阿里云
安骑士

用户指南

文档版本：20190321

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。
*## *	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 Agent 插件

1.1 安装Agent

安装安骑士Agent 后才能对您的主机提供防护。

您可以登录 云盾服务器安全#安骑士#管理控制台 - 资产管理 页面，查看您所有服务器的安骑士 Agent 在线状态。

若您的服务器安骑士 Agent 显示离线状态，请按照以下方式手动下载并安装安骑士 Agent 插件。安装前请确认您安装安骑士服务器的环境：

- 阿里云服务器，直接安装即可。
- 对于通过专线连接、内网通信的非阿里云服务器，需要修改服务器的DNS配置，指定以下安骑士服务端DNS解析地址：

  ```
  106.11.248.209/106.11.248.51 jsrv.aegis.aliyun.com
  ```

  ```
  106.11.248.90/106.11.250.224 update.aegis.aliyun.com
  ```

安装后如果出现离线情况请参考*Agent* 离线排查。

> 说明:
> 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。建议您在安装安骑士 Agent 插件前确认您的服务器上是否存在这类安全软件，如果存在建议您先关闭、或卸载该安全软件之后，再安装安骑士 Agent 插件。

操作步骤

1. 登录 **云盾服务器安全#安骑士#管理控制台 - 资产管理**，单击设置。

2. 单击安装/卸载进入安装安骑士Agent页面。

3. 根据您的服务器操作系统选择安装步骤，获取最新版本安骑士 Agent 插件。

   - Windows 系统

     a. 在安装安骑士Agent页面，单击点击下载下载最新版本安骑士Agent插件安装文件到本地计算机。

     b. 将安装文件上传至您的Windows服务器，例如通过FTP工具将安装文件上传到服务器。

     c. 在您的Windows服务器上以管理员权限运行安骑士Agent插件安装程序。

     d. 非阿里云服务器输入安装验证Key。

     您可在云盾安装安骑士页面找到您的安装验证Key。

> **说明:**
> 安装验证Key将用于关联您的阿里云账号，在云盾安骑士管理控制台登录您的阿里云账号即可保护您的服务器安全。

> **说明:**

每个安装验证KEY有效期为1小时，超过该时间将无法正确安装安骑士Agent插件。安装插件前请及时刷新安装验证KEY。

a. 完成安装。

b. 单击立即查看打开资产列表，查看资产在线状态。

- Linux 系统

a. 根据您的实际情况，在安装安骑士 Agent 页面选择 阿里云服务器 或 非阿里云服务器。

b. 以管理员身份登录您的 Linux 服务器。

c. 根据您的服务器，选择32位或64位的安装命令并复制至您的 Linux 服务器上。

d. 执行安装命令即可完成安骑士Agent插件的下载及安装。

说明:
该安装命令包含从阿里云站点下载最新的安骑士 Agent 插件，如您使用的是非阿里云服务器请确认您的服务器已连接公网。

4. 安骑士 Agent 插件安装完成约五分钟后，您即可在云盾服务器安全（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。

验证 Agent 安装

在您成功安装安骑士 Agent 后，建议您参考以下步骤进行验证：

1. 检查您的服务器上安骑士 Agent 的 AliYunDun 和 AliYunDunUpdate 这两个进程是否正常运行。
2. 在您的服务器上，执行以下 telnet 命令检查您的服务器是否能正常连通安骑士服务器。

说明:

确保以下 jsrv 和 update 两类服务器域名各至少有一个服务器能连通。

- `telnet jsrv.aegis.aliyun.com 80`
- `telnet jsrv2.aegis.aliyun.com 80`
- `telnet jsrv3.aegis.aliyun.com 80`
- `telnet update.aegis.aliyun.com 80`
- `telnet update2.aegis.aliyun.com 80`
- `telnet update3.aegis.aliyun.com 80`

如果安骑士 Agent 安装验证失败，请参考*Agent* 离线排查。

注意事项

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。

安骑士 Agent 插件文件目录

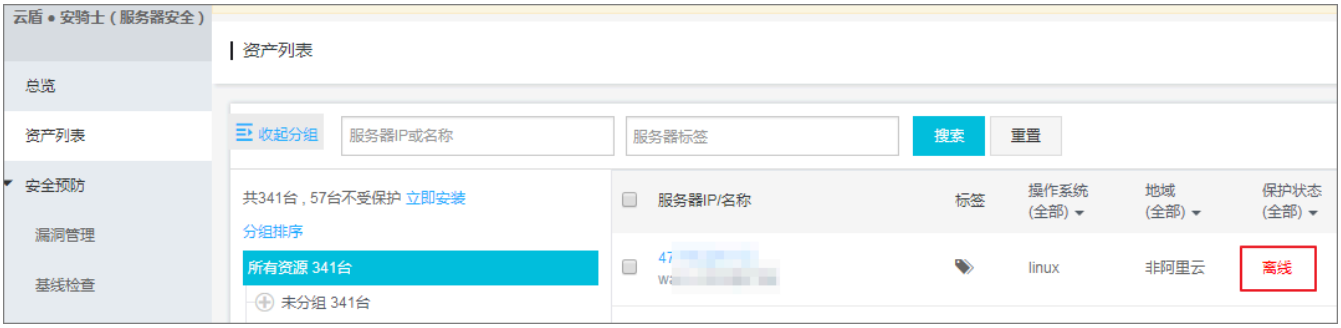
- Windows： C:\Program Files (x86)\Alibaba\Aegis
- Linux： /usr/local/aegis

1.2 Agent 离线排查

本文档介绍了安骑士 Agent 处于离线状态时如何进行问题排查和处理。

问题描述

安骑士控制台资产列表页面中Agent处于离线状态。



问题排查

建议按照以下步骤对Agent离线的问题进行排查：

1. 登录您的服务器查看安骑士 Agent 相关进程是否正常运行。如果Agent 相关进程没有正常运行，建议重启您的服务器，或者重新安装安骑士Agent。

   - Windows系统：在任务管理器中查看进程AliYunDun和AliYunDunUpdate是否正常运行。

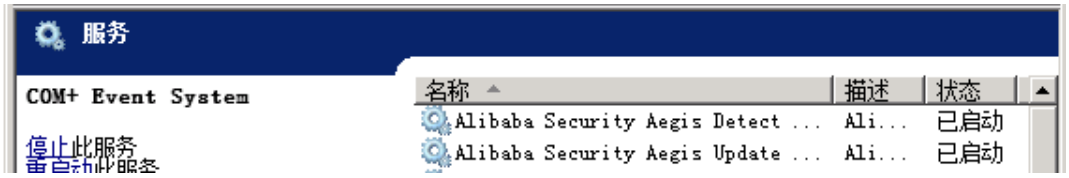
映像名称	用户名	CPU	内存(专用工作集)
AliYunDun.exe *32	SYSTEM	00	6,648 K
AliYunDunUpdate.exe *32	SYSTEM	00	1,000 K

   - Linux系统：执行命令`ps aux | grep AliYunDun`命令查看进程AliYunDun和AliYunDunUpdate是否正常运行。

   ```
   /usr/local/aegis/aegis_update/AliYunDunUpdate
   /usr/local/aegis/aegis_client/aegis_10_19/AliYunDun
   ```

2. 如果首次安装安骑士 Agent 后显示安骑士状态不在线，可参考以下方式重新启动安骑士 Agent：

   - Windows系统：在服务项中定位到以下两个进程服务项并右键单击重新启动即可。

   - Linux系统：执行命令`killall AliYunDun && killall AliYunDunUpdate && /usr/local/aegis/aegis_client/aegis_10_xx/AliYunDun`重启。

   > **说明：**
   > 将命令中的`xx`替换为该目录下的最大数字。

> **说明：**
> 购买ECS实例时勾选安全加固选项即可自动安装安骑士Agent。

3. 检查您的服务器网络连接是否正常。

   · 服务器有公网 IP （如经典网络、EIP、非阿里云主机）

     - Windows 系统： 在命令行中执行`ping jsrv.aegis.aliyun.com -l 1000`。
     - Linux 系统： 执行命令`ping jsrv.aegis.aliyun.com -s 1000`。

   · 服务器无公网 IP （只覆盖阿里云ECS，如金融云、VPC 专有网络）

     - Windows 系统： 在命令行中执行`ping jsrv3.aegis.aliyun.com -l 1000`。
     - Linux 系统：

       ■ VPC专有网络：在命令行中执行`ping jsrv2.aegis.aliyun.com -s 1000`命令。

       ■ 国内经典网络：在命令行中执行`ping jsrv4.aegis.aliyun.com -s 1000`命令。

       ■ 国外经典网络：在命令行中执行`ping jsrv5.aegis.aliyun.com -s 1000`命令。

说明:

连通以上任意一个网络即视为服务器网络连接正常。

4. 如果连接不通，请根据以下方法检查您的服务器网络连接状况：

   - 确认您的服务器的 DNS 服务正常运行。如果 DNS 服务无法运行，请您重启您的服务器或检查服务器 DNS 服务是否有问题。
   - 检查服务器是否设置了防火墙 ACL 规则、或阿里云安全组规则。如果有，请确认已将服务器安全（安骑士）的服务端 IP 加入防火墙白名单（出、入方向均需添加）以允许网络访问。

     将下列 IP 段的 80 端口添加至白名单，最后一个 IP 段需要同时添加 80 和 443 端口至白名单：

     - 10.84.135.0/24 Port: 80 443
     - 106.11.248.0/24 Port: 80 443
     - 106.11.250.0/24 Port: 80 443
     - 100.100.0.0/16 Port: 80 443
   - 检查您的服务器公网带宽是否为零。

