阿里云
专有云Enterprise版

安全管理员指南

产品版本：V3.0.0

文档版本：20171101

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

表 1: 格式约定

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

阿里云专有云包含了云盾基础版及高级版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一键处理。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。

2 配置要求

当您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: 配置要求表中要求才可以正常登录。

表 2: 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

前提条件

在 DTCenter 服务的**用户中心**页面创建专有云云盾安全中心用户并分配云安全中心安全管理员、云安全中心安全审计员及云安全中心系统管理员角色。

说明:

- **云安全中心安全管理员**：拥有云安全中心所有安全事件的操作权限。
- **云安全中心安全审计员**：拥有云安全中心审计日志、审计事件、审计规则等的操作权限。
- **云安全中心系统管理员**：拥有安全日志和报警设置管理、安全中心和控制台用户授权的权限。
- **云安全中心安全监察员**：拥有云安全中心所有安全事件的查看权限。

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，如图 *1: DTCenter*登录页面所示。

图 1: 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。单击**安全中心**，进入云盾安全中心页面，如图 *2:* 安全中心页面所示。

图 2: 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 DTCSC 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 注销

操作步骤

在专有云云盾控制台页面，单击页面右上角的退出图标，如图 *3:* 用户注销所示，即可退出登录。

图 3: 用户注销


退出

4 云盾（高级版）

4.1 产品概述

概述

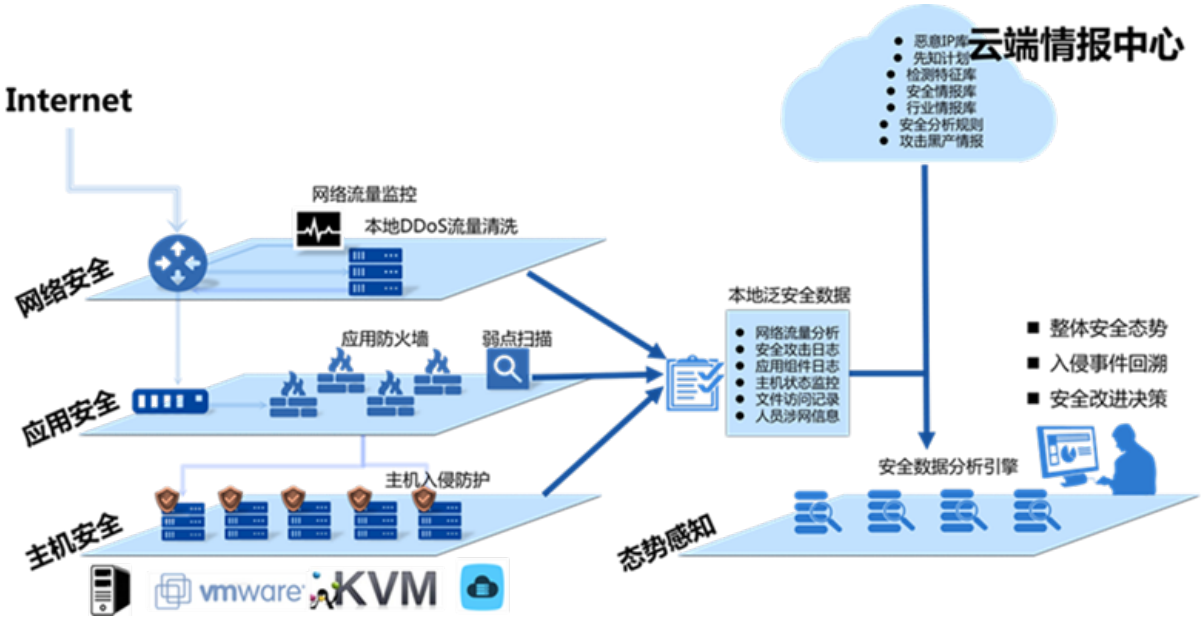
云盾以阿里云互联网攻防技术为核心，为您建设涵盖网络安全、应用安全、主机安全、安全态势感知的全方位互联网安全攻防体系。不同于以往以检测技术为主的边界防护方式，云盾防护以泛安全数据与情报联动分析为驱动，为您提供全景的安全态势感知、攻击溯源回溯、基础安全防护等功能。通过纯软件化的部署方式，云盾可以帮助您在自有 IDC、专有云、公共云、混合云等多种业务环境获得与阿里云同等强度的互联网防护能力。

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，能够为您提供 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。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，为您呈现整体安全态势、入侵事件回溯，如：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。

架构

专有云云盾体系架构如图 4: 专有云云盾体系架构所示。

图 4: 专有云云盾体系架构



4.2 云盾安全中心界面概述

专有云云盾安全中心的界面主要可以分为三大区域，如图 5: 云盾安全中心页面所示。

图 5: 云盾安全中心页面

Web 功能区域说明请参见表 3: 功能区域说明表：

表 3: 功能区域说明表

区域	说明

菜单导航树区	专有云云盾控制台包含态势感知、安全能力、服务器安全、资产管理、安全审计、系统管理六个部分，主要功能如下：
	• 态势感知：捕获和分析网络安全态势、对威胁进行关联回溯和大数据分析，展示可能产生的安全事件的威胁风险。
	• 安全能力：预防和检测攻击行为，以便管理员进行分析和处理。
	• 服务器安全：提供主机防护及主机入侵检测，保障服务器安全。
	• 资产管理：通过图表方式展现当前用户资产的总数、增减频率、以及区域分布等统计信息，并按分组、类型供管理员查询浏览资产的相关信息，帮助管理员从整体了解资产情况，以更好地管理资产。
	• 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。
	• 系统管理：
	  ▪ 用户管理：对登录系统的账号进行增删改和重置密码。
	  ▪ 情报同步：同步阿里公共云上的数据到本地数据库。作用一是在态势感知的情报里展示出来，作用二是用于匹配 WAF 攻击，匹配的结果在态势感知的威胁页面中展示。

区域	说明
	▪ 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	当选择了菜单项后，该菜单项的功能配置界面就会显示在右侧的操作视图区中。
操作按钮区	 ：单击此按钮退出当前登录。  ：单击此按钮进入修改个人信息页面  ：单击此按钮进入总览页面。

4.3 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。

动态感知主要包含五个部分：

- 安全总览：展现安全的整体态势、网络流量情况和大屏相关信息。
- 紧急事件：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：展现业务系统中目前面临的安全风险和威胁来源。
- 弱点分析：展现业务系统中存在的安全隐患。
- 情报分析：展现自身泄露的重要信息和目前网络安全的最新情报。

4.3.1 总览

4.3.1.1 简介

总览页面展示了态势感知的概貌，从紧急事件、威胁、弱点、情报、网络流量、访问分析和可视化大屏几个方面，对当前的安全态势进行概要性展示，以便用户快速了解和掌握当前安全态势。

总览主要包括如下几个方面：

- 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和整个互联网上目前的安全情报进行概要性展示。
- 紧急事件：紧急事件是目前用户系统中已经发生的事件，表明用户已经遭受或正在遭受安全攻击，用户需要紧急采取措施，抵御攻击。
- 威胁：威胁是尚未发生，但由云盾通过大数据分析和扫描器的信息收集，甄别出的系统可能面临的威胁事件，需要用户提高安全警惕性。
- 弱点：弱点是对用户系统自身存在的弱点或缺陷的扫描和分析，展示了用户系统中可能被黑客非法利用的漏洞信息，需要用户及时修正，提高系统的安全性。
- 情报：云安全的时代已经到来，单个系统对安全的感知是有限的，通过对整个互联网安全信息的过滤收集和有效分析，才能把握整个互联网的安全态势，也为单个系统的安全防御提供指导。
- 网络流量：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。
- 访问分析：访问分析可识别访问者身份，向用户展示访问者信息及访问页面信息。
- 可视化大屏：可视化大屏为用户提供最直观的安全形势和面临威胁的展示，为指导安全决策提供重要的参考指标。

4.3.1.2 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、最新情报和资产的概览情况，使您全方位、整体性把握自身系统的安全态势。

操作步骤

选择**态势感知** > **总览**，在此页面可以查看目前系统安全的总览情况，如图 *6:* 总览页面所示。

图 6: 总览页面

表 4: 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，从时间维度展示了系统安全态势的变化。
最新威胁	最新威胁展示了系统目前面临的安全威胁，急需用户积极关注。这些威胁事件都是由云盾的核心扫描器扫描并通过专有云特有的大数据分析模型分析获得。
最新情报	情报从公共云同步而来，针对单机环境对外界消息的闭塞，通过公共云强大的整个互联网的安全形势分析，为您提供重要安全参考和情报信息。
资产概览	选取您最关心的资产情况进行展示，使您实时掌握资产状态。

4.3.1.3 查看网络流量信息

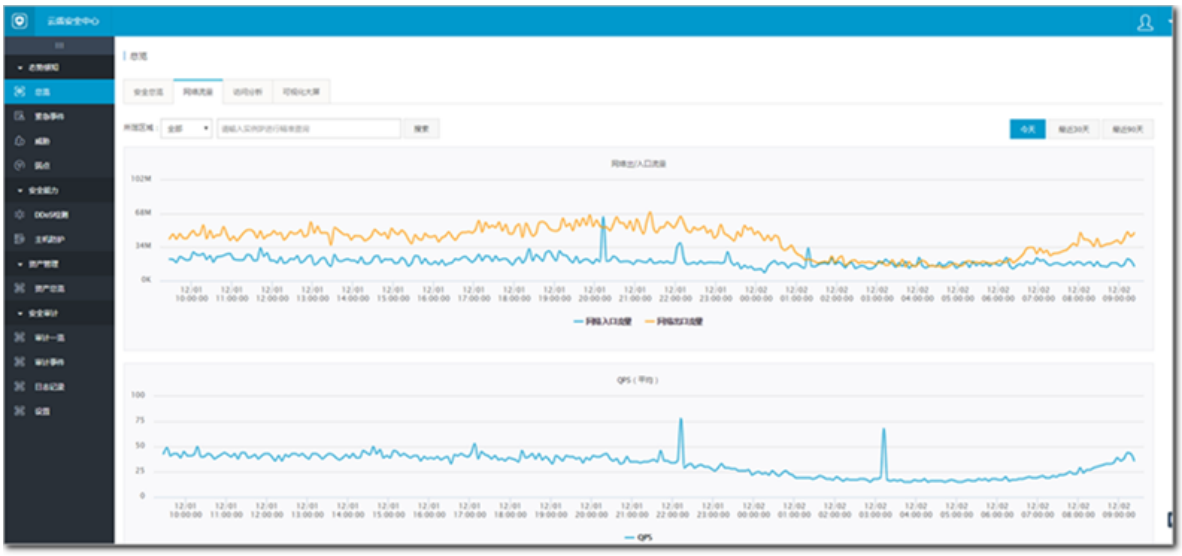
背景信息

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. 单击**总览** > **网络流量**，进入流量查看页面，如图 7: 网络流量页面所示。

图 7: 网络流量页面

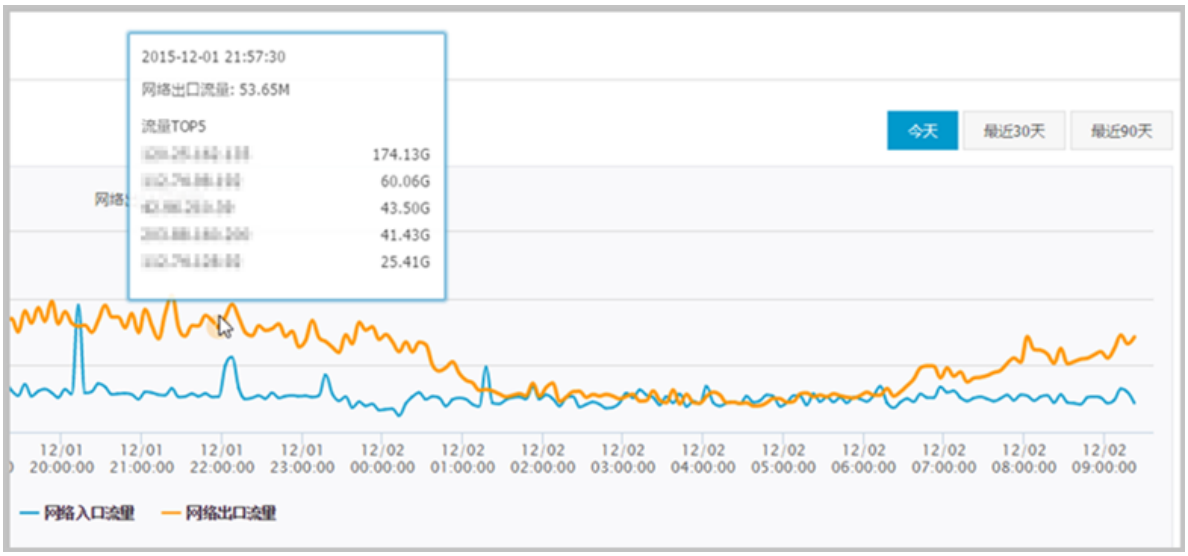


2. 单击页面上的**今天**、**最近30天**、**最近90天**按钮可以切换查看不同时间段的流量信息。
3. 在**所属区域**中可以选择区域信息，在搜索框中输入 IP，可以分区域、分 IP 查询流量信息，如图 *8:* 选择所属区域所示。

图 8: 选择所属区域

4. 将鼠标停留在流量折线图上，可以显示流量 TOP5 的 IP，如图 *9:* 查看流量 *TOP5* 的 *IP*所示。

图 9: 查看流量 TOP5 的 IP



4.3.1.4 查看访问分析结果

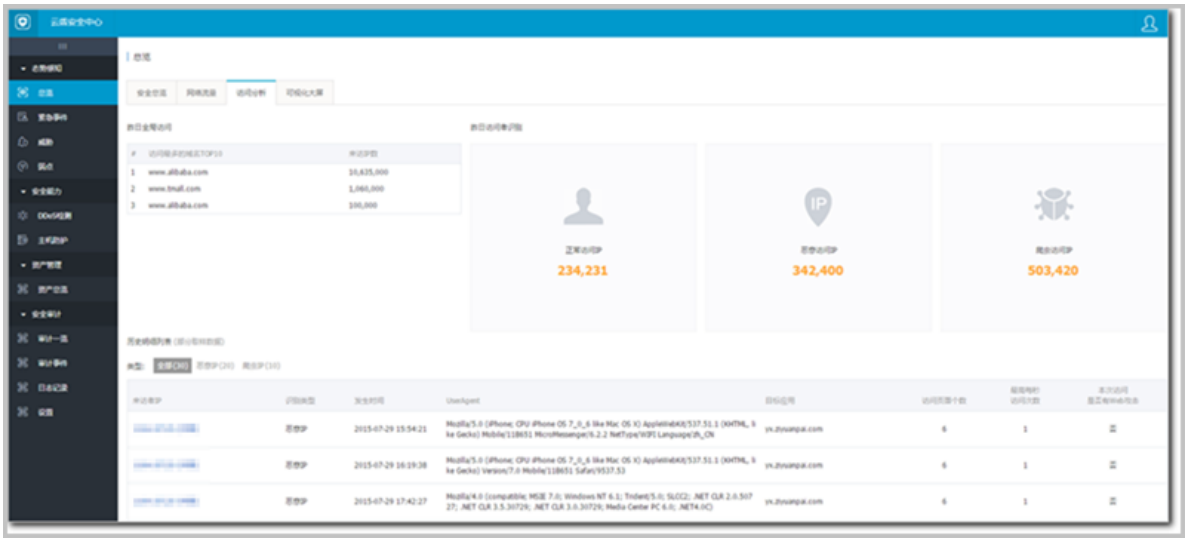
背景信息

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，您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

选择**总览** > **访问分析**，查看访问分析页面，如图 *10:* 访问分析页面所示。

图 10: 访问分析页面



4.3.1.5 查看可视化大屏

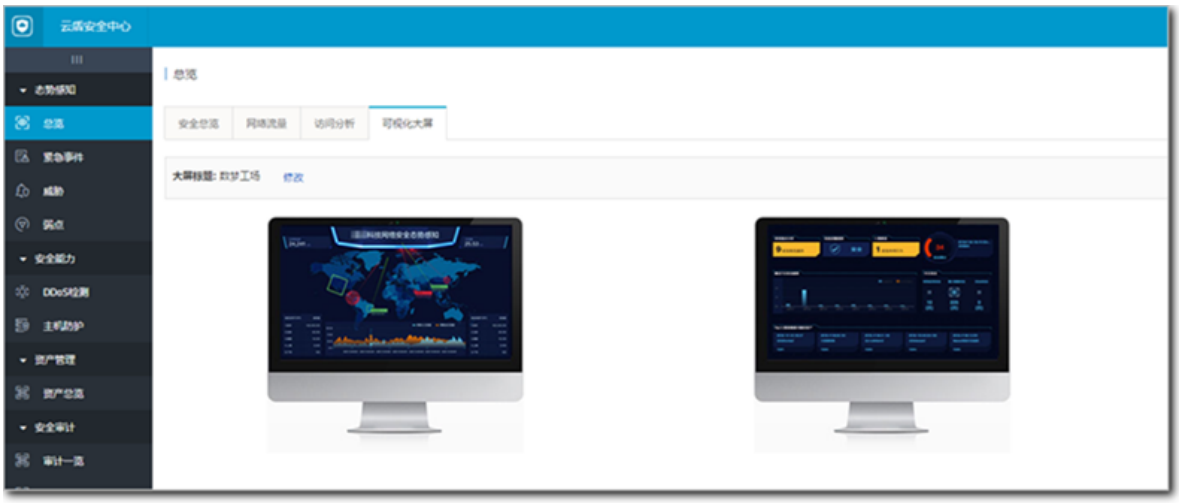
背景信息

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，使您一目了然地掌握当前的整体安全态势，为您的决策提供有效支持。目前开放的大屏有访问流量大屏和安全监控大屏。

操作步骤

1. 选择**总览** > **可视化大屏**，进入可视化大屏入口，如图 *11:* 可视化大屏页面所示。

   图 11: 可视化大屏页面

   单击页面上的**修改**，可以修改第一块大屏显示的标题。

2. 单击页面上显示的屏幕，可以进入大屏页面。

   - 访问流量大屏

     访问流量大屏是依托核心组件 beaver 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和数量进行统计，同时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，使您对请求的压力来源和攻击的地域分布有准确的了解，及时掌握攻击的分布的地域规律，如图 *12:* 访问流量大屏所示。

     访问流量大屏的流量来源和实现的机制参见表 *5:* 访问流量数据来源表。

     图 12: 访问流量大屏

表 5: 访问流量数据来源表

类型	实现的机制
请求分析	将您关注的资产推送给 beaver，beaver 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	由核心组件 beaver 检测，针对于类似 WAF 攻击的事件进行上报和展示。
流量展示	由 beaver 收集流量信息并上报给控制台记录。

- 访问安全监控大屏

  安全监控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，为系统的安全状况打分评价，提示目前系统的安全等级。此页面的数据主要是专有云云盾核心的组件：beaver、安骑士和漏洞扫描等模块进行扫描并上报。TOP5 黑客最感兴趣资产由大数据通过模型分析获得，如图 *13:* 访问安全监控大屏所示。

图 13: 访问安全监控大屏

4.3.2 紧急事件

紧急事件是系统中已经或正在发生的安全事件，事件被专有云云盾的核心组件扫描到并上报，需要用户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 *6:* 紧急事件类型表。

表 6: 紧急事件类型表

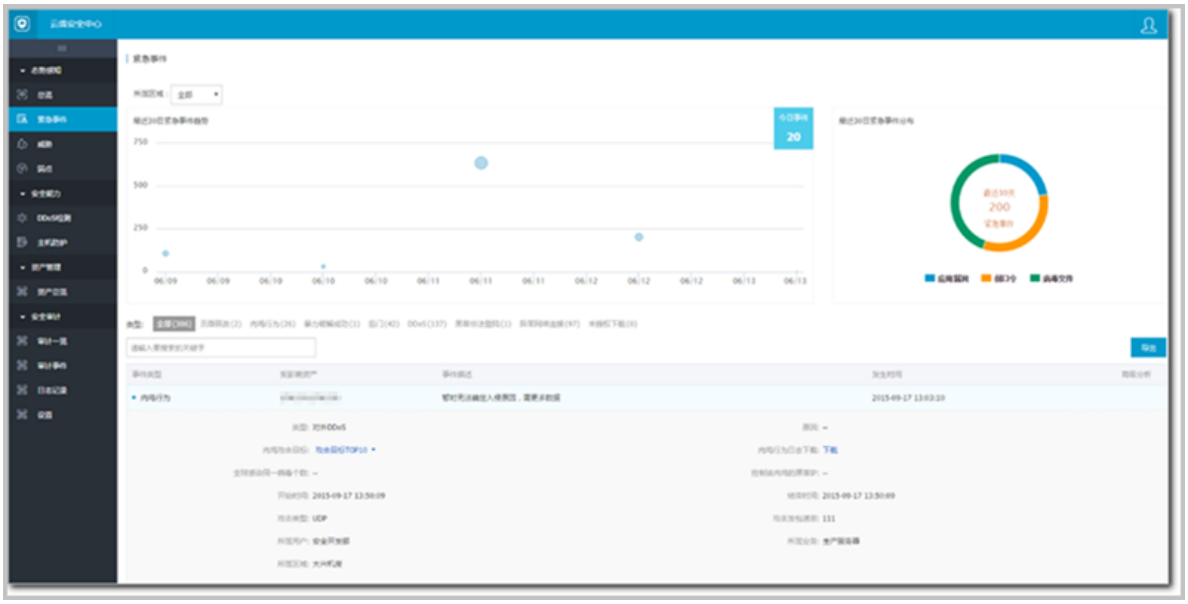
紧急事件类型	说明
后门	安骑士客户端将检测用户系统中的 webshell，大数据分析模块通过对 beaver 导入流量的分析，将检测出一句话木马和多功能木马。
暴力破解成功	用户每台主机都需要安装安骑士客户端，当暴力破解发生和爆破成功时，安骑士都会上报信息，爆破成功会在紧急事件中显示，需要用户紧急处理。
未授权下载	从 beaver 流量中选择出较为特别的，数量在一个范围内（大于1小于20）的 response 进行筛选，通过大数据分析模型分析得出未授权下载的情况。
肉鸡行为	用户的主机被黑客控制沦为肉鸡并对外进行攻击。
页面篡改	云盾的核心组件漏扫模块将对可达的页面进行扫描，上报页面的篡改信息，目前主要针对的类型是暗链。

4.3.2.1 查看紧急事件

操作步骤

1. 选择**态势感知** > **紧急事件**，进入紧急事件页面，如图 *14:* 紧急事件页面所示。

图 14: 紧急事件页面



2. 在**态势感知** > **紧急事件**页面**类型**一栏中，可以输入搜索关键字，进行页面搜索。

4.3.3 威胁

4.3.3.1 简介

威胁页面包括威胁分析和攻击两类。

威胁分析：是通过对流量信息进行专有云特有的大数据模型的分析，产出攻击特征，按攻击行为进行整合，提供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：

- 页面展示了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：是利用大数据模型进行分析处理，按照各个资产收到的威胁的得分的大小，选择威胁得分最高的 5 个资产进行展示，以便用户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 beaver 流量进行分析，分析和甄别出针对性攻击。目前包含的针对性攻击如表 *7:* 针对性攻击类型说明表所示。

表 7: 针对性攻击类型说明表

针对性攻击类型	说明
针对性主机密码爆破	针对性主机密码爆破是明显针对您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您的资产。
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您的网站，这将会导致您的用户利益遭受损失。
批量账号登录	检测到攻击者使用大量的低质量账号登陆，则这批账号很可能是僵尸账号。
定点 Web 攻击	定点 Web 攻击是明显针对您的 Web 攻击，这意味着相对于其他用户，黑客更关心您的 Web 站点，对您的 Web 站点进行了 SQL 注入、命令执行、目录扫描等恶意操作。
CMS 异常登录	检测到应用的管理后台存在异地登陆事件。如果本次登陆不是您本人操作，那么黑客可能已经窃取到您的后台密码，建议您检查密码是否存在弱口令，并尽快修改现有密码。

攻击主要包括 Web 应用攻击和暴力破解两类：

- Web 应用攻击：访问 Web 服务器的流量都会进过云盾的核心组件 beaver，beaver 将对流量进行监测，提取流量中的攻击信息。考虑到具体业务的需求，目前 beaver 尚未提供对攻击流量的阻断功能。
- 暴力破解：每台资产都需要安装安骑士客户端，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爆破的发生并上报给控制台。

4.3.3.2 查看威胁分析结果

操作步骤

选择**态势感知** > **威胁**，进入**威胁分析**页面，如图 *15:* 威胁分析页面所示。

图 15: 威胁分析页面

在此页面可以查看最近 7 日攻击趋势、最近 30 日攻击分析、黑客最感兴趣的资产 IP，及针对性攻击分析。

4.3.3.3 查看攻击信息

操作步骤

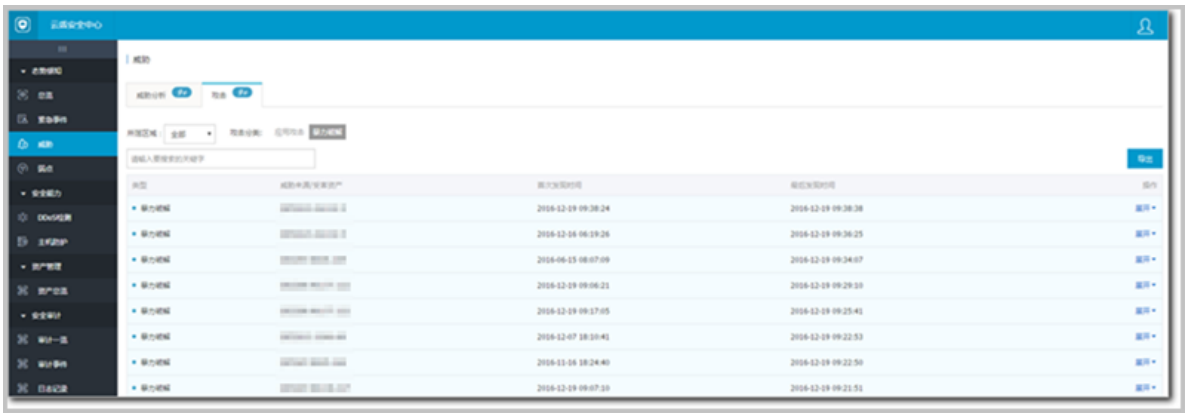
1. 选择**攻击** > **应用攻击**，进入**应用攻击**页面，如图 *16:* 应用攻击页面所示。

图 16: 应用攻击页面

您可以查看最近 7 日的攻击趋势、攻击的类型以及详细的攻击信息。

2. 选择**攻击** > **暴力破解**，查看暴力破解事件记录，如图 *17:* 暴力破解页面所示。

图 17: 暴力破解页面



4.3.4 弱点

4.3.4.1 简介

弱点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，需要您及时消除弱点，提升系统的安全性。目前弱点主要包括以下三类：

