阿里云
专有云Enterprise版

安全管理员指南（基础版）

产品版本：V3.3.0

文档版本：20180312

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. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	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

云数据中心环境下，安全业务复杂多样，需要多种安全能力协同保证平台的安全和业务的安全，多租户的场景下，租户的边界变得模糊，各租户的安全需求不一致，势必导致安全管理的不可控制。统一的云安全管理成为迫切需求，将替代传统的单点安全管理，被云用户所接受。

云盾以阿里云互联网攻防技术为核心，为用户建设涵盖网络安全、应用安全、主机安全、安全态势感知的全方位互联网安全攻防体系。不同于以往以检测技术为主的边界防护方式，云盾防护以泛安全数据与情报联动分析为驱动，为用户提供全景的安全态势感知、攻击溯源回溯、基础安全防护等功能。通过纯软件化的部署方式，云盾可以帮助您在自有 IDC、专有云、公共云、混合云等多种业务环境获得与阿里云同等强度的互联网防护能力。

云盾对专有云环境中的网络安全、主机安全进行监控，并有效防护各类安全威胁。安全管理人员可以通过专有云的云安全中心控制台实时了解专有云环境内的安全态势，并及时对安全风险项进行处理。同时，专有云云盾还具备安全审计功能，对云服务操作日志进行展示和审计，以便安全审计员及时发现并消除安全隐患。

阿里云专有云Enterprise V3.3中提供了云盾基础版及高级版。

2 配置要求

访问专有云云盾安全中心控制台时，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。

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 登录云盾安全中心

前提条件

在DTCenter的**系统管理** > **用户管理**页面，创建专有云云盾安全中心用户，并为该用户分配云盾安全中心相关的角色权限：

说明：
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、主机安全、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、主机安全、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。

背景信息

登录专有云云盾安全中心有以下两种方式：

- 登录DTCenter，从DTCenter页面上跳转到专有云云盾安全中心页面。
  a) 打开Chrome浏览器。
  b) 在地址栏中，输入DTCenter的网站地址（例如：http://*DTCenter*网站地址），按**Enter**，进入DTCenter登录页面。
  c) 在DTCenter登录页面，输入已创建的专有云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DTCenter后，在菜单导航栏选择云安全中心。
  f) 选择**区域**，单击**安全中心**，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

- 通过专有云云盾安全中心的网站地址，直接登录云盾安全中心页面。

> **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，输入专有云云盾安全中心的网站地址（例如：http://*DTCSC*网站地址），按**Enter**。

c) 输入已创建的专有云云盾安全中心用户的登录账号、密码及验证码。

d) 单击**登录**。

3.2 退出云盾安全中心

- 在专有云云盾控制台页面，单击页面右上角的**退出**，即可从云盾安全中心注销。

4 云盾基础版安全中心

4.1 概述

云盾基础版是保障云计算服务平台正常运行的云安全运营平台。云盾基础版以云计算资源为基础防护对象，以云上业务系统为防护核心，以安全事件管理为主要手段，及时准确地发现云平台的网络异常行为和安全威胁，协助安全管理员进行安全管理、风险分析、应急响应和综合决策。

云盾基础版为用户提供异常流量分析检测、Web层攻击检测/防御、主机防入侵的实时防护能力，并提供云计算平台的ECS、RDS、物理服务器、API服务的安全审计功能，还支持自定义审计类型的审计。

4.2 云盾基础版安全中心界面

云盾基础版的云安全中心界面主要可以分为三大区域，如图 *4-1:* 云盾基础版安全中心界面图所示。

图 4-1: 云盾基础版安全中心界面图

表 4-1: 云盾安全中心界面区域说明

区域	说明
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。
菜单导航树区	云盾安全中心基础版包括态势感知、网络安全、主机安全、安全审计和系统管理五个部分，主要功能如下：

区域	说明
	• **态势感知**：根据网络流量情况对当前的安全态势进行概要性的展示，帮助安全管理员了解当前专有云环境的网络流量情况。 • **网络安全**：查看云盾已拦截的网络异常行为和安全威胁，包括应用攻击和暴力破解攻击。 • **主机安全**：提供物理机及云主机的入侵防护，帮助安全管理员保障服务器主机安全。 • **安全审计**：对云服务操作日志进行展示和审计，以便安全审计员及时发现并消除安全隐患。 • **系统管理**： - 阿里云账号管理：管理专有云云盾配套的阿里云账号。 - 云端同步：将阿里公共云上的安全防护规则同步至专有云环境。 - 告警设置：设置告警联系人和告警通知。当安全事件发生时，如果符合告警通知方式，系统会自动上报告警，以便管理员及时了解系统发生的安全事件。 - 全局设置：供管理员对云盾监控的网段范围以及安骑士上报检测区域进行设置。
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。

4.3 态势感知

态势感知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。

云盾基础版态势感知主要展示专有云环境网络流量情况。

4.3.1 总览

总览页面根据网络流量情况对当前的安全态势进行概要性展示，让用户快速了解和掌握当前安全态势。

网络流量是对网络的出口、入口、QPS流量信息的分析，向用户展示流量的高峰、低谷、速率和地域来源的分布规律。

4.3.1.1 查看网络流量信息

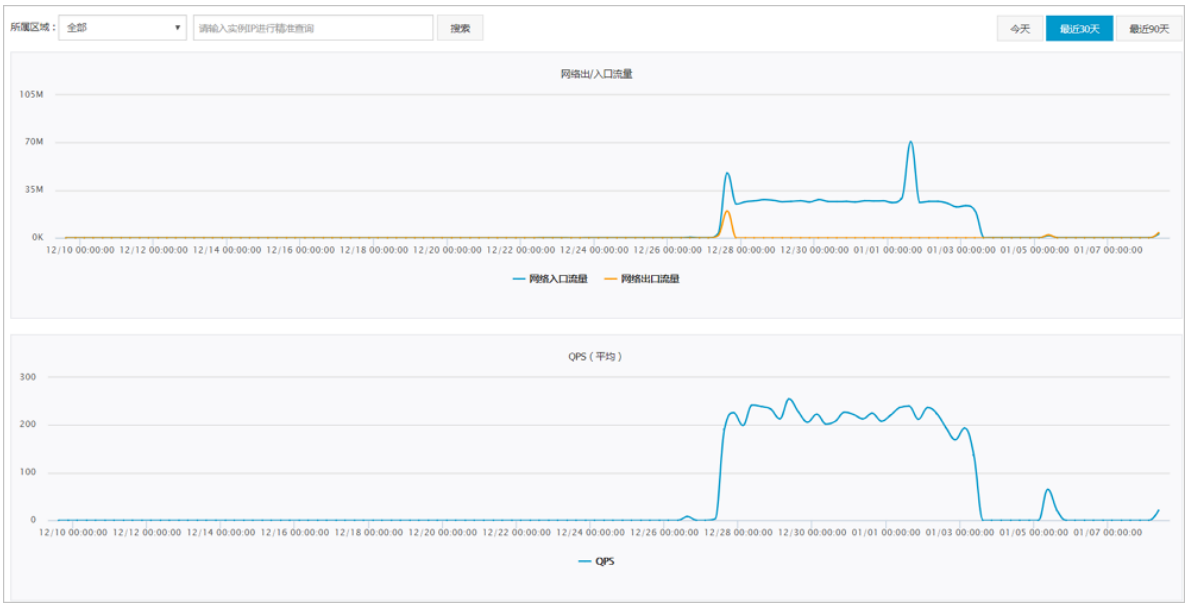
背景信息

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，可以有效甄别恶意的IP访问。

操作步骤

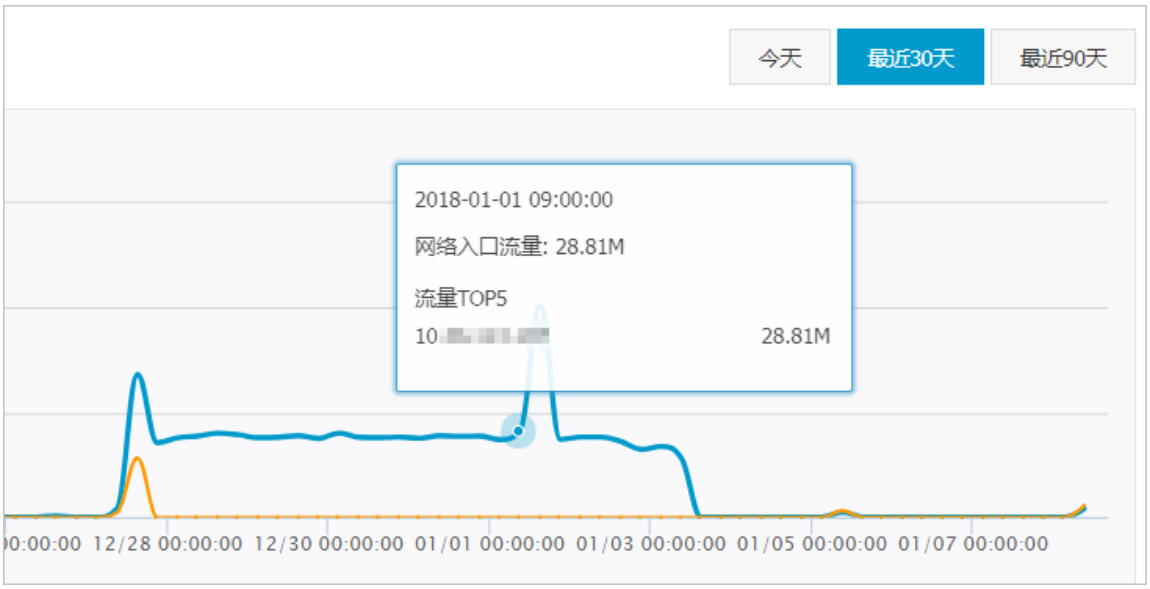
1. 定位到**态势感知** > **总览**，进入**总览**页面，如图 *4-2: 总览页面*所示。

