用**，可设置该审计策略是否生效。

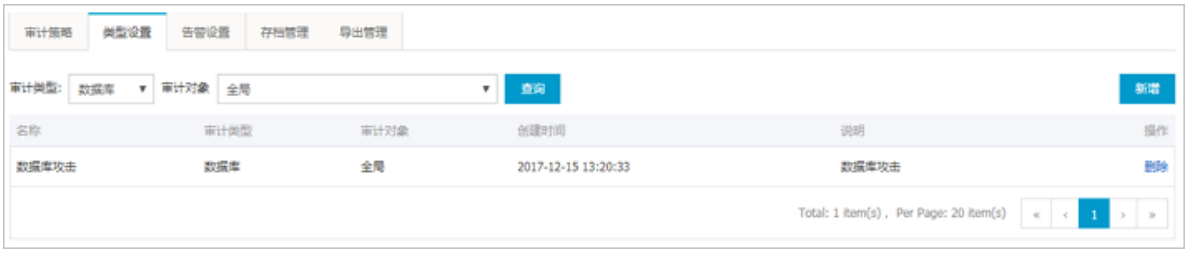
> **说明**：
> 新增的审计策略默认为启用状态。

12.4.2 管理操作类型

操作步骤

1. 登录云盾控制台。
2. 定位到**安全审计** > **策略设置**，选择**类型设置**页签，如图 *12-6:* 操作类型设置页面所示。

图 12-6: 操作类型设置页面



3. 选择**审计类型**、**审计对象**，单击**查询**，查看当前已设置的操作类型。

> **说明**：
> 在**审计对象**中选择**全局**，即显示对该审计类型的所有审计对象均适用的操作类型。

4. 管理操作类型。
   - 单击**新增**，在**新增事件类型**对话框中输入相关信息即可添加操作类型，如图 *12-7:* 新增事件类型所示。

图 12-7: 新增事件类型

- 单击**删除**，可删除该操作类型。

> **说明**：
> 系统默认的操作类型无法删除。

12.4.3 设置告警接收人

设置报警接收人的邮箱，在发生审计事件后，会将事件上报到所设置的告警人的邮箱。

操作步骤

1. 登录云盾控制台。
2. 定位到**安全审计** > **策略设置**，选择 **告警设置**页签，如图 *12-8:* 告警设置页面所示。

图 12-8: 告警设置页面

3. 选择**审计类型**、**审计对象**、风险等级，单击**查询**，查看当前已设置的告警接收人。

4. 设置告警接收人。

   - 单击**新增**，在**新增报警接收人**对话框输入相关信息即可添加告警接收人，如图 *12-9:* 新增报警接收人对话框所示。

     图 12-9: 新增报警接收人对话框

   - 单击**删除**，可删除该告警接收人。

12.4.4 管理事件日志存档

操作步骤

1. 登录云盾控制台。
2. 定位到**安全审计** > **策略设置**，选择**存档管理**页签，如图 *12-10:* 存档管理页面所示。

   图 12-10: 存档管理页面

3. 选择**审计类型**、**归档类型**，设置**发现时间**，单击**查询**，查看相应的归档信息。
4. 选择需要下载文件名，单击**下载**，可将该存档文件下载至本地。

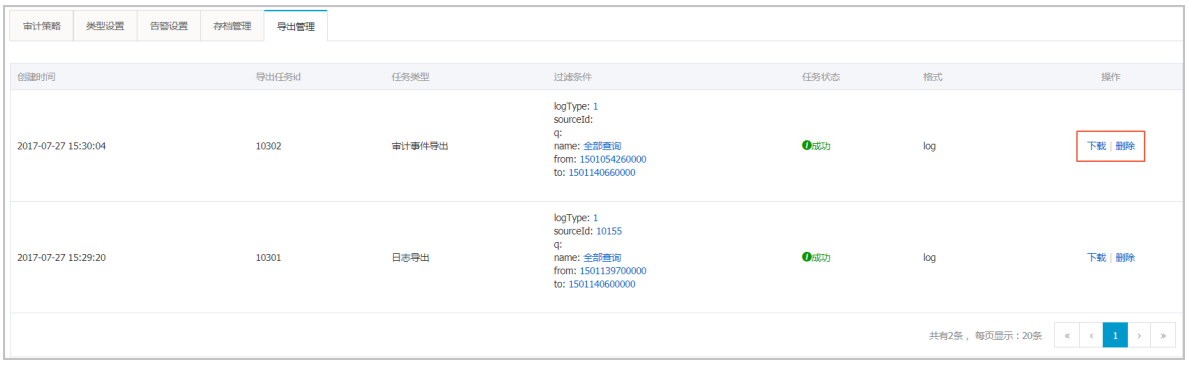
12.4.5 管理导出任务

在**审计查询**或**原始日志**页面，执行审计事件或日志导出后，可在导出管理页面对这些导出任务进行管理。

操作步骤

1. 登录云盾控制台。
2. 定位到**安全审计** > **策略设置**，选择**导出管理**页签。
3. 查看已创建的导出任务，如图 *12-11:* 导出管理页面所示。

图 12-11: 导出管理页面



4. 导出任务完成后，选择该导出任务，在操作栏单击**下载**，可将审计事件或日志文件下载到本地。
5. 单击**删除**，可删除该导出任务。

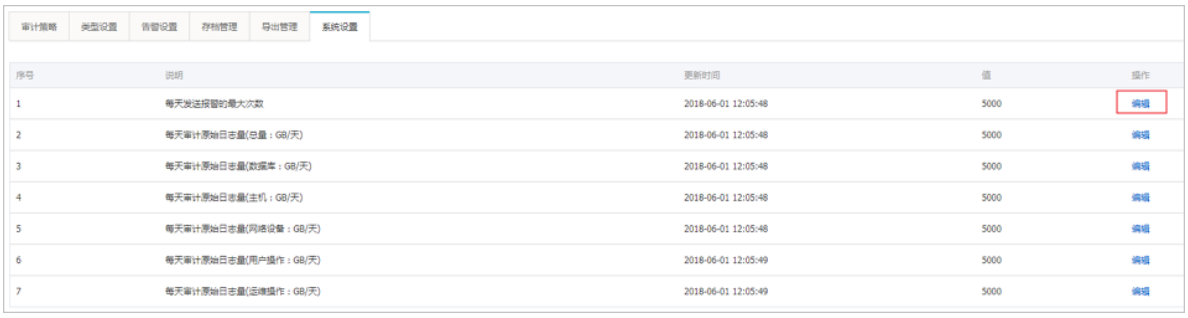
12.4.6 修改安全审计系统配置

通过设置安全审计的系统参数，可以配置系统单日最大报警次数及各类型原始日志的单日最大审计量。

操作步骤

1. 登录云盾控制台。
2. 定位到**安全审计** > **策略设置**，选择**系统设置**页签。
3. 定位到想要修改的系统参数，单击**编辑**如图 *12-12:* 系统设置所示。

图 12-12: 系统设置



4. 填写对应的参数值，单击**确认**。

13 数据库审计

数据库审计系统是一款专业、主动、实时监控数据库安全的审计产品。本系统采用有效的数据库审计方式，针对数据库漏洞攻击、SQL注入、风险操作等数据库风险行为进行记录与告警。同时，通过系统监控引擎可以定制不同的审计规则，例如信任、敏感和不审计语句等规则，从而有效地评估数据库潜在风险，实时监控数据库用户的访问操作行为。

数据库审计系统具有以下七大特点：

1. **B/S架构设计，使用简单**

   本系统采用B/S架构设计，操作使用简单，无需客户端，通过浏览器即可完成各项功能的使用。

2. **Agent式部署，Agent只转发流量，性能影响小**

   此种模式只需要在数据库端或应用端部署数据库审计系统的rmagent 插件。插件若部署在应用端则只能审计到应用访问数据库的操作；插件若部署在数据库端，进行相关配置后，能审计到通过网络或本地回环访问数据库的操作。插件rmagent本身没有复杂的处理逻辑，只根据受保护数据库设置情况转发数据流量，因而并不会对部署插件的服务器的负载产生过多影响。

3. **友好的人机交互，简单易用**

   本系统采用全新的人机交互操作模式，基于人性化、专业化和可用性三个层面设计产品界面。产品附加辅助型功能，采用页面向导和标注解析的方式帮助用户更加快速、熟练的掌握本产品，有效地完成数据库的监控与审计操作。

4. **规则制定简单快捷**

   为方便用户定制审计规则，本系统采用优先级由上而下的规则命中机制，从多个层面定义数据库审计规则。

5. **自动检测针对数据库漏洞的攻击**

   本系统具备针对数据库漏洞攻击行为进行检测的能力，应对多样的数据库漏洞。在没有漏洞补丁防护的前提下，数据库审计系统基于网络层级对数据库进行监控，避免数据库长期暴露在入侵风险的攻击下。

6. **细粒度审计数据库操作行为**

   本系统可实时监视数据库登录、访问行为，有效地实施审计策略。同时，本系统还提供强大的数据库活动审计分析能力，从多个角度灵活呈现数据库的活动状态，帮助用户有效地执行安全策略。

7. **审计结果查询分级处理，面面俱到**

本系统可进行单库（数据库）级和全库（数据库）级两个层的审计查询。采用多重页面钻取技术，逐层递进地引导客户完成审计日志的查询分析。在审计日志统计分析方面，本系统独创的综合性统计分析报表，基于日报、周报、月报等基础型业务报表（可定时推送），结合专项性的模式分析类报表，开启了数据库审计产品报表展现形式的新纪元。

13.1 快速部署指南

13.1.1 数据库审计系统部署

云盾数据库审计系统通过镜像方式部署在专有云Enterprise版平台上的ECS云服务器中。

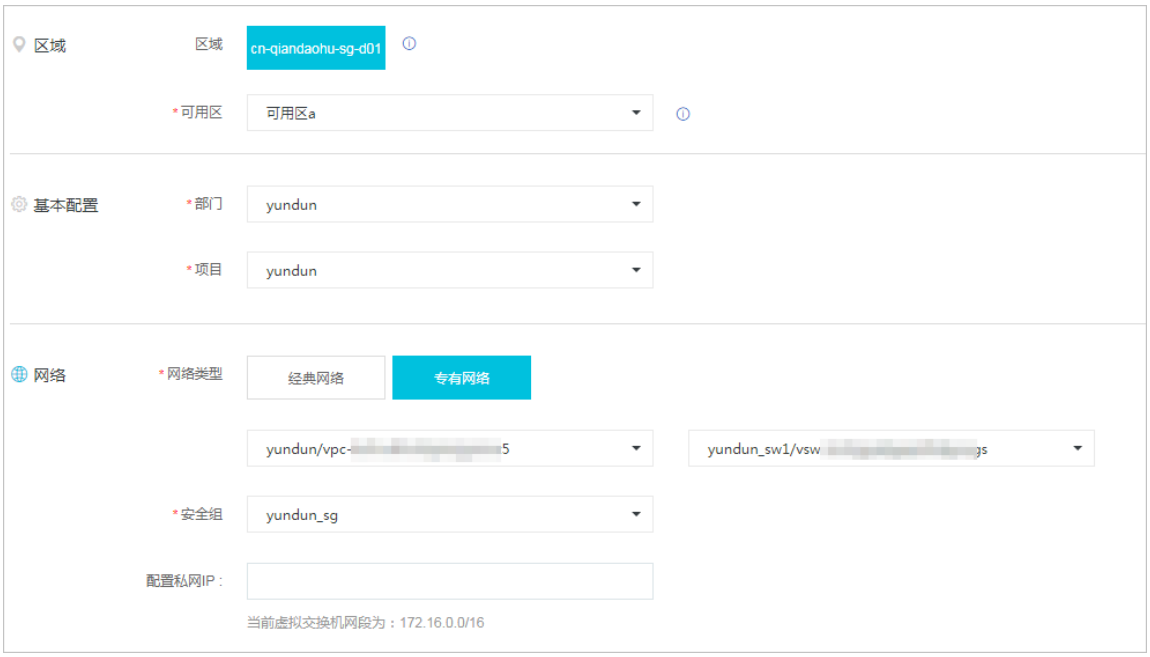
操作步骤

1. 登录Apsara Stack控制台。

> **说明**：
> 部署云盾数据库审计系统需要使用具有相关资源权限的用户进行操作。

2. 定位到**云管控中心** > **云基础产品** > **云服务器**，选择**实例**页签。
3. 单击**创建实例**，进入**创建云服务器ECS**页面，创建云盾数据库审计系统服务器。
   a) 设置区域、配置基本配置、网络等信息，如图 *13-1: 设置ECS实例配置属性*所示。

图 13-1: 设置ECS实例配置属性

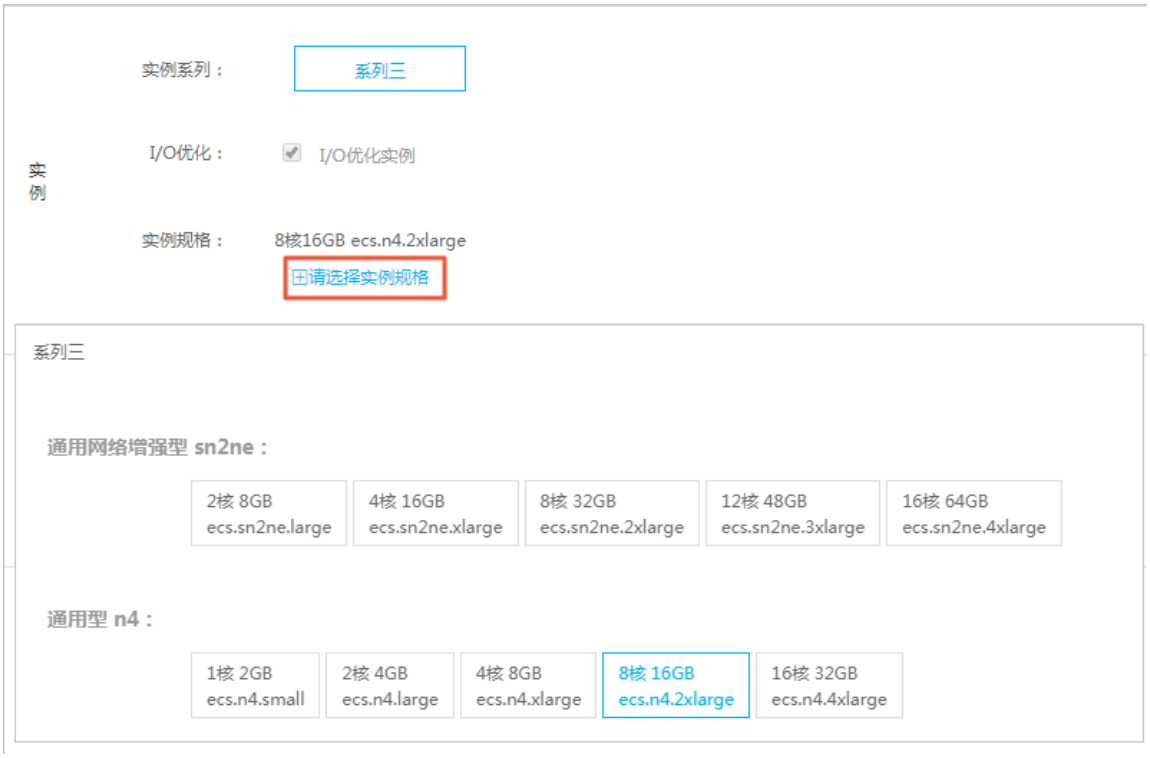


   b) 单击**选择实例规格**，选择8核16G类型的ECS实例规格，如图 *13-2: 选择ECS实例规格*所示。

说明：

云盾数据库审计系统服务器必须使用8核16G的实例规格。

图 13-2: 选择ECS实例规格



c) 选择**公共镜像**，选择**云盾数据库审计**镜像，并选择对应的版本，如图 *13-3: 选择数据库审计系统镜像*所示。

图 13-3: 选择数据库审计系统镜像

d) 添加一块大小为4096GB（4T）的数据盘，如图 *13-4: 添加数据盘*所示。

说明：

云盾数据库审计系统服务器必须添加一块大小为4T的数据盘。

图 13-4: 添加数据盘

e) 填写服务器密码、实例名称，单击**创建**，创建云盾数据库审计系统ECS实例，如图 *13-5: 设置服务器密码、实例名称*所示。

图 13-5: 设置服务器密码、实例名称

4. 联系销售人员，申请云盾数据库审计系统正式版的License许可。

   云盾数据库审计系统默认提供3个月的试用License。

13.1.2 登录云盾数据库审计系统

前提条件

- 请确认您所使用的客户端能够正常访问云盾数据库审计系统。
- 请确认您已经从云盾数据库审计系统部署人员处获得云盾数据库审计系统的访问地址。
- 请确认您已经从云盾数据库审计系统部署人员处获得用户名和密码。

用户	说明
sysadmin	系统管理员账号 默认密码：F2AD03E67CC3014F0A
secadmin	安全管理员账号
sysauditor	审计管理员账号

操作步骤

1. 打开Chrome浏览器。
2. 在地址栏中，输入https://云盾数据库审计系统的访问地址，按回车键（Enter），进入系统登录页面。
3. 在云盾数据库审计系统登录页面，输入用户名、密码及验证码。
4. 单击**登录**。

> **说明**：
> 首次登录成功后，用户必须修改密码。

13.1.3 数据库审计系统初始化

13.1.3.1 前提条件

数据库审计产品由Agent和Web控制台两部分组成，在使用数据库审计系统之前需要开放下列端口。

源	目的	端口	备注
运维管理端	Web控制台	443	Web控制台HTTPS服务通讯端口
Agent	Web控制台	9266	Agent与Web控制台之间的通讯端口
运维管理端	Web控制台	22	Web控制台SSH服务通讯端口

13.1.3.2 导入License文件

操作步骤

1. 使用系统管理员#*sysadmin*#账号登录云盾数据库审计系统。

2. 定位到**系统** > **证书管理**，如图 *13-6:* 证书管理页面所示。

图 13-6: 证书管理页面

3. 在**证书管理**页面，单击**浏览**，选择从销售人员处获取到的正式版License文件的存放路径，然后单击**上传**。

   校验通过后，您才可以正常使用云盾数据库审计系统。

13.1.3.3 添加被审计的数据库实例

云盾数据库审计系统支持对云服务器自建数据库实例和云服务商提供的云数据库实例进行审计。

操作步骤

1. 使用安全管理员*#secadmin#*登录云盾数据库审计系统。
2. 在**概况**页面，单击**添加数据库**，如图 *13-7:* 添加数据库所示。

图 13-7: 添加数据库

3. 在**添加数据库**页面中，填写被审计的数据库实例的相关信息，单击**保存**，如图 *13-8: 填写数据库实例相关信息*所示。

图 13-8: 填写数据库实例相关信息

表 13-1: 数据库实例信息说明

参数	说明
数据库名	为被审计的数据库实例指定一个名字。
数据库类型	根据被审计的数据库实例的类型选择。
数据库版本	可以手动选择或者由系统自动获取。输入数据库主机IP、数据库主机端口、数据库实例名、用户名、密码，单击**确认**，系统会

参数	说明
	自动获取数据库的版本（对于Oracle数据库同时会获取到字符集）。
IP地址	• **云服务器（ECS）自建数据库**：被审计数据库实例的IP地址。 • **云数据库（RDS）实例**：被审计的RDS数据库实例的URL连接串。
端口	被审计数据库实例的端口号。
实例名	仅Oracle与Postgres类型的数据库需要填写，其他类型的数据库可以不填写。
描述	为被审计的数据库实例添加注释。

数据库添加成功后，可以在**概况**页面下方的数据库列表处看到所添加的数据库的摘要信息，如图 *13-9: 数据库实例添加成功*所示。

图 13-9: 数据库实例添加成功

13.1.3.4 部署Agent程序

13.1.3.4.1 Agent程序部署位置

Agent程序需要部署到数据库或应用服务器上，用于获取访问数据库的流量，帮助审计系统对获取到的流量实现分析审计。

- **服务器自建数据库实例**：Agent程序需要部署在数据库所在的服务器上。
- **RDS数据库实例**：Agent程序需要部署在对应的应用服务器上。

13.1.3.4.2 自动部署Agent程序

自动部署Agent程序功能目前仅支持Linux系统的服务器。对于自建数据库实例，数据库所在的服务器必须使用Linux系统；对于RDS数据库实例，对应的应用服务器必须使用Linux系统。

操作步骤

1. 使用安全管理员#secadmin#登录云盾数据库审计系统。
2. 在**维护**页面，选择**Agent管理**，单击**Agent自动部署**。
3. 在**Agent自动部署**对话框中，填写部署参数，如图 *13-10: Agent自动部署*所示。

图 13-10: Agent自动部署

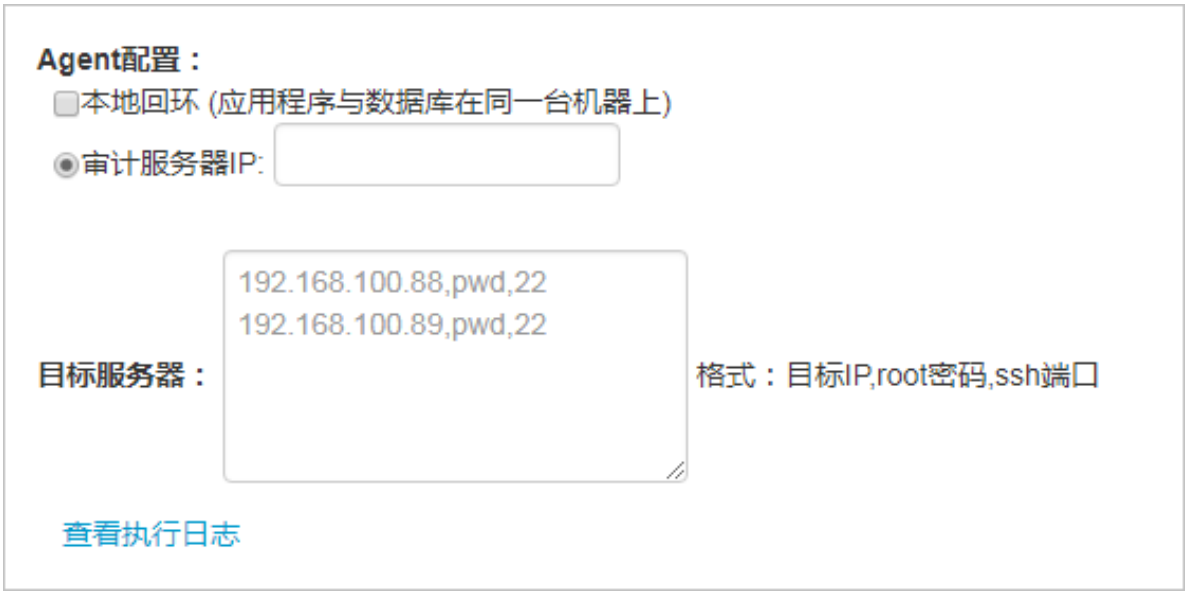


表 13-2: Agent自动部署设置

参数	说明
本地回环	如果应用服务与数据库部署在同一台服务器中，在自动部署Agent程序时，需要勾选**本地回环**。
审计服务器IP	审计服务器IP地址。
目标服务器	部署Agent服务器的信息，格式为：`目标IP,root密码,ssh端口`。 如果需要部署多个目标服务器，每个服务器的信息后面，按回车（Enter）换行。

4. 单击**部署**，即可将Agent程序自动部署到相应的服务器中。
5. Agent程序自动部署完成后，返回**Agent管理**页面，单击**Agent部署配置**。
6. 在**Agent部署配置**对话框中，输入已部署Agent程序的服务器IP地址，然后单击**添加**，如图*13-11: Agent部署配置*所示。

说明：

- 如果需要部署Agent程序的服务器与数据库审计系统处于同一个内网，则直接添加内网地址即可；如果与数据库审计系统不在同一个内网需要通过外网进行通信的，则需添加该服务器的外网地址。
- 如果不添加部署Agent程序的服务器IP地址，审计系统将无法抓取该服务器的数据进行审计。

图 13-11: Agent部署配置

13.1.3.4.3 手动部署Agent程序

13.1.3.4.3.1 Windows系统服务器部署Agent程序

13.1.3.4.3.1.1 应用服务与数据库部署在不同的服务器的情况

操作步骤

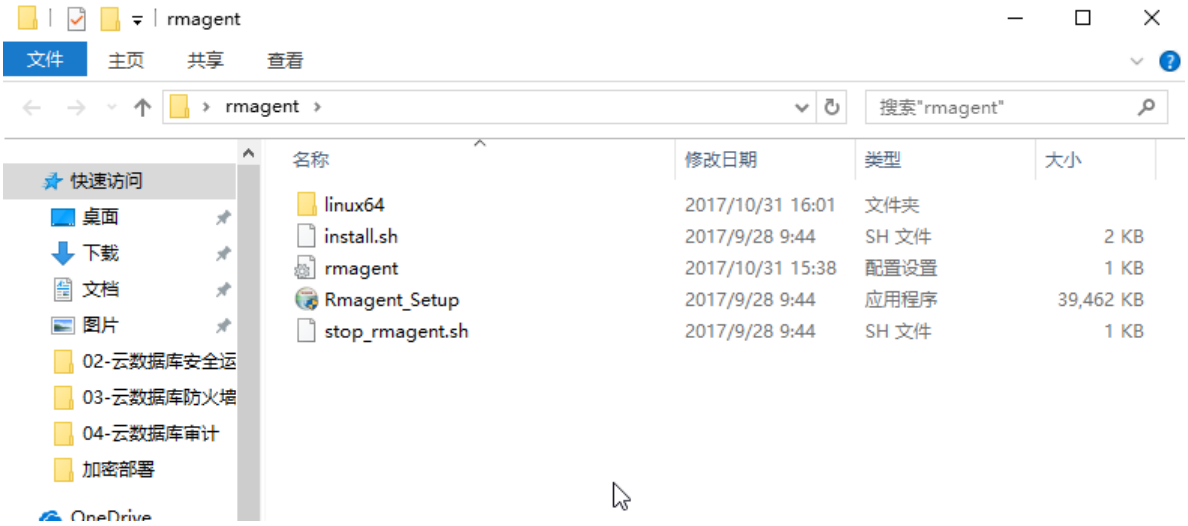
1. 使用安全管理员#secadmin#登录云盾数据库审计系统。
2. 在**维护**页面，选择**Agent管理**，单击**下载Agent**。

   系统自动弹出Agent部署配置提示，且浏览器自动开始将Agent程序（即rmagent.tar.gz文件）下载至本地。
3. 在**Agent部署配置**对话框中，输入需要部署Agent程序的服务器IP地址，然后单击**添加**。

   说明：

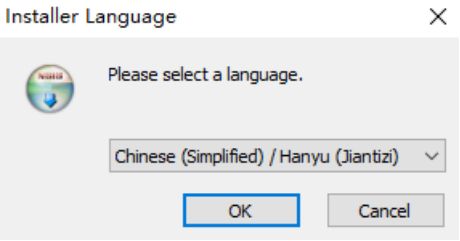
   - 如果需要部署Agent程序的服务器与数据库审计系统处于同一个内网，则直接添加内网地址即可；如果与数据库审计系统不在同一个内网需要通过外网进行通信的，则需添加该服务器的外网地址。
   - 如果不添加部署Agent程序的服务器IP地址，审计系统将无法抓取该服务器的数据进行审计。
4. 将Agent程序（即rmagent.tar.gz文件）文件上传到需要部署Agent程序的服务器，并将其解压缩，如图 *13-12: 解压Agent安装程序*所示。

   图 13-12: 解压Agent安装程序



5. 打开解压后的Agent程序文件夹，双击运行Rmagent_Setup.exe程序文件。
6. 在**Installer Language**对话框中，单击**OK**，如图 *13-13: 选择语言*所示。

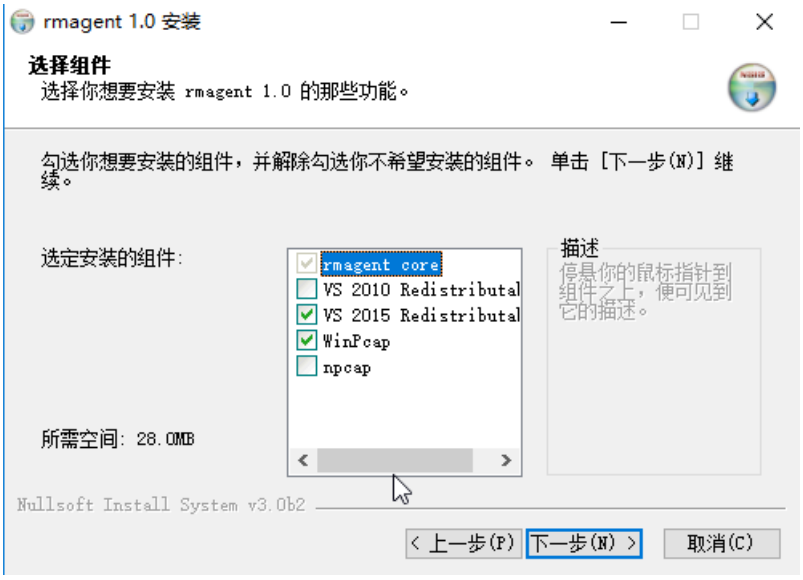
图 13-13: 选择语言



7. 在**rmagent1.0**安装对话框中，单击**下一步**，直到Agent程序开始安装。

> **说明**：
> 选择组件时，必须勾选VS 2015 Redistributable和WinPcap组件，如图 *13-14:* 选择组件所示，在Agent程序安装过程中会自动运行相关组件的安装程序。

图 13-14: 选择组件



8. 所有组件及Agent程序安装完成后，重新启动服务器。

13.1.3.4.3.1.2 应用服务与数据库部署在同一台服务器的情况

操作步骤

1. 使用安全管理员*#secadmin#*登录云盾数据库审计系统。
2. 在**维护**页面，选择**Agent管理**，单击**下载Agent**。

   系统自动弹出Agent部署配置提示，且浏览器自动开始将Agent程序（即rmagent.tar.gz文件）下载至本地。

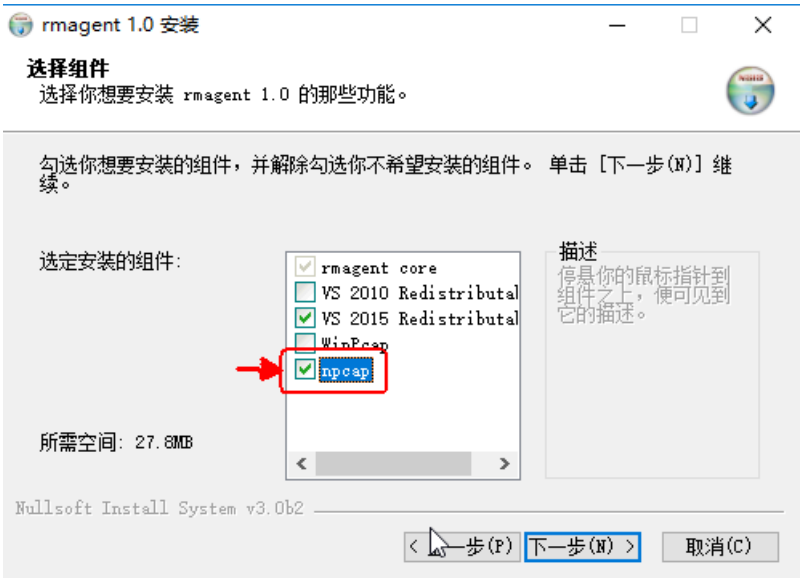
3. 在**Agent部署配置**对话框中，输入需要部署Agent程序的服务器IP地址，然后单击**添加**。

> **说明**：
>
> - 如果需要部署Agent程序的服务器与数据库审计系统处于同一个内网，则直接添加内网地址即可；如果与数据库审计系统不在同一个内网需要通过外网进行通信的，则需添加该服务器的外网地址。
> - 如果不添加部署Agent程序的服务器IP地址，审计系统将无法抓取该服务器的数据进行审计。

4. 将Agent程序（即rmagent.tar.gz文件）文件上传到需要部署Agent程序的服务器，并将其解压缩。
5. 打开解压后的Agent程序文件夹，双击运行Rmagent_Setup.exe程序文件。
6. 在**Installer Language**对话框中，单击**OK**。
7. 在**rmagent1.0**安装对话框中，单击**下一步**，直到Agent程序开始安装。

> **说明**：
>
> 选择组件时，必须勾选VS 2015 Redistributable和npcap组件，如图 *13-15: 选择组件*所示，在Agent程序安装过程中会自动运行相关组件的安装程序。

图 13-15: 选择组件



8. 所有组件及Agent程序安装完成后，修改`C:\Users\<用户名>\AppData\Roaming\rmagent\rmagent.ini`文件，将其中`#loopback=1`一行中的“#”删除以解除注释，保存文件，如图*13-16: 修改Agent程序配置文件*所示。

图 13-16: 修改Agent程序配置文件

9. 重新启动服务器。

13.1.3.4.3.2 Linux系统服务器部署Agent程序

13.1.3.4.3.2.1 应用服务与数据库部署在不同的服务器的情况

操作步骤

1. 使用安全管理员*#secadmin#*登录云盾数据库审计系统。
2. 在**维护**页面，选择**Agent管理**，单击**下载Agent**。

   系统自动弹出Agent部署配置提示，且浏览器自动开始将Agent程序（即rmagent.tar.gz文件）下载至本地。
3. 在**Agent部署配置**对话框中，输入需要部署Agent程序的服务器IP地址，然后单击**添加**。

说明：

- 如果需要部署Agent程序的服务器与数据库审计系统处于同一个内网，则直接添加内网地址即可；如果与数据库审计系统不在同一个内网需要通过外网进行通信的，则需添加该服务器的外网地址。
- 如果不添加部署Agent程序的服务器IP地址，审计系统将无法抓取该服务器的数据进行审计。

4. 以root用户登录需要安装Agent程序的服务器，将rmagent.tar.gz文件上传到服务器，并将其解压缩，如图 *13-17: 解压rmagent.tar.gz文件*所示。

图 13-17: 解压rmagent.tar.gz文件

```
[root@rsdsdf ~]# ls
anaconda-ks.cfg  install.log  install.log.syslog  rmagent_.tar.gz
[root@rsdsdf ~]# tar -xvf rmagent_.tar.gz
./
./stop_rmagent.sh
./Rmagent_Setup.exe
./linux64/
./linux64/rmagent
./rmagent.ini
./install.sh
[root@rsdsdf ~]#
```

5. 执行`chmod 755 install.sh`命令，给install.sh文件增加权限。
6. 安装Agent程序，如图 *13-18: 安装Agent程序*所示。

图 13-18: 安装Agent程序

```
[root@rsdsdf ~]# ./install.sh
start rmagent ...
start rmagent success
[root@rsdsdf ~]# ^C
[root@rsdsdf ~]# _
```

7. 安装完成后，启动Agent程序（rmagent），如图 *13-19: 启动Agent程序*所示。

图 13-19: 启动Agent程序

```
[root@mysql rmagent]# cd /usr/local//rmagent/
[root@mysql rmagent]# ./rmagent
[root@mysql rmagent]#
```

13.1.3.4.3.2.2 应用服务与数据库部署在同一台服务器的情况

操作步骤

1. 使用安全管理员#secadmin#登录云盾数据库审计系统。
2. 在**维护**页面，选择**Agent管理**，单击**下载Agent**。

   系统自动弹出Agent部署配置提示，且浏览器自动开始将Agent程序（即rmagent.tar.gz文件）下载至本地。
3. 在**Agent部署配置**对话框中，输入需要部署Agent程序的服务器IP地址，然后单击**添加**。

说明：

- 如果需要部署Agent程序的服务器与数据库审计系统处于同一个内网，则直接添加内网地址即可；如果与数据库审计系统不在同一个内网需要通过外网进行通信的，则需添加该服务器的外网地址。
- 如果不添加部署Agent程序的服务器IP地址，审计系统将无法抓取该服务器的数据进行审计。

4. 以root用户登录需要安装Agent程序的服务器，将rmagent.tar.gz文件上传到服务器，并将其解压缩，如图 *13-20: 解压rmagent.tar.gz文件*所示。

图 13-20: 解压rmagent.tar.gz文件

```
[root@rsdsdf ~]# ls
anaconda-ks.cfg  install.log  install.log.syslog  rmagent_.tar.gz
[root@rsdsdf ~]# tar -xvf rmagent_.tar.gz
./
./stop_rmagent.sh
./Rmagent_Setup.exe
./linux64/
./linux64/rmagent
./rmagent.ini
./install.sh
[root@rsdsdf ~]#
```

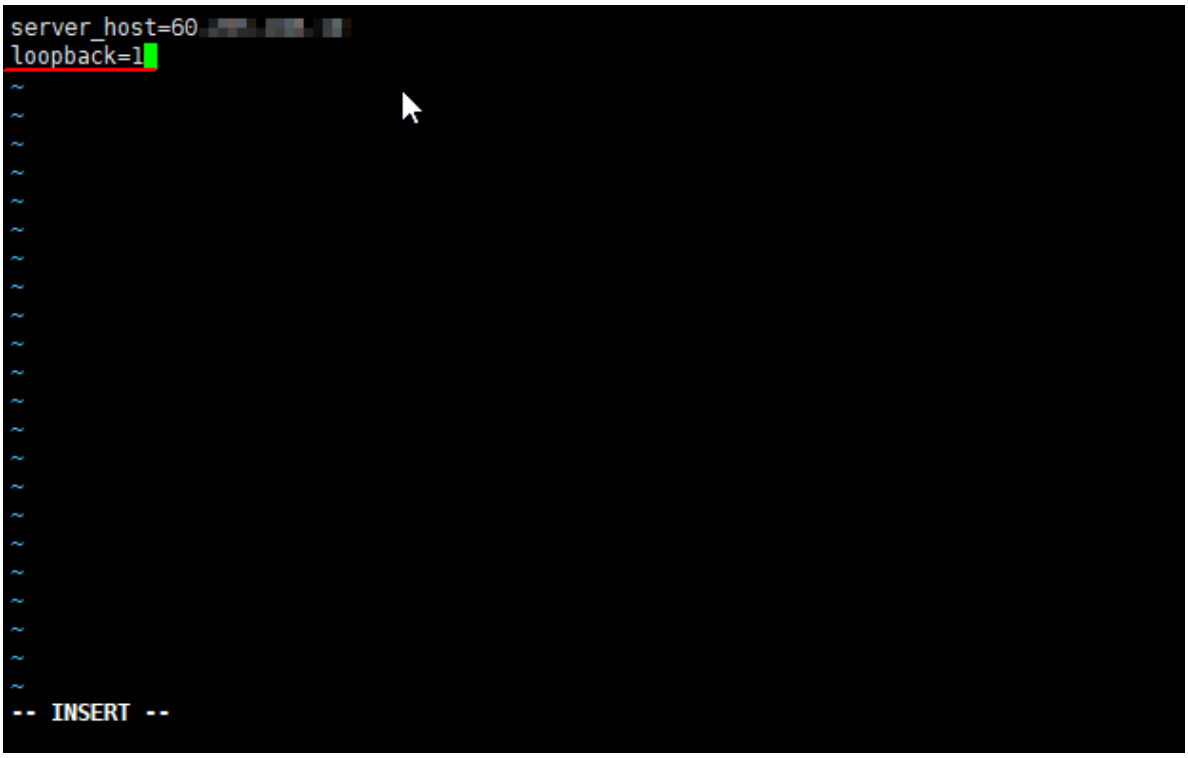
5. 执行`chmod 755 install.sh`命令，给install.sh文件增加权限。
6. 安装Agent程序，如图 *13-21: 安装Agent程序*所示。

图 13-21: 安装Agent程序

```
[root@rsdsdf ~]# ./install.sh
start rmagent ...
start rmagent success
[root@rsdsdf ~]# ^C
[root@rsdsdf ~]#
```

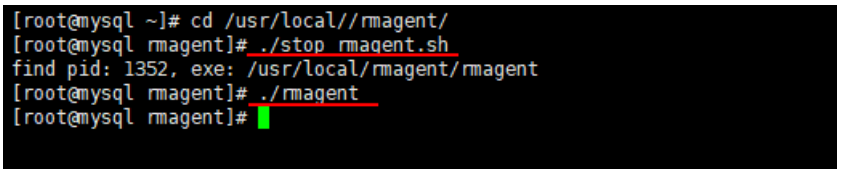
7. 安装完成后，进入rmagent安装目录，使用VI编辑器修改rmagent.ini配置文件，在文件最后加入一行`loopback=1`，然后保存，如图 *13-22: 修改Agent程序配置文件*所示。

图 13-22: 修改Agent程序配置文件



8. 执行`./stop_rmagent.sh`命令停止rmagent进程后，执行`./rmagent`命令重启Agent程序，如图 *13-23: 重启Agent程序*所示。

图 13-23: 重启Agent程序



13.1.3.4.3.3 部署注意事项

Agent程序默认连接云盾数据库审计系统的内网IP，如果部署Agent程序的服务器与云盾数据库审计系统之间通过外网连接则需要修改rmagent.ini中的IP地址。

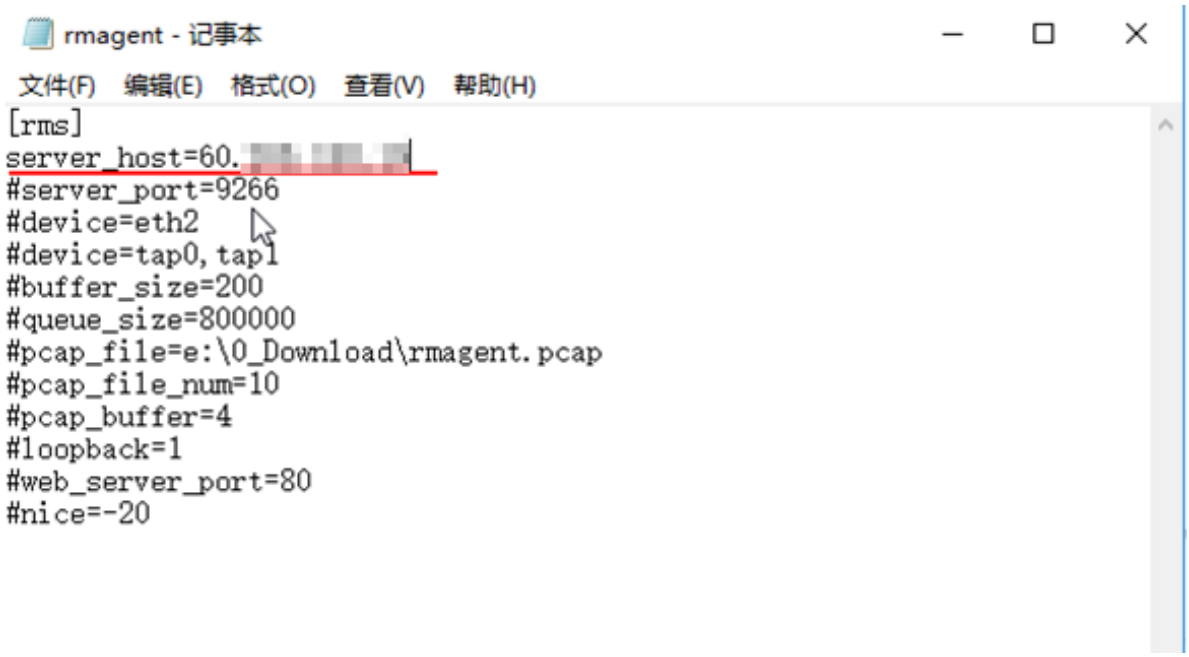
13.1.3.4.3.3.1 Windows系统服务器修改Agent程序连接地址

操作步骤

1. 登录数据库所在服务器或RDS数据库实例所对应的应用服务器。

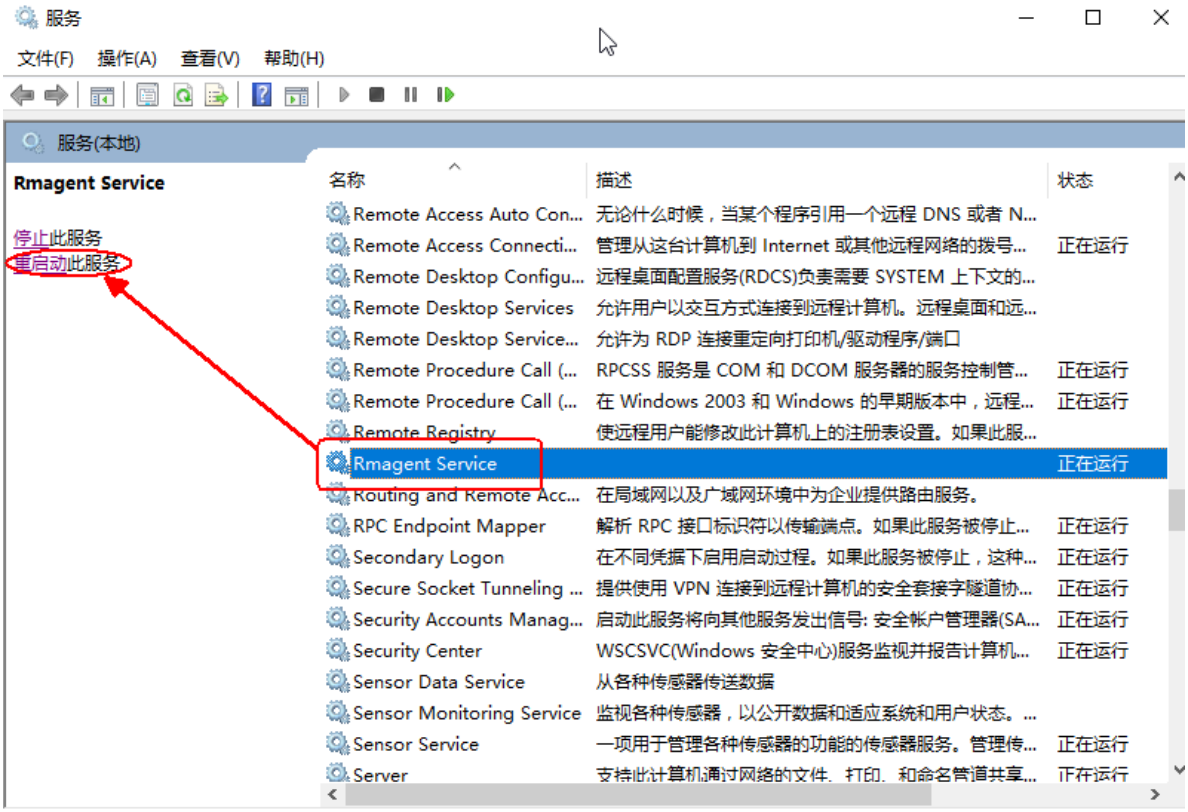
2. 找到并修改*C:\Users*用户名*\AppData\Roaming\rmagent\rmagent.ini*配置文件，将其中server_host一行的IP地址修改为云盾数据库审计系统的外网IP地址，保存文件，如图 *13-24: 修改Agent程序连接地址*所示。

图 13-24: 修改Agent程序连接地址



3. 重新启动rmagent服务。在服务管理器，选中Rmagent Service服务，单击**重启动此服务**，如图 *13-25: 重启Agent程序服务*所示。

图 13-25: 重启Agent程序服务



13.1.3.4.3.3.2 Linux系统服务器修改Agent程序连接地址

操作步骤

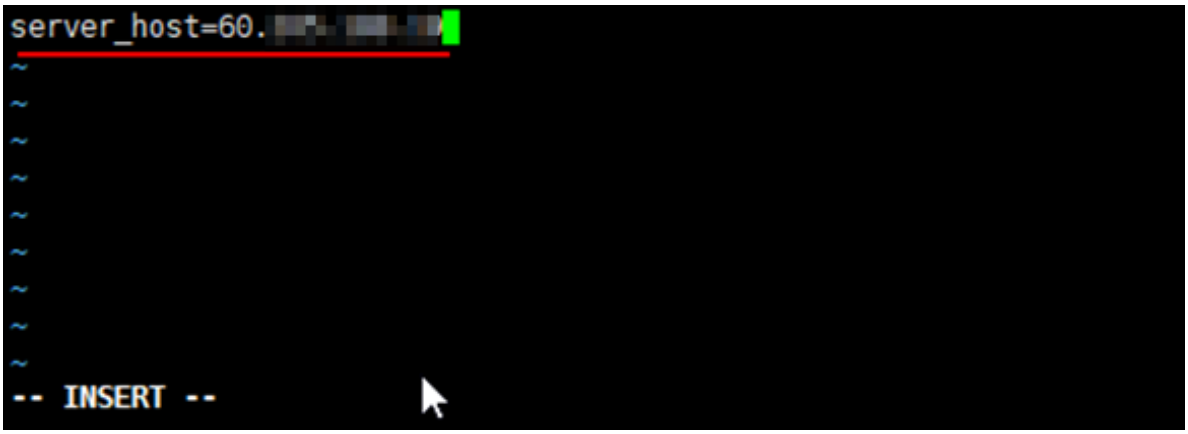
1. 登录数据库所在服务器或RDS数据库实例所对应的应用服务器。
2. 进入rmagent安装目录，使用VI编辑器修改rmagent.ini配置文件，如图 *13-26: 修改Agent程序配置文件*所示。

图 13-26: 修改Agent程序配置文件

```
[root@mysql ~]# cd /usr/local//rmagent/
[root@mysql rmagent]# vi rmagent.ini
```

3. 将server_host的值修改为云盾数据库审计系统的外网IP地址，然后保存，如图 *13-27: 修改Agent程序连接地址*所示。

图 13-27: 修改Agent程序连接地址



4. 执行`./stop_rmagent.sh`命令停止rmagent进程后，执行`./rmagent`命令重启Agent程序。

13.1.3.4.4 部署测试

您可以通过已安装Agent程序的应用服务器访问被审计的数据库实例并执行SQL语句，然后使用安全管理员账号登录云盾数据库审计系统，查看是否有审计信息。

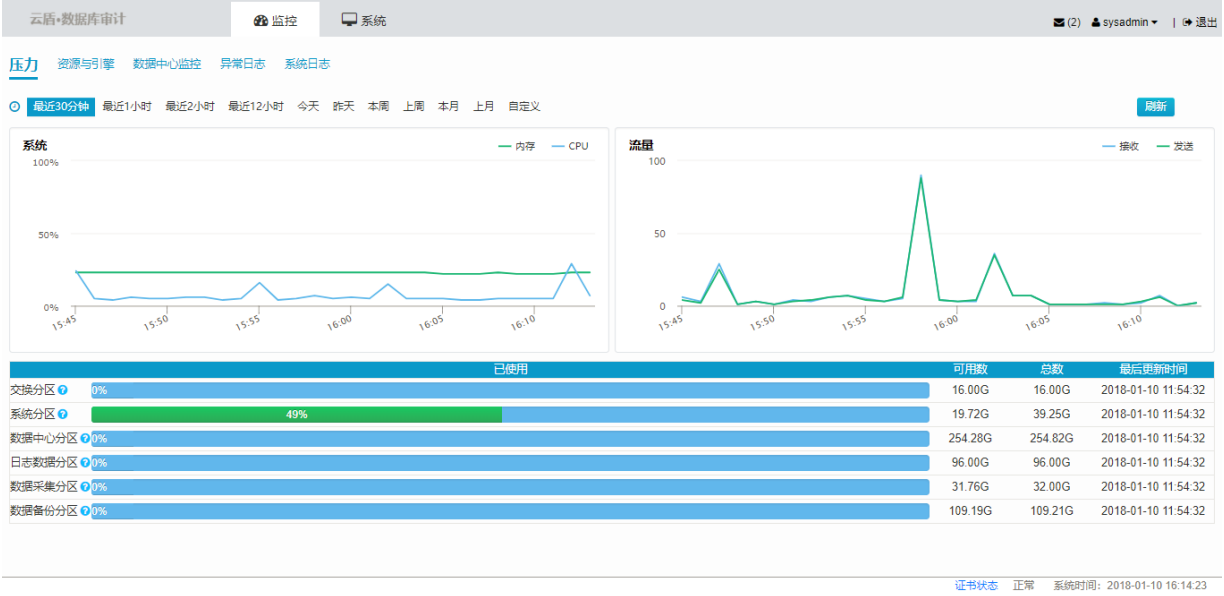
- 如果云盾数据库审计系统正常记录了该数据库实例的审计信息，则说明数据库实例部署成功。
- 如果云盾数据库审计系统未能记录到审计信息，请检查对应的Agent配置部署信息、Agent程序的服务进程和连接配置等。