- 漏洞
  - 应用漏洞：漏扫模块依赖 agent 引擎具备的规则对系统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：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：是检测用户资产中简单的、容易被人猜测到或破解的口令，以便提醒用户及时修改用户和密码，提升用户名和密码的复杂度。

  弱密码和弱口令对于用户系统来说是巨大的安全隐患，我们建议您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；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，专有云云盾支持用户自定义弱口令，可以将用户习惯性的用户名和密码添加到漏扫模块的扫描规则中，实现对用户系统个性化的弱口令扫描。
- 配置项泄露：是指用户的系统配置文件或者敏感文件由于存放位置不当导致，被攻击者在未授权的情况下获得，导致用户关键信息的泄露，漏扫模块将对用户系统中的配置文件扫描，并提示可能被未授权访问的配置项文件。

专有云云盾的核心组件弱扫模块包括 cactus-batch 和 cactus-keeper 两个模块，batch 模块负责数据的处理，将需要扫描的 url 处理后通过消息队列发送给 keeper 模块消费。cactus-keeper 集成了扫描引擎，具备阿里云积淀丰富的扫描规则和插件库，能对系统的漏洞、弱口令和配置项进行细致的扫描，及时发现和上报系统中存在的弱点，让您对自身系统的缺陷不足有充分的了解，以便采取措施应对这些缺陷。

4.3.4.2 查看漏洞信息

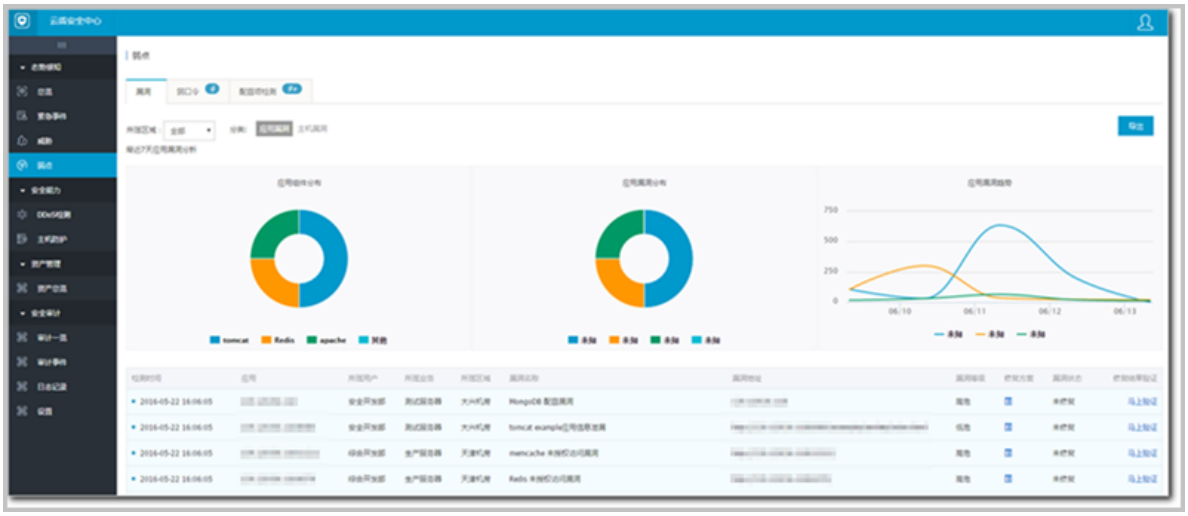
背景信息

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，主机漏洞是主机本本身存在的漏洞信息，由安骑士模块扫描并上报。应用漏洞页面显示如下。**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。

操作步骤

1. 选择**态势感知** > **弱点**，进入**漏洞**页面，查看应用漏洞信息，如图 *18:* 应用漏洞页面所示。

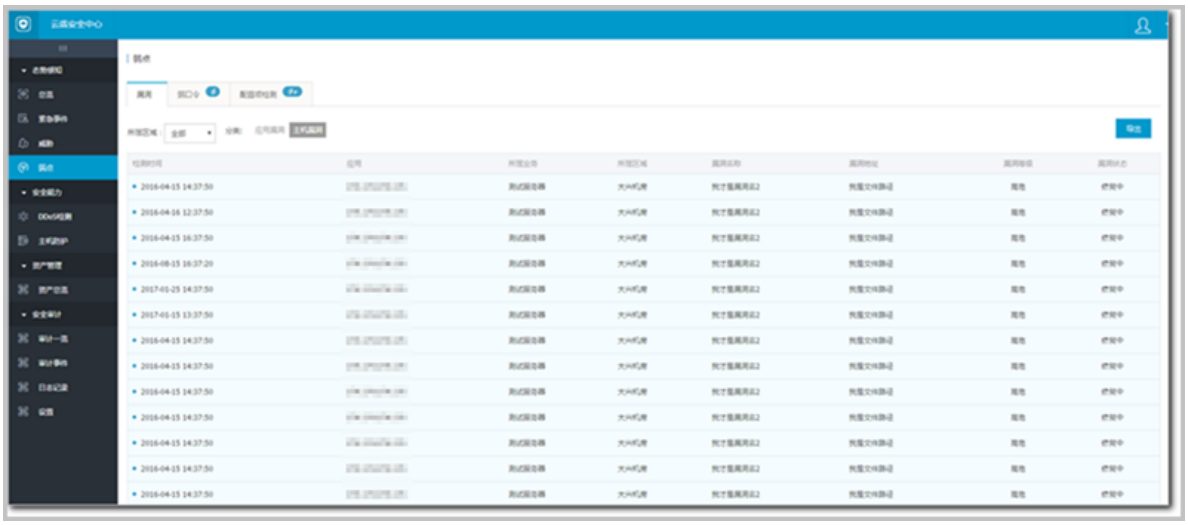
图 18: 应用漏洞页面



单击应用漏洞列表**修复结果验证**一栏的**马上验证**，可以向漏扫模块发出验证信息，校验当前漏洞的修复状态。

2. 单击**漏洞** > **主机漏洞**，可查看主机漏洞信息，如图 *19:* 主机漏洞页面所示。

图 19: 主机漏洞页面



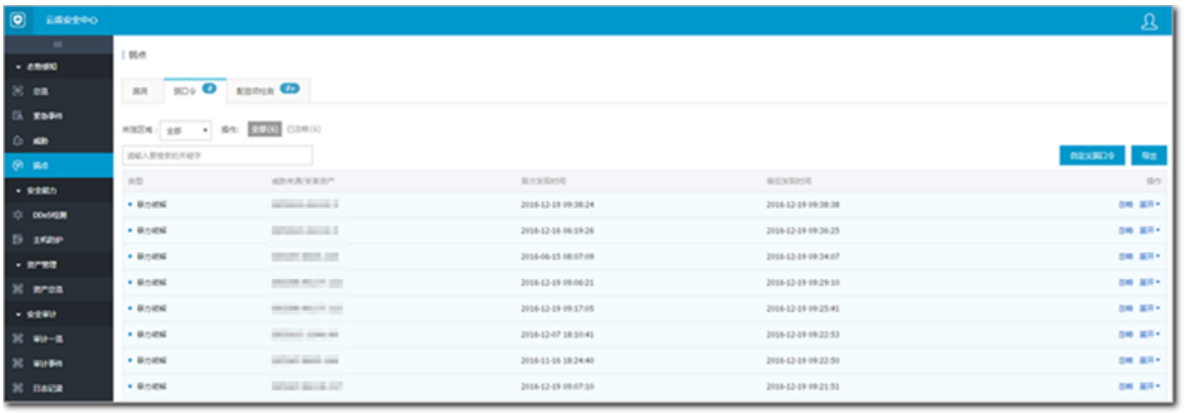
说明: 此处的漏洞信息由安骑士上报，对漏洞的具体操作请前往**服务器安全** > **主机防护** > **补丁管理**页面。

4.3.4.3 查看及添加弱口令

操作步骤

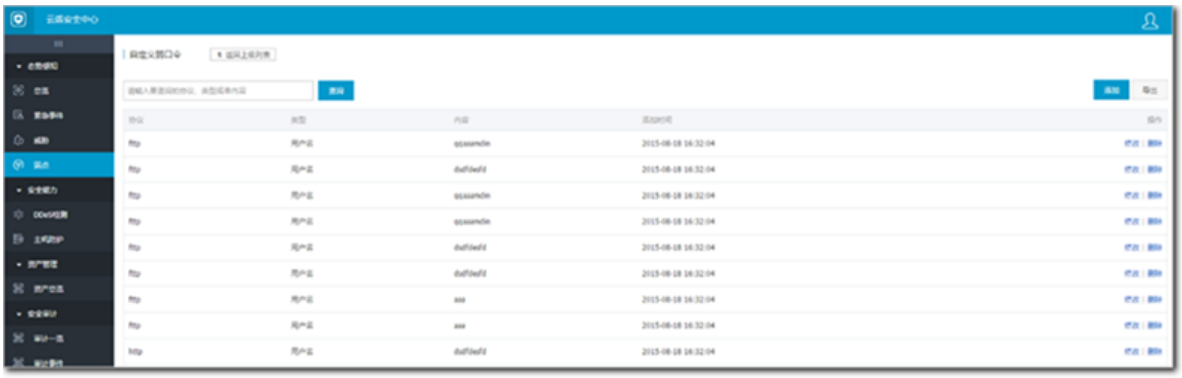
1. 单击**弱口令**，查看已检测到的弱口令信息，如图 *20:* 弱口令页面所示。

图 20: 弱口令页面



2. 单击**自定义弱口令**，可以实现对部分类型的弱口令自定义的功能，如图 *21:* 自定义弱口令页面所示。

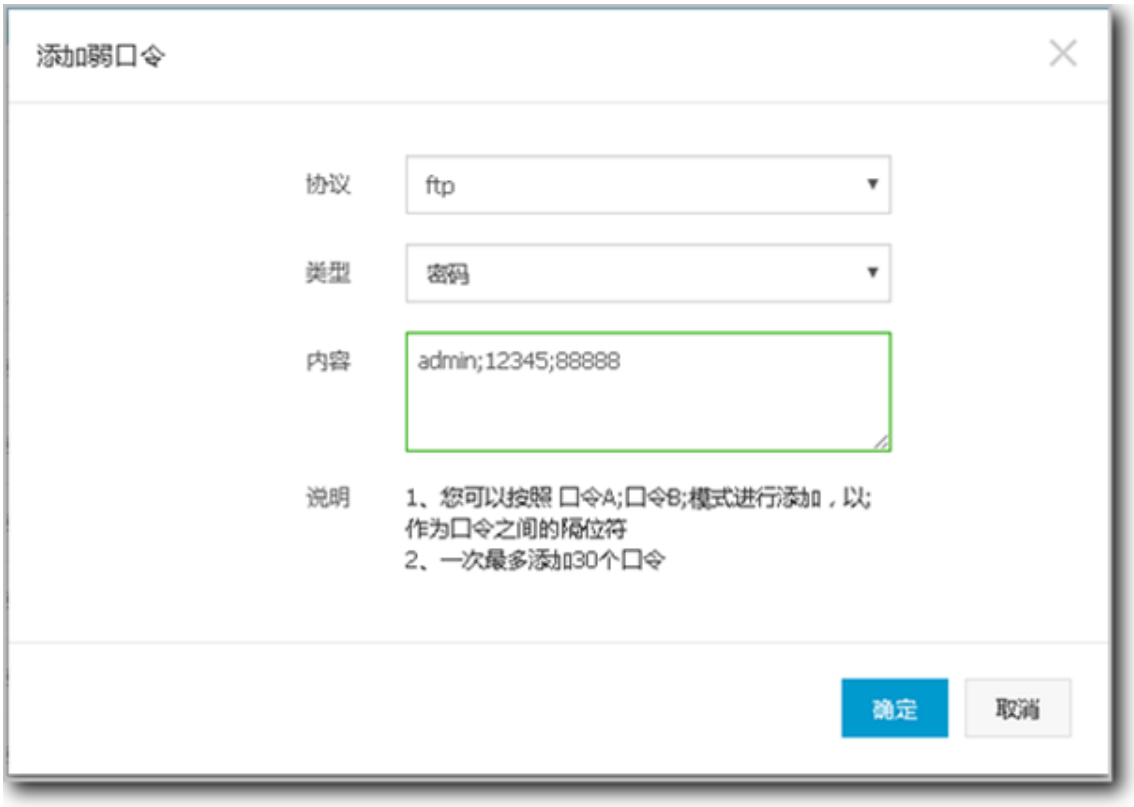
图 21: 自定义弱口令页面



页面显示目前漏洞模块已经配置的弱用户名和弱密码，您可以单击**添加**按钮添加自定义弱口令，添加自定义弱口令并使之生效的步骤如下：

1. 单击**添加**，打开添加弱口令对话框，如图 *22:* 添加弱口令对话框所示。

图 22: 添加弱口令对话框



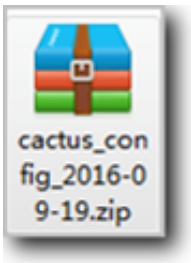
2. 按照提示信息进行弱口令的添加，单击**确定**，如图 *23:* 添加弱口令成功提示信息所示。

图 23: 添加弱口令成功提示信息

3. 添加完成后，单击**导出**，生成并下载新的弱口令配置文件，如图 *24:* 弱口令配置文件所示。

   说明: 文件固定保存路径为*C:\Users*\用户名*Downloads*，下载的文件为zip格式的压缩包，不用解压。

图 24: 弱口令配置文件



4. 将此压缩文件上传至 Cactus-keeper 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*，如如图 *25:* 执行脚本界面所示。