     如果您的服务器公网带宽为零，请参考以下步骤进行解决：

     a. 在您服务器的 hosts 文件添加以下域名解析记录：

        - 国内经典网络：`100.100.110.61 jsrv.aegis.aliyun.com`、`100.100.45.131 jsrv.aegis.aliyun.com`100.100.110.62 update.aegis.aliyun.com 和 `100.100.45.29 update.aegis.aliyun.com`
        - 国外经典网络：`100.100.103.52 jsrv.aegis.aliyun.com`、`100.100.30.54 jsrv.aegis.aliyun.com`、`100.100.30.55 update.aegis.aliyun.com`和 `100.100.103.54 update.aegis.aliyun.com`

     b. 修改 hosts 文件后，执行`ping jsrv.aegis.aliyun.com`命令。

        如果返回的结果不是`100.100.25.3`，请重启服务器或检查服务器 DNS 服务是否有问题。

     c. 如果仍然无法解析到正确的 IP，您可以尝试修改安骑士安装目录下 conf 目录中的 network_config 配置文件，将t_srv_domain对应值修改为`100.100.30.25`、将h_srv_domain对应值修改为`100.100.167.125`。修改完成后，重启安骑士 Agent 进程。

        说明：
        修改前请务必备份 network_config 配置文件。

        说明：

此方法只适用于公网带宽为0且安骑士 Agent 离线的服务器。

d. 如果 Ping 命令执行解析成功，再次执行 Telnet 命令`telnet 140.205.140.205 80`查看是否能连通解析出的域名 IP 的 80 端口。如果无法连通，请确认防火墙是否存在相关限制。

5. 检查您的服务器 CPU、内存是否长期维持较高占用率（如 95%、100%），此情况可能导致安骑士 Agent 进程无法正常工作。
6. 检查服务器是否已安装第三方的防病毒产品（如安全狗、云锁等）。部分第三方防病毒软件可能会禁止安骑士Agent 插件访问网络。如果有，请暂时关闭该产品并重新安装安骑士 Agent。

1.3 卸载Agent

本文档介绍了如果您决定不再使用安骑士的所有功能时，如何卸载Agent的相关操作和说明。

背景信息

卸载安骑士Agent前您需了解以下信息：

- 卸载Agent后再次安装Agent时，历史的告警数据、隔离文件无法关联您的资产，请谨慎卸载。
- 安骑士 Agent 卸载后，控制台中该主机资产的保护状态将变更为离线状态，您可以使用解绑功能删除处于离线状态的主机资产的记录。
- 通过本文档步骤来卸载指定主机安骑士，请务必确保当前机器安骑士处于在线状态，否则无法接收到卸载指令。如果卸载后重新安装安骑士，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）。

控制台卸载Agent操作步骤

1. 登录 云盾服务器安全#安骑士#管理控制台，单击左侧导航栏设置 > 安装/卸载 。
2. 单击页面右上角的 卸载安骑士。

3. 在弹出的卸载提示对话框中，选择您决定卸载安骑士 Agent 的服务器，并单击确认卸载。

系统将自动卸载您选择的服务器上的安骑士 Agent。

手动卸载Agent操作步骤

请提交工单获取手动卸载Agent的命令和步骤。

2 控制台总览

安骑士在控制台总览页面中显示待处理的告警事件、弱点发现趋势、入侵事件趋势以及不受保护的ECS资产信息，帮助您实时了解资产的安全状态和存在的隐患。

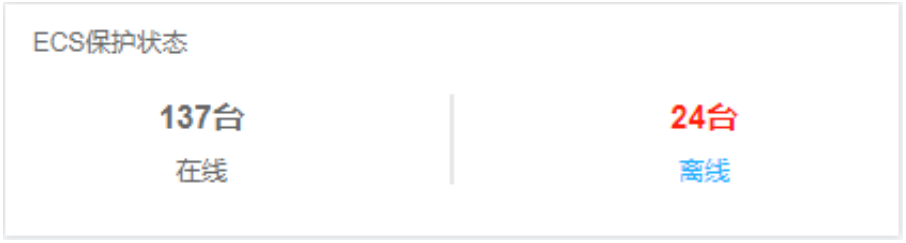
待处理的告警事件数量

控制台总览页面显示待处理的告警事件数量及其紧急程度、检测到的告警事件总数、已处理事件的数量。

待处理告警事件包含以下类型：

- 漏洞待处理
- 基线配置不当
- 异常登录
- 网站后门
- 主机异常

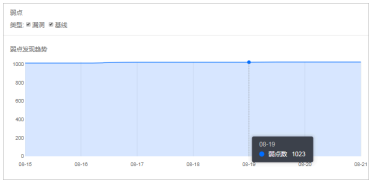
ECS保护状态



显示受安骑士保护（在线）和未受安骑士保护（离线）的资产数量。

如果您有ECS资产显示离线状态，单击离线打开安骑士安装/卸载页面安装Agent（安骑士插件），对您的资产进行保护。

弱点发现趋势



显示资产7天或30天内弱点数量走向（弱点数量从每日凌晨开始统计，无固定统计时间）。

设置弱点类型显示以下弱点发现趋势：

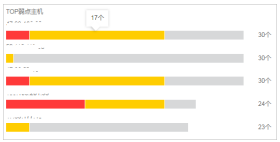
- 漏洞
- 基线

- 漏洞和基线

单击弱点右侧的7天/30天按钮，可选择显示7天内或30天内的弱点趋势图。

> 说明:
> 不支持同时取消勾选漏洞和基线。

TOP弱点主机



显示弱点严重等级前五名的主机信息和弱点数量。

主机IP地址下方的颜色条表示主机事件的严重程度：

- 红色：高危事件
- 黄色：中危事件
- 灰色：低危事件

事件类型

显示资产7天或30天内入侵事件走向（入侵事件数量从每日凌晨开始统计，无固定统计时间）。

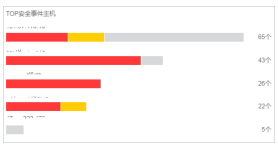
设置事件类型在总览页面显示以下入侵事件趋势：

- 异常登录
- 网站后门
- 主机异常

单击事件右侧的7天/30天按钮，可选择显示7天内或30天内的入侵事件趋势图。

> 说明:
> 不支持同时取消勾选异常登陆、网站后门和主机异常。

TOP安全事件主机



显示入侵事件严重等级前五名的主机信息和入侵事件数量。

主机IP地址下方的颜色条表示弱点的严重程度：

- 红色：高危弱点
- 黄色：中危弱点
- 灰色：低危弱点

最近重要弱点和保护事件

显示最近的、未处理的严重程度前五名的弱点和事件名称、以及主机的详细信息。

单击弱点和事件名称跳转到控制台主机异常界面查看事件详情和进行相应的处理。

通过控制台主机异常界面处理状态查看未处理/已处理的事件。

3 资产列表

在安骑士管理控制台的资产列表页面，您可以查看安骑士已防护的服务器的状态。为了方便对特定服务器资产进行安全管控，您可以对资产进行分组，通过资产分组的维度查看安全事件。

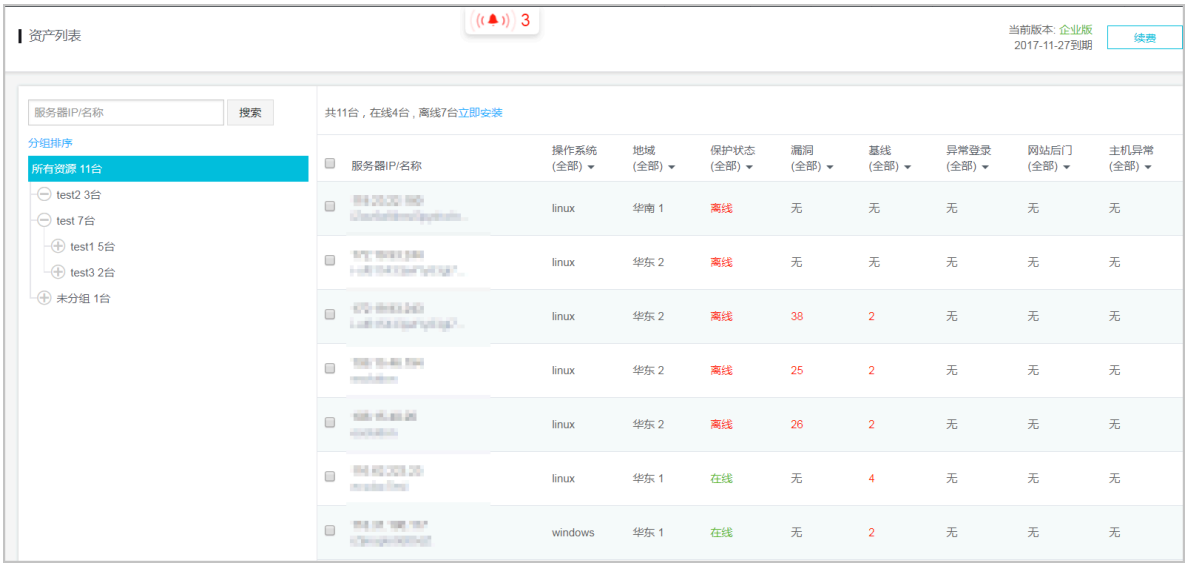
操作步骤

1. 登录 云盾服务器安全#安骑士#管理控制台。
2. 单击资产列表，查看安骑士已防护的服务器的保护状态。

   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。具体离线原因及排查方法，请参考Agent 离线排查。
   - 暂停防护：勾选处于在线状态的服务器，单击更多操作 > 暂停保护可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。

   > 说明:
   > 如您使用的是按量付费的计费方式，处于暂停保护状态的服务器仍会计算安全点。



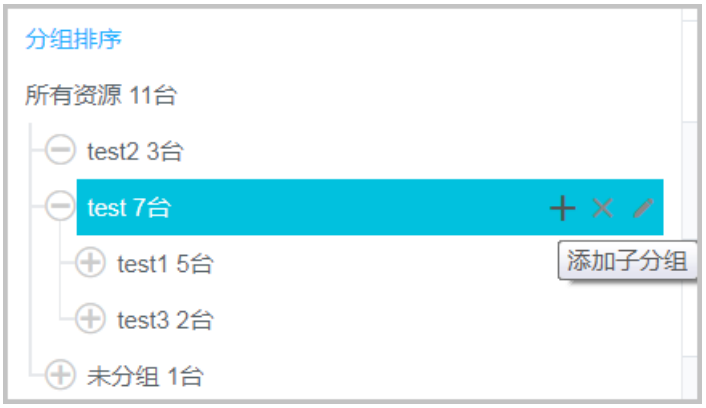
3. 对您的服务器资产进行分组。

   > 说明:

未进行资产分组时，您所有的服务器资产都在未分组中。或者，当您删除某个分组时，该分组中的资产也将默认移入未分组中。

- 单击所有资源右侧的+可以创建资产分组。

- 您也可以单击已创建的资产分组右侧的+创建子分组，或者对该资产分组进行重命名及删除。



说明:

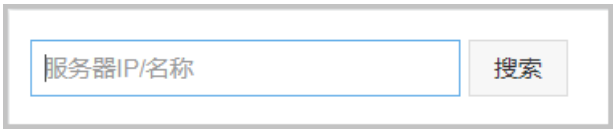
目前，最多可支持三级资产子分组。

4. 勾选服务器资产，单击更换分组，可将选定的服务器资产放至指定的资产分组。

说明:

服务器资产与子分组不能归属在同一级资产分组。例如，资产分组A下已有子分组B，则您无法将服务器资产C放至资产分组A中。

5. 单击分组排序，您可对已创建的资产分组进行排序，以便更好地对您的服务器资产进行管理。
6. 如果您想查看某台服务器的安全状态，您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资产的详细信息和安全信息。



4 安全预防

4.1 基线检查

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

安骑士企业版支持基线检查功能，可检查的风险类型详见基线检查项目列表。

检测周期：默认每天00:00-06:00点进行一次全面自动检查。您可以在安全设置页面设置检测周期和检测执行的时间。

说明:

基础版用户需要升级到服务器安全（安骑士）企业版才能使用此功能。

说明:

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

基线检查项目列表

检测项	系统范围
Windows 启动项检测（Windows 的注册表项 *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit* 中的键值是否包含可疑的可执	

检测项	检测内容
Windows系统配置检测（Windows的注册表*HKEY_LOCAL_MACHINE**SYSTEM**CurrentControlSet**Control**LSA**RestrictAnonymous*中的键值，查看该键值控制是否允许远程	

检测项	检测策略
Windows检测（Windows服务器中以下账号相关的安全策略：	· 账号密码长度最小值 · 密码复杂度（数字、大小写字母、特殊字符

检测项	
SSH弱口令检测	Linux基线检测器中以下SSH登录安全策略配置： · 登录端口是否为默认22端口 · root账号是否允许直接登录 · 是

检测项	
登录Linux密码破解	检测Linux操作系统服务器的登录账号的密码是否为常见弱口令，及SSH登录的密码是否常见弱口令。

检测项	
检测SQLServer弱口令	检测服务器中SQLServer登录账号的密码是否为常见弱口令。

检测项	
Windows系统登录账号的密码是否为常见弱口令，及RDP登录的密码是否为常见弱口令。	检测Windows系统服务器检测系统登录账号的密码是否为常见弱口令，及RDP登录的密码是否为常见弱口令。

检测项	检测FTP服务器是否开启匿名登录。

检测项	检测服务器的MySQL服务的登录账户是否为常见弱口令。

检测项	检测服务器中PostgreSQL数据库登录账号的密码是否为常见弱口令。

检测项	检测服务描述
统中可疑的隐藏账号、及克隆账号。	

检测项 检测策略

Linux系统服务器中的以下账户密码策略：

- 账号密码最大使用期限
- 密码修改最小间隔时间
- 密码最小长度

检测项	检测服务器检测码为空的账号。
Linux检测	Linux系统服务检测中新增账号的完整性。

检测项	风险描述	处理建议
Redis监听配置在0.0.0.0容易被外部攻击者入侵，并利用该弱点在内网横向移动渗透其他服务器，建议您		

检测项	
Linux基线	检测Linux基线。
Tomcat7基线	检测Tomcat7基线。

检测项	
基于CIS基线检测	Linux centos7

查看基线检查详情和修复建议

操作步骤

1. 登录云盾服务器安全#安骑士#管理控制台。

2. 单击左侧导航栏基线检查打开基线检查页面，查看安骑士检测到的您服务器上存在的配置风险项。

您可在基线检查页面进行以下操作：

- 单击某个风险项，进入该基线风险项的详情页面，查看该风险项的检测说明、影响的资产信息和基线检查风险项修复建议，并进行相应的处理。
- 风险修复后，您可以单击验证，一键验证该风险是否已修复成功。如果您未进行手动验证，安骑士会在风险修复成功后 72 小时内执行自动验证。

> 说明：
> 您也可单击忽略，忽略该风险，安骑士将不再对此服务器上的该风险项进行上报和告警。

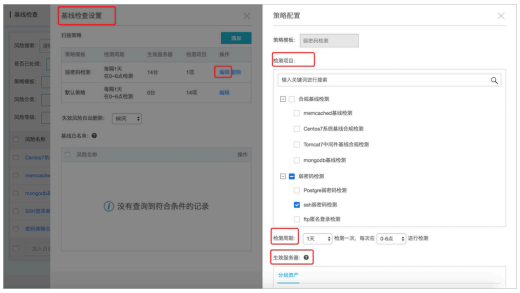
设置基线检查项

您可以在安骑士管理控制台的安全设置页面根据您的实际业务情况设置基线检测项，检测周期、检测风险等级。

操作步骤

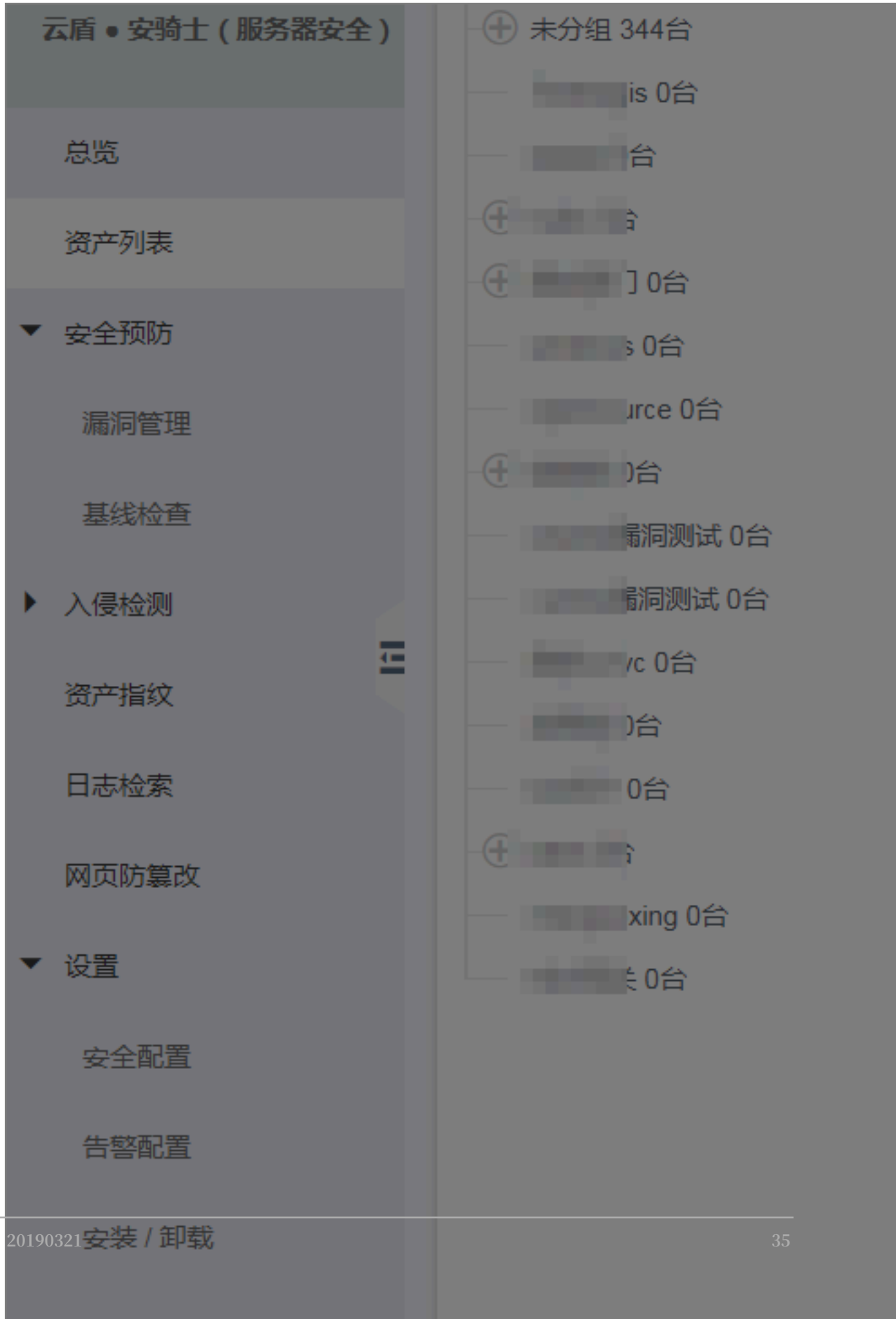
1. 登录云盾服务器安全#安骑士#管理控制台。
2. 在左侧导航栏单击基线检查打开基线检查页面。
3. 单击右上角基线检查设置。

4. 新建或者编辑默认策略：可选择检测项目、检测周期、对应需要检测的服务器。



基线检查策略设置完成后，可跳转到资产列表页面，执行一键安全检查快速检测一遍，无需等待周期检

测。



基线检查白名单

如果您需要对某些基线检查项目彻底忽略，可以将此检测项添加到基线检查白名单。添加成功后，安骑士将不再对基线检查白名单中的检测项目所发现的风险进行上报并告警。

加入白名单或忽略操作支持填写备注，以便后续查看。

操作步骤

1. 登录云盾服务器安全#安骑士#管理控制台。
2. 在基线检查列表中勾选单个项目并单击左下角的加入白名单，或单击某个项目进入基线 检查详情页面，并选择加入白名单。

3. 在加入白名单对话框中对该加白操作进行备注并单击确定完成基线加入白名单设置。

说明:

将基线风险项加入白名单后，该风险记录将从基线检查风险列表中删除，并且后续不再对该风险项进行告警。如需取消该风险项白名单设置，需在基线检查设置页面进行操作。

导出基线检查风险列表

单击基线检查页面右上角的导出按钮，可将excel格式的基线检查风险列表下载到本地。

5 入侵检测

5.1 异常登录

安骑士异常登录功能检测您服务器上的登录行为，对于在非常用登录地的登录行为进行告警；企业版中可允许客户设置合法登录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。