图 4-2: 总览页面



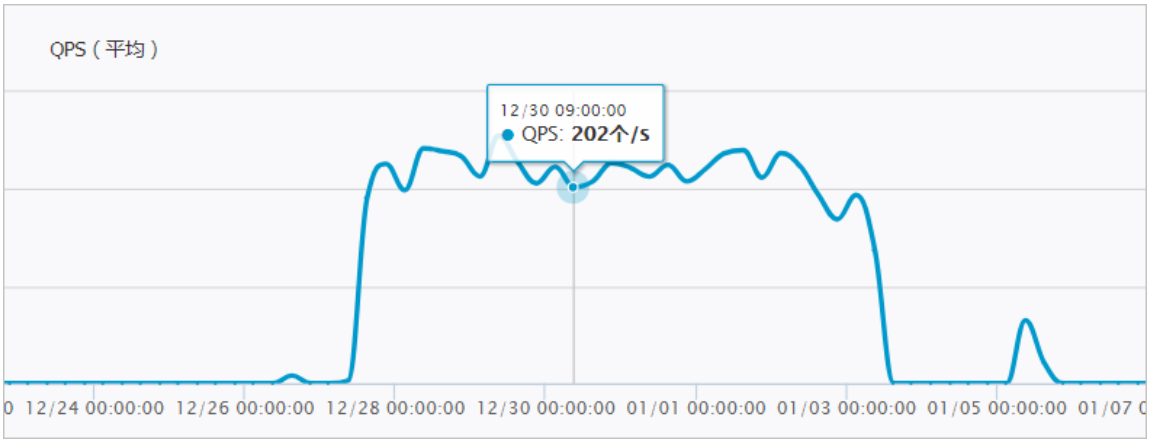
2. 查看不同时期、区域或单个IP的流量情况。
   - 在**总览**页面，单击**今天**、**最近30天**、**最近90天**可以切换查看不同时间段的流量信息。
   - 在**所属区域**中可以选择区域信息，或在搜索框中输入IP，可以分区域、分IP查询流量信息。
3. 查看某时间节点具体流量信息。
   - 在网络出/入口流量图中，将鼠标停留在流量折线上，可查看该时间点出口或入口流量的详细信息及流量TOP5的IP，如图 *4-3: 查看流量 TOP5 的 IP*所示。

图 4-3: 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 *4-4: 查看QPS详细信息*所示。

图 4-4: 查看QPS详细信息



4.4 网络安全

云盾安全中心基础版包含威胁感知功能，该功能记录了云盾检测到的Web应用攻击和暴力破解两大类安全威胁信息：

- **Web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，流量安全监控模块对流量进行监测，提取流量中的攻击信息。

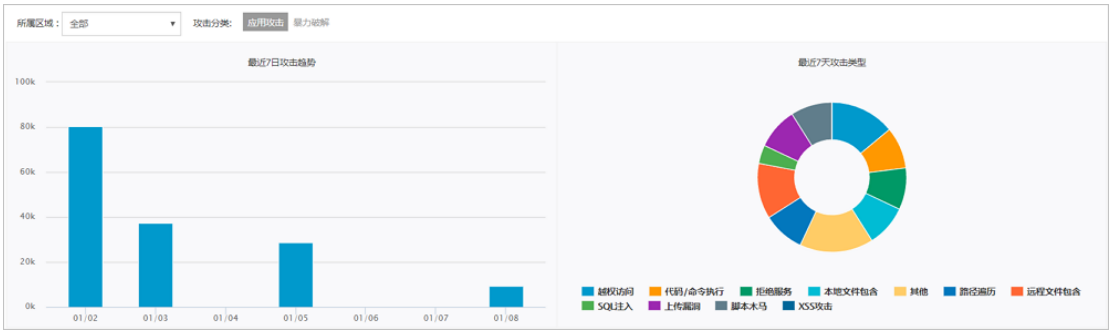
- **暴力破解**：当黑客针对某个资产进行暴力破解的时候，安骑士客户端能够及时监测到暴力破解攻击的发生并上报给云盾安全中心。

4.4.1 查看威胁攻击信息

操作步骤

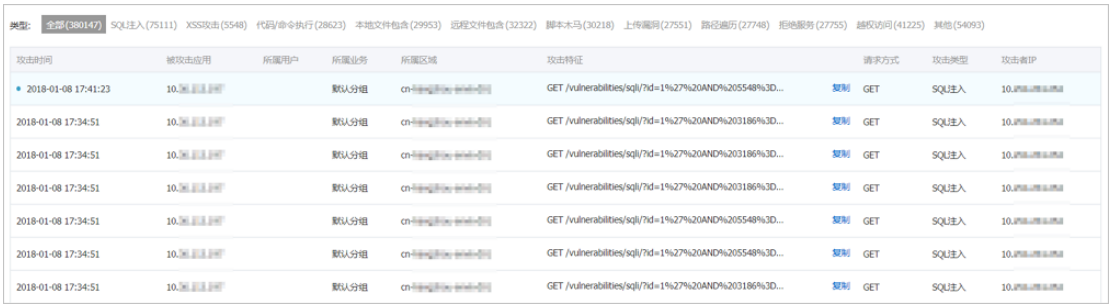
1. 定位到**网络安全 > 威胁**，进入**威胁**页面。
2. 查看云盾安全中心检测到的威胁攻击信息。
   - 单击**应用攻击**，选择**所属区域**，查看应用攻击信息及上报的应用攻击事件。
     - 查看最近7天检测到的攻击趋势、攻击类型信息，如图 *4-5:* 最近7天攻击趋势及攻击类型所示。

       图 4-5: 最近7天攻击趋势及攻击类型

     - 查看全部攻击事件的详细信息，如图 *4-6:* 应用攻击事件记录所示。

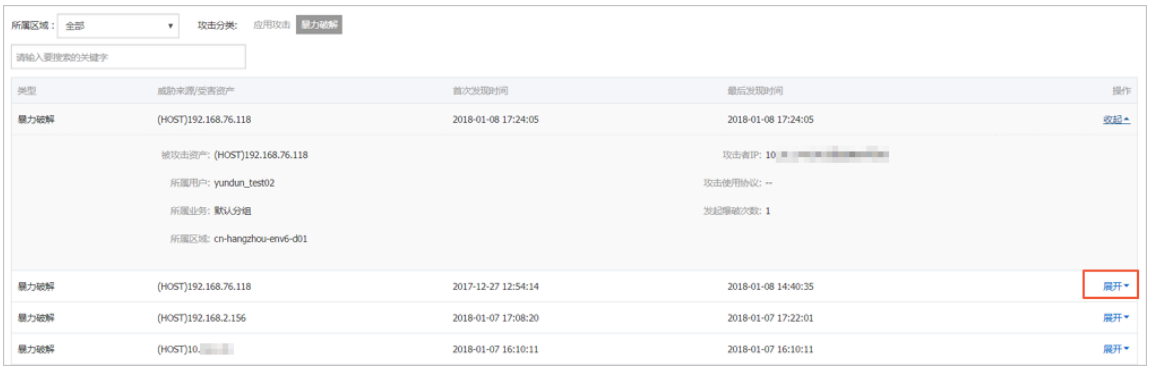
       图 4-6: 应用攻击事件记录

       > **说明**：
       > 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。

   - 单击**暴力破解**，选择**所属区域**，查看暴力破解事件记录，如图 *4-7:* 暴力破解页面所示。

图 4-7: 暴力破解页面



说明：

单击**展开**，可查看该暴力破解事件的详细信息。

4.5 主机安全

专有云云盾安全中心能够防护每一台用户主机的安全，主机安全包括安骑士基础版和主机入侵检测功能：

- **云主机防护——安骑士基础版**：

  安骑士（Aegis）是云盾的一个核心组件，提供了主机防护及主机入侵检测功能。安骑士分为客户端和服务器端。安骑士客户端配合安骑士服务器，监测系统层和应用层的攻击行为，实时发现黑客入侵行为。安骑士基础版包含以下功能：

  - **防护基线**：云盾能够实时展示安骑士的防护状态，并且当防护状态离线时，云盾将展示安骑士的最后在线时间。
  - **登录安全**：云盾登录安全防护包括异地登录提醒和暴力破解告警。支持常用登录地和白名单的配置。
    - 异地登录提醒：安骑士维护了每一台已安装Agent的机器的常用登录地，如果在非常用登录地有登录行为，会上报事件到安骑士服务器端。同时，支持RDP、SSH登录方式的异地登录告警。
    - 暴力破解防护：安骑士Agent对所有的登录行为进行审计并实时上报到安骑士服务器端。服务器端进行汇总和分析，若匹配到暴力破解行为则会立即写进数据库并展示在页面上。同时，支持RDP、SSH等登录方式的暴力破解攻击防护。
  - **木马查杀**：恶意文件通过本地自动查杀及匹配服务器端样本库查杀，支持PHP、JSP等后门文件类型的查杀。

- **物理机防护——主机入侵检测**：

  主机入侵检测功能检测专有云环境中所有物理服务器上的文件篡改、异常进程、异常网络连接、可疑端口监听等行为，帮助安全管理员及时发现服务器安全隐患。

4.5.1 云主机防护

4.5.1.1 防护状态

安骑士防护状态必须保持在线才能为云主机提供稳定可靠的入侵防御告警功能。因此云盾提供了主机防护状态查询功能，供安全管理员查询安骑士防护状态是否在线和最后在线时间。

工作原理

安骑士客户端和安骑士服务器端通过TCP长连接通道进行消息传递。这个通道是安骑士模块中最核心的部分，稳定性高达99.99 %，通道间模拟SSL加密并严格保证单一通道的协议处理不影响其他通道。

在安骑士客户端成功与安骑士服务器端建立通信并登录后，该主机的防护状态便被设置为在线。此后，安骑士服务器端会定时向安骑士客户端发送心跳检测。当客户端断开连接时，服务器端将会更新安骑士的防护状态信息，记录最后在线时间。

