阿里云
专有云企业版

安全管理员指南（基础版）

产品版本：V3.5.2

文档版本：20180831

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表本文档中的内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止**： 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告**： 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意**： 导出的数据中包含敏感信息，请妥善保存。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明**： 您也可以通过按**Ctrl** + **A**选中全部文件。
>	多级菜单递进。	**设置** > **网络** > **设置网络类型**
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 概述

云盾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。

2 配置要求

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

表 2-1: 配置要求表

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

3 登录和注销

3.1 用户权限说明

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

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

表 3-1: 云盾安全中心默认角色说明

角色名称	角色说明
云安全中心系统管理员	负责云盾安全中心系统管理设置，具备阿里云账号管理、云端同步、告警设置、及全局设置的权限。
云安全中心安全管理员	负责整个专有云平台的安全状态，管理云盾各功能模块的安全策略设置，包括态势感知、云主机安全、物理机安全、资产管理各目录下的所有功能节点权限。
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，包括包括态势感知、云主机安全、物理机安全、资产管理各目录下的所有功能节点权限。同时，部门管理员还可以设置该部门中安全事件告警的联系人及告警方式。
云安全中心审计员	负责整个专有云平台安全审计工作，查看审计事件、原始日志并设置相关审计策略，具备安全审计目录下所有功能节点权限。

3.2 登录云盾安全中心

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

- 登录Apsara Stack控制台，从Apsara Stack控制台页面上跳转到云盾安全中心页面。
  a) 打开Chrome浏览器。
  b) 在地址栏中，输入Apsara Stack控制台的网站地址（例如：http://*Apsara Stack*控制台网站地址），按**Enter**，进入Apsara Stack控制台登录页面。
  c) 在Apsara Stack控制台登录页面，输入已创建的云盾安全中心用户的登录账号、密码及验证码。

d) 单击**登录**。

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

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

图 3-1: 安全中心页面

- 通过云盾安全中心的网站地址，直接登录。

  说明：
  从部署人员处获取相关网站地址信息，通过浏览器直接访问页面。

  a) 打开Chrome浏览器。

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

  c) 输入已创建的云盾安全中心用户的登录账号、密码及验证码。

  d) 单击**登录**。

3.3 退出云盾安全中心

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

4 云盾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、主机安全、安全审计和系统管理，主要功能如下： • **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。 • **云主机安全**：提供云主机的入侵防护，帮助安全管理员保障服务器主机安全。 • **物理机安全**：提供物理机的入侵防护，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。 ▪ 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。

区域	说明
	- 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。

5 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。

5.1 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。

5.1.1 查看网络流量信息

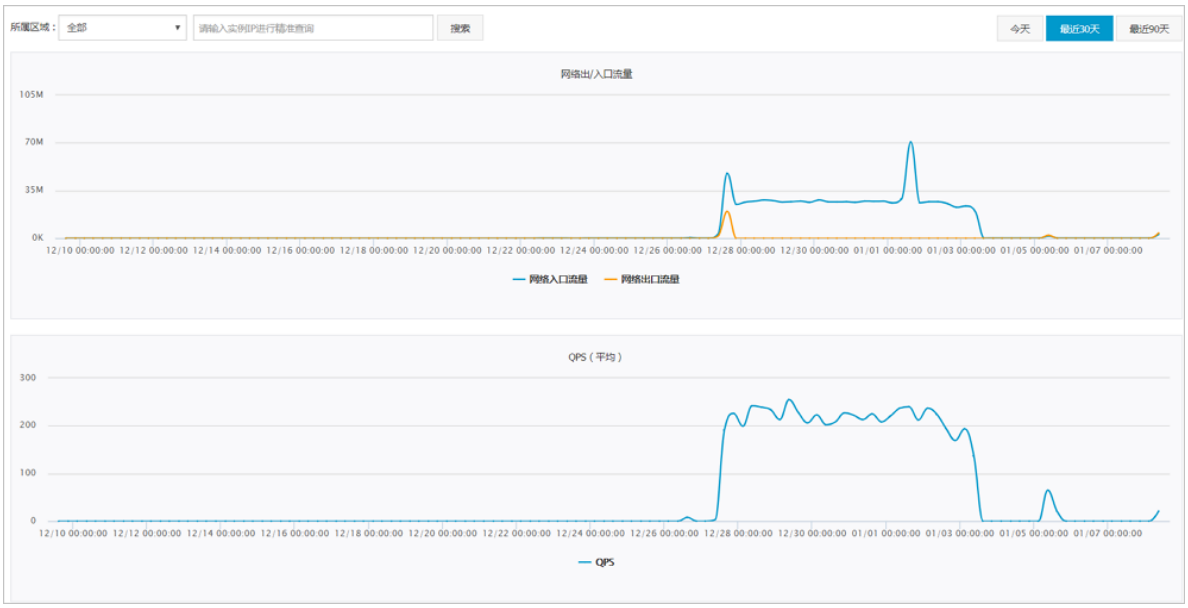
背景信息

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. 登录云盾控制台。
2. 定位到**态势感知** > **总览**，进入**总览**页面，如图 *5-1:* 总览页面所示。