在云盾服务器安全（安骑士）管理控制台中的异常登录界面，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。

异常登录功能原理

安骑士 Agent 通过定时收集您服务器上的登录日志并上传到云端，在云端进行分析和匹配。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。

当安骑士首次应用于您的服务器上时，由于服务器未设置常用登录地，这段期间内的登录行为不会触发告警；当从某个公网IP第一次成功登录服务器后，会将该IP地址的位置记为常用登录地，从该时间点往后顺延24小时内的所有公网登录地也会记为常用登录地；当超过24小时后，所有不在上述常用登录地的登录行为均视为异地登录进行告警。当某个IP被判定为异地登录行为，只会有第一次登录行为进行短信告警。如果该IP成功登录6次或6次以上，安骑士默认将此IP的地点记录为常用登录地。

注意：异地登录只针对公网IP。

告警策略： 安骑士会对某个异地IP的第一次登录行为短信告警。如果持续登录则只在控制台告警，直到该IP地址登录满6次会被自动记录为常用登录地。

如果您的安骑士的版本为企业版，您可以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。

操作步骤

1. 登录 服务器安全#安骑士#管理控制台。

2. 点击 事件 > 异常登录，查看异常登录告警事件。

3. 在异常登录页面右上角选择 登录安全设置，可以针对服务器自主添加常用登录地。

4. 在登录安全设置页面针对服务器自主设置常用登录地、合法登录IP、合法登录时间、合法登录账号。

您也可根据安骑士检测到的异常登录事件信息，在您的服务器上直接查看对应的登录日志记录：

- Linux系统：可在该文件目录下查看相关登录日志`/var/log/secure`。
- Windows系统：在 控制面板 > 管理工具 > 事件查看器 中，查看 Windows日志 > 安全 目录中相关的登录审核日志。

5.2 暴力破解

安骑士具备出色的防暴力破解能力，可以有效对暴力破解行为进行阻断，并将暴力破解行为进行记录。云盾服务器安全（安骑士）管理控制台中的暴力破解拦截页面展示您的服务器上近三天内的暴力破解拦截记录。

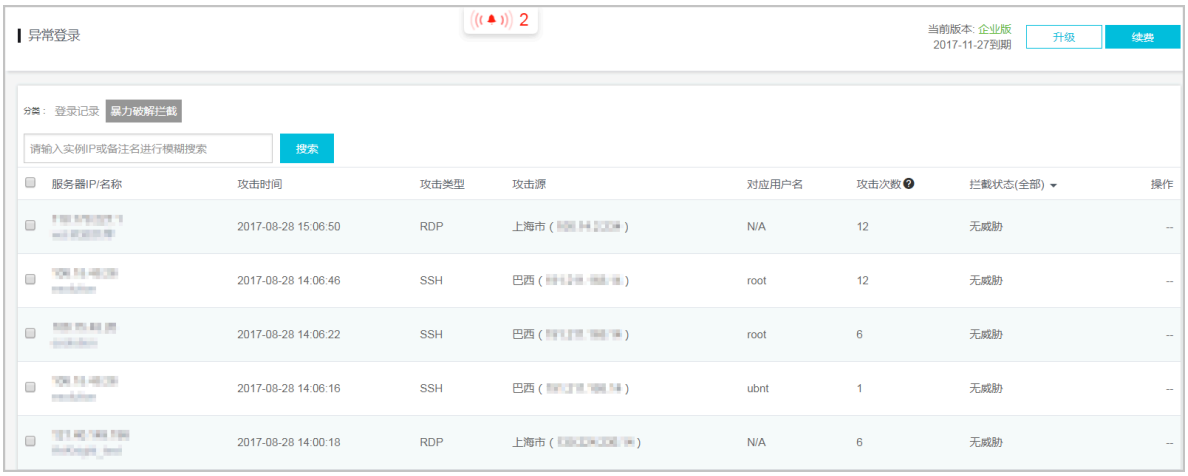
暴力破解拦截功能原理

安骑士 Agent 通过定时收集您服务器上的登录日志并上传到云端，在云端进行分析和匹配。如果发现存在暴力破解行为，将同步到阿里云处罚中心并对攻击源 IP 的行为进行拦截。同时，如果黑客暴力破解密码成功，且成功登录您的服务器，将会触发事件告警。

注意： 您可在 服务器安全#安骑士#管理控制台 > 设置 > 告警设置 中，选择 “登录安全－暴力破解成功” 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）。

操作步骤

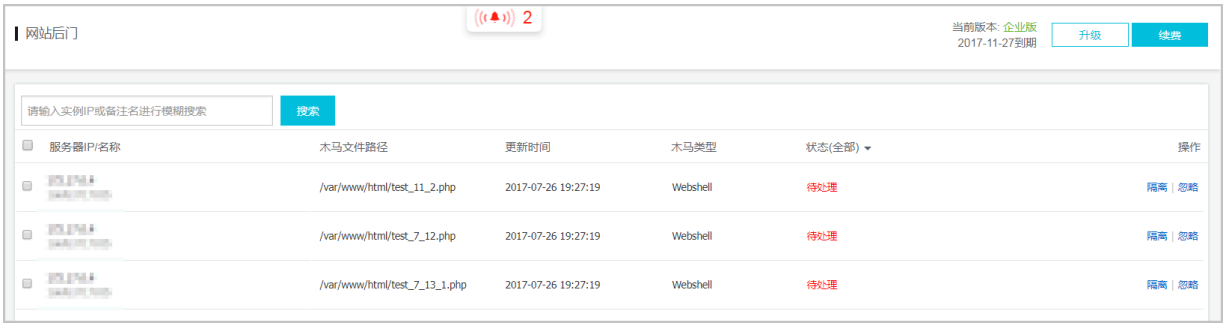
1. 登录 服务器安全#安骑士#管理控制台。
2. 定位到 入侵检测 > 异常登录，选择 暴力破解拦截，查看您的安骑士已防护的服务器上三天内的暴力破解拦截记录。



3. 在拦截状态栏中，可选择 破解成功、无威胁、已拦截、或 已处理 状态，查看相关事件信息，并对该暴力破解行为进行处理。
   - 破解成功： 表示您的服务器被暴力破解密码成功，很有可能已经被入侵登录服务器。请参考 被暴力破解成功之后该怎么办，尽快对您的服务器安全进行加固。
   - 已拦截： 表示该暴力破解行为已经被安骑士成功拦截。
   - 无威胁： 表示安骑士扫描到有暴力破解的攻击行为，但是判断对您的服务器没有威胁。
   - 已处理： 表示您已对该暴力破解事件进行相应的处理。

5.3 网站后门

安骑士自主研发的网站后门查杀引擎，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。



注意： 安骑士企业版提供网站后门文件检测和处理功能；基本版不支持。

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 网站后门文件。如果发现您的服务器存在网站后门文件，安骑士将会触发告警信息。

注意： 您可在 服务器安全#安骑士#管理控制台 > 设置 > 告警设置 中，选择 “木马查杀－发现后门” 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）。

检测周期

安骑士网站后门检测采用动态检测及静态检测两种方式。

默认情况下，安骑士对所有防护的服务器开启静态检测。

- 动态检测： 一旦 Web 目录中的文件发生变动，安骑士将扫描针变动的内容执行即时动态检测。
- 静态检测： 每天凌晨，安骑士扫描整个 Web 目录执行静态检测。

对服务器开启网站后门文件周期检测参见操作步骤4。

检测范围

安骑士自动扫描并添加您服务器中的Web目录作为网站后门的检测范围。

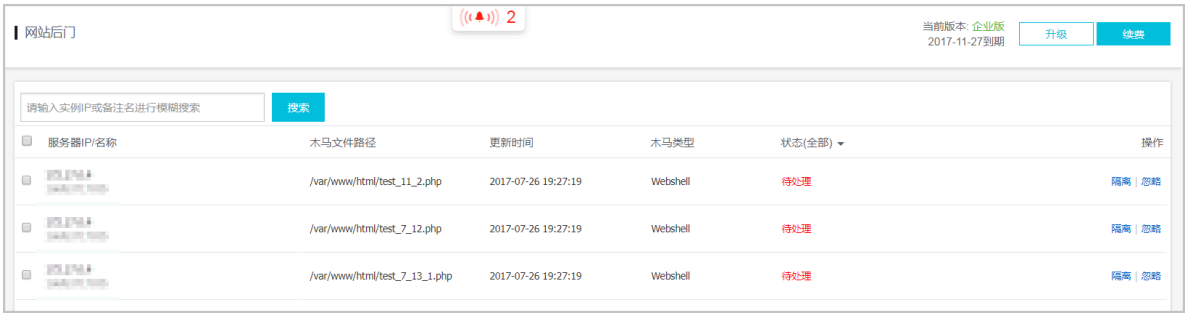
您也可以在安骑士控制台手动添加需要检测的Web目录，详情参见操作步骤5。

注意：出于性能效率考虑，不支持直接添加root目录作为Web目录。

操作步骤

1. 登录 服务器安全#安骑士#管理控制台。

2. 定位到 入侵检测 > 网站后门，查看您的安骑士已防护的服务器上发现的网站后门文件记录。



3. 对发现的网站后门文件进行隔离、恢复或忽略。

- 隔离： 对发现的网站后门文件进行隔离操作，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，将此文件从隔离区中恢复出来。
- 忽略： 忽略该后门文件后，安骑士将不再对此文件提示风险告警。

注意：

安骑士不会直接删除您服务器上的网站后门文件，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，安骑士将不再对此文件进行告警。

隔离区可阻止其它任何程序访问隔离区内的文件，不会对服务器造成威胁。

4. 定位到 设置 > 安全设置 > 木马查杀 页面，单击 周期检查Web目录 选项右侧的 管理 添加/删除需要开启周期检测Web目录的服务器。

5. 定位到 入侵检测 > 网站后门 页面，单击右上角 网站后门设置，手动添加/删除需要检测的Web目录。

- 添加：在网站后门设置页面单击右上角添加，输入需要进行网站后门检测的Web目录路径、并勾选需要添加应用的服务器，单击确定，将该Web目录添加到网站后门检测范围内。