4.5.1.1.1 查看云主机防护状态

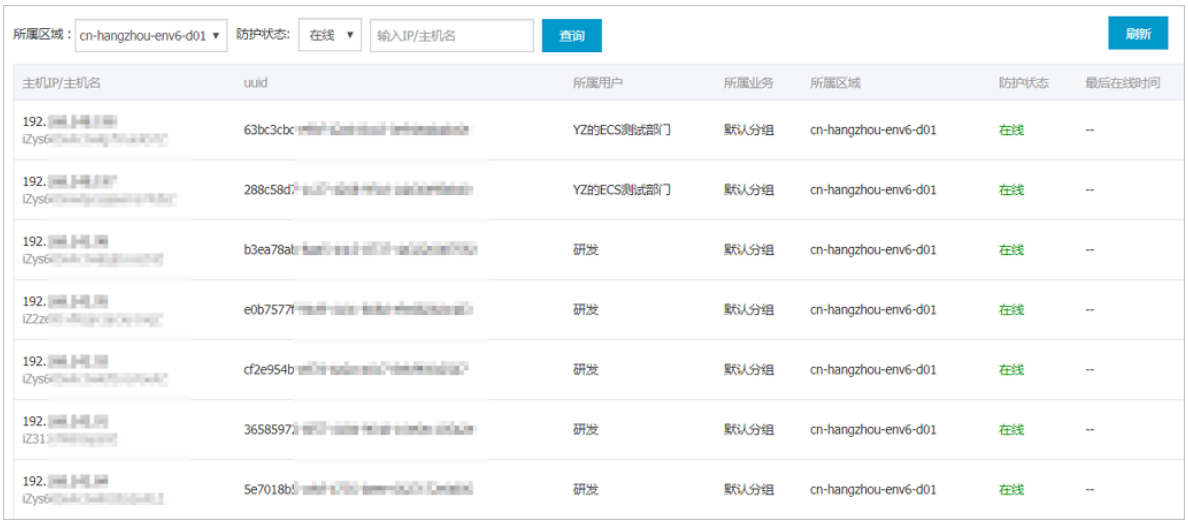
背景信息

云主机防护状态分为在线和离线。支持按照状态、区域筛选，支持主机IP及主机名的模糊查询，并支持列表刷新操作。

操作步骤

1. 定位到**主机安全** > **云主机防护** > **防护基线**，进入**防护基线**页面，如图 *4-8:* 防护基线列表所示。

图 4-8: 防护基线列表



说明：

防护基线页面默认展示全部区域，并按照IP排序展示所有云主机的防护状态。

2. 设置查询条件，单击**查询**，查看主机防护状态。
   - 选择**所属区域**，查看该区域的主机防护状态。
   - 选择**防护状态**，查看在线或离线状态的主机列表。
   - 输入主机IP或主机名，查看该主机的防护状态。
3. 单击**刷新**，可根据当前的查询条件刷新主机防护状态列表。

4.5.1.1.2 离线原因排查

背景信息

如果发现云主机处于离线状态，可以参考以下步骤进行排查：

操作步骤

1. 检查网络是否连接。
2. 检查是否设置了防火墙ACL规则。需要将安骑士服务端IP加入云主机的防火墙白名单以允许网络访问（80端口）。
3. 查看是否有第三方的防病毒产品。如果有，尝试关闭该防病毒产品后重新安装安骑士客户端，部分第三方的防病毒软件可能会禁止安骑士客户端访问网络。

4.5.1.2 登录安全

登录安全主要分为异地登录和暴力破解两部分，安全管理员可以在云盾安全中心中查看异地登录和暴力破解的告警信息，并查询登录记录和暴力破解的来源等详细信息。同时，安全管理员可以对异地登录和破解成功的记录进行处理，处理后标记为已处理的异常登录事件将不再进行告警。

4.5.1.2.1 登录记录

安全管理员可以在配置中心为云主机服务器设置常用登录地。如果发现存在不在常用登录地的登录行为，将在云盾安全中心提示异地登录事件。同时，在告警设置中可以为异地登录事件配置手机通知和邮箱通知的告警方式。

常用登录地的设置请参见配置登录地，告警设置请参见告警设置。

工作原理

1. 安骑士客户端通过TCP协议上报登录信息到安骑士服务器端。
2. 安骑士服务器端通过消息模块将上报的信息发送到Defender模块。
3. Defender模块分析登录信息，判断是否异地登录，并将结果写入Aegis-DB。如果为异地登录，将消息发送给云盾安全中心进行进一步处理，判断是否通过手机、邮件提醒用户。

4.5.1.2.2 查询登录记录

背景信息

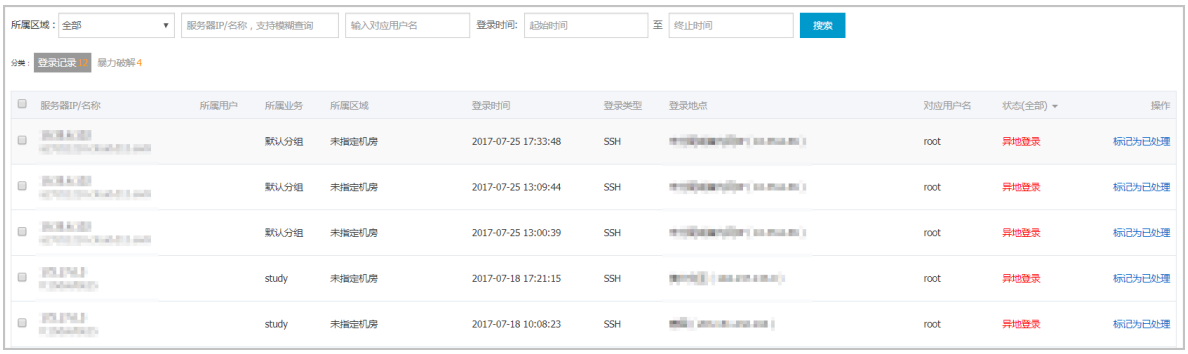
登录记录状态主要有**异地登录**、**正常登录**和**已处理**三种状态。支持通过主机IP、主机名进行模糊查询，并且支持根据登录用户及登录时间进行筛选。

通过查询登录记录，管理员可以了解安骑士发现的异地登录事件，并及时进行排查处理，检查是否有黑客入侵行为。

操作步骤

1. 定位到**主机安全** > **云主机防护** > **登录安全**页面，选择**登录记录**，如图 *4-9:* 登录记录页面所示。

图 4-9: 登录记录页面



2. 设置查询条件，单击**搜索**，查看登录记录。
   - 选择**所属区域**，查看该区域的登录记录。
   - 输入**主机IP**或**主机名**，查看该主机的登录记录。
   - 输入**对应用户名**，查看以该用户名登录的记录。
   - 设置**登录时间**，查看该时间段内的登录记录。
3. 确认登录事件。
   - 如发现该登录记录为异常记录，请立即修改该登录用户的密码，并检查该云主机的安全状态。
   - 如确认该登录记录为正常登录，单击**标记为已处理**，并在弹出的对话框中单击**确定**。该事件状态被修改为**已处理**，并且不再在控制台提示该记录。

4.5.1.2.3 暴力破解

安全管理员可以在配置中心设置登录白名单，如果暴力破解成功且登录源IP不在白名单内，将在专有云云盾安全中心提示暴力破解成功。同时，在告警设置中，可以为暴力破解事件配置手机通知和邮箱通知的告警方式。

白名单的设置请参见配置白名单，告警设置请参见告警设置。

工作原理

1. 安骑士客户端通过本地监控主机的登录记录来发现暴力破解事件，通过TCP协议上报暴力破解消息到安骑士服务器端。
2. 安骑士服务器端通过消息模块将上报的信息发送到Defender。

3. Defender分析暴力破解信息，判断暴力破解类型，以及是否暴力破解成功，并将相关信息写入Aegis-DB。如果破解成功，会将消息发送给云盾安全中心进行进一步处理，判断是否通过手机、邮件提醒用户。

暴力破解事件类型

暴力破解事件类型主要有破解成功、有威胁、无威胁和已处理，事件类型说明请参见表 *4-2:* 暴力破解事件类型表。

表 4-2: 暴力破解事件类型表

事件类型	说明
破解成功	暴力破解已成功
有威胁	暴破次数较多
无威胁	暴破次数较少
已处理	已经解决的暴力破解成功事件

4.5.1.2.4 查询暴力破解事件

背景信息

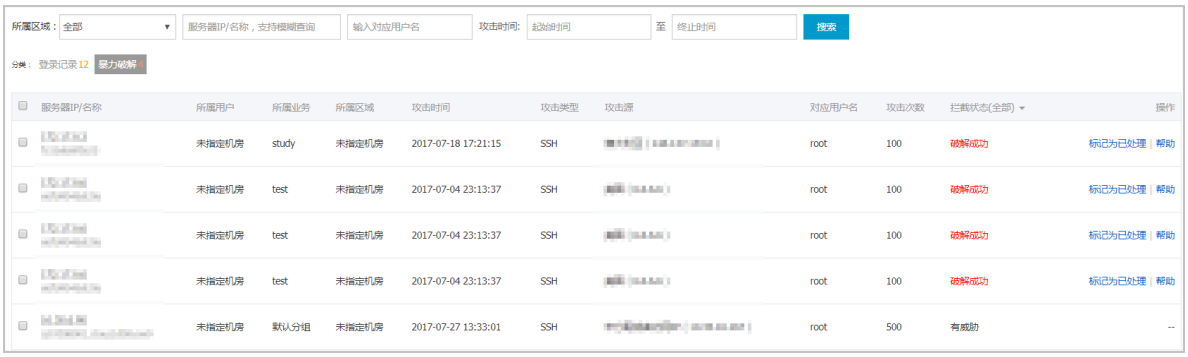
通过查询暴力破解事件，安全管理员可以了解暴力破解的攻击源、攻击次数以及拦截状态。当控制台显示暴力破解成功意味着用户的主机已经被黑客暴力破解出密码并且成功登录了主机，安全管理员需要及时进行排查处理。

暴力破解事件查询支持通过主机IP、主机名进行模糊查询，并且支持根据登录用户及登录时间进行筛选。

操作步骤

1. 定位到**主机安全** > **云主机防护** > **登录安全**页面，选择**暴力破解**，如图 *4-10:* 暴力破解事件页面所示。

图 4-10: 暴力破解事件页面



2. 设置查询条件，单击**搜索**，查看暴力破解事件。
   - 选择**所属区域**，查看该区域的暴力破解事件。
   - 输入**主机IP**或**主机名**，查看该主机的暴力破解事件。
   - 输入**对应用户名**，查看针对该用户名的暴力破解事件。
   - 设置**攻击时间**，查看该时间段内的暴力破解事件。
3. 调查暴力破解事件的原因，排除风险后，单击**标记为已处理**，在弹出对话框中单击**确定**，该事件状态被修改为**已处理**。