图 5-1: 总览页面



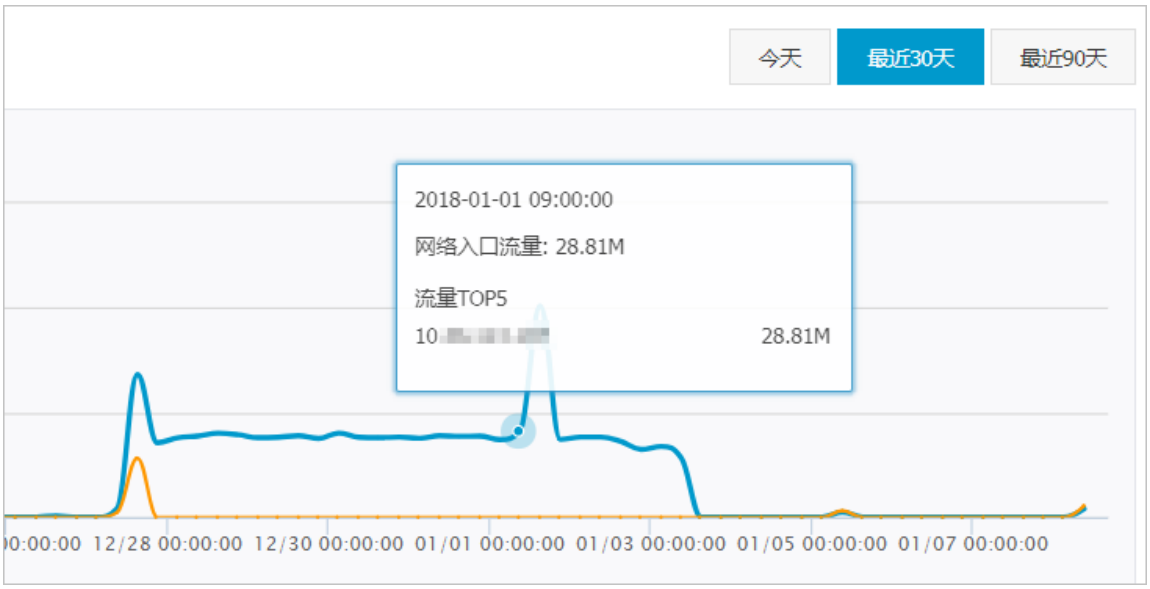
3. 查看不同时期、区域或单个IP的流量情况。

   - 在**总览**页面，单击**今天**、**最近30天**、**最近90天**可以切换查看不同时间段的流量信息。
   - 在**所属区域**中可以选择区域信息，或在搜索框中输入IP，可以分区域、分IP查询流量信息。

4. 查看某时间节点具体流量信息。

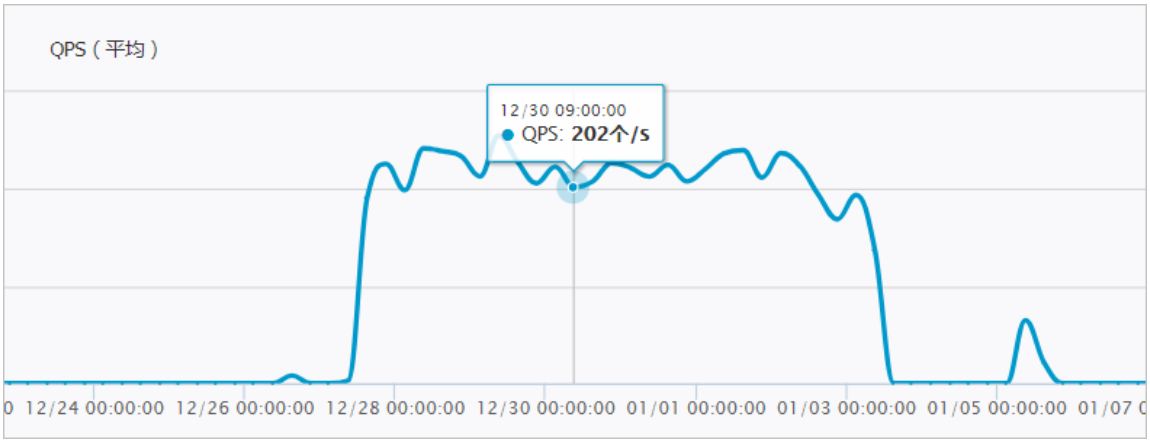
   - 在网络出/入口流量图中，将鼠标停留在流量折线上，可查看该时间点出口或入口流量的详细信息及流量TOP5的IP，如图 *5-2: 查看流量 TOP5 的 IP*所示。

图 5-2: 查看流量 TOP5 的 IP



- 在QPS（平均）图中，将鼠标停留在流量折线上，可查看该时间点的具体QPS信息，如图 *5-3:* 查看*QPS*详细信息所示。

图 5-3: 查看QPS详细信息



5.2 查看威胁分析结果

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

操作步骤

1. 登录云盾控制台。
2. 定位到**态势感知** > **威胁感知**，进入**威胁感知**页面，如图 *5-4:* 威胁感知所示。

图 5-4: 威胁感知

3. 查看最近7日攻击趋势、最近30日攻击分析，了解专有云平台上的主机、应用近期遭受的攻击。
4. 查看TOP5黑客最感兴趣资产IP。

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

   - 选择**类型**，可查看云盾安全中心检测到的指定类型的针对性攻击。
   - 选择已检测到的针对性攻击记录，单击**查看**，可查看该次攻击的详细信息及解决方案。