图 25: 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]#
```

5. 脚本执行完成后，新添加的弱口令生效。

4.3.4.4 查看配置项检测结果

单击**配置项检测**，可查看配置项检测结果。

检测结果页面显示漏洞扫描模块扫描到的配置项泄露的地址。

黑客在未授权的情形下访问该地址，将可能获取用户的敏感信息，造成信息泄露。

您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。

4.4 安全能力

4.4.1 DDoS检测

DDoS 攻击（Distributed Denial of Service）即分布式拒绝服务。

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。

一般 DDoS 攻击由攻击者搜集目标，利用漏洞控制的一些傀儡机，在准备发起攻击时，登录并控制所有的傀儡机同时向目标发起 DDOS 攻击。目标主机由于网络带宽大量被占用或者服务的 CPU 内存资源被耗尽而无法提供正常的服务。这样目标主机无法对正常的用户的请求发起响应。

DDoS 的攻击类型有：

- SYN / ACK Flood 攻击：这种攻击方法是经典最有效的 DDoS 方法，可通杀各种系统的网络服务，主要是通过向受害主机发送大量伪造源 IP 和源端口的 SYN 或 ACK 包，导致主机的缓存资源被耗尽或忙于发送回应包而造成拒绝服务；
- TCP 全连接攻击：这种攻击是为了绕过常规防火墙的检查而设计的，一般情况下，常规防火墙大多具备过滤 TearDrop、Land 等 DDoS 攻击的能力，但对于正常的 TCP 连接是放过的，殊不知很多网络服务程序（如：IIS、Apache 等 Web 服务器）能接受的 TCP 连接数是有限的，一旦有大量的 TCP 连接，即便是正常的，也会导致网站访问非常缓慢甚至无法访问，TCP 全连接攻击就是通过许多僵尸主机不断地与受害服务器建立大量的 TCP 连接，直到服务器的内存等资源被耗尽而被拖跨，从而造成拒绝服务；
- Script 脚本攻击：这种攻击主要是针对存在 ASP、JSP、PHP、CGI 等脚本程序，并调用 MSSQLServer、 MySQLServer、Oracle 等数据库的网站系统而设计的，特征是和服务器建立正常的 TCP 连接，并不断地向脚本程序提交查询、列表等大量耗费数据库资源的调用。

  一般来说，提交一个 GET 或 POST 指令对客户端的耗费和带宽的占用是几乎可以忽略的，而服务器为处理此请求却可能要从上万条记录中去查出某个记录，这种处理过程对资源的耗费是很大的，常见的数据库服务器很少能支持数百个查询指令同时执行，而这对于客户端来说却是轻而易举的，因此攻击者只需通过 Proxy 代理向主机服务器大量递交查询指令，只需数分钟就会把服务器资源消耗掉而导致拒绝服务，常见的现象就是网站慢如蜗牛、ASP 程序失效、PHP 连接数据库失败和数据库主程序占用 CPU 偏高。

4.4.1.1 Beaver 流量检测

DDoS 检测功能由专有云云盾的 beaver 流量采集设备提供，Beaver 是一套毫秒（ms）级镜像检测产品，beaver 对流量进行深度包分析，实时检测出各种攻击和异常行为，同时会上报安全事件到专有云云盾控制台，并与其他防护系统产生联动。Beaver 提供丰富的信息输出与基础的数据支持。

- 系统输入：

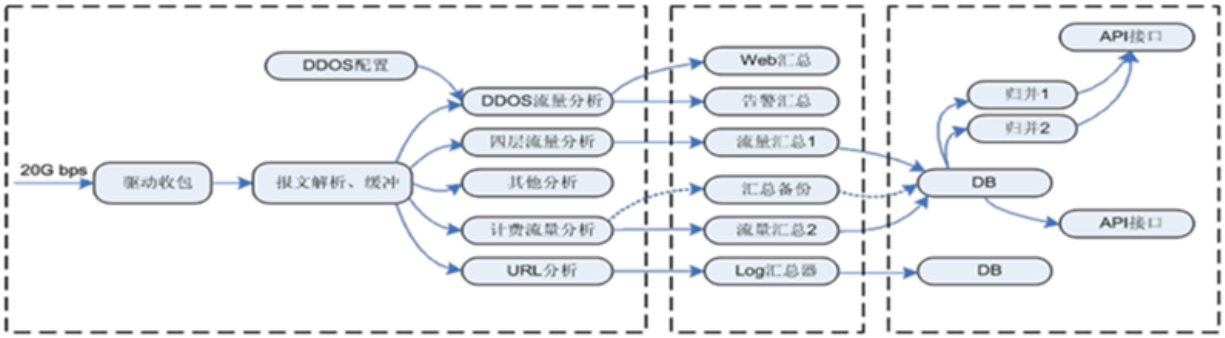
  机房入口镜像流量，有两种方式：

  - 万兆交换机的端口镜像流量
  - 通过分光器、分流器输出的流量

- 系统输出
  - 输出告警信息（目前专有云暂无清洗设备）
  - 输出流量信息到数据库
  - 输出 Http 日志到 spark 平台
  - 检测四层 / 七层攻击，并发送到控制台

DDoS 检测原理如图 *26: DDoS检测原理*所示。

图 26: DDoS检测原理



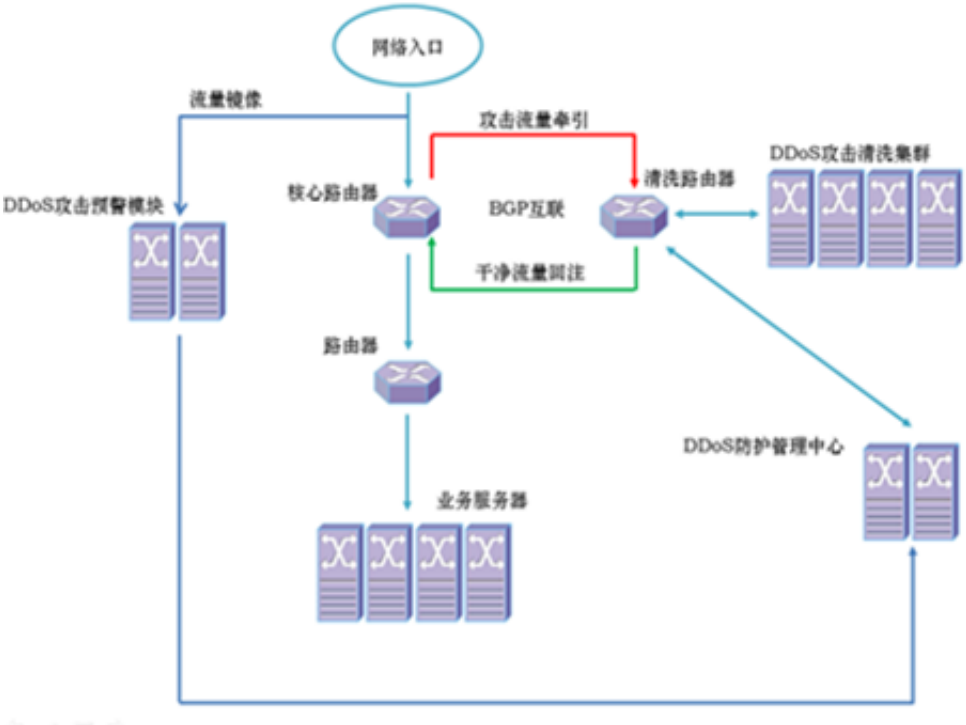
Beaver 的数据数据处理分为收集、汇总、输出三个步骤，分别对应如下三个虚框。虚框之间使用 socket 进行数据交换。虚框中的每个方框代表一个进程（内核态无进程概念），箭头表示数据流向。

- 收集：左边那个虚框表示数据收集。通常这个虚框代表一台高性能 PC（安装双端口万兆网卡），虽然 Beaver 由多台这样的 PC 组成，但位于底层的 PC 处理性能直接决定了整个系统的处理性能。
- 汇总：中间那个虚框表示数据汇总。由于种种原因，一个 IP 的流量可能经过多个收集器，因此必须汇总后才能交给最终用户。
- 输出：右边那个虚框表示数据存储和输出。

4.4.1.2 Guard 流量清洗

通过 beaver 的检测和调度，guard 对流量进行牵引、清洗和回注，如图 *27: Guard 流量清洗过程示意图*所示，提供对 DDoS 攻击的防御，保证业务正常进行。

图 27: Guard 流量清洗过程示意图



受害主机在达到 DDoS 攻击阈值时，由专有云云盾自动进行识别和清洗。

云盾在进行流量清洗时，会上报安全事件到专有云云盾安全中心，在**DDoS防护**页面单击**查询**中可看到这一事件，如图 *28: DDoS防护页面*所示。

图 28: DDoS防护页面

在清洗结束后，云盾同样会上报安全事件到专有云云盾安全中心，此时再次单击**查询**，可查看到状态为**清洗结束**的安全事件。

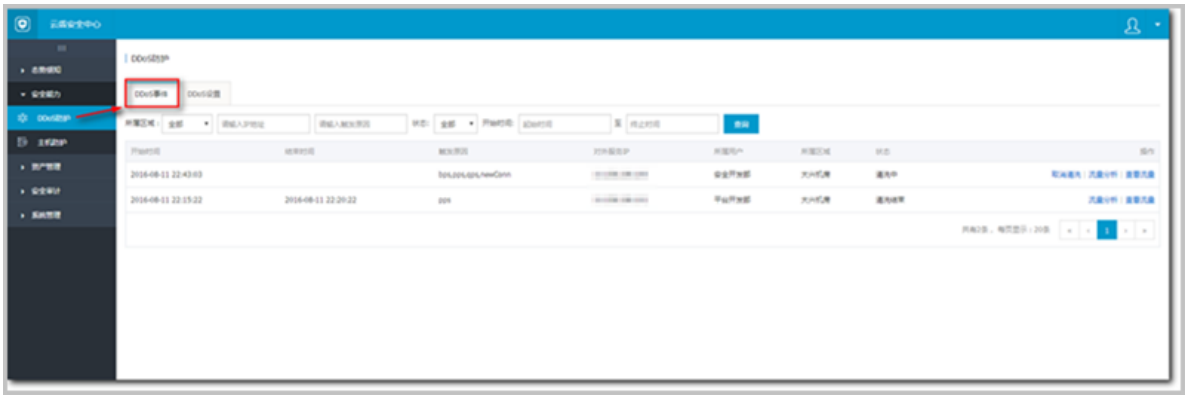
4.4.2 DDoS事件

4.4.2.1 查看DDoS事件列表

操作步骤

1. 选择**云盾安全中心** > **安全能力** > **DDoS检测** > **DDoS事件**，可查看当前所有事件列表，如图 *29: DDoS事件页面*所示。

图 29: DDoS事件页面



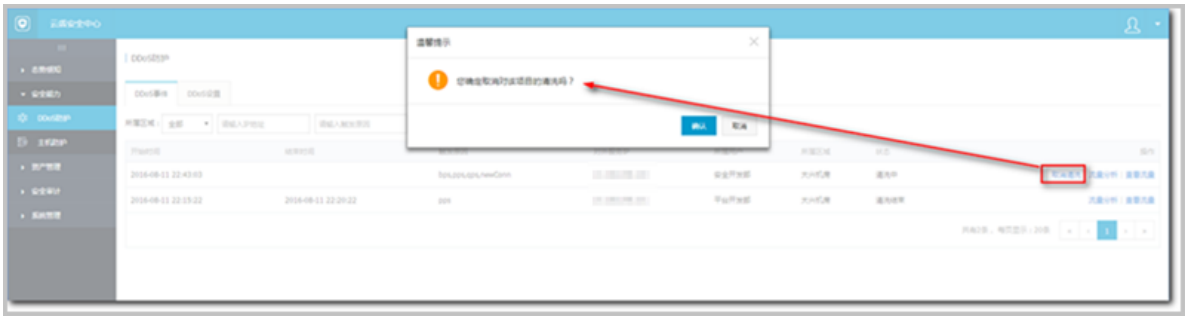
2. 设置查询条件，单击**查询**，可根据查询条件返回满足条件的事件列表，如图 *30: DDoS事件查询条件*所示。

图 30: DDoS事件查询条件

4.4.2.2 查看DDoS事件详细信息

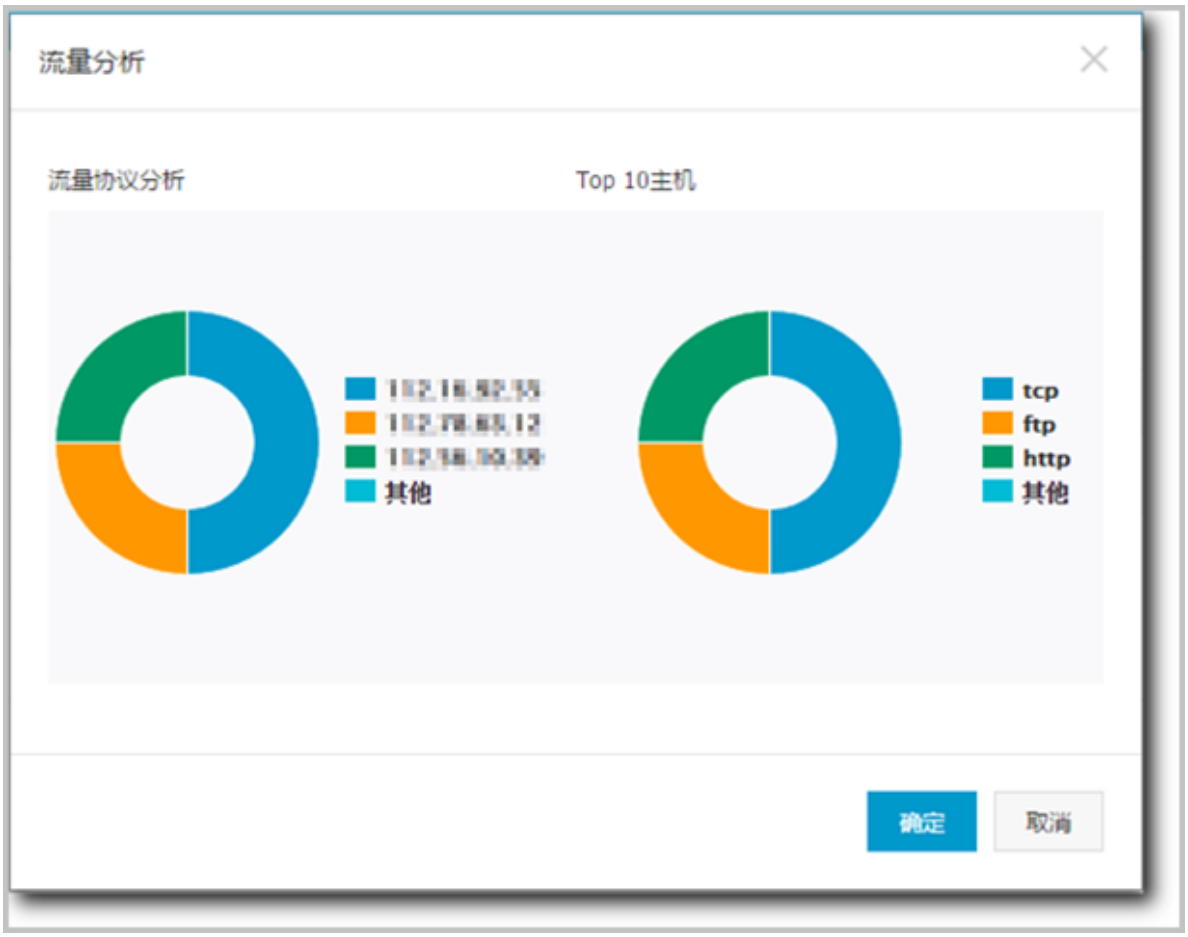
- 选择**云盾安全中心** > **安全能力** > **DDoS防护** > **DDoS事件**页面中处于**清洗中**状态的 DDoS 事件项，单击**取消清洗**，可以取消对该主机流量的清洗，如图 *31: 取消DDoS流量清洗*所示。

图 31: 取消DDoS流量清洗



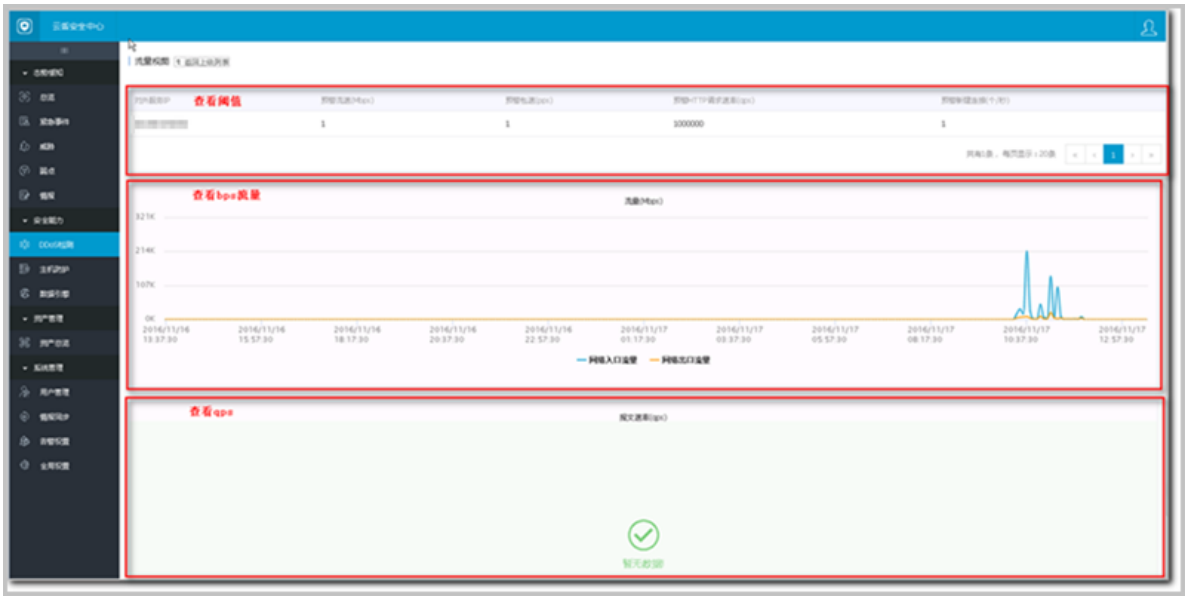
- 选择**云盾安全中心** > **安全能力** > **DDoS防护** > **DDoS事件**页面的某一行表项，单击**流量分析**，可以查看当前攻击事件的流量成分、Top10 攻击机分析，如图 *32: 流量分析页面*所示。

图 32: 流量分析页面



- 选择**云盾安全中心** > **安全能力** > **DDoS防护** > **DDoS事件**页面的某一行表项，单击**查看流量**，可以查看对应主机的当前设置阈值及流量图，如图 *33:* 主机流量图所示。

图 33: 主机流量图



4.4.3 DDoS设置

4.4.3.1 设置DDoS防护策略

报警阈值即当访问该服务器的流量达到阈值后触发流量报警。服务器的阈值设置以服务器的流量作为依据，当流量异常过大时，表示可能受到 DDoS 攻击。阈值的一般设置为比流量的高峰期值稍大即可。

专有云云盾有全局阈值设置和单个主机阈值设置方式。

- 全局阈值：全局阈值无添加操作，默认值在服务初始化时导入。
- 网段阈值：根据网段的流量，设置待设定网段的报警阈值。该方式相对全局阈值能更精准的设置对应网段的报警阈值。
- 单台主机阈值：根据每台主机的流量，分别设置每台主机的报警阈值。该方式相对网段阈值能更精准的设置每台主机的报警阈值。

表 8: DDoS 防护策略参数说明

参数	说明
qps	设置机房主机收到的 HTTP 请求速率报警阈值，当机房入+出包速率达到该值时，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，建议阈值设置为 100000 qps 以上。HTTP 请求速率单位为：qps（请求个数 / 秒）。
pps	设置机房包速率报警阈值，当机房入+出包速率达到该值时，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，建议阈值设置为 20000 pps 以上。 包速率单位为： pps（包个数 / 秒）。
newconn	设置机房主机接收新建连接个数报警阈值，当新建连接数达到该值时，触发 DDoS 检测，一般根据业务实际需求设置，比峰值略大，建议阈值设置为 1000 个以上。 新建连接数单位为：个 / 秒。
bps	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，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，建议阈值设置为 100 Mbps 以上。 带宽单位为：Mbps（兆比特 / 秒）。

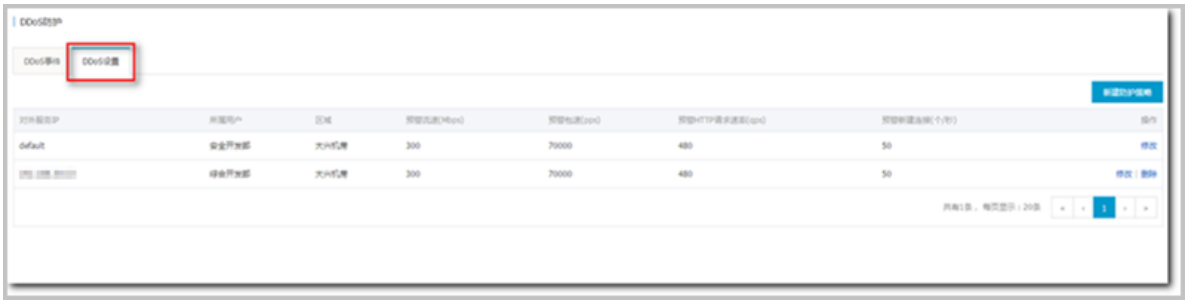
说明: 添加阈值时务必提前确认对应的网段已经在**系统管理** > **全局设置** > **流量网段采集**页面中添加成功。

4.4.3.2 查看阈值列表

操作步骤

选择**云盾安全中心** > **安全能力** > **DDoS检测** > **DDoS设置**，即可查看当前所有阈值列表，如图 *34: 阈值列表*所示。

图 34: 阈值列表



4.4.3.3 设置预警阈值

背景信息

单独对一台主机设置阈值时，以其阈值为准触发 DDoS 检测，否则按照全局阈值触发 DDoS 检测。

操作步骤

1. 在**云盾安全中心** > **安全能力** > **DDoS检测** > **DDoS设置**页面中，单击**新增防护策略**。
2. 在弹出的**新增防护策略**的对话框中，输入对应的网段和阈值，单击**确定**，设置预警阈值，如图 *35: 新增防护策略对话框*所示。

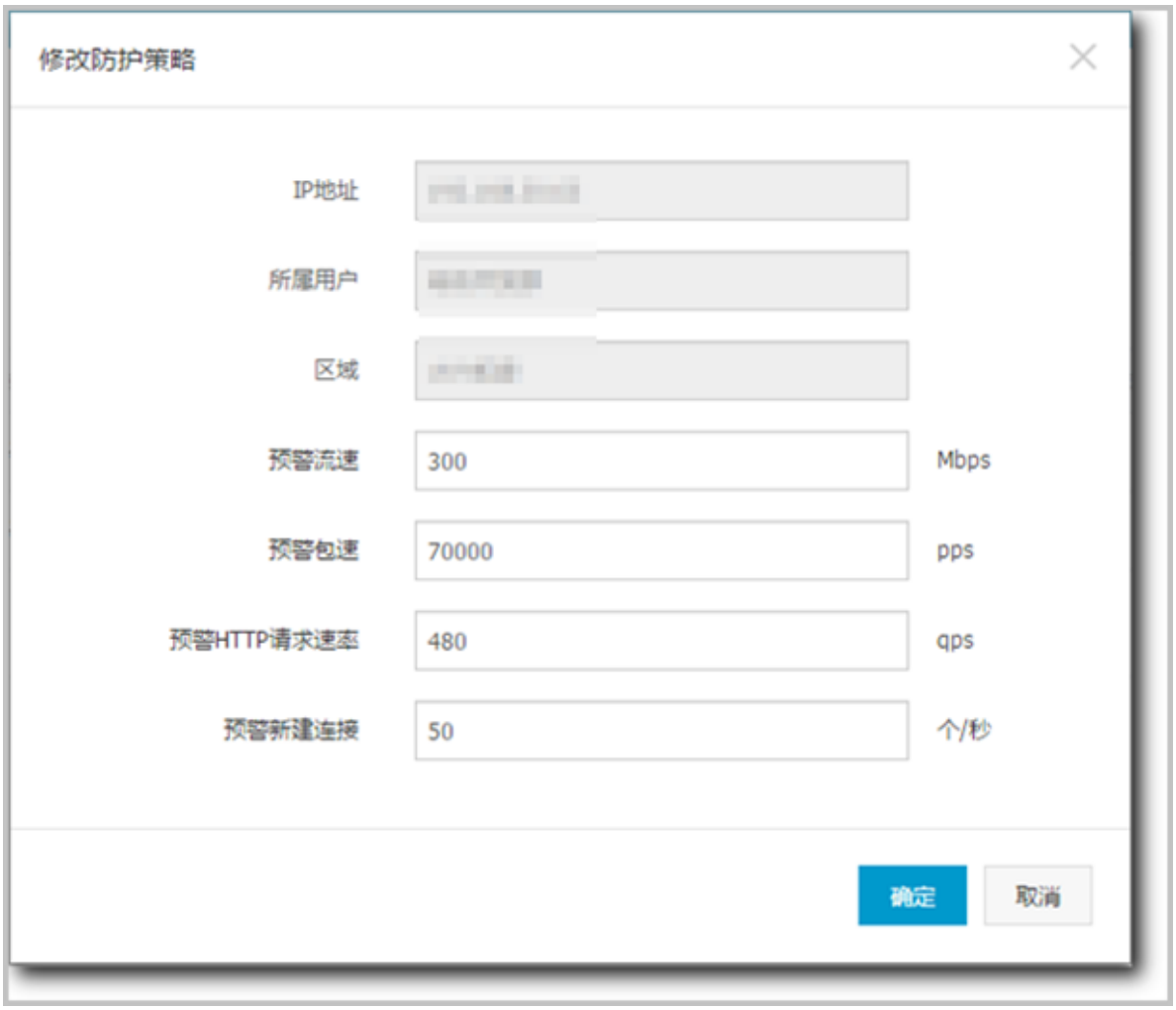
图 35: 新增防护策略对话框

4.4.3.4 修改预警阈值

操作步骤

1. 在**云盾安全中心** > **安全能力** > **DDoS检测** > **DDoS设置**页面的某一行表项，单击**修改**。
2. 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，如图 *36:* 修改防护策略对话框所示。

图 36: 修改防护策略对话框

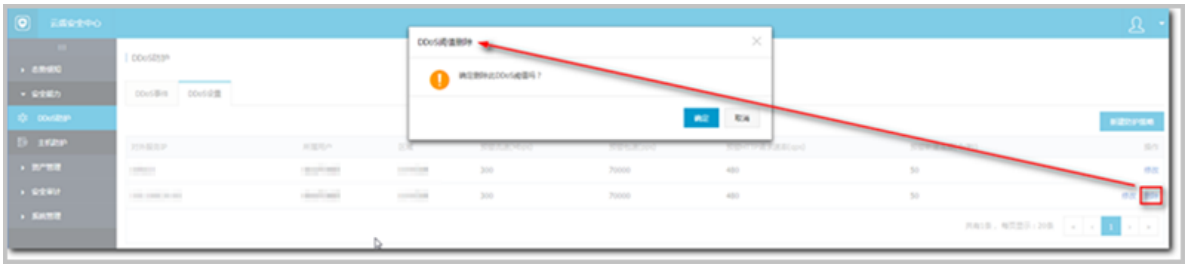


4.4.3.5 删除预警阈值

操作步骤

1. **云盾安全中心** > **安全能力** > **DDoS检测** > **DDoS设置**页面的某一行表项，单击**删除**。
2. 在弹出的**DDoS阈值删除**对话框中，单击**确定**，删除该预警阈值，如图 *37: 删除DDoS阈值*所示。

图 37: 删除DDoS阈值



4.5 服务器安全

4.5.1 简介

专有云云盾能够防护每一台用户主机的安全，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。

主机防护具有以下功能：

- 防护基线：云盾能够实时展示安骑士的防护状态和基线检查状态，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：云盾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。支持RDP/SSH的异地登录告警。
  - 暴力破解防护：安骑士插件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。支持RDP/SSH等应用的密码破解攻击防护。
- 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。
- 补丁管理：及时获取最新漏洞预警和补丁，并能通过云端一键下发补丁更新。

主机入侵检测功能列出所有服务器上发现的文件篡改、异常进程、异常网络连接、可疑端口监听等行为，帮助您及时发现服务器安全隐患。

4.5.1.1 安骑士客户端原理

安骑士客户端程序包含 Webshell 特征库、Webshell 隔离模块、补丁特征库和补丁修复模块，功能分别如下：

- Webshell 特征库的功能是用来检测文件是否符合特征库的特征，如果符合，会发送木马文件到安骑士服务器，由安骑士服务器结合更多的特征库进一步分析是否为木马文件；
- Webshell 隔离模块的功能是安骑士客户端通过向安骑士服务器确认为木马文件之后，对该文件进行隔离；
- 补丁特征库的功能是用来检测文件是否符合特征库的特征，如果符合，会发送漏洞文件到安骑士服务器，由安骑士服务器结合更多的特征库进一步分析是否为漏洞文件；

- 补丁修复模块的功能是是安骑士客户端通过向安骑士服务器确认为漏洞文件之后，对该文件进行修复。

安骑士客户端提供了 Windows 版本和 Linux 版本，可以根据主机操作系统选择相应版本，安装后安骑士客户端可以自动连接到安骑士服务器端进行在线升级。

4.5.1.2 安骑士服务器端原理

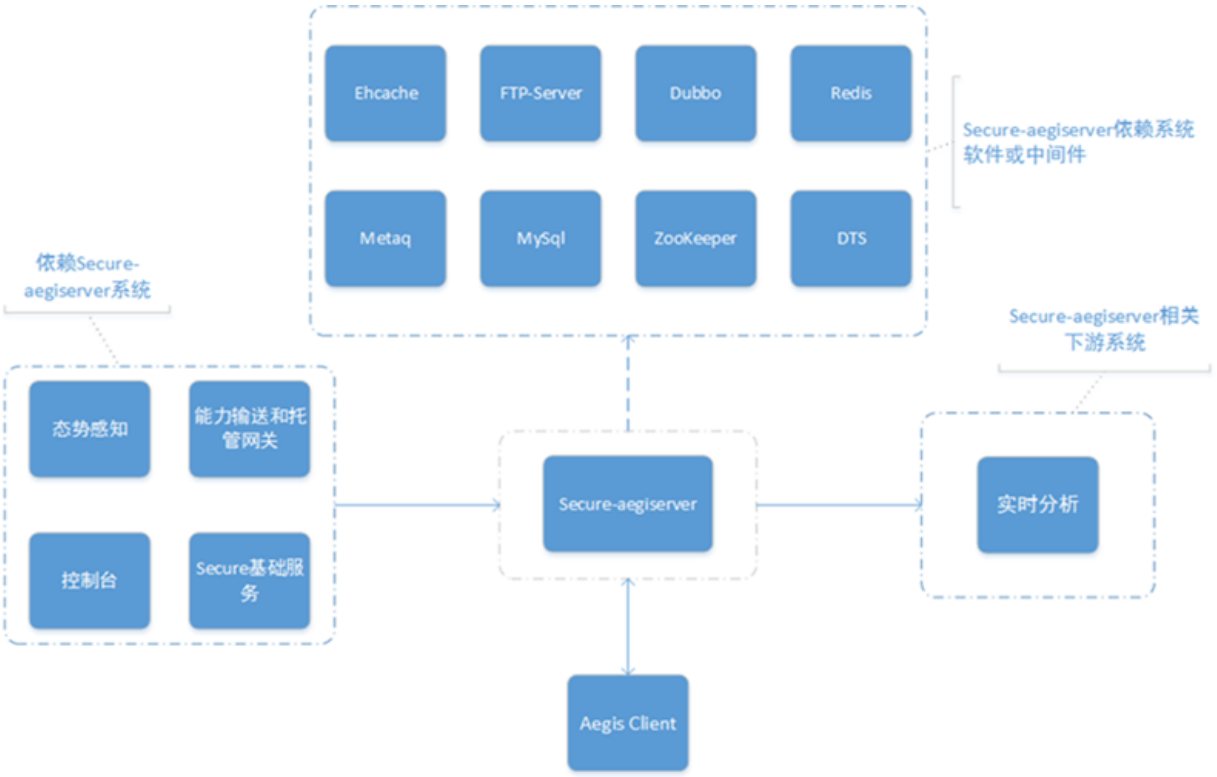
安骑士服务器端包括 aegis-server、defender 和 aegis-health-check 三个模块。其功能分别如下：

- aegis-server 包括通讯模块和客户端检查模块，主要功能是向下和 aegis-client 交互，收集木马文件，补丁文件等信息，向上和 defender 反馈异地登录信息、爆破信息和爆破成功等信息；
- defender 的主要功能是异地登录分析、暴力破解分析和暴力破解是否成功的分析；
- aegis-health-check 的主要功能是进行基线检查，通过 aegis-server向客户端下发基线检查的命令，并且通过aegis-server 接收客户端返回的数据，修改基线检查的状态。

安骑士服务器端提供了 API 供专有云云盾控制台来获取信息，解析安全事件并分析后呈现给管理员，管理员可以下发命令对木马文隔离或者忽略，可以下发命令对补丁文件进行修复或者忽略。

安骑士整体架构如图 *38:* 安骑士整体架构所示。

图 38: 安骑士整体架构



- 使用通用软件进行建站

  极易因为通用软件的漏洞而被黑客入侵，使用服务器安全（安骑士）进行漏洞监测，一旦爆发漏洞可快速进行一键修复。