- **删除：在网站后门设置页面勾选无需进行Web目录检测的文件路径，单击左下角的删除，对该目录取消网站后门检测。**

注意：

建议对所有Web目录文件开启网站后门检测。

5.4 主机异常

5.4.1 主机异常事件告警类型

安骑士全面和实时监测您主机的安全状况，并通过告警自动化关联分析能力帮助您更快速、准确地定位到安全风险事件，并对入侵事件和风险提供全面和准确的分析。

主机异常告警类型

安骑士企业版支持主机异常检测和处理；基础版不支持主机异常检测和处理，基础版用户将无法查看主机异常检测事件。

说明:

安骑士基础版和企业版功能差异参见功能列表。

主机异常事件名称	告警说明
进程异常行为	检测资产中是否存在超出正常执行流程的行为。
异常事件	程序运行过程中发生的异常行为。
敏感文件篡改	对服务器中的敏感文件进行恶意修改。
恶意进程（病毒云查杀）	采用云+端的查杀机制，对服务器进行实时检测，并对检测到的病毒文件提供实时告警。您可通过控制台对病毒程序进行处理。
异常网络连接	网络显示断开或不正常的网络连接状态。
异常账号	非合法登陆账号。
异常登录	检测服务器上的异常登录行为。通过设置合法登录IP、时间及账号，对于例外的登录行为进行告警。支持手动添加和自动更新常用登陆地，对指定资产的异地登陆行为进行告警。
网站后门	使用自主查杀引擎检测常见后门文件，支持定期查杀和实时防护，并提供一键隔离功能： · Web目录中文件发生变动会触发动态检测，每日凌晨扫描整个Web目录进行静态检测。 · 支持针对网站后门检测的资产范围配置。 · 对发现的木马文件支持隔离、恢复和忽略。
实时拦截	对特定的恶意进程进行主动拦截。
网页防篡改	实时监控网站目录并通过备份恢复被篡改的文件和目录，保障主机的网站信息不被恶意篡改。

5.4.2 查看和处理/批量处理主机异常事件

您可以在安骑士管理控制台查看和处理主机异常告警事件，并通过告警自动关联全面了解和集中处理安全威胁或入侵事件。

操作步骤

1. 登录安骑士管理控制台。
2. 在左侧导航栏选择入侵检测 > 主机异常。
3. 在主机异常列表中查看或搜索所有检测到的主机入侵和威胁告警及其详细信息。

   您可在主机异常列表页面进行以下操作：

   - 通过输入告警名称或受影响的资产名称来搜索相关的告警事件。

   - 将主机异常威胁文件加入文件隔离箱：确认主机异常警信息后，单击该操作可将威胁文件加入文件隔离箱。被隔离的文件将无法对主机造成威胁，详细信息参见文件隔离箱。

     说明：
     安骑士只支持对网站后门文件进行隔离操作。您可定位到入侵检测 > 网站后门页面对网站后门文件进行隔离。

     说明：

被成功隔离的文件在30天内可执行一键恢复，过期后系统将自动清除该文件。

- 确认线下处理：确认告警并线下进行处理后，单击该操作后该告警状态将变为已处理。

- 忽略本次：忽略本次告警，该告警状态将变为已处理，后续安骑士不会再对该事件进行告警。
- 标记为误报：标记本次告警为误报后该告警状态将变为已处理，后续安骑士不会再对该事件进行告警。您可以在已处理列表中定位到该事件对其进行取消标记误报的操作。

说明：

告警误报是指系统对正常程序进行告警。常见的告警误报有对外异常TCP发包可疑进程，提示您服务器上有进程在对其他设备发起了疑似扫描行为。

批量处理告警事件

您也可以通过主机异常列表左下角的批量处理工具栏对多个告警事件进行批量处理。

说明:

批量处理告警事件前请详细了解告警事件的信息。

5.4.3 主机异常告警自动化关联分析

安骑士企业版支持主机异常告警自动化关联分析。您可在主机异常页面单击单个告警事件名称进入该告警事件的自动关联分析页面、查看和处理告警事件所有关联的异常情况，帮助您对告警事件进行全方位分析。

主机异常告警自动关联分析功能特性

- 主机异常告警自动关联分析功能可对相关的异常事件进行实时自动化关联，挖掘出潜藏的入侵威胁。
- 告警自动化关联以告警发生的时间顺序聚合成关联的告警，帮助您更便捷地分析和处理告警事件，提升您系统的应急响应机制。

操作步骤

1. 登录安骑士管理控制台。
2. 在左侧导航栏定位到入侵检测 > 主机异常。
3. 在主机异常页面单击需要查看的入侵告警事件名称打开告警事件详情页面。

4. 在入侵告警事件详情页面查看告警事件的详细信息、关联的异常事件和对告警/异常事件进行处理。

   · 查看告警详细信息：您可查看受该告警事件影响的资产信息、告警开始/结束事件、关联异常事件的详情。

   · 查看受影响资产：单击受影响的资产名称可跳转到对应资产的详情页面，方便您集中查看该资产的全部告警信息、漏洞信息、基线检查漏洞、资产指纹和安全配置等信息。

   · 查看和处理关联异常：您可在关联异常区域查看该告警事件关联的所有异常情况的详细信息、建议处理方案和处理方式。

- **确认线下处理：确认告警并线下进行处理后，单击该操作后该告警状态将变为已处理。**

- 忽略本次：忽略本次告警，该告警状态将变为已处理，后续态势感知不会再对该事件进行告警。
- 标记为误报：标记本次告警为误报后该告警状态将变为已处理，后续态势感知不会再对该事件进行告警。您可以在已处理列表中定位到该事件对其进行取消标记误报的操作。

 说明:

为方便您集中查看和处理相关的异常事件，关联异常区域中显示的关联异常事件将不会显示在主机异常列表中。

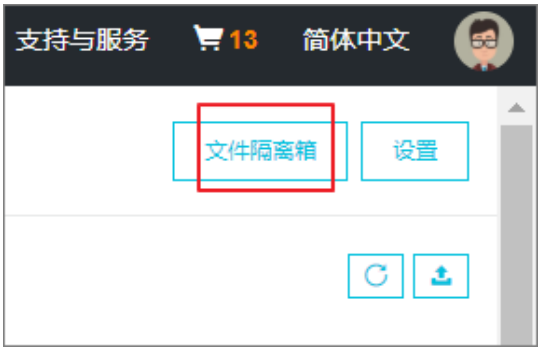
5.4.4 文件隔离箱

安骑士企业版可对检测到的主机异常告警事件进行隔离处理。被加入到文件隔离箱的文件将不会显示在主机异常告警列表中。

操作步骤

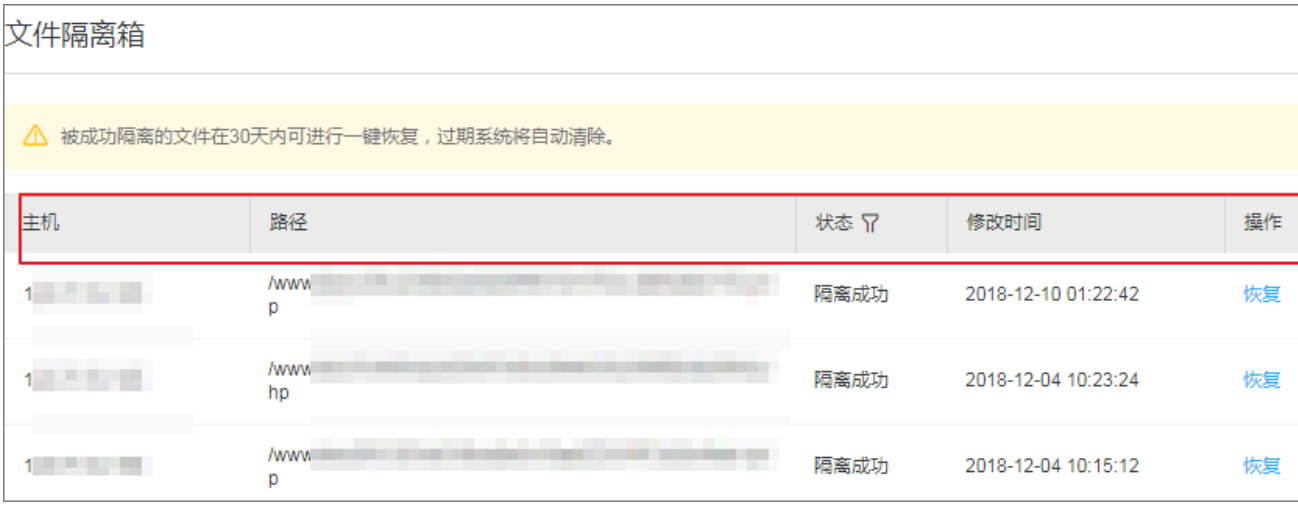
1. 登录安骑士管理控制台。
2. 在左侧导航栏选择入侵检测 > 主机异常。

3. 在主机异常页面单击右上角文件隔离箱。



您可在文件隔离箱页面进行以下操作：

- 在文件隔离箱列表中查看被隔离的文件主机地址、文件路径、隔离状态和操作时间等信息。



- 单击文件隔离箱页面右侧操作栏的恢复，可以将指定的被隔离文件从文件隔离箱中恢复。恢复的文件将重新回到主机异常告警列表中。

说明：

文件被成功隔离后可在30天内进行一键恢复，过期系统将自动清除被隔离的文件。

5.4.5 一键导出主机异常告警列表

安骑士企业版支持一键导出所有主机异常告警事件。

操作步骤

1. 登录安骑士管理控制台。
2. 在左侧导航栏单击入侵检测 > 主机异常。
3. 单击主机异常页面右上角的导出按钮  导出报表。报表导出完成后，安全告警页面右上角会提示导出完成。