13.2 系统管理员指南

系统管理员是云盾数据库审计系统的三大管理员之一，基于系统级别的操作对本系统进行统一的监控与管理。系统管理员可以监控系统性能、控制网络配置、管理系统升级和进行系统安全管理。

通过系统管理员（sysadmin）账号登录云盾数据库审计系统，如图 *13-28: 系统管理页面*所示。

图 13-28: 系统管理页面



云盾数据库审计系统为系统管理员提供以下两大功能模块：

- **监控模块**：基于产品的系统层面，监控产品性能
- **系统模块**：产品系统级配置

13.2.1 系统

系统管理员第一次登录云盾数据库审计系统后，需要进入**系统**模块完成相应的系统及配置。

13.2.1.1 证书管理

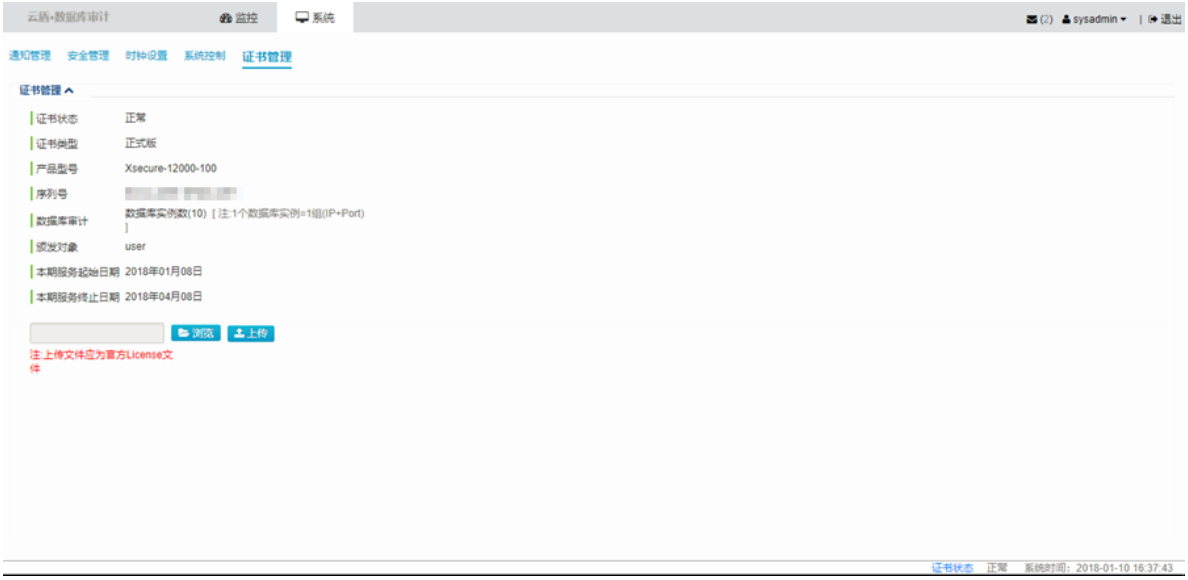
背景信息

证书管理页面，用于进行License的校验。只有在上传有效证书，且校验通过后系统才可以正常使用云盾数据库审计系统。

操作步骤

1. 使用系统管理员*#sysadmin#*账号登录云盾数据库审计系统。
2. 定位到**系统** > **证书管理**页面，单击**浏览**。
3. 从本地选择正式版License文件，单击**打开**，单击**上传**。
4. 证书上传且校验通过后，可查看证书信息，如图 *13-29:* 证书信息所示。

图 13-29: 证书信息



13.2.1.2 系统控制

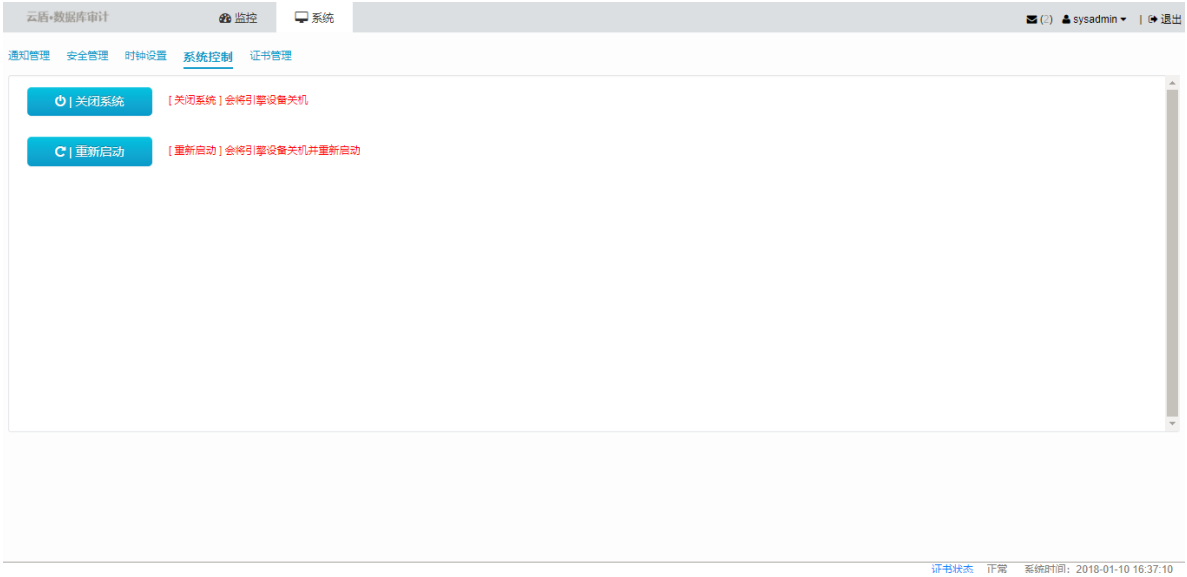
背景信息

在**系统控制**页面，系统管理员可以管理数据库审计系统服务器。

操作步骤

1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
2. 定位到**系统** > **系统控制**，管理数据库审计系统服务器，如图 *13-30:* 系统控制页面所示。
   - 单击**关闭系统**，可关闭数据库审计系统服务器。
   - 单击**重新启动**，可重启数据库审计系统服务器。

图 13-30: 系统控制页面



说明：

云盾数据库审计系统服务器关闭或重新启动期间，将无法提供任何功能，请谨慎操作。

13.2.1.3 时钟设置

背景信息

在**时钟设置**页面，系统管理员可以启用自动同步时间功能。不启用自动同步功能时，云盾数据库审计系统默认使用系统当前时间。

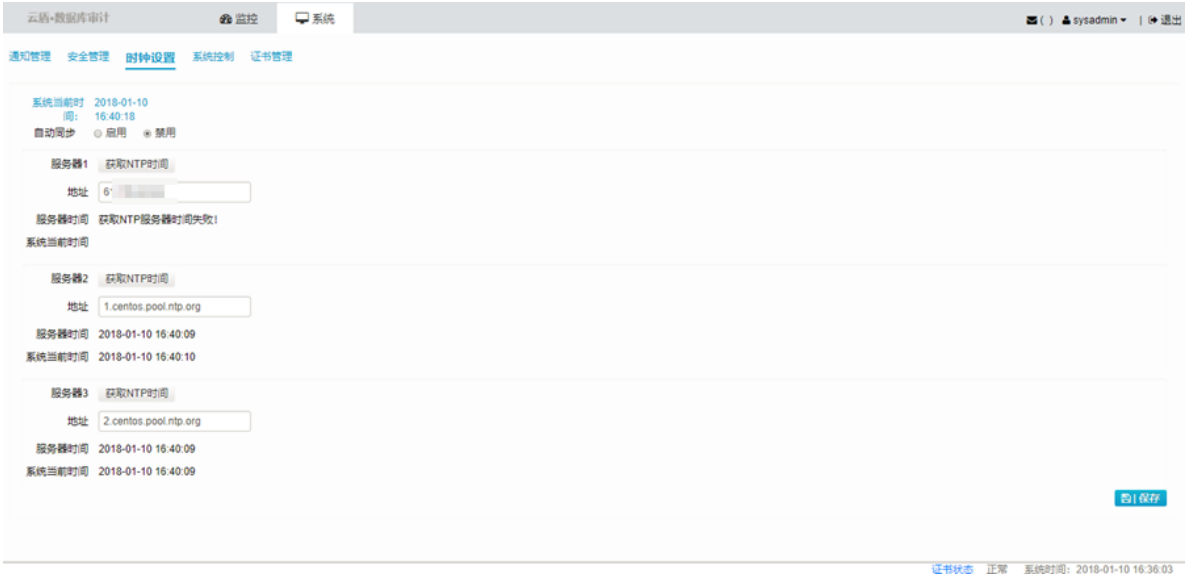
说明：

自动同步功能默认为禁用状态。

操作步骤

1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
2. 定位到**系统** > **时钟设置**页面，单击**启用**，如图 *13-31:* 时钟设置页面所示。

图 13-31: 时钟设置页面



3. 设置时间同步服务器地址，单击**获取NTP时间**。
4. 服务器时间获取成功后，单击**保存**，即开启自动同步功能。

13.2.1.4 安全管理

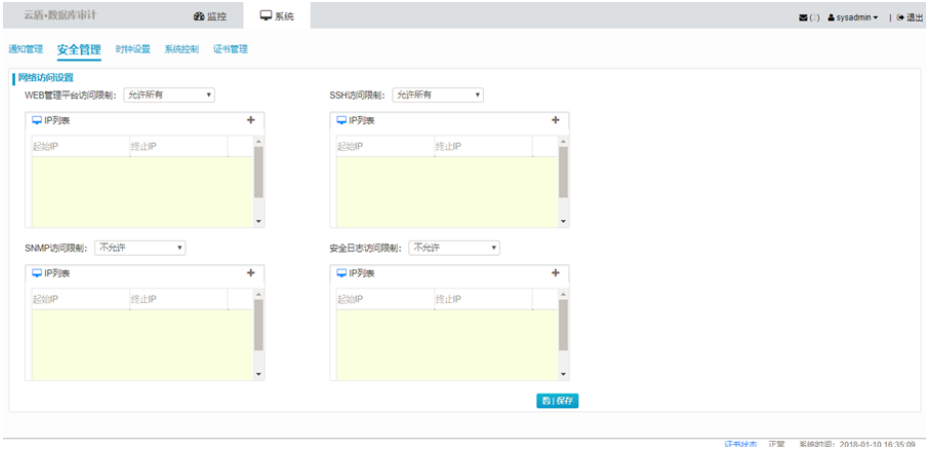
背景信息

在**安全管理**页面，系统管理员可以设置DNS服务器配置以及网络访问配置。

操作步骤

1. 使用系统管理员*#sysadmin#*账号登录云盾数据库审计系统。
2. 定位到**系统** > **安全管理**页面，分别为WEB管理平台、SNMP、SSH、安全日志设置访问限制，如图 *13-32:* 网络访问设置所示。

图 13-32: 网络访问设置



- 选择**允许所有**，即允许任何IP连接。
- 选择**不允许**，即不允许任何IP连接。

> **说明**：
> WEB管理平台访问限制无法设置为不允许。

- 选择**IP列表允许**，即只允许下方列表中的IP连接。单击IP列表右上方的添加按钮，可添加允许访问的IP或IP段；选择已添加IP，单击删除按钮可删除该IP。

> **说明**：
> IP列表中的IP或IP段之间用英文分号（；）分隔，IP段用半字线符号（-）连接。例如，192.168.1.1-192.168.1.10;192.168.1.200-192.168.1.255。

3. 设置完成后，单击**保存**，网络访问设置即生效。

13.2.1.5 通知管理

背景信息

在**通知管理**页面，系统管理员可设置发送告警通知的Email服务器配置信息，并可以对Email配置信息的正确性进行验证。

操作步骤

1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
2. 定位到**系统** > **通知管理**页面，设置发送告警通知的Email服务器配置信息，如图 *13-33:* 告警通知管理所示。

图 13-33: 告警通知管理

3. 填写完Email配置信息后，单击**保存**。
4. 填写收件人地址，单击**发送测试邮件**，可对Email配置信息的正确性进行验证。

   如设置的收件人邮箱可收到测试邮件，表示Email配置信息正确。

13.2.2 监控

系统管理员具备对云盾数据库审计整体系统监控的能力，监控内容包括压力、资源与引擎、数据中心监控、异常日志、系统日志等信息。

13.2.2.1 压力

背景信息

在**压力**页面，展示云盾数据库审计整体系统压力分析的情况，主要包括两大区域：

- **区域一**：**根据指定时间周期或自定义周期查询系统压力情况**

  系统监控：内存、CPU使用情况，用于判断性能压力

  流量监控：接收、发送的流量情况，用于判断网络压力

- **区域二**：**查询系统各分区使用情况**

  针对系统的交换分区、系统分区、数据中心分区、日志数据分区、数据采集分区、数据备份分区等进行监控，并以百分比形式展现分区已使用情况。

操作步骤

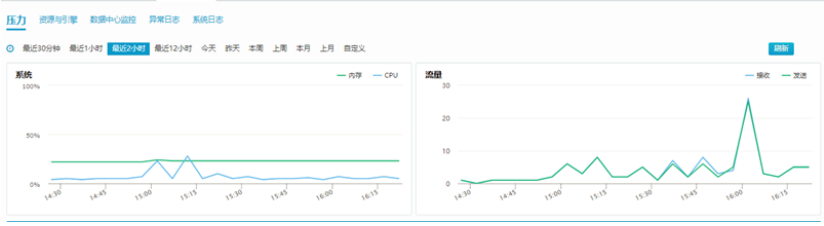
1. 使用系统管理员#*sysadmin*#账号登录云盾数据库审计系统。
2. 定位到**监控** > **压力**页面，选择时间周期，查看数据库审计系统的压力分析情况。

说明：

单击**刷新**，可刷新当前压力页面的展示信息。

- 查看系统压力情况，如图 *13-34: 系统压力情况*所示。

图 13-34: 系统压力情况

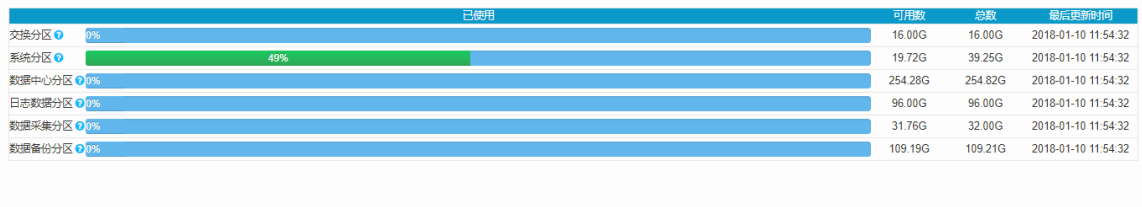


说明：

将鼠标移至系统监控图或流量监控图中，可查看该时间点的具体性能情况或网络情况。

- 查看系统各分区使用情况，如图 *13-35: 系统分区使用情况*所示。

图 13-35: 系统分区使用情况



	已使用	可用数	总数	最后更新时间
交换分区	0%	16.00G	16.00G	2018-01-10 11:54:32
系统分区	49%	19.72G	39.25G	2018-01-10 11:54:32
数据中心分区	0%	254.28G	254.82G	2018-01-10 11:54:32
日志数据分区	0%	96.00G	96.00G	2018-01-10 11:54:32
数据采集分区	0%	31.76G	32.00G	2018-01-10 11:54:32
数据备份分区	0%	109.19G	109.21G	2018-01-10 11:54:32

13.2.2.2 资源与引擎

背景信息

资源与引擎页面，主要用于监控各引擎的运行状态及资源的使用情况。

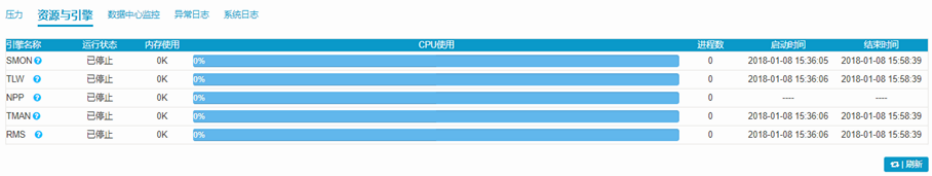
操作步骤

1. 使用系统管理员*#sysadmin#*账号登录云盾数据库审计系统。
2. 定位到**监控** > **资源与引擎**页面，查看各引擎的运行状态及资源的使用情况，如图 *13-36: 引擎运行状态及资源使用情况*所示。

说明：

单击**刷新**，可刷新各引擎的运行状态及资源实时使用情况。

图 13-36: 引擎运行状态及资源使用情况



13.2.2.3 数据中心监控

背景信息

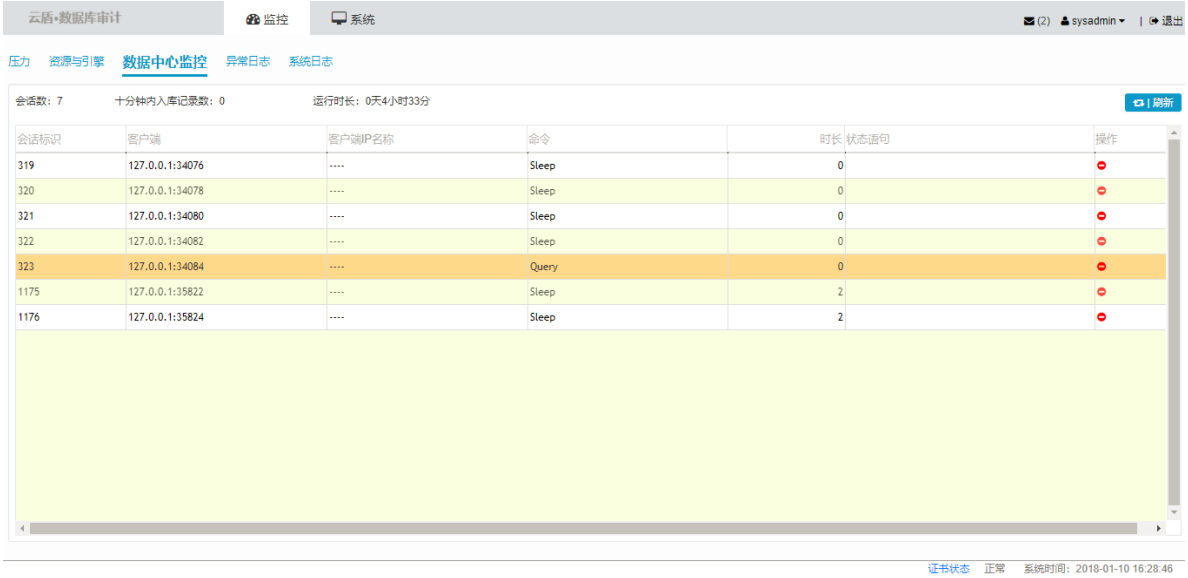
数据中心监控页面，用于监控数据中心的状态、最近十分钟入库记录数、运行时长、以及相关的会话信息等。

操作步骤

1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
2. 定位到**监控** > **数据中心监控**页面，查看数据中心监控状态，如图 *13-37:* 数据中心监控情况所示。

> **说明**：
> 单击**刷新**，可刷新数据中心实时监控状态。

图 13-37: 数据中心监控情况



选择监控会话，单击操作栏的结束会话按钮，可以终止该会话以释放资源。

13.2.2.4 异常日志

背景信息

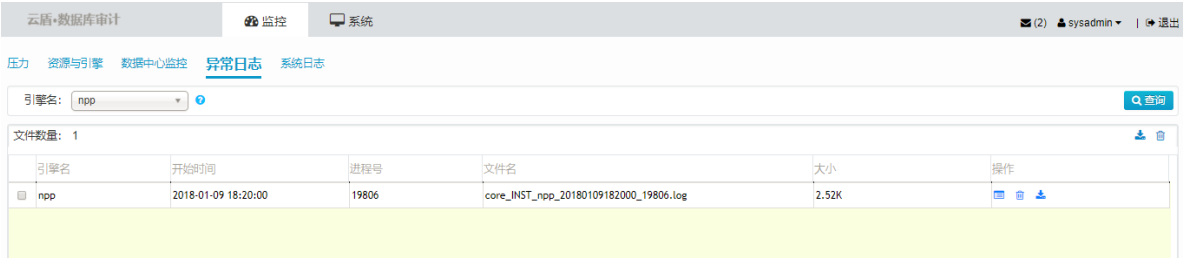
异常日志页面记录了各个引擎的异常信息，用于分析排查系统异常错误。

操作步骤

1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
2. 定位到**监控** > **异常日志**页面，选择**引擎名**，单击**查询**，查看该引擎的异常日志记录，如图*13-38: 引擎异常日志*所示。

> **说明**：
> 选择引擎名时提示无数据，表示没有引擎出现异常。

图 13-38: 引擎异常日志



3. 选择异常日志文件，可进行以下操作。
   - 单击操作栏中的查看按钮，查看异常日志文件详细信息。
   - 单击操作栏中的删除按钮，删除该异常日志文件记录。
   - 单击操作栏中的下载按钮，可将该异常日志文件下载到本地。

> **说明**：
> 选择多个异常文件记录，单击右上方的批量下载、批量删除按钮，可将选中的异常日志文件批量下载至本地或删除。

13.2.2.5 系统日志

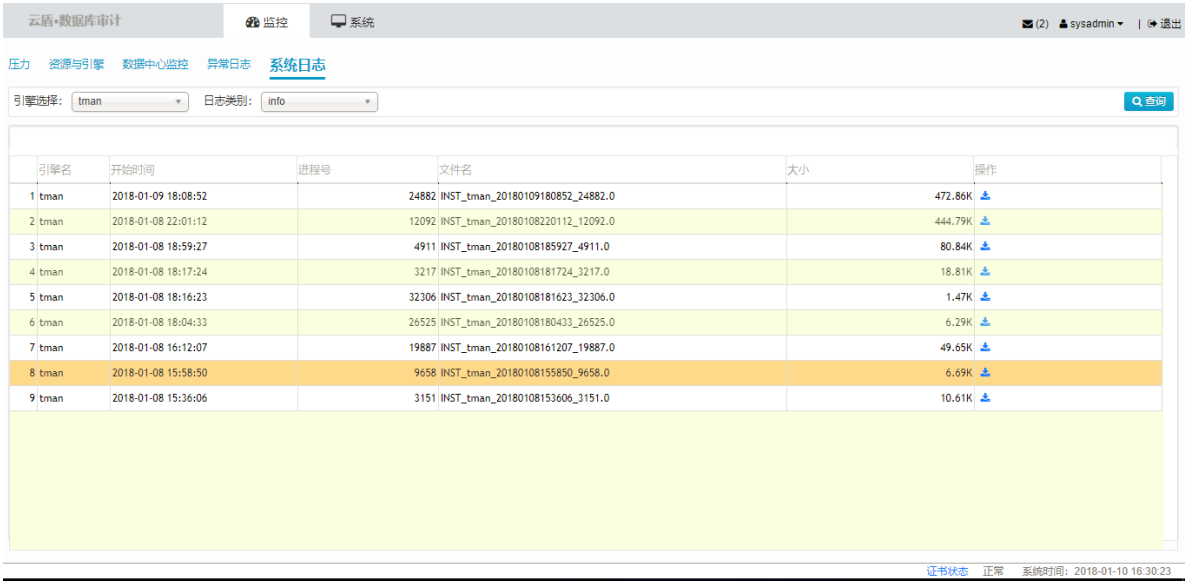
背景信息

系统日志页面记录了每个引擎运行期间的日志信息，包括alw、gmon、im、npc、npp、smon、tlw、tman、dlp等引擎，日志类别包括error和info两种日志。

操作步骤

1. 使用系统管理员#sysadmin#账号登录云盾数据库审计系统。
2. 定位到**监控** > **系统日志**页面，选择引擎、日志类别，单击**查询**，查看该引擎的系统日志记录，如图 *13-39:* 引擎系统日志所示。

图 13-39: 引擎系统日志



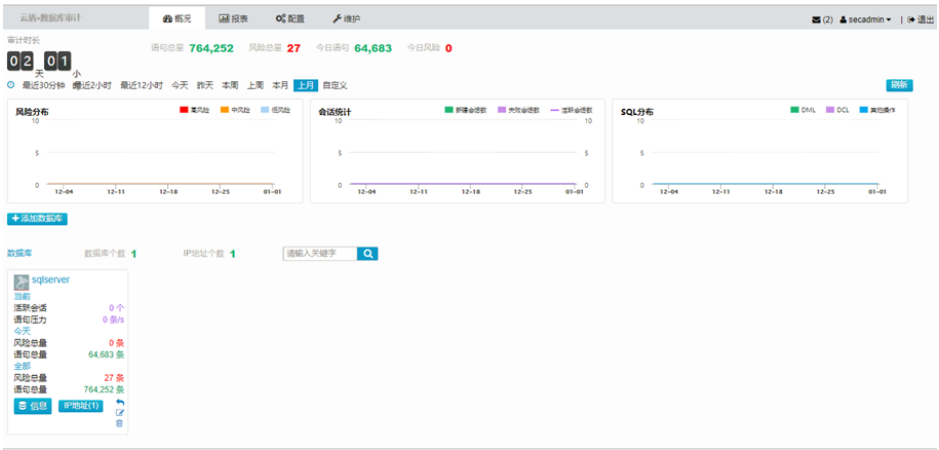
3. 选择日志文件，单击操作栏中的下载按钮，可将该日志文件下载到本地。

13.3 安全管理员指南

安全管理员（secadmin）是系统默认存在的用户，是监控、管理、制定审计安全策略的工作人员。

通过安全管理员登录数据库审计系统，如图 *13-40:* 安全管理页面所示。

图 13-40: 安全管理页面



数据库审计系统为安全管理员提供四大功能模块，包括概况、报表、配置、维护。

13.3.1 概况

概况页面由上而下分为两个区域，系统检测与数据库监控。

13.3.1.1 系统检测

背景信息

系统检测区域展示当前数据库审计系统的审计状态，包括审计时长、系统风险总量、SQL分布情况等。

操作步骤

1. 使用安全管理员#secadmin#登录云盾数据库审计系统。
2. 定位到**概况**页面，查看当前数据库审计系统的审计状态，如图 *13-41: 审计状态*所示。

图 13-41: 审计状态

- **审计时长**：系统的审计时间，统计本系统自开始审计至今的总时长。
- **语句总量**：本系统审计到的所有数据库语句总量。
- **风险总量**：本系统所有数据库审计到的风险总量。
- **今日语句**：本系统截止访问时间当日的审计语句量。
- **今日风险**：本系统截止访问时间当日的风险总数。

3. 选择时间维度，查看风险分布、会话统计、SQL分布图。

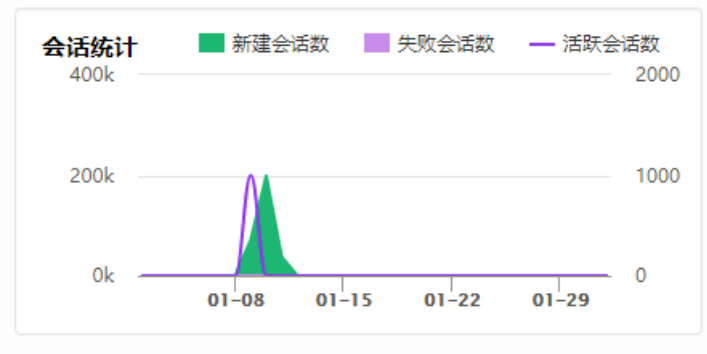
> **说明**：
> 根据选择的时间范围，图形的统计粒度也相应调整。

- **风险分布**：风险分布图基于高、中、低风险，以时间为单位统计某一时间范围内所有数据库总体风险分布情况。风险分布图采用动态展现形式，可以通过单击统计图例，根据统计需求动态展现风险分布情况，如图 *13-42: 风险分布图*所示。

图 13-42: 风险分布图

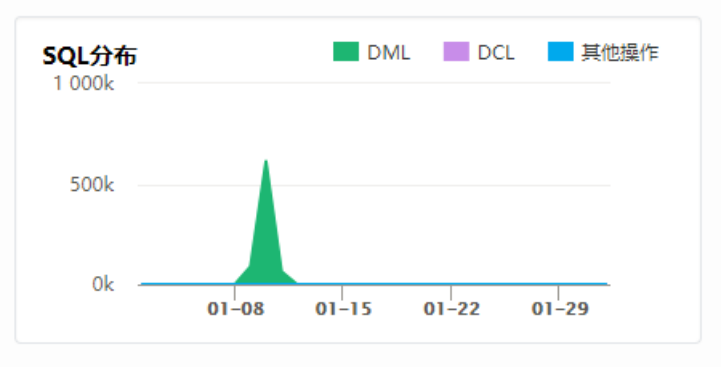
- **会话统计**：会话统计图基于新建会话数、活跃会话数等统计某一时间范围内会话数变化趋势。与风险分布图相同，在会话统计图中也可以通过单击统计图例，根据统计需求动态展现会话统计情况，如图 *13-43: 会话统计图*所示。

图 13-43: 会话统计图



  - 新建会话数：指某一时间段内新建生成的会话数
  - 活跃会话数：指某一时间段内同步产生的会话数
- **SQL分布**：SQL分布图，基于DML（数据管理）、DCL（数据控制）和其他操作分类统计某一时间范围内SQL语句类分布情况。SQL分布图同样支持通过单击统计图例，根据统计需求动态展现SQL分布情况，如图 *13-44: SQL分布图*所示。

图 13-44: SQL分布图



13.3.1.2 数据库监控

数据库监控区域，是针对当前系统审计所有数据库的汇总展示区域，可以一览当前数据库审计的全貌。数据库列表汇总展现了每个数据库的审计信息，包括当前活跃会话、当前语句压力；今天风险总量、今天语句总量；全部风险总量、全部语句总量，如图 *13-45:* 数据库监控区域所示。

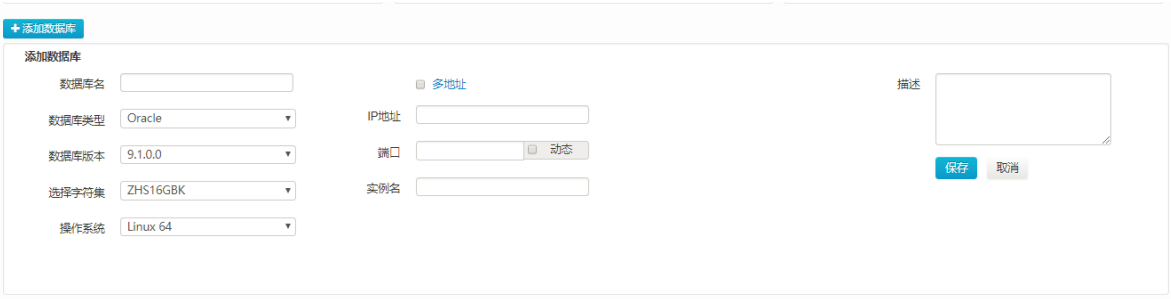
图 13-45: 数据库监控区域

13.3.1.2.1 添加数据库

操作步骤

1. 使用安全管理员*#secadmin#*登录云盾数据库审计系统。
2. 定位到**概况**页面，单击**添加数据库**，打开添加数据库页面，如图 *13-46:* 添加数据库页面所示。

图 13-46: 添加数据库页面



3. 在**添加数据库**页面中，设置所需添加的数据库的相关信息，单击**保存**。

> **说明**：
> 添加SQL Server数据库时，还需要完成**会话识别配置**，输入具有一定权限的用户及其登录密码，单击**校验用户权限**，确认该用户有访问权限。安全管理员也可以单击**下载创建用户参考脚本**，根据参考脚本在相关数据库中创建特定用户用于数据库审计。

13.3.1.2.2 管理已添加的数据库

操作步骤

1. 使用安全管理员#secadmin#登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，进行数据库的配置信息查看、修改与删除等操作，如图 *13-47:* 数据库列表操作所示。

图 13-47: 数据库列表操作

- 单击已添加数据库的区块，上方系统检测区域的风险分布、会话统计、SQL分布图将只显示该数据库的审计状态；单击返回全数据库区域图按钮，则重新显示所有数据库的审计状态。
- 单击**信息**，查看该数据库详细审计信息，包括审计时长、系统风险总量、SQL分布情况等，如图 *13-48: 单数据库详细审计信息*所示。

图 13-48: 单数据库详细审计信息

关于单数据库详细审计信息的更多内容，参考数据库详细信息。

> **说明**：
> 单击左上角数据库名称，选择全数据库即返回概况页面。

- 单击**IP地址**，查看该数据库IP分布情况。
- 单击修改按钮，可在数据库修改页面修改该数据库的相关配置信息，修改完成后单击保存即生效。
- 单击删除按钮，在弹出的信息提示对话框中单击确定，即删除对该数据库的审计。

13.3.2 数据库详细信息

将数据库添加至数据库审计系统后，可查看该数据库的详细审计信息并为该数据库设置具体的审计规则。

数据库详细信息页面包括概况（单库）、风险、语句、会话、报表、规则六大功能模块，并在页面左侧展示该数据库的审计状态信息。

13.3.2.1 概况（单库）

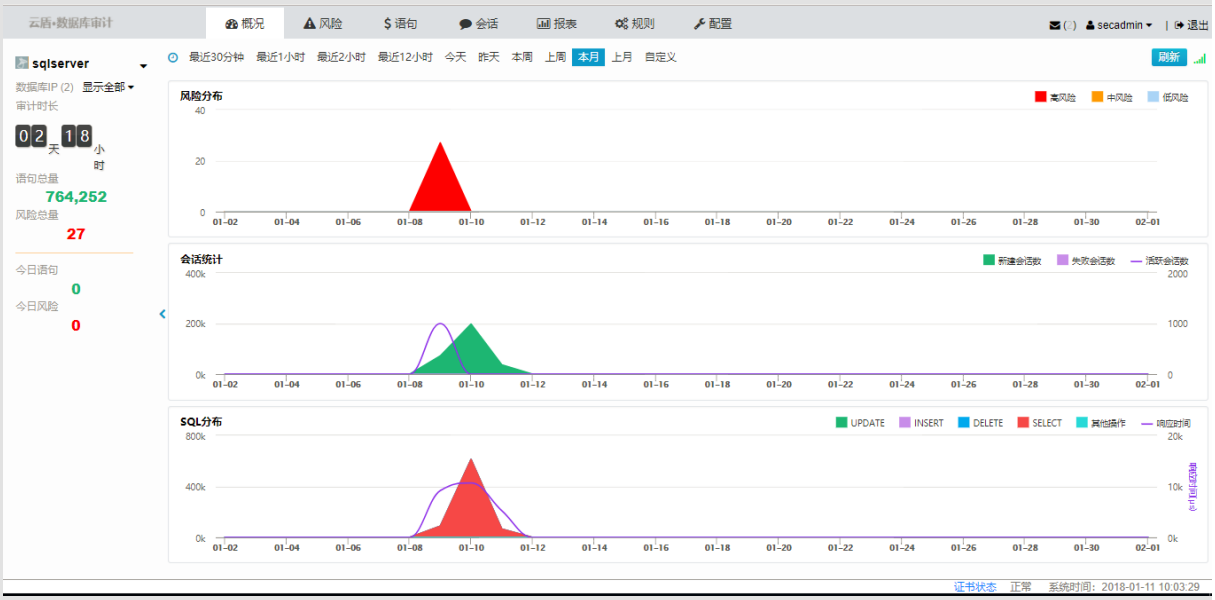
数据库详细信息的**概况**页面根据选择的数据库显示该数据库单库的审计状态，并且显示的三个统计图都支持超链接钻取，单击统计图中的具体时间点即可跳转到对应的页面查看详细审计记录。

- 风险分布图对应**风险**页面
- 会话统计图对应**会话**页面
- SQL分布图对应**语句**页面

说明：

数据库详细信息的**概况**页面中的SQL分布图采用双轴统计的方式，相比数据库审计系统**概况**页面系统检测区域中的SQL分布图，增加了数据库SQL语句的响应时间，并以折现的形式展现，如*图 13-49: 单数据库概况页面*所示。

图 13-49: 单数据库概况页面



13.3.2.1.1 查看单数据库审计状态

操作步骤

1. 使用安全管理员*#secadmin#*登录云盾数据库审计系统。

2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 查看页面左侧的该数据库的审计状态信息，如图 *13-50: 单数据库审计状态信息*所示。

图 13-50: 单数据库审计状态信息

说明：

单击数据库名称下拉菜单，选择数据库可以切换到不同的数据库详细信息页面。选择**全数据库**，则返回数据库审计系统整体的**概况**页面。

13.3.2.1.2 查看单数据库详细信息概况

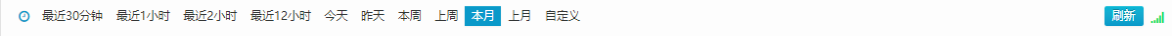
操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**概况**页面，选择时间范围，查看单数据库概况。

说明：

选择**自定义**，设置具体时间范围，单击**查询**，可查看自定义时间范围内该数据库的风险分布、会话统计、SQL分布情况，如图 *13-51: 选择时间范围*所示。

图 13-51: 选择时间范围



13.3.2.2 风险

风险页面的主要功能是对被审计的数据库进行各种风险结果的查询及分析，主要包含敏感语句、SQL注入、漏洞攻击、风险操作等风险。风险的统计结果与所设置的审计规则是息息相关的，根据为该数据库所设置的审计规则产生相应的风险记录。

13.3.2.2.1 查看风险统计结果

背景信息

风险统计是对指定数据库某一查询周期内各类风险的统计概要说明，通过图表结构展现风险统计情况。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**风险** > **风险统计**页面，选择时间范围，查看风险统计图表。

> **说明**：
> 选择**自定义**，设置具体时间范围，单击**查询**，可查看自定义时间范围内该数据库的风险统计信息。

- **风险统计交叉表**

图 13-52: 风险统计交叉表

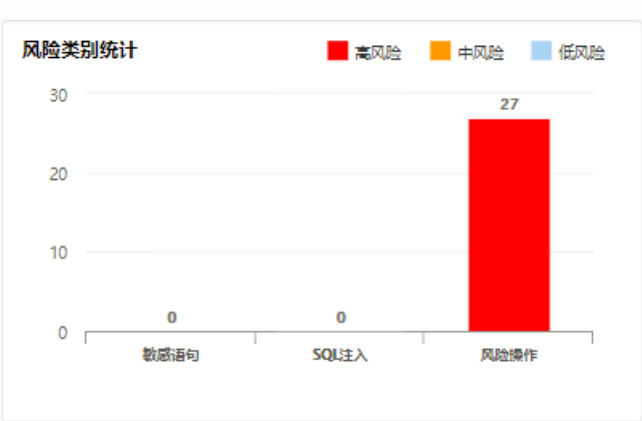
序号	风险类别	高风险	中风险	低风险
1	敏感语句	0	0	0
2	SQL注入	0	0	0
3	风险操作	27	0	0

说明：

单击表中的蓝色数值，可跳转至**规则命中**页面查看详细分析记录。

- **风险类别统计图**

图 13-53: 风险类别统计图



说明：

风险类别统计图部分采用柱形展现各类风险分布情况，便于安全管理员进行直观分析。通过单击统计图右上方的风险类别可控制是否显示该风险类别的统计数据。

13.3.2.2.2 查看规则命中记录

背景信息

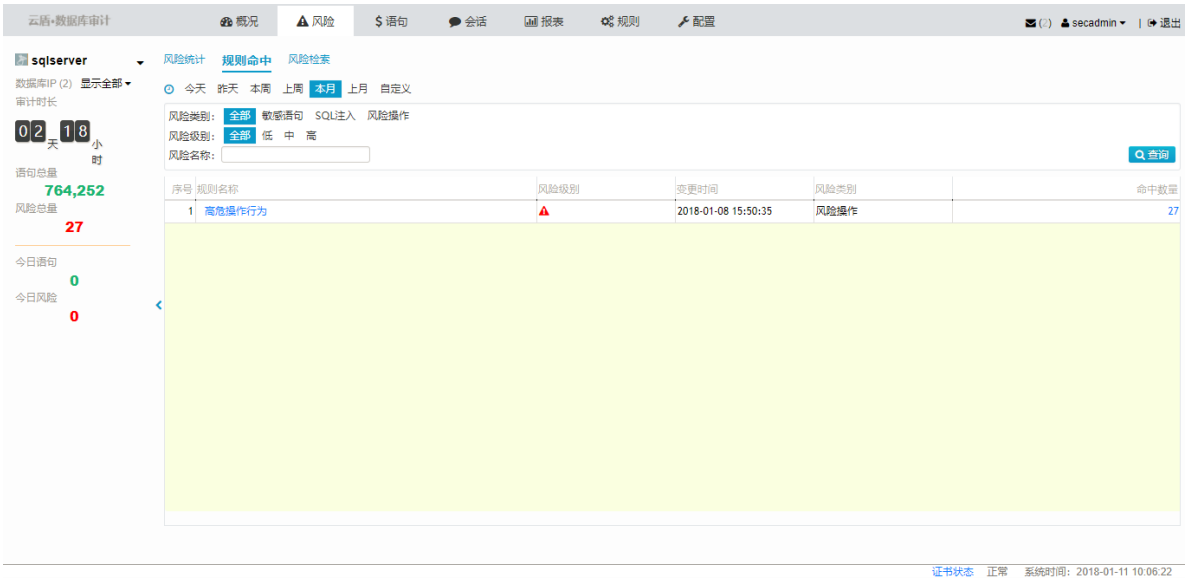
基于对风险统计结果的延伸，**规则命中**页面展现每条风险记录命中规则的详细信息。安全管理员在**规则命中**页面可以以时间为检索条件，逐一查询不同风险类别下不同风险级别的详细命中规则。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**风险** > **规则命中**页面。
4. 设置查询时间范围，选择风险类别、风险级别，查看规则清单，如图 *13-54: 查看规则清单*所示。

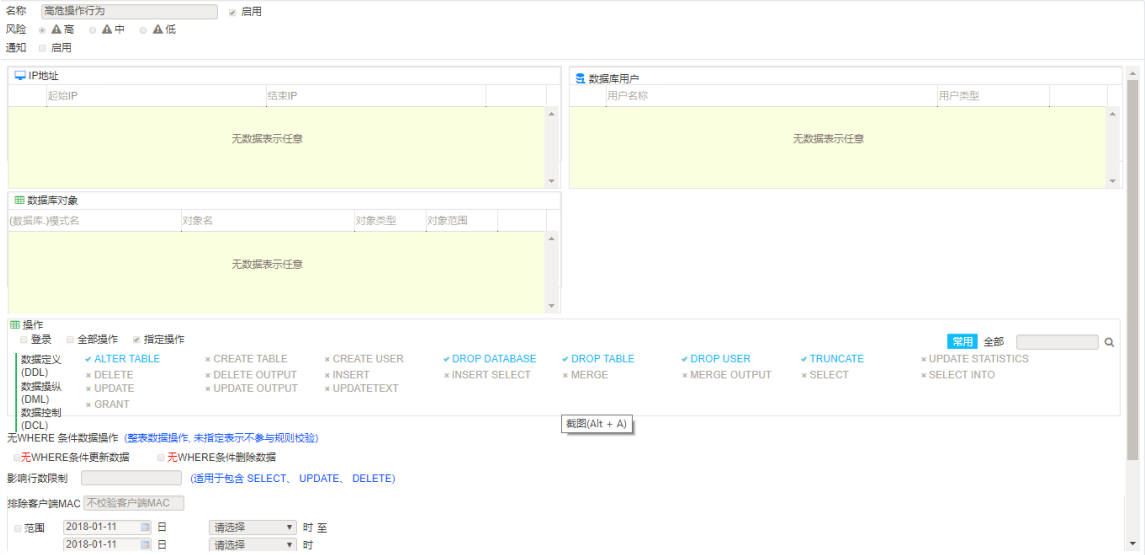
> **说明**：
> 输入风险名称，单击**查询**，可查看包含指定风险名称的规则清单。

图 13-54: 查看规则清单



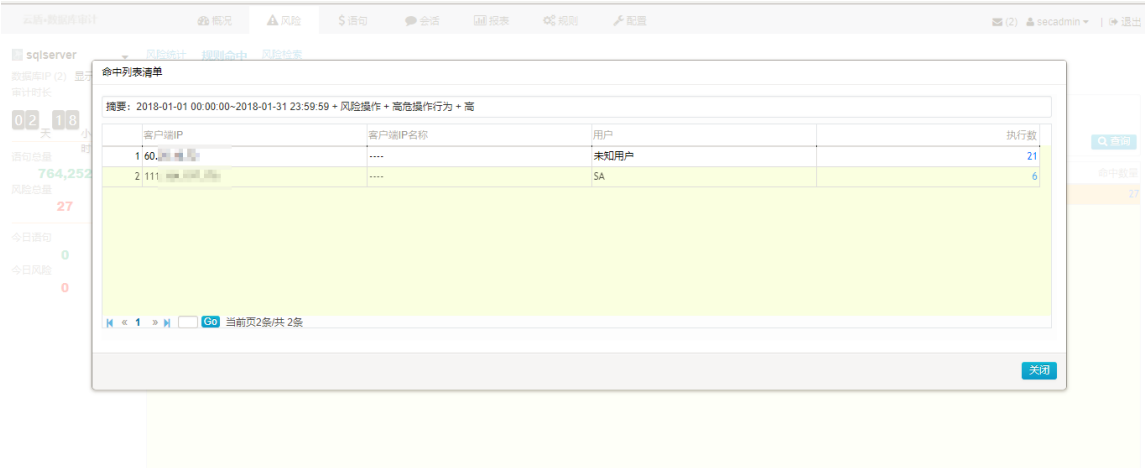
5. 查看详细信息。
   - 单击规则名称，打开**风险规则**页面，查看该规则的详细信息，如图 *13-55: 查看风险规则详细信息*所示。

图 13-55: 查看风险规则详细信息



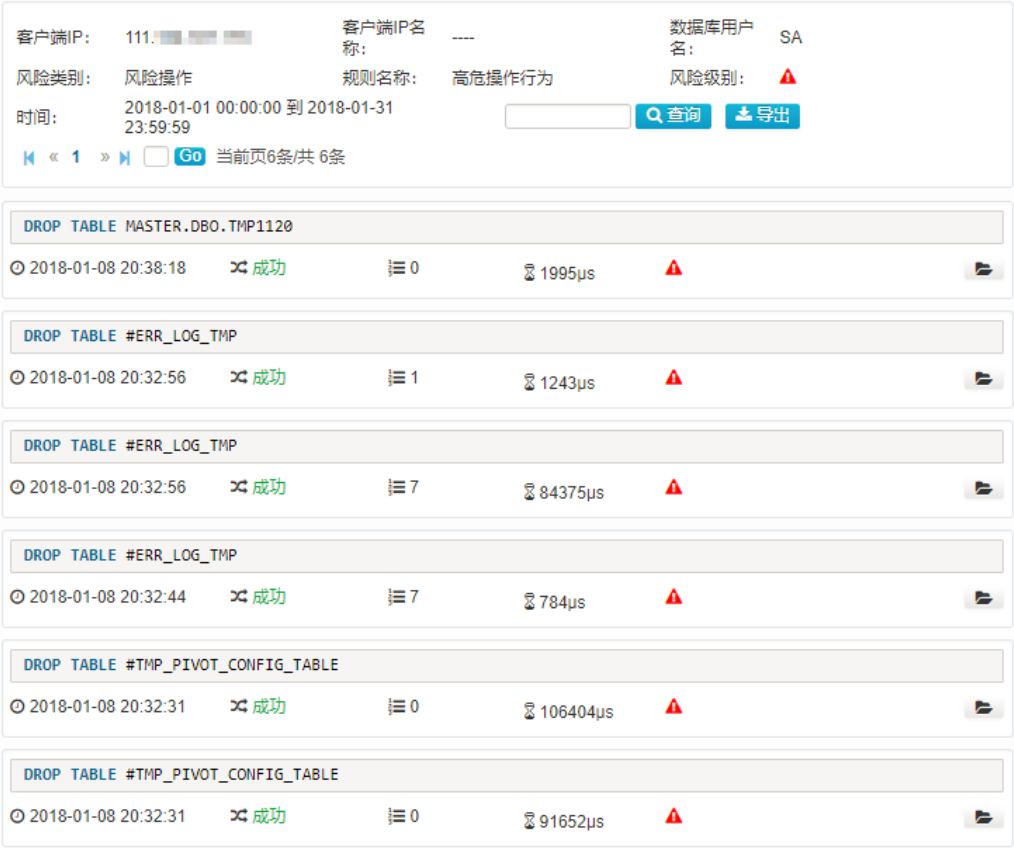
- 单击命中数量，打开**命中列表清单**页面，查看风险命中的详细信息。命中列表清单页面概要说明了风险命中信息，并列举了风险发生的客户端IP、用户、执行数，如图 *13-56: 命中列表清单*所示。

图 13-56: 命中列表清单



单击命中列表清单中的执行数，打开风险命中列表详情页面。风险命中详情页面上方的查询模板记录客户端IP、用户名称、风险类别、规则名称、风险级别、时间范畴以及“模糊查询”检索字段；下方的命中列表详细罗列了每条风险语句的触发时间、SQL、执行结果、影响行数、响应时间、风险等级，如图 *13-57: 风险命中详情页面*所示。

图 13-57: 风险命中详情页面



说明：

- 风险命中列表详情页面支持模糊查询，在查询框中输入关键字，单击**查询**，可查询特定的风险语句记录。
- 风险命中列表详情信息支持导出，单击**导出**，选择导出行数进行导出，如图 *13-58: 导出风险命中列表详情*所示。

图 13-58: 导出风险命中列表详情

导出的文件格式为csv，文件名默认为数据信息。

13.3.2.2.3 风险语句检索及处理

背景信息

风险检索是风险设置的核心组件，以列表清单的方式逐条展现风险语句的详情。风险语句的详细信息包括具体的SQL语句、（触发）时间、风险类别、风险名称、风险等级、数据库用户、客户端IP等。通过对检索到的风险语句进行设置，可将风险语句添加到信任规则、敏感语句或者不审计语句中。