- 有 Web 服务

  不管是内部 Web 服务还是外部 Web 服务，黑客均可以通过 Web 服务窃取网站的核心数据，开启 Web 攻击拦截可有效阻止黑客从外部的攻击和内部的渗透。

4.5.2 主机防护

4.5.2.1 防护基线

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

4.5.2.1.1 原理简介

Aegis-client 和 aegis-server 端通过 TCP 长连接通道进行消息传递，这个通道是 aegis 产品中最核心的部分，稳定性高达 99.99 %，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 aegis-client 成功与 aegis-server 建立通信并登录后，该主机的 aegis 防护状态便被置为在线，此后，sever 会定时向 client 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，记录下最后在线时间。

aegis-health-check 工程通过 aegiserver 向 Linux 或者 Windows 主机下发安全体检的命令，aegiserver 收到客户端返回的体检结果，通过 metaq 发消息给 aegis-health-check，更新体检结果。支持对体检结果进行修复，验证，忽略等功能，以此提高主机的安全性，还可以查看最近十次的体检记录 ，历史体检记录不支持验证，忽略和修复，支持回滚功能。支持查看已忽略体检记录，并且可以取消忽略。

4.5.2.1.2 查看主机防护状态

背景信息

Aegis 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，并支持刷新列表，默认展示全部区域，按照 IP 排序。

操作步骤

在**服务器安全** > **主机防护** > **防护基线**页面，设置查询条件，单击**查询**，查看主机防护状态。

4.5.2.1.3 立即执行主机安全检查

操作步骤

1. 如果主机从未进行过安全巡检，可选择该主机，单击**查看详情**。
2. 单击**立即检查**。
3. 在**选择巡检内容**对话框中，选择需要检测的具体项目。
4. 单击**确定**，下发安全巡检命令。

4.5.2.1.4 重新执行主机安全检查

操作步骤

1. 如需对主机重新进行安全巡检，选择该主机，单击**查看详情**。
2. 单击**重新检查**。
3. 在**选择巡检内容**对话框中，选择需要检测的具体项目。
4. 单击**确定**，重新下发安全巡检命令。

4.5.2.1.5 查看主机安全体检记录

操作步骤

1. 检查完成后，选择该主机，单击**查看详情**。
2. 单击**查看体检记录**，可查看近 10 次的体检记录。

说明: 历史体检结果不支持验证、忽略和修复，支持回滚功能。

4.5.2.1.6 查看已忽略检查项目

操作步骤

1. 检查完成后，选择该主机，单击**查看详情**。
2. 单击**已忽略项目**，可查看已被手动忽略项目，取消忽略后可进行风险检测。

4.5.2.1.7 处理风险项

操作步骤

1. 检查完成后，选择该主机，单击**查看详情**。
2. 选择待处理的风险项，可对风险项进行**修复**、**验证**、**忽略**等操作。

4.5.2.1.8 离线原因排查

排查步骤如下：

- 检查网络是否连接。
- 检查您是否设置了防火墙 ACL 规则。需要将服务器安全（安骑士）的服务端 IP 加入防火墙白名单以允许网络访问（80端口）。
- 查看是否有第三方的防病毒产品，如果有，尝试关掉之后重新安装 Agent，部分第三方的防病毒软件可能会禁止 Agent 访问网络。

4.5.2.2 登录安全

登录安全主要分为异地登录和暴力破解两部分，管理员可以在专有云云盾上看到异地登录和暴力破解的告警信息，并可以查询登录记录和暴力破解的来源等详细信息，针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便可不再告警。

4.5.2.2.1 登录记录

您可以在配置中心设置服务器的常用登录地，如果没有在常用登录地登录，会在专有云云盾控制台提醒异地登录，在告警设置中可以为异地登录配置手机通知和邮箱通知。常用登录地的设置请参见配置白名单，告警设置请参见告警设置。

流程分析

1. Aegis-client 通过 tcp 协议上报登录信息到 aegis-server。
2. Aegis-server 通过 metaq 消息将上报信息发送到 defender。
3. Defender 分析登录信息，判断是否异地登录，并写入 aegis-db。如果为异地登录，会将消息通过 metaq 发送给 sas 进行进一步处理，判断是否通过手机、邮件提醒用户。

4.5.2.2.2 查询登录记录

背景信息

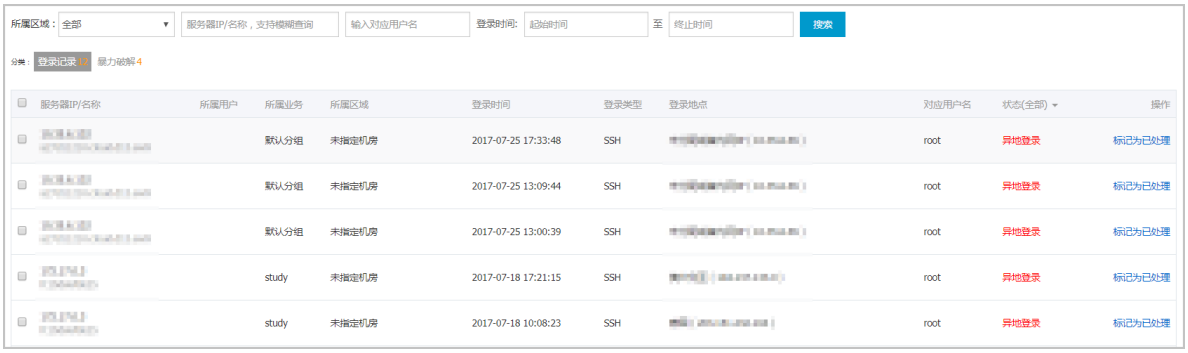
登录记录状态主要有异地登录、正常登录和已处理，支持主机 IP、主机名的模糊查询、登录用户及登录时间的筛选。

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. 在**服务器安全** > **主机防护** > **登录安全**页面，选择**登录记录**，如图 *39:* 登录记录页面所示。

图 39: 登录记录页面



2. 设置查询条件。
3. 单击**搜索**，显示符合条件的登录记录。
4. 确认登录正常后，您可以单击**标记为已处理**。
5. 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醒该记录。

4.5.2.2.3 暴力破解

您可以在配置中心设置白名单，如果暴力破解成功且源 IP 不在白名单内，会在专有云云盾控制台提醒暴力破解成功，在告警设置中可以为暴力破解配置手机通知和邮箱通知。白名单的设置请参见配置中心，告警设置请参见告警设置。

流程分析

1. Aegis-client 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 协议上报暴破消息到 aegis-server。
2. Aegis-server 通过 metaq 消息将上报信息发送到 defender。
3. Defender 分析暴破信息，判断暴破类型，以及是否暴力破解成功，并将暴破信息写入 aegis-db。如果破解成功，会将消息通过 metaq 发送给 sas 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暴破成功、有威胁、无威胁和已处理，时间类型说明请参见表 *9:* 暴力破解事件类型表。

表 9: 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

4.5.2.2.4 查询暴力破解事件

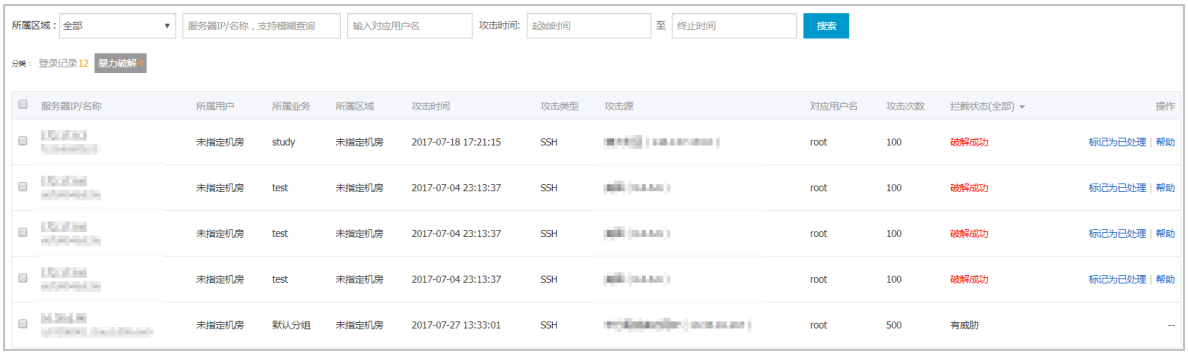
背景信息

通过查询暴力破解事件，您可以了解暴力破解的攻击源、攻击次数以及拦截状态。当控制台产生暴力破解成功意味着您的主机已经被黑客暴力破解出密码并且成功登陆了主机，管理员需要及时进行排查处理。暴力破解事件查询支持主机 IP 及主机名的模糊查询和登录用户及时间的筛选。

操作步骤

1. 在**服务器安全 > 主机防护 > 登录安全**页面，选择**暴力破解**，设置查询条件，单击**搜索**，查看暴力破解事件，如图 *40:* 暴力破解事件页面所示。

图 40: 暴力破解事件页面



2. 调查暴力破解的原因，排除风险后，您可以单击**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**。

4.5.2.3 木马查杀

黑客入侵网站后，通常会将木马文件放入主机的 Web 服务目录下，和正常文件混在一起，然后用浏览器来访问恶意文件，达到控制网站服务器的目的。而木马查杀则能及时检测木马文件并向管理远告警，管理员可以在专有云云盾控制台查看云盾发现的木马文件，并可以对木马进行隔离、忽略、

恢复、移除信任文件一系列操作。在设置了手机或邮件提醒的情况下，同一木马只会在首次发现时推送提醒，设置提醒请参见告警设置。

功能特色

自研网站后门查杀引擎，拥有本地查杀加云查杀体系，同时共享全网最大服务器端的恶意后门文件样本库，支持所有常见后门文件类型，查杀率全球领先。

4.5.2.3.1 操作说明

注意：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。

表 10: 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

4.5.2.3.2 状态说明

表 11: 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。
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。

4.5.2.3.3 查询木马文件信息

背景信息

木马查杀状态主要有待处理、已隔离和信任文件，支持服务器名称和 IP 模糊查询，以及时间段的筛选，可以按紧急程度排序，也可以按照组合服务器查看。

通过查询木马文件事件，您可以了解安骑士发现的木马文件信息。

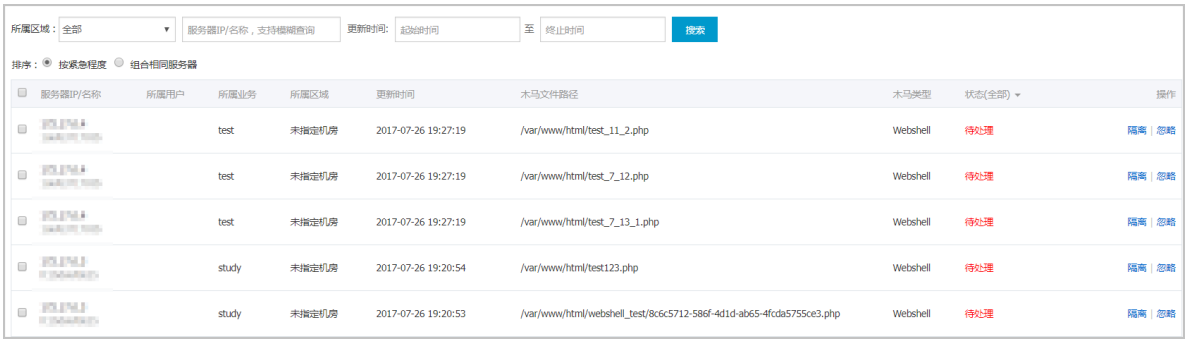
操作步骤

1. 在**服务器安全 > 主机防护 > 木马查杀**页面，设置查询条件，单击**查询**。

   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 *41:* 按紧急程度排序展示所示。

   图 41: 按紧急程度排序展示

   组合相同服务器排序

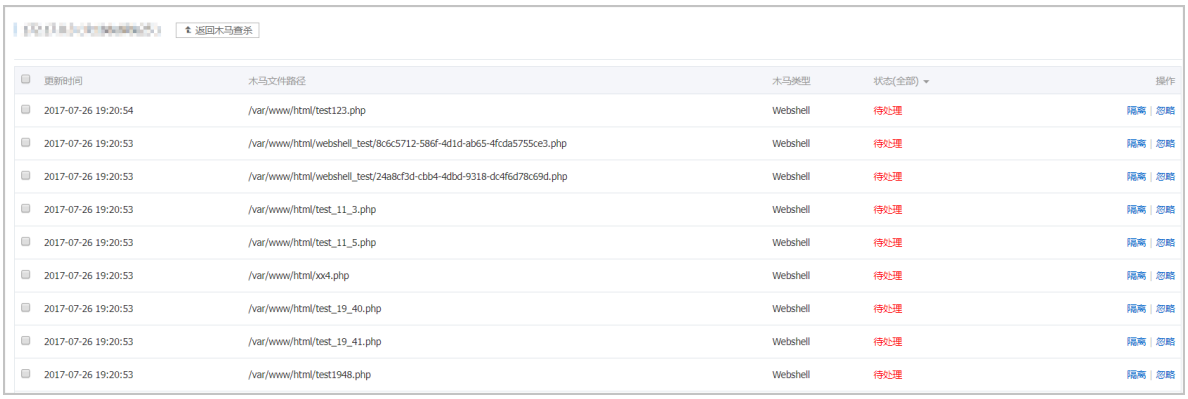
   按待处理个数降序排列，如图 *42:* 组合相同服务器排序展示所示。

   图 42: 组合相同服务器排序展示

2. 单击组合服务器排序下的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，展示按紧急程度排序后，按发现时间降序，如图 *43:* 查看服务器详情所示。

   图 43: 查看服务器详情



3. 单击**返回木马查杀**，可以回到木马查杀页面重新进行查询。

4.5.2.3.4 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，由管理员来决定是否隔离恶意文件。

对准备删除的木马文件可以执行隔离操作。对误认为是木马文件，已进行隔离的，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，该木马文件仍然保留。对信任文件可执行移除信任文件，该记录将会从列表中删除。

- 隔离木马文件。

  在**服务器安全 > 主机防护 > 木马查杀**页面的某个待处理事件一行，单击**隔离**，可将该木马文件隔离，如图 *44:* 隔离木马文件所示。

  图 44: 隔离木马文件

- 恢复已隔离的木马文件。

  在**服务器安全 > 主机防护 > 木马查杀**页面的某个已隔离事件一行，单击**恢复**，可将该隔离文件恢复，如图 *45:* 恢复已隔离文件所示。

  图 45: 恢复已隔离文件

- 忽略木马文件。

在**服务器安全** > **主机防护** > **木马查杀**页面的某个待处理事件一行，单击**忽略**，可忽略该木马文件，如图 *46:* 忽略木马文件所示。

图 46: 忽略木马文件

- 移除信任文件。

  在**服务器安全** > **主机防护** > **木马查杀**页面的某个信任文件事件一行，单击**忽略**，可将该信任文件移除，如图 *47:* 移除信任文件所示。

  图 47: 移除信任文件

4.5.2.4 配置中心

4.5.2.4.1 简介

配置中心支持以下配置内容：

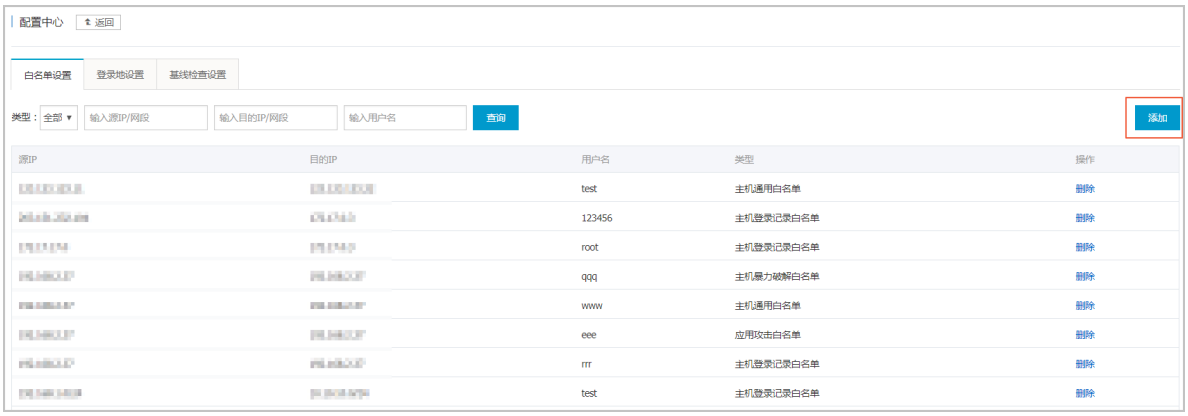
- 白名单设置：登录 IP 白名单主要用于过滤暴力破解和暴力破解成功。如果源 IP 和目的 IP 在登录 IP 白名单中，暴力破解失败。
- 登录地设置：常用登录地主要用于异地登录的判断。如果不设置常用登录地，不管在哪里登录，都不是异地登录。如果设置了常用登录地，在非常用登录地登录的第一次和第五次会提醒此次登录为异地登录，其余都是正常登陆。如果在一个登录地登录次数大于等于六，这个登录地会被加入到常用登录地，并在页面上展示出来。
- 基线检查设置：支持设置周期性自动安全体检策略。

4.5.2.4.2 配置白名单

操作步骤

1. 在**服务器安全** > **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 *48:* 白名单设置页面所示。

   图 48: 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，单击**确认**，添加白名单 IP，如图 *49: 添加白名单对话框*所示。

图 49: 添加白名单对话框

4.5.2.4.3 配置登录地

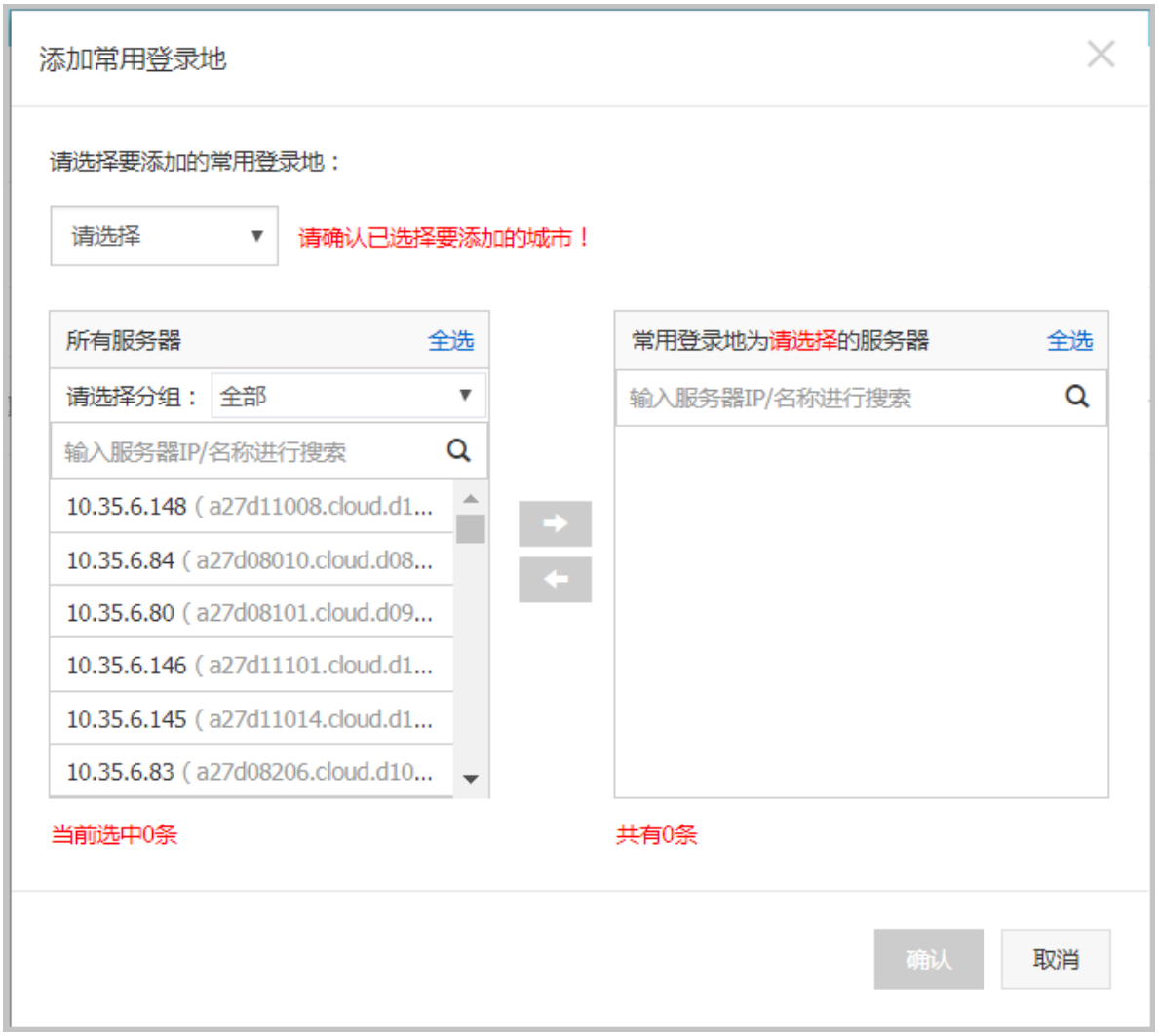
操作步骤

1. 在**服务器安全 > 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 *50:* 登录地设置页面所示。

图 50: 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 *51:* 添加白名单对话框所示。

图 51: 添加白名单对话框



4.5.2.4.4 配置基线检查策略

操作步骤

1. 在**服务器安全** > **主机防护**，单击**配置中心**，单击**基线检查设置**，进入**基线检查设置**页面，如图 *52:* 基线检查设置页面所示。

   图 52: 基线检查设置页面

2. 单击**添加**。
3. 在**安全体检策略**对话框中，设置需要的周期性安全体检策略，单击**确认**，添加安全体检策略，如图 *53:* 安全体检策略对话框所示。

   图 53: 安全体检策略对话框

4.5.3 主机入侵检测

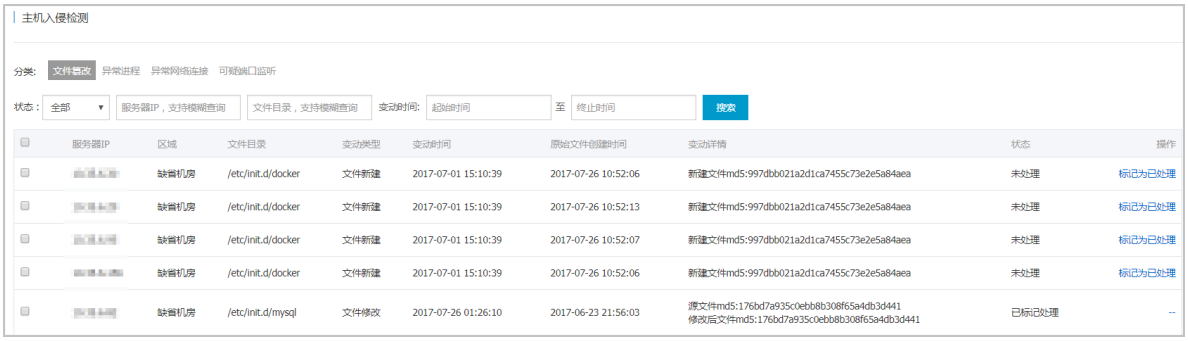
4.5.3.1 查看文件篡改事件记录

操作步骤

1. 在**服务器安全 > 主机入侵检测**页面，单击**文件篡改**。

2. 查看文件篡改事件记录，如图 *54:* 文件篡改事件记录所示。

图 54: 文件篡改事件记录

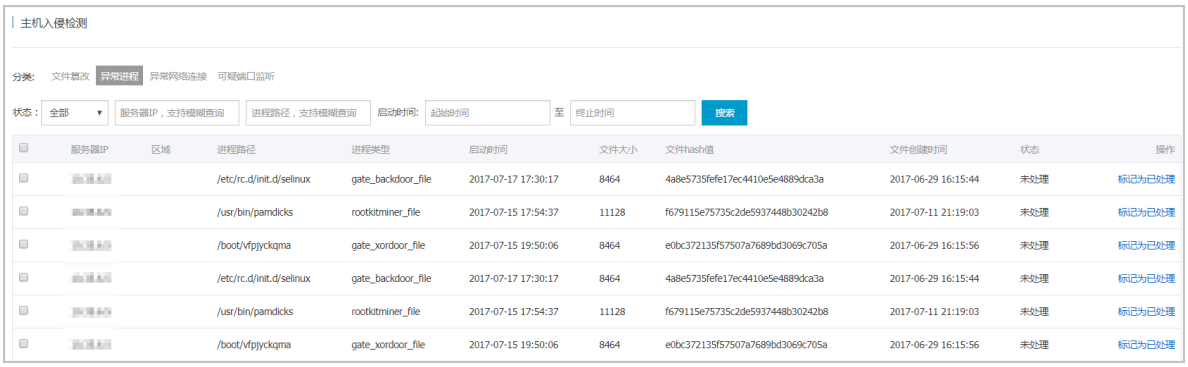


4.5.3.2 查看异常进程记录

操作步骤