6 网络安全

6.1 启用网络安全阻断功能

操作步骤

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

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

图 6-1: 阻断开关设置

7 云主机安全

7.1 主机列表

以云主机维度，展示各主机的安全状况信息。

7.1.1 管理主机列表

在主机列表页面，可以查看安骑士已防护的服务器的状态。

背景信息

服务器保护状态分为在线、离线、暂停保护三种。

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

操作步骤

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

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

   单击右上角的  ，设置服务器具体显示哪些信息列。信息主要分为以下几类。

类别	信息
服务器基本信息	• 服务器IP/名称 • 标签 • 操作系统 • 地域
保护状态	保护状态
安全预防	• 漏洞 • 基线

类别	信息
入侵检测	• 异常登录 • 网站后门 • 主机异常
主机指纹	• 进程数 • 端口数 • Root账号

5. 管理服务器。

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

7.1.2 管理分组

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

背景信息

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

操作步骤

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

- 新建子分组。

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

  > **说明**：
  > 最多支持三级子分组。

- 修改子分组。

  单击子分组右侧的修改按钮，输入子分组名称并单击**确认**。

- 删除子分组。

  单击子分组右侧的删除按钮，在弹出的确认框中单击**确认**。

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

4. 给服务器进行分组。

   a) 在右侧的服务器列表中，勾选服务器。

   b) 单击**更换分组**。

   c) 在弹出窗口的下拉菜单中选择分组。

   d) 单击**确认**。

5. 切换分组排序。

   单击**分组排序**，可以把优先级高的分组移动到上面。

7.2 入侵检测

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

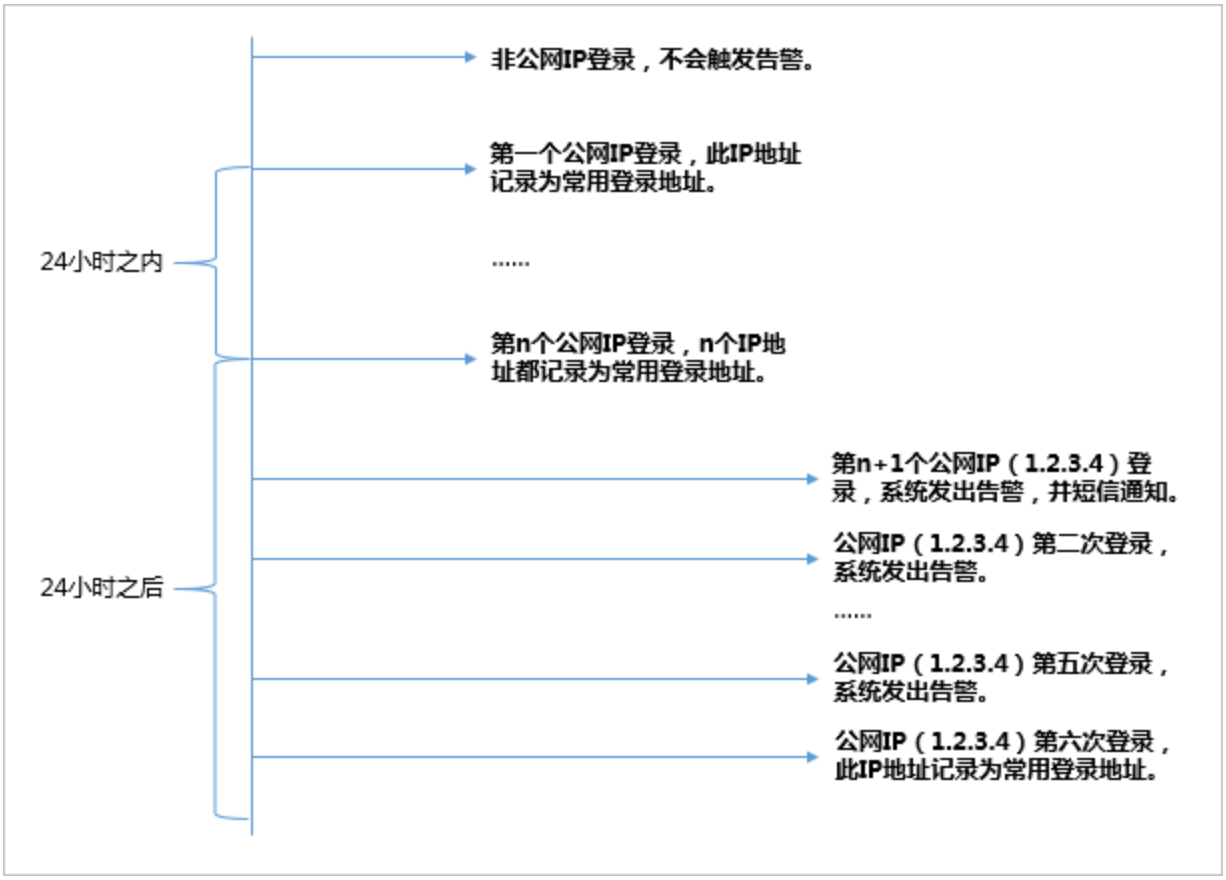
7.2.1 异常登录

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

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

异地登录告警策略如图 *7-1:* 异地登录策略所示。

图 7-1: 异地登录策略



说明：

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

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

7.2.1.1 查看异常登录

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

操作步骤

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

   通过搜索和筛选功能，快速定位到具体异常登录信息，如图 7-2: 查找异常登录信息所示。

   图 7-2: 查找异常登录信息

4. 处理异常登录信息。

   选择异常登录信息，判断是否存在误报。

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

7.2.1.2 设置登录安全策略

设置登录安全策略，包括常用登录地、合法登录IP、合法登录时间和合法账号。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **入侵检测** > **异常登录**。
3. 在**异常登录**页面右上角，单击**登录安全设置**。
4. 设置常用登录地。

   a) 单击**添加**。

b) 在下拉菜单中选择常用登录地。

c) 设置常用登录地对哪些服务器生效。

- **全部资源**中可以选择具体服务器。
- **分组资产**中可以根据分组信息选择服务器。

d) 单击**确定**，完成新增规则操作。

e) 选择具体规则，单击**编辑**修改规则。

f) 选择具体规则，单击**删除**删除规则。

5. 设置合法登录IP。
6. 设置合法登录时间。
7. 设置合法账号。

7.2.2 网站后门

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

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

安骑士网站后门检测采用动态检测及静态检测两种方式：

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

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

7.2.2.1 管理网站后门

查看和隔离网站后门文件。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **入侵检测** > **网站后门**。
3. 选择资产，查看已发现的网站后门文件记录，如图 *7-3:* 选择资产所示。

图 7-3: 选择资产

4. 处理网站后门文件。

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

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

7.2.3 主机异常

查看在服务器上检测到的异常进程行为、和恶意进程等。

7.2.3.1 管理主机异常

查看服务器上的主机异常告警，并修复相应问题。

操作步骤

1. 登录云盾控制台。
2. 定位到**云主机安全** > **入侵检测** > **主机异常**。
3. 选择资产，查看已发现的主机异常事件。
4. 根据主机异常事件影响情况，选择相应的处理方式，如表 *7-1:* 处理主机异常事件所示。