操作步骤

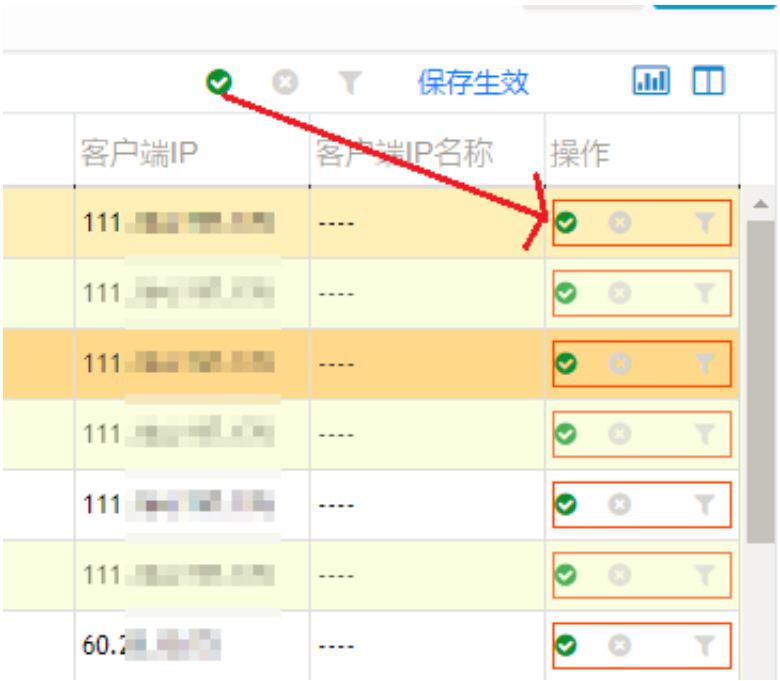
1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**风险** > **风险检索**页面，选择查询时间范围，查看风险语句记录，如图 *13-59:* 风险语句检索所示。

图 13-59: 风险语句检索

4. 选择某条风险语句，进行处理。
   - 添加到信任语句。

     单击操作栏中的设置为信任语句按钮，即可将该SQL语句设为信任语句，系统对该语句不再作风险记录，如图 *13-60:* 设置为信任语句所示。

图 13-60: 设置为信任语句



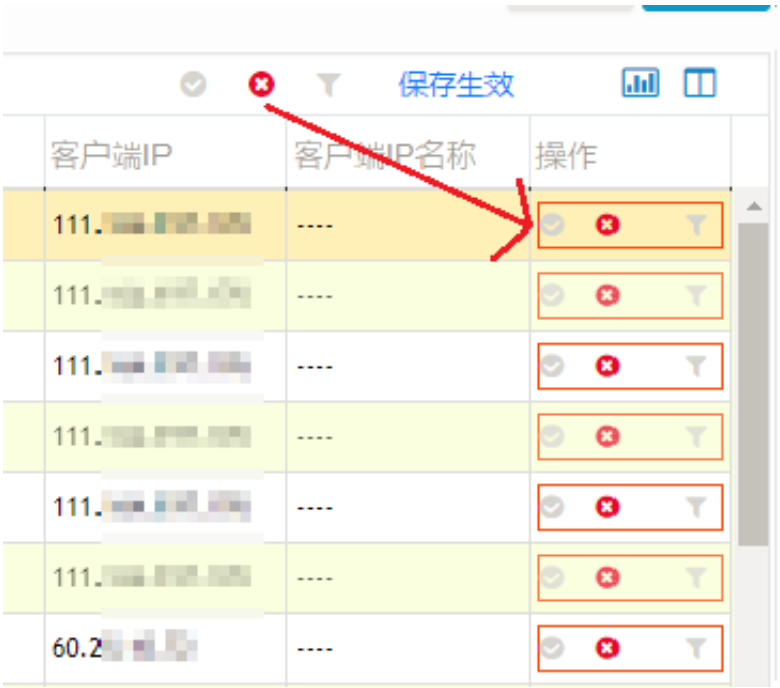
说明：

单击风险语句列表上方的全部设置为信任语句按钮，可将当前列表中的所有SQL语句设为信任语句。

- 添加到敏感语句。

  单击操作栏中的设置为敏感语句按钮，即可将该SQL语句设为敏感语句，系统将针对敏感风险进行告警，如图 *13-61: 设置为敏感语句*所示。

图 13-61: 设置为敏感语句



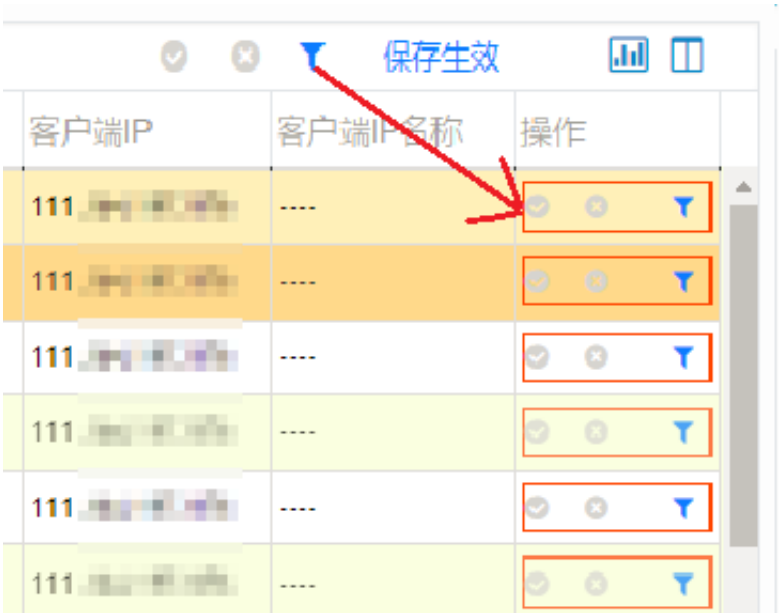
说明：

单击风险语句列表上方的全部设置为敏感语句按钮，可将当前列表中的所有SQL语句设为敏感语句。

- 设置为不审计语句。

  单击操作栏中的设置为不审计语句按钮，即可将该SQL语句设为不审计语句，系统将不再审计该语句，如图 *13-62:* 设置为不审计语句所示。

图 13-62: 设置为不审计语句



说明：

单击风险语句列表上方的全部设置为不审计语句按钮，可将当前列表中的所有SQL语句设为不审计语句。

5. 处理完成后，单击**保存生效**，根据风险语句设置的审计规则即时生效。

   保存生效后，单击**导出报告**，单击**csv导出**，可将当前风险语句列表导出，如图 *13-63:* 导出风险语句报告所示。

图 13-63: 导出风险语句报告

13.3.2.3 语句

语句页面记录了本系统审计到的所有数据库语句记录，基于语句分析可以清晰地对数据库访问的各类SQL语句进行分类查询、分析。云盾数据库审计系统支持的分析方式包括SQL统计、语句检索、模板检索、失败SQL、TopSQL、新型语句等。

13.3.2.3.1 查看SQL统计

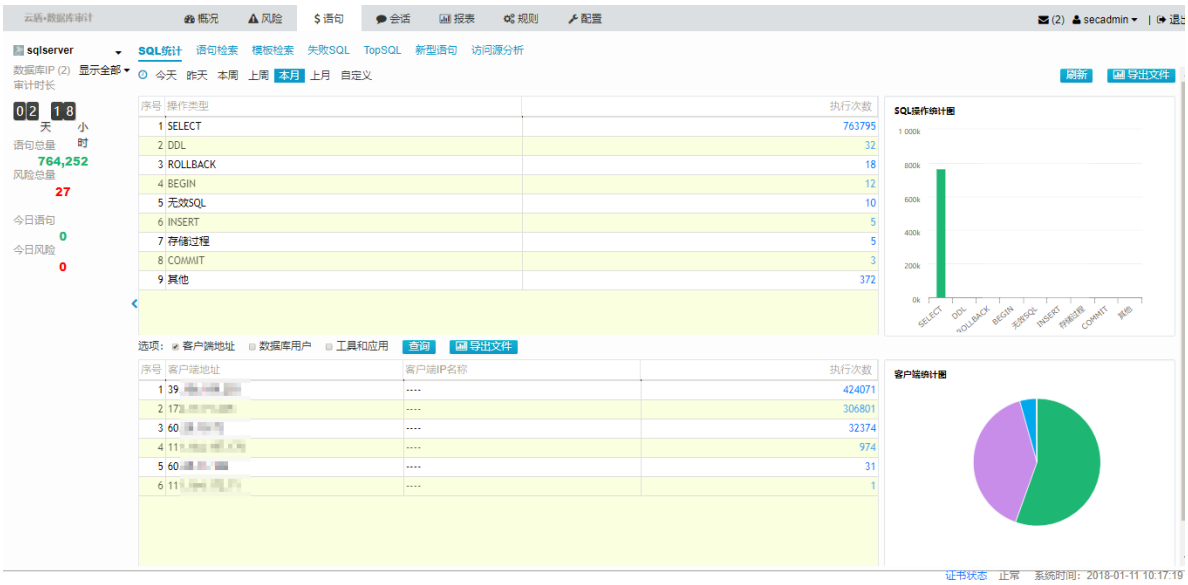
背景信息

SQL统计是对指定数据库在某一查询周期内各类SQL语句的统计概要说明，通过图表结构展现语句分布状态及语句来源统计。

操作步骤

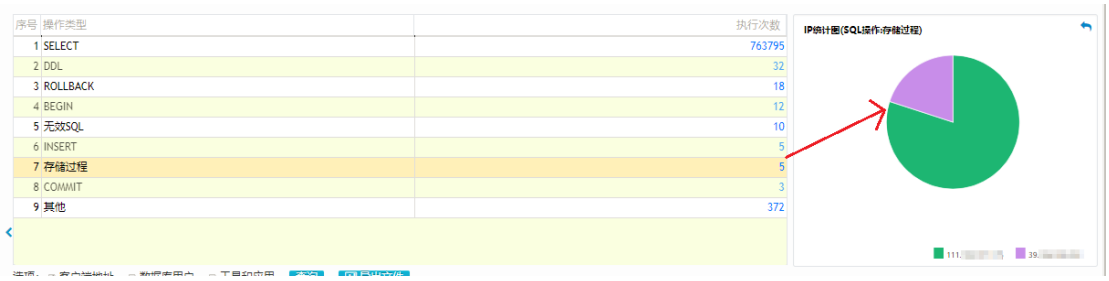
1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**语句** > **SQL统计**页面，选择查询时间范围，查看操作类型及语句来源统计结果，如图 *13-64: SQL统计页面*所示。

图 13-64: SQL统计页面



- **SQL操作类型分类统计**
  - 单击选择某操作类型，右侧的SQL操作统计图将以饼图的形式展示该操作类型的客户端IP分布情况，如图 *13-65: 查看某操作类型IP统计图*所示。

图 13-65: 查看某操作类型IP统计图



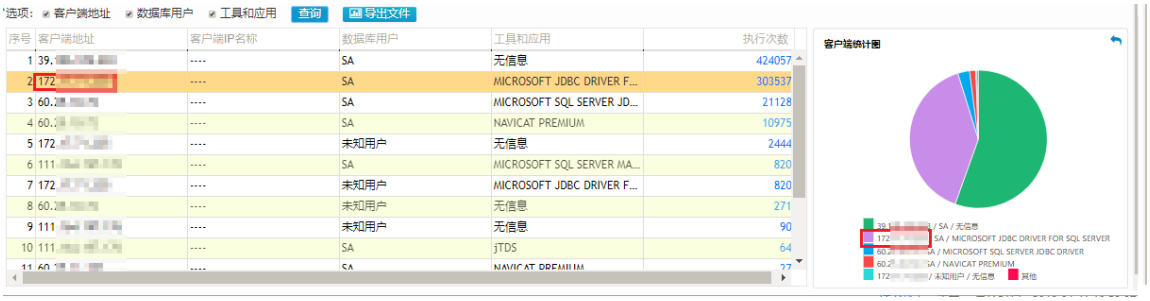
- 单击某操作类型的执行次数，可跳转至**模板检索**页面实现数据钻取。

- **语句来源分类统计**

语句来源的分类方式包括客户端IP、数据库用户、工具三种分类统计形式，支持选择多项分类，并通过饼状图帮助安全管理员直观地了解分布情况。

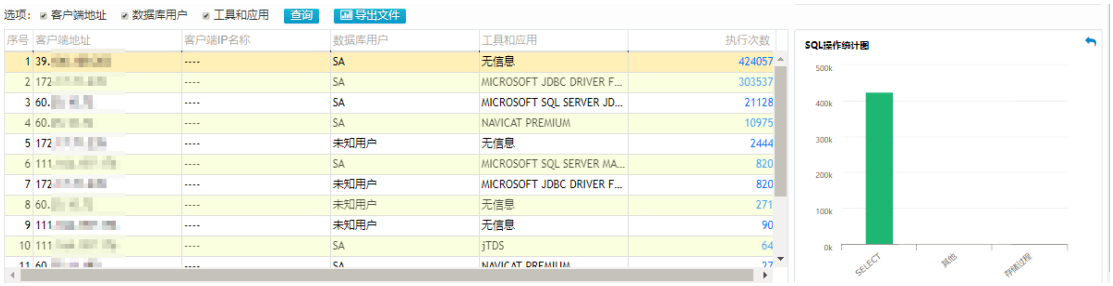
例如，在客户端地址分类的基础上，勾选数据库用户、工具和应用分类，单击**查询**，如图 *13-66: 查看某操作类型IP统计图*所示。

图 13-66: 查看某操作类型IP统计图



- 单击选择某条统计结果，右侧的统计图将以柱形图的形式统计该语句来源的SQL操作类型分布，如图 *13-67: 查看某语句来源SQL操作统计图*所示。

图 13-67: 查看某语句来源SQL操作统计图



- 单击**导出文件**，可将当前语句来源统计结果导出到本地。

13.3.2.3.2 检索SQL语句

背景信息

在**语句检索**页面，安全管理员可以以时间为语句检索条件检索本系统审计的SQL语句。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**语句** > **语句检索**页面，选择查询时间范围。
4. 单击**展开检索条件**，设置检索条件，单击**检索**。

   说明：

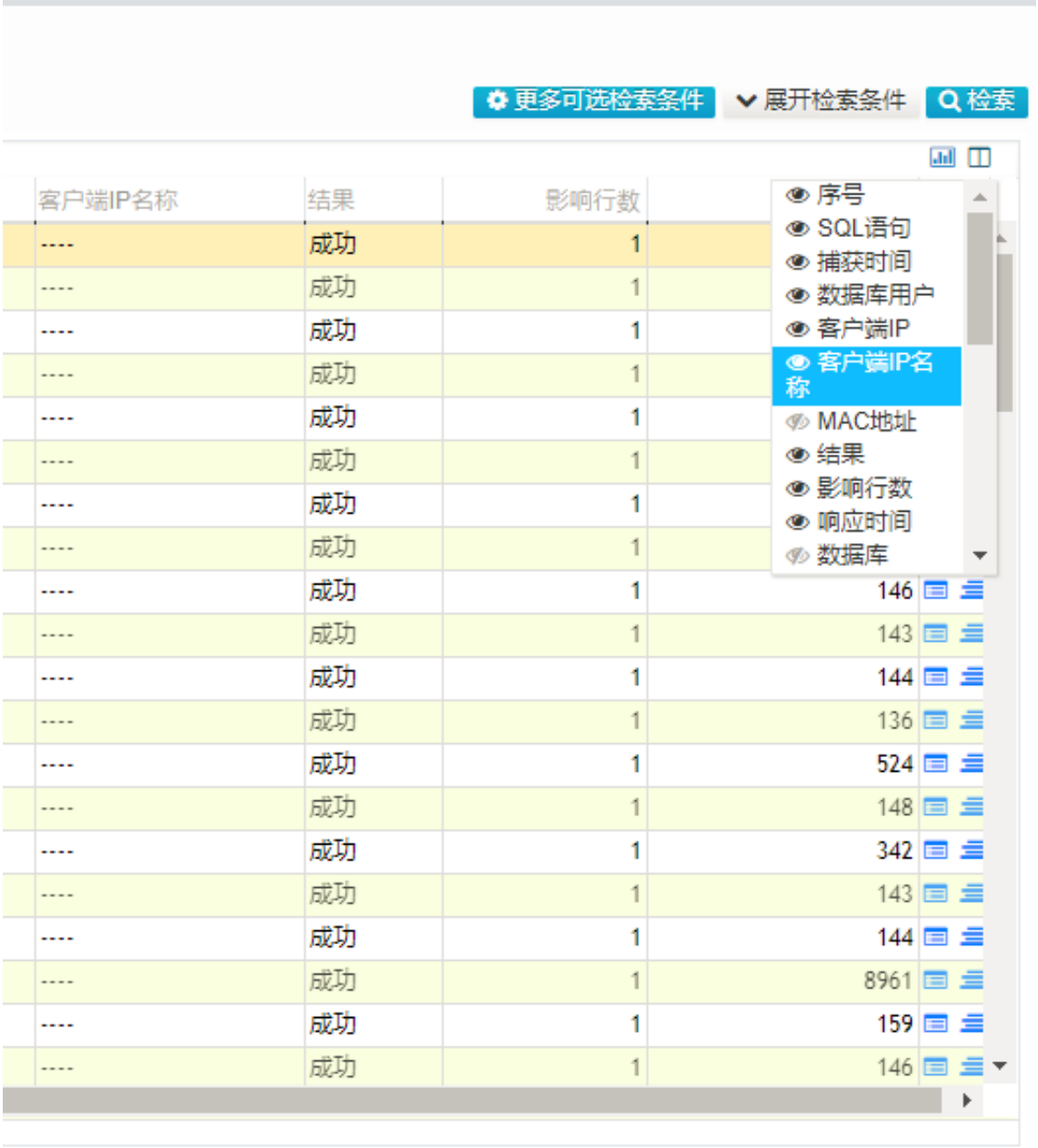
   单击**更多可选检索条件**，在**检索条件设置**对话框中，可添加更多检索条件。

5. 查看符合所设置的检索条件的语句。

   语句列表以网格式报表的形式进行SQL语句检索分析结果。SQL语句分析项包括SQL语句、捕获时间、数据库用户、客户端IP、执行结果、影响行数等信息。

   - 通过单击列表右上角的列设置按钮，可以选择列表项展示内容，如图 *13-68: 列表项显示设置*所示。

图 13-68: 列表项显示设置



- 单击导出报表按钮，选择**csv导出**，可将当前语句列表导出到本地。

6. 定位到某条语句，进一步查看该语句的详细信息。

- 单击列表下方的**展开语句信息**，可概要地查看该SQL语句的相关信息，包括会话信息、客户端信息、服务器信息、SQL信息等。
- 单击语句详情按钮，在语句详情页面查看该SQL语句的相关信息，包括访问来源、应用身份、SQL语句、受影响对象等，如图 *13-69:* 查看语句详情所示。

图 13-69: 查看语句详情

- 单击会话详情按钮，在会话详情列表中查看SQL语句所在通讯会话的会话信息以及此段会话中审计到的所有SQL语句概况，如图 *13-70: 查看会话详情*所示。

图 13-70: 查看会话详情

说明：

会话详情列表支持模糊查询审计到的SQL语句，并支持将会话详情列表导出到本地。

13.3.2.3.3 检索语句模板

背景信息

在**模板检索**页面可以对SQL语句模板进行查询。本系统采用语句模板的方式将SQL语句进行归纳整理，通过简化的SQL语句结构，对同一类SQL语句进行记录。安全管理员通过模板检索功能，可以快速定位高危SQL语句信息。

操作步骤

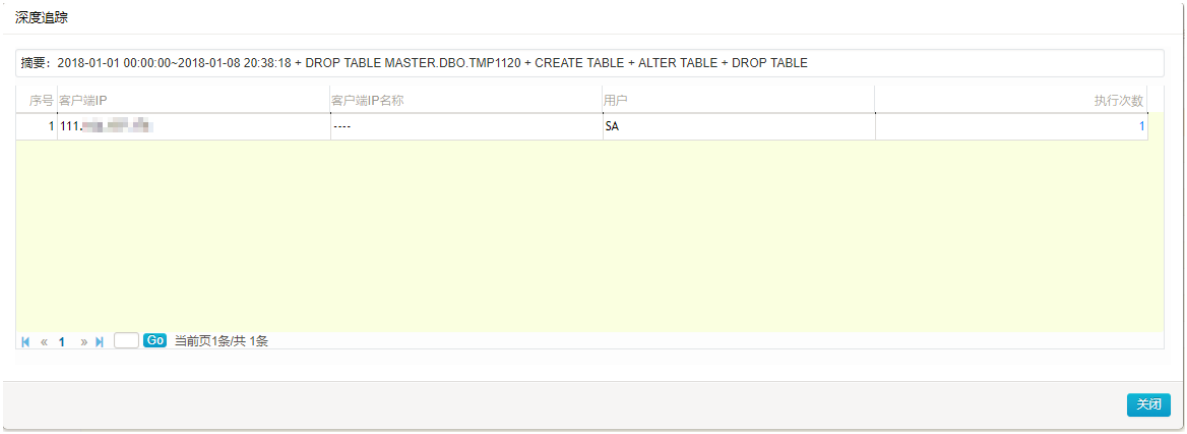
1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。

2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**语句** > **模板检索**页面，选择查询时间范围，单击**查询**。

> **说明**：
> **模板检索**页面支持客户端IP、数据库用户、工具和应用、MAC地址、模板类型、Sql语句类型、对象信息等查询条件。

4. 查看语句模板列表，包括模板语句、语句最后执行时间、执行次数等信息。
5. 选择列表中的语句模板，单击列表右侧的深度追踪按钮，可进一步查看该语句模板的信息，如图*13-71: 深度追踪信息*所示。

图 13-71: 深度追踪信息



6. 在语句模板列表，选择语句模板记录，在类型设置栏单击按钮可直接为该语句模板配置审计规则。
   - 单击操作栏中的设置为信任语句按钮，即可将该模板语句设为信任语句，系统对该类语句不再作风险记录。
   - 单击操作栏中的设置为敏感语句按钮，即可将该模板语句设为敏感语句，系统将针对该类语句作为敏感风险进行告警。
   - 单击操作栏中的设置为不审计语句按钮，即可将该模板语句设为不审计语句，系统将不再审计该类语句。

   单击语句模板列表上方相应的全部设置处理按钮，可为当前列表中的所有模板语句设置审计规则。

13.3.2.3.4 查看执行失败的SQL语句

背景信息

在**失败SQL**页面可以查看选定时间内所有执行失败的语句。针对失败SQL语句进行分析，帮助安全管理员分析数据库可能存在的风险途径。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**语句** > **失败SQL**页面，选择查询时间范围，单击**查询**。
4. 查看所设置时间范围内的执行失败的SQL语句列表。
   - 单击列表右上角的列设置按钮，可以选择列表项展示内容，如图 *13-72: 失败SQL列表展示列设置*所示。

     图 13-72: 失败SQL列表展示列设置

   - 选择失败SQL记录，单击会话标识，打开会话详情页面，查看该会话所执行的所有SQL语句，如图 *13-73: 查看会话详情*所示。

图 13-73: 查看会话详情

- 选择失败SQL记录，单击SQL语句，打开语句详情页面，查看该语句执行的详细情况，如图*13-74:* 查看语句详情所示。

图 13-74: 查看语句详情

- 单击列表右上角的导出报表按钮，选择**csv导出**，可将当前列表中的失败SQL语句信息导出。

13.3.2.3.5 查看TopSQL语句

背景信息

TopSQL页面，支持从平均耗时、耗时总量、执行次数维度针对数据库执行的语句信息进行查询排序，由大到小展示系统审计到的SQL语句。

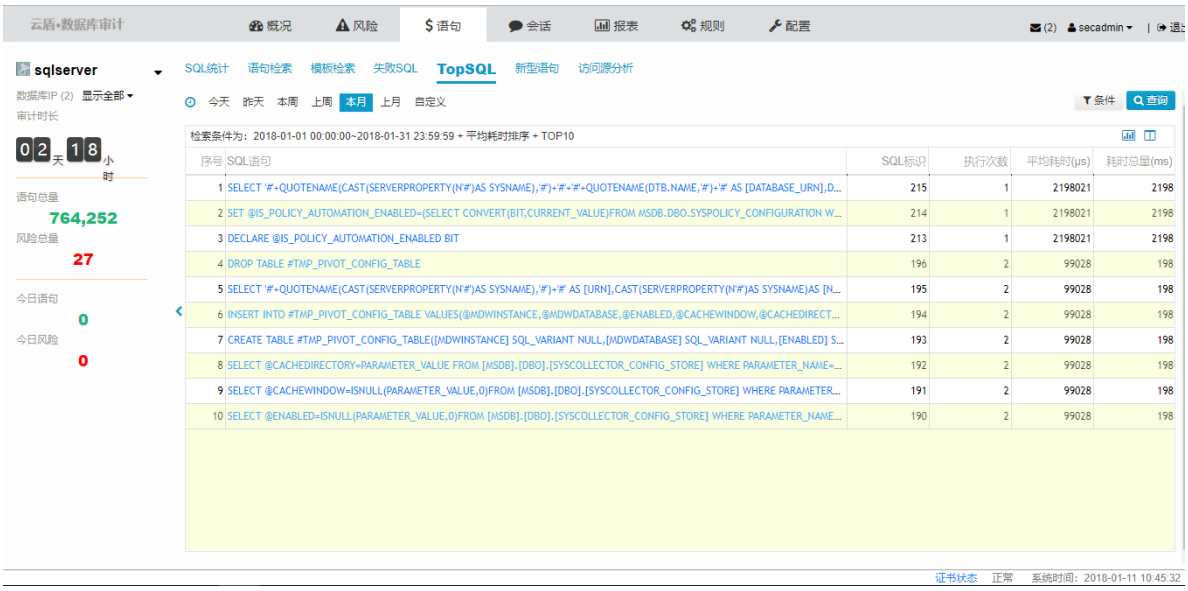
操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**语句** > **TopSQL**页面，选择查询时间范围，单击**查询**。

> **说明**：
>
> **TopSQL**页面支持以下查询条件：
>
> - **排序方式**：平均耗时、耗时总量、执行次数
> - **Top统计数**：10、50、100
> - **分析内容**：每分钟耗时大于**us，并且执行次数多于**次

4. 查看Top SQL语句统计表，如*图 13-75: 查看Top SQL语句统计情况*所示。

图 13-75: 查看Top SQL语句统计情况



- 单击列表右上角的列设置按钮，可以选择列表项展示内容。
- 单击列表右上角的导出报表按钮，选择**csv导出**，可将当前列表中的Top SQL语句导出。

13.3.2.3.6 查看新型语句

背景信息

新型语句页面统计汇总了该数据库某一时间周期内审计到的新的语句模板，安全管理员可以查询系统审计到的新型语句的详细信息，并为新型语句指定审计规则。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**语句** > **新型语句**页面，选择查询时间范围，单击**查询**。
4. 查看系统审计到的新型语句，如图 *13-76: 查看新型语句*所示。

图 13-76: 查看新型语句

> **说明**：
> 在列表中单击语句，可查看该语句的详情。

5. 在新型语句列表中，选择语句记录，在类型设置栏单击按钮可直接为该语句配置审计规则。
   - 单击操作栏中的设置为信任语句按钮，即可将该语句设为信任语句，系统对该类语句不再作风险记录。
   - 单击操作栏中的设置为敏感语句按钮，即可将该语句设为敏感语句，系统将针对该类语句作为敏感风险进行告警。

- 单击操作栏中的设置为不审计语句按钮，即可将该语句设为不审计语句，系统将不再审计该类语句。

单击新型语句列表上方相应的全部设置处理按钮，可为当前列表中的所有语句设置审计规则。

13.3.2.3.7 分析访问源

背景信息

访问源分析页面主要用于统计所访问数据库地址、数据库用户、客户端地址、工具和应用等信息。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**语句** > **访问源分析**页面，选择查询时间范围，查看访问源分析结果，如图 *13-77: 查看访问源分析结果*所示。

> **说明**：
> 勾选数据库地址、数据库用户、客户端地址、工具和应用选项可显示相应维度的分析结果，支持多维度分析。

图 13-77: 查看访问源分析结果

- **访问源统计表**：根据所选择的分析维度，展示在查询时间范围内每个访问源的执行次数。

- **访问源统计图**：通过饼图的方式直观地展示各访问源的占比情况。

13.3.2.4 会话

会话分析是对数据库的所有会话（Session）行为进行分类统计、分析和追踪，包括会话统计、会话检索、失败登录、活跃会话、应用会话五个功能模块。通过会话分析功能，基于数据库通讯会话进行线索分析，可以快速定位风险，提高数据库风险分析的效能。

13.3.2.4.1 查看会话统计

背景信息

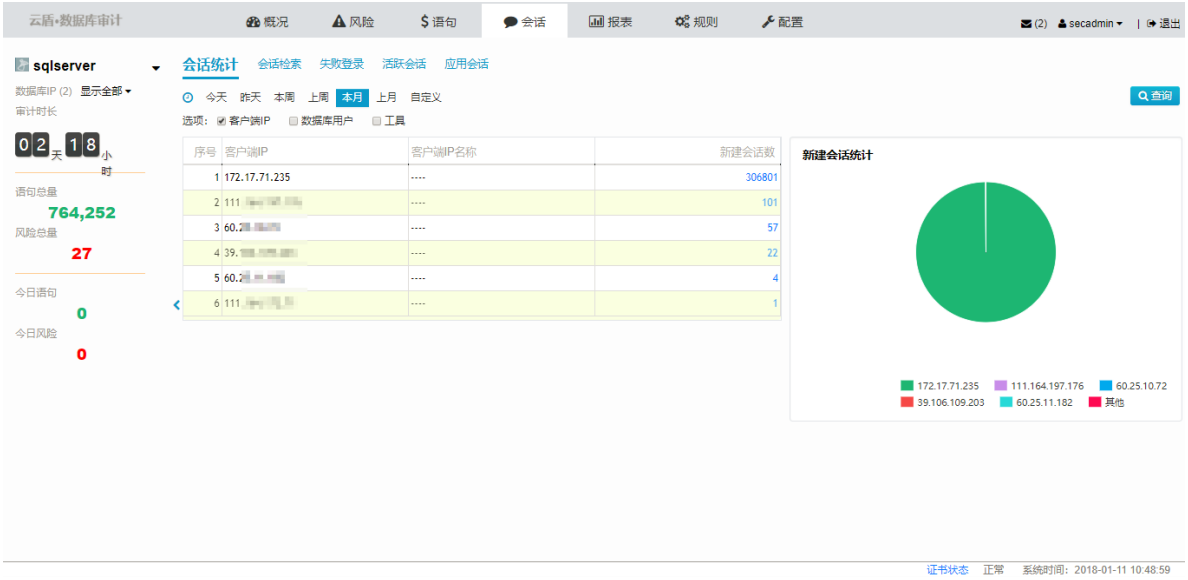
会话统计页面对被审计数据库进行整体性的会话统计、分析。基于时间范围，根据客户端IP、数据库用户、工具等维度统计新建会话数量信息。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**会话** > **会话统计**页面，选择查询时间范围，单击**查询**，查看会话统计情况，如图 *13-78: 查看会话统计结果*所示。

> **说明**：
> 勾选客户端IP、数据库用户、客户端地址、工具选项可显示相应维度的会话统计结果，支持多维度统计。

图 13-78: 查看会话统计结果



- **新建会话统计表**

  根据所选择的维度，展示在查询时间范围内各个维度的新建会话数量。

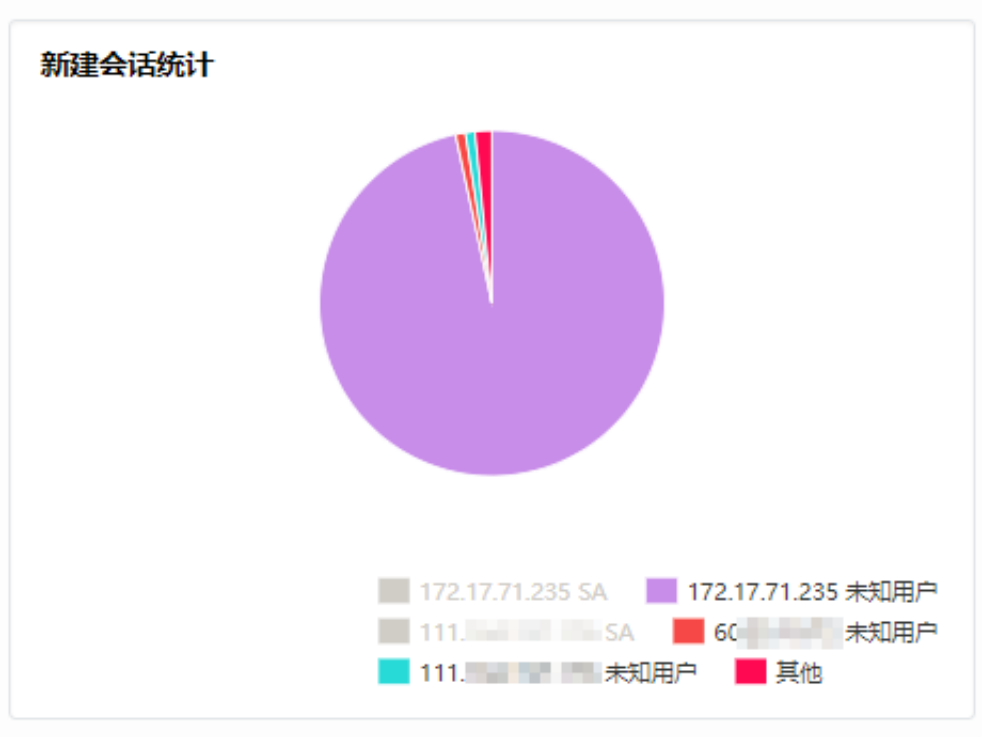
  > **说明**：
  > 单击新建会话数，打开**会话详情**页面，查看详细信息。

- **新建会话统计图**

  以饼状图的形式直观展现不同客户端IP、数据库用户、工具在新建会话中的占比情况。

  > **说明**：
  > 新建会话统计图，支持动态展现、图形隐藏等功能，单击某个统计维度可在统计图中隐藏该维度的信息，如图 *13-79:* 新建会话统计图所示。

图 13-79: 新建会话统计图



13.3.2.4.2 检索会话信息

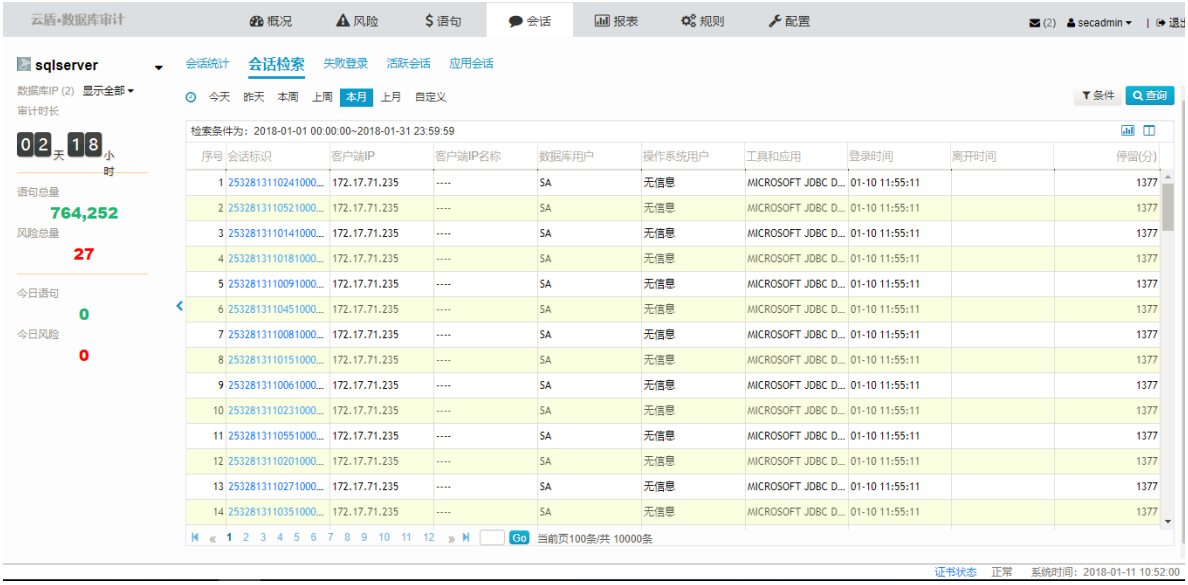
背景信息

在**会话检索**页面，安全管理员通过可选条件可以分析会话信息。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**会话** > **会话检索**页面，选择查询时间范围，单击**查询**，检索会话信息，如图 *13-80: 会话检索页面*所示。

图 13-80: 会话检索页面



说明：

会话列表中的停留（分）指的是该会话的会话时长。

- 单击会话标识，打开会话详情页面，查看该会话的详细信息。
- 单击列表右上角的列设置按钮，可以选择列表项展示内容。
- 单击列表右上角的导出报表按钮，选择**csv导出**，可将当前列表中的会话记录导出。

13.3.2.4.3 查看登录失败会话

背景信息

失败登录页面记录登录失败的会话信息，以网格式报表展现会话的相关信息，并统计失败总数。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**会话** > **失败登录**页面，选择查询时间范围，单击**查询**，查看登录失败的会话信息，如图 *13-81: 失败登录页面*所示。

图 13-81: 失败登录页面

- 单击失败总数，打开**失败登录清单**页面，查看详细的失败登录记录，如图 *13-82: 失败登录清单*所示。

图 13-82: 失败登录清单

- 单击列表右上角的列设置按钮，可以选择列表项展示内容。
- 单击列表右上角的导出报表按钮，选择**csv导出**，可将当前列表中的失败登录会话记录导出。

13.3.2.4.4 查看活跃会话

背景信息

活跃会话页面对某一时间段内较为活跃会话进行统计描述，以活跃会话趋势图、活跃会话统计表、活跃会话统计图的形式进行展示。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**会话** > **活跃会话**页面，选择查询时间范围，单击**查询**，查看所设定的时间范围内的活跃会话情况，如图 *13-83: 活跃会话页面*所示。

图 13-83: 活跃会话页面

13.3.2.4.5 查看应用会话

背景信息

应用会话页面主要用于统计三层应用关联的会话审计信息。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**会话** > **应用会话**页面，选择查询时间范围，单击**查询**，查看通过系统审计到的由应用创建的会话情况，如图 *13-84: 应用会话页面*所示。

说明：

单击**条件**，可设置应用相关的过滤条件。

图 13-84: 应用会话页面

- 单击列表右上角的列设置按钮，可以选择列表项展示内容。
- 单击列表右上角的导出报表按钮，选择**csv导出**，可将当前列表中的应用会话记录导出。

13.3.2.5 报表（单库）

报表功能是审计日志大数据系统化分析的具体表现。利用审计报告、定时推送的报表功能将审计日志和风险分析体系中所要求的数据库安全趋势以更加直观的形式进行展现，帮助安全管理员更加便捷、深入地剖析数据库运行风险。

本章节主要介绍云盾数据库审计系统的数据库单库报表，即针对单个数据库的统计报表。

13.3.2.5.1 查看报表（单库）

操作步骤

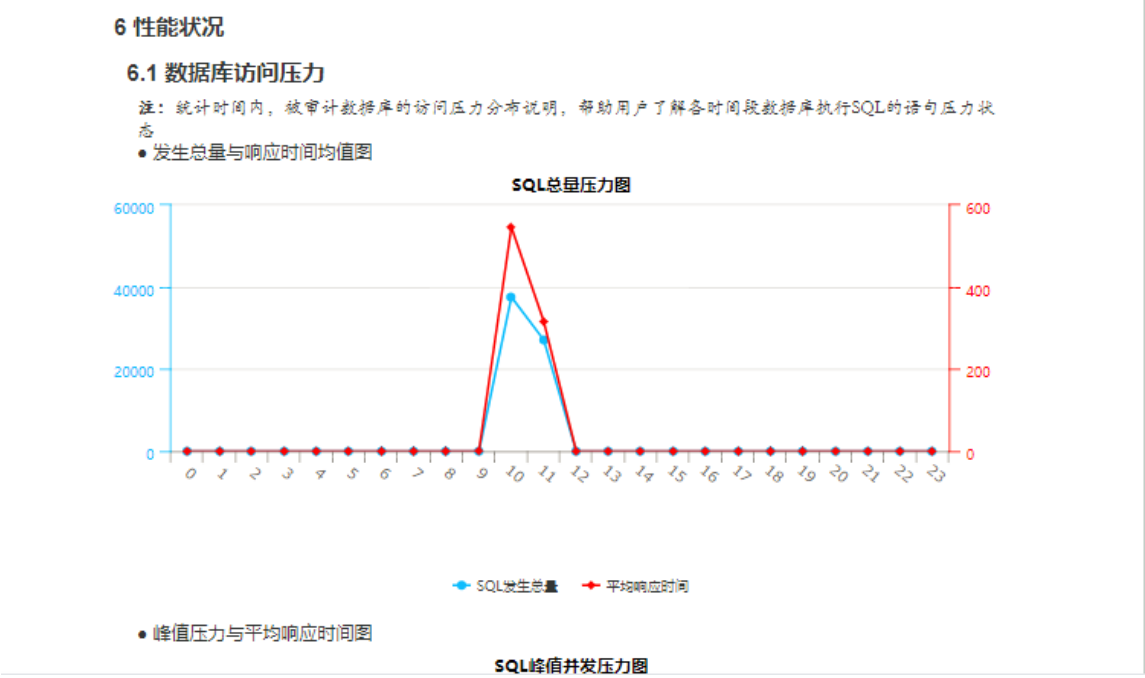
1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。

3. 定位到**报表**页面，选择报表类型，选择时间范围，单击**预览**，查看该数据库的单库报表，如图 *13-85:* 报表页面所示。

图 13-85: 报表页面

- **报表类型**：日报、周报和月报，萨班斯报告、PCI报告、客户端分析报告、风险登录分析报告等。
- **报表内容**：包括总体访问情况、风险分布、会话分布、语句分布、性能状况等。
- **统计图展现形式**：包括饼状图、柱形图、条形图、双轴折线图等。
- **报表样例**：例如，日报中的数据库访问压力统计报告，如图 *13-86:* 数据库访问压力统计报告所示。

图 13-86: 数据库访问压力统计报告



4. 导出报表或为当前报表设置定时推送。

   - 单击**导出**，选择导出格式，单击**确定**，可导出当前报表。

     说明：

     报表支持以Word、PDF、HTML格式导出。

   - 单击**加入定时推送任务**，选择推送任务，填写报表名称，选择报表格式，单击**确定**，可为当前报表设置定时推送。

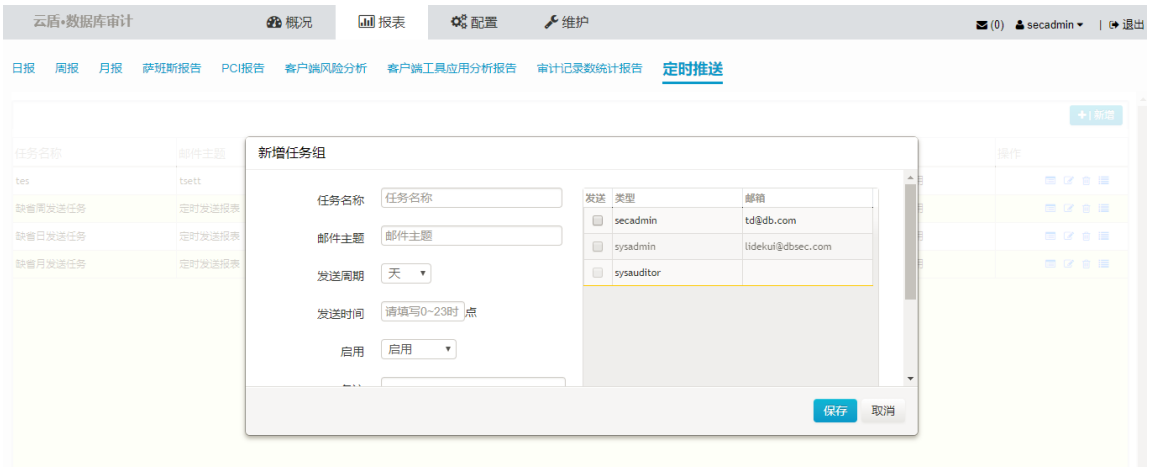
13.3.2.5.2 管理定时推送任务（单库）

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**报表**页面，单击**定时推送**，管理定时推送任务。

   - 单击**新增**，在**新增任务组**对话框中，输入任务名称、邮件主题，设置发送周期、发送时间，勾选需要发送的用户，单击**保存**，可新增定时推送任务组，如图 *13-87: 新增定时推送任务组*所示。

图 13-87: 新增定时推送任务组



- 选择任务列表中的任务，单击右侧操作栏中的编辑按钮，可修改该任务组的相关参数，并可启用或禁用该任务组。
- 选择任务列表中的任务，单击右侧操作栏中的删除按钮，单击**确定**，可删除该任务组。
- 选择任务列表中的任务，单击右侧操作栏中的任务列表按钮，可查看该任务组中的报表定时推送任务，并且通过单击编辑和删除按钮，可以修改该任务的报告格式及任务名称，或删除该推送任务。
- 选择任务列表中的任务，单击右侧操作栏中的发送历史按钮，可查看该任务组已发送报表的历史记录。

13.3.2.6 规则

审计规则是云盾数据库审计系统的灵魂所在，系统正是通过所设置的审计规则完成对数据库的合规审计。本系统的审计规则设置针对于指定的单个数据库，符合一个数据库一套审计规则的原则。

本系统提供优先级视图、分类视图两种规则划分方式：

- 优先级视图包括风险忽略、高风险、中风险、低风险等规则类型，通过多个等级的规则实现数据库的合规审计和告警功能。
- 分类视图包括风险操作、SQL注入、语句管理等分类，根据风险攻击来源定义审计规则。

表 13-3: 管理规则

视图	级别/分类	包括规则类型
优先级视图	风险忽略	• 优先级视图下管理信任语句 • 优先级视图下管理信任规则

视图	级别/分类	包括规则类型
	高风险	• 优先级视图下管理敏感语句 • 优先级视图下管理*SQL*注入规则 • 优先级视图下管理风险操作规则
	中风险	• 优先级视图下管理*SQL*注入规则 • 优先级视图下管理风险操作规则
	低风险	• 优先级视图下管理*SQL*注入规则 • 优先级视图下管理风险操作规则
分类视图	风险操作	分类视图下管理风险操作规则
	SQL注入	分类视图下管理*SQL*注入规则
	语句管理	分类视图下语句管理

13.3.2.6.1 优先级视图下管理信任语句

对系统审计到的SQL语句进行定义，对于被设置为信任语句的SQL语句和操作，系统将予以放行，不进行风险审计处理。在信任语句列表中，安全管理员可以为语句重新定义审计规则。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**规则**页面，单击右上角**优先级视图**。
4. 单击**信任语句**，界面如图 *13-88:* 管理信任语句所示。

图 13-88: 管理信任语句

5. 在信任语句列表中，选择相应语句。

> **说明**：
> 在信任语句列表上方，设置查询条件，单击**查询**，可查询特定信任语句。

6. 单击**类型设置**栏中按钮，设置信任语句、敏感语句、不审计语句。
7. 单击**保存生效**后，相应设置即生效。

13.3.2.6.2 优先级视图下管理信任规则

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**规则**页面，单击右上角**优先级视图**。
4. 选择**信任规则**，单击新建规则按钮 ，进入**新建信任规则**页面，如图 13-89: 新建信任规则所示。

图 13-89: 新建信任规则

a) 在**名称**中填写规则名称。

b) 在**IP地址**、**数据库用户**、**数据库对象**和**操作**中填入规则信息。

根据信任规则，可设置对于指定客户端IP和数据库用户可以基于指定数据库对象（数据表、视图等）执行指定的操作，系统不做风险审计和告警。

c) （可选）勾选**有WHRER条件数据操作**选项，设定信任规则只针对有where语句的SQL操作有效。

d) （可选）单击高级设置的展开按钮，为信任规则设置具体的时间范畴，如*图 13-90: 设置具体时间范畴*所示。

图 13-90: 设置具体时间范畴

e) （可选）对于已被定义为信任语句的SQL语句，可以设置是否不审计该语句，如*图 13-91: 设置是否不审计该语句*所示。

图 13-91: 设置是否不审计该语句

f) 单击右上角的**保存**，保存信任规则。

5. 管理已存在信任规则。

表 13-4: 管理信任规则

操作	说明
复制	单击复制按钮，可将该规则的相关设置复制至**新建信任规则**页面，便于安全管理员添加相似的规则。
移动	信任规则之间存在生效优先级，通过上移或下移按钮可以调整信任规则的排序，顺序靠前的规则优先生效。
启用切换	单击启用或禁用按钮，可以设置是否启用该规则。
编辑	单击编辑按钮，可以修改该规则设置。
删除	单击删除按钮，可以删除该规则。

13.3.2.6.3 优先级视图下管理敏感语句

对系统审计到的SQL语句进行定义，对于被设置为敏感语句的SQL语句和操作，系统将根据所设置的审计规则记录风险并触发告警。在敏感语句列表中，安全管理员可以为语句重新定义审计规则。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**规则**页面，单击右上角**优先级视图**。
4. 单击**敏感语句**，进入管理敏感语句页面。
5. 在敏感语句列表中，选择相应语句。

   说明：
   在敏感语句列表上方，设置查询条件，单击**查询**，可查询特定敏感语句。

6. 单击**类型设置**栏中按钮，设置信任语句、敏感语句、不审计语句。
7. 单击**保存生效**后，相应设置即生效。

13.3.2.6.4 优先级视图下管理SQL注入规则

以列表形式展现系统当前已有SQL注入规则。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**规则**页面，单击右上角**优先级视图**。
4. 单击**SQL注入**，进入管理SQL注入规则页面。

   高风险、**中风险**和**低风险**中都包含**SQL注入**，请根据具体需求选择管理。

5. 单击新建规则按钮 ，定义新的SQL注入规则。

   可设置对于包含指定SQL命令特征的指定SQL操作，判定为风险操作并进行告警，如*图 13-92: 新建SQL注入规则*所示。

图 13-92: 新建SQL注入规则

6. 管理已存在SQL注入规则。

表 13-5: 管理SQL注入规则

操作	说明
复制	单击复制按钮，可将该规则的相关设置复制至**新建SQL注入规则**页面，便于安全管理员添加相似的规则。
启用切换	单击启用或禁用按钮，可以设置是否启用该规则。
编辑	单击编辑按钮，可以修改该规则设置。
删除	单击删除按钮，可以删除该规则。