4.5.1.3 木马查杀

黑客入侵网站后，通常会将木马文件放在主机的Web服务目录下，和正常文件混在一起，然后通过浏览器来访问恶意文件，从而达到控制网站服务器的目的。木马查杀功能及时检测木马文件并向安全管理员告警，安全管理员可以在云盾安全中心查看已发现的木马文件，并对木马文件进行隔离、忽略、恢复、移除信任文件操作。

说明：
在已设置手机或邮件提醒的情况下，同一个木马文件只会在首次发现时推送提醒，设置提醒请参见告警设置。

4.5.1.3.1 木马事件状态说明

表 4-3: 木马事件状态说明表

状态	说明
待处理	表明该文件是有危险的木马文件。
已隔离	表明该木马已被查杀。

状态	说明
信任文件	表明该文件已查明无危险。
无需处理	表明隔离时该木马已不存在。

4.5.1.3.2 木马文件操作说明

表 4-4: 木马文件操作说明表

操作	说明	操作前状态	操作后状态
忽略	忽略木马后，将不再提示风险。	待处理	信任文件
恢复	从FTP服务器把木马文件下载到本地。	已隔离	信任文件
移除信任文件	移除信任文件后，将会继续提示风险。	信任文件	无数据
隔离	把本地木马文件删除掉，上传到FTP服务器中进行隔离。	待处理	已隔离/无需处理

说明：
当移除信任文件后，该条告警将被删除，后续扫描将会重新上报木马信息。

4.5.1.3.3 查询木马文件信息

背景信息

木马查杀状态主要分为**待处理**、**已隔离**和**信任文件**，支持通过主机名称和主机IP进行模糊查询，并且支持根据时间段进行筛选。木马事件列表可以按紧急程度排序，也可以按照组合服务器查看。

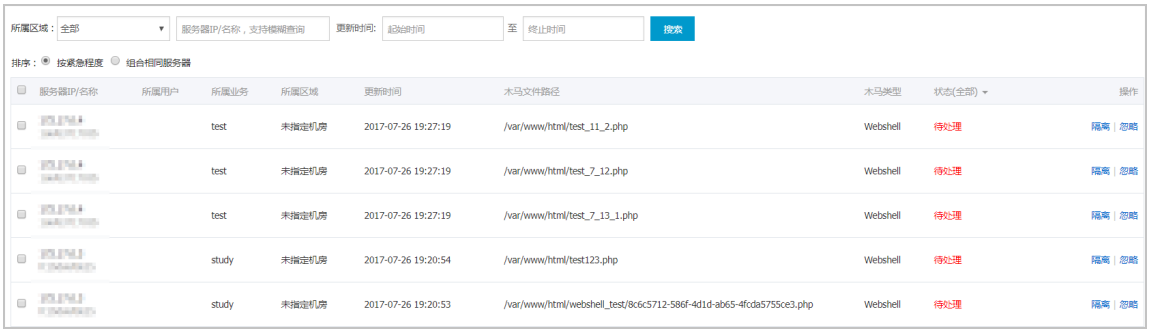
通过查询木马事件，安全管理员可以了解安骑士发现的木马文件信息。

操作步骤

1. 定位到**主机安全** > **云主机防护** > **木马查杀**页面，设置查询条件，单击**查询**。
   - 选择**所属区域**，查看该区域中云主机的木马文件记录。
   - 输入**主机IP**或**主机名**，查看该主机的木马文件记录。
   - 设置**更新时间**，查看该时间段内的木马文件记录。
2. 选择排序方式。

- 单击**按紧急程度排序**，优先展示待处理状态的木马查杀信息，再按发现时间降序排列展示，如图 *4-11: 按紧急程度排序展示*所示。

图 4-11: 按紧急程度排序展示

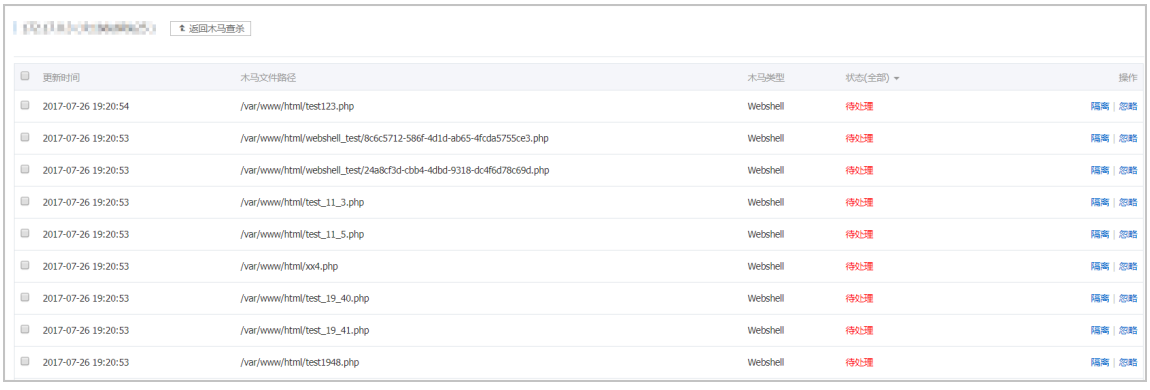


- 单击**组合相同服务器排序**，按待处理个数降序排列，如图 *4-12: 组合相同服务器排序展示*所示。

图 4-12: 组合相同服务器排序展示

在组合相同服务器排序展示情况下，单击某个服务器所在行对应的**查看详情**，可以查看该服务器下所有木马查杀的情况，根据发现时间按紧急程度排序，如图 *4-13: 查看服务器详情*所示。

图 4-13: 查看服务器详情



4.5.1.3.4 处理木马文件

背景信息

安骑士对完整的木马文件会自动隔离，对于正常内容中嵌入恶意代码的文件，安全管理员需要根据实际情况判断是否隔离恶意文件。

- 对需要删除的木马文件可执行隔离操作，该文件将被移至隔离区。
- 对被误认为是木马且已进行隔离的文件，可执行恢复操作，该文件将被恢复。
- 对非木马文件可执行忽略操作，该文件仍然保留。
- 对信任文件可执行移除信任文件操作，该信任记录将会从列表中删除。

操作步骤

1. 定位到**主机安全** > **云主机防护** > **木马查杀**页面。
2. 处理木马文件。
   - 选择待处理事件，单击**隔离**，可将该木马文件隔离。
   - 选择已隔离事件，单击**恢复**，可将该隔离文件恢复。
   - 选择待处理事件，单击**忽略**，可忽略该木马文件。
   - 选择已信任的文件，单击**移除信任文件**，可将该信任文件移除。

4.5.1.4 配置中心

配置中心支持以下配置内容：

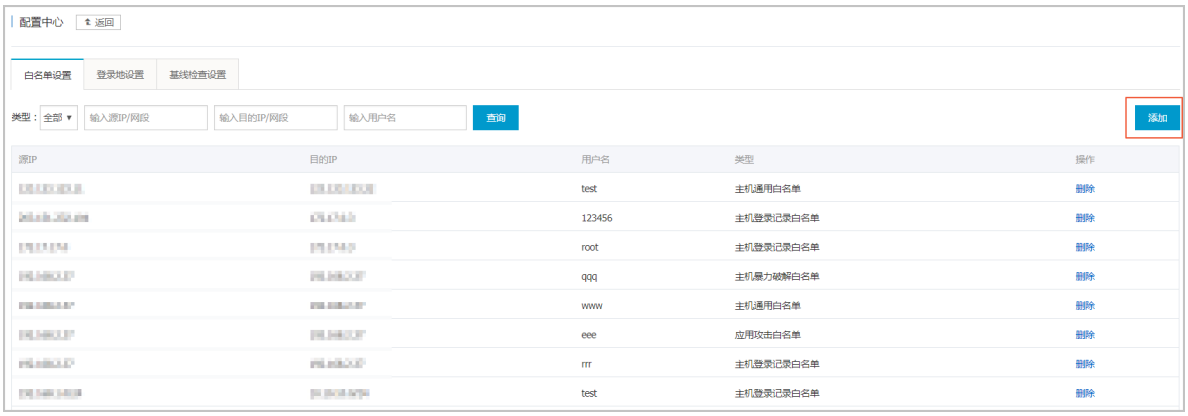
- **白名单设置**：登录IP白名单主要用于过滤暴力破解和暴力破解成功事件。如果访问源IP和目的IP在登录IP白名单中，暴力破解失败。
- **登录地设置**：常用登录地主要用于异地登录的判断。如果不设置常用登录地，不管在哪里登录，都不是异地登录。如果设置了常用登录地，在非常用登录地登录的第一次和第五次会提醒此次登录为异地登录，其余都判定为正常登录。如果在一个登录地登录次数大于等于六，这个登录地会被自动加入到常用登录地，并在页面上展示出来。

4.5.1.4.1 配置白名单

操作步骤

1. 定位到**主机安全** > **云主机防护**，单击**配置中心**，单击**白名单设置**，进入**白名单设置页面**，如图 *4-14:* 白名单设置页面所示。

图 4-14: 白名单设置页面



2. 单击**添加**。
3. 在**添加白名单**对话框中，设置需要添加的白名单 IP，选择**类型**，单击**确认**，添加白名单 IP，如图 *4-15: 添加白名单对话框*所示。

> **说明**：
> 白名单类型：
>
> - 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。
> - 主机通用白名单：符合该白名单中的登录行为、访问行为将不会被检测，包括异地登录、暴力破解、应用攻击等。
> - 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。
> - 主机登录记录白名单：符合该白名单中的登录行为将不进行异地登录检测。