表 7-1: 处理主机异常事件

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

操作	说明
查看	查看本次告警详细信息。

7.3 设置

本章主要说明安全配置、告警配置、安装和卸载安骑士Agent插件。

7.3.1 管理安全配置

操作步骤

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

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

7.3.2 安装安骑士Agent插件

在Windows服务器或Linux服务器上手动安装安骑士Agent插件。

前提条件

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

背景信息

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

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

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

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

操作步骤

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

   进入安骑士Agent插件安装页面，如图 *7-4: Agent安装*所示。

   图 7-4: Agent安装

3. 根据您的服务器操作系统，获取并安装安骑士Agent插件。

   - **Windows系统**

     1. 在左侧区域，单击**点击下载**，下载安装文件到本地计算机。
     2. 将安装文件上传至您的Windows服务器。例如，您可以通过FTP工具，将安装文件上传到服务器。
     3. 在Windows服务器上，以管理员权限运行安装文件，完成安装。

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

- **Linux系统**

  1. 在右侧区域，根据您的实际情况，选择**阿里云服务器**或**非阿里云服务器**。
  2. 根据您的操作系统类型，选择32位或64位的安装命令，单击**复制**。
  3. 以管理员身份登录您的Linux服务器。
  4. 在Linux服务器上执行安装命令，下载和安装安骑士Agent插件。

4. 查看服务器在线情况。

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

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

7.3.3 卸载安骑士Agent插件

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

背景信息

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

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

操作步骤

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

8 物理机安全

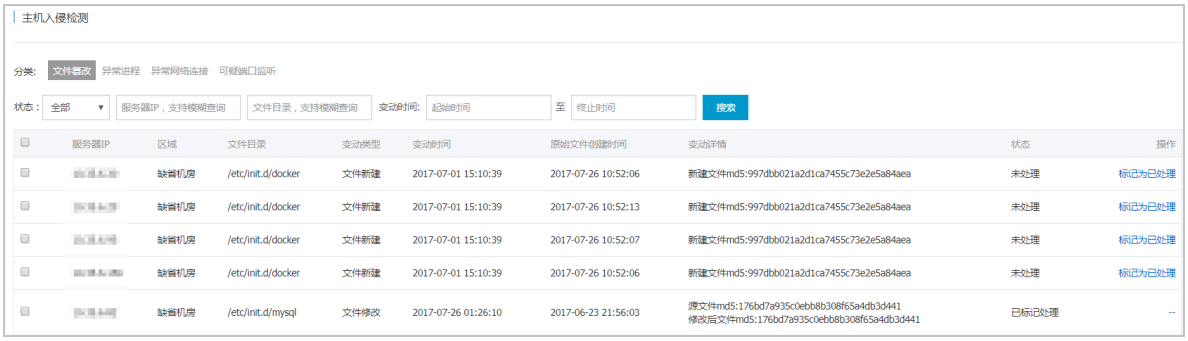
8.1 查看并处理文件篡改事件记录

监控主机系统特定目录中文件的完整性，及时发现篡改行为并进行告警。

操作步骤

1. 登录云盾控制台。
2. 定位到**物理机安全** > **物理机防护**页面，选择**文件篡改**。
3. 查看文件篡改事件记录，如图 *8-1: 文件篡改事件记录*所示。

图 8-1: 文件篡改事件记录



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

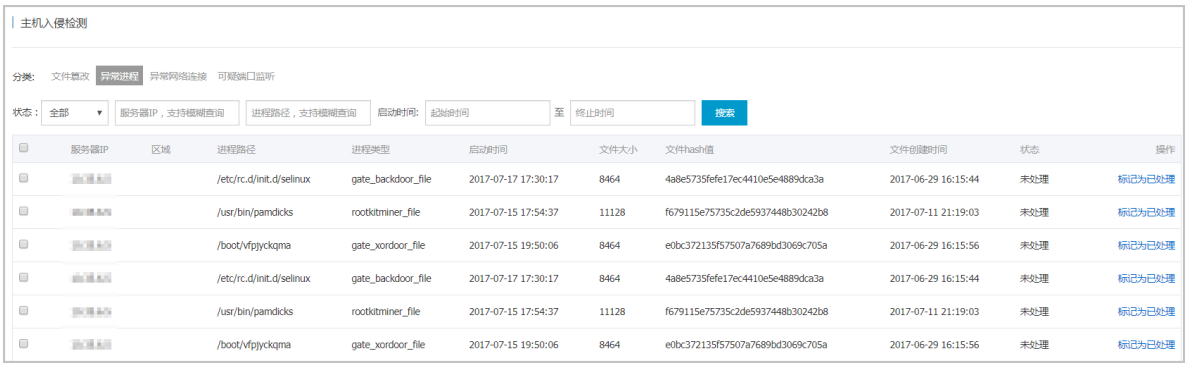
8.2 查看并处理异常进程记录

及时发现异常进程启动，并进行告警。

操作步骤

1. 登录云盾控制台。
2. 定位到**物理机安全** > **物理机防护**页面，选择**异常进程**。
3. 查看异常进程记录，如图 *8-2: 异常进程记录*所示。

图 8-2: 异常进程记录



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

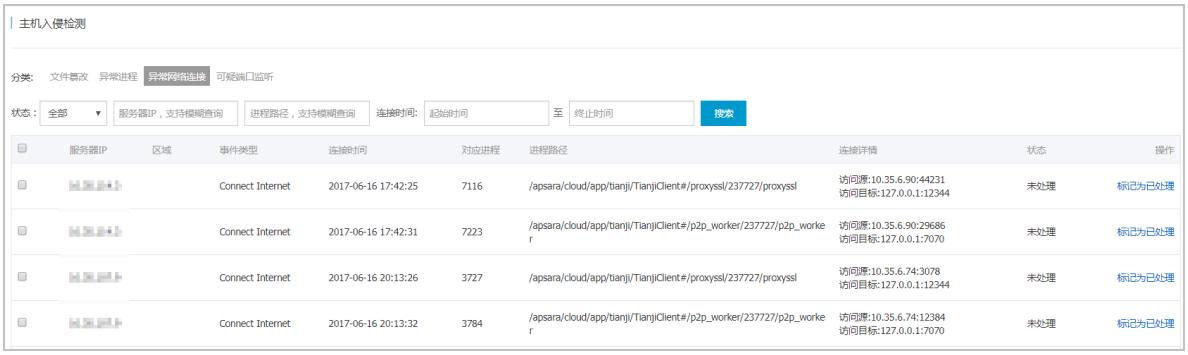
8.3 查看并处理异常网络连接记录

及时发现主动外连公网的网络连接，并进行告警。

操作步骤

1. 登录云盾控制台。
2. 定位到**物理机安全 > 物理机防护**页面，选择**异常网络连接**。
3. 查看异常网络连接记录，如图 *8-3:* 异常网络连接所示。