1. 在**服务器安全 > 主机入侵检测**页面，单击**异常进程**。
2. 查看异常进程记录，如图 *55:* 异常进程记录所示。

图 55: 异常进程记录

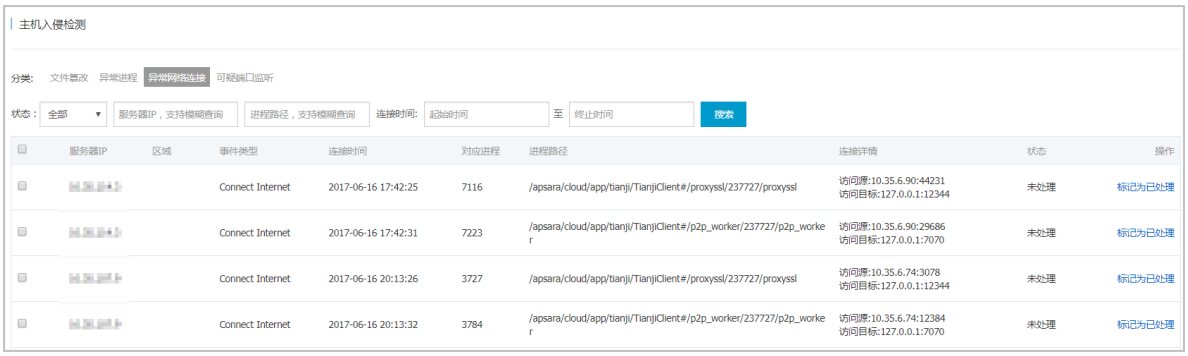


4.5.3.3 查看异常网络连接记录

操作步骤

1. 在**服务器安全 > 主机入侵检测**页面，单击**异常网络连接**。
2. 查看异常网络连接记录，如图 *56:* 异常网络连接所示。

图 56: 异常网络连接

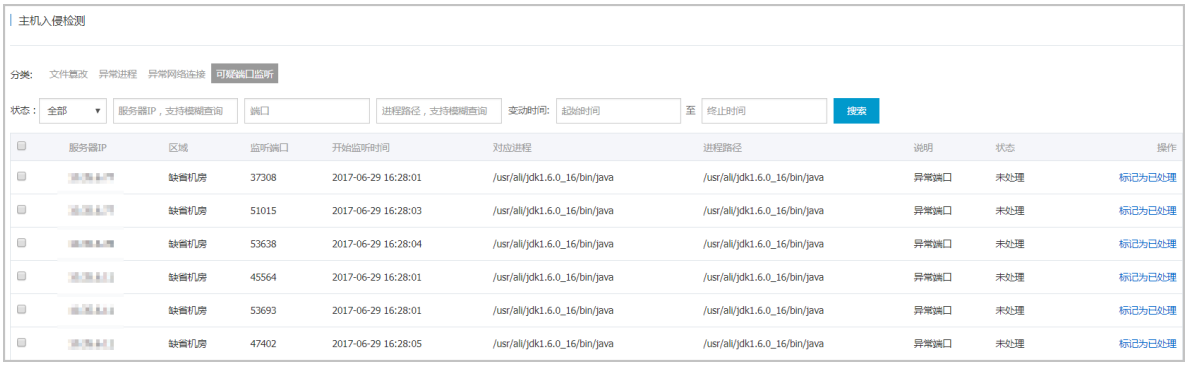


4.5.3.4 查看异常端口监听记录

操作步骤

1. 在**服务器安全 > 主机入侵检测**页面，单击**可疑端口监听**。
2. 查看异常端口监听记录，如图 *57: 异常端口监听记录*所示。

图 57: 异常端口监听记录



4.6 资产总览

专有云云盾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、类型供管理员查询浏览资产的相关信息，帮助管理员从整体了解资产情况，以更好地管理资产。

4.6.1 简介

您可以在**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，帮助您更好地管理资产，如图 *58: 资产总览页面*所示。

图 58: 资产总览页面

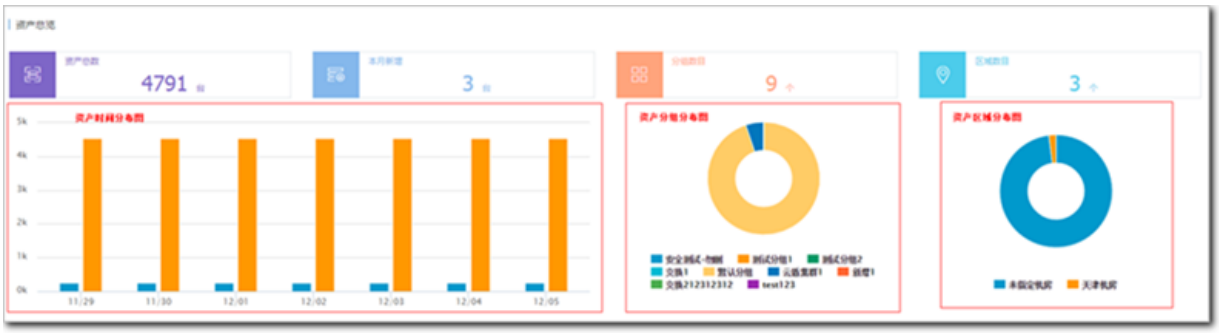


表 12: 资产总览页面参数说明表

参数	说明
分组数目	当前已有的分组数目。
区域数目	当前配置的区域数目。
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。
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。
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。
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 资产统计。

4.6.2 分组管理

分组管理主要用于对分组进行增加、删除、重新排序。将资产分组，可以方便区分不同资产的特定作用。查询资产信息和对资产信息进行修改。

分组最多只能有 10 个，默认分组不可被删除且不可更改名称，分组中存在资产时不可被删除。

4.6.3 添加分组

操作步骤

1. 在**资产管理** > **资产总览**页面，单击**分组管理**按钮，弹出**业务分组**对话框，如图 *59:* 业务分组对话框所示。

   图 59: 业务分组对话框

2. 单击**添加分组**按钮。
3. 填写分组名称。
4. 单击**确认**，添加资产分组。

4.6.4 删除分组

操作步骤

1. 在**业务分组**对话框内，单击对应分组条目后的**删除**，如图 *60:* 删除业务分组所示。

图 60: 删除业务分组

2. 单击**确认**，删除该资产分组。

4.6.5 调整分组排序

操作步骤

1. 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。
2. 单击**确认**，完成资产分组的排序调整。

4.6.6 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略有差异，您可以切换查看不同类型的资产信息。

表 13: 资产类型表

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

4.6.7 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，您可以掌握各资产的大致情况，比如操作系统、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。

主机资产的查询支持按照操作系统、区域筛选、分组筛选，支持主机 IP 及主机名的模糊查询，默认展示全部区域，按照 IP 排序。

- 在**资产管理** > **资产总览**页面，选择**主机资产**，设置查询条件，单击**查询**，查看主机资产信息，如图 *61:* 主机资产页面所示。

图 61: 主机资产页面

- 在**主机资产**页面，单击**详情**，可以查看主机端口开放情况，如图 *62:* 主机端口详情所示。

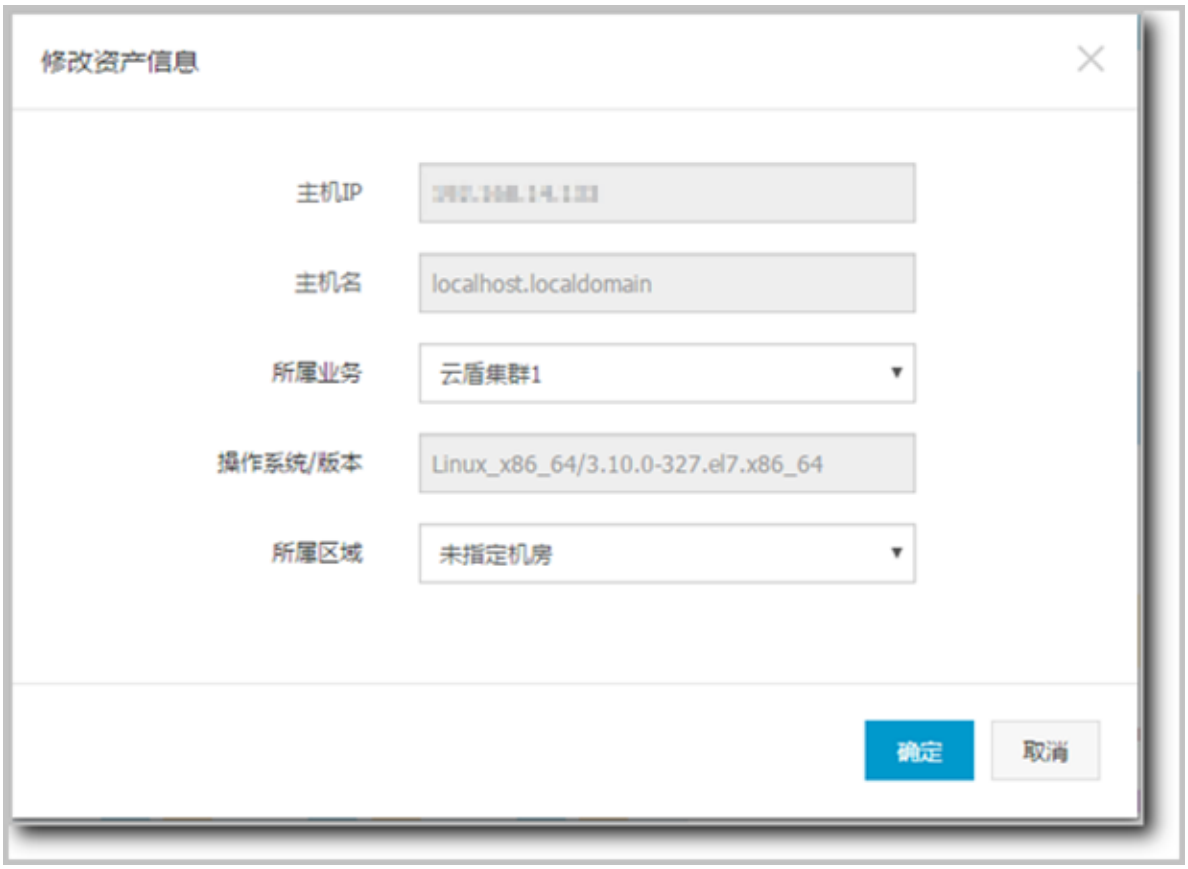
图 62: 主机端口详情

- 在**主机资产**页面，单击**展开应用信息**，可以查看主机已有的可监测应用信息，如图 *63:* 主机监测信息所示。

图 63: 主机监测信息

- 在**主机资产**页面，单击**修改**，弹出**修改资产信息**对话框，如图 *64:* 修改资产信息对话框所示。

图 64: 修改资产信息对话框



修改信息，单击**确定**，完成主机资产修改。

- 在**主机资产**页面，单击**删除**，弹出删除对话框，单击**确定**进行删除。

  如果主机中卸载了安骑士，或者在专有云中删除了一台 ECS 主机，则这些主机对应的资产需要手动删除。

4.6.8 管理NAT资产

背景信息

NAT 资产，可以理解为 IP 资产，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，不同端口会被指向不同主机。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。

通过查询 NAT 资产，您可以了解当前专有云云盾为您守护的 NAT 资产的基本信息，也可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。

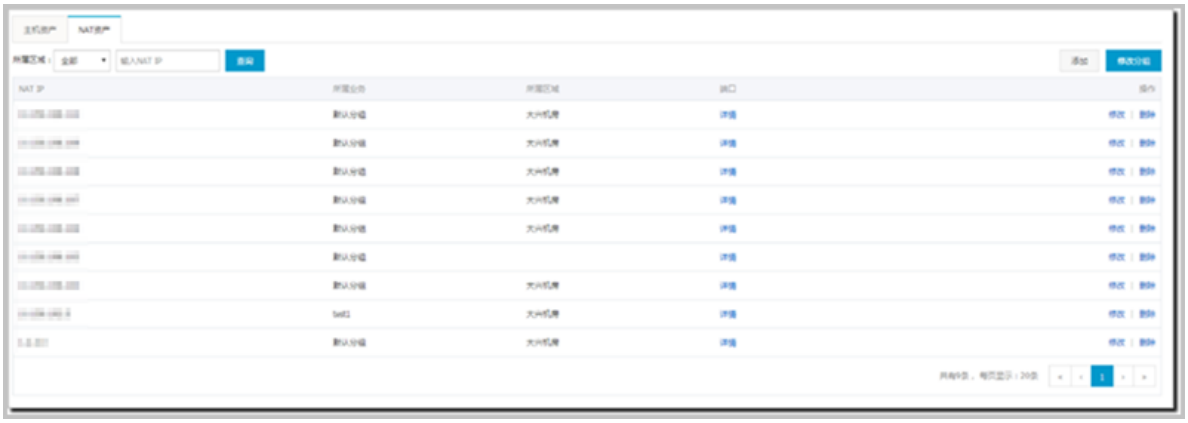
NAT 资产的查询支持按区域、分组筛选，支持 IP 的模糊查询，默认展示全部区域，按照 IP 排序。

操作步骤

1. 在**资产管理** > **资产总览**页面，选择**NAT 资产**.

2. 设置查询条件，单击**查询**，查看 NAT 资产信息，如图 *65: NAT 资产页面*所示。

图 65: NAT 资产页面



3. 在**NAT 资产页面**，单击列表右上方**添加**按钮，弹出添加资产对话框。输入 IP 地址或者 IP 表达式，选择所属业务和所属区域，单击**确定**，完成添加。

   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。

4. 选择需要的 NAT 资产，进行如下操作：

   - 查看详情

     在**NAT 资产页面**，单击**详情**，可以查看端口开放情况。

   - 修改 NAT 资产

     在**NAT 资产页面**，单击**修改**，弹出修改对话框。修改信息，单击**确定**，完成修改，如图 *66: 修改资产信息对话框*所示。

     图 66: 修改资产信息对话框

- 删除 NAT 资产

  在**NAT 资产页面**，单击**删除**，弹出删除对话框，单击**确定**进行删除。

4.6.9 批量修改资产分组

背景信息

可以通过两种方式来修改资产的分组信息，单个修改和批量修改。单个修改适用于要修改信息的主机数量只有一台，或者有数台要修改的主机，但它们既不在同一个网段，主机名也没有任何规律，不同类型资产的修改方法已在前文中详细说明。批量修改适用于对多台主机进行修改并且这些主机属于同一个网段。

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。

暂时不支持对资产的批量删除操作。

操作步骤

1. 在**资产管理** > **资产总览**页面，单击**修改分组**，弹出**修改分组**对话框，如图 *67: 修改分组对话框*所示。

   图 67: 修改分组对话框

2. 您可以选择按网段或者主机名进行修改。
3. 单击**确定**，完成修改。

4.7 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。阿里云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，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。

阿里云的安全审计主要由阿里的 auditlog 核心组件完成。专有云云盾高级版调用 auditlog 的 api 接口获取审计日志数据、审计策略和审计事件，对审计日志和审计事件做分析和以图表方式呈现，有利于管理员直观了解系统面临的风险和威胁。

4.7.1 审计一览

审计一览提供云平台日志趋势、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管理员，便于分析云服务面临的风险趋势。

- 云平台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。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。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。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。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。

在**安全审计** > **审计一览**页面，设置查询时间，单击**查询**，查看审计报表，如图 *68:* 审计一览页面所示。

说明: 缺省情况下查看一周的审计报表。

图 68: 审计一览页面

4.7.2 审计查询

审计查询会记录日志创建时间、日志内容、日志类型、事件类型、风险级别。日志的内容为对应模块的日志调试信息，如需了解日志的具体含义，请联系运维人员咨询相关内容。

审计查询生成的过程为：auditlog 收集系统日志，将日志匹配审计规则，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。您可以根据需要在**安全审计** > **策略设置** > **审计策略**查看默认的审计规则，也可以自己定义审计规则的正则表达式。

在**安全审计** > **审计查询**页面，设置查询条件，查看相关审计日志记录。

4.7.3 原始日志

Auditlog 是云盾的审计模块，auditlog 收集了网络设备、ECS、物理服务器、RDS、OpenAPI 的日志记录，专有云云盾高级版通过调用 API 的方式从 auditlog 中获取日志记录。日志中记录了应用在运行时产生的必要的调试信息，维护人员可以根据这些调试信息定位系统出现的故障。

单击**安全审计** > **原始日志**进入**原始日志**页面，选择审计类型、审计对象，通过输入查询关键字及起始时间来设置查询条件，单击**查询**，查看原始日志记录。

4.7.4 策略设置

4.7.4.1 添加审计策略

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。

Auditlog 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，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. 选择**策略设置** > **审计策略**，选择审计类型及审计对象，可以进行审计策略的查询。
2. 单击**新增**，在**新增规则**对话框中输入相关信息可添加审计策略，如图 *69:* 新增规则对话框所示。

图 69: 新增规则对话框

3. 配置审计规则参数。

   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下文中设置的报警接收人。例如设置了正则表达式：*hi|hello*，并设置了 ECS 日志类型、登录尝试事件、高风险事件，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审计事件，发送一封告警邮件给告警接收人。

4.7.4.2 添加审计类型

操作步骤

1. 在**策略设置** > **类型设置**页面可以查看已经存在的审计类型列表。
2. 单击**新增**，在**新增事件类型**对话框中设置要添加的事件类型。

3. 单击**确定**，完成添加审计类型。

4.7.4.3 设置报警接收人

设置报警接收人的邮箱，在发生审计事件后，会将事件上报到告警人的邮箱。

操作步骤

1. 在**安全审计** > **策略设置** > **告警设置**页面，单击**新增**，弹出**新增报警接收人**对话框，如图 *70:* 新增报警接收人对话框所示。

图 70: 新增报警接收人对话框

2. 在**邮箱**的输入框中，输入报警接收人的邮箱地址，在**风险等级**的下拉框中，选择风险等级。
3. 单击**确定**，添加报警接收人。

4.7.4.4 管理事件日志存档

操作步骤

选择**策略设置** > **存档管理**，可以查看存档列表，如图 *71:* 存档管理页面所示。

图 71: 存档管理页面

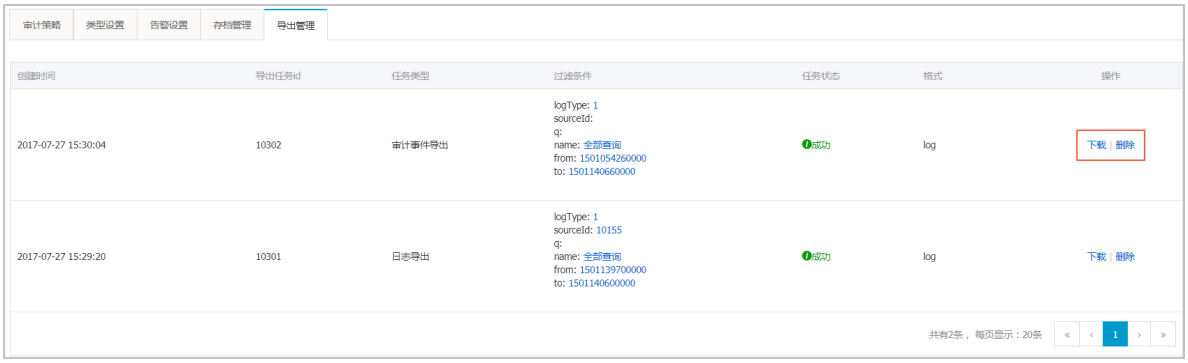
说明: 在输入框输入起始时间可以进行条件筛选。

4.7.4.5 管理导出任务

操作步骤

1. 选择**策略设置** > **导出管理**，可以查看已创建的导出任务，如图 72: 导出管理页面所示。

图 72: 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**可下载审计日志文件。
3. 选择导出任务，在操作栏单击**删除**可删除该导出任务。

4.8 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。

阿里云 WAF 目前防护的流量定位在 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。

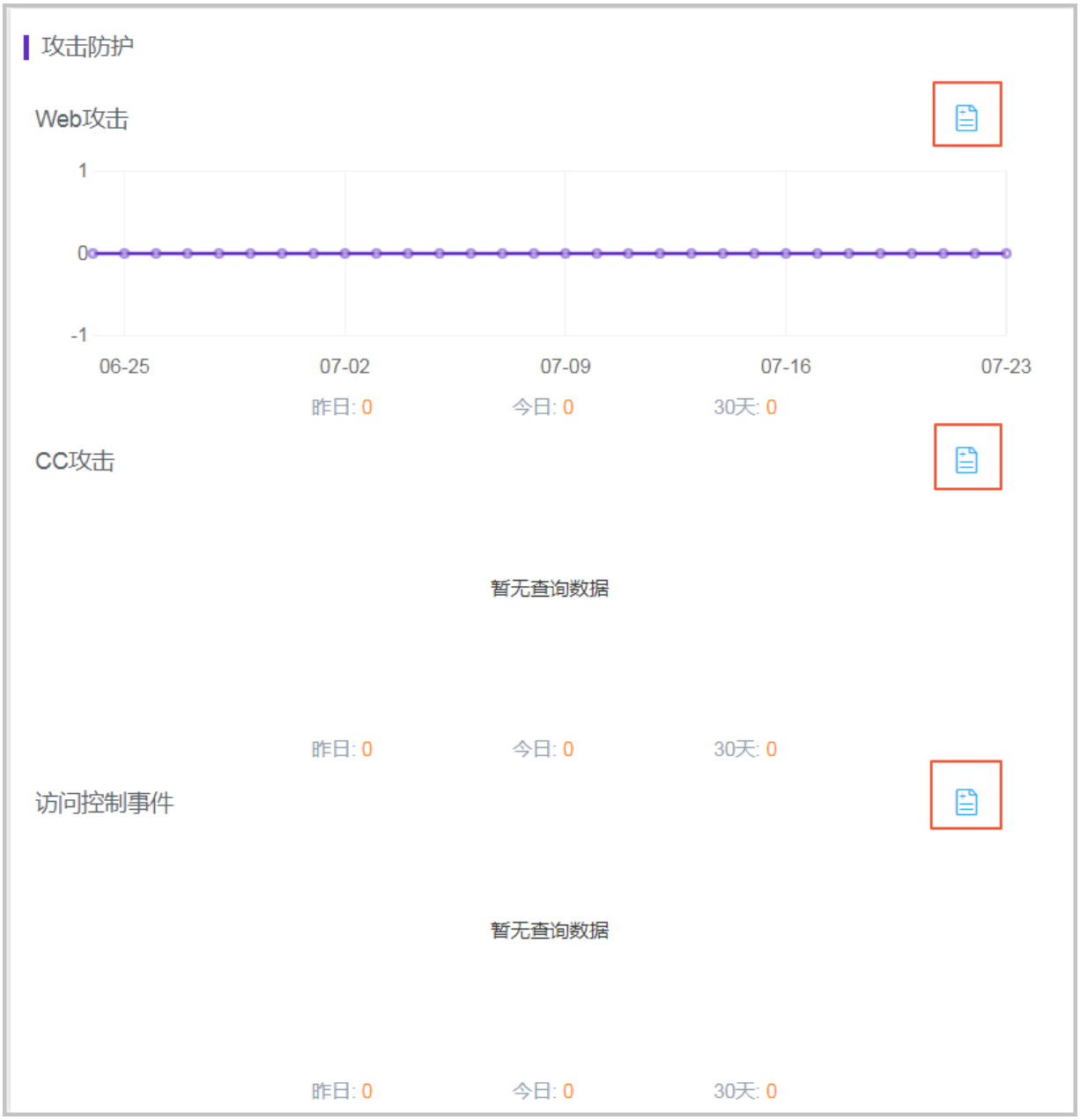
4.8.1 安全总览

安全总览页面提供攻击防护报表和消息页面。

- 攻击防护报表分Web 攻击、CC 攻击、及访问控制事件三块防护情况展现，并显示昨日、今日、及30天内防护次数，单击报表右上方查看详情按钮，可查看详细攻击防护情况。
- 消息页面实时发布WAF防护相关规则更新。

在**Web应用防火墙**，单击**安全总览**，查看 WAF Web 攻击防护信息，如图 73: 安全总览页面所示。

图 73: 安全总览页面



4.8.2 安全报表

安全报表可查看Web应用防火墙详细防护情况。