图 4-15: 添加白名单对话框

白名单添加成功后，单击**删除**，可删除已不需要的白名单。

4.5.1.4.2 配置登录地

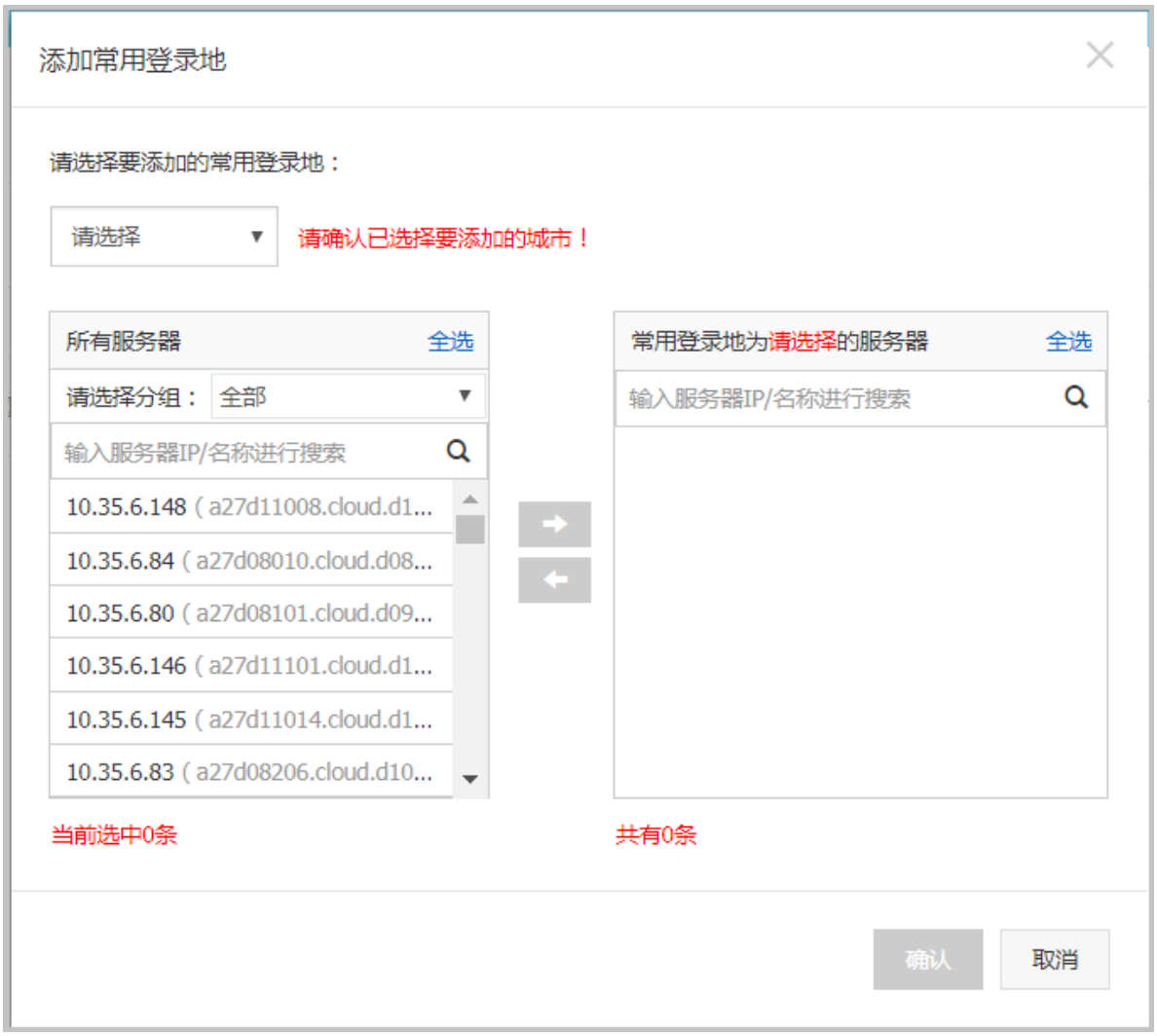
操作步骤

1. 定位到**主机安全** > **云主机防护**，单击**配置中心**，单击**登录地设置**，进入**登录地设置**页面，如图 *4-16: 登录地设置页面*所示。

图 4-16: 登录地设置页面

2. 单击**添加**。
3. 在**添加常用登录地**对话框中，设置需要添加的常用登录地，单击**确认**，添加常用登录地信息，如图 *4-17: 添加白名单对话框*所示。

图 4-17: 添加白名单对话框



常用登录地添加后，将鼠标移至已添加的常用登录地，单击编辑或删除按钮，可以修改适用该常用登录地的服务器或删除该常用登录地记录。

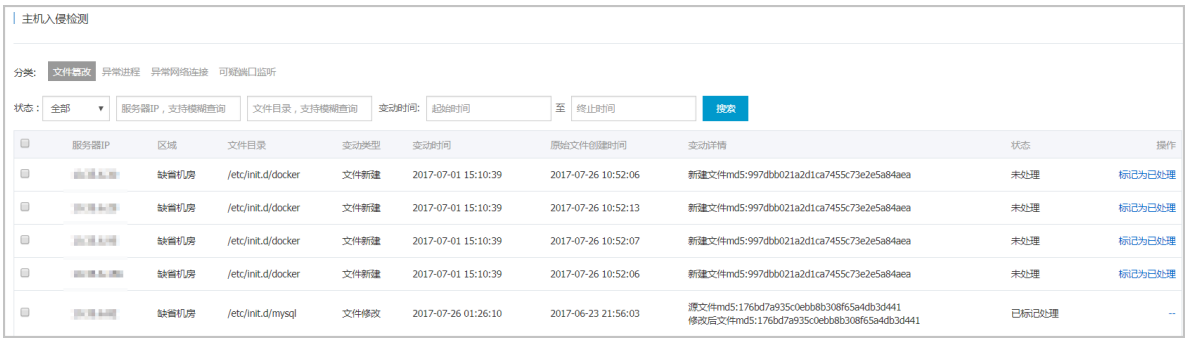
4.5.2 物理机防护

4.5.2.1 查看并处理文件篡改事件记录

操作步骤

1. 定位到**主机安全** > **物理机防护**页面，选择**文件篡改**。
2. 查看文件篡改事件记录，如图 *4-18: 文件篡改事件记录*所示。

图 4-18: 文件篡改事件记录



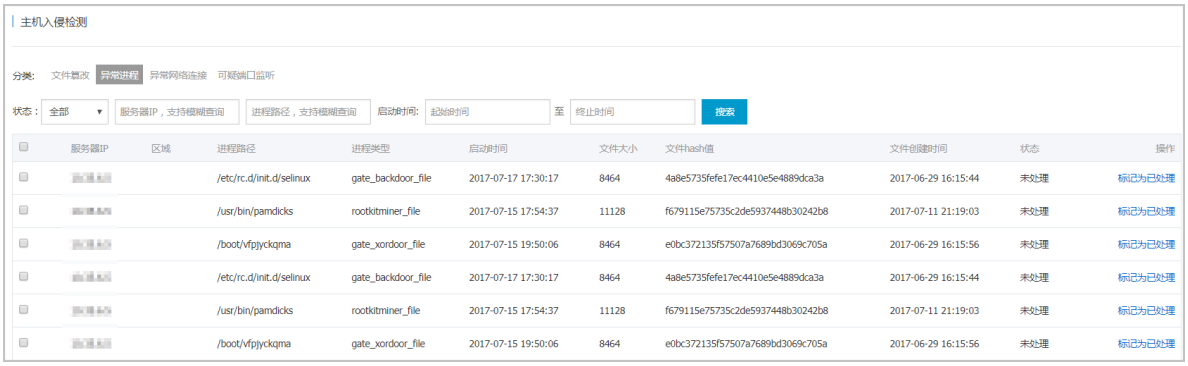
3. 进一步排查该文件篡改事件。
   - 如确认该事件为异常事件，请立即对该服务器采取安全加固措施，并进一步检查、分析被入侵的原因。
   - 如确认该事件为正常事件或已处理完该入侵事件，单击**标记为已处理**，在弹出的对话框中单击**确定**，将该事件标记为已处理。

4.5.2.2 查看并处理异常进程记录

操作步骤

1. 定位到**主机安全** > **物理机防护**页面，选择**异常进程**。
2. 查看异常进程记录，如图 *4-19: 异常进程记录*所示。

图 4-19: 异常进程记录



3. 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。

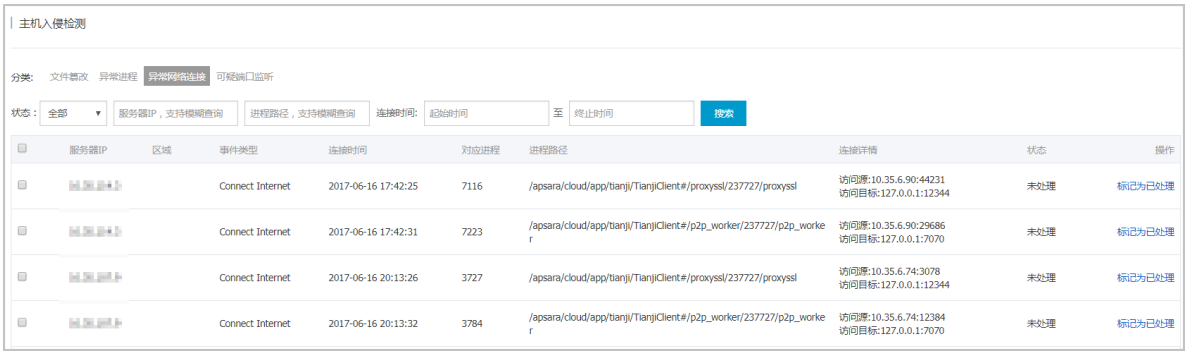
- 如确认该进程为正常进程或已处理完该异常进程事件，单击**标记为已处理**，在弹出的对话框中单击**确定**，将该事件标记为已处理。