13.3.2.6.5 优先级视图下管理风险操作规则

以列表形式展现系统当前已有风险操作规则。

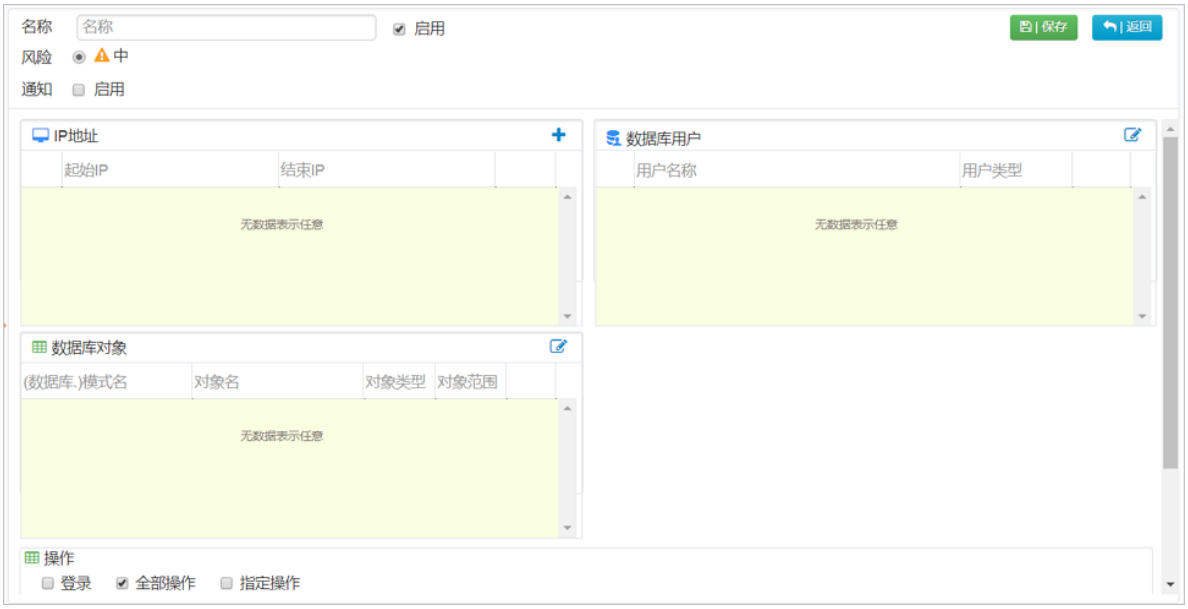
操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**规则**页面，单击右上角**优先级视图**。
4. 单击**风险操作**，进入管理风险操作规则页面。

高风险、**中风险**和**低风险**中都包含**风险操作**，请根据具体需求选择管理。

5. 单击新建规则按钮 ，定义新的风险操作规则，如图 *13-93:* 新建风险操作规则所示。

图 13-93: 新建风险操作规则



a) 在**名称**中填写规则名称。

b) 在**IP地址**、**数据库用户**、**数据库对象**和**操作**中填入规则信息。

根据风险操作规则，可设置对于指定客户端IP和数据库用户可以基于指定数据库对象（数据表、视图等）执行指定的操作，进行风险审计和告警。

c) （可选）勾选**有WHRER条件数据操作**选项，设定风险操作规则只针对有where语句的SQL操作有效。

d) （可选）单击高级设置的展开按钮，为风险操作规则设置具体的时间范畴，如图 *13-94:* 设置具体时间范畴所示。

图 13-94: 设置具体时间范畴

e) 单击右上角的**保存**，保存风险操作规则。

6. 管理已存在的风险操作规则。

表 13-6: 管理风险操作规则

操作	说明
复制	单击复制按钮，可将该规则的相关设置复制至**新建风险操作规则**页面，便于安全管理员添加相似的规则。
移动	风险操作规则之间存在生效优先级，通过上移或下移按钮可以调整规则的排序，顺序靠前的规则优先生效。
启用切换	单击启用或禁用按钮，可以设置是否启用该规则。
编辑	单击编辑按钮，可以修改该规则设置。
删除	单击删除按钮，可以删除该规则。

13.3.2.6.6 分类视图下管理风险操作规则

通过风险操作页面可以针对高、中、低风险、信任等不同风险级别，进行分类查询和审计规则配置。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。

3. 定位到**规则**页面，单击右上角**分类视图**。
4. 单击**风险操作**，进入管理风险操作规则页面。
5. 单击新建规则按钮 ，定义新的风险操作规则。
   a) 在**名称**中填写规则名称。
   b) 在**风险**中选择风险级别。
   c) 在**IP地址**、**数据库用户**、**数据库对象**和**操作**中填入规则信息。

      根据风险操作规则及所选择的风险级别，可设置对于指定客户端IP和数据库用户可以基于指定数据库对象（数据表、视图等）执行指定的操作，进行风险审计。
   d) （可选）勾选**有WHRER条件数据操作**选项，设定风险操作规则只针对有where语句的SQL操作有效。
   e) （可选）单击高级设置的展开按钮，为风险操作规则设置具体的时间范畴。
   f) 单击右上角的**保存**，保存风险操作规则。
6. 管理已存在的风险操作规则。

表 13-7: 管理风险操作规则

操作	说明
复制	单击复制按钮，可将该规则的相关设置复制至**新建风险操作规则**页面，便于安全管理员添加相似的规则。
移动	风险操作规则之间存在生效优先级，通过上移或下移按钮可以调整规则的排序，顺序靠前的规则优先生效。
启用切换	单击启用或禁用按钮，可以设置是否启用该规则。
编辑	单击编辑按钮，可以修改该规则设置。
删除	单击删除按钮，可以删除该规则。

13.3.2.6.7 分类视图下管理SQL注入规则

通过对SQL语句进行特征描述，定义需要阻止的SQL注入语句或危险SQL语句。

背景信息

系统内建了部分SQL注入规则，安全管理员可以对内建规则的风险级别和是否启用进行设置，但无法修改内建规则的内容。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**规则**页面，单击右上角**分类视图**。
4. 单击**SQL注入**，进入管理SQL注入规则页面。
5. 单击新建规则按钮 ，定义新的SQL注入规则。

   可设置对于包含指定SQL命令特征的指定SQL操作，判定为风险操作并进行告警。
6. 管理已存在SQL注入规则。

   表 13-8: 管理SQL注入规则

操作	说明
复制	单击复制按钮，可将该规则的相关设置复制至**新建SQL注入规则**页面，便于安全管理员添加相似的规则。
启用切换	单击启用或禁用按钮，可以设置是否启用该规则。
编辑	单击编辑按钮，可以修改该规则设置。
删除	单击删除按钮，可以删除该规则。

13.3.2.6.8 分类视图下语句管理

安全管理员可以为语句重新定义审计规则。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**规则**页面，单击右上角**分类视图**。
4. 单击**语句管理**，进入管理SQL语句页面。
5. 在语句列表中，选择相应语句。通过**类型设置**栏中的按钮将所选择语句设为信任语句、敏感语句、不审计语句。
6. （可选）通过选择**敏感语句风险**可为敏感语句设定风险级别。

说明：

在敏感语句列表上方，设置查询条件，单击**查询**，可查询特定敏感语句。

7. 单击**保存生效**后，相应设置即生效。

13.3.2.7 配置（单库）

13.3.2.7.1 配置单库的规则告警通知

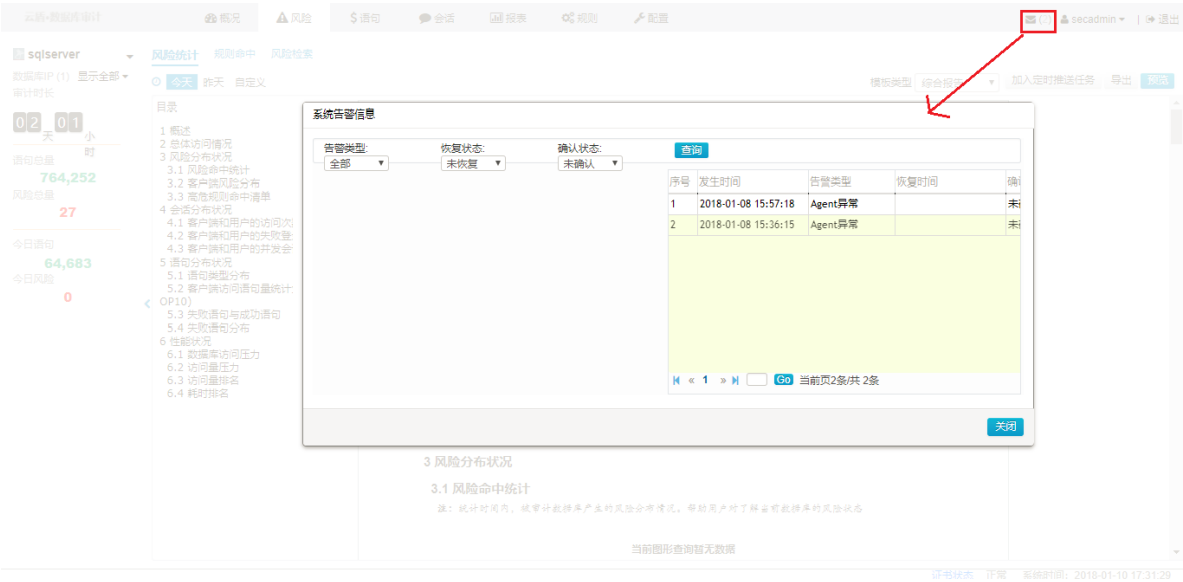
背景信息

规则告警信息支持通过邮件的方式进行通知，便于相关管理人员及时了解数据库风险异常。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**概况**页面，在数据库列表区域，选择已添加的数据库，单击**信息**，进入数据库详细信息页面。
3. 定位到**配置** > **规则告警通知**页面，如图 *13-95: 规则告警设置*所示。

图 13-95: 规则告警设置



4. 勾选需要通过邮件通知的管理人员。

> **说明**：
> 修改管理人员的邮件地址，需使用管理员账号登录后，单击右上角的账户名，在下拉菜单中选择**用户资料**，在**用户资料**对话框中即可进行修改。

5. 填写邮件标题，在文本框中输入邮件内容。

单击文本框上方的危险事件类型、服务器IP、服务器端口等参数，可将这些变量信息添加至邮件内容中。

6. 填写最短告警周期，即最短多少分钟内发送一次系统告警邮件通知，单击**确定**。

13.3.3 报表

数据库审计系统采用聚集式报表展现形式，将报表分为全局报表、数据库单库报表两种表现形式。

本章节主要介绍数据库审计系统的全局报表，关于数据库单库报表说明，参见报表#单库#。全局报表式以聚合报表的展现形式，分栏展现系统内所有数据库的审计状态报表。报表形式分为日报、周报、月报，以及萨班斯报告、PCI报告、客户端风险分析、客户端工具应用分析报告、审计记录数据统计报告等报表。同时，数据库审计系统提供定时推送功能，可将报表定时发送至指定人员的邮箱。

13.3.3.1 查看报表

操作步骤

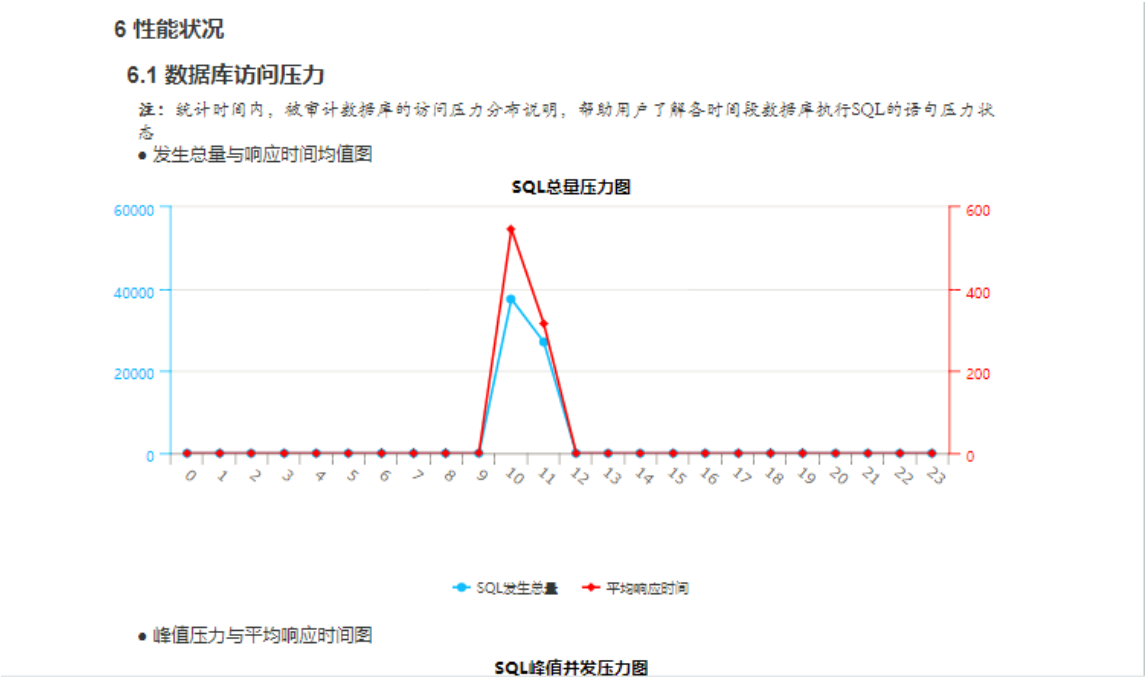
1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**报表**页面，选择报表类型，选择时间范围，单击**预览**，查看全局报表，如图 *13-96: 报表页面*所示。

图 13-96: 报表页面

- **报表类型**：日报、周报和月报，萨班斯报告、PCI报告、客户端风险分析、客户端工具应用分析报告、审计记录数据统计报告等。

- **报表内容**：包括多数据库综合分析、性能状态、会话分布、语句分布、风险分析等。
- **统计图展现形式**：包括饼状图、柱形图、条形图、双轴折线图等。
- **报表样例**：例如，日报中的数据库访问压力统计报告，如图 *13-97:* 数据库访问压力统计报告所示。

图 13-97: 数据库访问压力统计报告



3. 导出报表或为当前报表设置定时推送。
   - 单击**导出**，选择导出格式，单击**确定**，可导出当前报表。

     说明：
     报表支持以Word、PDF、HTML格式导出。
   - 单击**加入定时推送任务**，选择推送任务，填写报表名称，选择报表格式，单击**确定**，可为当前报表设置定时推送。

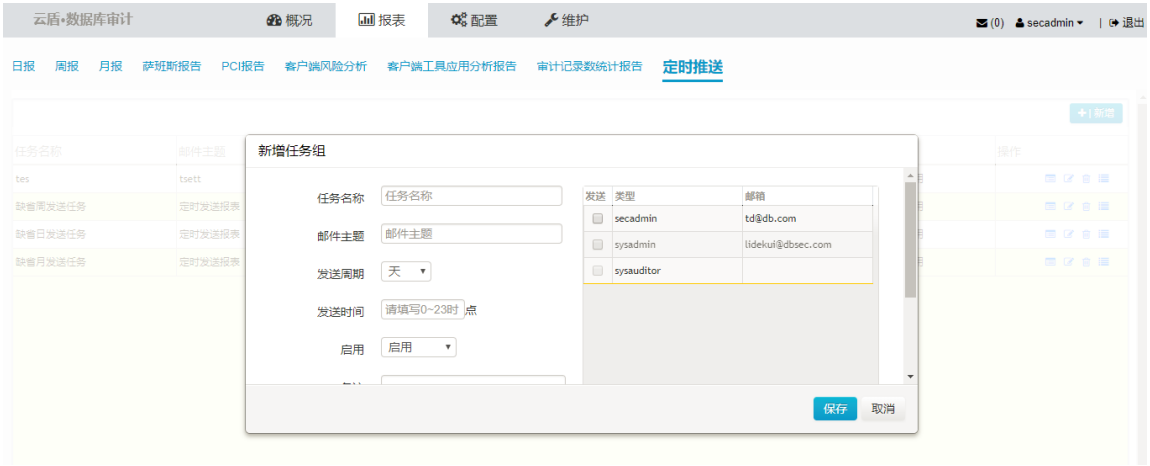
13.3.3.2 管理定时推送任务

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**报表**页面，单击**定时推送**，管理定时推送任务。

- 单击**新增**，在**新增任务组**对话框中，输入任务名称、邮件主题，设置发送周期、发送时间，勾选需要发送的用户，单击**保存**，可新增定时推送任务组，如图 *13-98: 新增定时推送任务组*所示。

图 13-98: 新增定时推送任务组



- 选择任务列表中的任务，单击右侧操作栏中的编辑按钮，可修改该任务组的相关参数，并可启用或禁用该任务组。
- 选择任务列表中的任务，单击右侧操作栏中的删除按钮，单击**确定**，可删除该任务组。
- 选择任务列表中的任务，单击右侧操作栏中的任务列表按钮，可查看该任务组中的报表定时推送任务，并且通过单击编辑和删除按钮，可以修改该任务的报告格式及任务名称，或删除该推送任务。
- 选择任务列表中的任务，单击右侧操作栏中的发送历史按钮，可查看该任务组已发送报表的历史记录。

13.3.4 系统告警信息

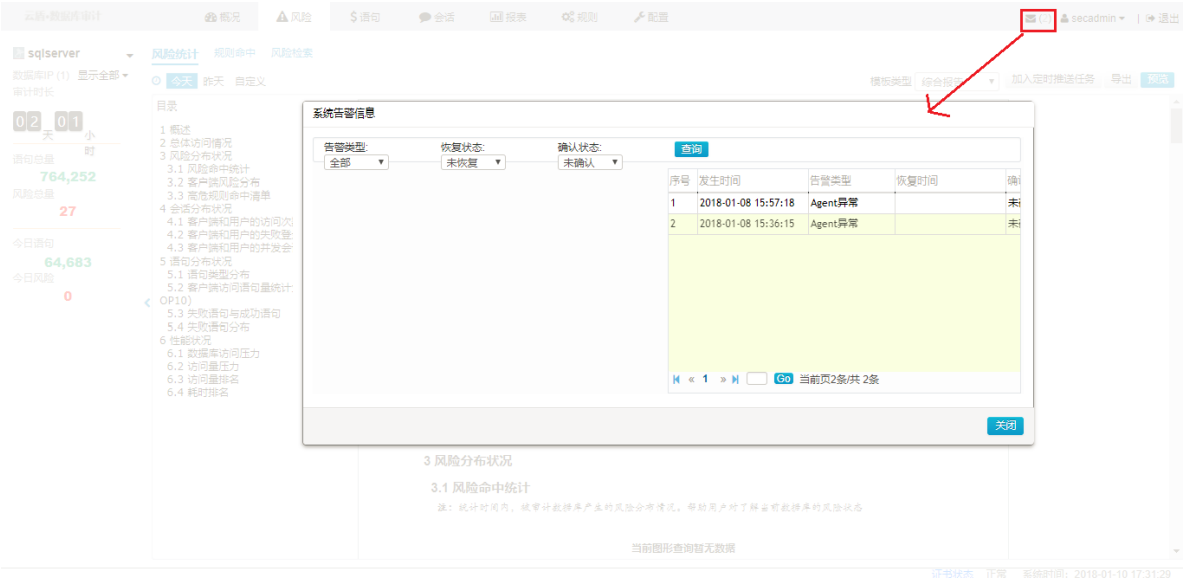
云盾数据库审计系统具备系统监控能力，支持通过系统内告警信息的方式提示安全管理员系统异常情况。

13.3.4.1 查看系统告警信息

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 单击页面右上角的系统告警按钮，打开**系统告警信息**对话框，如图 *13-99: 查看系统告警信息*所示。

图 13-99: 查看系统告警信息



3. 选择告警类型、恢复状态、确认状态，单击**查询**，可查看指定类型或状态的告警信息。

> **说明**：
> 在描述栏中可查看该告警信息的具体触发原因。

4. 检查并处理该系统异常后，单击操作栏中的确认按钮，该信息将不再告警。

13.3.4.2 配置系统告警

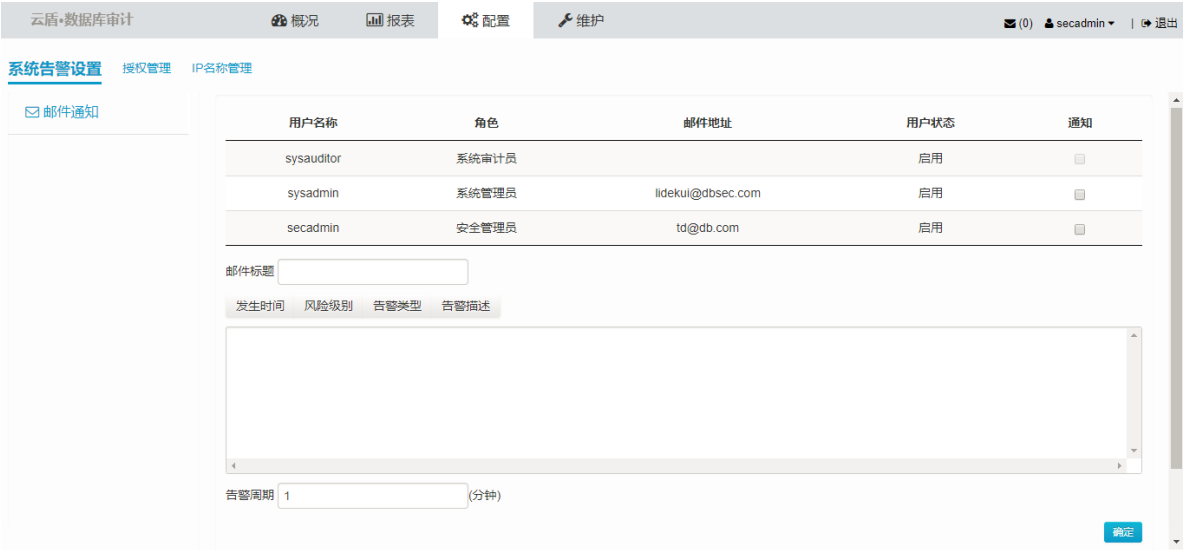
背景信息

系统告警信息也支持通过邮件方式进行通知，便于相关管理人员及时了解系统异常。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**配置**页面，单击**系统告警设置**，如图 *13-100: 系统告警设置*所示。

图 13-100: 系统告警设置



3. 勾选需要通过邮件通知的管理人员。

> **说明**：
> 修改管理人员的邮件地址，需使用管理员账号登录后，单击右上角的账户名，在下拉菜单中选择**用户资料**，在**用户资料**对话框中即可进行修改。

4. 填写邮件标题，在文本框中输入邮件内容。

> **说明**：
> 单击文本框上方的发生时间、风险级别、告警类型、告警描述，可将这些变量信息添加至邮件内容中。

5. 填写最短告警周期，即最短多少分钟内发送一次系统告警邮件通知，单击**确定**。

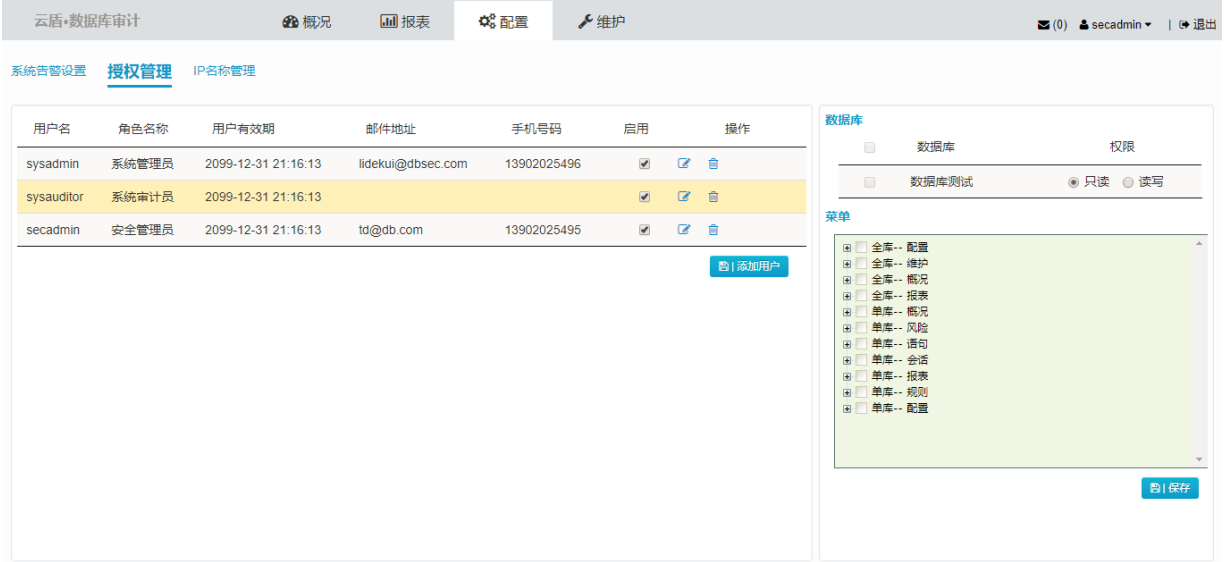
13.3.5 配置

配置页面主要用于云盾数据库审计系统的告警信息配置及授权管理配置，包含系统告警设置、授权管理、IP名称管理等。

13.3.5.1 授权管理

在授权管理页面，安全管理员可进行用户管理及功能授权，如图 *13-101:* 授权管理页面所示。

图 13-101: 授权管理页面



13.3.5.1.1 用户管理

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**配置**页面，单击**授权管理**，管理数据库审计系统用户，如图 *13-102: 用户管理*所示。

> **说明**：
> 默认的系统管理员、系统审计员、安全管理员无法修改或删除。

图 13-102: 用户管理

- 单击**添加用户**，在**添加用户**对话框中，设置用户信息（其中，用户名、密码、用户有效期为必填项），单击**保存**，即添加新用户。
- 在用户列表中，选择用户，勾选或取消启用，可设置是否启用该用户。
- 在用户列表中，选择用户，单击修改按钮，可修改该用户的信息。
- 在用户列表中，选择用户，单击删除按钮，单击**确定**，可删除该用户。

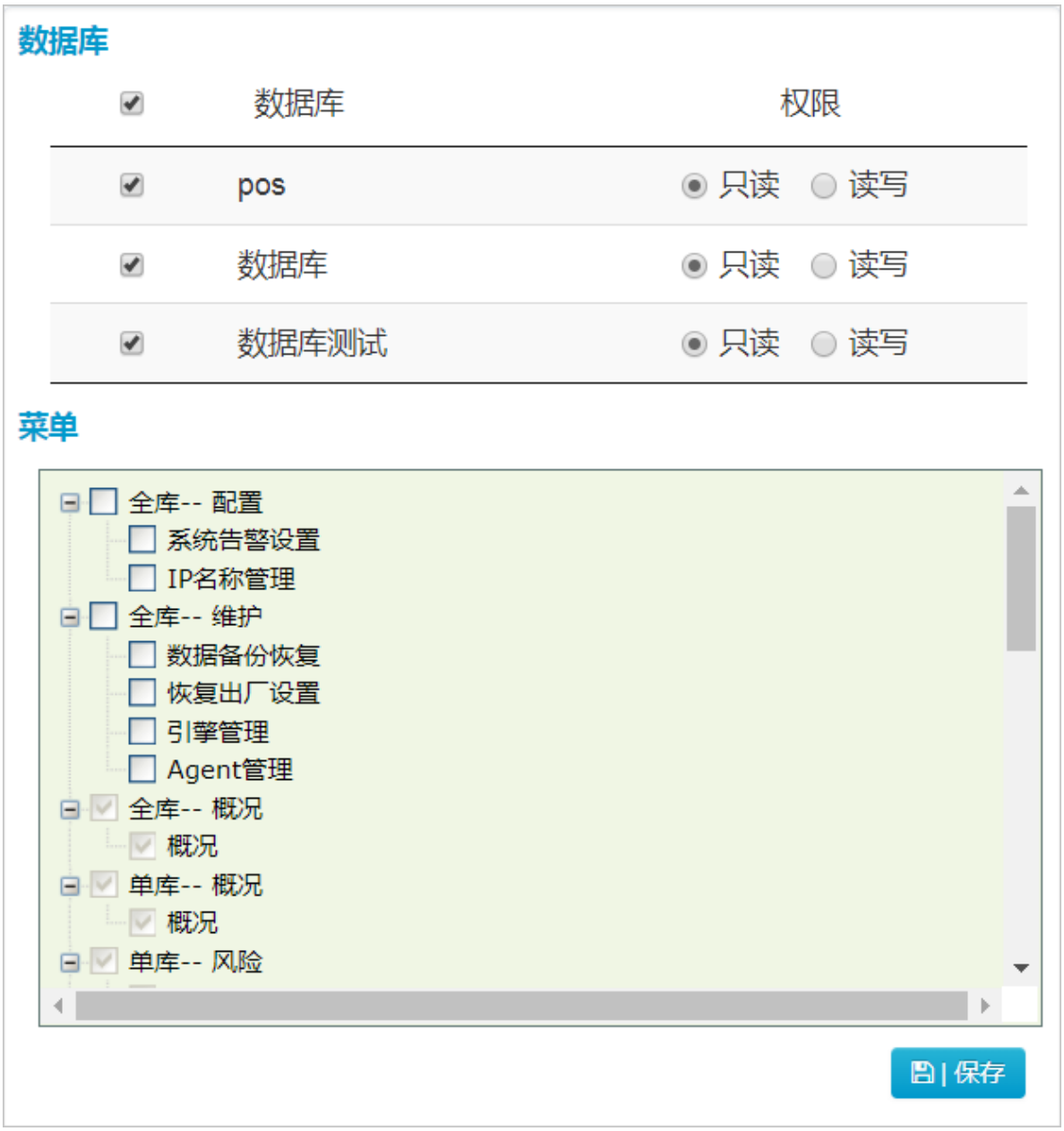
13.3.5.1.2 功能授权

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**配置**页面，单击**授权管理**，选择已启用的用户，为该用户进行授权，如图 *13-103:* 功能授权所示。

> **说明**：
> 默认的系统管理员、系统审计员、安全管理员的权限无法修改。

图 13-103: 功能授权



- 数据库权限：勾选需要授权给该用户的数据库，并选择**只读**或**读写**权限。
- 菜单权限：勾选需要授权给该用户的功能节点

3. 单击**保存**，单击**确定**。

13.3.5.2 IP名称管理

背景信息

IP名称管理主要用于实现IP业务化，将IP地址与具有业务含义的IP名称关联，便于云盾数据库审计系统的用户理解某些IP地址的业务含义。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**配置**页面，单击**IP名称管理**，如图 *13-104: IP名称管理*所示。

图 13-104: IP名称管理

- 单击**添加**，在**添加业务化IP**对话框中，输入IP地址或IP段，及对应的IP名称，单击**确定**，即可添加IP名称记录。
- 单击**导入**，选择格式规范的CSV文件，单击**确定**，可批量导入业务化IP信息。

> **说明**：
> 在**导入业务化数据**对话框中，单击**请先下载IP业务化文件模板**，可下载标准格式模板。

- 单击**导出**，可将当前IP业务化列表以CSV格式导出至本地。
- 在IP业务化列表上方，设置IP地址或IP段、IP名称、变更时间查询条件，单击**查询**，可查看相应的IP业务化记录。

13.3.6 维护

维护页面用于对审计系统本身业务安全与稳定性进行保障维护。数据库审计系统是以审计日志及日志存储文件为基础。因此，如何妥善存储、备份、整理审计日志是本系统确保安全的关键。

维护页面包含数据备份恢复、Agent管理、恢复出厂设置、引擎管理四大功能模块。

13.3.6.1 数据备份恢复

本系统基于审计日志的安全性和永久性考虑，进行常规的审计日志的备份操作。通过对审计日志进行定制的备份存储，减少系统存储压力。同时，通过便捷的日志恢复功能，随时对备份数据进行查询与恢复。

数据备份恢复页面分为上下两栏，包括备份机制和备份清单查询。

本系统支持自动备份与手动备份两种备份方式：

- **自动备份**：备份审计日志
- **手动备份**：备份系统配置数据

13.3.6.1.1 设置自动备份

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**维护**页面，单击**数据备份恢复**。
3. 在自动备份配置区域，设置开始备份时间、备份内容，选择是否将备份上传FTP服务器，如图*13-105: 设置自动备份*所示。

   图 13-105: 设置自动备份

   - **开始备份时间**：自动备份以天为单位，通过开始备份时间确定在哪一整点时间开始每天的自动备份。
   - **备份内容**：自动备份默认备份3天前的数据，即备份自当天起三天前的数据。例如，在12月17日，自动备份默认备份12月14日当天的审计日志数据。
   - **FTP设置**：启用后，系统根据分区空间自动向FTP服务器的指定路径上传审计日志。
4. 单击**保存**。

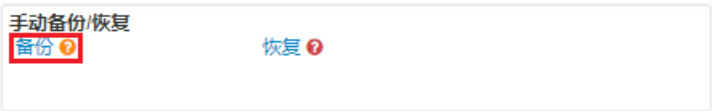
13.3.6.1.2 手动备份与恢复

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**维护**页面，单击**数据备份恢复**。

3. 在手动备份/恢复区域，单击**备份**，如图 *13-106: 手动备份*所示。

图 13-106: 手动备份



4. 单击**确定**，对当前系统配置数据进行备份。

   备份成功后，在手动备份/恢复区域，单击**恢复**，选择备份文件，单击**确认**，即将该备份的系统配置数据恢复并覆盖当前系统配置数据，如图 *13-107: 手动恢复*所示。

图 13-107: 手动恢复

13.3.6.1.3 查询备份清单

背景信息

自动备份的数据默认会存储到数据库审计系统的硬盘，也可以选择上传到FTP服务器转存。安全管理员可在备份清单表中查看备份执行记录。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**维护**页面，单击**数据备份恢复**。
3. 设置查询日期，默认查询条件以月为单位，统计某月内的备份记录。
4. 选择数据状态，可选择的数据状态包括：
   - **全部**：本系统审计到的全部数据查询。
   - **在线**：本系统中未被清理、恢复，并且在线可查询的初始数据。
   - **已恢复**：本系统中清理后被恢复的数据。
   - **已清理**：本系统中达到系统阈值被清理的数据。
   - **处理中**：本系统当前正在进行清理或者恢复的数据。

5. 单击**查询**或**刷新**，查看相应的备份记录。备份清单列表包含备份日期、数据状态、备份结果、FTP上传状态、空间占用等信息。

> **说明**：
> 如果自动备份启用FTP设置，且备份已成功转存至FTP服务器，在操作栏中单击**恢复**，可将该日志备份恢复至数据库审计系统硬盘。

13.3.6.2 Agent管理

Agent管理主要包含Agent下载、Agent配置部署等功能。

13.3.6.2.1 下载Agent

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**维护**页面，单击**Agent管理**。
3. 单击**下载Agent**，如图 *13-108: 下载Agent*所示。

图 13-108: 下载Agent

4. 单击**确定**，打开**Agent部署配置**对话框。
5. 将已下载的Agent程序上传并安装至需要被审计的数据库服务器。
6. 在**Agent部署配置**对话框中，输入数据库所在服务器的IP地址，单击**添加**。

   在IP地址栏中输入多个IP地址（每个IP地址一行），单击**添加**，可批量添加服务器IP地址。

> **说明**：
> 请务必完成Agent部署配置。如未配置，Agent程序抓取的数据将无法被审计。

部署配置完成后，云盾数据库审计系统即可对该数据库进行审计。

13.3.6.2.2 Agent自动部署

背景信息

> **说明**：
> 建议多应用环境的服务器使用该功能部署Agent，只支持Linux系统。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**维护**页面，单击**Agent管理**。
3. 单击**Agent自动部署**，打开**Agent自动部署**对话框，如图 *13-109: Agent自动部署*所示。

   图 13-109: Agent自动部署

4. 根据实际情况勾选是否**本地回环**（**应用程序与数据库在同一台机器上**），输入云盾数据库审计系统服务器IP及目标服务器信息，单击**部署**。

   说明：
   目标服务器信息格式为：目标服务器IP,root密码,ssh端口

5. 开始部署后，单击**查看执行日志**，可查看自动部署执行情况。
   等待部署完成，目标服务器会自动下载并安装Agent。Agent安装完成后，需要前往**Agent部署配置**对话框中完成Agent部署配置。

13.3.6.3 恢复出厂设置

背景信息

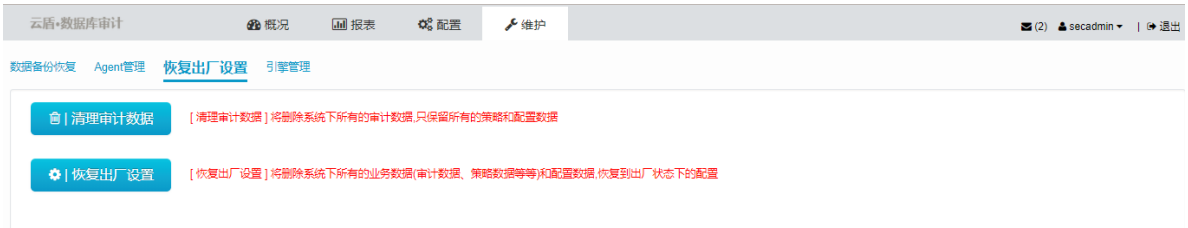
本系统出于安全性考虑，提供恢复出厂设置功能。

- **清理审计数据**：删除系统下所有的审计日志，仅保留所有的策略和配置数据。
- **恢复出厂设置**：删除系统下所有的业务数据（审计日志、配置数据等）以及配置数据，恢复至出厂状态配置。

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**维护**页面，单击**恢复出厂设置**，如图 *13-110: 恢复出厂设置*所示。

图 13-110: 恢复出厂设置



3. 根据需要，执行恢复出厂设置操作。
   - 单击**清理审计数据**。
   - 单击**恢复出厂设置**。
4. 单击**确定**。

13.3.6.4 引擎管理

操作步骤

1. 使用安全管理员（secadmin）账号登录云盾数据库审计系统。
2. 定位到**维护**页面，单击**引擎管理**，如图 *13-111: 引擎管理*所示。

图 13-111: 引擎管理

- 单击**启动**或**停止**，可启动或停止数据库审计引擎。
- 单击**刷新**，刷新引擎的当前状态及配置信息。
- 在常用配置区域，设置引擎的配置属性值，单击**保存**，修改引擎配置。

> **说明**：
> 单击**恢复默认值**，可将配置属性恢复至默认值。

13.4 审计管理员指南

审计管理员与系统管理员（sysadmin）和安全管理员（secadmin）不同，其主要职责是通过查看系统审计日志对云盾数据库审计系统本身进行审计管理。

13.4.1 查看系统操作日志

操作步骤

1. 使用审计管理员（sysauditor）账号登录云盾数据库审计系统。
2. 在**审计日志**页面，选择数据库，选择查询时间范围，单击**查询**，查看数据库审计系统操作日志，如图 *13-112: 审计日志*所示。

> **说明**：
> 单击**条件**，可针对用户、登录IP、动作等信息设置更精准的查询条件。

图 13-112: 审计日志

单击日志记录列表右上角的导出报告按钮，选择**csv导出**，可将当前列表中的审计日志记录导出到本地。

3. 选择审计日志记录，单击操作栏中的详细按钮，可以查看该审计日志的详细信息，如图 *13-113: 审计日志详细信息*所示。

   单击操作栏中的删除按钮，可以删除该日志记录。另外，单击日志记录列表上方的清空日志记录按钮，可删除所有日志记录。

图 13-113: 审计日志详细信息

14 堡垒机

云盾堡垒机为云服务器的运维提供完整的审计回放和权限控制服务。基于账号（Account）、认证（Authentication）、授权（Authorization）、审计（Audit）的AAAA统一管理方案，通过身份管理、授权管理、双因子认证、实时会话监控与切断、审计录像回放、高危指令查询等功能，增强运维管理的安全性。

云盾堡垒机符合各类法令法规的要求，包括等级保护、银监会、证监会、PCI安全标准委员会、企业内控管理等相关政策规定要求。

14.1 堡垒机系统部署

堡垒机系统通过镜像方式部署在专有云Enterprise版平台上的ECS云服务器中。

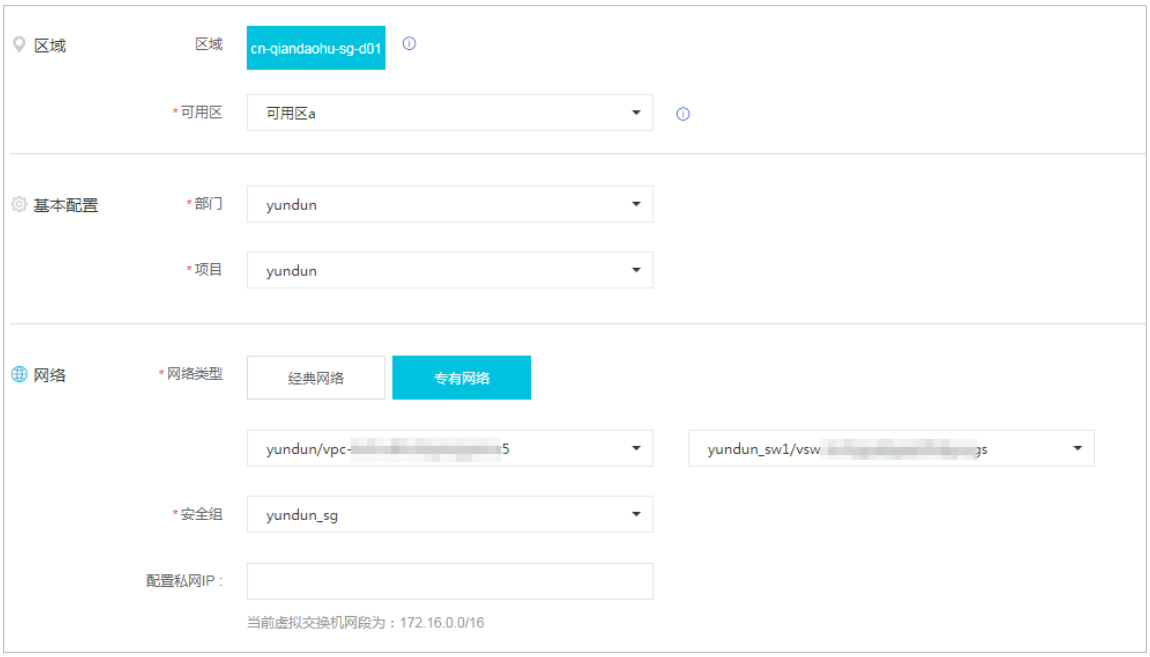
操作步骤

1. 登录Apsara Stack控制台。

   说明：
   部署堡垒机系统需要使用具有相关资源权限的用户进行操作。

2. 定位到**云管控中心** > **云基础产品** > **云服务器**，选择**实例**页签。
3. 单击**创建实例**，进入**创建云服务器ECS**页面，创建云盾堡垒机系统服务器。
   a) 设置区域、配置基本配置、网络等信息。

图 14-1: 设置ECS实例配置属性



b) 单击**请选择实例规格**，选择ECS实例规格。

建议规格如下：

- CPU：4核
- 内存：8G

c) 选择**公共镜像**，下拉菜单中选择**堡垒机**镜像，并选择对应的版本。

d) 配置40G的系统盘和800G的数据盘。

> **说明**：
> 数据盘至少需要100G，否则服务无法启动。

e) 填写服务器密码、实例名称，单击**创建**，创建云盾堡垒机系统ECS实例。

14.2 admin管理员快速配置指南

14.2.1 登录云盾堡垒机系统

前提条件

- 请确认您所使用的客户端能够正常访问云盾堡垒机系统。
- 请确认您已经从云盾堡垒机系统部署人员处获得云盾堡垒机系统的访问地址。
- 请确认您已经从云盾堡垒机系统部署人员处获得超级管理员（admin）的初始密码。

操作步骤

1. 打开Chrome浏览器。
2. 在地址栏中，输入`https://`云盾堡垒机系统的访问地址，按回车键（Enter），进入系统登录页面，如图 *14-2: 云盾堡垒机系统登录页面*所示。

   图 14-2: 云盾堡垒机系统登录页面

3. 在云盾堡垒机系统登录页面，输入超级管理员用户名（admin）、密码及验证码。

4. 单击**登录**。

> **说明**：
> 首次登录成功后，管理员必须修改密码。

14.2.2 快速配置

云盾堡垒机系统采用集中配置模式，将用户、主机、授权集中由超级管理员配置。例如，必须由超级管理员（admin）新建用户、主机、授权，其他用户没有创建用户、主机、授权的权限。

14.2.2.1 新建用户

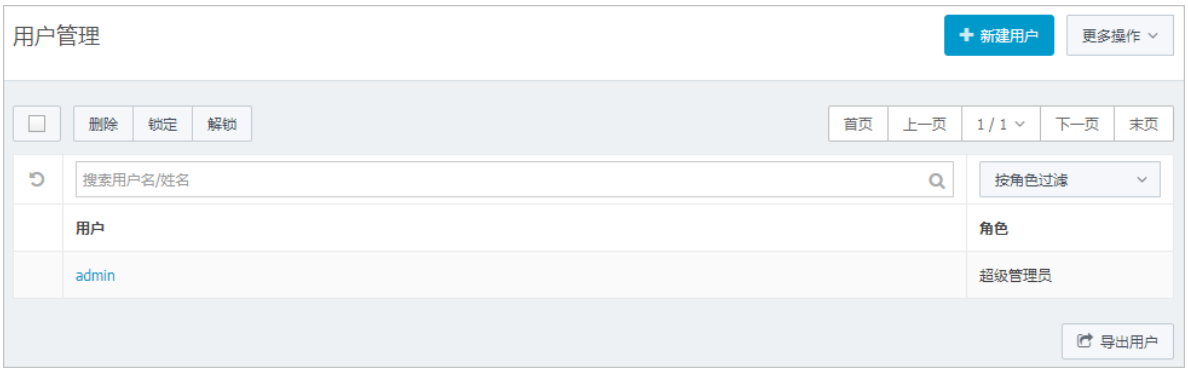
云盾堡垒机系统支持手工新建用户和批量导入用户两种添加方式。

14.2.2.1.1 手工新建用户

操作步骤

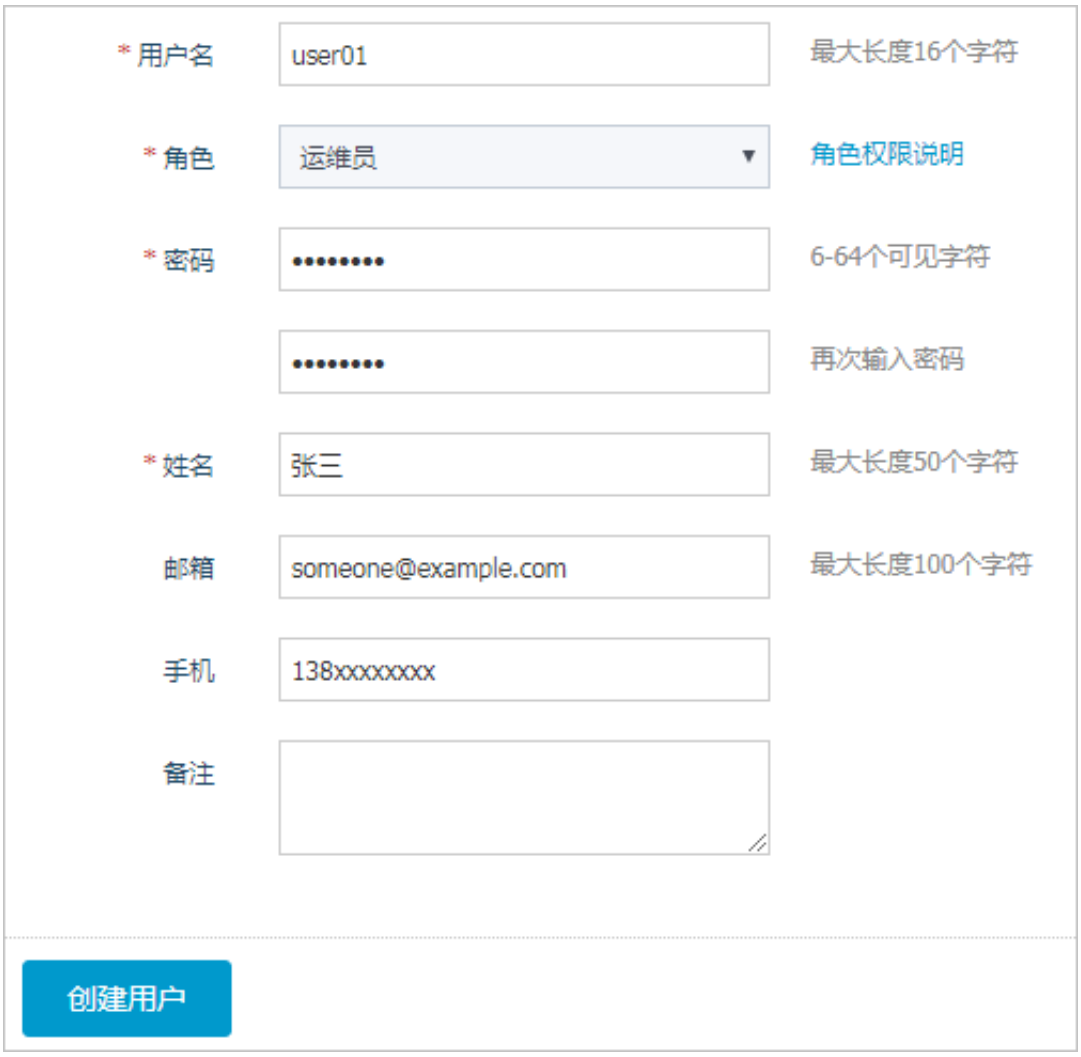
1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
2. 定位到**用户** > **用户管理**页面，如图 *14-3:* 用户管理页面所示。

图 14-3: 用户管理页面



3. 单击**新建用户**。
4. 在**新建用户**页面，输入用户信息，如图 *14-4:* 新建用户所示。

图 14-4: 新建用户



说明：

单击角色选择框右侧的**角色权限说明**可查看云盾堡垒机系统所有角色的对应权限，如图 *14-5: 角色权限说明*所示。

图 14-5: 角色权限说明

	超级管理员	部门管理员	运维管理员	审计管理员	运维员	审计员	系统管理员
用户管理 用户增加、删除、编辑	●	●	●	●			
用户组管理 用户组增加、删除、编辑	●	●	●				
资产管理 管理资产	●	●	●				
授权管理 管理运维规则，审批工单	●	●	●				
会话审计 查看、播放、下载历史会话	●	●		●		◐ 需要审计规则允许	
审计规则 管理审计规则	●	●		●			
主机运维 主机运维、应用运维、创建工单、查看运维报表	●	●	●	●	●	●	●
实时监控 管理、审批在线会话	●	●	●				
系统管理 系统配置、操作日志、系统报表、数据维护、系统维护	●						●

5. 单击**创建用户**。

   创建用户成功，系统提示用户已创建。

14.2.2.1.2 批量导入用户

操作步骤

1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
2. 定位到**用户** > **用户管理**页面。
3. 单击**更多操作**，选择**导入用户**。
4. 在**导入用户**页面，单击**下载模板文件**将用户列表模板下载至本地，如*图 14-6: 导入用户页面*所示。

图 14-6: 导入用户页面

5. 根据模板规范要求，制作需要导入的用户列表。
6. 单击**上传文件**，从本地选择制作好的用户列表文件。
7. 选择**认证模式**，勾选是否**覆盖已有同名用户**。