图 8-3: 异常网络连接



4. 进一步排查该异常网络连接。

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

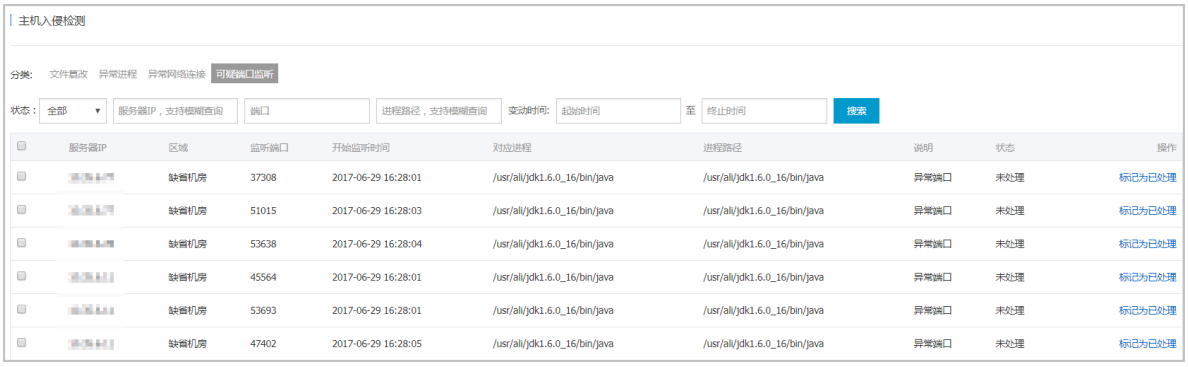
8.4 查看并处理异常端口监听记录

及时发现异常的端口监听，并进行告警。

操作步骤

1. 登录云盾控制台。
2. 定位到**物理机安全** > **物理机防护**页面，选择**可疑端口监听**。
3. 查看异常端口监听记录，如图 *8-4: 异常端口监听记录*所示。

图 8-4: 异常端口监听记录



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

9 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。

9.1 查看审计一览

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

背景信息

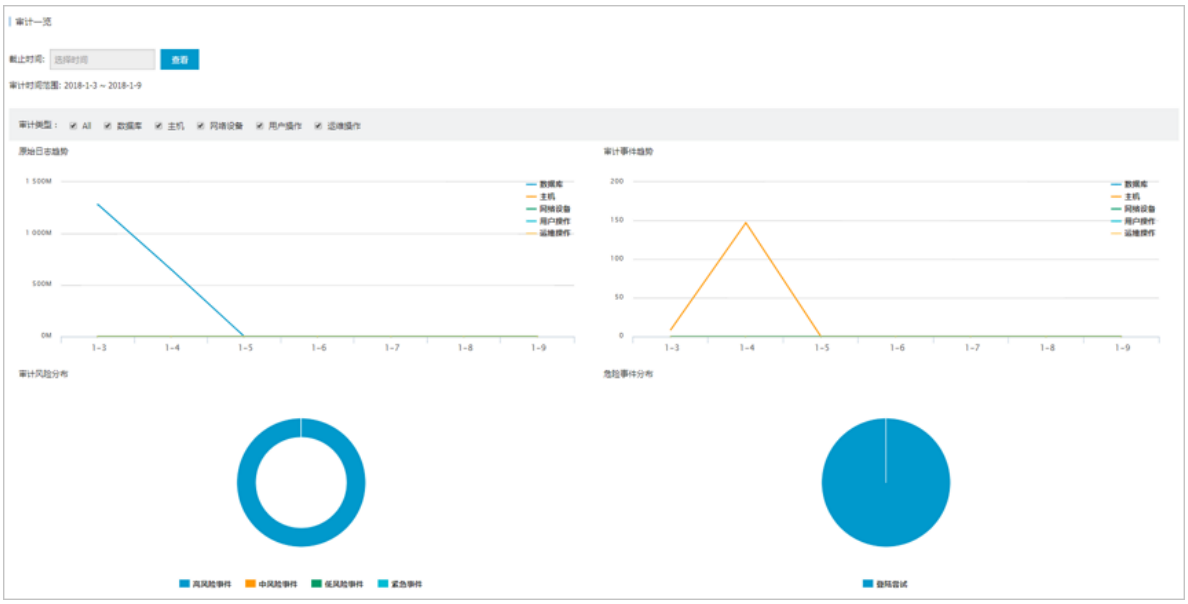
- **原始日志趋势**的数据是物理服务器、网络设备、RDS、ECS、OpenAPI一周内产生的日志个数。通过云平台日志趋势，安全管理员可以了解系统产生的日志数量是否正常。
- **审计事件趋势**的数据是物理服务器、网络设备、RDS、ECS、OpenAPI一周内产生的审计事件个数。通过审计事件趋势，安全管理员可以了解系统产生的审计事件数量是否正常。
- **审计风险分布**的数据是一周内高风险、中风险、低风险事件的个数。通过审计风险分布，安全管理员可以了解系统产生的审计事件级别是否正常。
- **危险事件分布**的数据是一周内不同事件类型占总事件的比例。通过危险事件分布，安全管理员可以了解什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