4.5.2.3 查看并处理异常网络连接记录

操作步骤

1. 定位到**主机安全 > 物理机防护**页面，选择**异常网络连接**。
2. 查看异常网络连接记录，如图 *4-20: 异常网络连接*所示。

图 4-20: 异常网络连接



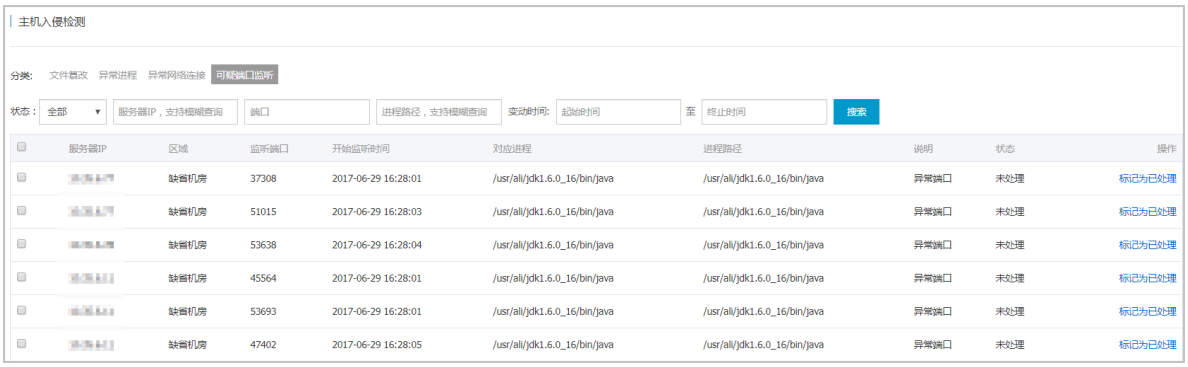
3. 进一步排查该异常网络连接。
   - 如确认该进程为异常连接，请立即对该服务器采取安全加固措施，并进一步检查、分析被入侵的原因。
   - 如确认该进程为正常连接或已处理完该异常网络连接事件，单击**标记为已处理**，在弹出的对话框中单击**确定**，将该事件标记为已处理。

4.5.2.4 查看并处理异常端口监听记录

操作步骤

1. 定位到**主机安全 > 物理机防护**页面，选择**可疑端口监听**。
2. 查看异常端口监听记录，如图 *4-21: 异常端口监听记录*所示。

图 4-21: 异常端口监听记录



3. 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。

4.6 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。

4.6.1 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。四种报表分别统计一周内发生的日志个数、事件个数、事件级别、事件类别分布，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。

- **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。

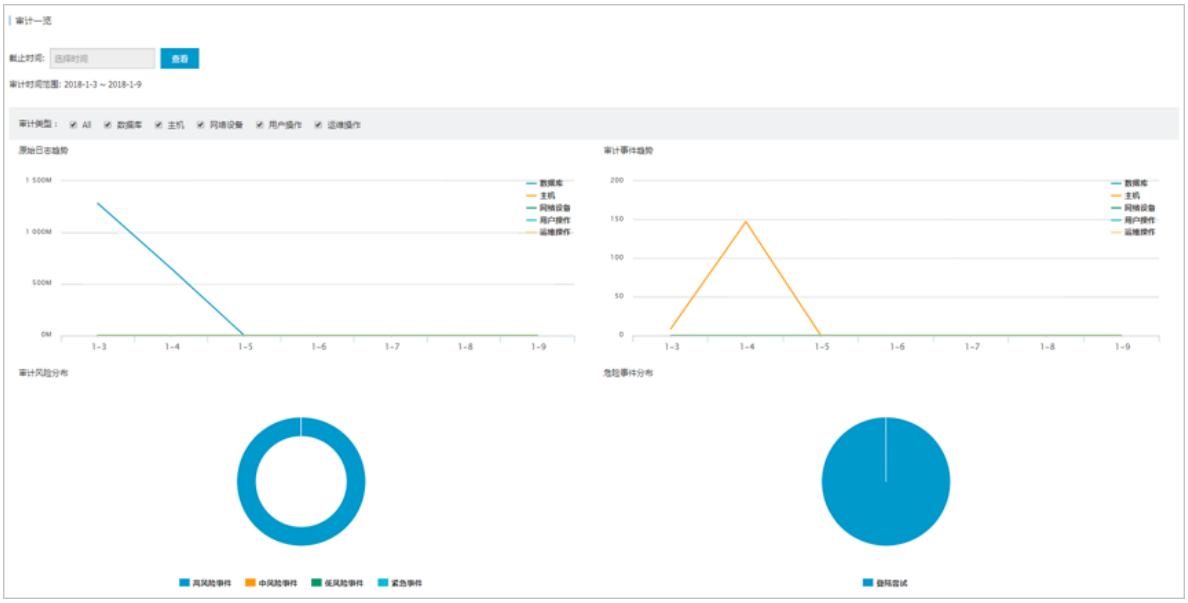
同时，在**审计一览**页面，安全管理员还可以了解指定时间范围内所有审计类型的日志量信息及存储用量情况。

4.6.1.1 查看审计一览

操作步骤

1. 定位到**安全审计** > **审计一览**，进入**审计一览**页面，如图 *4-22: 审计一览页面*所示。

   图 4-22: 审计一览页面



2. 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。

3. 勾选**审计类型**，可以选择是否显示该类型的审计日志信息。

4.6.2 审计查询

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。

审计查询生成的过程：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。

4.6.2.1 查看审计事件

操作步骤

1. 定位到**安全审计** > **审计查询**，进入**审计查询**页面。
2. 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。
3. 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。

4.6.3 原始日志

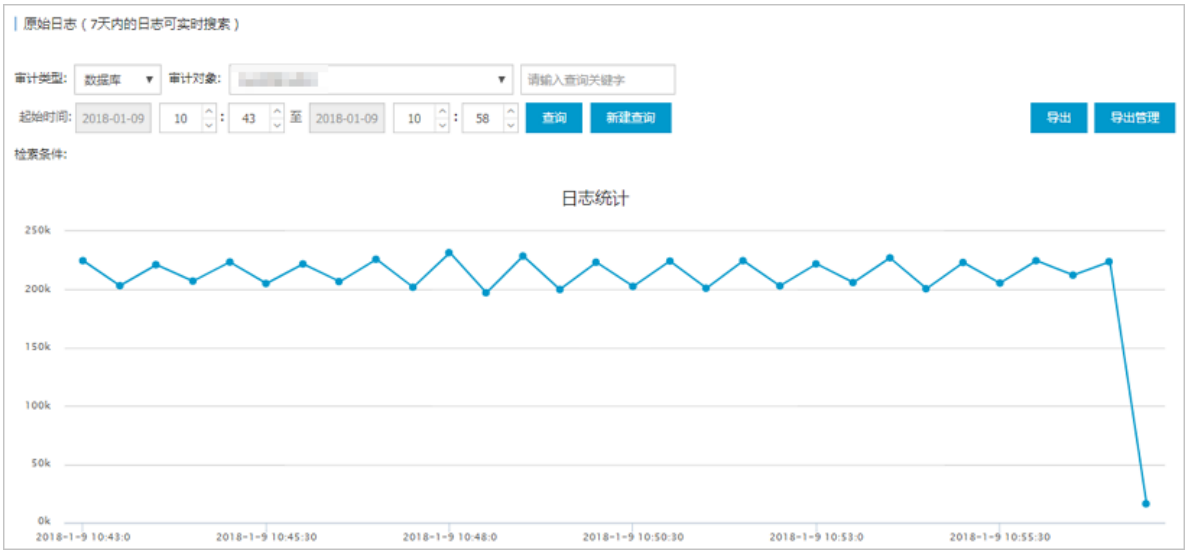
在**原始日志**页面中，可查看审计对象在运行时产生的原始日志。原始日志作为必要的调试信息，安全管理员可以根据这些日志信息定位系统出现的故障。

4.6.3.1 查看原始日志

操作步骤

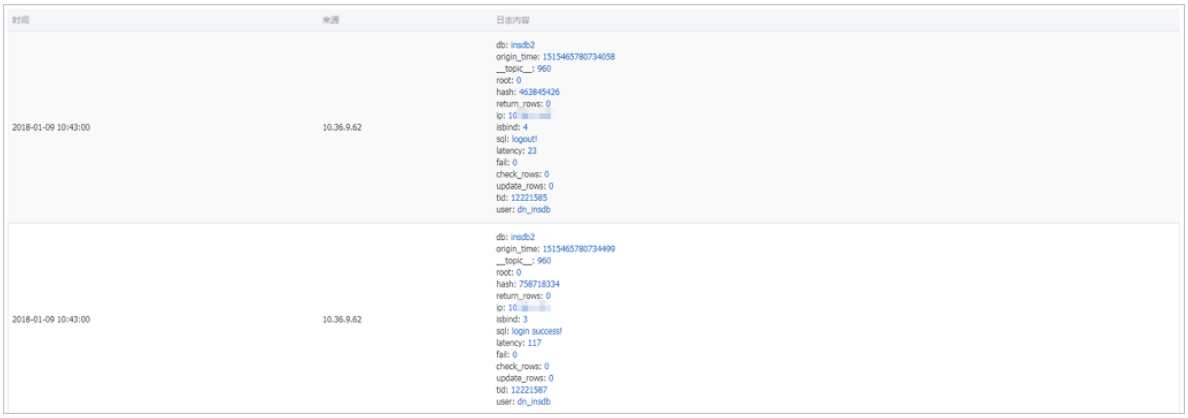
1. 定位到**安全审计** > **原始日志**，进入**原始日志**页面，如图 *4-23:* 原始日志页面所示。

图 4-23: 原始日志页面



2. 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 *4-24: 原始日志信息*所示。

图 4-24: 原始日志信息



3. 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。

4.6.4 策略设置

4.6.4.1 管理审计策略

背景信息

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。

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，^\d{5,12}$表示匹配5到12位数字，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. 定位到**安全审计** > **策略设置**，选择**审计策略**，进入**审计策略**页面，如图 *4-25: 审计策略页面*所示。