> **说明**：
> 如不勾选**覆盖已有同名用户**，则同名用户不会被导入。

8. 单击**导入用户**。

   等待用户导入完成，系统提示本次成功导入用户数量。

14.2.2.2 管理用户配置

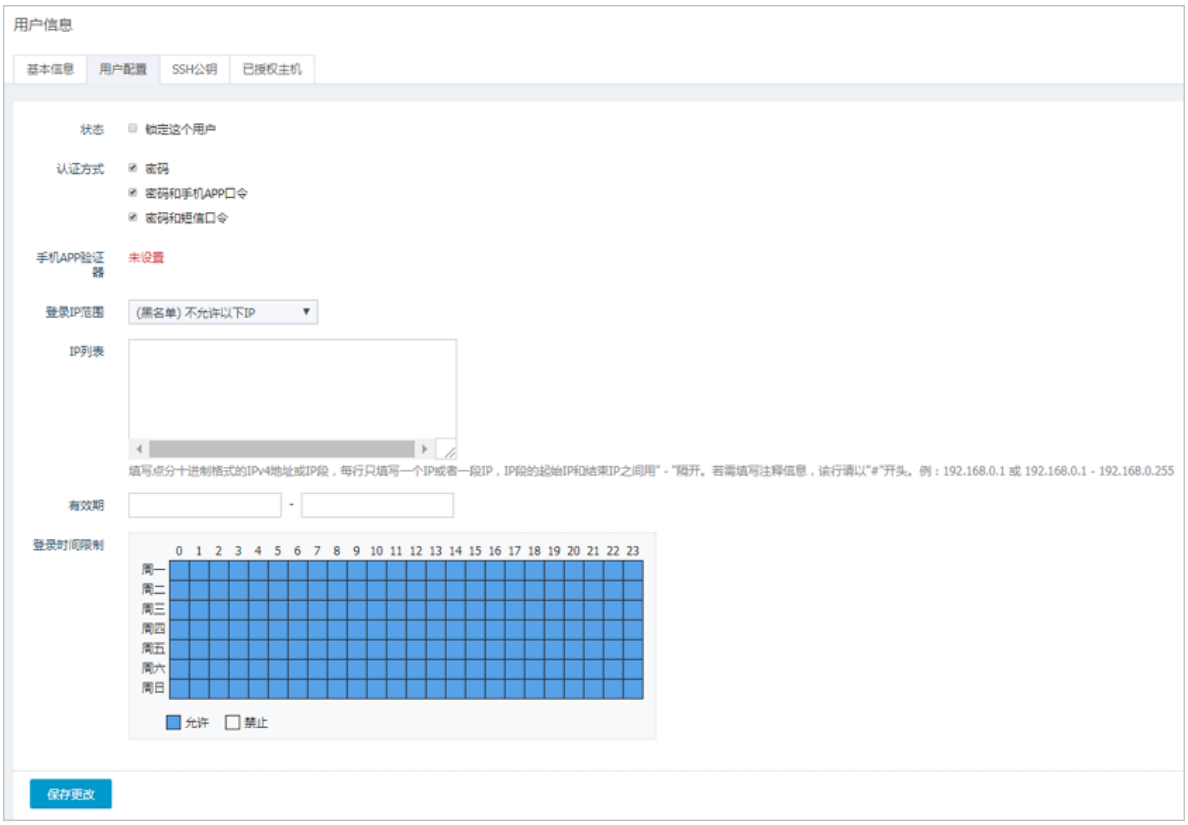
背景信息

用户创建成功后，管理人员可以对用户进行相关配置。

操作步骤

1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
2. 定位到**用户** > **用户管理**页面。
3. 单击已添加的用户，打开**用户信息**页面。
4. 选择**用户配置**页签，对该用户进行配置，单击**保存更改**，如*图 14-7: 更改用户配置*所示。

图 14-7: 更改用户配置



14.2.2.3 新建用户组

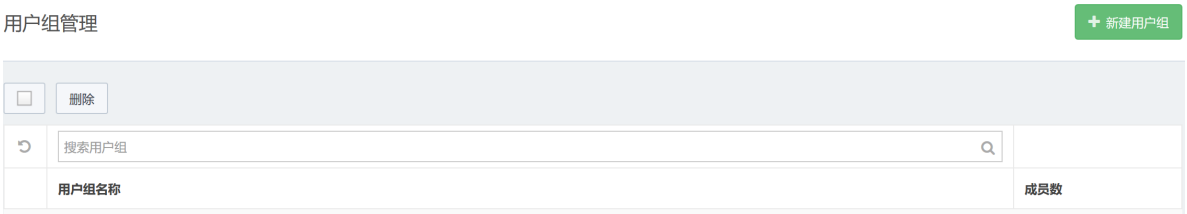
背景信息

用户组用于对用户进行分组或分类管理，一个用户可以属于多个用户组。

操作步骤

1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
2. 定位到**用户** > **用户组管理**页面，如图 *14-8:* 用户组管理页面所示。

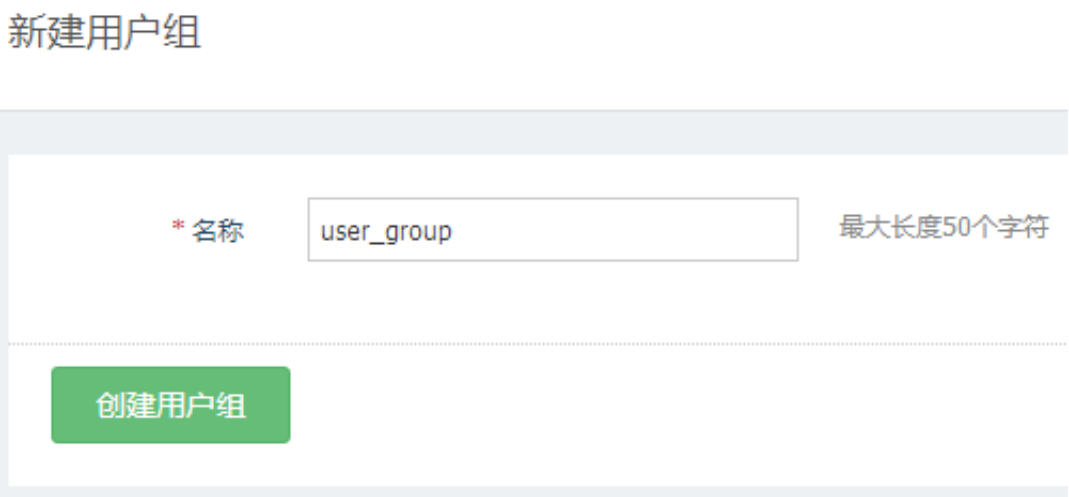
图 14-8: 用户组管理页面



3. 单击**新建用户组**。

4. 填写用户组**名称**，单击**创建用户组**，如图 *14-9: 新建用户组*所示。

图 14-9: 新建用户组



用户组创建成功后，在**用户组管理**页面单击已添加的用户组，选择**修改用户组名称**页签，可修改该用户组的名称。

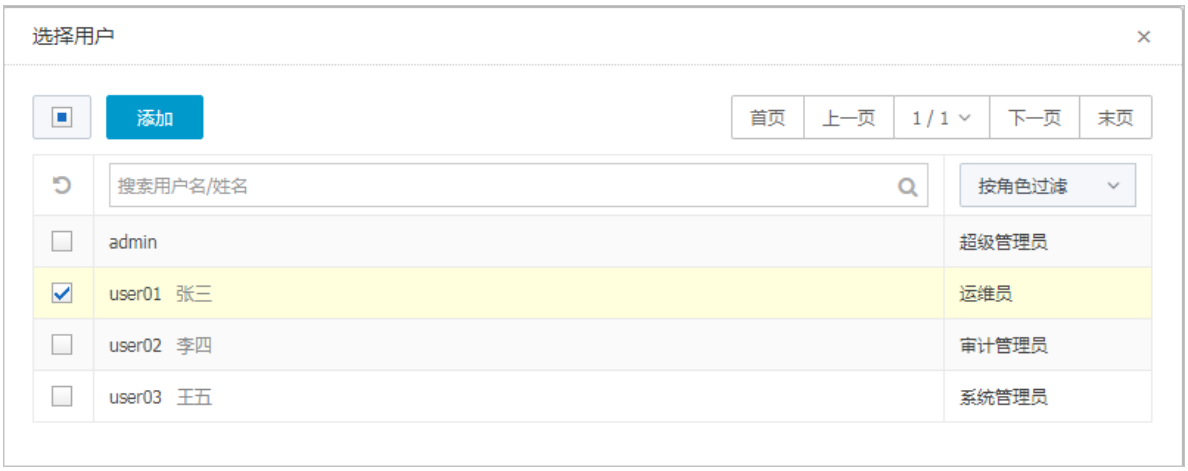
14.2.2.4 对用户进行分组

操作步骤

1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
2. 定位到**用户** > **用户组管理**页面。
3. 单击已添加的用户组，进入**用户组信息**页面。
4. 单击**添加成员**，在**选择用户**对话框中，勾选需要添加至该用户组的用户，单击**添加**，如图 *14-10: 选择用户*所示。

> **说明**：
> 在**选择用户**对话框中，可以输入用户名或姓名，单击查询按钮，只显示用户名/姓名包含所输入字段的用户；也可以选择按角色进行过滤的方式，只显示属于某种角色的用户。

图 14-10: 选择用户



成功添加用户后，在**用户组信息**页面，勾选该用户组中的用户，单击**移除**，可将该用户从用户组中移除。

14.2.2.5 新建主机

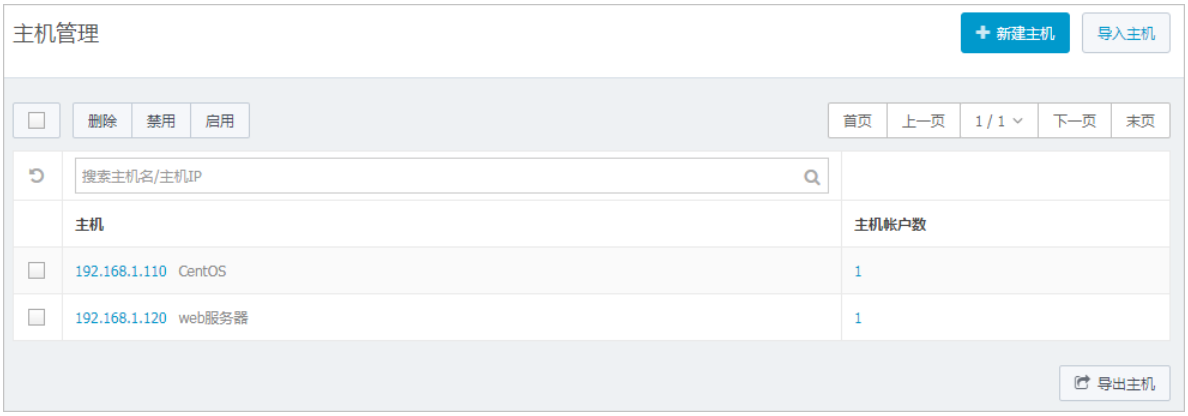
云盾堡垒机系统支持手工新建主机和批量导入主机两种添加方式。

14.2.2.5.1 手工新建主机

操作步骤

1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
2. 定位到**资产** > **主机管理**页面，如图 *14-11:* 主机管理页面所示。

图 14-11: 主机管理页面



3. 单击**新建主机**。
4. 在**新建主机**页面，输入**主机IP**、**主机名称**，如图 *14-12:* 新建主机所示。

图 14-12: 新建主机

说明：

如果不填写主机名称，主机创建之后，默认使用主机IP作为主机名称。

5. 单击**创建主机**。

   创建主机成功，系统提示主机已创建。

6. 在**主机管理**页面，单击已添加的主机IP，进入**主机信息**页面，如图 *14-13:* 主机信息页面所示。

图 14-13: 主机信息页面

说明：

在**基本信息**页签中修改主机IP或主机名称，单击**保存更改**，可修改主机的基本信息。

7. 选择**主机帐户**页签，进入**主机帐户管理**页面，如图 *14-14: 主机帐户管理*所示。

图 14-14: 主机帐户管理

8. 单击**添加主机帐户**，打开**新建主机帐户**对话框，如图 *14-15: 新建主机帐户*所示。

图 14-15: 新建主机帐户

说明：

管理员可以创建一个**协议**为**SYSDEF**、**登录模式**为**手动**的**[EMPTY]**空帐户。**SYSDEF**协议表示可以手工选择任何协议方式登录主机。

运维人员使用**[EMPTY]**空帐户登录目标主机进行运维时，需要手动输入目标主机帐户和密码。

9. 配置主机帐户信息，单击**验证**，验证主机帐户和密码是否正确。
10. 验证成功后，单击**创建主机帐户**。

后续操作

主机帐户创建成功后，在**主机管理**页面，可以查看已添加的主机及对应的主机帐户数。同时，在**主机帐户管理**页面可管理已添加的主机帐号：

- 单击主机帐户名称，可在**编辑主机帐户**对话框中，修改该帐户的属性。
- 勾选主机帐户，单击**删除**，可删除主机帐户。
- 在已设置密码的主机帐户的密码栏中单击**清除**，可清除该主机帐户的密码。
- 对于使用SSH协议的主机帐户，如需通过SSH密钥方式登录，可在SSH私钥栏中单击**设置**来上传对应的RSA私钥信息。

14.2.2.5.2 批量导入主机

操作步骤

1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
2. 定位到**资产** > **主机管理**页面。
3. 单击**导入主机**。
4. 在**导入主机**页面，单击**下载模板文件**将规范的主机列表模板下载至本地，如图 *14-16: 导入主机页面*所示。

   图 14-16: 导入主机页面

5. 根据模板规范，制作需要导入的主机列表文件。
6. 单击**上传文件**，从本地选择制作好的主机列表文件。
7. 勾选是否**覆盖已有主机和主机帐户**。

   说明：
   如不勾选**覆盖已有主机和主机帐户**，则同名主机和主机帐户不会被导入。

8. 单击**导入主机**。
   等待主机和相应的主机帐户导入完成，系统提示本次成功导入数量。

14.2.2.6 管理主机配置

背景信息

主机添加成功后，管理人员可以对主机进行相关配置。

操作步骤

1. 使用超级管理员*#admin#*账号登录云盾堡垒机系统。
2. 定位到**资产** > **主机管理**页面。
3. 单击已添加的主机，打开**主机信息**页面。
4. 选择**主机配置**页签，对该主机进行配置，单击**保存更改**，如图 *14-17:* 更改主机配置信息所示。

图 14-17: 更改主机配置信息

14.2.2.7 新建主机组

背景信息

主机组用于对主机进行分组或分类管理，一个主机可以属于多个主机组。

操作步骤

1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
2. 定位到**资产** > **主机组管理**页面，如图 *14-18:* 主机组管理页面所示

   图 14-18: 主机组管理页面

3. 单击**新建主机组**，进入**新建主机组**页面，如图 *14-19:* 新建主机组页面所示。

   图 14-19: 新建主机组页面

4. 填写**主机组名称**，单击**创建主机组**。

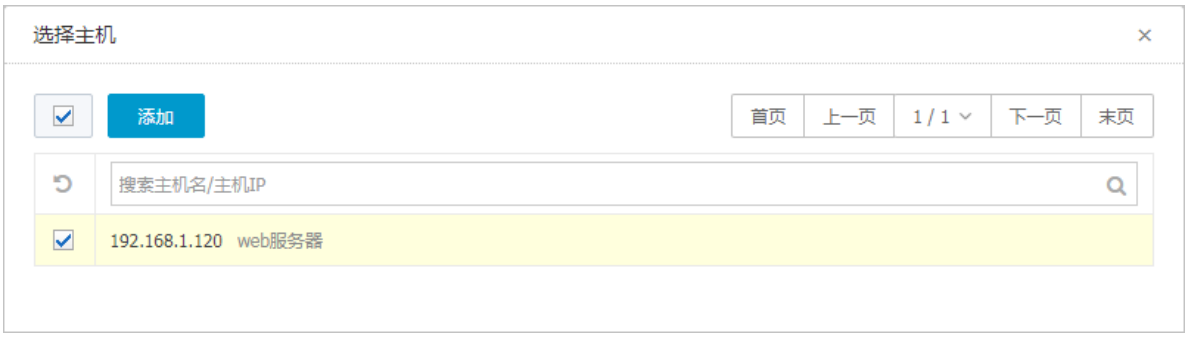
   主机组创建成功后，在**主机组管理**页面单击已添加的主机组，选择**修改主机组名称**页签，可修改该主机组的名称。

14.2.2.8 对主机进行分组

操作步骤

1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
2. 定位到**资产** > **主机组管理**页面。
3. 单击已添加的主机组，进入**主机组信息**页面。
4. 单击**添加主机**，在**选择主机**对话框中，勾选需要添加至该主机组的主机，单击**添加**，如图 *14-20: 选择主机*所示。

图 14-20: 选择主机



说明：

在**选择主机**对话框中，可以输入主机名或主机IP，单击查询按钮，只显示主机名/主机IP中包含所输入字段的主机。

成功添加主机后，在**主机组信息**页面，勾选该主机组中的主机，单击**移除**，可将该主机从主机组中移除。

14.2.2.9 运维授权

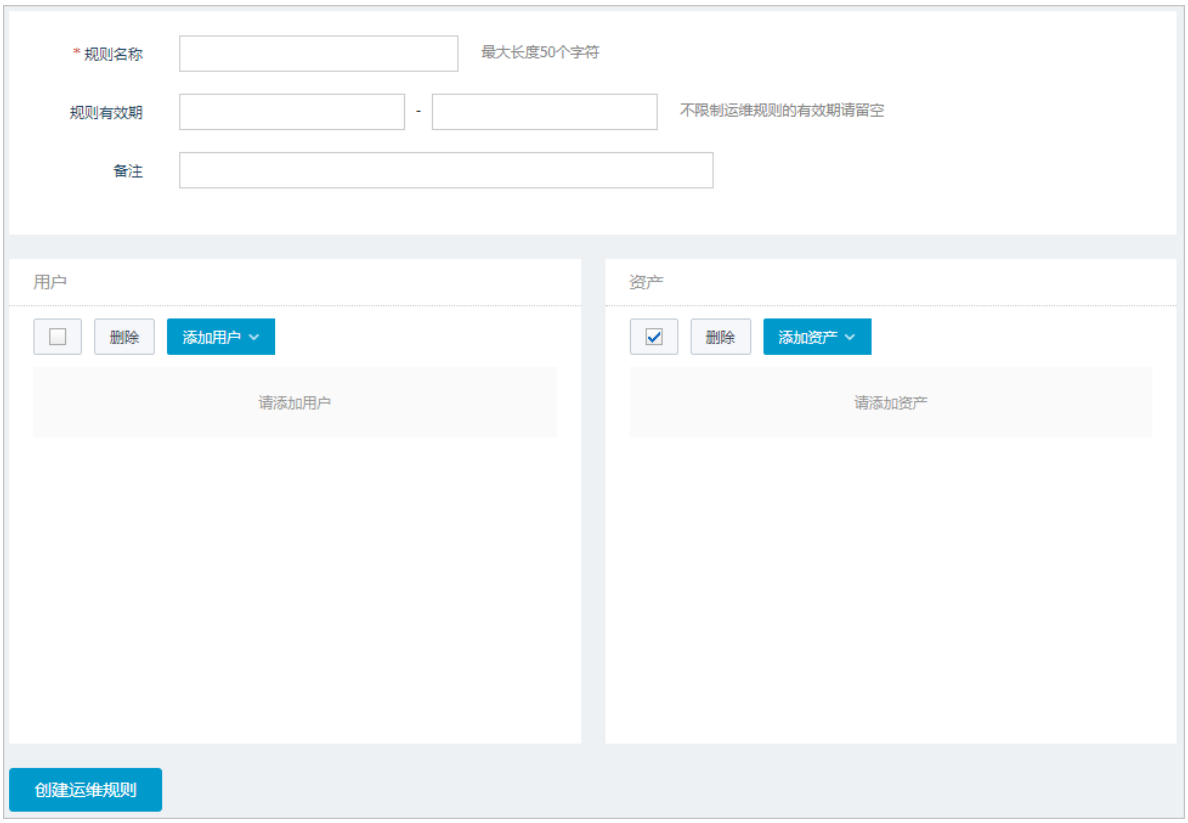
运维授权是为了梳理用户与主机之间的关系，本章节以基于用户授权主机账户的方式为例进行具体说明。

14.2.2.9.1 新建运维规则

操作步骤

1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
2. 定位到**授权** > **运维规则**页面。
3. 单击**新建运维规则**，进入**新建运维规则**页面，关联用户与资产的关系，如图 *14-21: 新建运维规则页面*所示。

图 14-21: 新建运维规则页面



a) 填写**规则名称**，设置**规则有效期**。

b) 单击**添加用户**，选择**添加用户**或**添加用户组**。

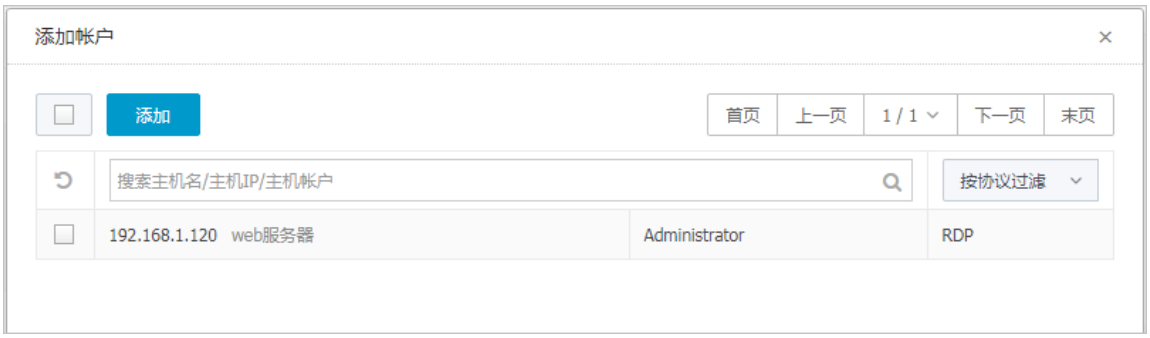
c) 勾选需要授权的用户或用户组，单击**添加**，如图 *14-22: 添加用户页面*所示。

图 14-22: 添加用户页面

d) 返回**新建运维规则**页面，单击**添加资产**，选择**添加主机帐户**、**添加帐户组**或者**添加主机组**。

e) 勾选需要授权的主机帐户、帐户组或者主机组，单击**添加**，如图 *14-23: 添加主机帐户页面*所示。

图 14-23: 添加主机帐户页面



4. 在**新建运维规则**页面，单击**创建运维规则**，即将所添加的用户和所添加的主机帐户进行关联。

14.2.2.9.2 管理运维规则

背景信息

运维规则创建后，管理人员可以对运维规则进行相关配置。

操作步骤

1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
2. 定位到**授权** > **运维规则**页面。
3. 选择已添加的运维规则，执行相关操作。
   - 单击**操作**，选择**编辑规则**，可变更该规则的相关信息。
     - 在**总览**页签，可修改该规则的名称，设置有效期或直接禁用该规则。
     - 在**用户/资产**页签，可修改该规则中用户与主机之间的关系。
     - 在**登录限制**页签，可对该规则启用登录限制并进行相关设置，如图 *14-24:* 设置登录限制所示。

图 14-24: 设置登录限制

- 在**命令控制**页签，可对该规则启用命令控制并进行相关设置，如图 *14-25:* 设置命令控制所示。

图 14-25: 设置命令控制

- 在**协议控制**页签，可对该规则启用协议控制并进行相关设置，如图 *14-26:* 设置协议控制所示。

图 14-26: 设置协议控制

说明：

协议控制设置与主机配置内容相同，但协议控制启用后仅针对该运维规则授权的用户生效，而主机配置对所有用户生效。

- 单击**操作**，选择**复制规则**，在**复制规则**对话框中输入新规则的名称并选择复制内容，可复制该规则的相关信息创建新的运维规则。
- 单击**操作**，选择**删除规则**，可删除该运维规则。

14.2.3 实时监控

背景信息

为运维人员配置运维规则后，运维人员就能通过云盾堡垒机系统对所授权的主机进行运维操作。在运维人员进行运维操作时，管理人员可以通过云盾堡垒机系统实时监控运维会话。

操作步骤

1. 使用超级管理员#admin#账号登录云盾堡垒机系统。
2. 定位到**运维** > **实时监控**页面。
3. 选择**所有会话**页签，选择实时会话，执行更多操作。
   - 单击操作栏中的**详情**，可查看详细的会话信息。
   - 单击操作栏中的**播放**，可通过Web方式查看会话实时回放。

     说明：
     通过Web方式查看会话审计，需要在本地安装Flash Player才可在线播放。如果本地客户端未安装Flash Player，单击云盾堡垒机系统页面右上角的用户名，选择**工具下载**，下载并安装Flash Player 12。
   - 单击**阻断会话**，可直接断开该实时运维会话，运维人员将被强制断开与目标主机的连接。

     说明：
     如果在运维规则中启用了命令控制功能，对于需要管理人员审批的命令，可在**实时监控**页面的**需要审批命令**页签查看详细信息，并进行审批操作。

14.3 运维人员操作指南

超级管理员参考快速配置手册为运维人员授权主机后，运维人员就能通过云盾堡垒机系统对所授权的主机进行运维操作。云盾堡垒机系统支持运维人员通过Web运维方式和客户端运维方式两种方式进行运维操作。

14.3.1 登录云盾堡垒机系统

前提条件

请确认您所使用的客户端能够正常访问云盾堡垒机系统。

操作步骤

1. 打开Chrome浏览器。
2. 在地址栏中，输入云盾堡垒机系统的访问地址，按回车键（Enter），进入系统登录页面。
3. 在云盾堡垒机系统登录页面，输入超级管理员所分配的用户名、密码，输入验证码。
4. 单击**登录**。

   首次登录成功后，运维人员需要修改登录密码。

14.3.2 下载运维工具

背景信息

工具下载页面为运维人员提供在登录主机前下载所需要用到的运维工具。

操作步骤

1. 登录云盾堡垒机系统。
2. 单击页面右上角的用户名，选择**工具下载**，进入**工具下载**页面，如图 *14-27:* 工具下载页面所示。

图 14-27: 工具下载页面

3. 选择所需要的工具，单击**本地下载**，即可将相应的安装程序下载到本地进行安装。

表 14-1: 运维工具说明

运维工具	说明
单点登录器	单点登录器是通过Web方式调用客户端运维工具时，必须安装的登录工具。
离线播放器	离线播放器与Adobe ATR是用于下载会话审计的会话日志后，进行离线播放的工具。
Adobe ATR	

运维工具	说明
Flash Player	Flash Player是通过Web方式查看会话审计的会话日志时，必须安装的工具。
字符客户端	字符客户端包括PuTTY、SecureCRT、Xshell、Windows Telnet等工具，用于连接SSH、Telnet协议的主机进行运维操作。
图形客户端	图形客户端包括Mstsc、RealVNC等工具，用于连接Windows服务器、VNC服务器进行运维操作。
文件传输客户端	文件传输客户端包括FileZilla、WinSCP、SecureFX等工具，用于连接SFTP、FTP服务器进行文件传输操作。

14.3.3 Web方式运维操作指南

本章节主要介绍通过云盾堡垒机系统的Web页面登录的方式对主机进行运维操作。

说明：

本章节中的操作步骤仅适用于使用Windows客户端的运维人员。

14.3.3.1 安装单点登录器

背景信息

单点登录器是Web方式运维必备工具。安装时，请注意不要被杀毒软件误拦截，建议关闭杀毒软件。

操作步骤

1. 登录云盾堡垒机系统。
2. 单击页面右上角的用户名，选择**工具下载**，进入**工具下载**页面，如图 *14-28:* 工具下载所示。

图 14-28: 工具下载

3. 定位到单点登录器，单击**本地下载**，将安装程序下载至本地客户端，如图 *14-29:* 单点登录器下载所示。

图 14-29: 单点登录器下载

名称	下载
单点登录器 运维登录必备工具	本地下载

4. 在本地客户端，双击单点登录器安装程序，选择**语言**，单击**OK**，单击**安装**。

   单点登录器安装完成后，提示安装成功，单击确定。

14.3.3.2 指定运维工具

背景信息

本章节以指定PuTTY工具为SSH协议登录方式为例介绍如何为SSH协议配置Web运维工具。您可以参考本章节中的操作步骤为其它登录协议指定运维工具。

操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**运维** > **主机运维**页面，单击右上角的**Web运维配置**。
3. 在**Web运维配置**对话框中，选择登录协议，例如选择**SSH & TELNET & Rlogin**。
4. 选择客户端程序，例如选择PuTTY。

   说明：
   确认您已安装了所选择的客户端程序。

5. 单击**保存**。

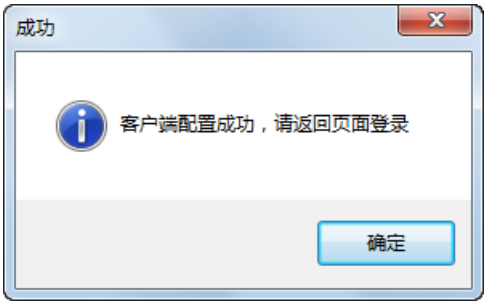
   说明：
   如果浏览器弹出**要打开URL**：**USM Single-On吗**？的提示，单击**打开**URL：**USM Single Sign-On**。

6. 在**单点登录配置**对话框中，单击**浏览**，定位到所选择客户端程序所在的位置，单击**打开**，单击**确定**，如图 *14-30:* 单点登录配置所示

图 14-30: 单点登录配置

配置成功后，弹出提示对话框，如图 *14-31: 单点登录配置成功*所示。

图 14-31: 单点登录配置成功



14.3.3.3 主机运维

14.3.3.3.1 通过SSH协议登录主机进行运维

操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**运维** > **主机运维**页面。

> **说明**：
> 在搜索框中输入主机IP、主机名、帐户等关键字信息，系统会自动过滤相关的目标主机。

3. 选择已授权的SSH协议的主机帐户，单击**登录**，如图 *14-32: SSH协议主机Web运维*所示。

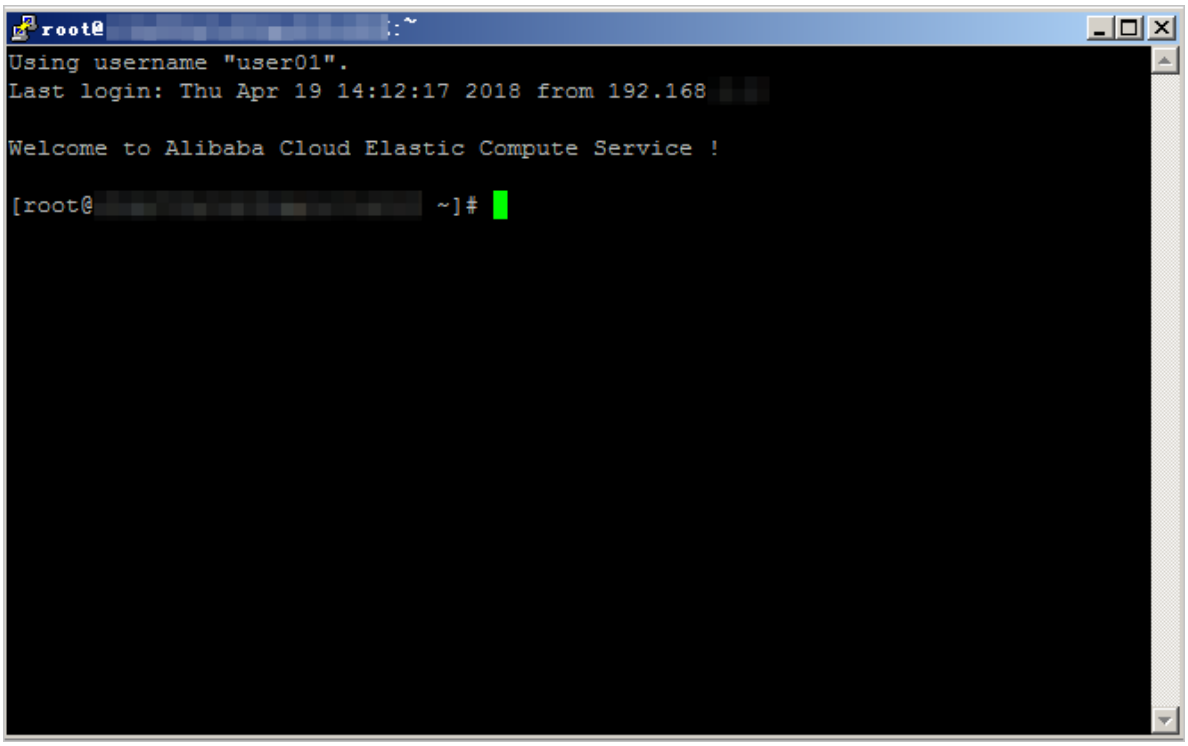
> **说明**：

如果浏览器弹出**要打开URL：USM Single-On吗？**的提示，单击**打开**URL：**USM Single Sign-On**。

图 14-32: SSH协议主机Web运维

4. 自动启动SSH运维工具，即可登录到目标主机中进行运维操作，如图 *14-33: SSH协议主机运维操作*所示。

图 14-33: SSH协议主机运维操作



说明：

如果使用**[EMPTY]**空帐户登录目标主机，需要手动选择协议，并输入目标主机帐户和密码。

14.3.3.3.2 通过RDP协议登录主机进行运维

操作步骤

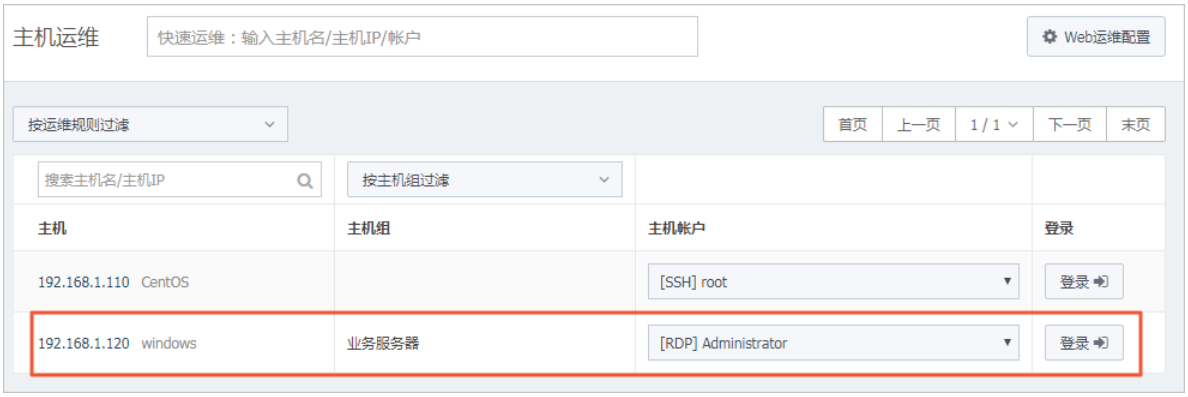
1. 登录云盾堡垒机系统。
2. 定位到**运维** > **主机运维**页面。

> **说明**：
> 在搜索框中输入主机IP、主机名、帐户等关键字信息，系统会自动过滤相关的目标主机。

3. 选择已授权的RDP协议的主机帐户，单击**登录**，如图 *14-34: RDP协议主机Web运维*所示。

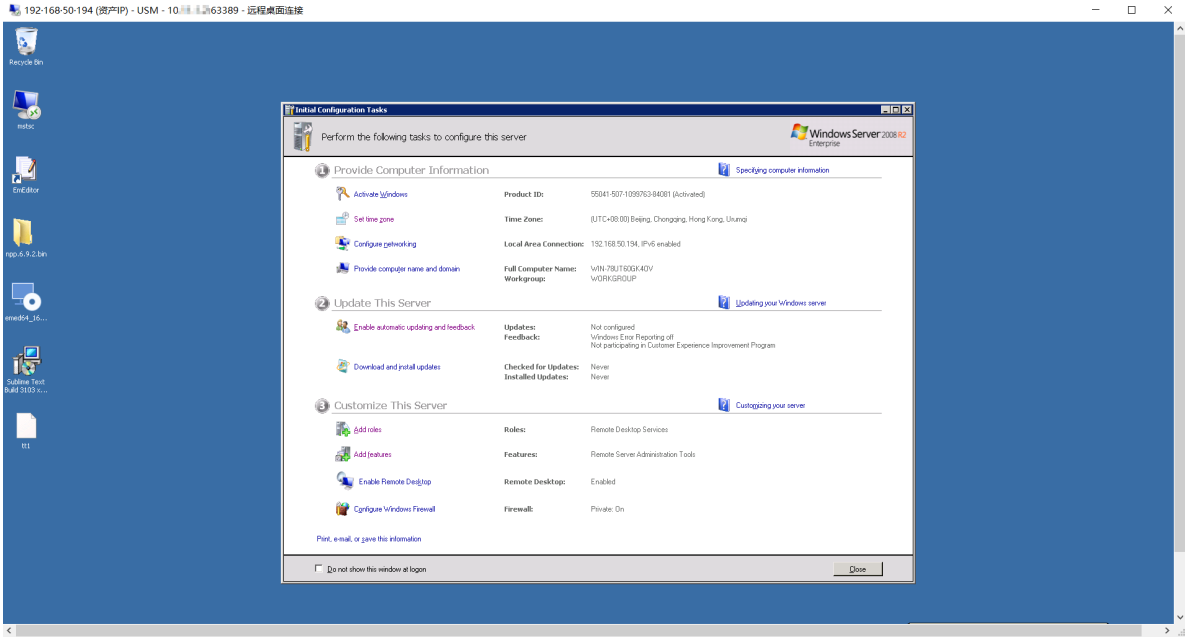
> **说明**：
> 如果浏览器弹出**要打开URL：USM Single-On吗？**的提示，单击**打开**URL：**USM Single Sign-On**。

图 14-34: RDP协议主机Web运维



4. 单击**确定**，启动远程桌面连接工具。
5. 在**远程桌面连接**对话框中，单击**连接**，即可登录到目标主机中进行运维操作，如图 *14-35: RDP协议主机运维操作*所示。

图 14-35: RDP协议主机运维操作



说明：

如果使用**[EMPTY]**空帐户登录目标主机，需要手动选择协议，并输入目标主机帐户和密码。

14.3.3.3.3 通过SFTP协议登录主机进行运维

操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**运维** > **主机运维**页面。

说明：

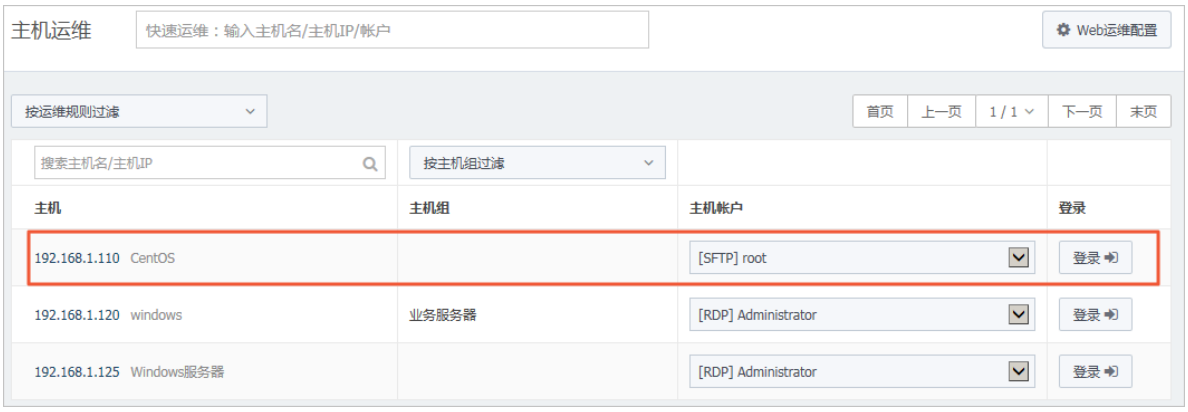
在搜索框中输入主机IP、主机名、帐户等关键字信息，系统会自动过滤相关的目标主机。

3. 选择已授权的SFTP协议的主机帐户，单击**登录**，如*图 14-36: SFTP协议主机Web运维*所示。

说明：

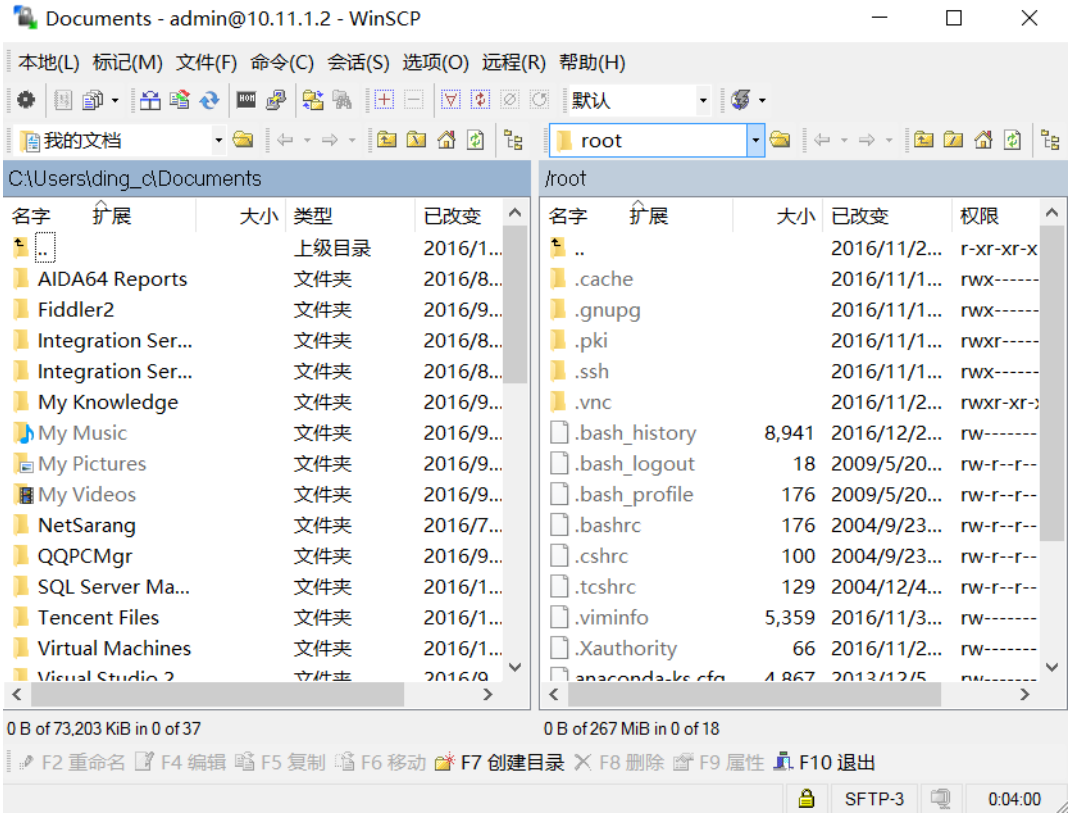
如果浏览器弹出**要打开URL：USM Single-On吗？**的提示，单击**打开**URL：**USM Single Sign-On**。

图 14-36: SFTP协议主机Web运维



4. 自动启动SFTP运维工具，即可启动客户端工具连接到目标主机进行运维操作，如*图 14-37: SFTP协议主机运维操作*所示。

图 14-37: SFTP协议主机运维操作



说明：

如果使用**[EMPTY]**空帐户登录目标主机，需要手动选择协议，并输入目标主机帐户和密码。

14.3.3.3.4 未授权登录主机进行运维

背景信息

如果运维人员知道某主机的IP、账户和密码信息，但该主机未被授权，不在主机运维列表中显示。此时，运维人员可以通过未授权登录的方式登录该主机进行运维操作。

> **说明**：
> 未授权登录功能默认禁用，需要超级管理员或系统管理员在**系统** > **系统设置**页面中启用该功能后才可以使用。

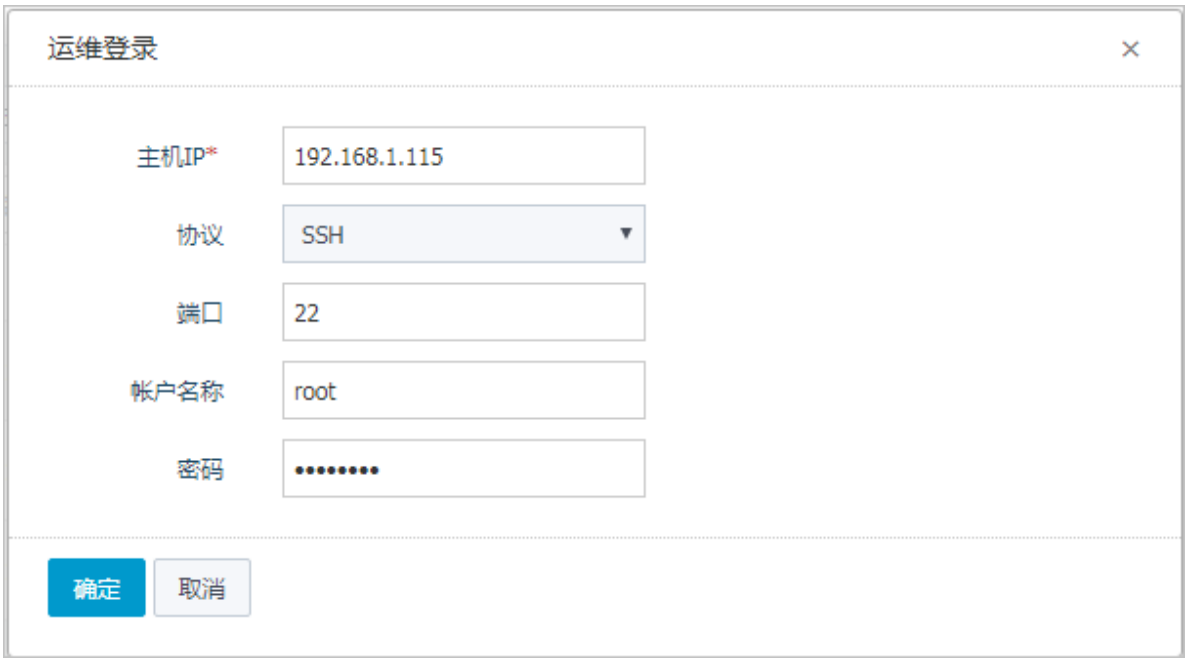
操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**运维** > **主机运维**页面，单击**未授权登录**，如图 *14-38:* 未授权登录所示。

图 14-38: 未授权登录

3. 在**运维登录**对话框中，输入主机IP等信息，单击**确定**，即可登录目标主机，如图 *14-39:* 未授权运维登录对话框所示。

图 14-39: 未授权运维登录对话框



说明：

通过未授权登录方式登录主机后，管理人员可在**授权** > **未授权登录审核**页面查看相关登录记录。

14.3.3.3.5 运维审批申请

背景信息

对于在**主机配置**中启用**开启会话二次审批**功能的主机，即使运维人员在主机运维页面可以看到该主机，也无法直接登录。运维人员单击**登录**后，系统会自动生成运维申请，需要由管理人员审批通过后，运维人员才能登录主机进行运维操作。

操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**运维** > **运维审批**页面，查看系统已自动生成的运维审批申请记录及审批状态。

说明：

对于已被批准的运维申请，运维人员即可在**主机运维**页面通过Web方式登录该主机进行运维操作，且该运维申请的状态将变为已登录。

14.3.4 CS方式运维操作指南

除上一章节中介绍的通过Web方式进行运维操作外，云盾堡垒机系统也支持通过客户端方式进行运维操作。

本章节主要介绍运维人员通过客户端登录云盾堡垒机系统，再访问目标主机的运维方式。

14.3.4.1 苹果系统客户端运维操作指南

14.3.4.1.1 准备工作

在使用苹果系统客户端登录云盾堡垒机系统进行主机运维操作前，请确保已完成下列准备工作：

- 本地已安装支持SSH协议的app，例如命令行终端、SecureCRT、Xshell等。
- 本地已安装支持RDP协议的app，例如远程桌面连接。
- 确保苹果系统客户端与云盾堡垒机系统的端口正常连通，主要包括以下两个端口：
  - 60022：用于访问SSH协议的主机。
  - 63389：用于访问RDP协议的主机。
- 确保云盾堡垒机系统与目标主机的运维端口正常连通，例如SSH协议及端口、RDP协议及端口。

14.3.4.1.2 通过命令行终端app的菜单方式登录目标主机进行运维

背景信息

本章节以命令行终端app为例，通过SSH协议登录目标主机进行运维。您可以参考本章节中的操作步骤使用其它app登录SSH协议的主机帐户。

操作步骤

1. 打开命令行终端app，输入以下命令，按回车键（Enter），如图 *14-40:* 通过命令行终端登录云盾堡垒机所示。

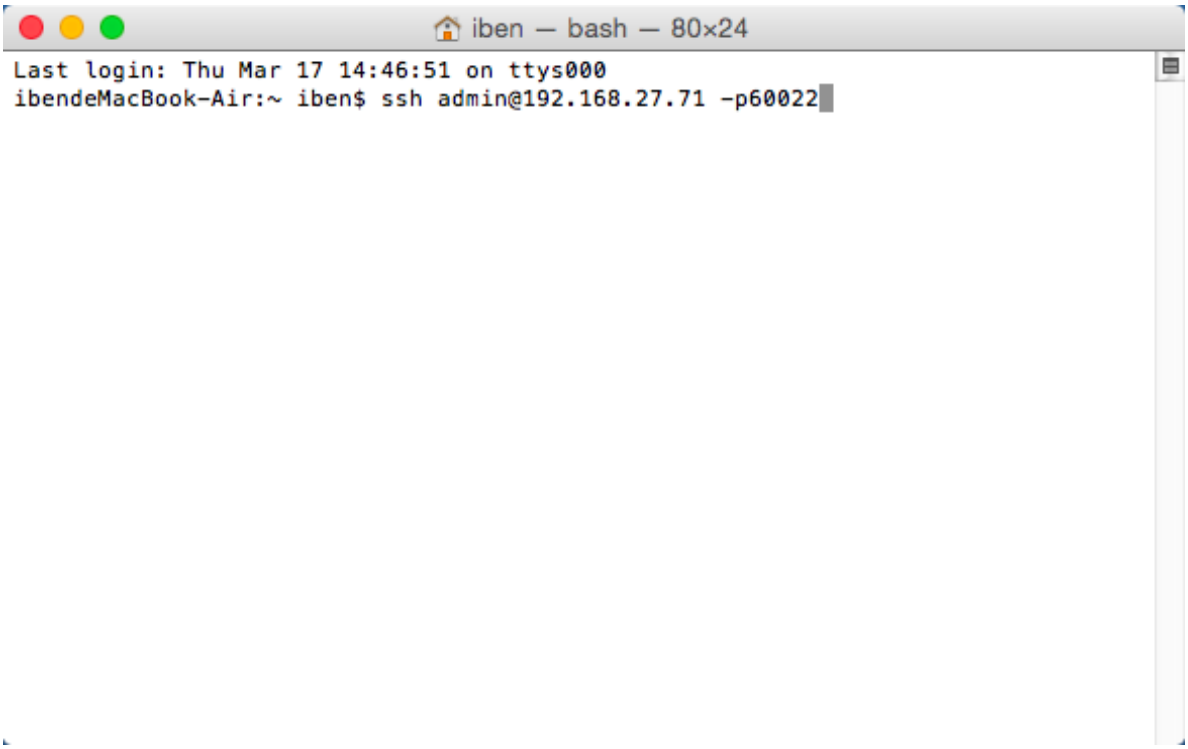
   `ssh 云盾堡垒机系统的用户名@云盾堡垒机系统的IP -p60022`

   说明：

   如果提示需要输入密码，请输入该用户的密码，按回车键（Enter）。

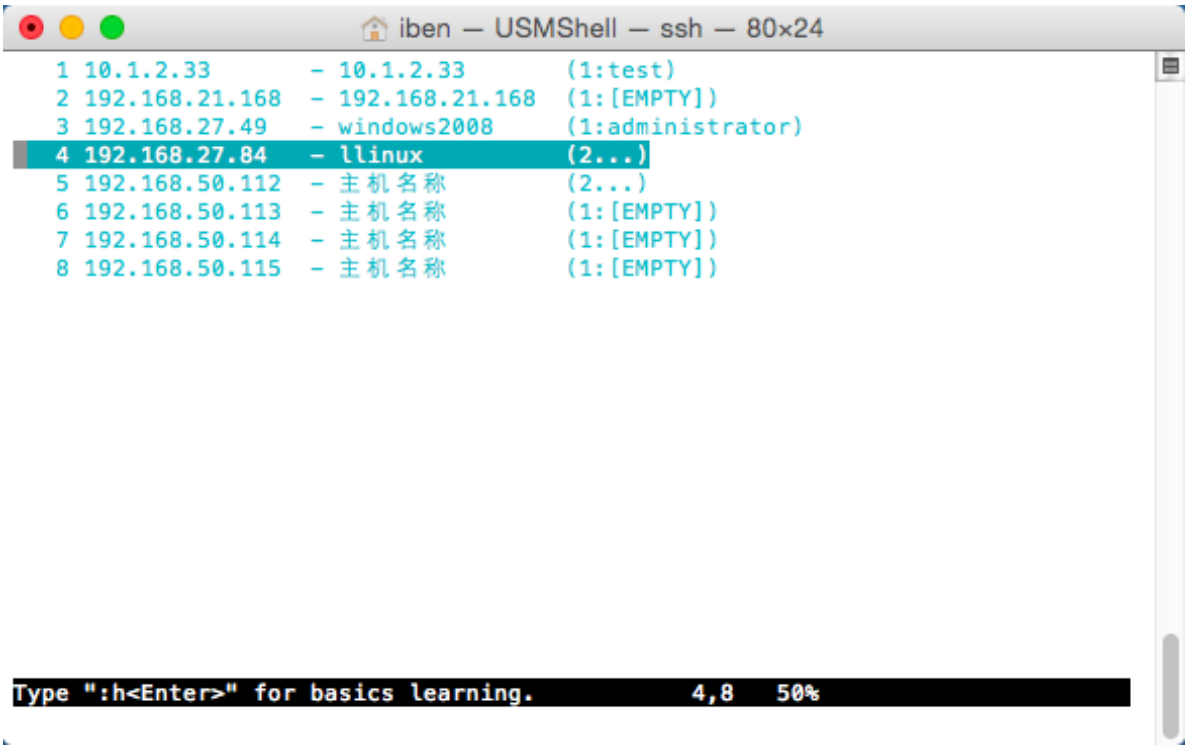
   - 云盾堡垒机系统的用户名指代管理员（例如admin）所创建的用户名。
   - 云盾堡垒机系统的*IP*指代云盾堡垒机系统的IP地址，请根据实际情况输入。