> **说明:**
> 安骑士基础版不支持导出主机异常报表功能。基础版需升级至企业版后才可导出报表。

4. 报表导出完成后，单击右上角导出完成提示对话框中的下载，将excel格式的报表下载到本地。

6 资产指纹

6.1 监听端口

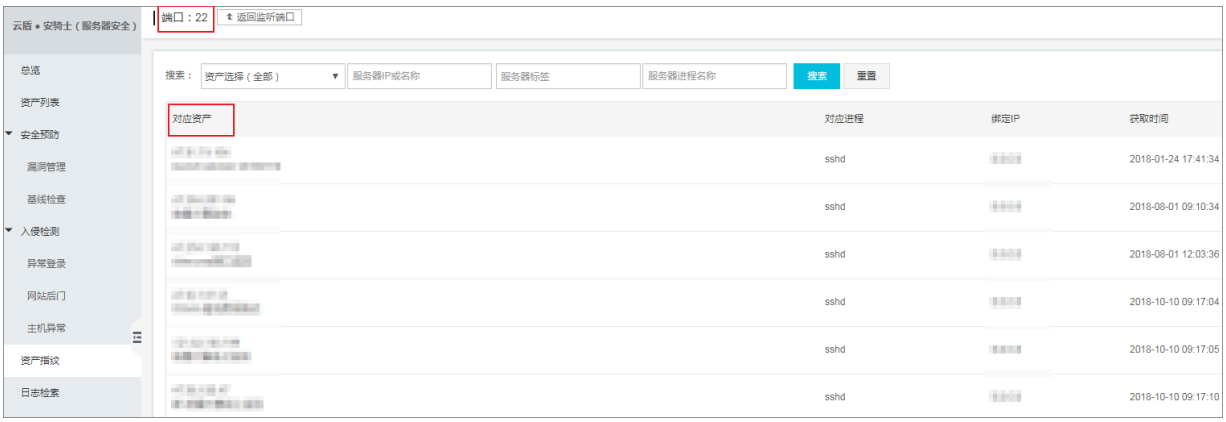
安骑士企业版支持监听端口功能，可定期收集服务器的对外端口监听信息，并对端口变动信息和历史端口信息进行记录和查看，便于您快速定位可疑监听行为。

目前监听端口的数据收集为每小时收集一次。

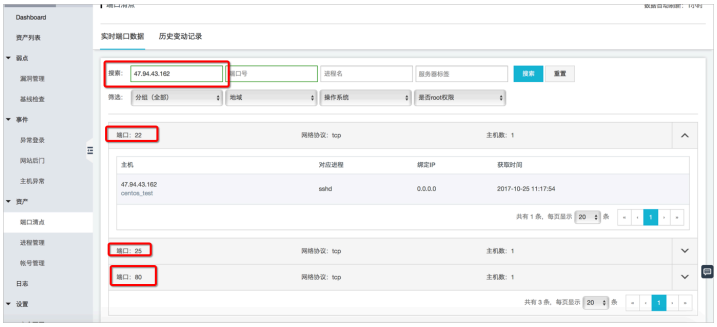
安骑士资产指纹监听端口功能支持监听以下实时端口数据：

- 监听单个端口的所有服务器信息。
- 一台服务器开放的所有端口信息。
- 异常监听端口的历史变动信息，可通过历史记录查看监听时间等信息。
- 端口详情
  - 端口号
  - 对应进程
  - 网络协议，tcp或udp
  - 绑定的IP
- 变动历史说明
  - 变动状态：启动（上次未发现监听，本次数据收集发现监听了）、停止（相反的逻辑）
  - 数据获取时间（由于为周期收集，变动记录的时间为获取到改动的时间，非真实发生的时间）

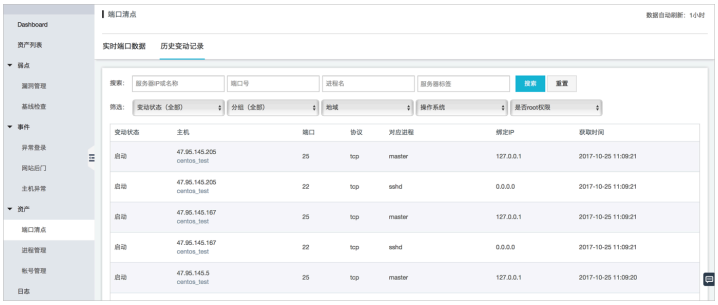
查看监听单个端口的所有服务器信息



查看一台服务器开放的所有端口信息



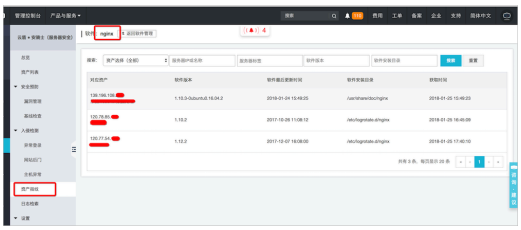
查看端口历史变动信息



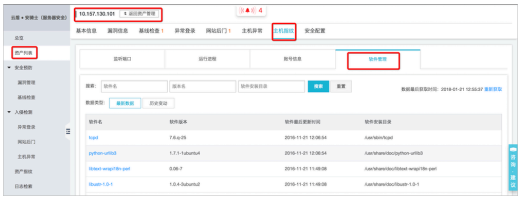
6.2 软件版本管理

- 功能版本：企业版
- 功能介绍：定期收集服务器的软件版本信息，并对变动情况进行记录，便于清点软件资产
- 数据收集周期：可自定义
- 使用场景
  - 清点非法的软件资产，不应该安装的软件被安装上了；
  - 清点版本过低的软件资产，某些软件还停留太低的版本需要软件更新；
  - 漏洞爆发后，可以快速定位到受影响的资产范围，加速漏洞处置
- 软件详情
  - 软件版本
  - 软件最后更新时间
  - 软件安装目录

一个软件多台机器安装了



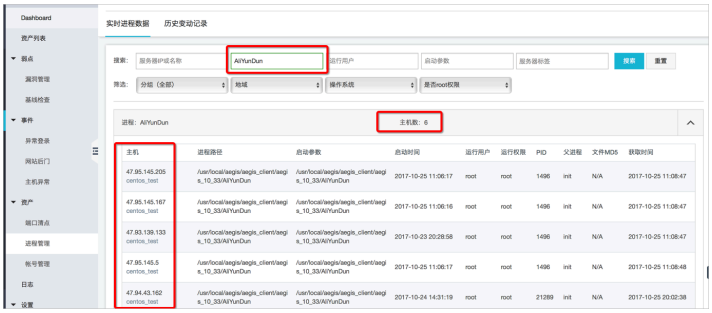
一台机器安装了多个软件



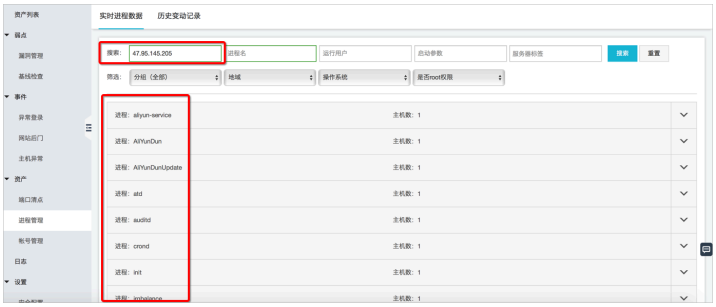
6.3 运行进程

- 功能版本：企业版
- 功能介绍：定期收集服务器的进程信息，并对变动情况进行记录，便于进程清点和历史进程变动查看
- 数据收集周期：每小时
- 使用场景
  - 清点一个进程，有多少服务器运行了
  - 清点一台服务器，运行了多少个进程
  - 发现了非法进程，通过历史记录可查看到启动的时间
- 进程详情
  - 进程名
  - 进程路径
  - 启动参数
  - 启动时间
  - 运行用户
  - 运行权限
  - PID
  - 父进程名
  - 文件MD5（小于1M的文件将计算）
- 变动历史说明
  - 变动状态：启动（上次未发现运行，本次数据收集发现运行了）、停止（相反的逻辑）
  - 数据获取时间（由于为周期收集，变动记录的时间为获取到改动的时间，非真实发生的时间）

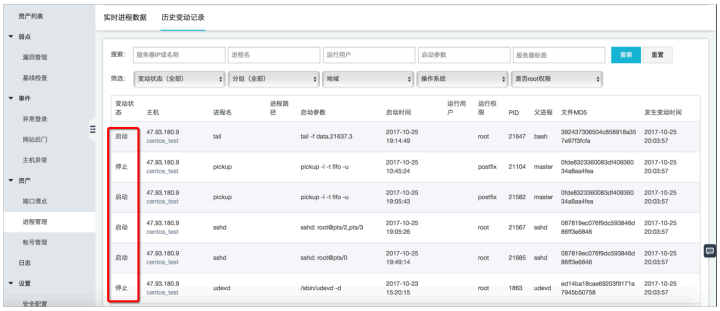
清点一个进程有多少服务器在运行



清点一台服务器运行了多少个进程



进程历史变动

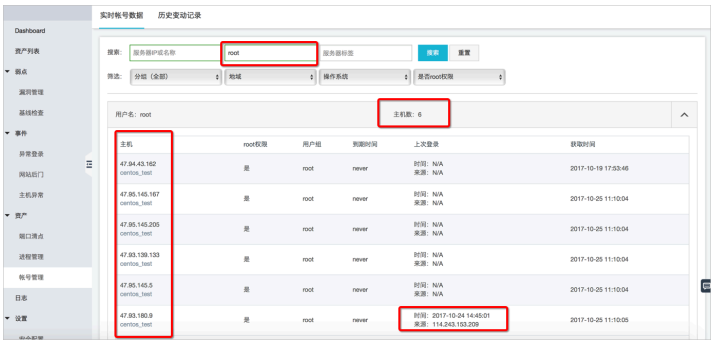


6.4 账号信息

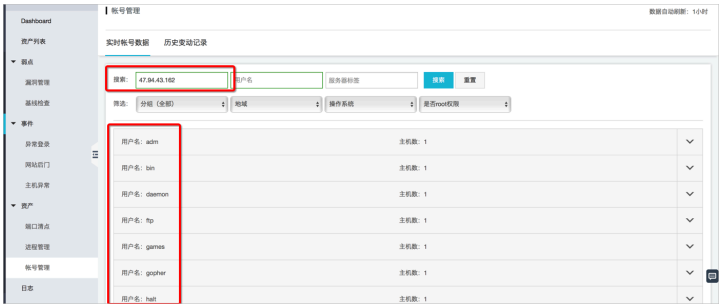
- 功能版本：企业版
- 功能介绍：定期收集服务器的账号信息，并对变动情况进行记录，便于账号清点和历史账号变动查看
- 数据收集周期：每小时
- 使用场景
  - 清点一个账号，有多少服务器创建了
  - 清点一台服务器，创建了多少个账号
  - 发现了非法账号，通过历史记录可查看到变动的时间