图 4-25: 审计策略页面

2. 选择**审计类型**、**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。

3. 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 *4-26: 新增规则对话框*所示。

图 4-26: 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。

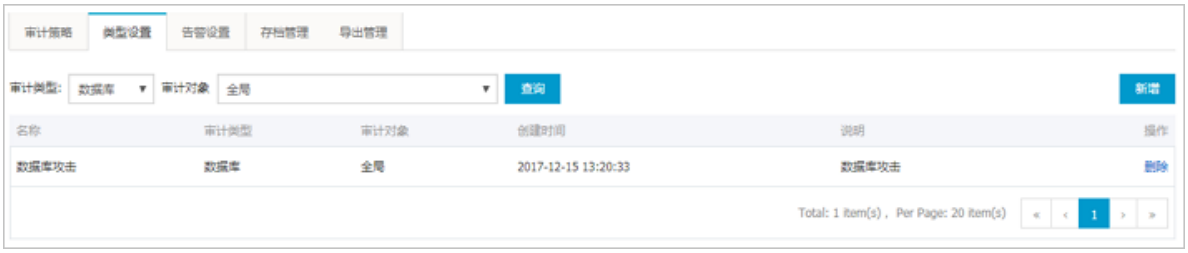
说明：
新增的审计策略默认为启用状态。

4.6.4.2 管理操作类型

操作步骤

1. 定位到**安全审计** > **策略设置**，选择**类型设置**，进入**类型设置**页面，如图 *4-27: 操作类型设置页面*所示。

图 4-27: 操作类型设置页面



2. 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。

3. 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 *4-28: 新增事件类型*所示。

图 4-28: 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。

4.6.4.3 设置告警接收人

背景信息

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. 定位到**安全审计** > **策略设置**，选择 **告警设置**，进入**告警设置** 页面，如图 *4-29:* 告警设置页面所示。

图 4-29: 告警设置页面

2. 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。
3. 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 *4-30:* 新增报警接收人对话框所示。

     图 4-30: 新增报警接收人对话框

   - 单击**删除**，可删除该告警接收人。

4.6.4.4 管理事件日志存档

操作步骤

1. 定位到**安全审计** > **策略设置**，选择**存档管理**，进入**存档管理**页面，如图 *4-31:* 存档管理页面所示。

图 4-31: 存档管理页面

2. 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。
3. 单击**下载**，可将该存档文件下载至本地。

4.6.4.5 管理导出任务

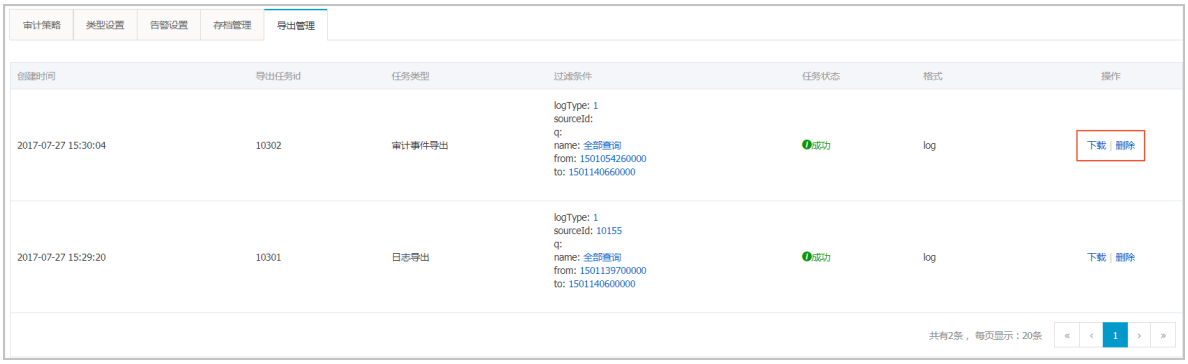
背景信息

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. 定位到**安全审计** > **策略设置**，选择**导出管理**，可以查看已创建的导出任务，如图 *4-32: 导出管理页面*所示。

图 4-32: 导出管理页面



2. 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。
3. 单击**删除**，可删除该导出任务。

4.7 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。

4.7.1 管理阿里云账号

操作步骤

1. 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 *4-33:* 阿里云账号管理页面所示。

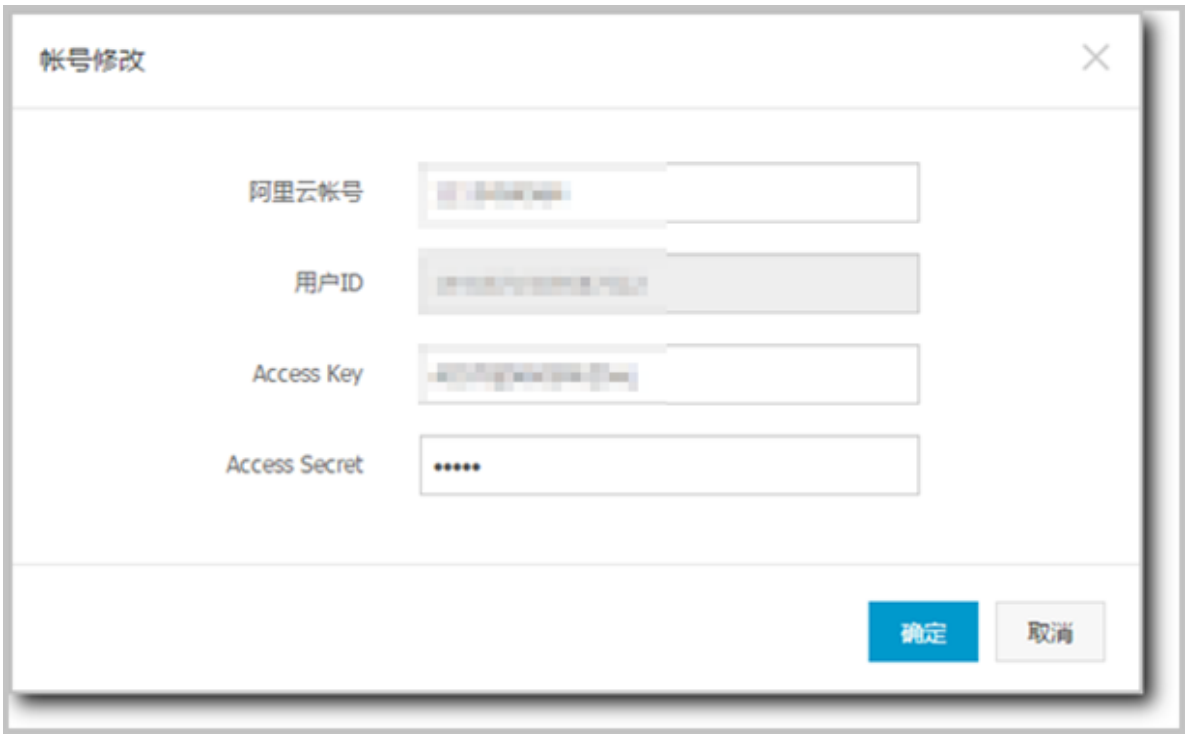
   云盾中的资产均与阿里云账号绑定，请谨慎修改。

   图 4-33: 阿里云账号管理页面

2. 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 *4-34:* 账号修改对话框所示。

图 4-34: 账号修改对话框



3. 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 *4-35:* 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 4-35: 账号详情

4.7.2 云端同步

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。

4.7.2.1 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 4-5: 同步状态说明表

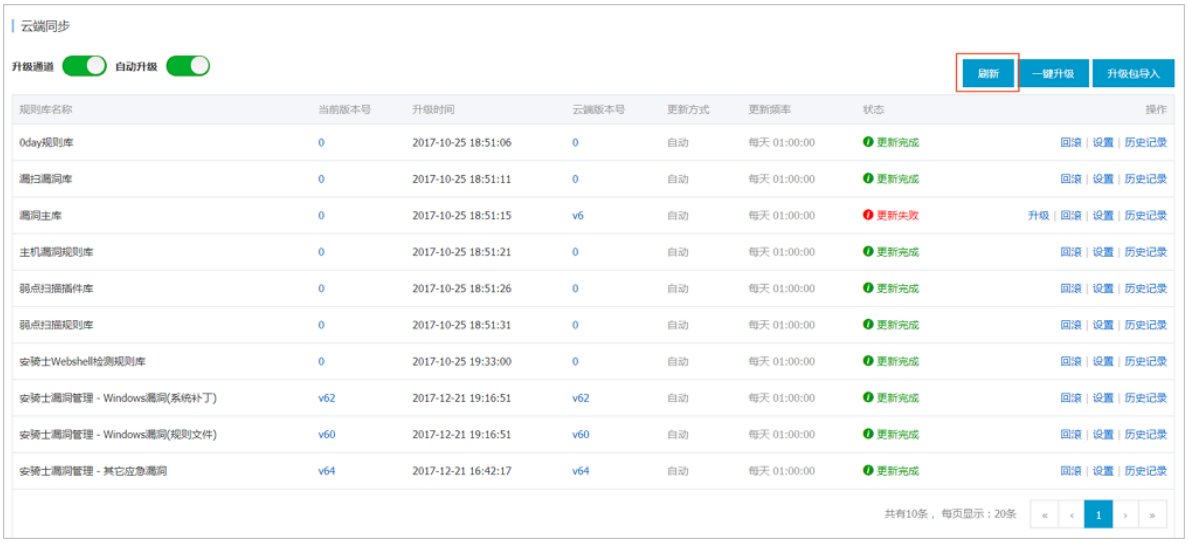
状态	说明
待更新	云端有新版本规则库可以更新。
更新中	从云端下载并更新规则库。
更新完成	规则库更新完成。
更新失败	规则库更新失败。

4.7.2.2 刷新云端同步列表

操作步骤

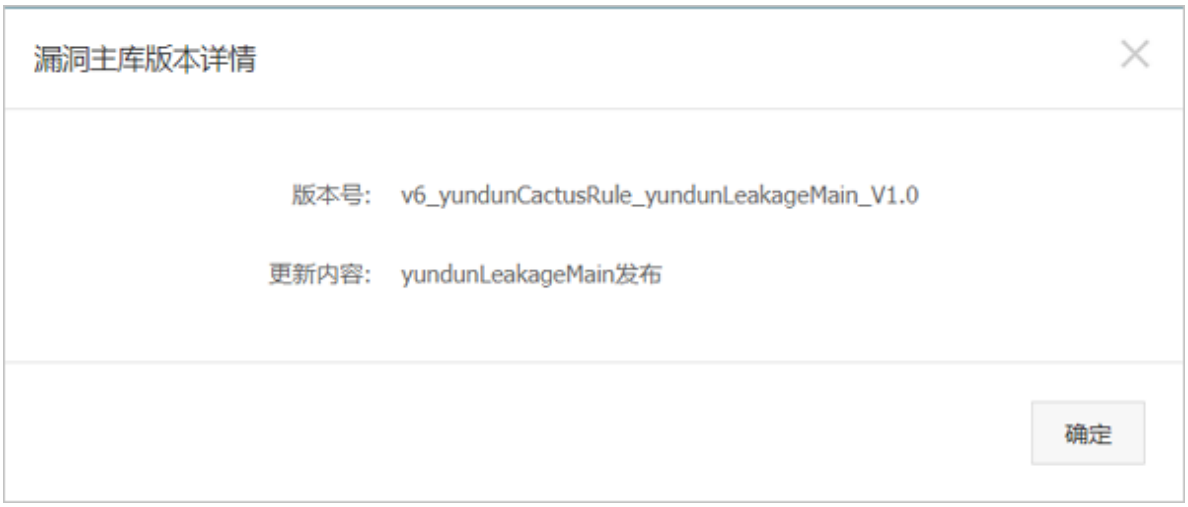
1. 定位到**系统管理** > **云端同步**页面，单击**刷新**，刷新云端同步列表，如图 *4-36: 云端同步页面*所示。