图 14-40: 通过命令行终端登录云盾堡垒机



2. 进入资产管理界面，通过上下键选择已授权的主机资产，按回车键（Enter），如图 *14-41:* 通过命令行终端选择主机资产所示。

图 14-41: 通过命令行终端选择主机资产

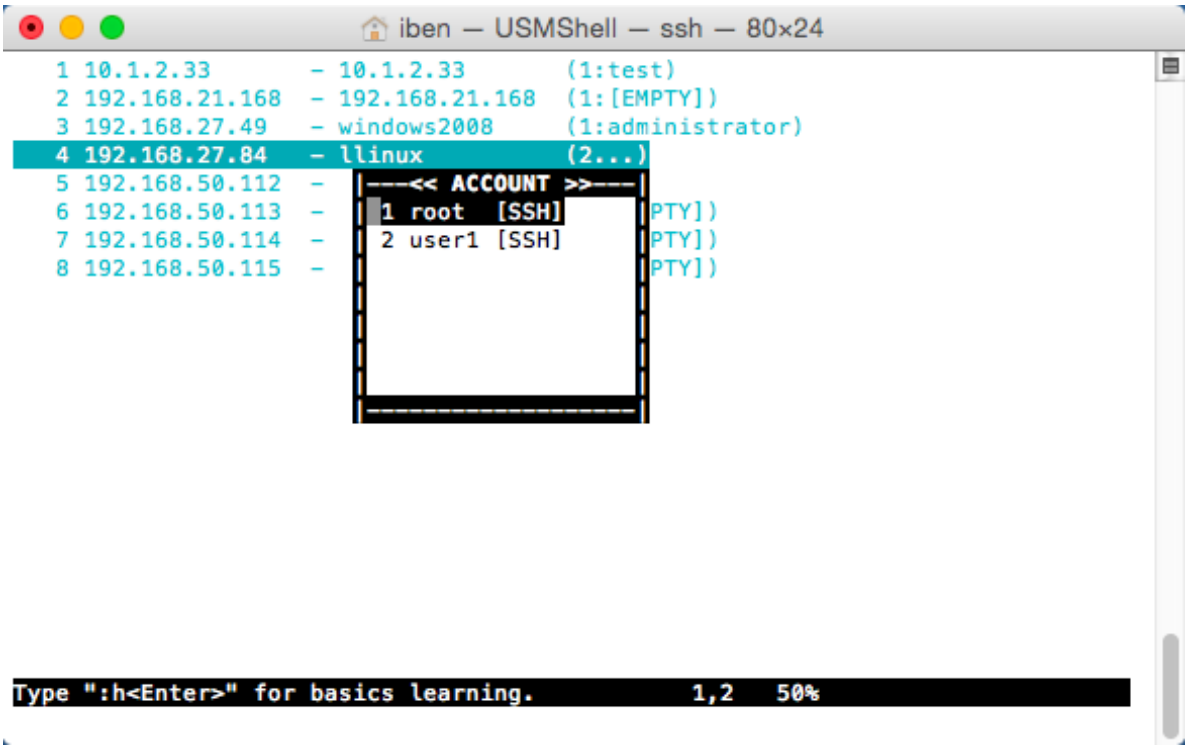


3. 选择主机账户，按回车键（Enter），如图 *14-42:* 通过命令行终端选择主机帐户所示。

说明：

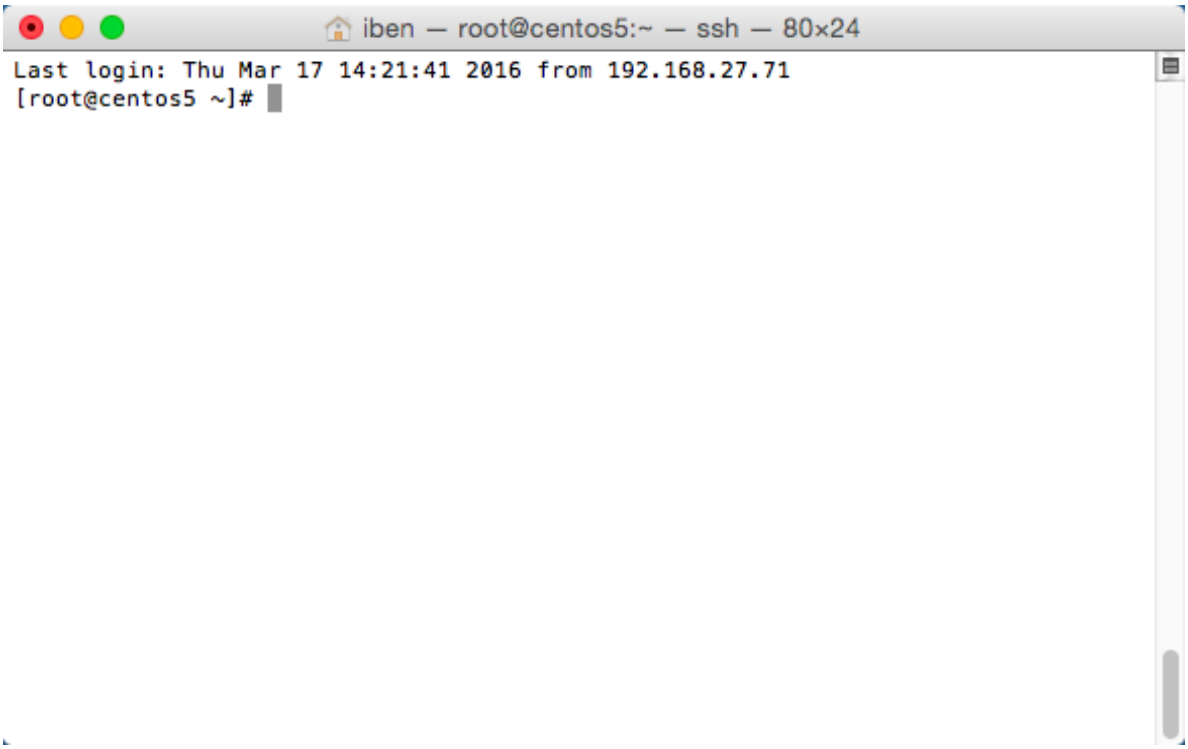
如提示需要输入密码，请输入该主机帐户的密码，按回车键（Enter）。

图 14-42: 通过命令行终端选择主机帐户



登录目标主机进行运维操作，如图 *14-43:* 通过命令行终端登录目标主机所示。

图 14-43: 通过命令行终端登录目标主机



14.3.4.1.3 通过远程桌面连接app的菜单方式登录目标主机进行运维

背景信息

本章节以远程桌面连接app为例，通过RDP协议登录目标主机进行运维。您可以参考本章节中的操作步骤使用其它app登录RDP协议的主机帐户。

操作步骤

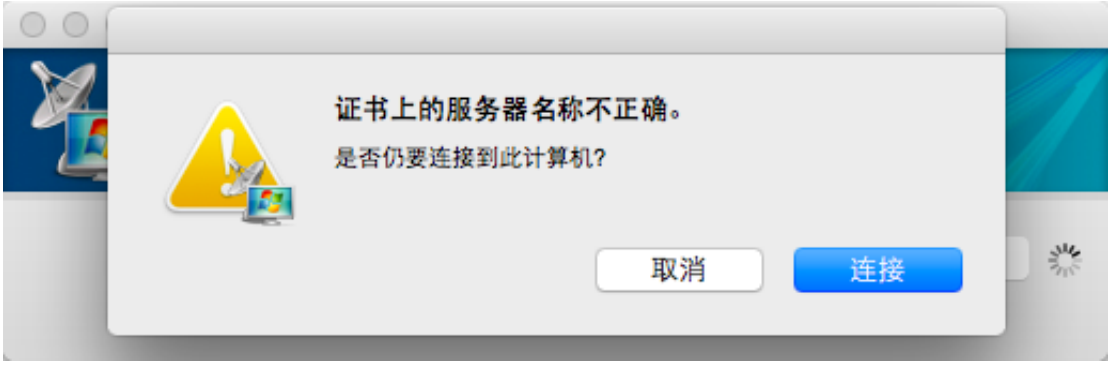
1. 打开远程桌面连接app，输入<云盾堡垒机系统IP>:63389，单击**连接**，如图 *14-44:* 通过远程桌面连接登录云盾堡垒机系统所示。

> **说明**：
> 其中，<云盾堡垒机系统的*IP*>指代云盾堡垒机系统的IP地址，请根据实际情况输入。

图 14-44: 通过远程桌面连接登录云盾堡垒机系统

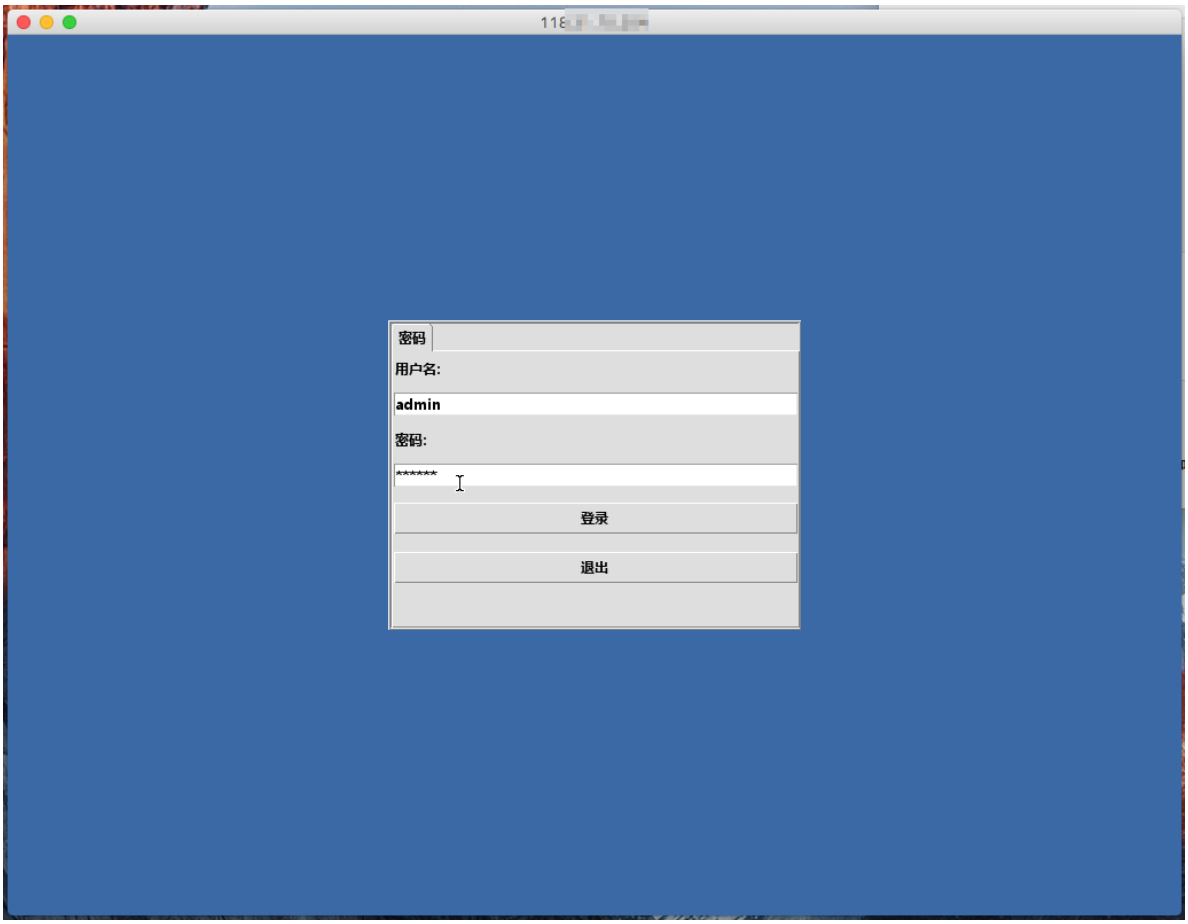
2. 在**是否仍要连接此计算机**？对话框中，单击**连接**，如图 *14-45:* 通过远程桌面连接连接云盾堡垒机系统所示。

图 14-45: 通过远程桌面连接连接云盾堡垒机系统



3. 在云盾堡垒机系统登录窗口，输入云盾堡垒机系统的用户名和密码，单击**登录**，如图 *14-46:* 登录云盾堡垒机系统所示。

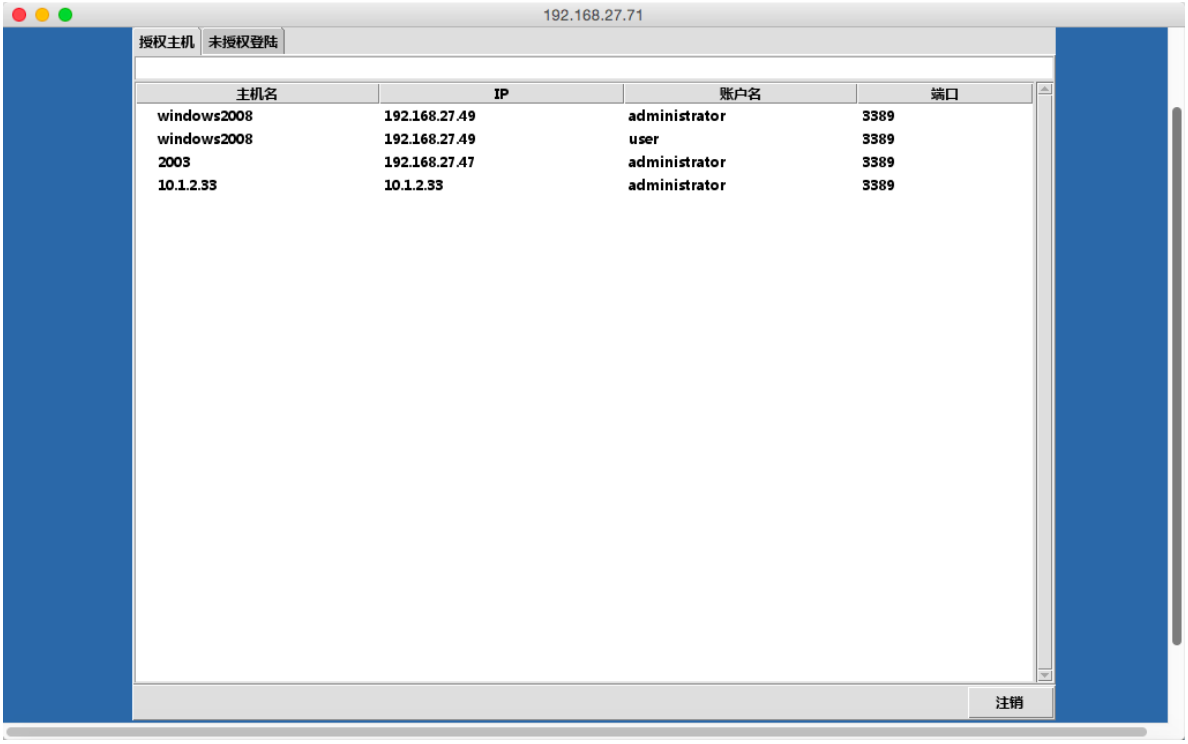
图 14-46: 登录云盾堡垒机系统



4. 在资产管理界面，双击选择已授权的主机资产，或者通过搜索框搜索主机资产，如图 *14-47: 通过远程桌面连接选择主机资产*所示。

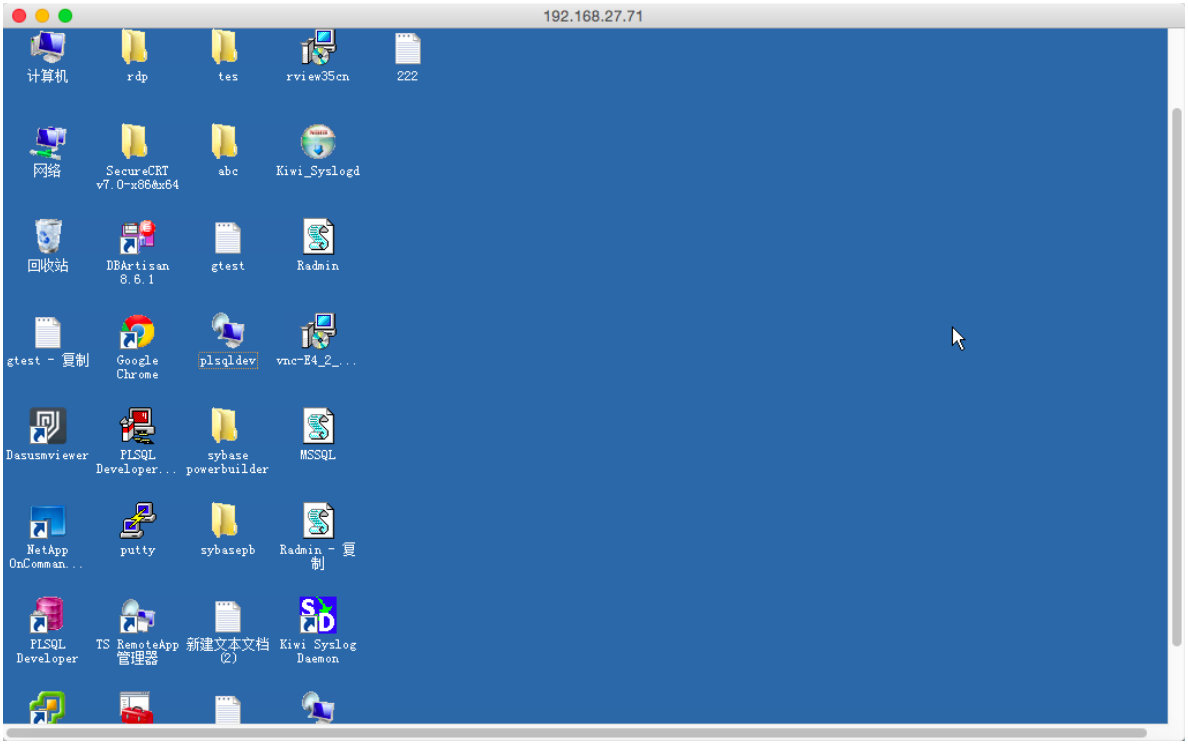
> **说明**：
> 如提示需要输入密码，请输入该主机帐户的密码，单击登录键。

图 14-47: 通过远程桌面连接选择主机资产



登录目标主机进行运维操作，如图 *14-48:* 通过远程桌面连接登录目标主机所示。

图 14-48: 通过远程桌面连接登录目标主机



14.3.4.2 Windows系统客户端运维操作指南

14.3.4.2.1 准备工作

在使用Windows系统客户端登录云盾堡垒机系统进行主机运维操作前，请确保已完成下列准备工作：

- 本地已安装支持SSH协议的运维工具，例如PuTTY、SecureCRT、Xshell等工具。
- 本地已安装支持RDP协议的运维工具，例如Windows系统自带的远程桌面连接工具。
- 本地已安装支持SFTP协议的运维工具，例如WinSCP、XFTP、FlashFXP等工具。
- 本地已安装支持FTP协议的运维工具，例如XFTP、FlashFXP等工具。
- 确保Windows系统客户端与云盾堡垒机系统的端口正常连通，主要包括以下端口：
  - 60022：用于访问SSH、Telnet、SFTP协议的主机。
  - 63389：用于访问RDP协议的主机。
  - 60021：用于访问FTP协议的主机。
- 确保云盾堡垒机系统与目标主机的运维端口正常连通，例如SSH协议及端口、RDP协议及端口。

说明：

SFTP、FTP协议的主机账号和密码必须设置为自动登录。通过客户端方式进行SFTP、FTP协议主机运维时，主机帐号和密码必须已在云盾堡垒机系统中配置，不支持手动登录。

14.3.4.2.2 通过SSH工具登录目标主机进行运维

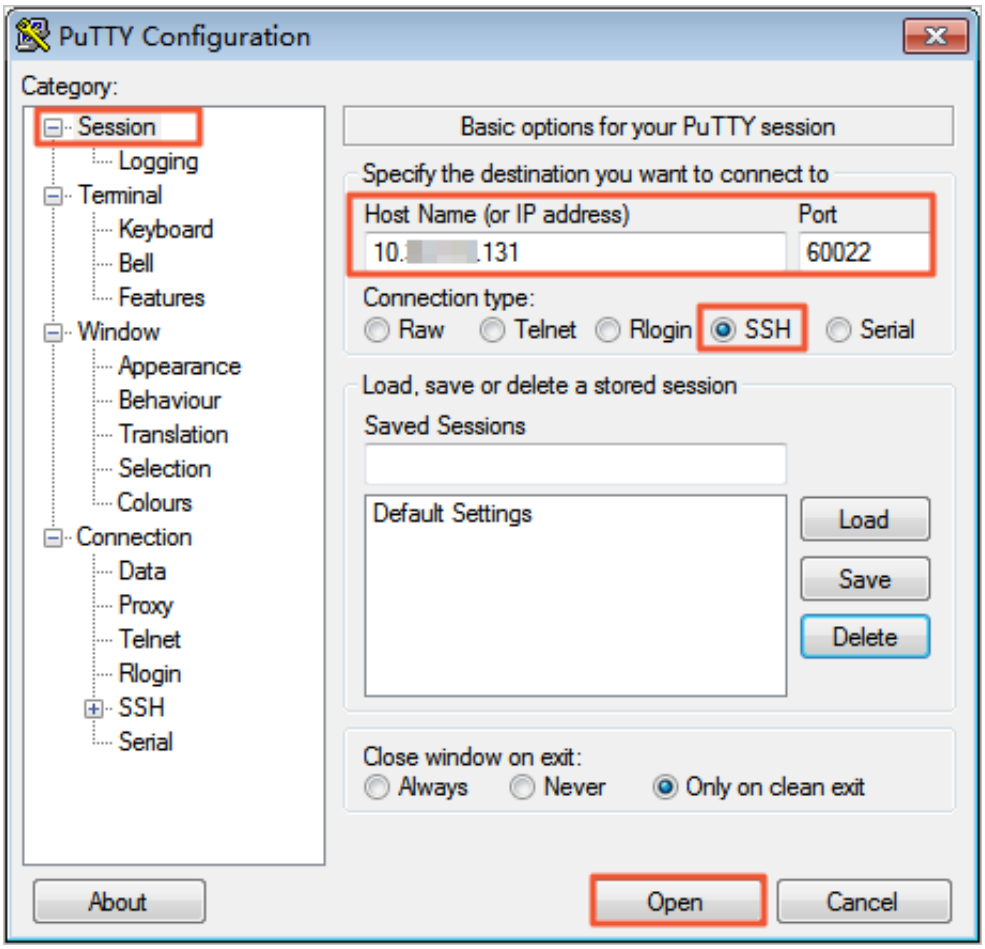
背景信息

本章节以PuTTY工具为例，通过SSH协议登录目标主机进行运维。您可以参考本章节中的操作步骤使用其它运维工具登录SSH、Telnet协议的主机帐户。

操作步骤

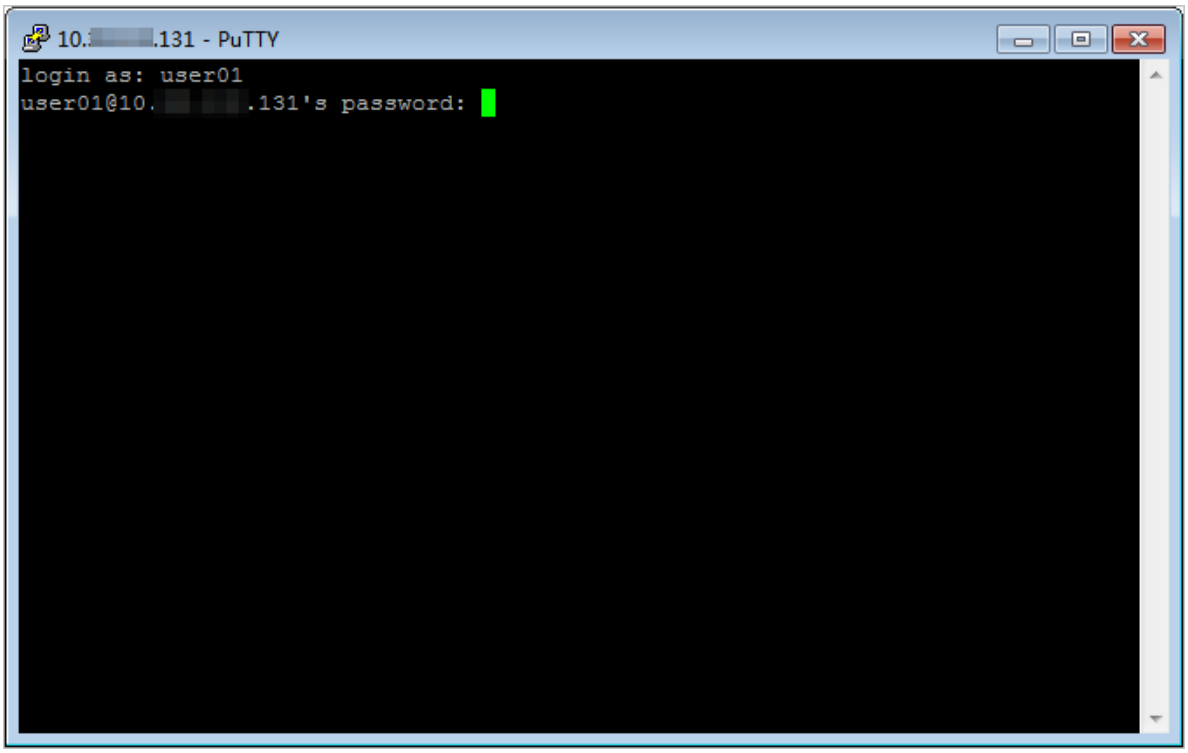
1. 打开PuTTY工具，在登录窗口中输入云盾堡垒机系统的IP和端口号（60022），单击**Open**，如图 *14-49:* 连接云盾堡垒机所示。

图 14-49: 连接云盾堡垒机



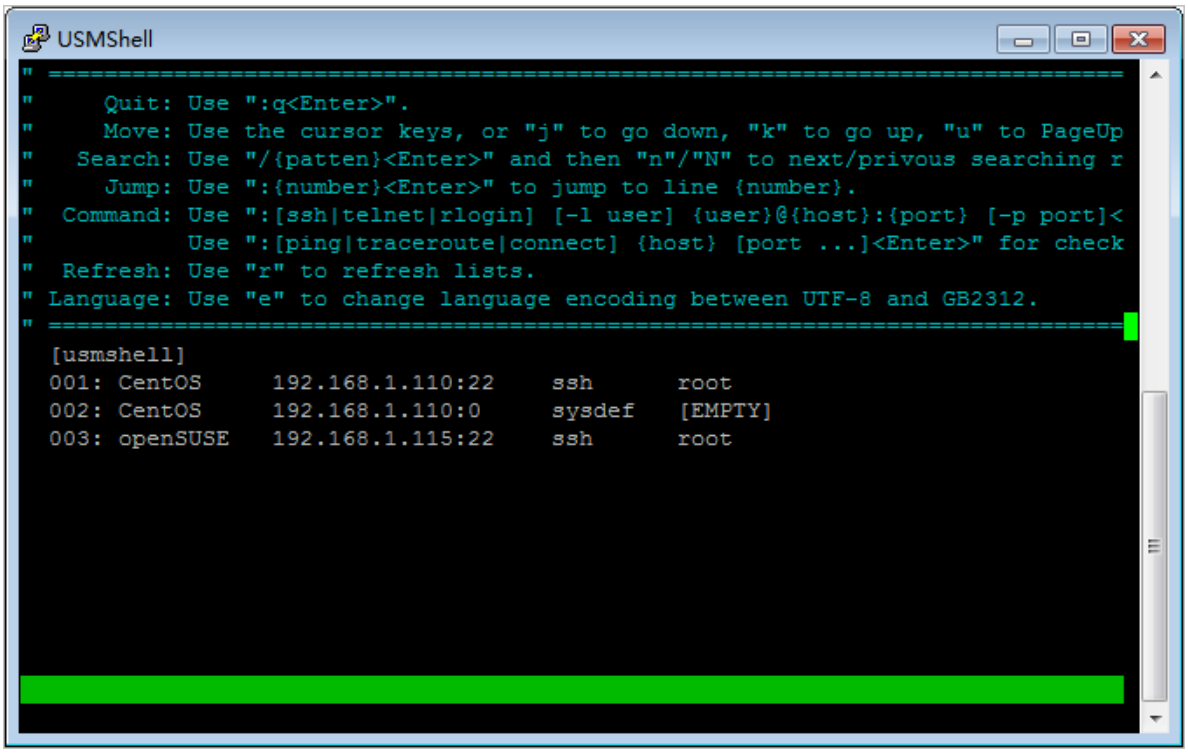
2. 输入云盾堡垒机系统的用户名和密码，按回车键（Enter），如图 *14-50: 登录云盾堡垒机*所示。

图 14-50: 登录云盾堡垒机



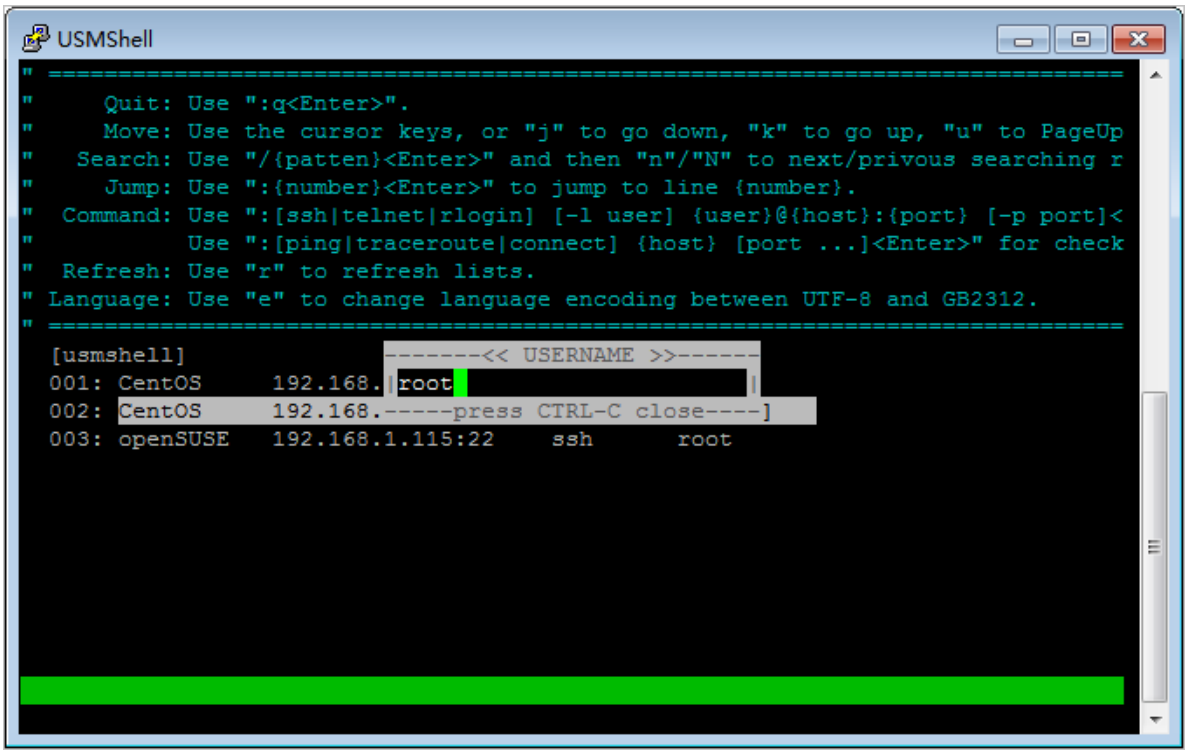
3. 进入资产管理界面，通过上下键选择已授权的主机资产，按回车键（Enter），如图 *14-51: 选择主机资产*所示。

图 14-51: 选择主机资产



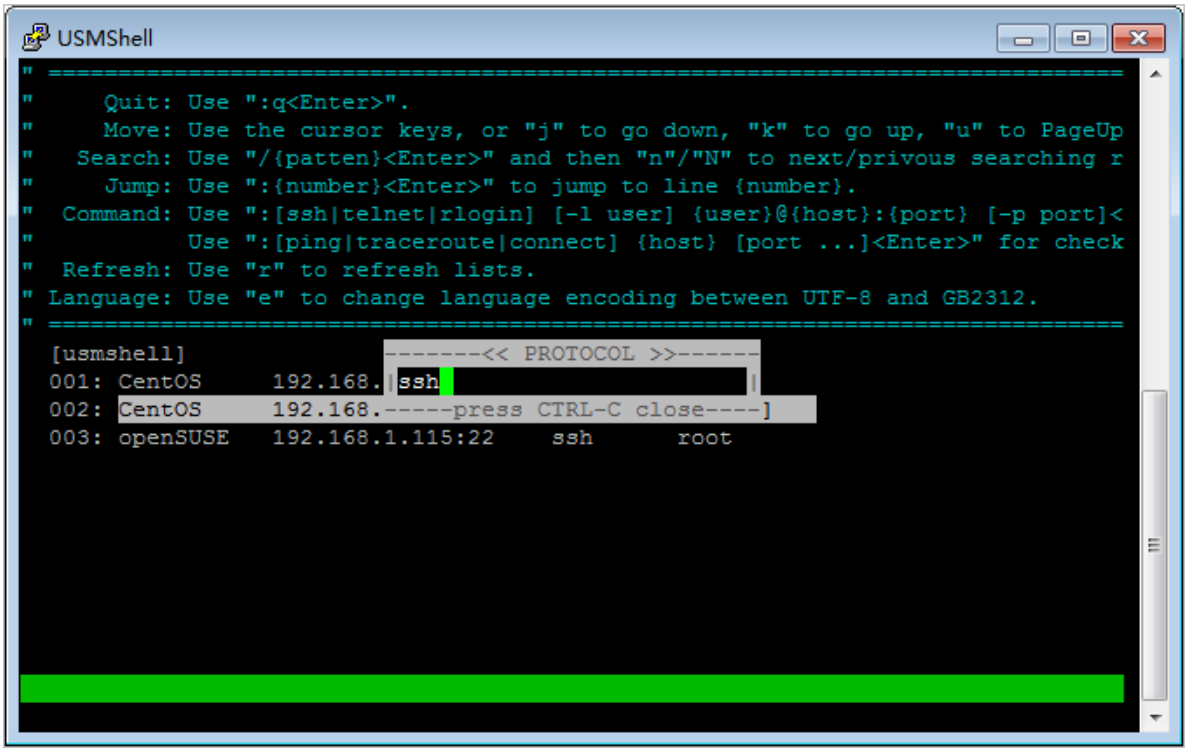
4. 在**USERNAME**中输入主机帐户，按回车键（Enter），如图 *14-52:* 输入主机帐户所示。

图 14-52: 输入主机帐户



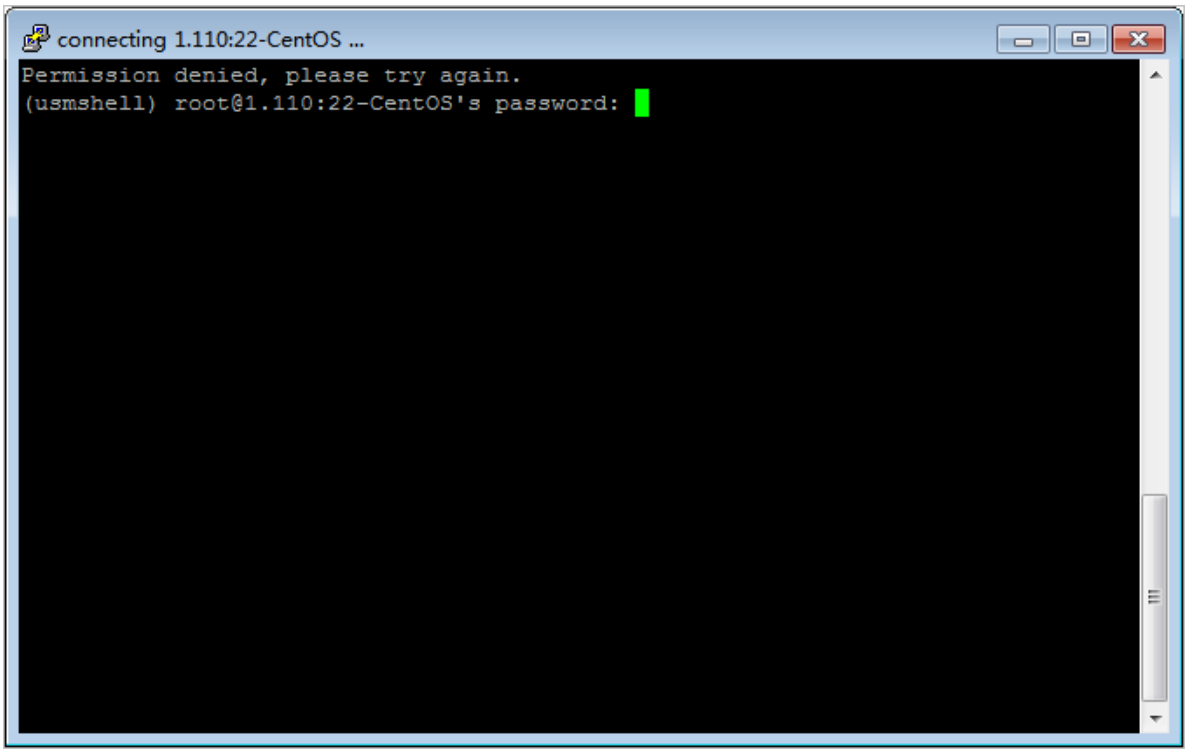
5. 在**PROTOCOL**中，输入ssh，按回车键（Enter），如图 *14-53: 输入SSH协议*所示。

图 14-53: 输入SSH协议



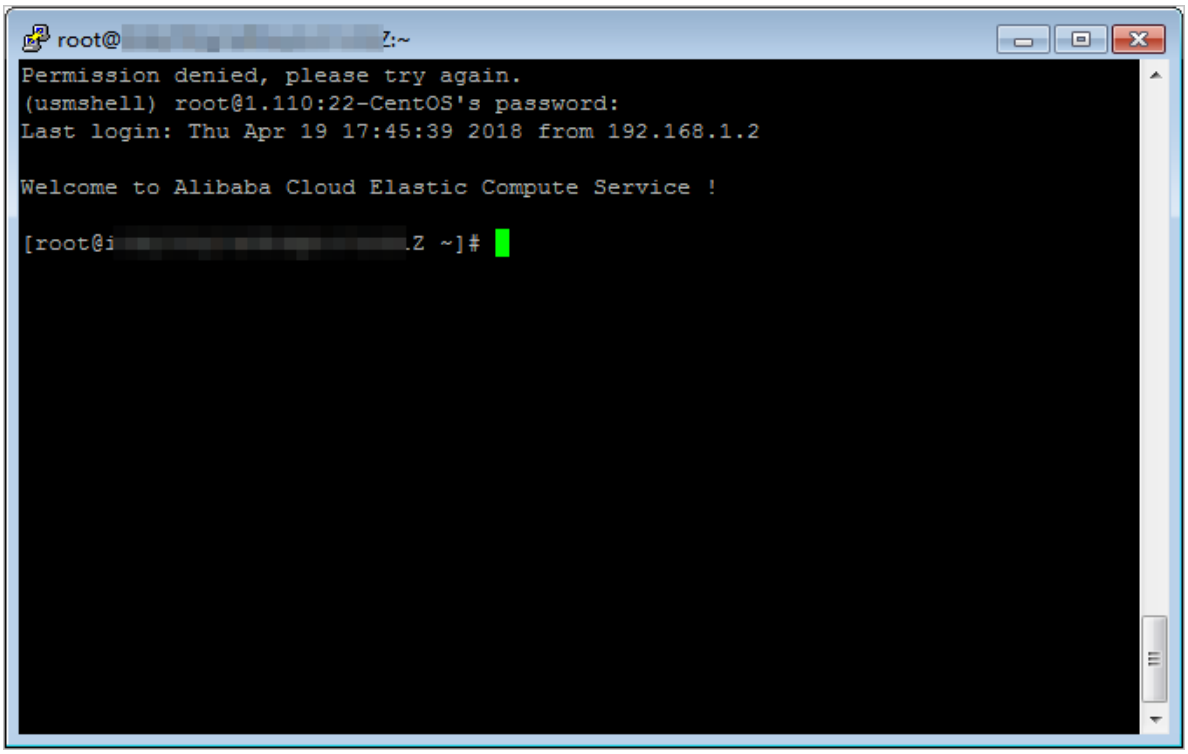
6. 在主机登录界面，输入主机帐户的密码，按回车键（Enter），如图 *14-54: 输入主机帐户密码*所示。

图 14-54: 输入主机帐户密码



登录目标主机进行运维操作，如图 *14-55: 通过PuTTY工具登录目标主机*所示。

图 14-55: 通过PuTTY工具登录目标主机



14.3.4.2.3 通过远程桌面连接工具的菜单方式登录目标主机进行运维

背景信息

本章节以远程桌面连接（MSTSC）工具为例，通过RDP协议登录目标主机进行运维。您可以参考本章节中的操作步骤使用其它运维工具登录RDP协议的主机帐户。

操作步骤

1. 打开远程桌面连接工具，输入<云盾堡垒机系统IP>:63389，单击**连接**，如图 *14-56:* 通过远程桌面连接工具登录云盾堡垒机系统所示。

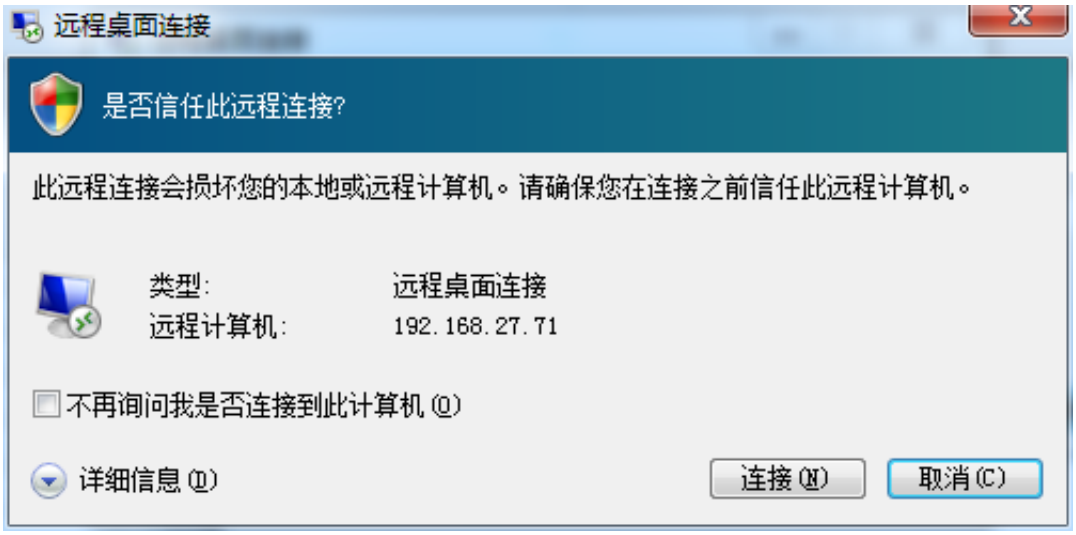
   说明：
   其中，<云盾堡垒机系统*IP*>指代云盾堡垒机系统的IP地址，请根据实际情况输入。

   图 14-56: 通过远程桌面连接工具登录云盾堡垒机系统

2. 在**是否信任此远程连接**？对话框中，单击**连接**，如图 *14-57:* 通过远程桌面连接工具连接云盾堡垒机系统所示。

图 14-57: 通过远程桌面连接工具连接云盾堡垒机系统

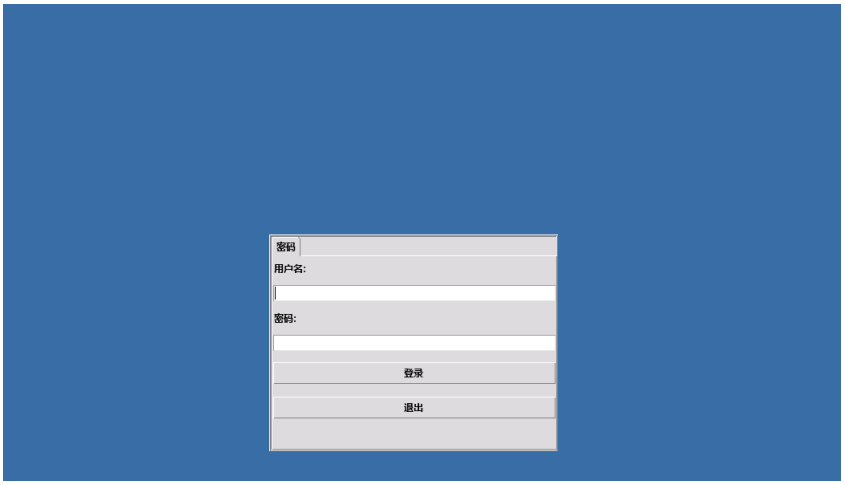


3. 在**无法验证次远程计算机的身份。是否仍要连接**？对话框中，单击**是**，如图 *14-58:* 通过远程桌面连接工具连接云盾堡垒机系统所示。

图 14-58: 通过远程桌面连接工具连接云盾堡垒机系统

4. 在云盾堡垒机系统登录窗口，输入云盾堡垒机系统的用户名和密码，单击**登录**，如图 *14-59: 登录云盾堡垒机系统*所示。

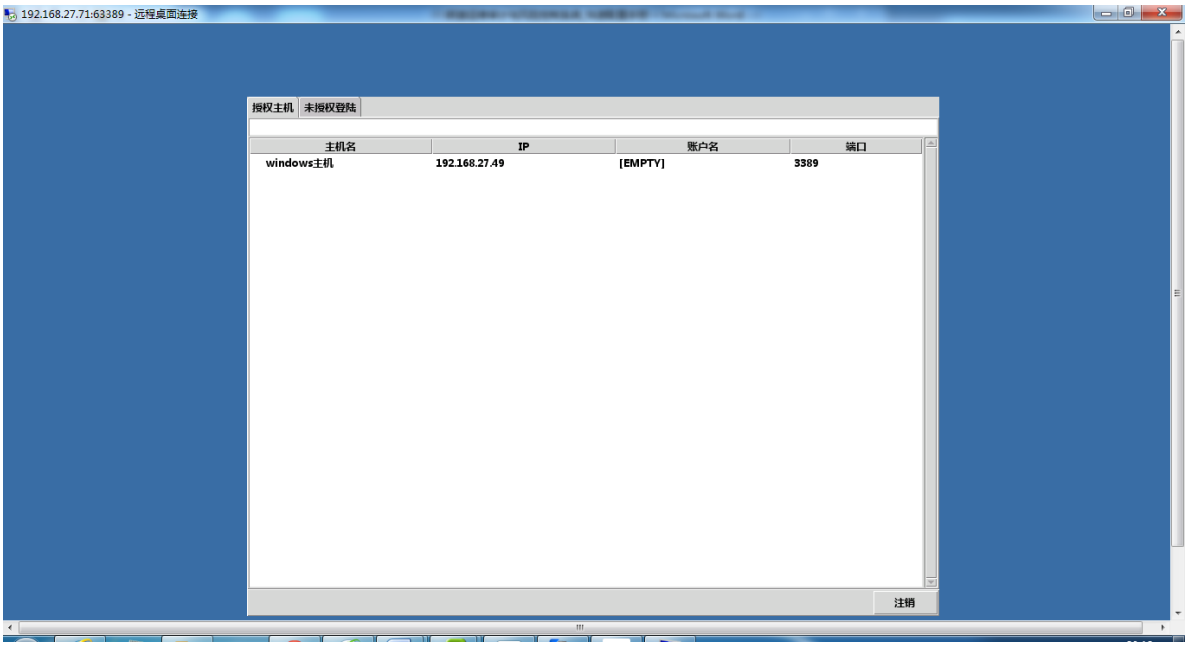
图 14-59: 登录云盾堡垒机系统



5. 在资产管理界面，双击选择已授权的主机资产，或者通过搜索框搜索主机资产，如图 *14-60: 通过远程桌面连接选择主机资产*所示。

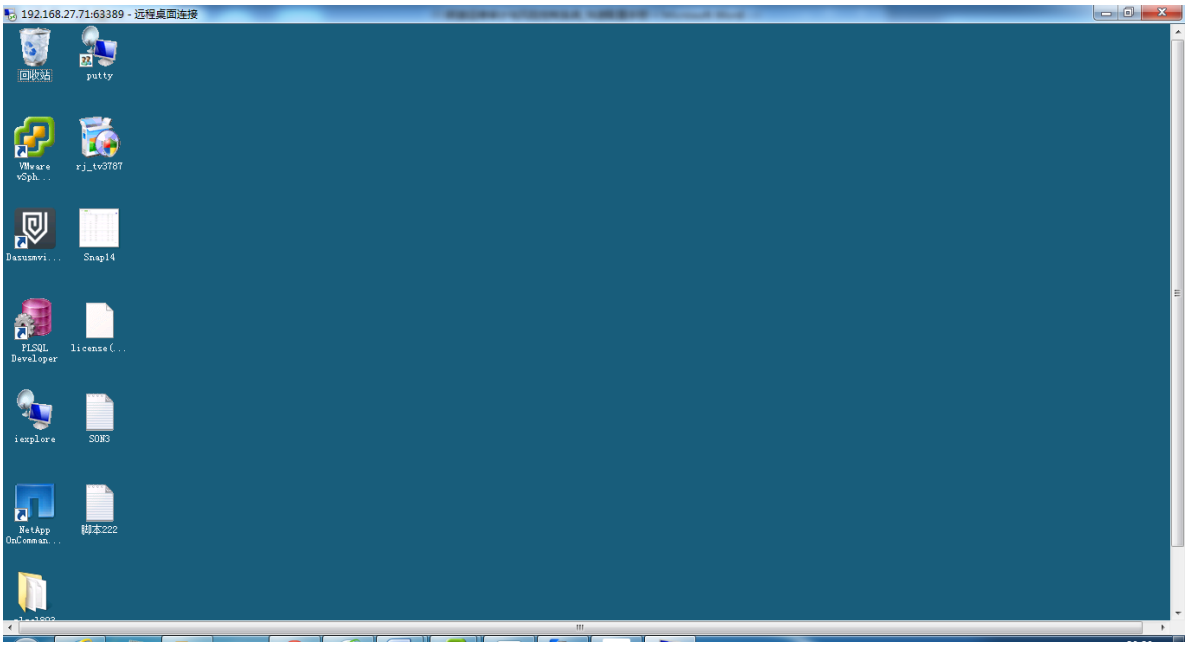
> **说明**：
> 如提示需要输入主机用户名和密码，请输入该主机的用户名和密码，单击登录键。