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

操作步骤

1. 登录云盾控制台。
2. 定位到**安全审计** > **审计一览**，进入**审计一览**页面，如图 *9-1:* 审计一览页面所示。

图 9-1: 审计一览页面



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

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

4. 勾选**审计类型**，可以选择是否显示该类型的审计日志信息。

9.2 查询审计事件

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

背景信息

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

操作步骤

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

说明：

单击**高级查询**，可设置更详细的审计事件过滤条件。

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

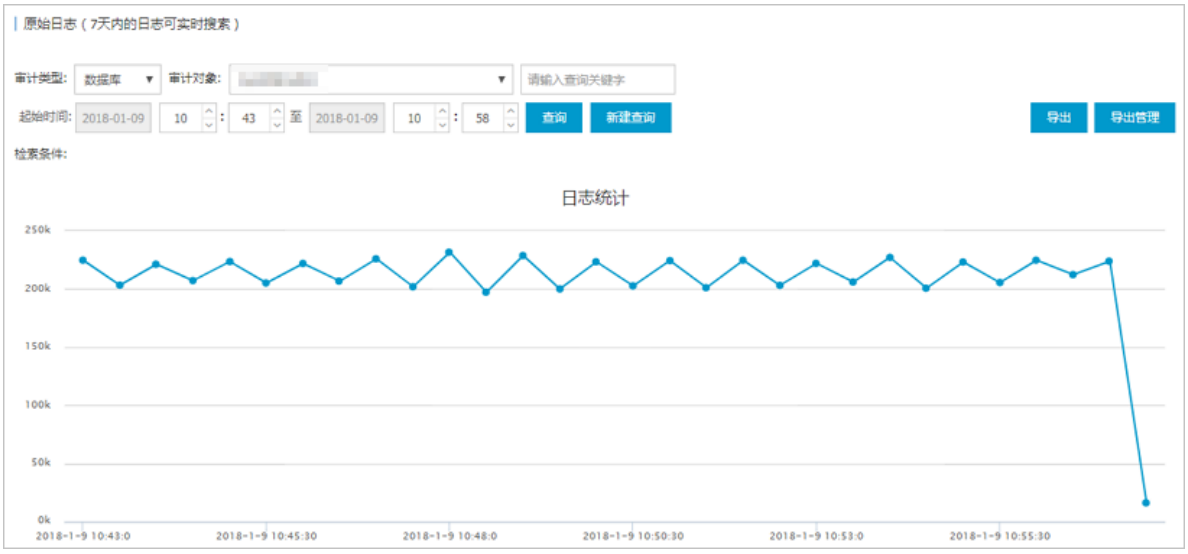
9.3 查看原始日志

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

操作步骤

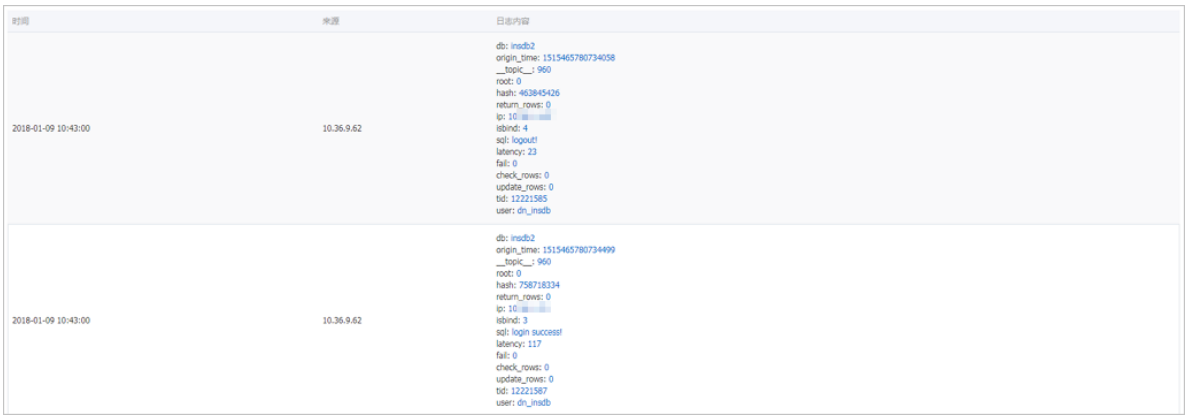
1. 登录云盾控制台。
2. 定位到**安全审计** > **原始日志**，进入**原始日志**页面，如图 *9-2:* 原始日志页面所示。