在**Web应用防火墙** > **安全报表**页面，选择类型，选择防护的域名，选择查询时间，查看不同类型防护的详细安全报表。

图 74: Web应用攻击页面

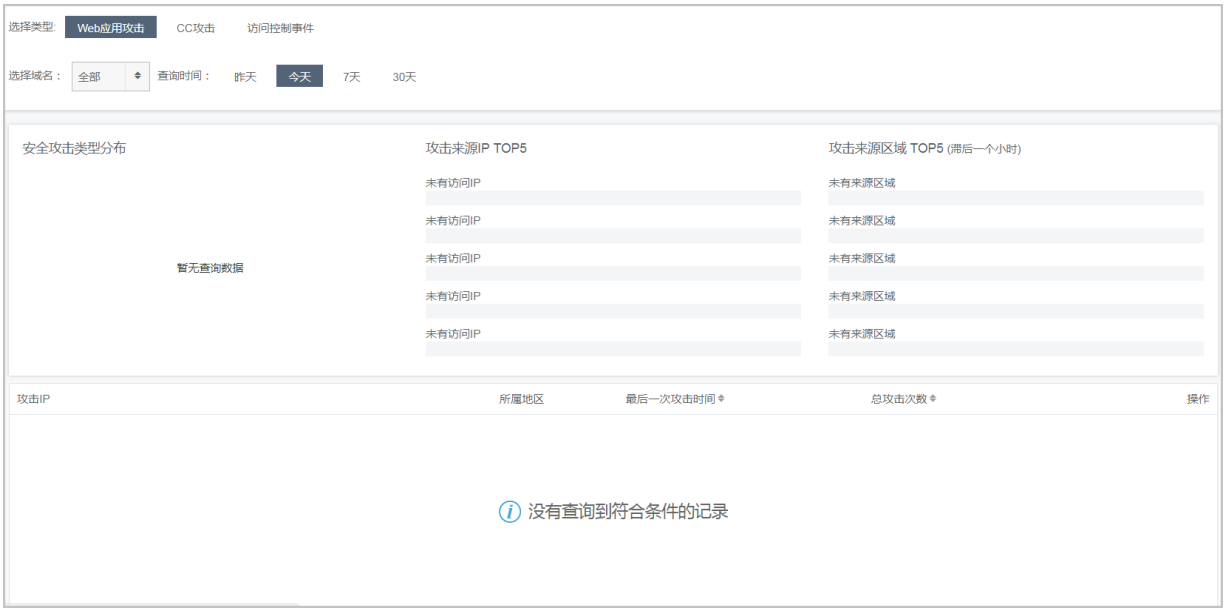


图 75: CC攻击页面

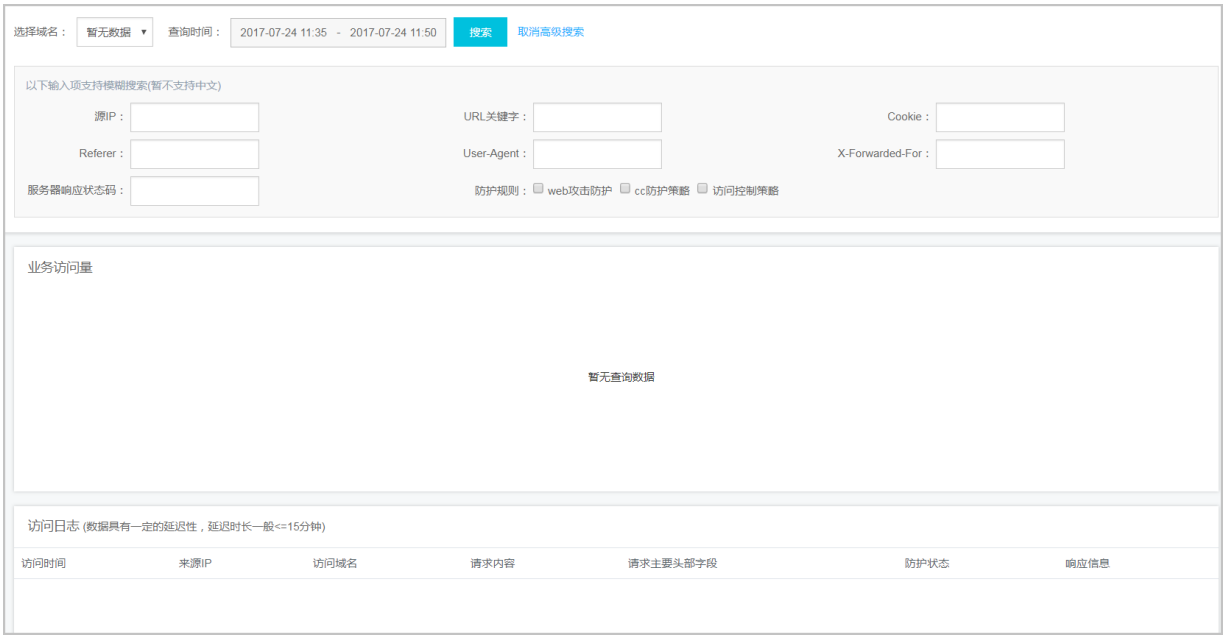
图 76: 访问控制事件页面

4.8.3 业务分析

业务分析结合 Web 应用防火墙的攻击拦截情况及访问流量，对业务访问情况进行分析，帮助您及时发现业务漏洞，提升防御能力。

在**Web应用防火墙** > **业务分析**页面，选择域名及查询时间，单击**搜索**，查看业务分析结果，如图 77: 业务分析页面所示。同时，业务分析页面支持高级搜索功能，支持包括请求IP、URL、User-Agent、Referer等字段的模糊搜索。

图 77: 业务分析页面



4.8.4 域名配置

域名配置页面可设置需要进行防护的域名。域名接入Web应用防火墙，访问流量将经过Web应用防火墙过滤。在配置完域名后，必须在您的DNS服务商处添加域名对应的Cname解析后，防护才能生效。

在**Web应用防火墙 > 域名配置**页面，按照提示步骤添加您想要防护的域名，如图 *78: 添加域名*所示。

图 78: 添加域名

4.9 系统管理

系统管理模块作为专有云云盾不可或缺的部分，为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：

- 用户管理：用于为专有云云盾的用户配置权限并管理专有云云盾配套的阿里云账号。
- 情报同步：用于配置查看专有云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：用于配置专有云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。

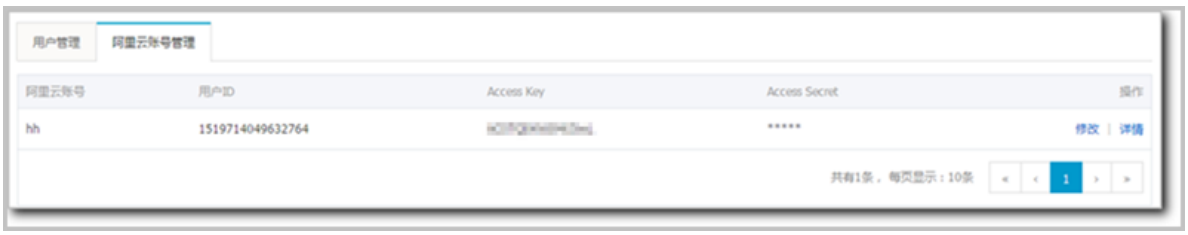
4.9.1 管理阿里云账号

操作步骤

1. 在**系统管理 > 阿里云账号管理**中，可以查看修改系统绑定的阿里云账号信息，如图 *79: 阿里云账号管理页面*所示。

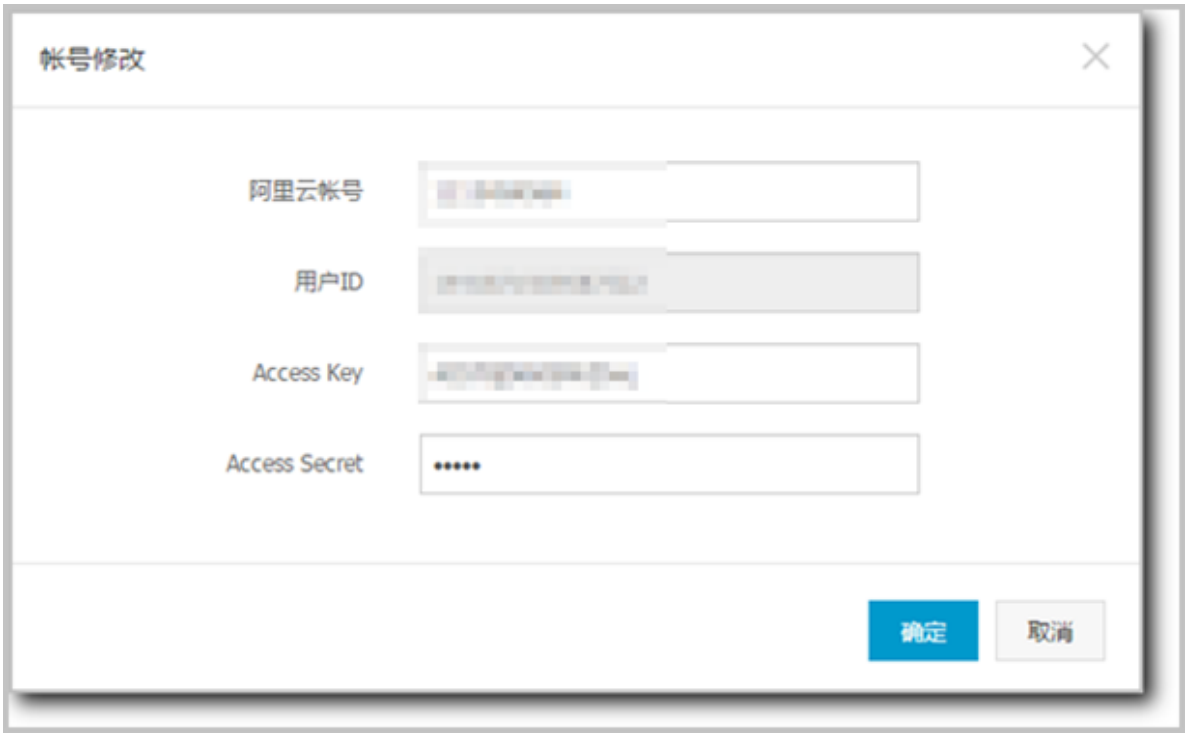
   云盾中的资产均与阿里云账号绑定，请谨慎修改。

   图 79: 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 *80:* 帐号修改对话框所示。

图 80: 帐号修改对话框



3. 单击**详情**，查看阿里云账号详细信息，包括证书到期时间、安骑士证书数目，如图 *81:* 帐号详情所示。这些信息均是通过配置的 ID、key 信息从阿里云获取。

图 81: 帐号详情

4.9.2 情报同步

情报同步是将阿里公共云上的应急响应信息库、人员注册账号库、人员泄漏信息库、人员信息扫描库、0day 规则库、漏扫漏洞库、漏洞主库和行业新闻库同步到本地数据库。同步下来的应急响应信息库、人员注册账号库、人员泄漏信息库、人员信息扫描库、漏扫漏洞库、漏洞主库和行业新闻库在态势感知的情报里展示出来，为用户系统重要安全参考和情报信息。0day 规则库用于大数据模型分析，分析出的数据展示在态势感知的威胁，展示了用户系统目前面临的安全威胁。

情报同步方式主要有云端推送和客户端拉取两种方式，详情请参见表 *14:* 情报同步方式表。

表 14: 情报同步方式表

	云端推送方案	客户端拉取方案
方案细节	1. 本地客户端向云端注册本地监听的端口和 IP，订阅同步的数据内容； 2. 初次连接后云端将本地数据全部推送到本地客户端；	1. 本地客户端向云端初次连接并注册，拉取关心的数据； 2. 本地客户端定时向云端拉取数据，先检查数据版本号是否一致，如果一致则不拉取，否则同步当前版本数据； 3. 数据拉取的频率默认为一天，可以通过配置修改；

	云端推送方案	客户端拉取方案
	3. 后续有新增或者修改数据后，将数据增量推送到客户端； 4. 本地客户端在接收数据时需要校验一下同步数据的版本号，如果一致则不处理； 5. 本地客户端可以发起数据同步的请求，云端将当前版本数据全部推送到客户端； 6. 数据同步到本地后，需要在专有云安全控制台中进行确认后才能生效。	4. 数据同步到本地后，需要在专有云安全控制台中进行确认后才能生效。
优点	数据能够实时同步到客户端。	可以自定义数据同步的频率，实现简单。
缺点	数据更新频繁或者数据量大时需要同时同步到多个客户端，同步压力较大，实现较复杂。	不能进行数据的实时同步。
结论	由于当前场景中对于数据的实时性要求不高，建议采用客户端拉取。	

4.9.2.1 同步状态说明

情报同步列表中的数据是初始化的，暂时只支持将阿里公共云上的应急响应信息库、人员注册账号库、人员泄漏信息库、人员信息扫描库、0Day 规则库、漏扫漏洞库、漏洞主库和行业新闻库同步到本地数据库。每种数据类型的数据把数据从云端同步下来的频率跟时间是可以通过单击设置，来设定的，可以是手动触发，也可以是自动触发，如果不设置，同步的频率按初始数据来定。为了缓冲数据，从云端同步下来的数据先被同步到缓冲区，然后才被同步到正式库中，因此情报同步列表中数据的状态会从下载中，已下载过渡到安装中，已安装。

表 15: 同步状态说明表

状态	说明
下载中	数据在从云端下载到隔离区中。
已下载	数据完成从云端下载到隔离区中。
安装中	数据在从隔离区下载到正式库中。
已安装	数据完成从隔离区下载到正式库中。

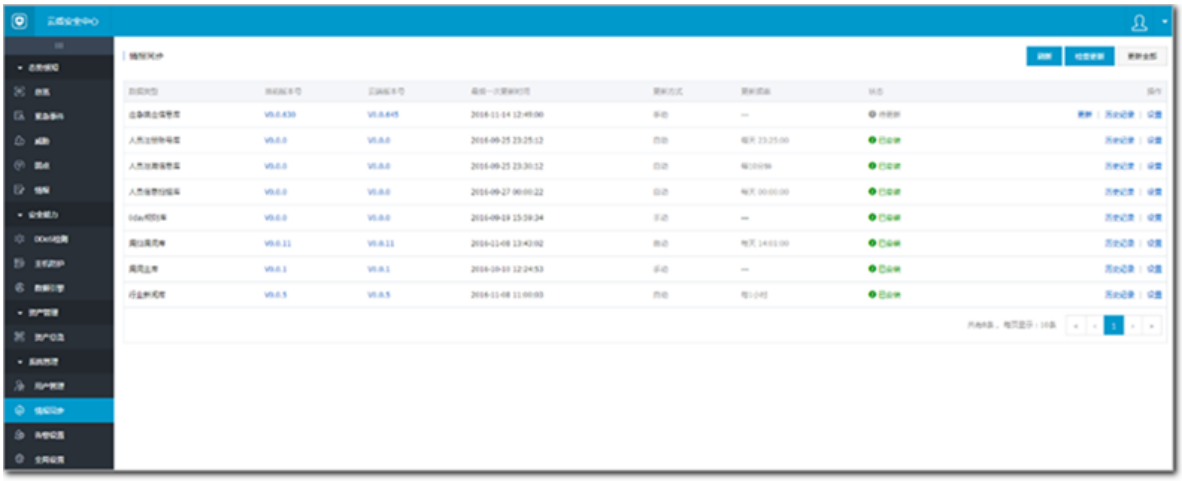
状态	说明
待更新	云端有新版本可以更新。

4.9.2.2 更新情报同步列表

操作步骤

在**系统管理** > **情报同步**页面，单击**更新**，刷新情报同步列表，如图 *82:* 情报同步页面所示。

图 82: 情报同步页面

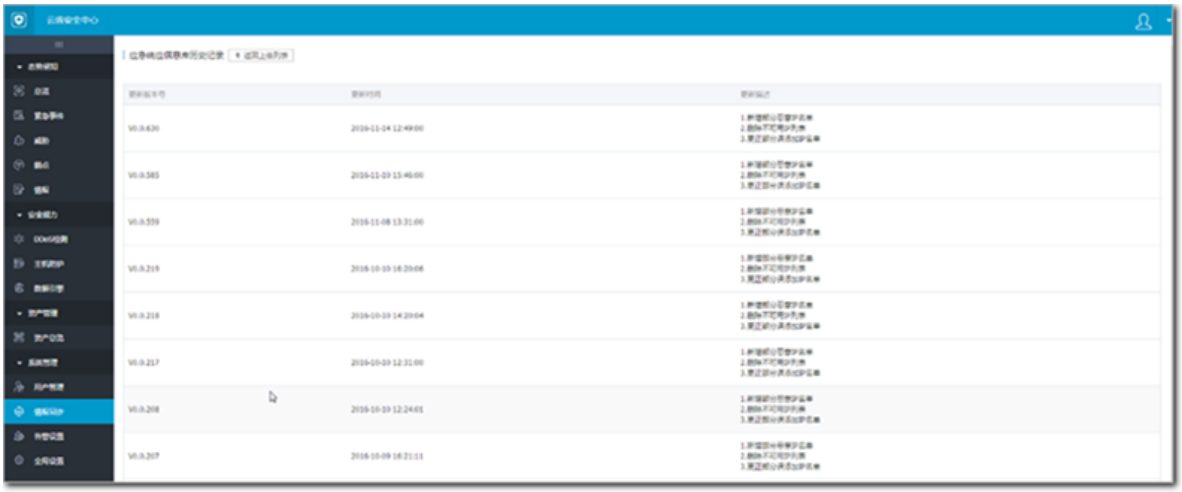


4.9.2.3 查看历史记录

操作步骤

通过查看历史记录，可以了解该种数据类型的数据的同步记录，如图 *83:* 查看历史记录所示。

图 83: 查看历史记录

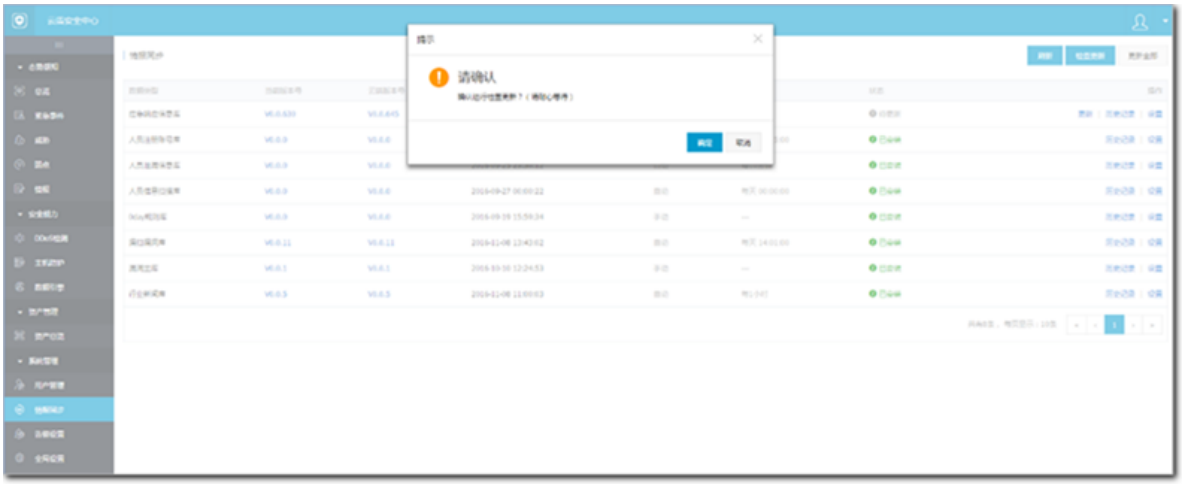


4.9.2.4 检查情报更新

操作步骤

在**系统管理** > **情报同步**页面，单击**检查更新**，会检测云端是否有新版本的数据需要更新，如果有，相应数据类型的数据状态会变成**待更新**，如图 *84:* 情报检查更新所示。

图 84: 情报检查更新

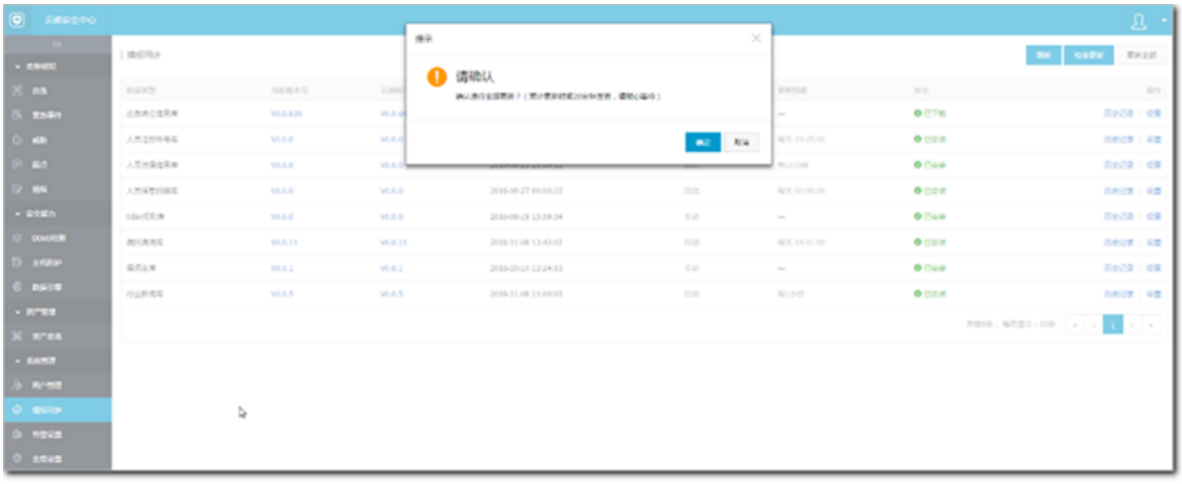


4.9.2.5 更新全部情报

操作步骤

在**系统管理** > **情报同步**页面，单击**更新全部** ，将数据从云端下载到版本库中，如图 *85:* 更新全部情报所示。

图 85: 更新全部情报



4.9.3 告警设置

告警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，以便管理员了解系统发生的安全事件。

4.9.3.1 设置告警联系人

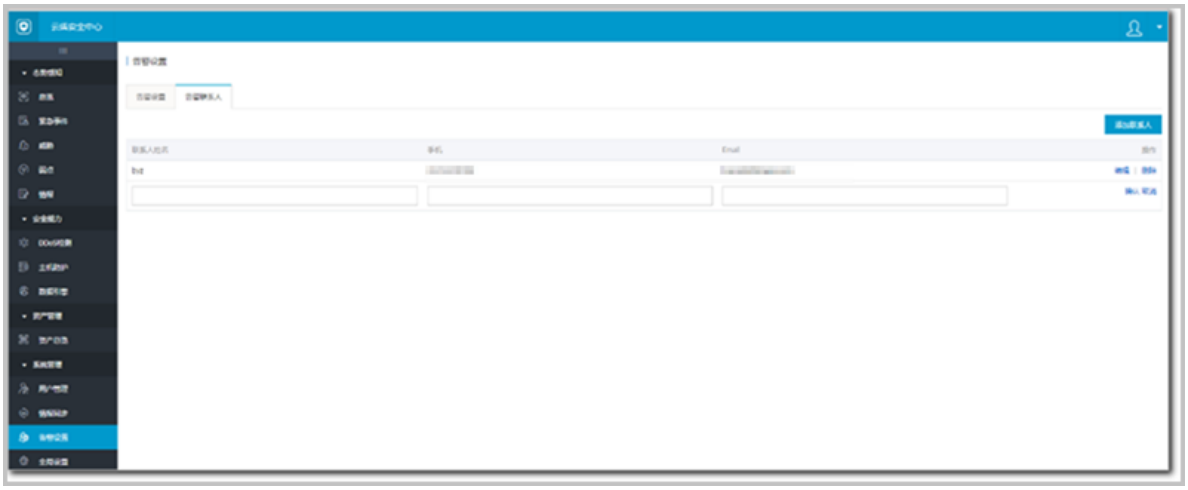
背景信息

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. 在**系统管理** > **告警设置** > **告警联系人**页面，单击**添加联系人**，如图 *86:* 告警联系人页面所示。

图 86: 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页面上的**编辑**和**删除**按钮，进行相关联系人信息的编辑或删除。

4.9.3.2 设置告警信息

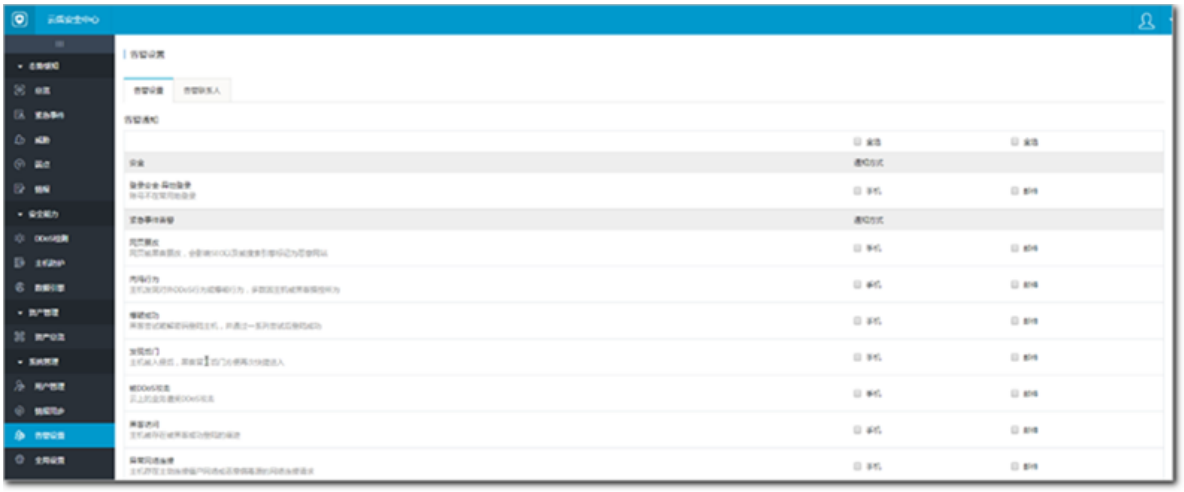
背景信息

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。

操作步骤

在**系统管理** > **告警设置** > **告警设置**页面，选择每个安全事件的通知方式单击**确认**，如图 *87: 告警设置页面*所示。

图 87: 告警设置页面



4.9.4 全局设置

专有云云盾提供全局设置，供管理员对云盾流量采集监控的网段范围以及安骑士上报检测区域进行设置。主要支持查询、添加、修改、删除操作。

流量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。

4.9.4.1 流量采集网段设置

网段设置主要针对流量监控服务进行网段配置，并且支持管理更改监控的网段范围，方便您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。更多信息可以参考流量监控。

网段设置更改后立即对流量监控生效，不需要管理员进行其他操作。

4.9.4.1.1 添加流量采集网段

操作步骤

1. 在**系统管理** > **全局设置** > **流量采集网段设置**中，单击**添加**，弹出**添加监控网段**对话框，如图 *88: 添加监控网段对话框*所示。

图 88: 添加监控网段对话框

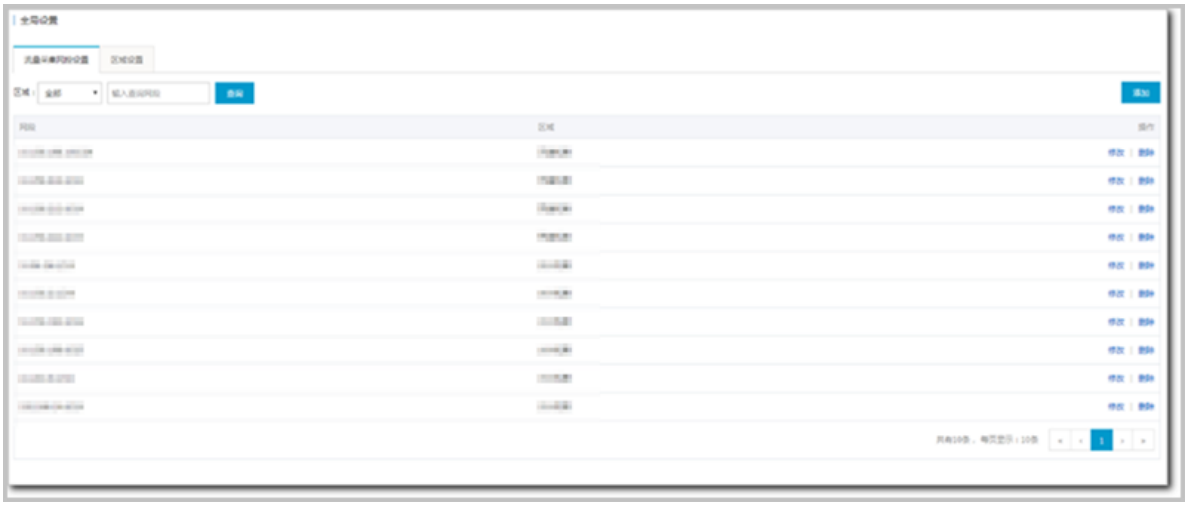
2. 填写网段，要求必须是合法网段，并且不允许重复添加。
3. 选择所属区域。
4. 单击**确定**，完成添加。

4.9.4.1.2 管理流量采集网段

操作步骤

1. 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 *89:* 全局设置页面所示。

图 89: 全局设置页面



2. 选择需要的网段，执行如下操作：
   - 修改流量采集网段

单击**修改**，弹出**修改网段**对话框（只支持区域修改），修改所属区域后，单击**确定**，完成修改。

- 删除流量采集网段

  单击**删除**，可以删除配置的监控网段。

4.9.4.2 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。

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，具体操作参见资产总览。

4.9.4.2.1 添加区域网段

操作步骤

1. 在**系统管理** > **全局设置** > **区域设置**中，单击**添加**按钮，弹出**添加网段**对话框，如图 *90:* 添加网段对话框所示。

   图 90: 添加网段对话框

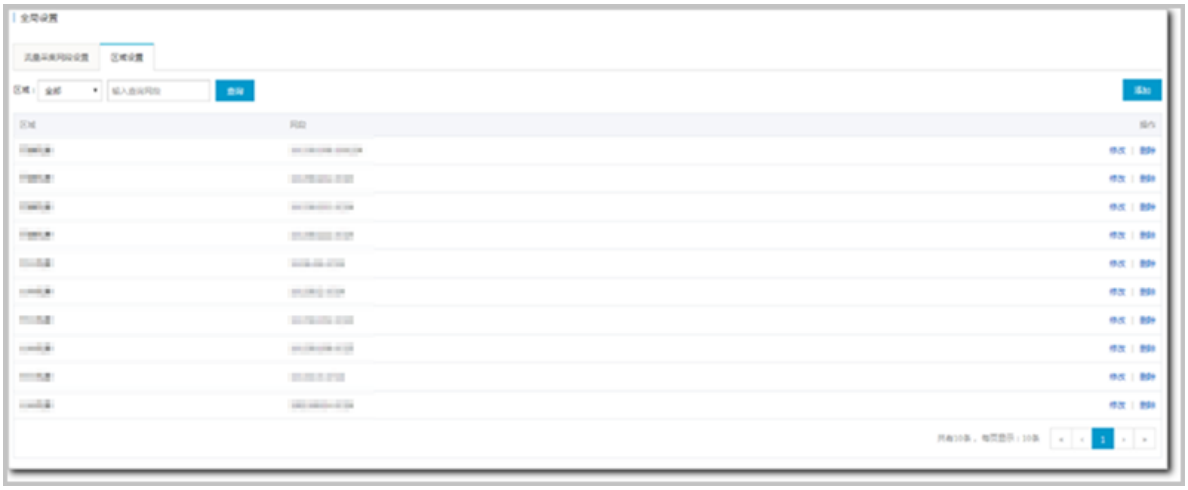
2. 填写网段，要求必须是合法网段，并且不允许重复添加。
3. 选择所属区域。
4. 单击**确定**，完成添加。

4.9.4.2.2 管理区域网段

操作步骤

1. 选择区域，输入查询网段，单击**查询**，查看区域网段信息，如图 *91:* 区域设置页面所示。

   图 91: 区域设置页面

2. 选择需要的网段，执行如下操作：

   - 修改区域网段

     单击**修改**，弹出修改网段对话框（只支持区域修改），修改所属区域后，单击**确定**，完成修改。

   - 删除区域网段

     单击**删除**，可以删除配置的网段区域。

5 云盾（基础版）

5.1 产品概述

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。

云盾基础版为您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，并能够提供云计算平台的 ECS、RDS、物理服务器、OpenApi 服务的安全审计，还支持对自定义的审计类型进行审计。

架构

专有云云盾基础版通过 DTCenter 获取 ECS 和租户信息，将云计算平台的安全事件和安全数据信息进行了分析和整理，以图表方式呈现给管理员，让云安全状况一目了然，让安全防御更简单。

5.2 云盾安全中心界面概述

云盾基础版的安全中心界面主要可以分为三大区域，如图 92: 云盾基础版安全中心界面图所示。

图 92: 云盾基础版安全中心界面图

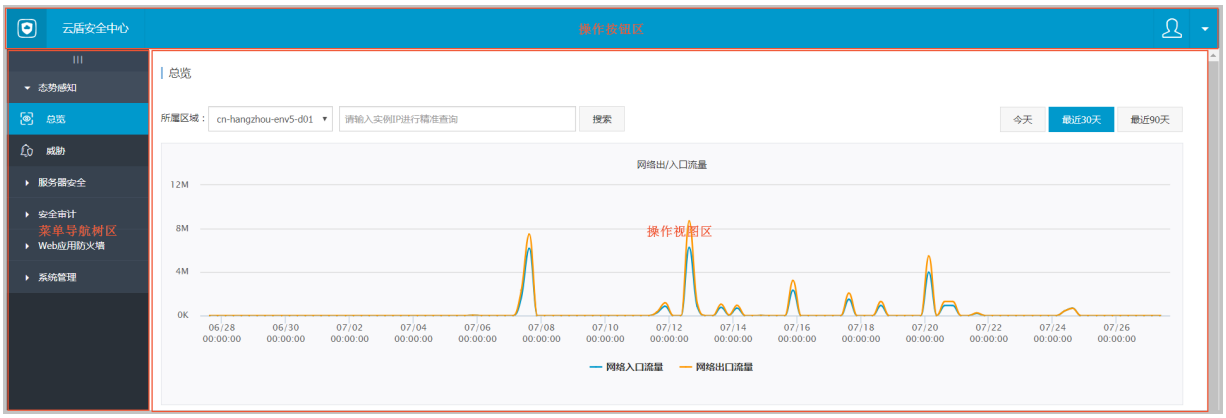


表 16: Web 界面区域说明

区域	说明
操作按钮区	单击此按钮将退出当前登录。 单击此按钮将进入全屏模式，再此点击则退出全屏模式。 帮助：单击该链接可以查看当前页面的帮助信息。
菜单导航树区	云安全中心管控平台包含安全大盘、云平台安全、安全审计、系统管理4个部分，主要功能如下： • 安全大盘：安全事件展示、趋势分析，实时流量监控和趋势展示，用于管理员了解当前云服务的防护情况。 • 云平台安全：流量监控、主机入侵、Web攻击、DDoS攻击、Web漏洞、恶意主机等安全事件展示，以便管理员进行分析和处理。 • 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。 • 系统管理：安全事件报警接收人设置，以便安全管理员及时处理云服务的安全事件。云安全中心和云安全控制台登录和操作日志展示，以便系统管理员进行分析和审计。
操作视图区	当选择了菜单项后，该菜单项的功能配置界面就会显示在右侧的操作视图区中。

5.3 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包含两个部分：

- 安全总览：展现安全的整体态势、网络流量情况和大屏相关信息。
- 威胁分析：展现业务系统中目前面临的安全风险和威胁来源。

5.3.1 总览

5.3.1.1 简介

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，让您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。

5.3.1.2 查看网络流量信息

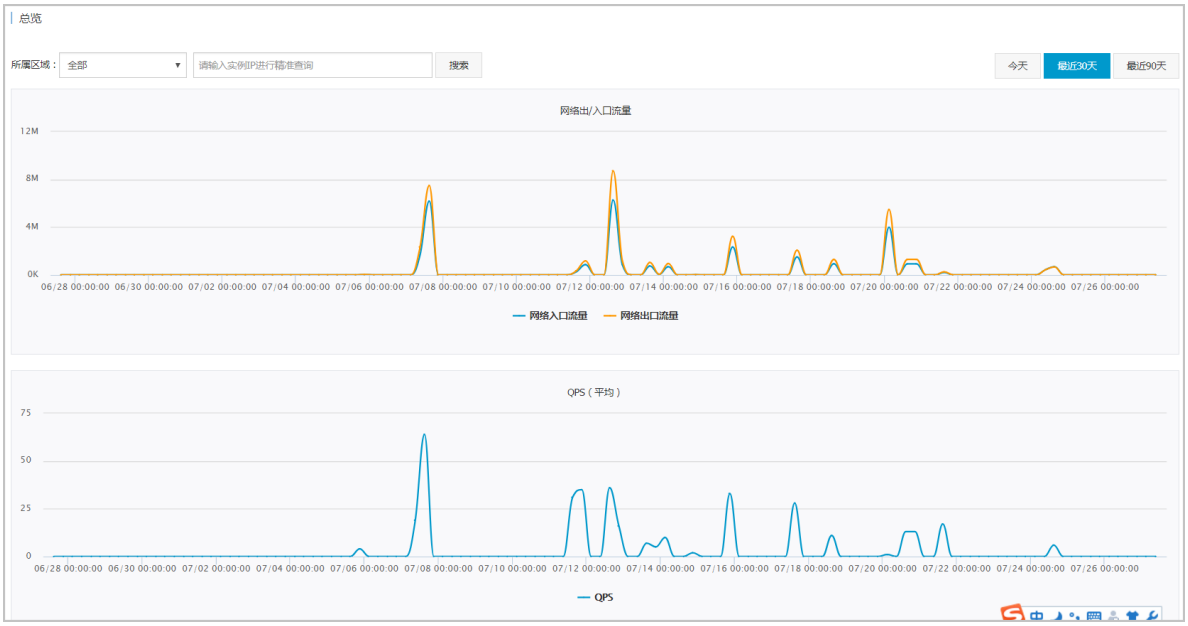
背景信息

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，可以有效甄别恶意的 IP 访问。

操作步骤

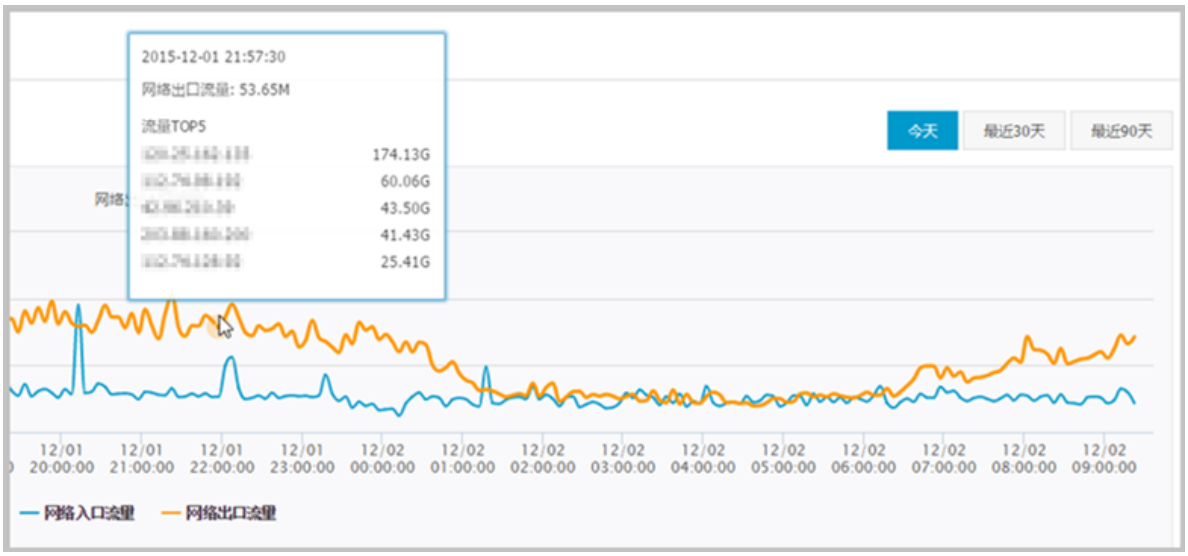
1. 单击**总览**，进入**总览**页面，如图 *93:* 总览页面所示。

图 93: 总览页面



2. 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。
3. 在**所属区域**中可以选择区域信息，在搜索框中输入 IP，可以分区域、分 IP 查询流量信息。
4. 将鼠标停留在流量折线图上，可以显示流量 TOP5 的 IP，如图 *94:* 查看流量 *TOP5* 的 *IP*所示。