- 账号详情
  - 账号名
  - 是否root权限
  - 用户组
  - 到期时间
  - 上次登录情况（登录时间、登录来源）
- 变动历史说明
  - 变动状态：新建（上次未发现，本次数据收集发现新建了）、删除（上次数据收集有，本次没有了）、修改（账号名没变，但是root权限、y用户组、到期时间变动了）
  - 数据获取时间（由于为周期收集，变动记录的时间为获取到改动的时间，非真实发生的时间）

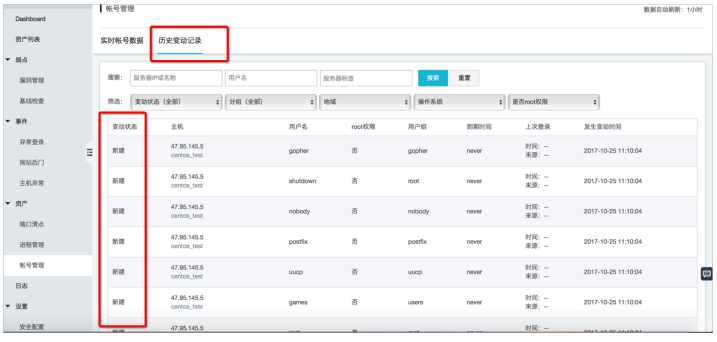
清点一个账号有多少服务器创建了



清点一台服务器创建了多少账号



账号历史变动



7 日志分析

7.1 开通日志分析服务

安骑士企业版支持全量日志服务，提供准确实时的日志查询和强大的日志分析功能。

使用日志分析服务之前，您需在安骑士控制台开通和购买日志服务。

安骑士基础版用户如需使用日志分析服务，需先升级到企业版。详细信息参见续费和升级。

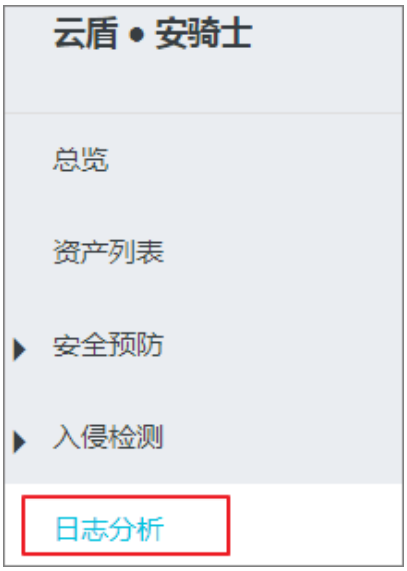
日志库限制说明

安骑士日志库属于专属日志库。

- 您无法通过API/SDK等方式在数据库中写入数据，或者修改日志库的属性（例如存储周期等）。
- 其他日志库功能，例如查询、统计、报警、流式消费等均支持，与一般日志库无差别。
- 日志服务对专属日志库不进行任何收费，但日志服务本身需处于已开通状态。
- 内置的报表可能会在以后更新并升级。

操作步骤

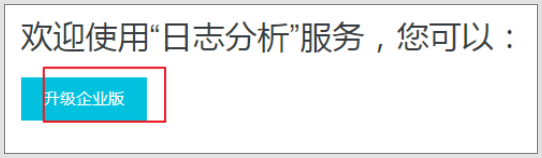
1. 登录安骑士管理控制台。
2. 在左侧导航栏单击日志分析进入日志分析开通引导页面。



3. 在日志分析开通引导页面单击立即开通。

> 说明:

基础版用户需单击升级至企业版才可开通和使用日志分析服务。



开通完成后您可以开始使用安骑士日志分析服务了。

7.2 日志分类及参数说明

本文档介绍了安骑士日志的类型和相关参数说明。

安骑士全量日志集中存放在aegis-log专属日志库中，您可以在储存日志服务的项目aegis-log-阿里云账户ID-区域名中找到专属日志库。

安骑士默认开启两大类日志：

- 主机日志
  - 暴力破解日志
  - 登录流水日志
  - 账户快照
  - 端口快照
  - 进程快照
- 安全日志
  - 异常登录
  - 主机异常
  - 网站后门
  - 基线日志
  - 漏洞日志

主机日志

主机日志参数说明见下表：

日志来源	主题（__topic__）	描述	备注
暴力破解日志	aegis-log-crack	登录失败的信息。	实时采集。
登录流水日志	aegis-log-login	登录的流水日志。	实时采集，1分钟内的重复登录时间会被合并为1条日志。

日志来源	主题（__topic__）	描述	备注
进程快照	aegis-snapshot-process	主机上进程快照信息。	资产指纹自动收集功能开启后才有数据。每台主机一天非固定时间收集一次。
账户快照	aegis-snapshot-host	主机上账户快照信息。	资产指纹自动收集功能开启后才有数据。每台主机一天非固定时间收集一次。
端口快照	aegis-snapshot-port	主机上端口侦听快照信息。	资产指纹自动收集功能开启后才有数据。每台主机一天非固定时间收集一次。

安全日志

安全日志参数说明见下表：

日志来源	主题（__topic__）	描述	备注
异常登录	aegis-login-log	主机的异常登录信息。	实时采集
主机异常	aegis-susp-log	主机的异常事件信息。	实时采集
网站后门	aegis-webshell-log	网站后门日志。	实时采集。
基线日志	sas-hc-log	基线日志。	实时采集。
漏洞日志	sas-vul-log	漏洞日志。	实时采集。

7.3 查询日志

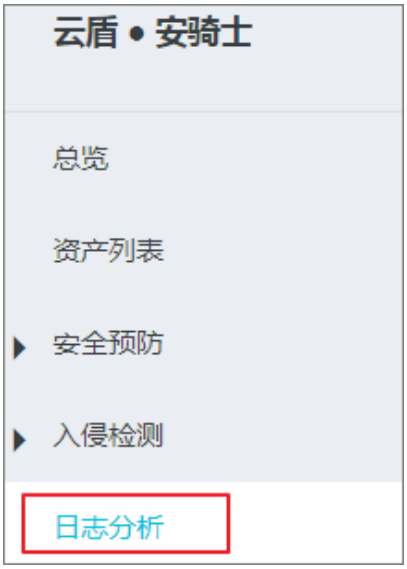
安骑士与阿里云日志服务打通，对外开放平台相关或者产生的日志，包括主机、安全两大类共10种子类日志。提供近实时的日志自动采集存储、并提供基于日志服务的查询分析、报表报警、下游计算对接与投递的能力。

选择特定类型的日志，即可对采集到的日志数据进行实时查询与分析、查看或编辑仪表盘、设置监控告警等。

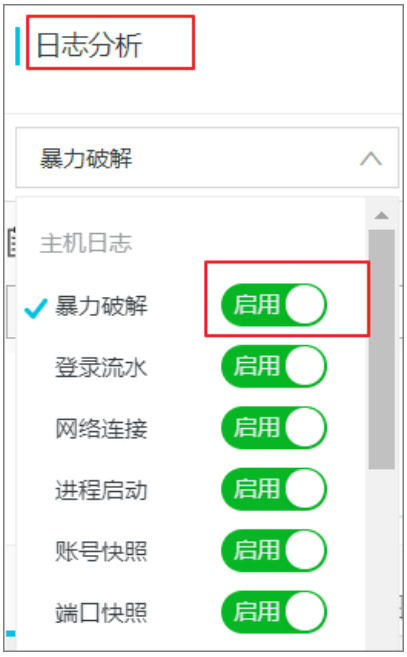
操作步骤

1. 登录安骑士管理控制台。

2. 在左侧导航栏中选择日志分析 。



3. 在日志分析页面选择您需要查看的日志类型，并将状态设置为启用。

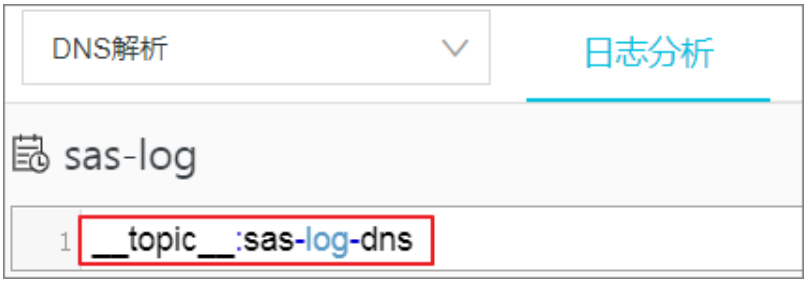


说明:

日志分析服务开通后，安骑士默认开启日志。

您还可以在日志分析页面进行以下操作：

- 单击日志分析打开日志服务查询和分析页面，页面将展示您选择的日志类型的查询和分析页面，并且系统会为您自动匹配查询语句。



- 单击搜索按钮上方的时间设置下拉框选择日志时间范围，然后单击搜索按钮查看您所选时间范围内的日志信息。

说明：
安骑士日志可保存180天，每条日志会在其日志时间的第180天被删除。

说明：
安骑士支持对7天内的日志进行查询和分析。如需搜索或分析超过7天的日志数据，请提交工单了解详情。

7.4 自定义日志查询与分析

您可在日志分析页面的日志搜索栏中对日志进行自定义查询与分析，查询多种复杂场景下的日志。

日志查询语句由查询语法（Search）和分析语法（Analytics）两部分组成，中间通过|进行分隔：

```
$Search |   $Analytics
```

查询语法和分析语法都可选。

- 查询（Search）：查询条件可以由关键词、模糊、数值、区间范围和组合条件等产生。如果为空或*，代表对该时间段所有数据不过滤任何条件、直接对所有查询结果进行统计。