图 9-2: 原始日志页面



3. 选择**审计类型**、**审计对象**，设置查询时间，单击**查询**，查看该时间段内指定审计对象的原始日志信息，如图 *9-3:* 原始日志信息所示。

图 9-3: 原始日志信息



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

9.4 策略设置

9.4.1 管理审计策略

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

背景信息

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

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

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

操作步骤

1. 登录云盾控制台。
2. 定位到**安全审计** > **策略设置**，选择**审计策略**页签，如图 *9-4:* 审计策略页面所示。

图 9-4: 审计策略页面

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

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

4. 管理审计策略。

   - 单击**新增**，在**新增规则**对话框中输入相关信息并单击**添加**，可添加审计策略，如图 *9-5:* 新增规则对话框所示。

图 9-5: 新增规则对话框

说明：

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

- 单击**删除**，可删除该审计策略。

说明：

系统默认的审计策略无法删除。

- 单击**启用**或**禁用**，可设置该审计策略是否生效。

说明：

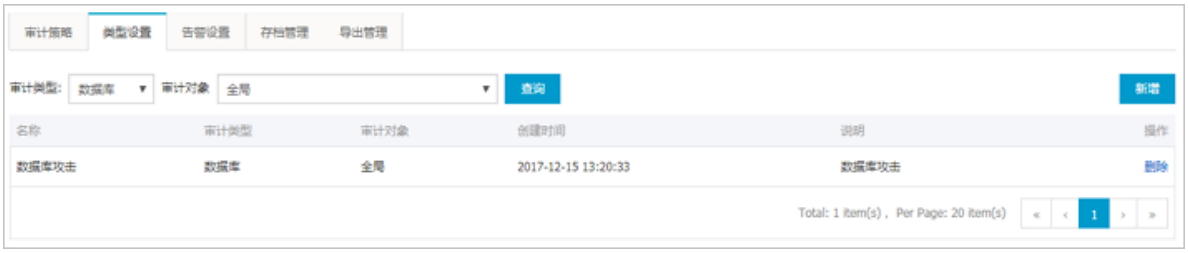
新增的审计策略默认为启用状态。

9.4.2 管理操作类型

操作步骤

1. 登录云盾控制台。
2. 定位到**安全审计 > 策略设置**，选择**类型设置**页签，如图 *9-6: 操作类型设置页面*所示。

图 9-6: 操作类型设置页面



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

说明：

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

4. 管理操作类型。
   - 单击**新增**，在**新增事件类型**对话框中输入相关信息即可添加操作类型，如图 *9-7: 新增事件类型*所示。

图 9-7: 新增事件类型

- 单击**删除**，可删除该操作类型。

> **说明**：
> 系统默认的操作类型无法删除。

9.4.3 设置告警接收人

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

操作步骤

1. 登录云盾控制台。
2. 定位到**安全审计** > **策略设置**，选择 **告警设置**页签，如图 *9-8:* 告警设置页面所示。

图 9-8: 告警设置页面

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

4. 设置告警接收人。

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

     图 9-9: 新增报警接收人对话框

   - 单击**删除**，可删除该告警接收人。

9.4.4 管理事件日志存档

操作步骤

1. 登录云盾控制台。
2. 定位到**安全审计** > **策略设置**，选择**存档管理**页签，如图 *9-10:* 存档管理页面所示。

   图 9-10: 存档管理页面

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

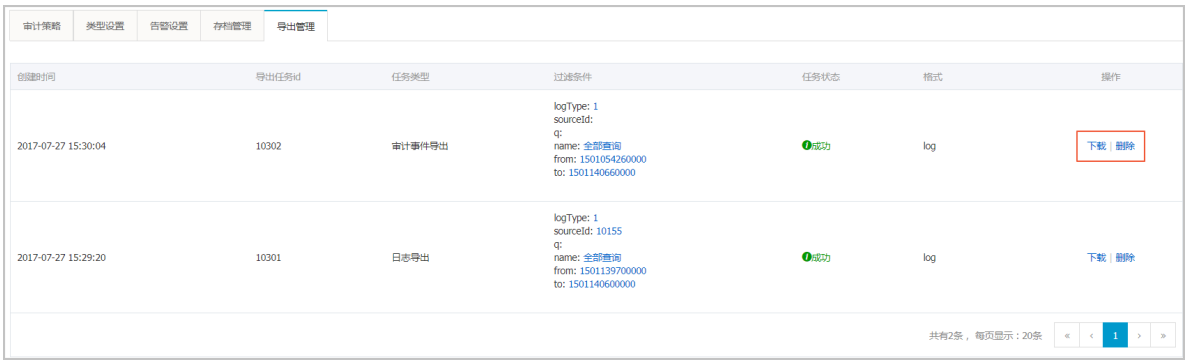
9.4.5 管理导出任务

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

操作步骤

1. 登录云盾控制台。
2. 定位到**安全审计** > **策略设置**，选择**导出管理**页签。
3. 查看已创建的导出任务，如图 *9-11: 导出管理页面*所示。

图 9-11: 导出管理页面



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

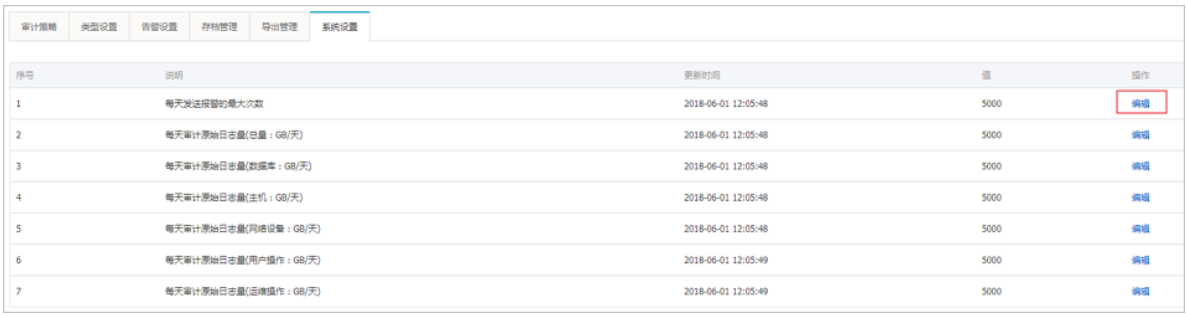
9.4.6 修改安全审计系统配置

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

操作步骤

1. 登录云盾控制台。
2. 定位到**安全审计** > **策略设置**，选择**系统设置**页签。
3. 定位到想要修改的系统参数，单击**编辑**如图 *9-12: 系统设置*所示。

图 9-12: 系统设置



4. 填写对应的参数值，单击**确认**。

10 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。
- **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。

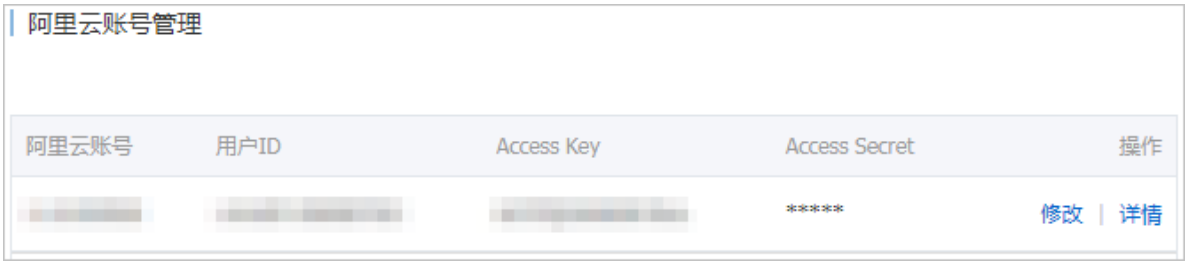
10.1 管理阿里云账号

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **阿里云账号管理**页面，可以查看、修改系统绑定的阿里云账号信息，如图 *10-1:* 阿里云账号管理页面所示。