图 14-60: 通过远程桌面连接选择主机资产



登录目标主机进行运维操作，如图 *14-61: 通过远程桌面连接登录目标主机*所示。

图 14-61: 通过远程桌面连接登录目标主机



14.3.4.2.4 通过WinSCP工具登录目标主机进行运维

背景信息

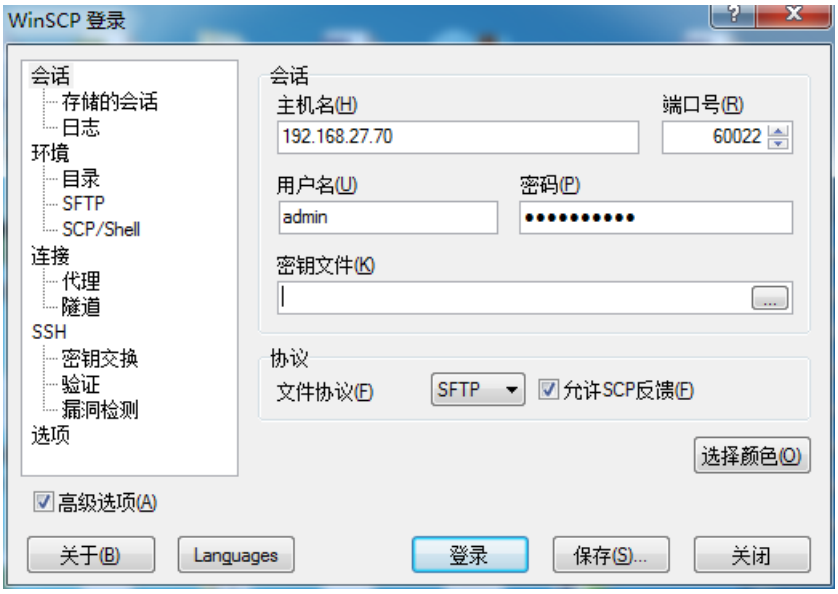
本章节以WinSCP工具为例，通过SFTP协议登录目标主机进行运维。您可以参考本章节中的操作步骤使用其它运维工具登录SFTP协议的主机帐户。

> **说明**：
> SFTP协议的主机账号和密码必须设置为自动登录。

操作步骤

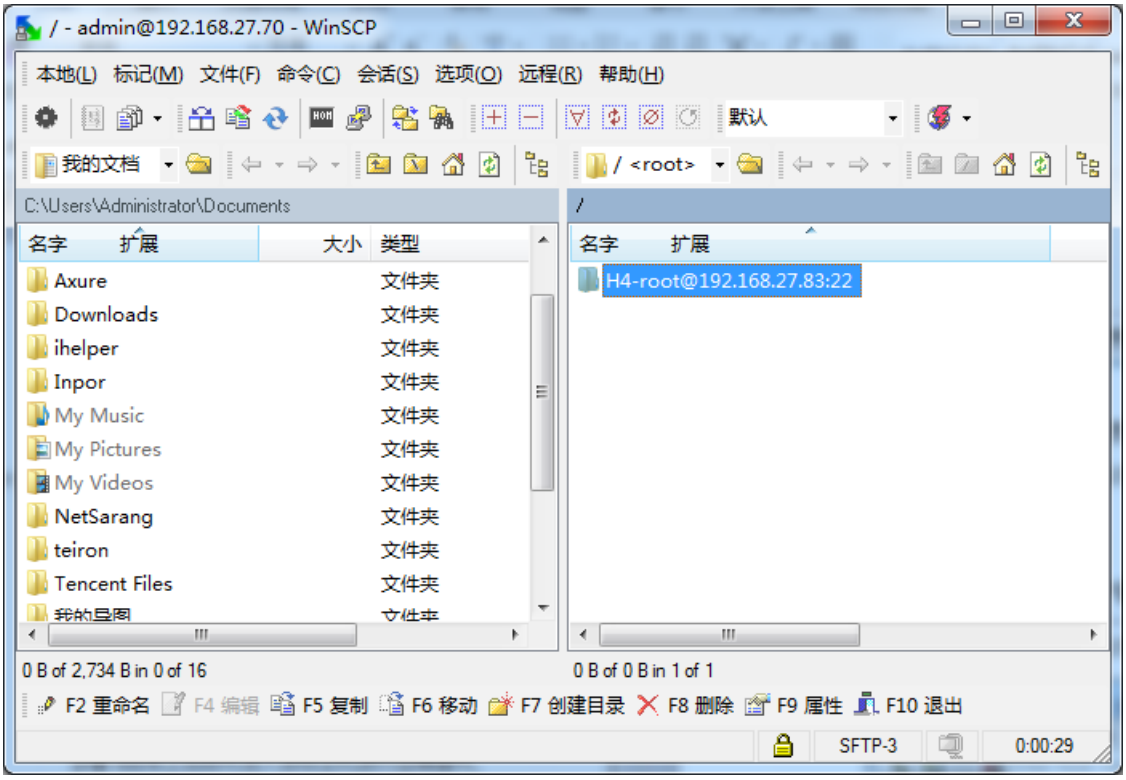
1. 打开WinSCP工具，在登录窗口中输入云盾堡垒机系统的IP、端口号（60022）、用户名、密码，单击**登录**，如图 *14-62: 通过WinSCP工具登录云盾堡垒机系统*所示。

图 14-62: 通过WinSCP工具登录云盾堡垒机系统



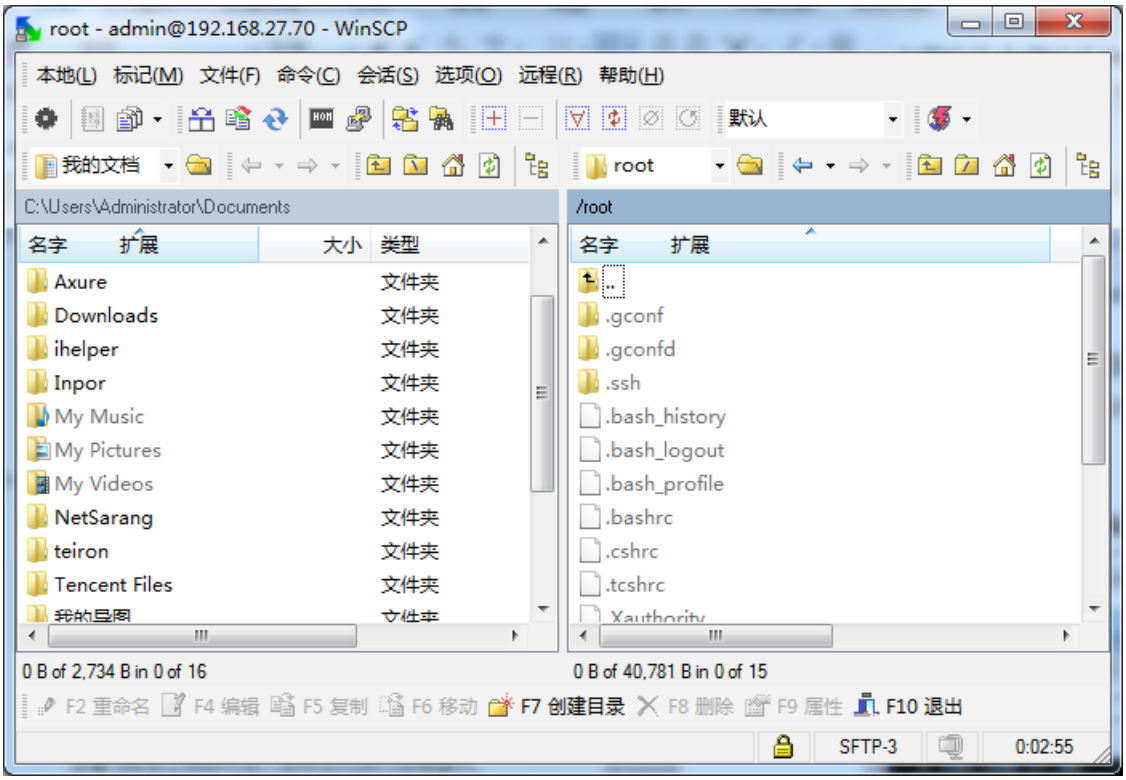
2. 在右侧的主机列表中，双击已授权的主机资产，进入该主机的文件目录，如图 *14-63: 通过WinSCP工具选择主机资产*所示。

图 14-63: 通过WinSCP工具选择主机资产



登录目标主机进行文件传输操作，如图 *14-64: 通过WinSCP工具操作目标主机*所示。

图 14-64: 通过WinSCP工具操作目标主机



14.3.4.2.5 通过XFTP工具登录目标主机进行运维

背景信息

本章节以XFTP工具为例，通过FTP协议登录目标主机进行运维。您可以参考本章节中的操作步骤使用其它运维工具登录FTP协议的主机帐户。

说明：

FTP协议的主机账号和密码必须设置为自动登录。

操作步骤

1. 登录云盾堡垒机系统。
2. 在页面右上角，单击用户名，选择**查看个人信息**，如图 *14-65:* 查看个人信息所示。

图 14-65: 查看个人信息

3. 在**个人信息**页面，选择**CS登录口令**页签，设置一个CS登录口令，单击**保存更改**，如图 *14-66: 设置CS登录口令*所示。

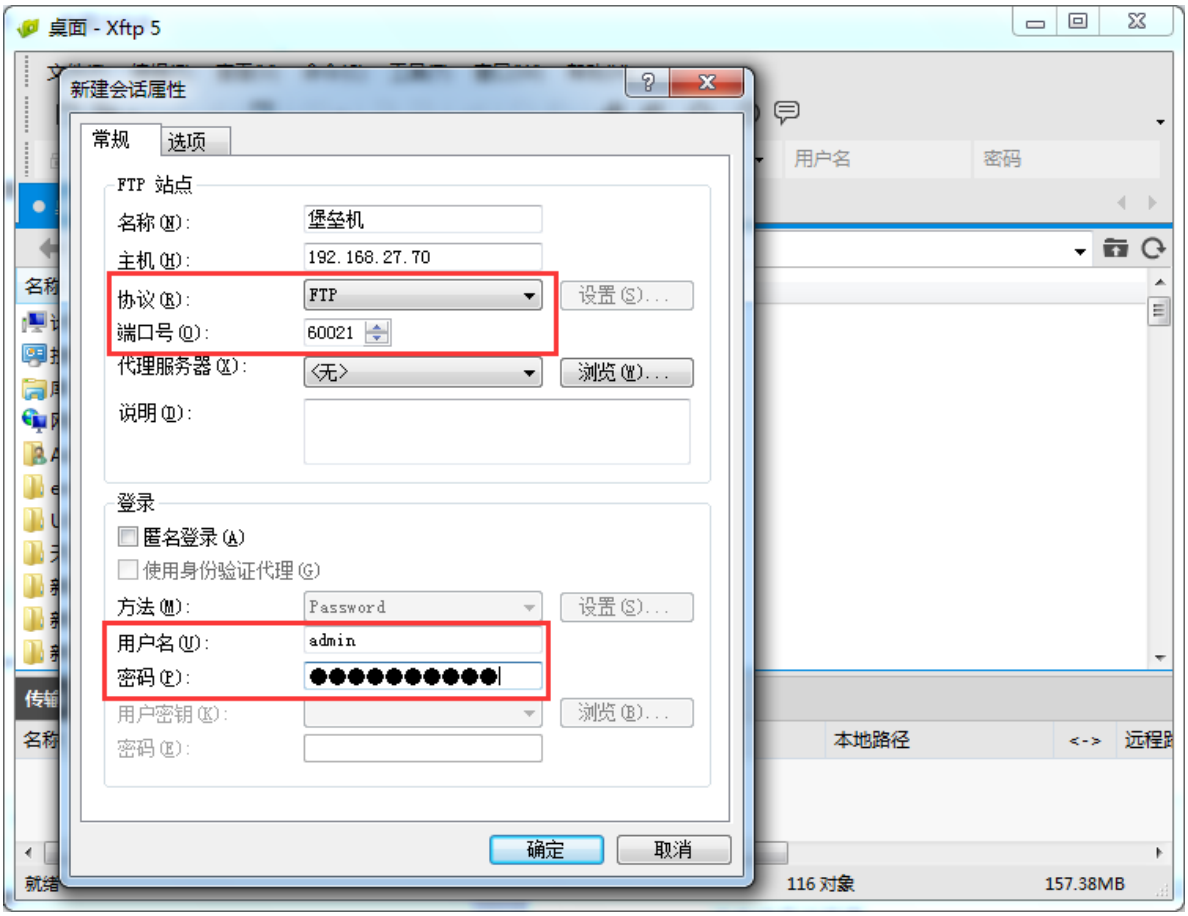
> **说明**：
> CS登录口令用于以FTP客户端登录系统。

图 14-66: 设置CS登录口令

4. 打开XFTP工具，在登录窗口中输入云盾堡垒机系统的IP、端口号（60021）、用户名、CS登录口令，选择FTP协议，单击**确定**，如图 *14-67: 通过XFTP工具登录云盾堡垒机*所示。

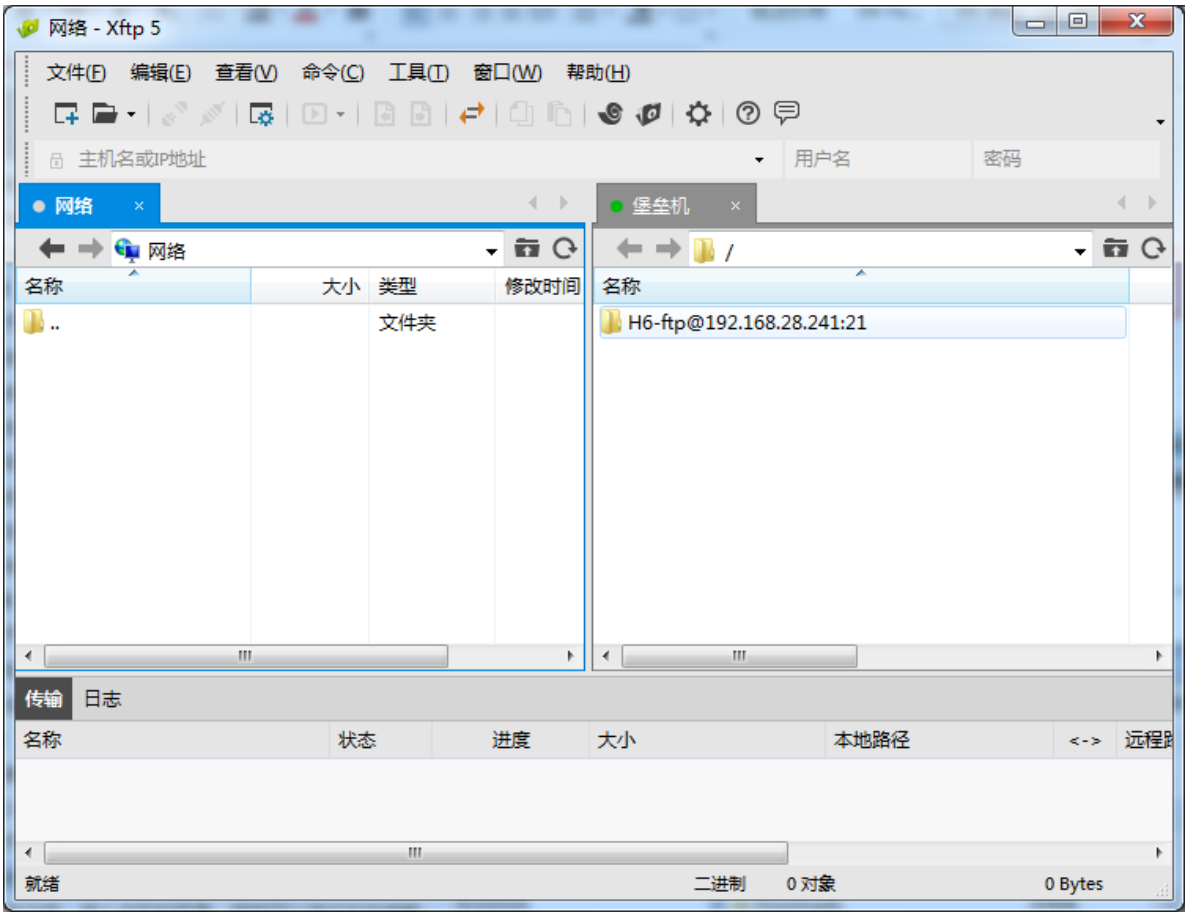
> **说明**：
> 此处的密码需填写在上述步骤中设置的CS登录口令。

图 14-67: 通过XFTP工具登录云盾堡垒机



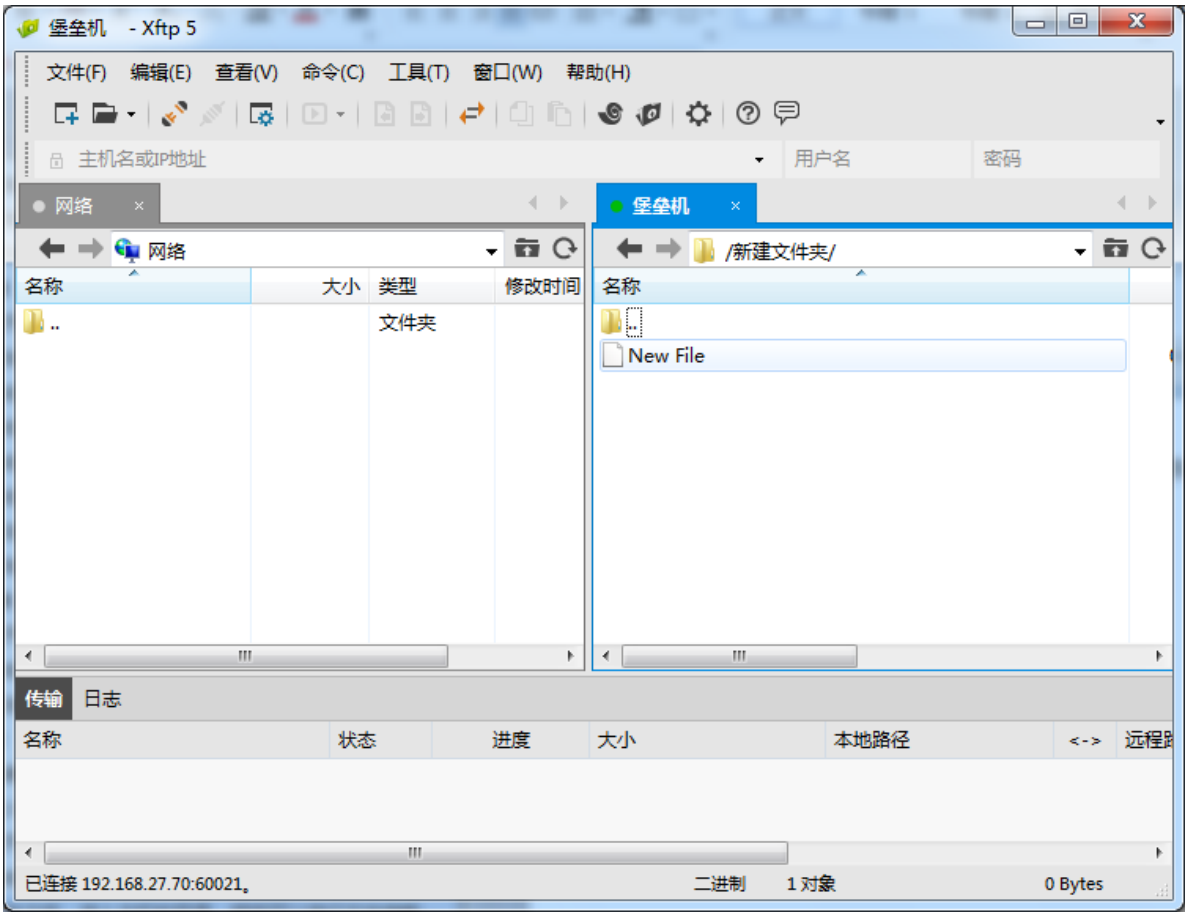
5. 在右侧的主机列表中，双击已授权的主机资产，进入该主机的文件目录，如*图 14-68: 通过XFTP工具选择主机资产*所示。

图 14-68: 通过XFTP工具选择主机资产



登录目标主机进行文件传输操作，如图 *14-69: 通过XFTP工具操作目标主机*所示。

图 14-69: 通过XFTP工具操作目标主机



14.4 审计管理员操作指南

14.4.1 登录云盾堡垒机系统

前提条件

请确认您所使用的客户端能够正常访问云盾堡垒机系统。

操作步骤

1. 打开Chrome浏览器。
2. 在地址栏中，输入云盾堡垒机系统的访问地址，按回车键（Enter），进入系统登录页面。
3. 在云盾堡垒机系统登录页面，输入审计管理员用户名、密码及验证码。

> **说明**：
> 审计管理员的用户名及密码是由超级管理员所创建的。

4. 单击**登录**。

首次登录成功后，审计管理员需要修改密码。

14.4.2 审计

审计功能用于审计管理员对主机的访问操作的日志进行审计。

14.4.2.1 会话审计

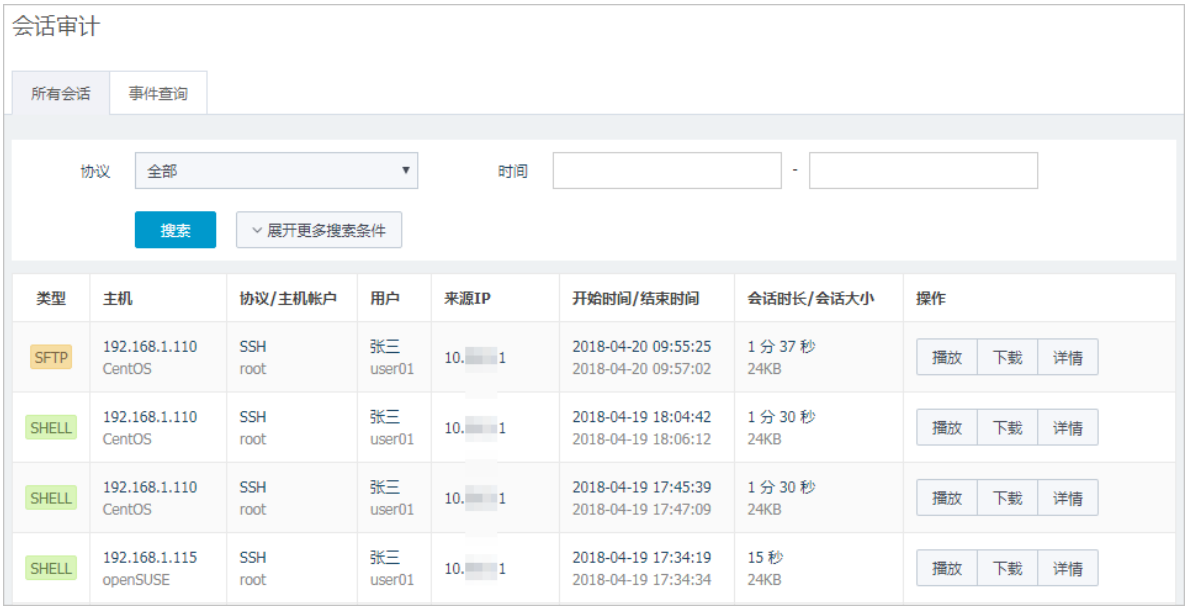
会话审计页面用于记录运维人员对主机操作过程的会话日志。

14.4.2.1.1 查看所有会话

操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**审计** > **会话审计**>页面，选择**所有会话**，查看字符、图形、文件、应用类型的会话审计日志，如图 *14-70: 查看所有会话*所示。

图 14-70: 查看所有会话



3. 选择会话日志，执行更多操作
   - 单击操作栏中的**详情**，可查看详细的会话信息，如图 *14-71: 查看会话详情*所示。

图 14-71: 查看会话详情

会话详情 ×

会话ID	caaa10ee5593a83d000000292f00000f		
时长	34秒	大小	569KB
开始时间	2015-07-01 16:43:41	结束时间	2015-07-01 16:44:15
用户	hehe	来源IP	192.168.50.246
来源MAC	00:50:56:8F:00:04	来源端口	50430
主机名称	RD-server	主机IP	10.[illegible]
主机帐户	administrator	协议	RDP
主机MAC	F4:EA:67:87:03:E7	主机端口	3389
会话备注			
审批人	-	操作	播放 下载

单击右上角关闭按钮，可返回**会话审计**页面。

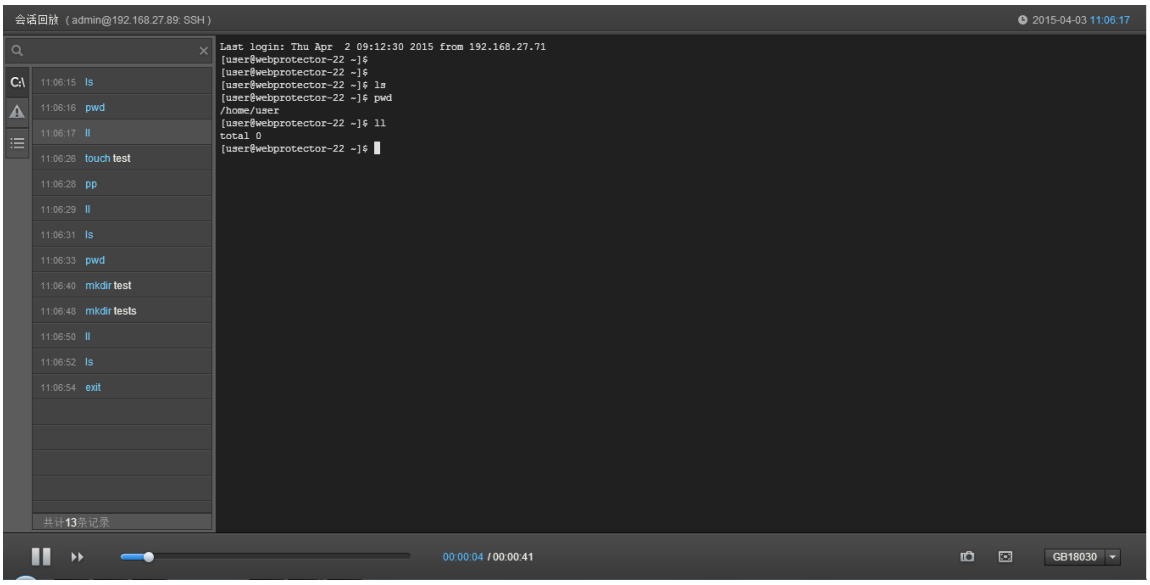
- 单击操作栏中的**下载**，可将会话文件下载到本地。会话文件下载完成后，可通过离线播放器进行播放。

> **说明**：
> 在本地播放会话文件需安装离线播放器和Adobe AIR 4.0工具。单击云盾堡垒机系统页面右上角的用户名，选择**工具下载**，可以下载离线播放器和Adobe AIR 4.0的安装程序。

- 单击操作栏中的**播放**，可通过Web方式查看会话审计回放。在线播放支持日志回放、命令记录、搜索等功能，如图 *14-72:* 查看会话审计回放所示。

> **说明**：
> 通过Web方式查看会话审计，须要在本地安装Flash Player才可在线播放。如果本地客户端未安装Flash Player，单击云盾堡垒机系统页面右上角的用户名，选择**工具下载**，下载并安装Flash Player 12。

图 14-72: 查看会话审计回放



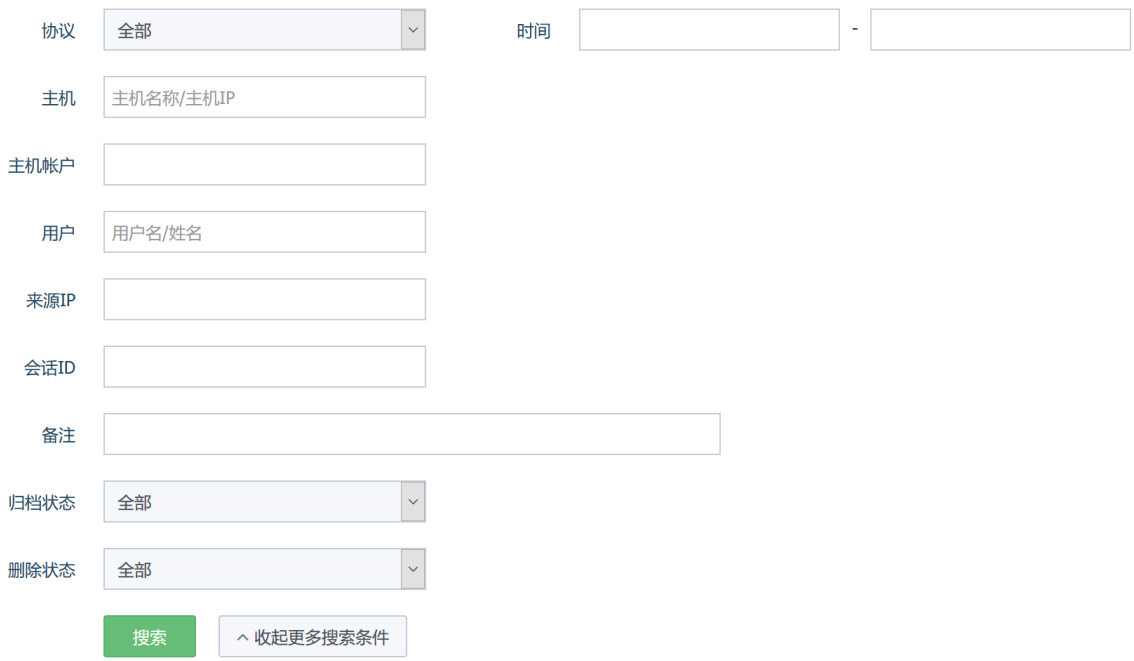
关闭Web页面，即可返回**会话审计**页面。

14.4.2.1.2 搜索审计会话

操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**审计** > **会话审计**页面，选择**所有会话**，单击**展开更多搜索条件**，如图 *14-73:* 会话审计搜索条件所示。

图 14-73: 会话审计搜索条件



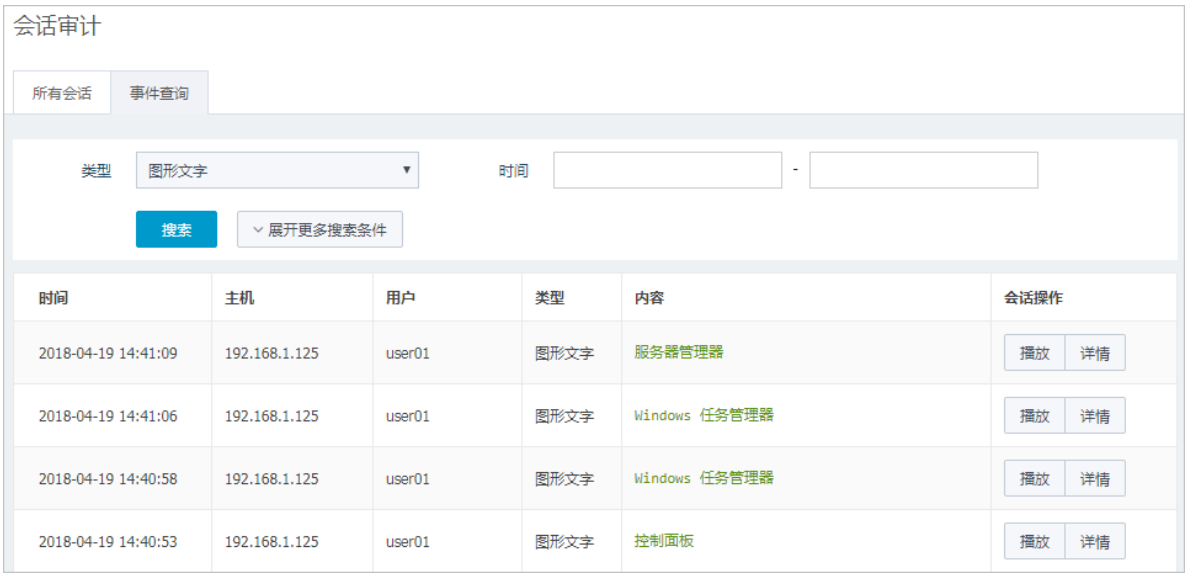
3. 根据需要设定搜索条件，单击**搜索**，查看符合条件的会话日志。

14.4.2.1.3 查询事件

操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**审计** > **会话审计**页面，选择**事件查询**，查看会话事件，如图 *14-74:* 查看运维事件所示。

图 14-74: 查看运维事件

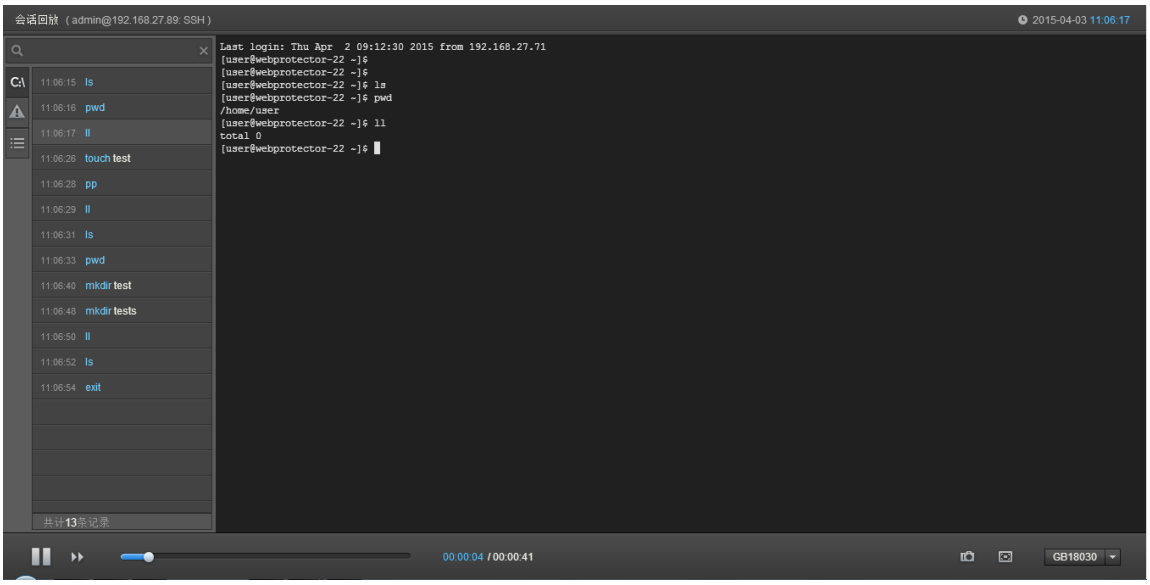


3. 选择会话事件，执行更多操作。

- 单击会话操作栏中的**详情**，可查看详细的会话信息。
- 单击会话操作栏中的**播放**，可通过Web方式查看会话事件回放。在线播放支持日志回放、命令记录、搜索等功能，如图 *14-75:* 查看会话审计回放所示。

> **说明**：
> 通过Web方式查看会话审计，须要在本地安装Flash Player才可在线播放。如果本地客户端未安装Flash Player，单击云盾堡垒机系统页面右上角的用户名，选择**工具下载**，下载并安装Flash Player 12。

图 14-75: 查看会话审计回放



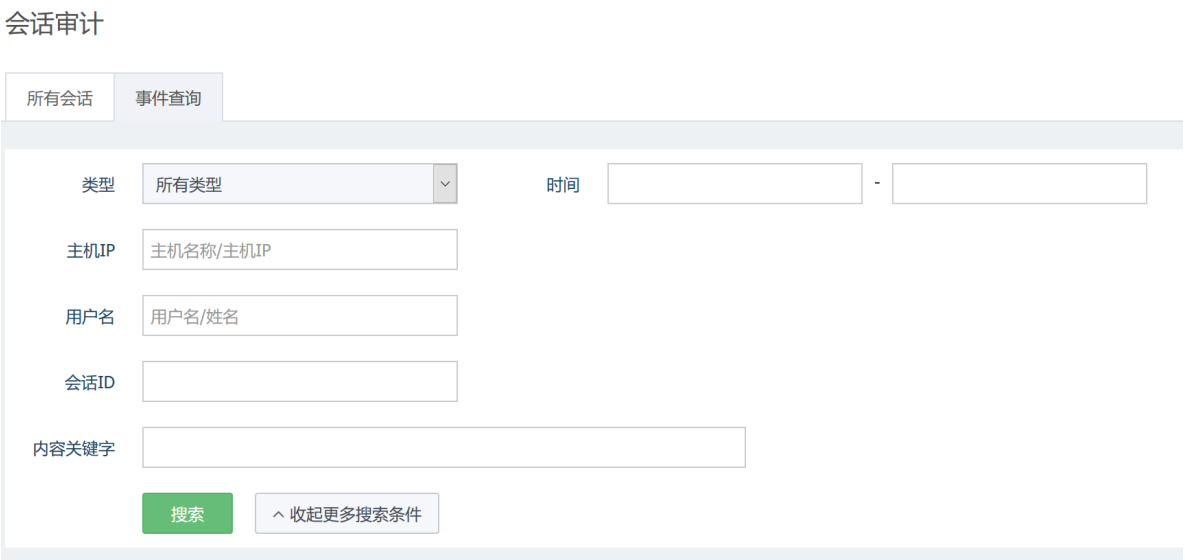
关闭Web页面，即可返回**会话审计**页面。

14.4.2.1.4 搜索事件

操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**审计** > **会话审计**页面，选择**事件查询**，单击**展开更多搜索条件**，如图 *14-76:* 事件查询搜索条件所示。

图 14-76: 事件查询搜索条件



3. 根据需要设定搜索条件，单击**搜索**，查看符合条件的事件会话。

14.4.2.2 审计规则

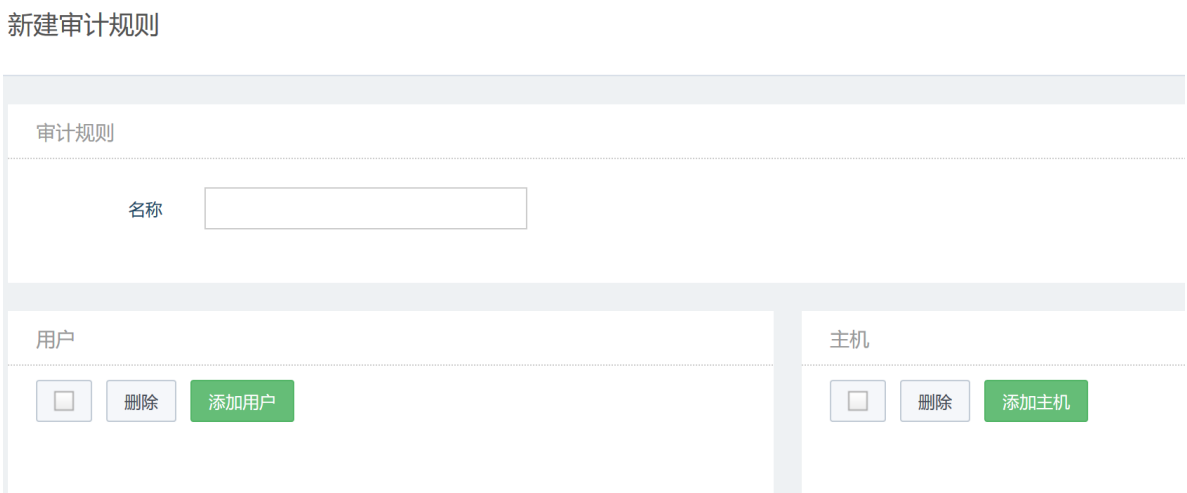
审计规则是创建审计管理员与主机之间的对应关系，代表某审计管理员具有审计某主机的权限。

14.4.2.2.1 添加审计规则

操作步骤

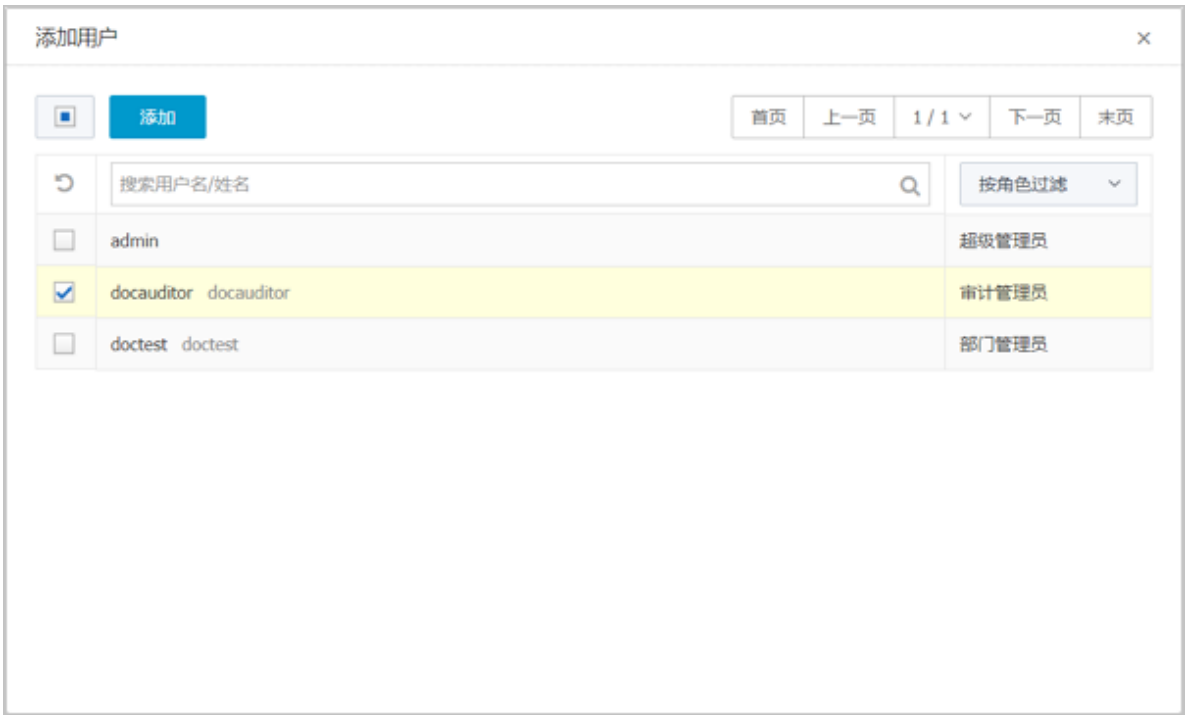
1. 登录云盾堡垒机系统。
2. 定位到**审计** > **审计规则**页面，选择**事件查询**，单击**新建审计规则**，打开**新建审计规则**页面，如图 *14-77: 新建审计规则*所示。

图 14-77: 新建审计规则



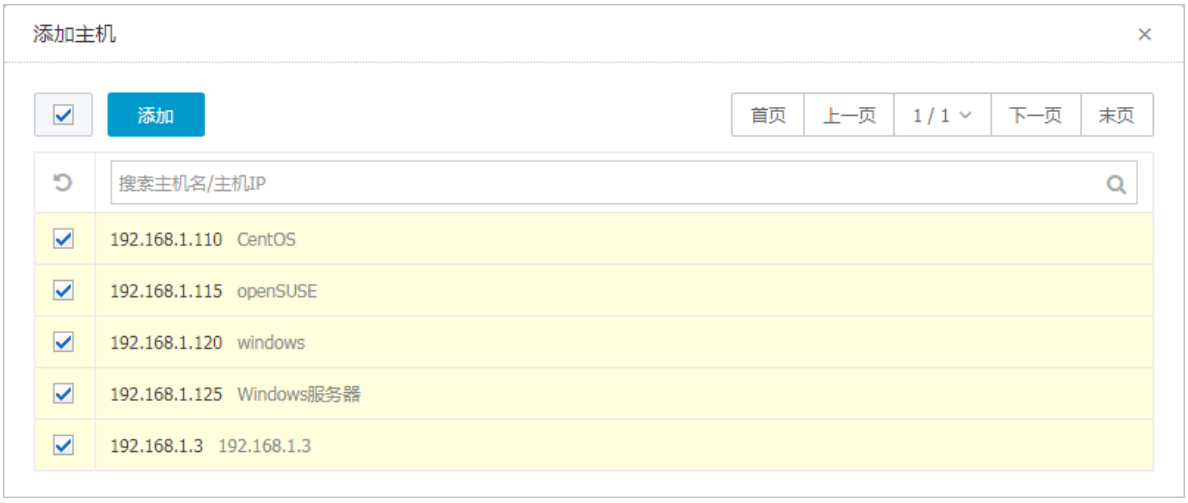
3. 单击**添加用户**，在**添加用户**对话框中勾选审计人员，单击**添加**，如图 *14-78: 添加审计管理员*所示。

图 14-78: 添加审计管理员



4. 单击**添加主机**，在**添加主机**对话框中勾选被审计的主机，单击**添加**，如图 *14-79: 添加被审计主机*所示。

图 14-79: 添加被审计主机



5. 填写审计规则名称，单击**创建审计规则**，即可通过该审计规则为选定的审计管理员赋予所选主机的审计权限。

   审计规则创建完成后，在**审计规则**页面，单击审计规则名称，可对该审计规则进行修改；勾选审计规则，单击上方**删除**，可删除该审计规则。

14.4.3 运维报表

运维报表用于统计当前用户的运维信息。

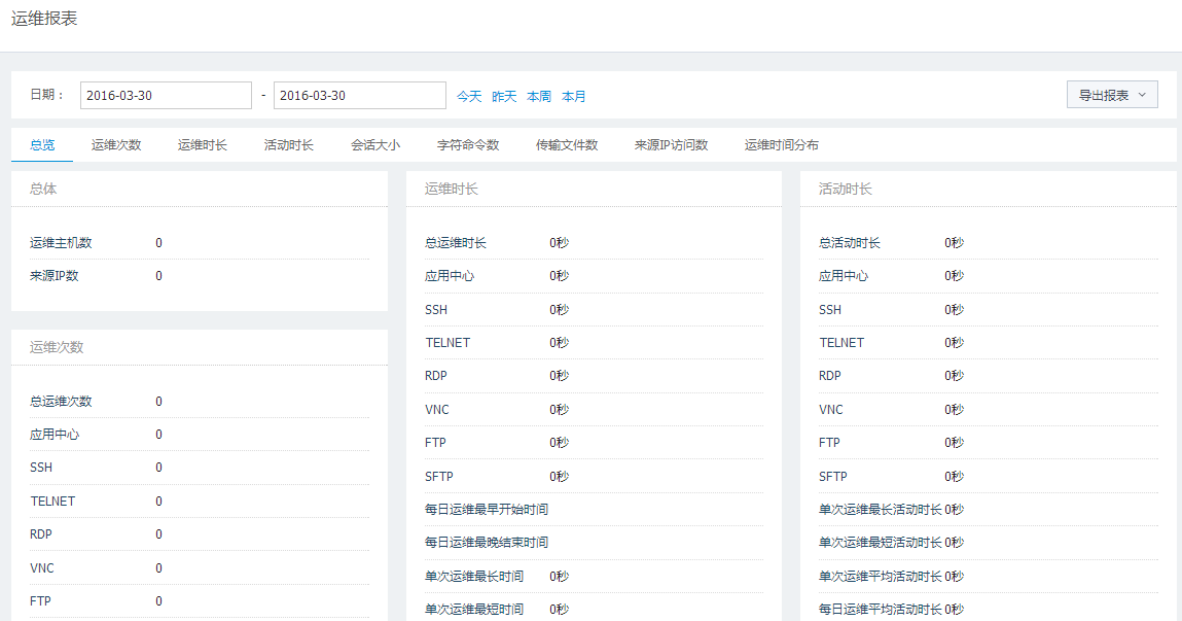
14.4.3.1 按时间范围查看运维报表

操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**运维** > **运维报表**页面，选择用户，设置时间范围，查看运维统计信息，如*图 14-80: 查看运维报表*所示。

> **说明**：
> 选择页签，可查看不同类型的运维统计信息。

图 14-80: 查看运维报表



3. 单击右上角**导出报表**，选择导出格式，可根据当前设置的用户、时间范围将报表以指定的格式导出到本地。

14.4.3.2 设置报表自动发送

操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**运维** > **运维报表**页面，单击页面右上角的报表自动发送。

3. 在**报表自动发送**对话框中，设置发送周期，选择报表文件格式，开启报表自动发送功能，单击**确定**，如图 *14-81: 设置报表自动发送*所示。

图 14-81: 设置报表自动发送

启用报表自动发送功能后，在每个周期开始时，系统将会自动生成上一周期的运维报表，并以邮件形式发送给部门管理员和审计管理员。

说明：
请确认相应的管理人员已在**用户信息**页面中设置邮箱信息。

14.5 系统管理员操作指南

14.5.1 登录云盾堡垒机系统

前提条件

请确认您所使用的客户端能够正常访问云盾堡垒机系统。

操作步骤

1. 打开Chrome浏览器。
2. 在地址栏中，输入云盾堡垒机系统的访问地址，按回车键（Enter），进入系统登录页面。
3. 在云盾堡垒机系统登录页面，输入系统管理员用户名、密码及验证码。