图 94: 查看流量 TOP5 的 IP



5.3.2 威胁

5.3.2.1 简介

云盾基础版威胁页面包括Web 应用攻击和暴力破解两类安全信息：

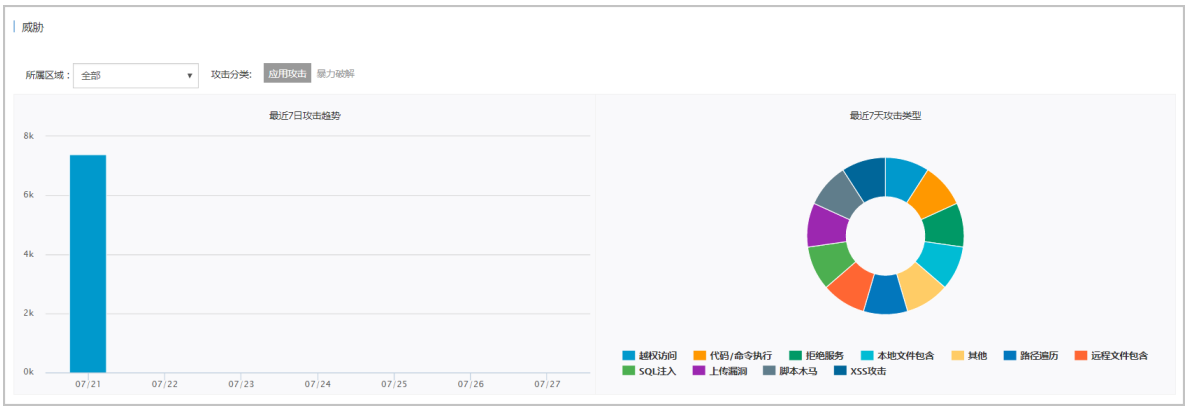
- Web 应用攻击：访问 Web 服务器的流量都会经过云盾的核心组件 beaver，beaver 将对流量进行监测，提取流量中的攻击信息。
- 暴力破解：每台资产都需要安装安骑士客户端，当黑客针对某个资产进行暴力破解的时候，安骑士客户端能够及时监测到爆破的发生并上报给控制台。

5.3.2.2 查看威胁攻击信息

操作步骤

1. 在**威胁**页面，单击 **应用攻击**，查看应用攻击信息及上报的应用攻击事件，如图 *95: 应用攻击页面*所示。

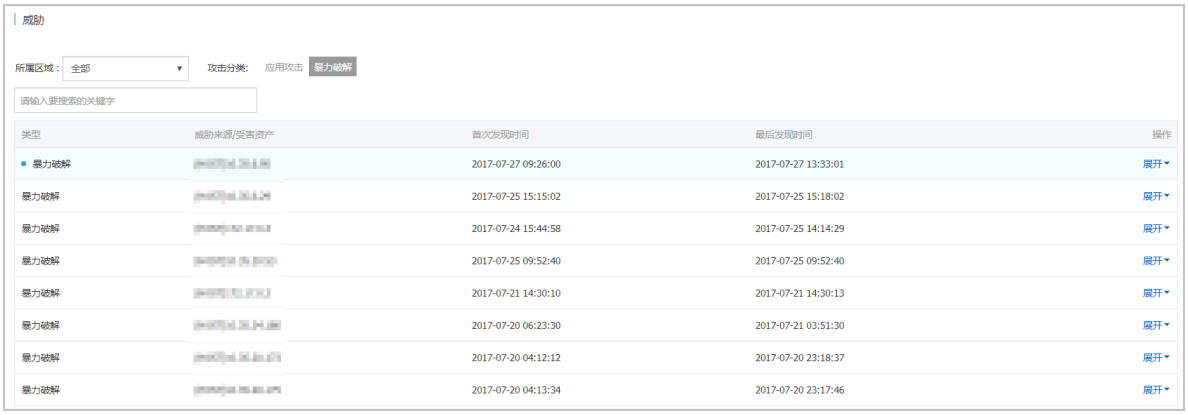
图 95: 应用攻击页面



您可以查看最近 7 日的攻击趋势、攻击的类型以及详细的攻击信息。

2. 单击**暴力破解**，查看暴力破解事件记录，如图 *96:* 暴力破解页面所示。

图 96: 暴力破解页面



5.4 服务器安全

5.4.1 简介

专有云云盾能够防护每一台用户主机的安全，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。

主机防护具有以下功能：

- 防护基线：云盾能够实时展示安骑士的防护状态和基线检查状态，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：云盾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。支持RDP/SSH的异地登录告警。
  - 暴力破解防护：安骑士插件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。支持RDP/SSH等应用的密码破解攻击防护。
- 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。
- 补丁管理：及时获取最新漏洞预警和补丁，并能通过云端一键下发补丁更新。

主机入侵检测功能列出所有服务器上发现的文件篡改、异常进程、异常网络连接、可疑端口监听等行为，帮助您及时发现服务器安全隐患。

5.4.1.1 安骑士客户端原理

安骑士客户端程序包含 Webshell 特征库、Webshell 隔离模块、补丁特征库和补丁修复模块，功能分别如下：

- Webshell 特征库的功能是用来检测文件是否符合特征库的特征，如果符合，会发送木马文件到安骑士服务器，由安骑士服务器结合更多的特征库进一步分析是否为木马文件；
- Webshell 隔离模块的功能是安骑士客户端通过向安骑士服务器确认为木马文件之后，对该文件进行隔离；
- 补丁特征库的功能是用来检测文件是否符合特征库的特征，如果符合，会发送漏洞文件到安骑士服务器，由安骑士服务器结合更多的特征库进一步分析是否为漏洞文件；
- 补丁修复模块的功能是是安骑士客户端通过向安骑士服务器确认为漏洞文件之后，对该文件进行修复。

安骑士客户端提供了 Windows 版本和 Linux 版本，可以根据主机操作系统选择相应版本，安装后安骑士客户端可以自动连接到安骑士服务器端进行在线升级。

5.4.1.2 安骑士服务器端原理

安骑士服务器端包括 aegis-server、defender 和 aegis-health-check 三个模块。其功能分别如下：

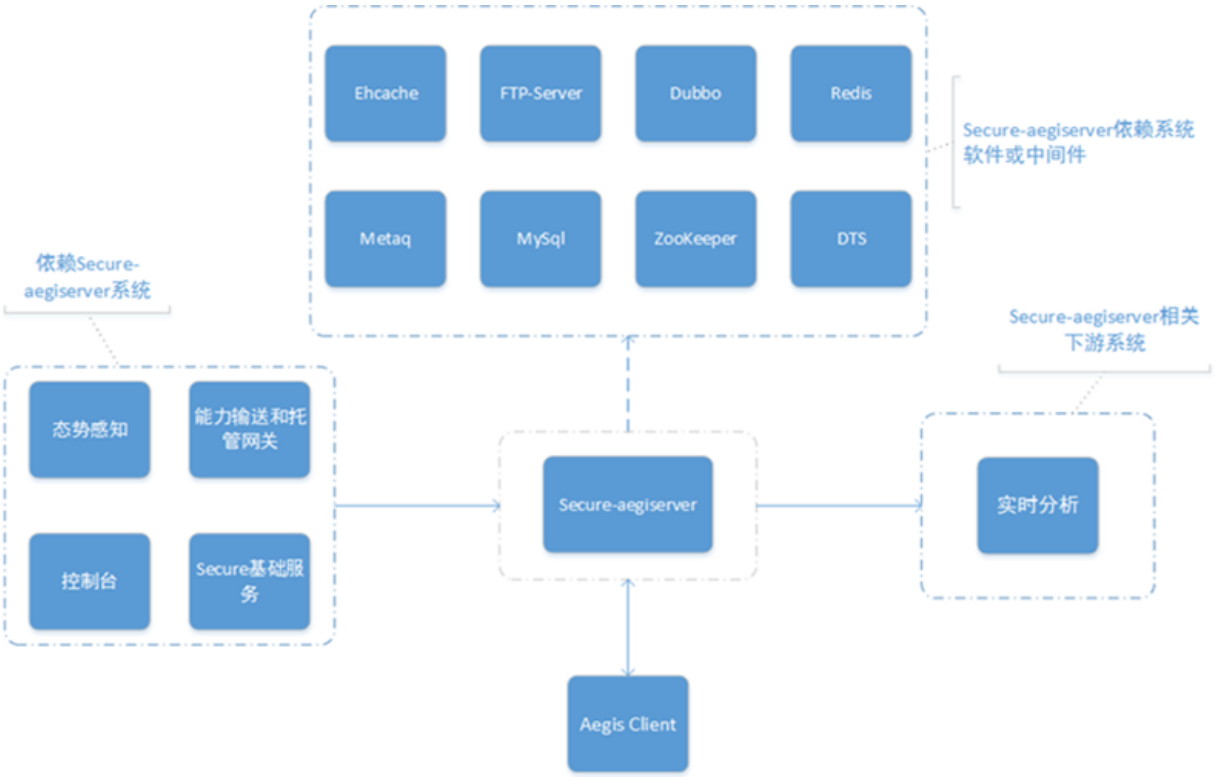
- aegis-server 包括通讯模块和客户端检查模块，主要功能是向下和 aegis-client 交互，收集木马文件，补丁文件等信息，向上和 defender 反馈异地登录信息、爆破信息和爆破成功等信息；
- defender 的主要功能是异地登录分析、暴力破解分析和暴力破解是否成功的分析；

- aegis-health-check 的主要功能是进行基线检查，通过 aegis-server向客户端下发基线检查的命令，并且通过aegis-server 接收客户端返回的数据，修改基线检查的状态。

安骑士服务器端提供了 API 供专有云云盾控制台来获取信息，解析安全事件并分析后呈现给管理员，管理员可以下发命令对木马文隔离或者忽略，可以下发命令对补丁文件进行修复或者忽略。

安骑士整体架构如图 97: 安骑士整体架构所示。

图 97: 安骑士整体架构



- 使用通用软件进行建站

  极易因为通用软件的漏洞而被黑客入侵，使用服务器安全（安骑士）进行漏洞监测，一旦爆发漏洞可快速进行一键修复。

- 有 Web 服务

  不管是内部 Web 服务还是外部 Web 服务，黑客均可以通过 Web 服务窃取网站的核心数据，开启 Web 攻击拦截可有效阻止黑客从外部的攻击和内部的渗透。

5.4.2 主机防护

5.4.2.1 防护基线

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

5.4.2.1.1 原理简介

Aegis-client 和 aegis-server 端通过 TCP 长连接通道进行消息传递，这个通道是 aegis 产品中最核心的部分，稳定性高达 99.99 %，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 aegis-client 成功与 aegis-server 建立通信并登录后，该主机的 aegis 防护状态便被置为在线，此后，sever 会定时向 client 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，记录下最后在线时间。

aegis-health-check 工程通过 aegiserver 向 Linux 或者 Windows 主机下发安全体检的命令，aegiserver 收到客户端返回的体检结果，通过 metaq 发消息给 aegis-health-check，更新体检结果。支持对体检结果进行修复，验证，忽略等功能，以此提高主机的安全性，还可以查看最近十次的体检记录 ，历史体检记录不支持验证，忽略和修复，支持回滚功能。支持查看已忽略体检记录，并且可以取消忽略。

5.4.2.1.2 查看主机防护状态

背景信息

Aegis 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，并支持刷新列表，默认展示全部区域，按照 IP 排序。

操作步骤

在**服务器安全** > **主机防护** > **防护基线**页面，设置查询条件，单击**查询**，查看主机防护状态。

5.4.2.1.3 立即执行主机安全检查

操作步骤

1. 如果主机从未进行过安全巡检，可选择该主机，单击**查看详情**。
2. 单击**立即检查**。
3. 在**选择巡检内容**对话框中，选择需要检测的具体项目。
4. 单击**确定**，下发安全巡检命令。

5.4.2.1.4 重新执行主机安全检查

操作步骤

1. 如需对主机重新进行安全巡检，选择该主机，单击**查看详情**。
2. 单击**重新检查**。
3. 在**选择巡检内容**对话框中，选择需要检测的具体项目。
4. 单击**确定**，重新下发安全巡检命令。

5.4.2.1.5 查看主机安全体检记录

操作步骤

1. 检查完成后，选择该主机，单击**查看详情**。
2. 单击**查看体检记录**，可查看近 10 次的体检记录。

说明: 历史体检结果不支持验证、忽略和修复，支持回滚功能。

5.4.2.1.6 查看已忽略检查项目

操作步骤

1. 检查完成后，选择该主机，单击**查看详情**。
2. 单击**已忽略项目**，可查看已被手动忽略项目，取消忽略后可进行风险检测。

5.4.2.1.7 处理风险项

操作步骤

1. 检查完成后，选择该主机，单击**查看详情**。
2. 选择待处理的风险项，可对风险项进行**修复**、**验证**、**忽略**等操作。

5.4.2.1.8 离线原因排查

排查步骤如下：

- 检查网络是否连接。
- 检查您是否设置了防火墙 ACL 规则。需要将服务器安全（安骑士）的服务端 IP 加入防火墙白名单以允许网络访问（80端口）。
- 查看是否有第三方的防病毒产品，如果有，尝试关掉之后重新安装 Agent，部分第三方的防病毒软件可能会禁止 Agent 访问网络。

5.4.2.2 登录安全

登录安全主要分为异地登录和暴力破解两部分，管理员可以在专有云云盾上看到异地登录和暴力破解的告警信息，并可以查询登录记录和暴力破解的来源等详细信息，针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便可不再告警。

5.4.2.2.1 登录记录

您可以在配置中心设置服务器的常用登录地，如果没有在常用登录地登录，会在专有云云盾控制台提醒异地登录，在告警设置中可以为异地登录配置手机通知和邮箱通知。常用登录地的设置请参见配置白名单，告警设置请参见告警设置。

流程分析

1. Aegis-client 通过 tcp 协议上报登录信息到 aegis-server。
2. Aegis-server 通过 metaq 消息将上报信息发送到 defender。
3. Defender 分析登录信息，判断是否异地登录，并写入 aegis-db。如果为异地登录，会将消息通过 metaq 发送给 sas 进行进一步处理，判断是否通过手机、邮件提醒用户。

5.4.2.2.2 查询登录记录

背景信息

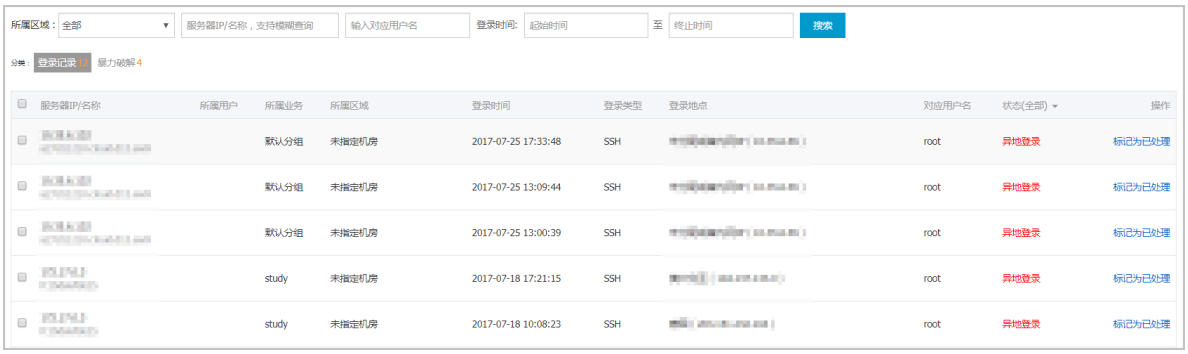
登录记录状态主要有异地登录、正常登录和已处理，支持主机 IP、主机名的模糊查询、登录用户及登录时间的筛选。

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. 在**服务器安全** > **主机防护** > **登录安全**页面，选择**登录记录**，如图 *98:* 登录记录页面所示。

图 98: 登录记录页面



2. 设置查询条件。
3. 单击**搜索**，显示符合条件的登录记录。
4. 确认登录正常后，您可以单击**标记为已处理**。
5. 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醒该记录。

5.4.2.2.3 暴力破解

您可以在配置中心设置白名单，如果暴力破解成功且源 IP 不在白名单内，会在专有云云盾控制台提醒暴力破解成功，在告警设置中可以为暴力破解配置手机通知和邮箱通知。白名单的设置请参见配置中心，告警设置请参见告警设置。

流程分析

1. Aegis-client 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 协议上报暴破消息到 aegis-server。
2. Aegis-server 通过 metaq 消息将上报信息发送到 defender。
3. Defender 分析暴破信息，判断暴破类型，以及是否暴力破解成功，并将暴破信息写入 aegis-db。如果破解成功，会将消息通过 metaq 发送给 sas 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暴破成功、有威胁、无威胁和已处理，时间类型说明请参见表 *17:* 暴力破解事件类型表。

表 17: 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

5.4.2.2.4 查询暴力破解事件

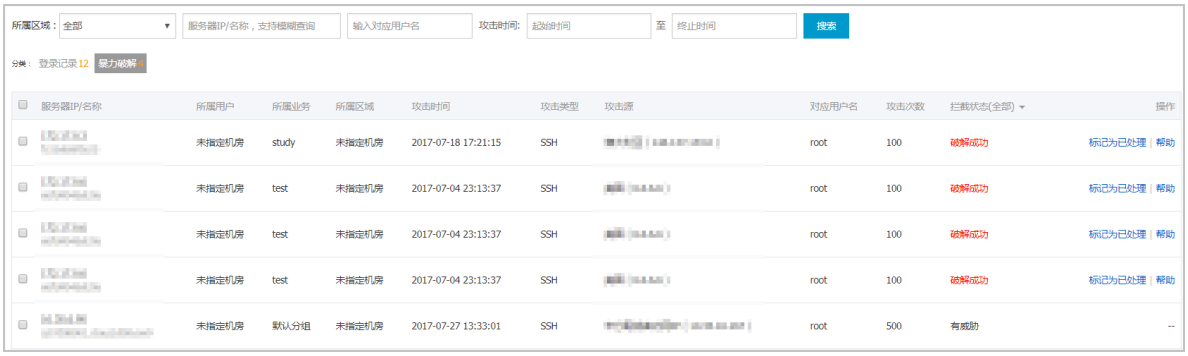
背景信息

通过查询暴力破解事件，您可以了解暴力破解的攻击源、攻击次数以及拦截状态。当控制台产生暴力破解成功意味着您的主机已经被黑客暴力破解出密码并且成功登陆了主机，管理员需要及时进行排查处理。暴力破解事件查询支持主机 IP 及主机名的模糊查询和登录用户及时间的筛选。

操作步骤

1. 在**服务器安全 > 主机防护 > 登录安全**页面，选择**暴力破解**，设置查询条件，单击**搜索**，查看暴力破解事件，如图 *99: 暴力破解事件页面*所示。

   图 99: 暴力破解事件页面



2. 调查暴力破解的原因，排除风险后，您可以单击**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**。

5.4.2.3 木马查杀

黑客入侵网站后，通常会将木马文件放入主机的 Web 服务目录下，和正常文件混在一起，然后用浏览器来访问恶意文件，达到控制网站服务器的目的。而木马查杀则能及时检测木马文件并向管理远告警，管理员可以在专有云云盾控制台查看云盾发现的木马文件，并可以对木马进行隔离、忽略、恢复、移除信任文件一系列操作。在设置了手机或邮件提醒的情况下，同一木马只会在首次发现时推送提醒，设置提醒请参见告警设置。

功能特色

自研网站后门查杀引擎，拥有本地查杀加云查杀体系，同时共享全网最大服务器端的恶意后门文件样本库，支持所有常见后门文件类型，查杀率全球领先。

5.4.2.3.1 操作说明

注意：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。

表 18: 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

5.4.2.3.2 状态说明

表 19: 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。
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。

5.4.2.3.3 查询木马文件信息

背景信息

木马查杀状态主要有待处理、已隔离和信任文件，支持服务器名称和 IP 模糊查询，以及时间段的筛选，可以按紧急程度排序，也可以按照组合服务器查看。

通过查询木马文件事件，您可以了解安骑士发现的木马文件信息。

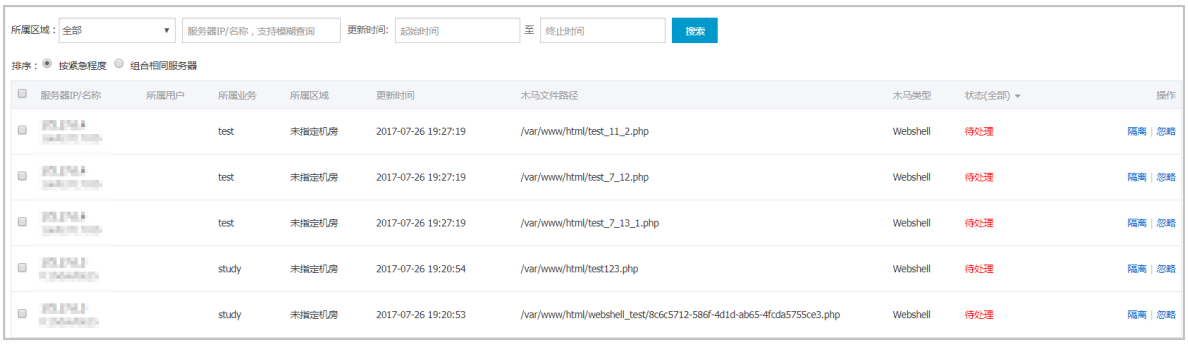
操作步骤

1. 在**服务器安全** > **主机防护** > **木马查杀**页面，设置查询条件，单击**查询**。

   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 *100: 按紧急程度排序展示*所示。

   图 100: 按紧急程度排序展示



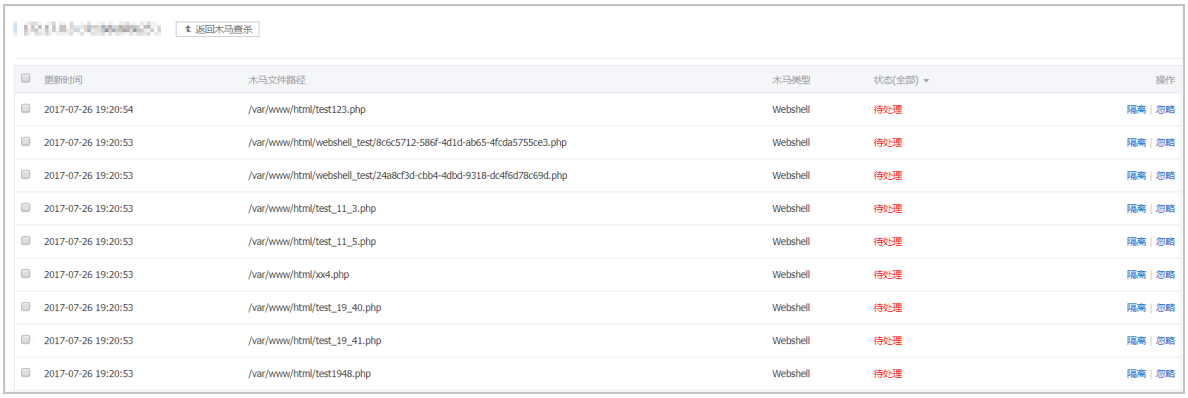
组合相同服务器排序

按待处理个数降序排列，如图 *101:* 组合相同服务器排序展示所示。

图 101: 组合相同服务器排序展示

2. 单击组合服务器排序下的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，展示按紧急程度排序后，按发现时间降序，如图 *102:* 查看服务器详情所示。