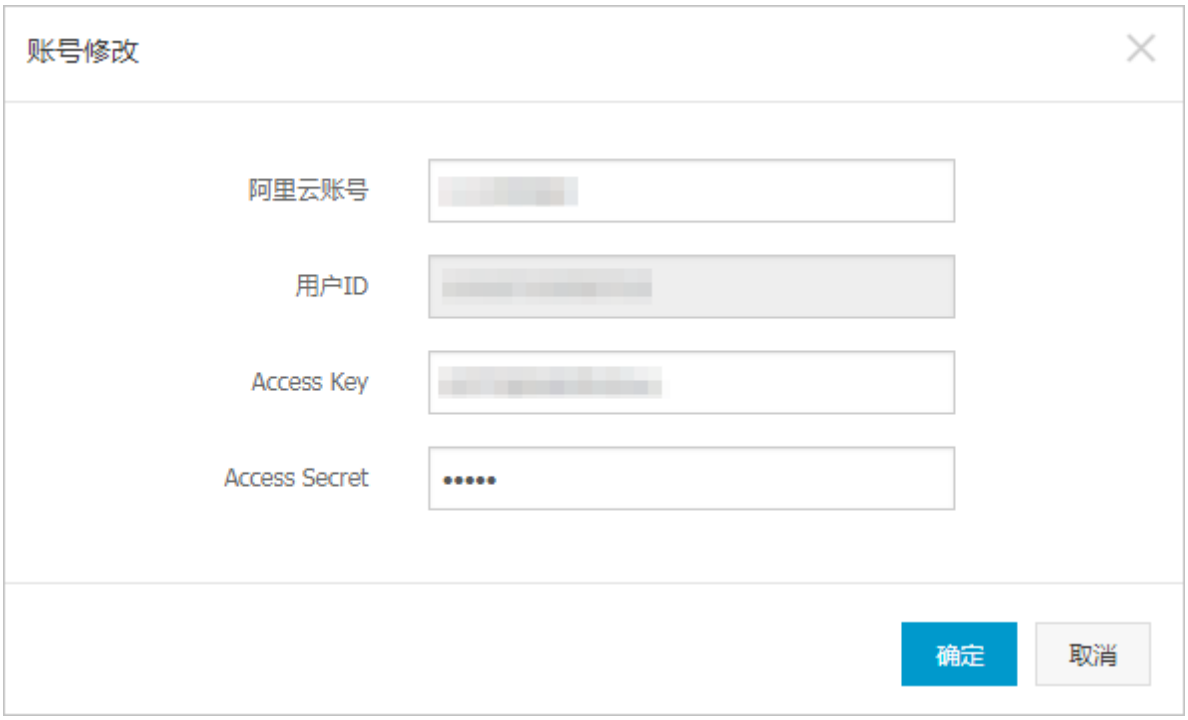
   云盾中的资产均与阿里云账号绑定，请谨慎修改。

   图 10-1: 阿里云账号管理页面

3. 单击**修改**，弹出修改对话框，信息修改后单击**确定**，完成修改，如图 *10-2:* 账号修改对话框所示。

图 10-2: 账号修改对话框



4. 单击**详情**，查看阿里云账号详细信息，包括许可到期时间、安骑士许可数目，如图 *10-3:* 账号详情所示。这些信息均是通过配置的用户ID、Access Key信息获取。

图 10-3: 账号详情

10.2 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。

10.2.1 设置告警联系人

告警联系人是告警消息的接收人，告警消息的发送方式有手机短信和邮件。当监控数据满足报警规则时会发送告警信息给报警联系人。

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **告警设置** > **告警联系人**页面，如图 *10-4:* 告警联系人页面所示。

图 10-4: 告警联系人页面

3. 单击**添加联系人**。
4. 填写联系人信息，单击**确认**，添加告警联系人。

   添加后的告警联系人可以通过单击**编辑**或**删除**，对该联系人信息进行编辑或删除。

10.2.2 设置告警信息

告警设置可以对各种安全事件进行告警，告警方式包括手机和邮件。

操作步骤

1. 登录云盾控制台。
2. 定位**系统管理** > **告警设置** > **告警设置**页面。
3. 在**告警通知**区域，为各种安全事件选择通知方式，如图 *10-5:* 告警设置页面所示。

图 10-5: 告警设置页面

4. 单击**确认**，完成设置。

10.3 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。

10.3.1 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。

10.3.1.1 添加流量采集网段

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **全局设置** > **流量采集网段设置**页面。
3. 单击**添加**，弹出**添加监控网段**对话框，如图 *10-6:* 添加监控网段对话框所示。

图 10-6: 添加监控网段对话框

4. 设置监控网段参数。
   - 填写网段。

     说明：
     所填写的网段必须是合法网段，并且不允许重复添加。

- 选择所属区域。

5. 单击**确定**，完成添加。

10.3.1.2 管理流量采集网段

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **全局设置** > **流量采集网段设置**页面。
3. 选择区域，输入查询网段，单击**查询**，查看流量采集网段信息，如图 *10-7:* 流量采集网段所示。

图 10-7: 流量采集网段

4. 管理流量采集网段。
   - 单击**修改**，在**修改网段**对话框中修改所属区域，单击**确定**，修改流量采集网段所属区域。
   - 单击**删除**，可删除该流量采集网段。

10.3.2 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。

10.3.2.1 添加区域网段

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **全局设置** > **区域设置**页面。
3. 单击**添加**，弹出**添加网段**对话框，如图 *10-8: 添加网段对话框*所示。

   图 10-8: 添加网段对话框

4. 设置网段参数。
   - 填写网段。

     说明：
     所填写的网段必须是合法网段，并且不允许重复添加。
   - 选择所属区域。
5. 单击**确定**，完成添加。

10.3.2.2 管理区域网段

操作步骤

1. 登录云盾控制台。
2. 定位到**系统管理** > **全局设置** > **区域设置**页面。
3. 选择区域，输入查询网段，单击**查询**，查看区域网段信息，如图 *10-9: 区域设置页面*所示。

图 10-9: 区域设置页面

4. 管理区域网段。

   - 单击**修改**，在修改网段对话框中修改所属区域，单击**确定**，修改区域网段信息。
   - 单击**删除**，删除该区域网段信息。