> **说明：**
> 系统管理员的用户名及密码是由超级管理员所创建的。

4. 单击**登录**。

   首次登录成功后，系统管理员需要修改密码。

14.5.2 系统管理

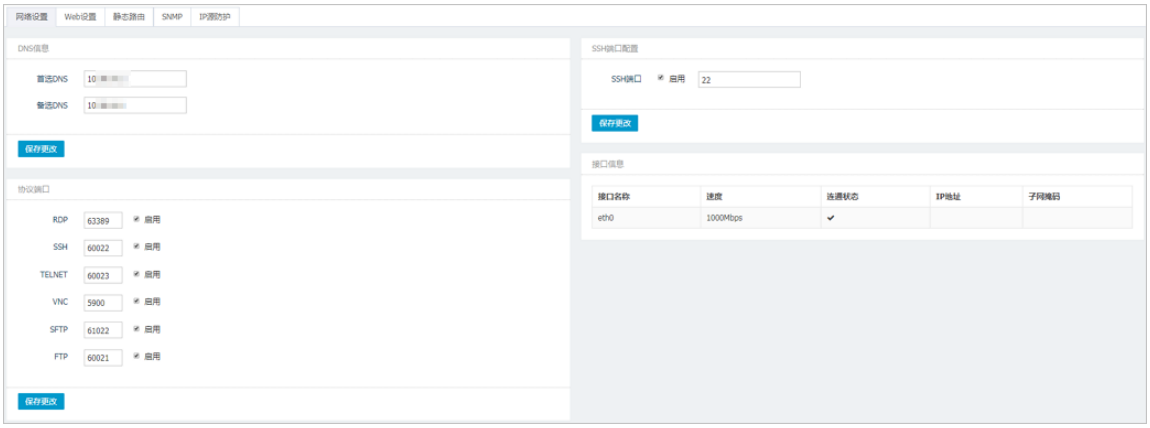
系统管理用于对云盾堡垒机系统自身配置进行管理。

14.5.2.1 管理网络相关设置

操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**系统** > **网络设置**页面。
3. 管理云盾堡垒机系统网络相关设置。
   - 选择**网络设置**页签，进行网络相关配置，如图 *14-82: 网络设置页签*所示。

     图 14-82: 网络设置页签

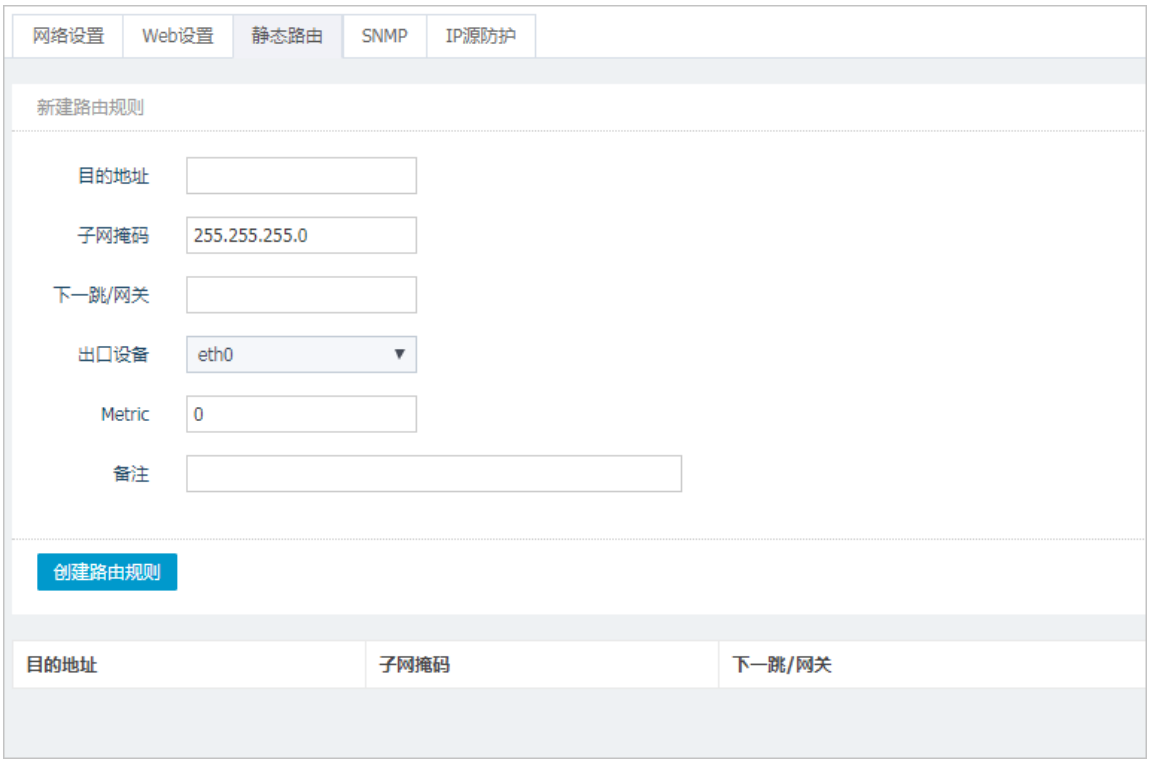
     

   - 选择**Web设置**页签，进行Web相关配置，如图 *14-83: Web设置页签*所示。

图 14-83: Web设置页签

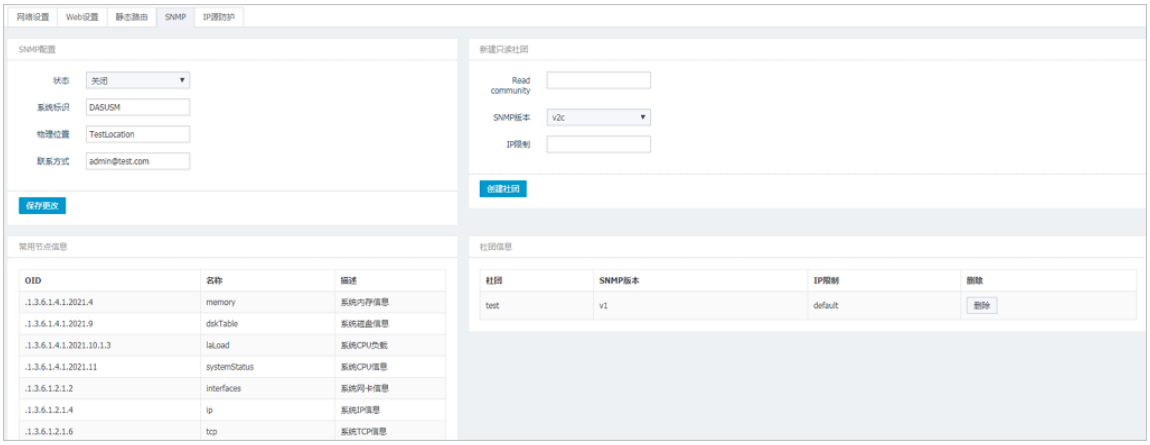
- 选择**静态路由**页签，设置静态路由规则，如图 *14-84:* 静态路由页签所示。

图 14-84: 静态路由页签



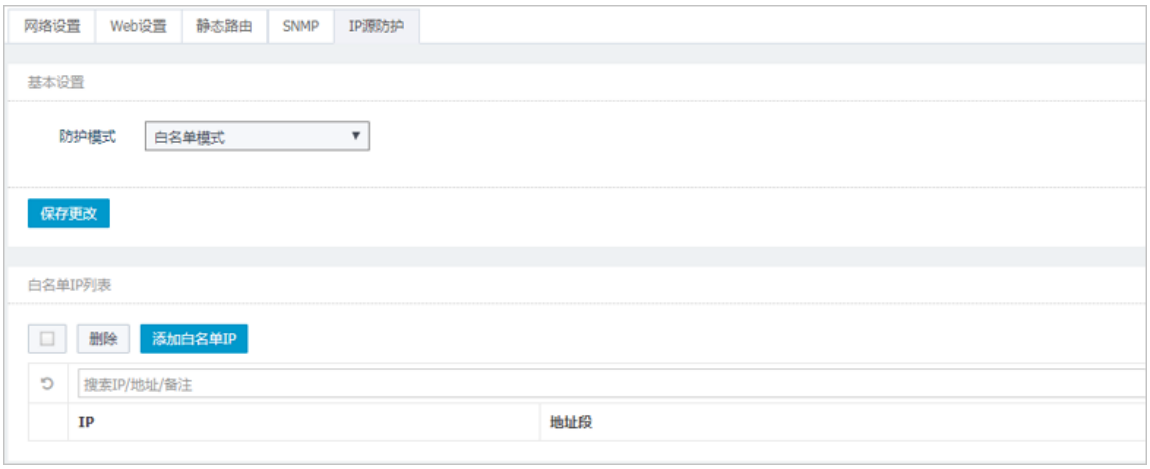
- 选择**SNMP**页签，设置简单网络管理协议及社团信息，如图 *14-85: SNMP页签*所示。

图 14-85: SNMP页签



- 选择**IP源防护**页签，选择防护模式并设置黑白名单IP列表，如图 *14-86: IP源防护页签*所示。

图 14-86: IP源防护页签



14.5.2.2 管理认证相关配置

操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**系统** > **认证管理**页面。
3. 管理云盾堡垒机系统登录认证相关配置。
   - 选择**安全设置**页签，进行登录安全相关配置，如图 *14-87:* 安全配置页签所示。

图 14-87: 安全配置页签

- 选择**远程认证**页签，进行远程认证相关设置，如图 *14-88:* 远程认证页签所示。

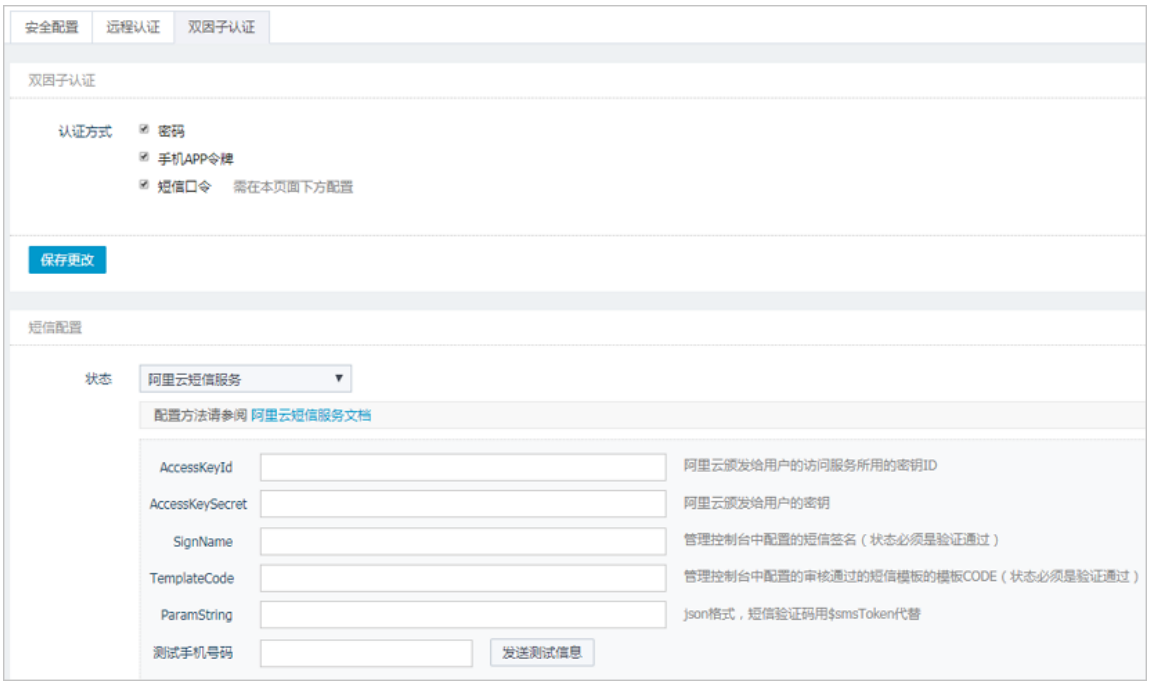
> **说明**：
> 在**远程认证**页签，也可以选择关闭本地认证方式，仅通过远程认证方式登录云盾堡垒机系统。

图 14-88: 远程认证页签

- 选择**双因子认证**页签，设置双因子认证方式及短信配置，如图 *14-89:* 双因子认证页签所示。

> **说明**：
> 云盾堡垒机系统的短信配置支持使用阿里云短信服务。

图 14-89: 双因子认证页签



14.5.2.3 管理系统相关配置

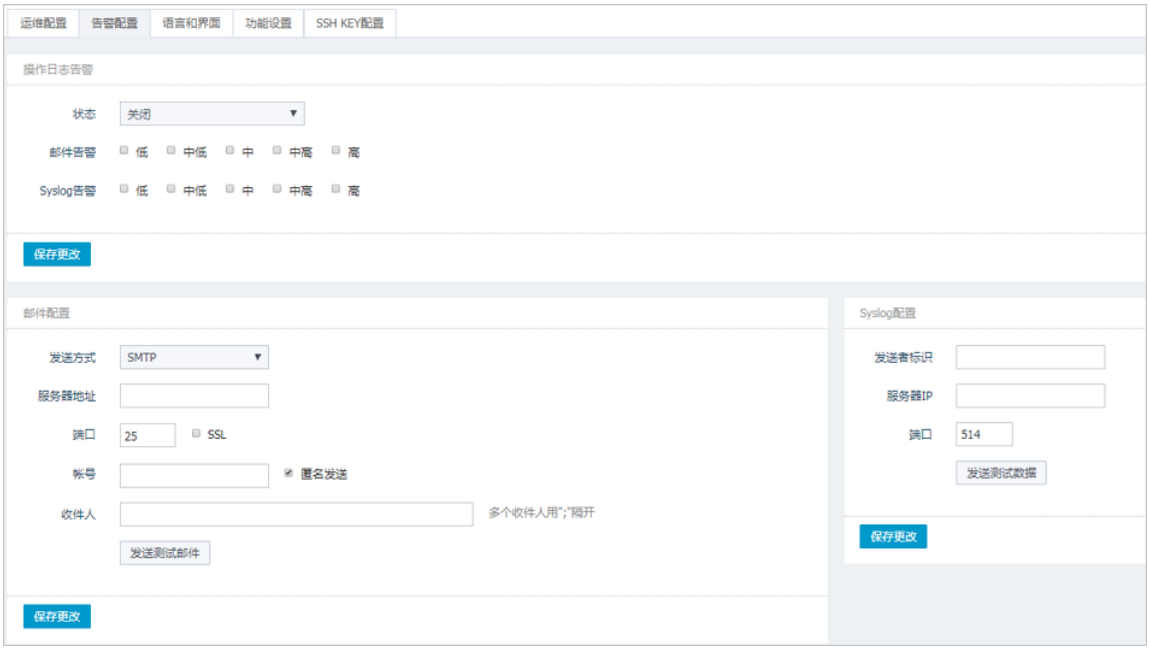
操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**系统** > **系统配置**页面。
3. 管理云盾堡垒机系统相关配置。
   - 选择**运维设置**页签，进行运维相关配置，如*图 14-90: 运维配置页签*所示。

图 14-90: 运维配置页签

- 选择**告警配置**页签，进行系统操作告警相关配置，如图 *14-91: 告警配置页签*所示。

图 14-91: 告警配置页签



- 选择**语言和界面**页签，可以设置云盾堡垒机系统的语言，如图 *14-92: 语言和界面页签*所示。

图 14-92: 语言和界面页签

- 选择**功能设置**页签，可以开启报表自动统计功能，如图 *14-93: 功能设置页签*所示。

图 14-93: 功能设置页签

- 选择**SSH KEY配置**页签，可以设置云盾堡垒机系统使用的RSA、DSA密钥，如图 *14-94: SSH KEY配置页签*所示。

图 14-94: SSH KEY配置页签

14.5.2.4 管理系统存储

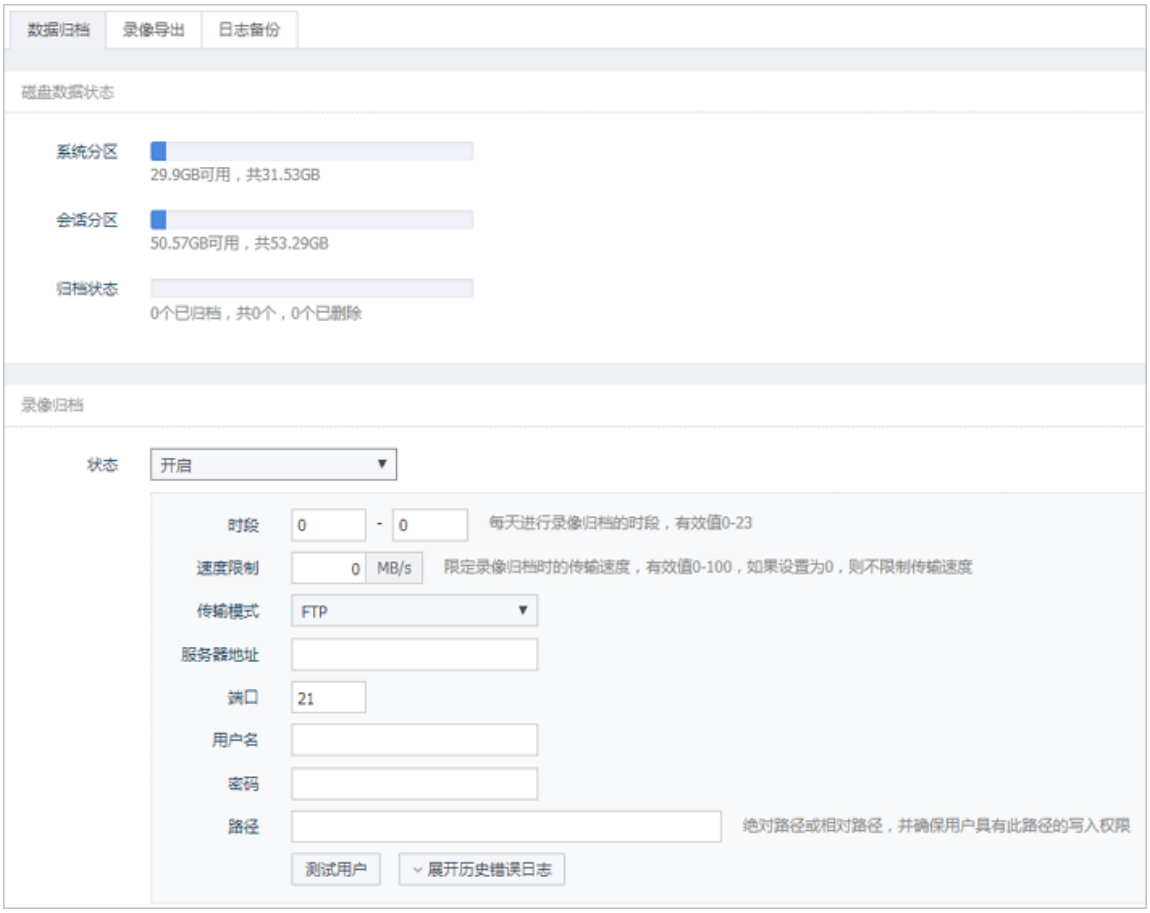
操作步骤

1. 登录云盾堡垒机系统。

2. 定位到**系统** > **存储管理**页面。
3. 管理云盾堡垒机系统存储空间。
   - 选择**数据归档**页签，查看磁盘数据状态并设置录像归档配置，如图 *14-95: 数据归档页签*所示。

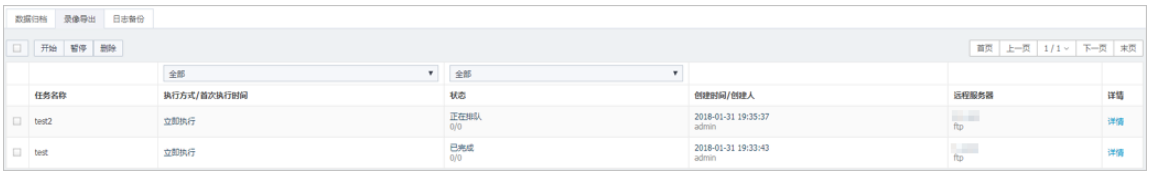
> **说明**：
> 在**数据归档**页签，还可以配置录像自动删除规则或手动删除系统数据。

图 14-95: 数据归档页签



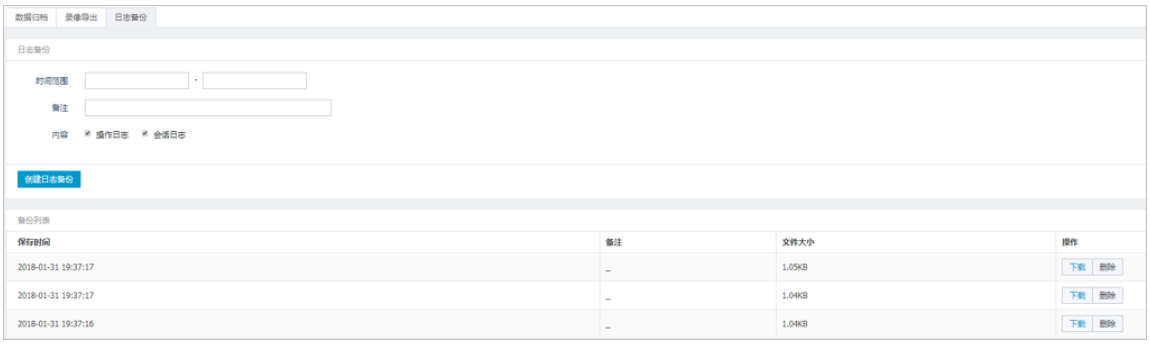
   - 选择**录像导出**页签，可以通过创建录像导出任务将系统已记录的指定范围内的运维会话录像导出其它FTP服务器，如图 *14-96: 录像导出页签*所示。

图 14-96: 录像导出页签



- 选择**日志备份**页签，可以为系统操作日志和运维会话日志创建备份，并将备份文件下载至本地，如图 *14-97:* 日志备份页签所示。

图 14-97: 日志备份页签



14.5.2.5 查看系统操作日志

操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**系统** > **操作日志**页面。
3. 选择**操作日志配置**页签，选择操作日志类型，为每类操作设置重要性，如图 *14-98:* 操作日志配置页签所示。

> **说明**：
> 云盾堡垒机系统为每种操作都设置了默认重要性。

图 14-98: 操作日志配置页签

操作日志配置

登录日志

重要性	默认重要性	日志描述
低	低	登录系统
低	低	退出系统
中低	中低	登录系统，未知系统错误
中低	中低	登录系统，用户不存在
中低	中低	登录系统，有效期之外登录
中低	中低	登录系统，用户被锁定
中低	中低	登录系统，密码错误
中低	中低	登录系统，本地认证被禁用
中低	中低	登录系统，远程认证被禁用
中低	中低	登录系统，认证模式不匹配
中低	中低	登录系统，从禁止的IP地址登录
中低	中低	登录系统，禁止admin从Web登录
中低	中低	登录系统，在禁止的时间段登录
中低	中低	登录系统，连接远程认证服务器失败
中低	中低	登录系统，认证方式未启用

4. 选择**操作日志**页签，设置搜索条件，单击**搜索**，查看操作日志记录，如图 *14-99:* 操作日志页签所示。

图 14-99: 操作日志页签

说明：

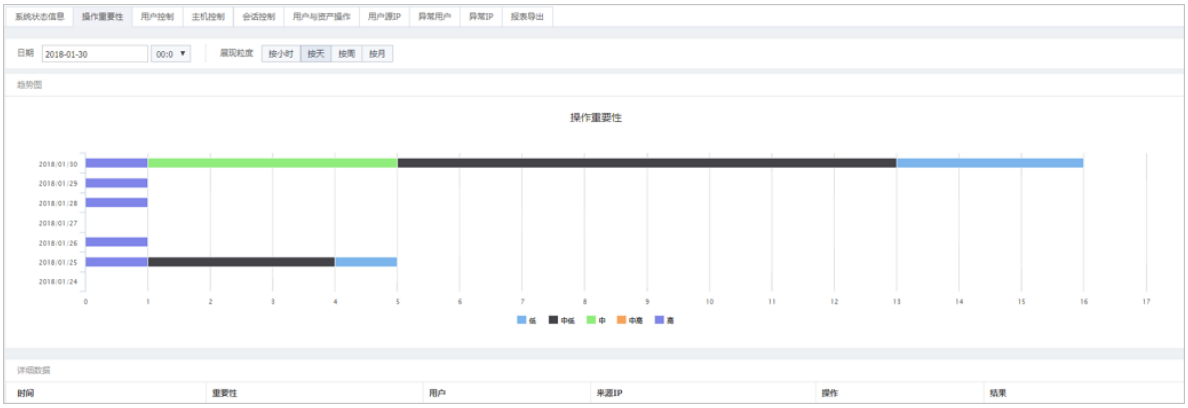
单击**导出日志**，可将当前页面的操作日志记录以CSV格式文件导出到本地。

14.5.2.6 查看系统报表

操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**系统** > **系统报表**页面。
3. 选择系统报表页签，设置时间范围和展现粒度，查看各方面的系统报表趋势图和详细数据，如*图 14-100: 查看系统报表*所示。

图 14-100: 查看系统报表



4. 选择**报表导出**页签，选择报表周期、起始时间、导出格式，单击**导出系统报表**，可将完整的系统报表导出到本地。

14.5.2.7 维护本机系统

操作步骤

1. 登录云盾堡垒机系统。
2. 定位到**系统** > **本机维护**页面。
3. 对云盾堡垒机系统本机进行维护。
   - 选择**系统管理**页签，进行系统管理相关配置，包括系统时间、系统升级、重启或关闭设备等，如图 *14-101: 系统管理页签*所示。

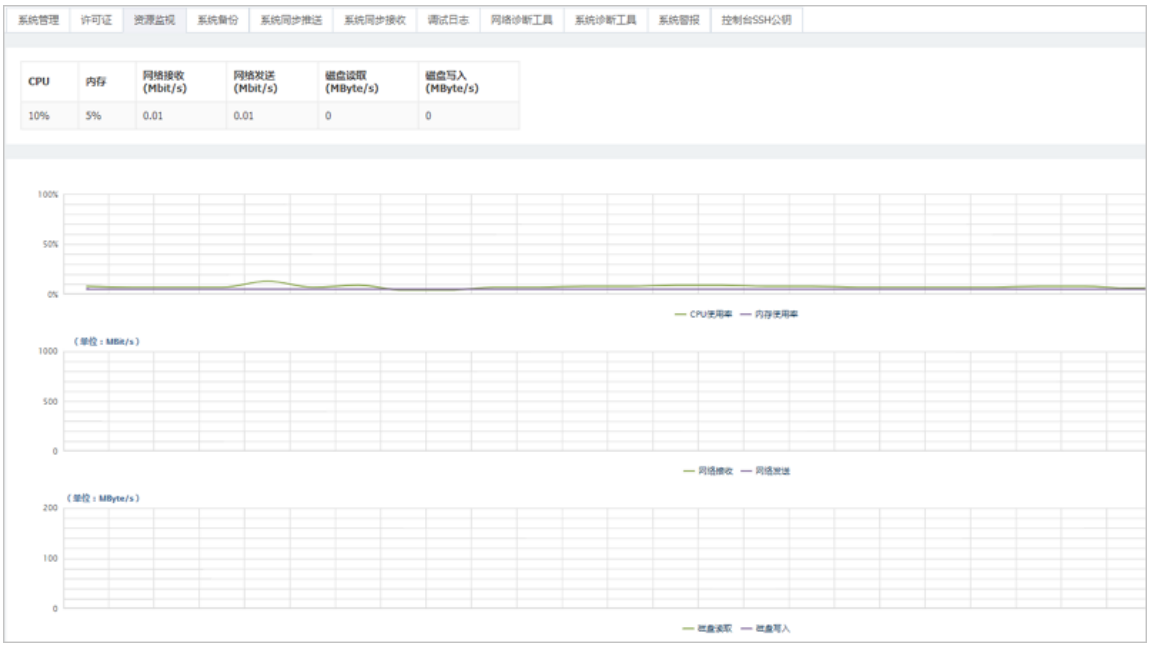
图 14-101: 系统管理页签

- 选择**许可证**页签，查看许可证信息或导入新的许可证，如图 *14-102: 许可证页签*所示。

图 14-102: 许可证页签

- 选择**资源监视**页签，查看云盾堡垒机系统实时系统资源使用情况，如图 *14-103: 资源监视页签*所示。

图 14-103: 资源监视页签



- 选择**系统备份**页签，设置系统配置自动备份，手动备份或还原系统配置，如图 *14-104: 系统备份页签*所示。

图 14-104: 系统备份页签

- 选择**系统同步推送**页签，设置系统配置推送功能，可将本系统的配置定期自动推送至其他云盾堡垒机系统，如图 *14-105: 系统同步推送页签*所示。

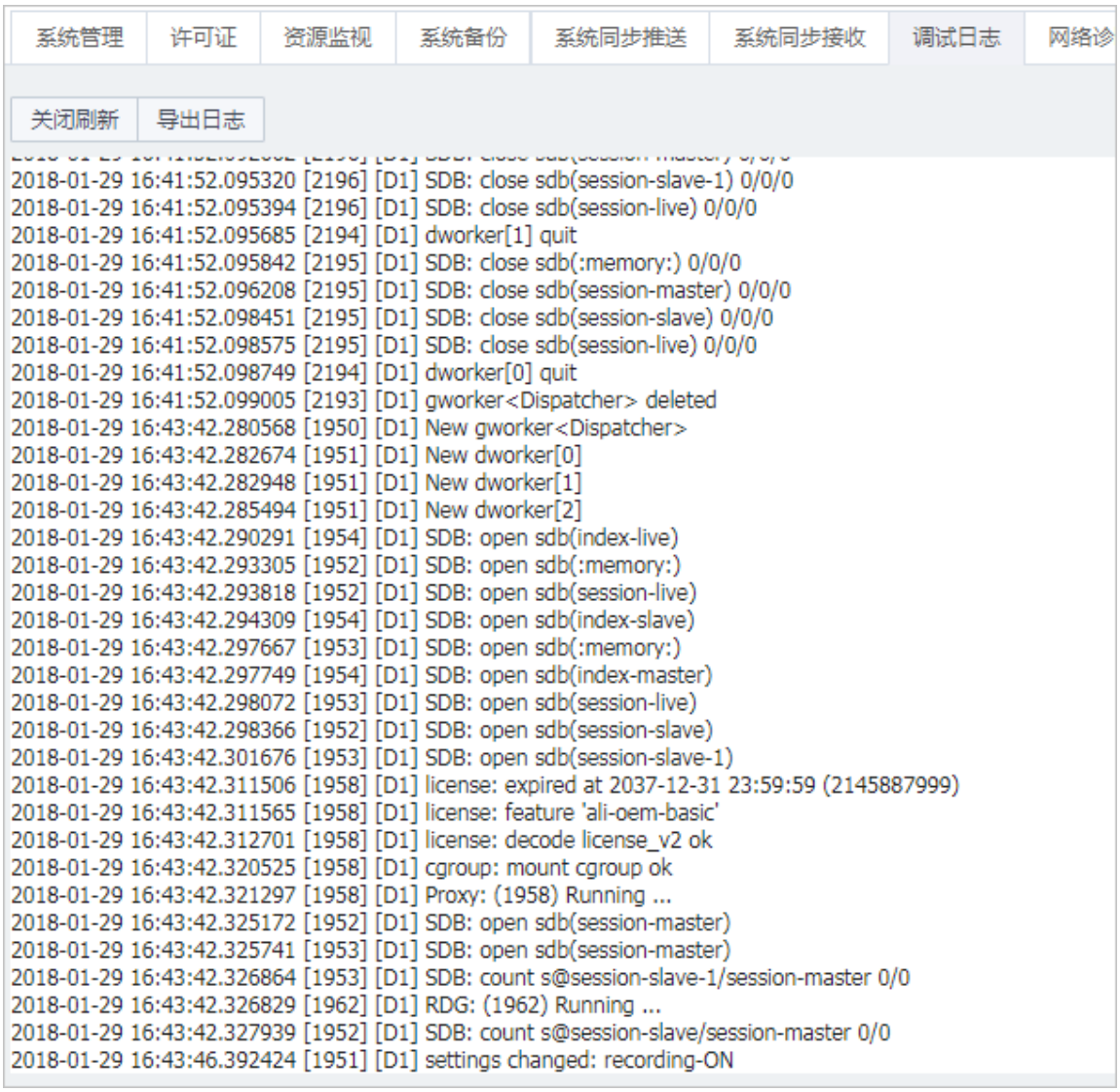
图 14-105: 系统同步推送页签

- 选择**系统同步接收**页签，设置系统配置接收功能，接收其他系统向本系统推送的系统配置，如图 *14-106: 系统同步接收页签*所示。

图 14-106: 系统同步接收页签

- 选择**调试日志**页签，查看系统调试日志，并可将日志导出到本地，如图 *14-107:* 调试日志页签所示。

图 14-107: 调试日志页签



- 选择**网络诊断工具**页签，可通过连通性检测测试云盾堡垒机系统与目标主机之间的连通情况并进行诊断，如*图 14-108: 网络诊断工具页签*所示。

图 14-108: 网络诊断工具页签

- 选择**系统诊断工具**页签，选择所需诊断的系统信息，可查看诊断日志，如图 *14-109: 系统诊断工具页签*所示。

图 14-109: 系统诊断工具页签

说明：

单击**下载诊断日志**，可将当前系统信息日志下载至本地。

- 选择**系统警报**页签，可查看系统警报记录，如图 *14-110: 系统警报页签*所示。

图 14-110: 系统警报页签

说明：

针对系统警报信息进行检测排查后，可选择相关警报，单击**确认警报**，将该系统警报标识为已确认。

- 选择**控制台SSH公钥**页签，可查看控制台SSH公钥信息，如图 *14-111: 控制台SSH公钥页签*所示。

图 14-111: 控制台SSH公钥页签

说明：

单击**重置控制台SSH公钥**，可重新生成一对SSH密钥，系统会保存公钥并显示私钥的内容，但不会保存私钥，请妥善保管私钥。

15 系统管理

系统管理模块作为云盾安全中心不可或缺的部分，为安全管理员调整系统人员、配置提供了极大的便利。

系统管理主要包含四个部分：

- **阿里云账号管理**：用于管理专有云云盾配套的阿里云账号。
- **云端同步**：用于查看云盾情报库的更新方式及更新情况。
- **告警设置**：用于配置各类安全事件、紧急信息等的告警方式以及联系人信息。
- **全局设置**：用于配置云盾相关的网段信息，包括流量监控网段和区域网段两部分。

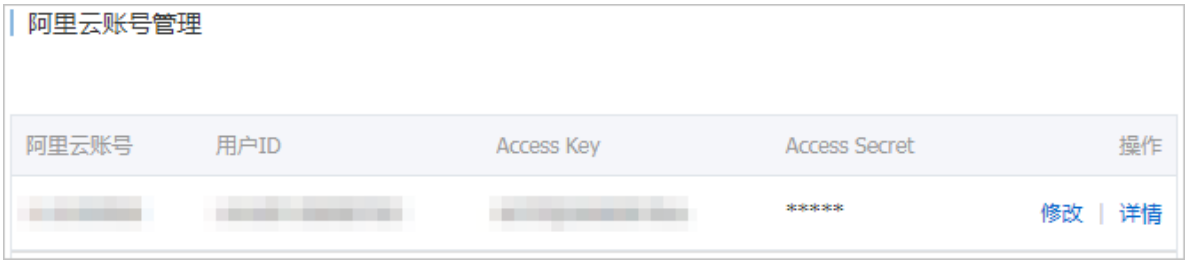
15.1 管理阿里云账号

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **阿里云账号管理**页面，可以查看、修改系统绑定的阿里云账号信息，如图 *15-1:* 阿里云账号管理页面所示。

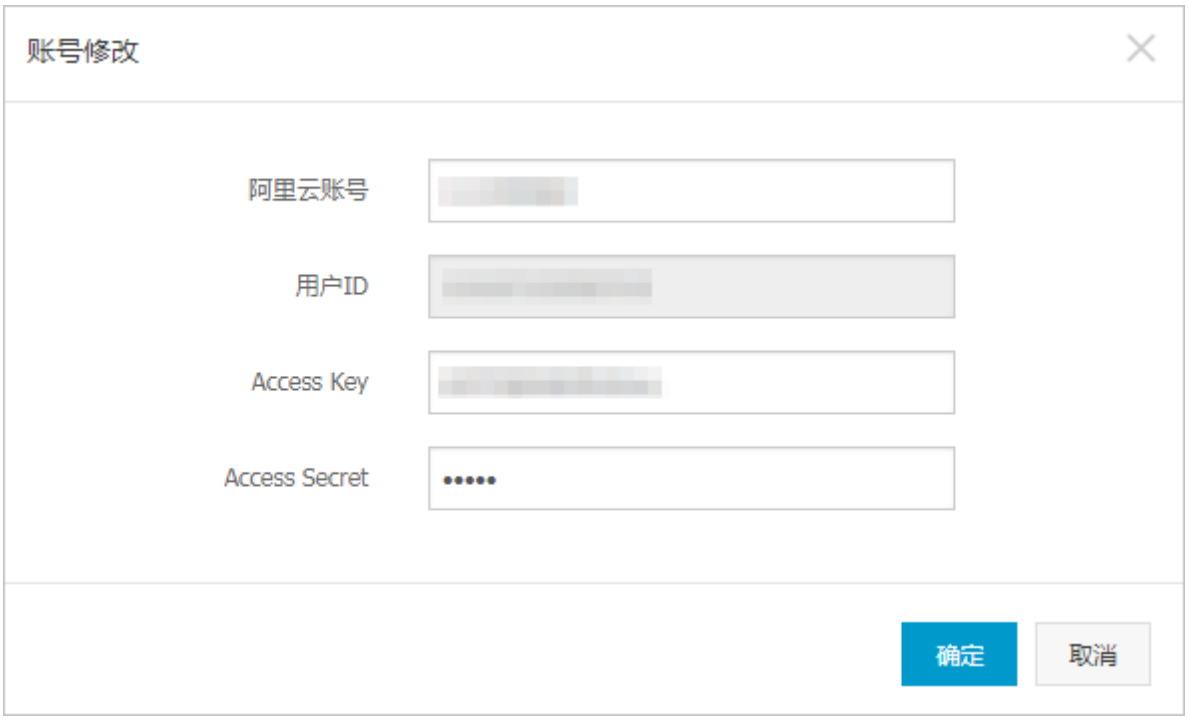
   云盾中的资产均与阿里云账号绑定，请谨慎修改。

   图 15-1: 阿里云账号管理页面

3. 单击**修改**，弹出修改对话框，信息修改后单击**确定**，完成修改，如图 *15-2:* 账号修改对话框所示。

图 15-2: 账号修改对话框



4. 单击**详情**，查看阿里云账号详细信息，包括许可到期时间、安骑士许可数目，如图 *15-3:* 账号详情所示。这些信息均是通过配置的用户ID、Access Key信息获取。

图 15-3: 账号详情

15.2 云端同步

云端同步是将阿里公共云上的一些规则库、漏洞等安全信息同步到本地数据库。

云端同步是将阿里公共云上的0day规则库、漏扫漏洞库、漏洞主库、主机漏洞规则库、弱点扫描插件库、弱点扫描规则库、安骑士Webshell检测规则库、安骑士漏洞管理 - Windows漏洞（系统补丁）、安骑士漏洞管理 - Windows漏洞（规则文件）和安骑士漏洞管理 - 其它应急漏洞信息同步到本地数据库。所同步的规则信息将应用于专有云云盾各对应功能模块中，确保在专有云环境中具备与阿里云公共云同等的安全能力。

云端同步根据专有云环境的部署方式分为在线升级及离线升级包导入两种方式。

15.2.1 同步状态说明

云端同步列表中的数据是初始化的，只支持将阿里公共云上的各类规则库同步到本地数据库。

规则库信息与云端同步的频率和时间可以由管理员进行设置，可以是手动触发，也可以是自动触发；如果不设置，同步的频率将按照初始设置。

表 15-1: 同步状态说明表

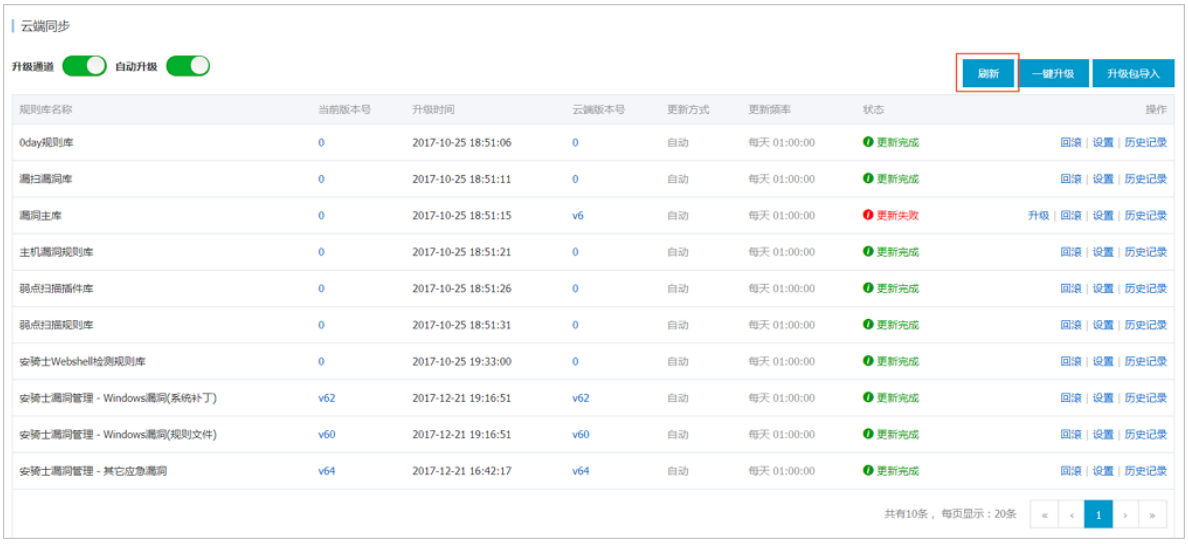
状态	说明
待更新	云端有新版本规则库可以更新。
更新中	从云端下载并更新规则库。
更新完成	规则库更新完成。
更新失败	规则库更新失败。

15.2.2 刷新云端同步列表

操作步骤

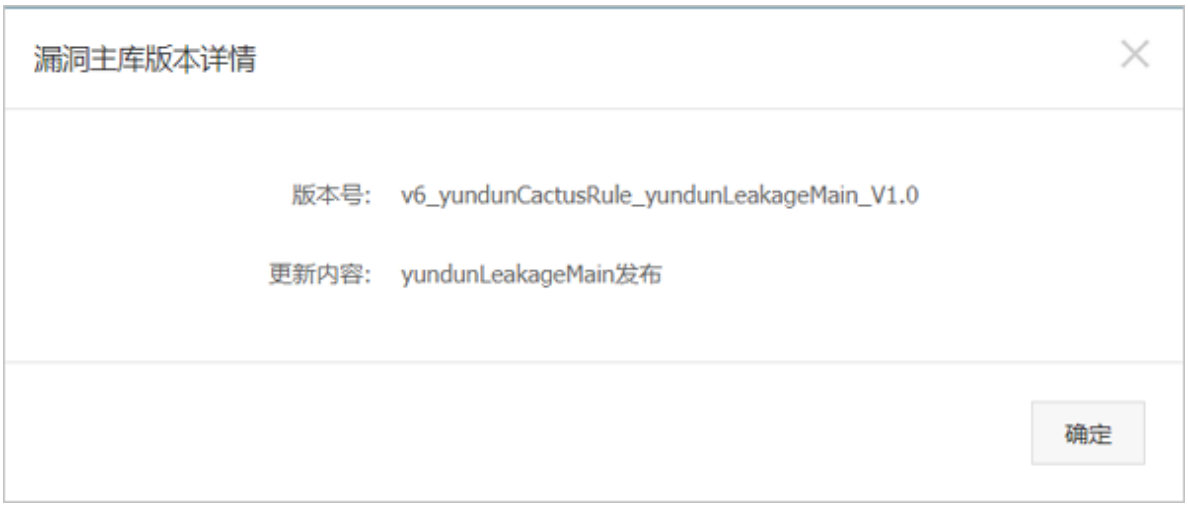
1. 登录云盾控制台。
2. 定位到**系统管理** > **云端同步**页面，单击**刷新**，刷新云端同步列表，如图 *15-4: 云端同步页面*所示。

图 15-4: 云端同步页面



3. 刷新成功后，在**云端同步**页面，查看规则库在专有云环境中的当前版本号、云端版本号，以及更新方式、更新频率、状态等信息。选择规则库，单击当前版本号或云端版本号可查看规则库版本详情，如图 *15-5: 规则库版本详情*所示。

图 15-5: 规则库版本详情



15.2.3 设置更新方式及频率

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **云端同步**页面，选择规则库，单击**设置**。
3. 在更新设置对话框中，选择更新方式、更新频率，并设置更新发生时间，单击**确定**，如图 *15-6: 规则库更新设置*所示。

图 15-6: 规则库更新设置

如设置为自动更新，系统将按照所设定的更新频率及时间自动检查云端规则库版本并进行自动更新。

15.2.4 手动更新规则库

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **云端同步**页面。
3. 选择规则库，单击**升级** ，将规则库信息从云端下载到版本库中。

> **说明**：
> 单击**云端同步**页面右上方的**一键升级**，可以手动更新所有规则库。

15.2.5 回滚规则库

规则库更新完成后，可以通过回滚操作将规则库恢复至以前版本。

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **云端同步**页面。
3. 选择规则库，单击**回滚**。
4. 在**版本回滚**对话框中，选择想要恢复到的规则库版本，如图 *15-7:* 版本回滚所示。

图 15-7: 版本回滚

5. 单击**确定**。

15.2.6 查看历史记录

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **云端同步**页面。
3. 选择规则库，单击**历史记录**，可以查看该规则库的同步记录，如图 *15-8: 查看历史记录*所示。

图 15-8: 查看历史记录

15.2.7 导入离线升级包

如果专有云环境无法与阿里云公共云连通，可以通过导入离线升级包的方式更新规则库。

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **云端同步**页面。
3. 单击右上方的**升级包导入**。
4. 在**离线升级包**对话框中，单击**选择文件**，选择已下载至本地的离线升级包，如图 *15-9: 导入离线升级包*所示。

   图 15-9: 导入离线升级包

   根据导入的离线升级包，云盾将完成相应规则库的更新，并在**云端同步**页面更新该规则库的状态。
5. 单击**确定**。

15.3 告警设置

告警设置功能包括设置告警联系人和按照不同的安全事件设置告警通知方式。当发生对应的安全事件时，系统自动上报告警，以便安全管理员了解系统发生的安全事件。

15.3.1 设置告警联系人

告警联系人是告警消息的接收人，告警消息的发送方式有手机短信和邮件。当监控数据满足报警规则时会发送告警信息给报警联系人。

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **告警设置** > **告警联系人**页面，如图 *15-10: 告警联系人页面*所示。

图 15-10: 告警联系人页面

3. 单击**添加联系人**。
4. 填写联系人信息，单击**确认**，添加告警联系人。

   添加后的告警联系人可以通过单击**编辑**或**删除**，对该联系人信息进行编辑或删除。

15.3.2 设置告警信息

告警设置可以对各种安全事件进行告警，告警方式包括手机和邮件。

操作步骤

1. 登录云盾控制台。
2. 定位**系统管理** > **告警设置** > **告警设置**页面。
3. 在**告警通知**区域，为各种安全事件选择通知方式，如*图 15-11: 告警设置页面*所示。

   图 15-11: 告警设置页面

4. 单击**确认**，完成设置。

15.4 全局设置

云盾安全中心提供全局设置，供安全管理员对云盾流量安全监控模块的网段范围以及安骑士模块上报检测的区域进行设置。

说明：
流量安全监控模块的采集网段设置和区域设置中如果配置同一网段，则区域信息必须一致。

15.4.1 流量采集网段设置

网段设置主要针对流量安全监控模块进行网段配置，并且支持更改监控的网段范围，方便安全管理员根据需求调整监控的网段。配置的监控网段仅对所属区域机房生效。

说明：
网段设置更改后立即对流量监控生效，不需要安全管理员进行其他操作。

15.4.1.1 添加流量采集网段

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **全局设置** > **流量采集网段设置**页面。
3. 单击**添加**，弹出**添加监控网段**对话框，如*图 15-12: 添加监控网段对话框*所示。

图 15-12: 添加监控网段对话框

4. 设置监控网段参数。
   - 填写网段。

     说明：
     所填写的网段必须是合法网段，并且不允许重复添加。

- 选择所属区域。

5. 单击**确定**，完成添加。

15.4.1.2 管理流量采集网段

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **全局设置** > **流量采集网段设置**页面。
3. 选择区域，输入查询网段，单击**查询**，查看流量采集网段信息，如图 *15-13:* 流量采集网段所示。

图 15-13: 流量采集网段

4. 管理流量采集网段。
   - 单击**修改**，在**修改网段**对话框中修改所属区域，单击**确定**，修改流量采集网段所属区域。
   - 单击**删除**，可删除该流量采集网段。

15.4.2 区域设置

区域设置主要针对不同机房安骑士客户端的区域检测，配置后，所属区域对应网段下的安骑士主机上报后，可以自动检测匹配对应的机房。

说明：

区域设置支持更改已配置网段的所属区域，但是更改后必须在资产总览中批量修改对应网段资产的区域。

15.4.2.1 添加区域网段

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **全局设置** > **区域设置**页面。
3. 单击**添加**，弹出**添加网段**对话框，如图 *15-14:* 添加网段对话框所示。

图 15-14: 添加网段对话框

4. 设置网段参数。
   - 填写网段。

     说明：
     所填写的网段必须是合法网段，并且不允许重复添加。

   - 选择所属区域。
5. 单击**确定**，完成添加。

15.4.2.2 管理区域网段

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **全局设置** > **区域设置**页面。
3. 选择区域，输入查询网段，单击**查询**，查看区域网段信息，如图 *15-15:* 区域设置页面所示。

图 15-15: 区域设置页面

4. 管理区域网段。
   - 单击**修改**，在修改网段对话框中修改所属区域，单击**确定**，修改区域网段信息。
   - 单击**删除**，删除该区域网段信息。

15.4.3 配置白名单

操作步骤

1. 定位到**系统管理** > **全局设置** > **白名单设置**。
2. 单击**添加**。
3. 在**添加白名单**对话框中，设置白名单参数，如图 *15-16:* 添加白名单对话框所示。

图 15-16: 添加白名单对话框

参数	说明
源IP	源IP/网段。
目的IP	目的IP/网段。
用户名	添加白名单记录的用户名称
类型	• bwaf源ip白名单：符合该白名单的流量将不会被检测。 • 主机暴力破解白名单：符合该白名单中的登录行为将不进行暴力破解检测。 • 应用攻击白名单：符合该白名单中的疑似应用攻击行为将不会被检测。

4. 单击**确认**。

   白名单添加成功后，单击**删除**，可删除已不需要的白名单。