图 102: 查看服务器详情



3. 单击**返回木马查杀**，可以回到木马查杀页面重新进行查询。

5.4.2.4 配置中心

5.4.2.4.1 简介

配置中心支持以下配置内容：

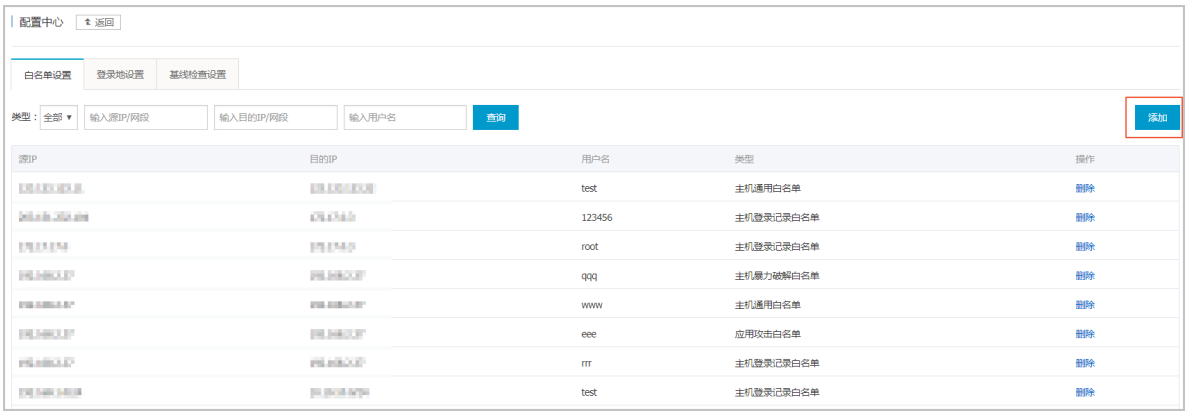
- 白名单设置：登录 IP 白名单主要用于过滤暴力破解和暴力破解成功。如果源 IP 和目的 IP 在登录 IP 白名单中，暴力破解失败。
- 登录地设置：常用登录地主要用于异地登录的判断。如果不设置常用登录地，不管在哪里登录，都不是异地登录。如果设置了常用登录地，在非常用登录地登录的第一次和第五次会提醒此次登录为异地登录，其余都是正常登陆。如果在一个登录地登录次数大于等于六，这个登录地会被加入到常用登录地，并在页面上展示出来。
- 基线检查设置：支持设置周期性自动安全体检策略。

5.4.2.4.2 配置白名单

操作步骤

1. 在**服务器安全** > **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 *103: 白名单设置页面*所示。

   图 103: 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，单击**确认**，添加白名单 IP，如图 *104: 添加白名单对话框*所示。

   图 104: 添加白名单对话框

5.4.2.4.3 配置登录地

操作步骤

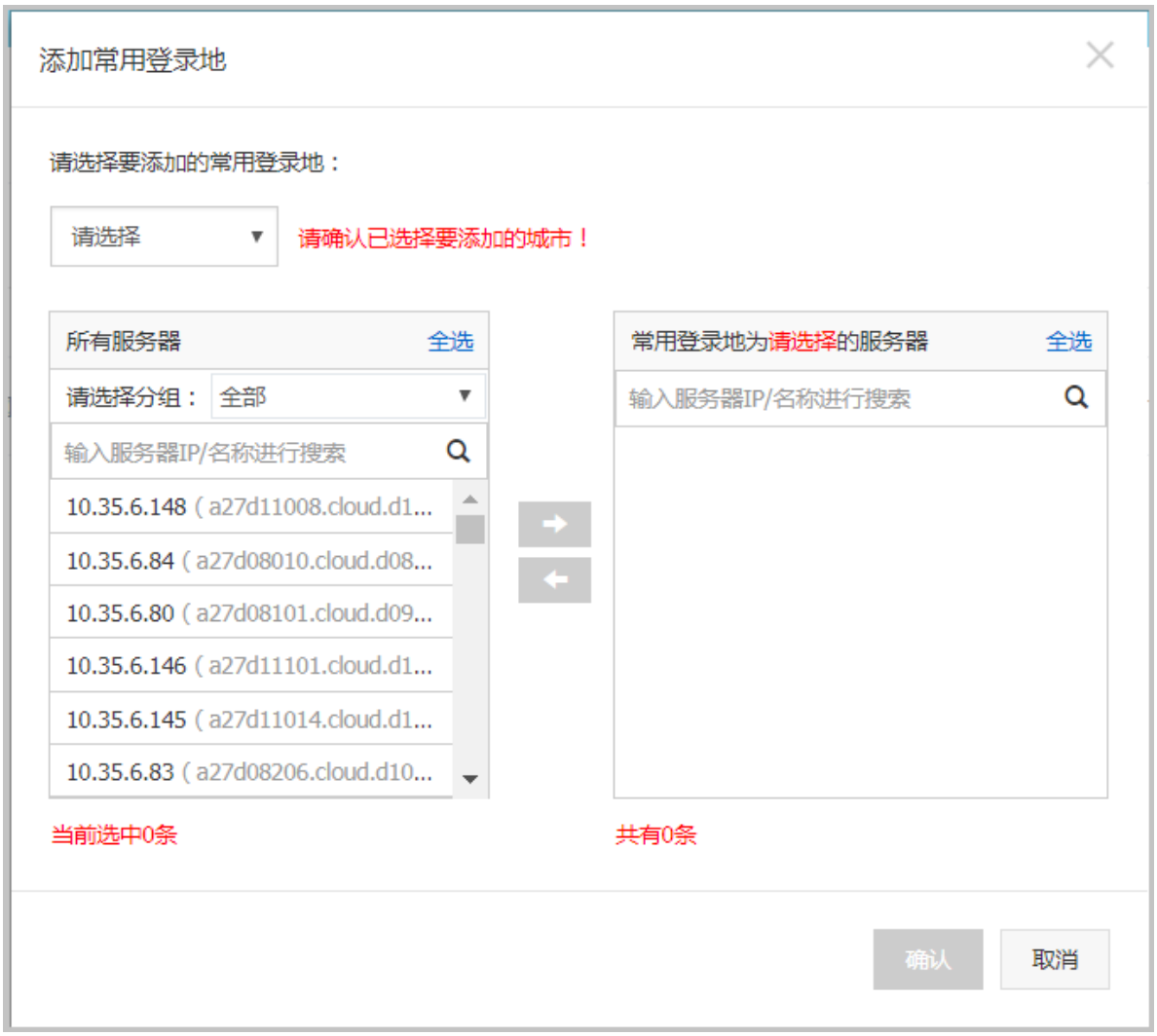
1. 在**服务器安全** > **主机防护**，单击**配置中心**，单击**登录地设置**，进入**登录地设置**页面，如图 *105: 登录地设置页面*所示。

   图 105: 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 *106: 添加白名单对话框*所示。

   图 106: 添加白名单对话框



5.4.2.4.4 配置基线检查策略

操作步骤

1. 在**服务器安全** > **主机防护**，单击**配置中心**，单击**基线检查设置**，进入**基线检查设置**页面，如图 *107:* 基线检查设置页面所示。

图 107: 基线检查设置页面

2. 单击**添加**。
3. 在**安全体检策略**对话框中，设置需要的周期性安全体检策略，单击**确认**，添加安全体检策略，如图 *108:* 安全体检策略对话框所示。

图 108: 安全体检策略对话框

5.4.3 主机入侵检测

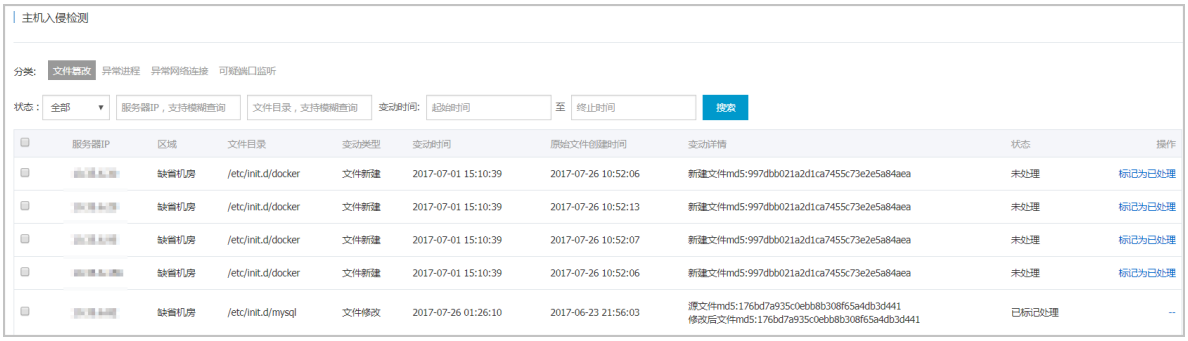
5.4.3.1 查看文件篡改事件记录

操作步骤

1. 在**服务器安全 > 主机入侵检测**页面，单击**文件篡改**。

2. 查看文件篡改事件记录，如图 *109:* 文件篡改事件记录所示。

图 109: 文件篡改事件记录



5.5 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。阿里云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，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。

阿里云的安全审计主要由阿里的 auditlog 核心组件完成。专有云云盾高级版调用 auditlog 的 api 接口获取审计日志数据、审计策略和审计事件，对审计日志和审计事件做分析和以图表方式呈现，有利于管理员直观了解系统面临的风险和威胁。

5.5.1 审计一览

审计一览提供云平台日志趋势、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管理员，便于分析云服务面临的风险趋势。

- 云平台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。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。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。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。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。

在**安全审计** > **审计一览**页面，设置查询时间，单击**查询**，查看审计报表，如图 *110:* 审计一览页面所示。

说明: 缺省情况下查看一周的审计报表。

图 110: 审计一览页面

5.5.2 审计查询

审计查询会记录日志创建时间、日志内容、日志类型、事件类型、风险级别。日志的内容为对应模块的日志调试信息，如需了解日志的具体含义，请联系运维人员咨询相关内容。

审计查询生成的过程为：auditlog 收集系统日志，将日志匹配审计规则，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。您可以根据需要在**安全审计** > **策略设置** > **审计策略**查看默认的审计规则，也可以自己定义审计规则的正则表达式。

在**安全审计** > **审计查询**页面，设置查询条件，查看相关审计日志记录。

5.5.3 原始日志

Auditlog 是云盾的审计模块，auditlog 收集了网络设备、ECS、物理服务器、RDS、OpenAPI 的日志记录，专有云云盾高级版通过调用 API 的方式从 auditlog 中获取日志记录。日志中记录了应用在运行时产生的必要的调试信息，维护人员可以根据这些调试信息定位系统出现的故障。

单击**安全审计** > **原始日志**进入**原始日志**页面，选择审计类型、审计对象，通过输入查询关键字及起始时间来设置查询条件，单击**查询**，查看原始日志记录。

5.5.4 策略设置

5.5.4.1 添加审计策略

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。

Auditlog 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，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. 选择**策略设置** > **审计策略**，选择审计类型及审计对象，可以进行审计策略的查询。
2. 单击**新增**，在**新增规则**对话框中输入相关信息可添加审计策略，如图 *111:* 新增规则对话框所示。

图 111: 新增规则对话框

3. 配置审计规则参数。

   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下文中设置的报警接收人。例如设置了正则表达式：*hi|hello*，并设置了 ECS 日志类型、登录尝试事件、高风险事件，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审计事件，发送一封告警邮件给告警接收人。

5.5.4.2 添加审计类型

操作步骤

1. 在**策略设置** > **类型设置**页面可以查看已经存在的审计类型列表。
2. 单击**新增**，在**新增事件类型**对话框中设置要添加的事件类型。

3. 单击**确定**，完成添加审计类型。

5.5.4.3 设置报警接收人

设置报警接收人的邮箱，在发生审计事件后，会将事件上报到告警人的邮箱。

操作步骤

1. 在**安全审计** > **策略设置** > **告警设置**页面，单击**新增**，弹出**新增报警接收人**对话框，如图 *112: 新增报警接收人对话框*所示。

图 112: 新增报警接收人对话框

2. 在**邮箱**的输入框中，输入报警接收人的邮箱地址，在**风险等级**的下拉框中，选择风险等级。
3. 单击**确定**，添加报警接收人。

5.5.4.4 管理事件日志存档

操作步骤

选择**策略设置** > **存档管理**，可以查看存档列表，如图 *113: 存档管理页面*所示。

图 113: 存档管理页面

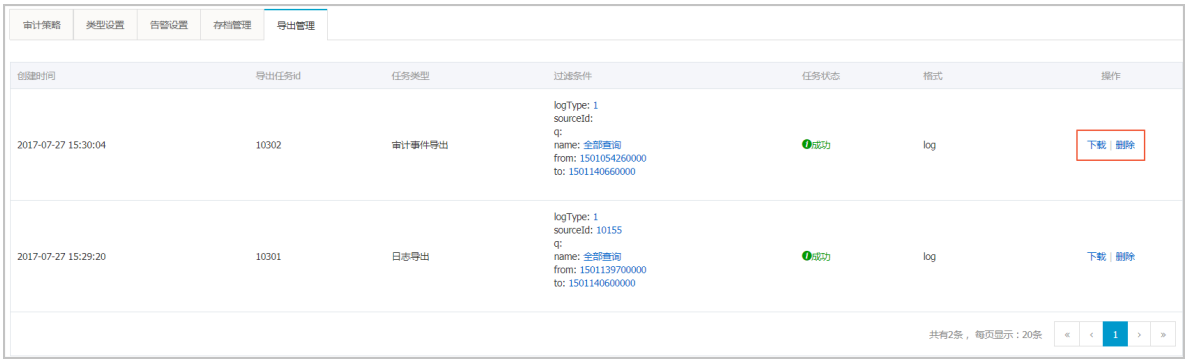
说明: 在输入框输入起始时间可以进行条件筛选。

5.5.4.5 管理导出任务

操作步骤

1. 选择**策略设置** > **导出管理**，可以查看已创建的导出任务，如图 *114: 导出管理页面*所示。

图 114: 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**可下载审计日志文件。
3. 选择导出任务，在操作栏单击**删除**可删除该导出任务。

5.6 系统管理

系统管理模块作为专有云云盾不可或缺的部分，为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：

- 用户管理：用于为专有云云盾的用户配置权限并管理专有云云盾配套的阿里云账号。
- 情报同步：用于配置查看专有云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：用于配置专有云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。

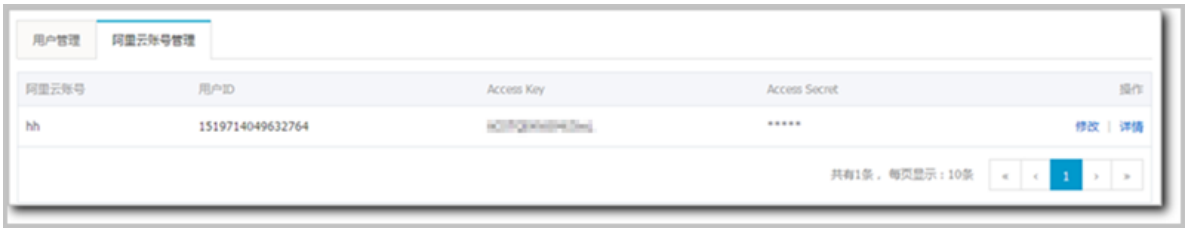
5.6.1 管理阿里云账号

操作步骤

1. 在**系统管理** > **阿里云账号管理**中，可以查看修改系统绑定的阿里云账号信息，如图 *115:* 阿里云账号管理页面所示。

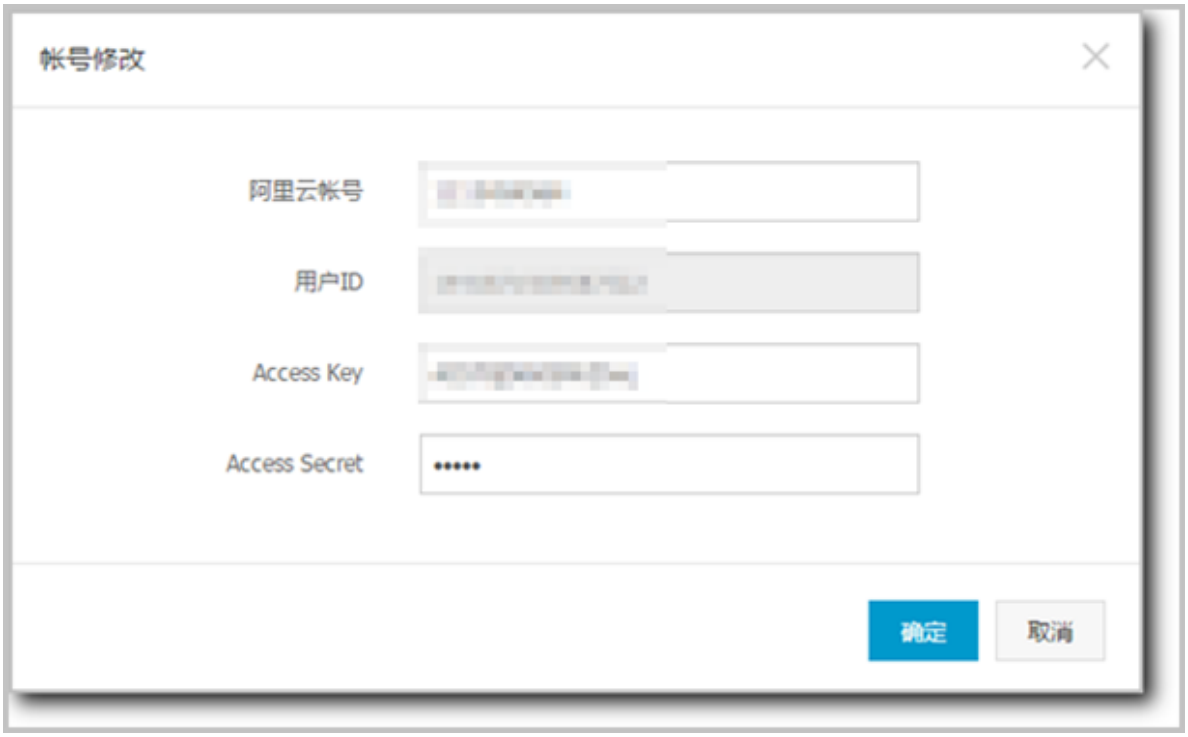
   云盾中的资产均与阿里云账号绑定，请谨慎修改。

   图 115: 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 *116:* 帐号修改对话框所示。

   图 116: 帐号修改对话框



3. 单击**详情**，查看阿里云账号详细信息，包括证书到期时间、安骑士证书数目，如图 *117: 帐号详情*所示。这些信息均是通过配置的 ID、key 信息从阿里云获取。

图 117: 帐号详情

5.6.2 告警设置

告警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，以便管理员了解系统发生的安全事件。

5.6.2.1 设置告警联系人

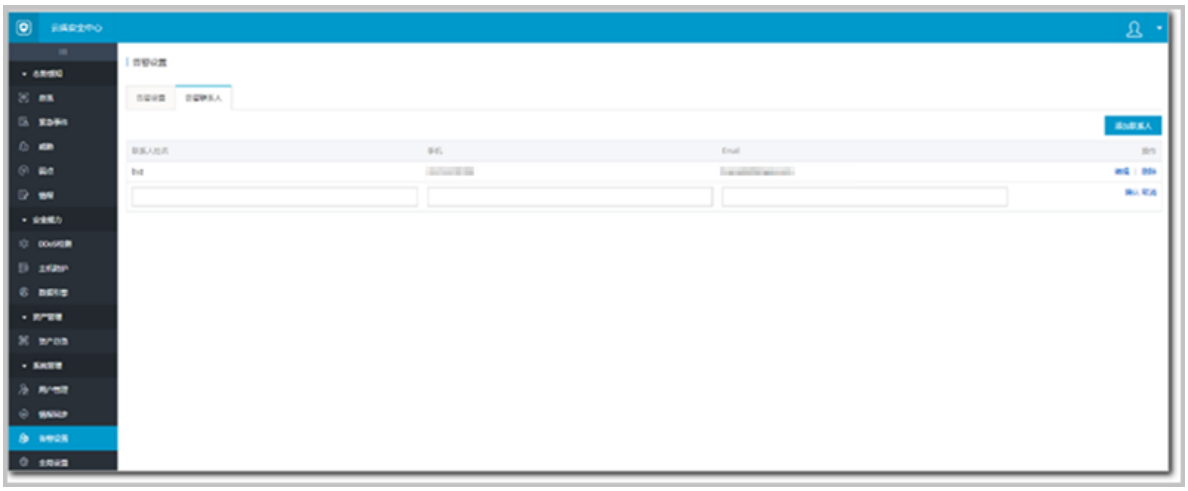
背景信息

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. 在**系统管理** > **告警设置** > **告警联系人**页面，单击**添加联系人**，如图 *118: 告警联系人页面*所示。

图 118: 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页面上的**编辑**和**删除**按钮，进行相关联系人信息的编辑或删除。

5.6.2.2 设置告警信息

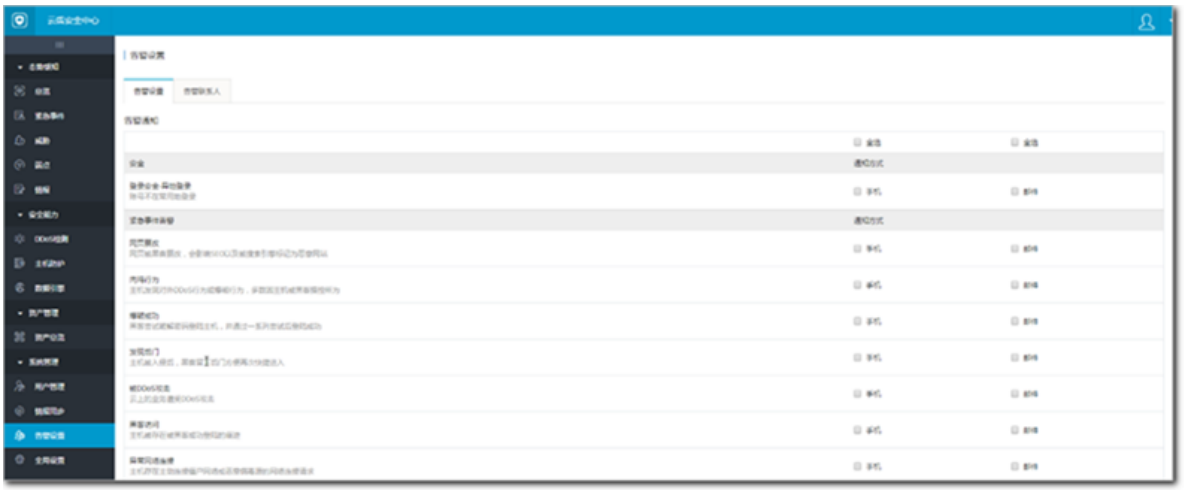
背景信息

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。

操作步骤

在**系统管理** > **告警设置** > **告警设置**页面，选择每个安全事件的通知方式单击**确认**，如图 *119: 告警设置页面*所示。

图 119: 告警设置页面



5.6.3 全局设置

专有云云盾提供全局设置，供管理员对云盾流量采集监控的网段范围以及安骑士上报检测区域进行设置。主要支持查询、添加、修改、删除操作。

流量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。

5.6.3.1 流量采集网段设置

网段设置主要针对流量监控服务进行网段配置，并且支持管理更改监控的网段范围，方便您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。更多信息可以参考流量监控。

网段设置更改后立即对流量监控生效，不需要管理员进行其他操作。

5.6.3.2 添加流量采集网段

操作步骤

1. 在**系统管理** > **全局设置** > **流量采集网段设置**中，单击**添加**，弹出**添加监控网段**对话框，如图 *120: 添加监控网段对话框*所示。

   图 120: 添加监控网段对话框

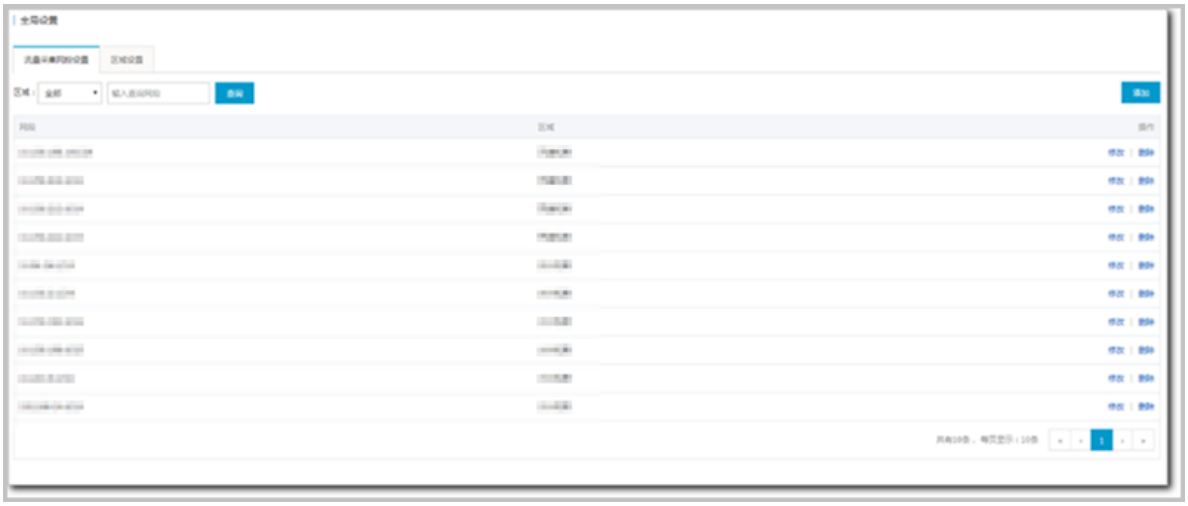
2. 填写网段，要求必须是合法网段，并且不允许重复添加。
3. 选择所属区域。
4. 单击**确定**，完成添加。

5.6.3.3 管理流量采集网段

操作步骤

1. 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 *121:* 全局设置页面所示。

图 121: 全局设置页面



2. 选择需要的网段，执行如下操作：
   - 修改流量采集网段

单击**修改**，弹出**修改网段**对话框（只支持区域修改），修改所属区域后，单击**确定**，完成修改。

- 删除流量采集网段

  单击**删除**，可以删除配置的监控网段。

5.6.3.4 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。

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，具体操作参见资产总览。

5.6.3.5 添加区域网段

操作步骤

1. 在**系统管理** > **全局设置** > **区域设置**中，单击**添加**按钮，弹出**添加网段**对话框，如图 *122:* 添加网段对话框所示。

   图 122: 添加网段对话框

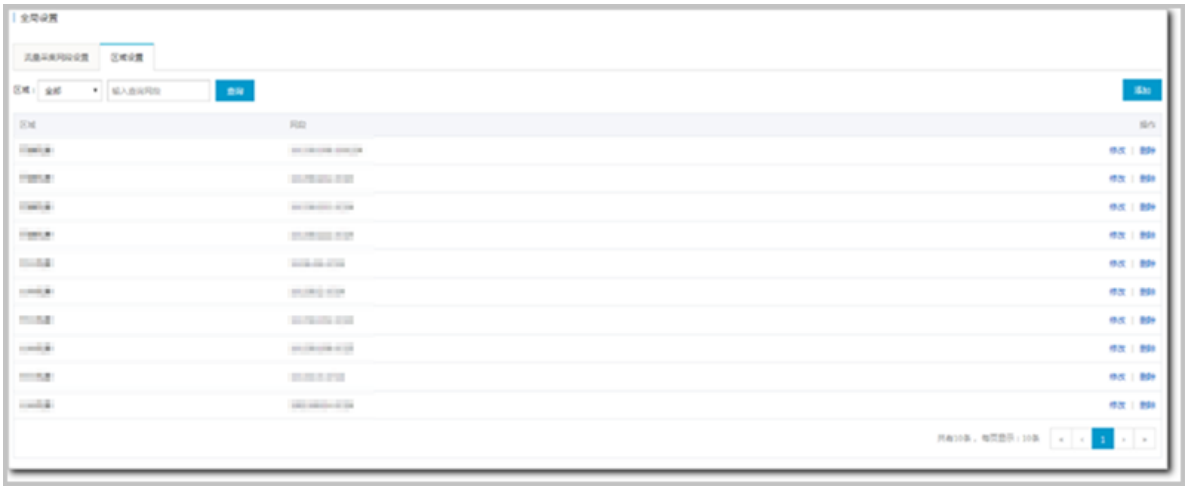
2. 填写网段，要求必须是合法网段，并且不允许重复添加。
3. 选择所属区域。
4. 单击**确定**，完成添加。

5.6.3.6 管理区域网段

操作步骤

1. 选择区域，输入查询网段，单击**查询**，查看区域网段信息，如图 *123:* 区域设置页面所示。

   图 123: 区域设置页面

2. 选择需要的网段，执行如下操作：

   - 修改区域网段

     单击**修改**，弹出修改网段对话框（只支持区域修改），修改所属区域后，单击**确定**，完成修改。

   - 删除区域网段

     单击**删除**，可以删除配置的网段区域。