   图 4-36: 云端同步页面

2. 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 *4-37: 规则库版本详情*所示。

图 4-37: 规则库版本详情



4.7.2.3 设置更新方式及频率

操作步骤

1. 定位到**系统管理** > **云端同步**页面，选择规则库，单击**设置**。
2. 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 *4-38: 规则库更新设置*所示。

图 4-38: 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。

4.7.2.4 手动更新规则库

- 定位到**系统管理** > **云端同步**页面，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。

4.7.2.5 回滚规则库

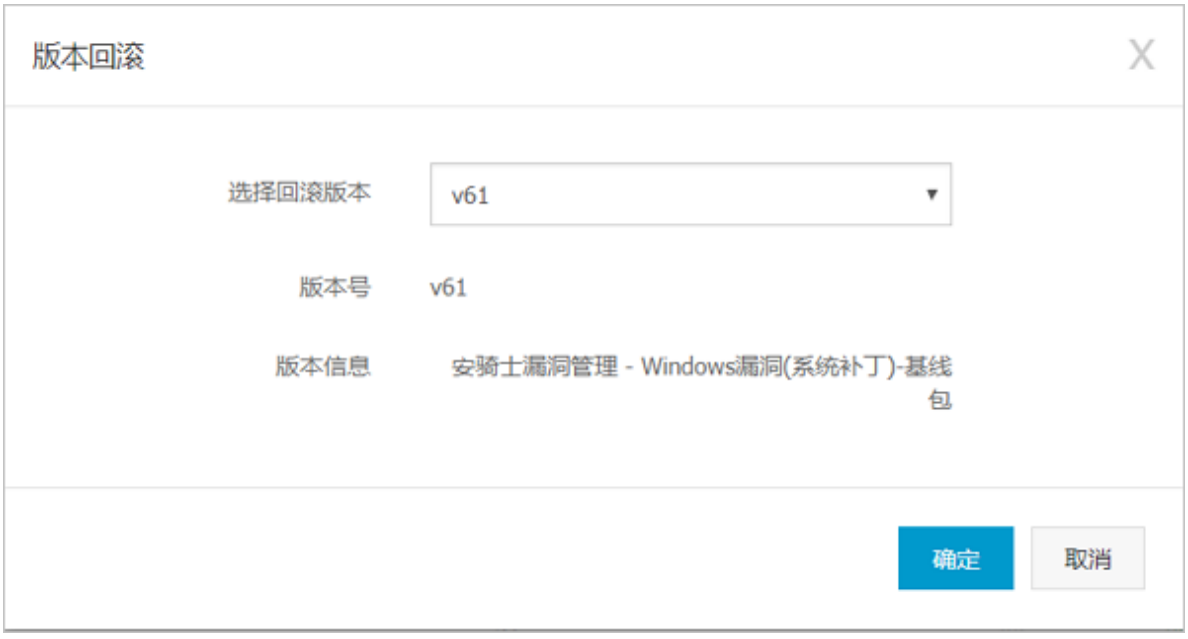
背景信息

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. 定位到**系统管理** > **云端同步**页面，选择规则库，单击**回滚。**
2. 在**版本回滚**对话框中，选择想要恢复到的规则库版本，单击**确定**，如图 *4-39: 版本回滚*所示。

图 4-39: 版本回滚



4.7.2.6 查看历史记录

- 定位到**系统管理** > **云端同步**页面，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 *4-40: 查看历史记录*所示。

图 4-40: 查看历史记录

4.7.2.7 导入离线升级包

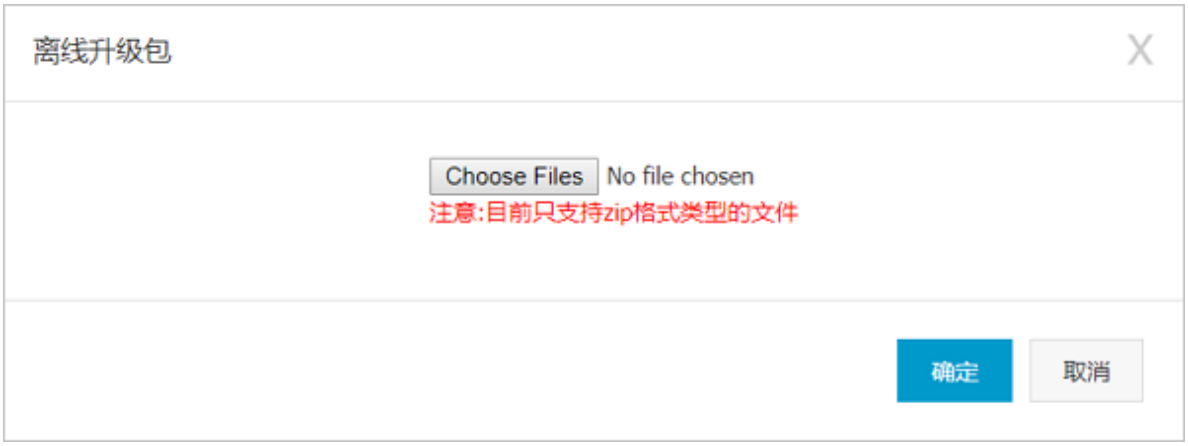
背景信息

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. 定位到**系统管理** > **云端同步**页面，单击右上方的**升级包导入**。
2. 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，单击**确定**，如图 *4-41: 导入离线升级包*所示。

图 4-41: 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。

4.7.3 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。

4.7.3.1 设置告警联系人

背景信息

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. 定位到**系统管理** > **告警设置** > **告警联系人**页面，单击**添加联系人**，如图 *4-42: 告警联系人页面*所示。

   图 4-42: 告警联系人页面

2. 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。

4.7.3.2 设置告警信息

背景信息

告警设置可以对安全事件（登录安全-异地登录）、紧急事件告警（网页篡改、肉鸡行为、爆破成功、发现后门、被DDoS攻击、黑客访问、异常网络连接和未授权下载）、攻击告警（暴力破解攻击、高级威胁攻击和Web应用攻击）、弱点告警（发现弱口令、发现漏洞和应用配置项隐患）、情报信息告警（人员信息泄露、重要漏洞、应急响应和行业新闻）进行告警，告警方式包括手机和邮件。

- 定位**系统管理** > **告警设置** > **告警设置**页面，为各个安全事件选择通知方式，单击**确认**，如图 *4-43: 告警设置页面*所示。

图 4-43: 告警设置页面

4.7.4 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。

4.7.4.1 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。

4.7.4.1.1 添加流量采集网段

操作步骤

1. 定位到**系统管理** > **全局设置** > **流量采集网段设置**页面，单击**添加**，弹出**添加监控网段**对话框，如图 *4-44:* 添加监控网段对话框所示。

图 4-44: 添加监控网段对话框

2. 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。

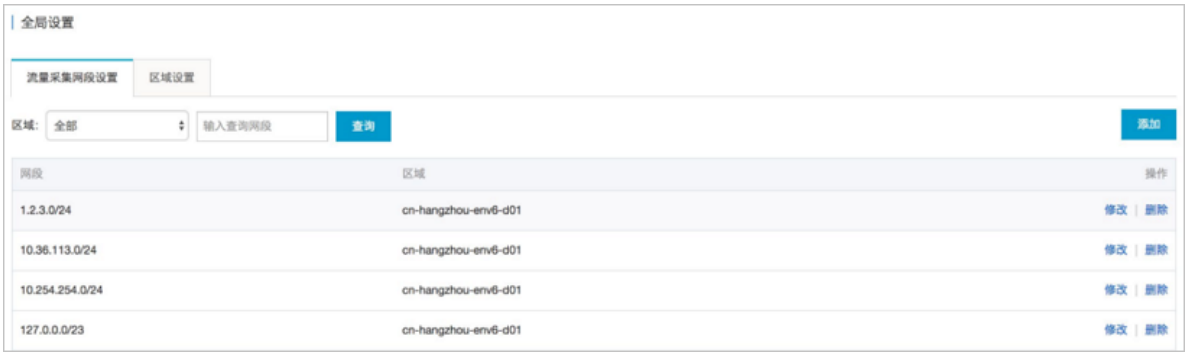
3. 选择所属区域。
4. 单击**确定**，完成添加。

4.7.4.1.2 管理流量采集网段

操作步骤

1. 定位到**系统管理** > **全局设置** > **流量采集网段设置**页面，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 *4-45: 全局设置页面*所示。

图 4-45: 全局设置页面



2. 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。

4.7.4.2 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。

4.7.4.2.1 添加区域网段

操作步骤

1. 定位到**系统管理** > **全局设置** > **区域设置**页面，单击**添加**，弹出**添加网段**对话框，如图 *4-46: 添加网段对话框*所示。

   图 4-46: 添加网段对话框

2. 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。

3. 选择所属区域。

4. 单击**确定**，完成添加。

4.7.4.2.2 管理区域网段

操作步骤

1. 定位到**系统管理** > **全局设置** > **区域设置**页面，选择区域，输入查询网段，单击**查询**，查看区域网段信息，如图 *4-47: 区域设置页面*所示。

   图 4-47: 区域设置页面

2. 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。