- 分析（Analytics）：对查询结果或全量数据进行计算和统计。如果为空，代表只返回查询结果、不做统计。

查询语法

日志服务查询语法支持全文查询和字段查询，查询框支持换行显示、语法高亮等功能。

- 全文查询

  不需要指定字段，直接输入关键字查询。可以用双引号（""）包裹关键字，多个关键字之间以空格或and分割。

  - 多关键字查询示例

    搜索所有包含`www.aliyun.com`和`404`的日志。例如：

    ```
    www.aliyun.com 404
    ```

    或者：

    ```
    www.aliyun.com and 404
    ```

  - 条件查询示例

    搜索所有包含`www.aliyun.com`并且包含`error`或者`404`的日志。例如：

    ```
    www.aliyun.com and (error and 404)
    ```

  - 前缀查询示例

    搜索所有包含`www.aliyun.com`并且包含`failed_`开头关键字的日志。例如：

    ```
    www.aliyun.com and failed_*
    ```

    说明：

    字段查询只支持后缀加`*`，不支持前缀加`*`。

- 字段查询

  可实现数值类型字段的比较，格式为字段：值或字段>=值，通过and、or等进行组合。也可以和全文搜索组合使用，同样通过and、or组合。

  日志服务支持基于字段进行更精准的查询。

  - 查询多字段示例

    搜索所有严重等级的安全报警的日志。例如：

    ```
    __topic__ : sas-security-log and level: serious
    ```

    搜索某个客户端1.2.3.4上所有的SSH登录。例如：

    ```
    __topic__:aegis-log-login and ip:1.2.3.4 and warn_type:SSHLOGIN
    ```

    说明：

    每条日志中都包含一个__topic字段表示主题，日志都是通过该字段来区分。示例中用的字段level、warn_type、ip等都是特定日志类型的字段。

  - 查询数值字段示例

    搜索所有响应时间超过1秒的本地DNS查询日志。例如：

    ```
    __topic__:local-dns and time_usecond > 1000000
    ```

    也支持区间查询，查询响应时间大于1秒且小于等于10秒的本地DNS查询日志。例如：

    ```
    __topic__:local-dns and time_usecond in [1000000,10000000]
    ```

  详细的查询语法说明请参考索引与查询。

分析语法

您可以使用SQL/92语法对日志数据进行分析与统计。日志服务支持的语法与函数参见实时分析简介。

分析语句中可以省略SQL标准语法中的from表格名语句，即from log。

日志数据默认返回前100条，您可以通过*LIMIT*语法修改返回范围。

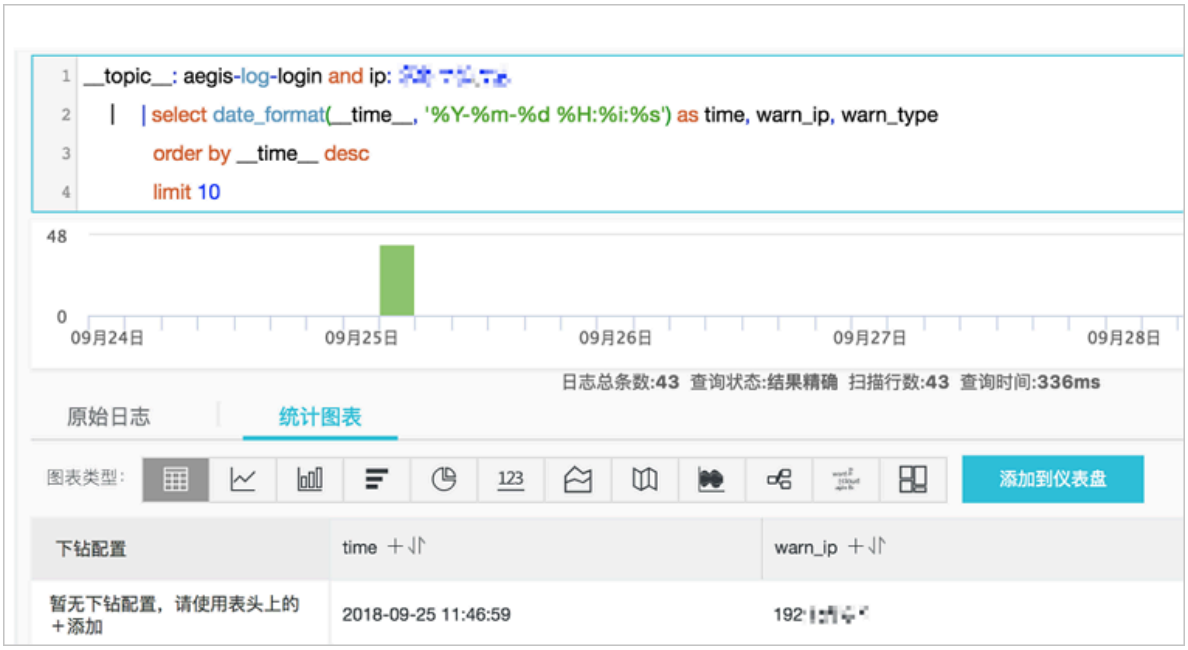
基于日志时间的查询分析

每条日志都有一个内置字段__time__，表示这条日志的时间，以便在统计时进行基于时间的计算。其格式为 Unix时间戳，本质是一个自从1970-1-1 0:0:0 UTC时间开始的累计过去的秒数。因此实际使用时，经过可选的计算后，需要格式化才可以展示。

- **选择并展示时间**

  这里在特定时间范围内，选择ip为`1.2.3.4`的最新10条登录日志，展示其中时间、来源IP以及登录类型。例如：

```
__topic__: aegis-log-login and ip: 1.2.3.4
| select date_format(__time__, '%Y-%m-%d %H:%i:%s') as time, warn_ip
, warn_type
order by __time__ desc
limit 10
```



- **计算时间**

  查询登录过后的天数，可以使用`__time__`进行计算。例如：

```
__topic__: aegis-log-login and ip: 1.2.3.4
| select date_format(__time__, '%Y-%m-%d %H:%i:%s') as time, warn_ip
, warn_type ,
round((to_unixtime(now()) - __time__)/86400,1) as "days_passed"
order by __time__ desc
limit 10
```

  这里使用`round((to_unixtime(now()) - __time__)/86400, 1)`，先用to_unixtime将now()获取的时间转化为Unix时间戳，再与内置时间字段`__time__`相

减，获得已经过去的时间秒数。最后除以86400，即一天的总秒数，再用函数round(data, 1)圆整为小数点后1位数的值，可得出每条攻击日志距离现在已经过去了几天。

- 基于特定时间分组统计

  如果想知道特定时间范围内某个设备的登录趋势，可使用如下SQL：

```
__topic__: aegis-log-login and ip: 1.2.3.4
| select date_trunc('day', __time__) as dt,
count(1) as PV
group by dt
order by dt
```

  这里使用内置字段`__time__`，传给函数`date_trunc('day', ..)`对时间按天对齐，将每条日志分组到了其所属的天的分区中进行统计总数（count(1)），并按照分区时间块排序。函数`date_trunc`第一个参数提供更多其他单位进行对齐，包括`second`、`miniute`、`hour`、`week`、`month`、`year`等，函数说明参见日期和时间函数。

dt	PV
2018-09-28 00:00:00.000	1
2018-09-29 00:00:00.000	13
2018-09-30 00:00:00.000	1

- **基于灵活时间分组统计**

  如果想知道更灵活的分组时间规律，例如整个账户下设备每5分钟的登录趋势，可以使用如下SQL：

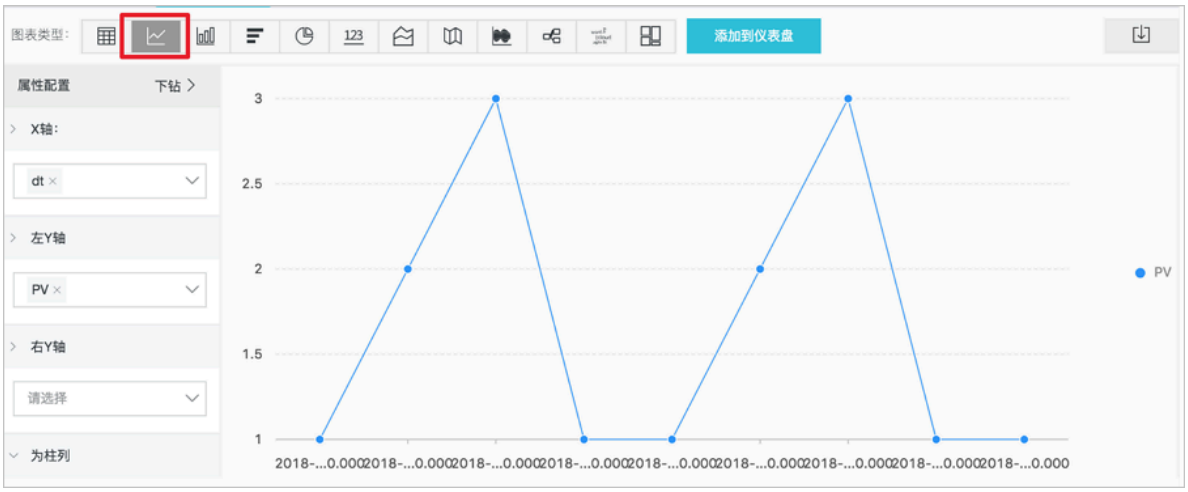
```
__topic__: aegis-log-login
| select from_unixtime(__time__ - __time__% 300) as dt,
count(1) as PV
group by dt
order by dt
```

```
limit 1000
```

使用计算的内置时间字段计算`__time__ - __time__% 300`，同时使用函数`from_unixtime`进行格式化，将每条日志分组到了一个5分钟（300秒）的分区中进行统计总数`(count(1))`，并按照分区时间块排序，获得前1000条，相当于选择时间内的前83小时的数据。

dt	PV
2018-09-28 10:15:00.000	1
2018-09-29 13:00:00.000	2
2018-09-29 13:05:00.000	3
2018-09-29 13:10:00.000	1
2018-09-29 14:30:00.000	1
2018-09-29 16:10:00.000	2
2018-09-29 16:15:00.000	3

折线图显示如下：



更多关于时间解析的函数，例如将一个时间格式转化为另外一个格式，需要使用`date_parse`与`date_format`，函数说明参见日期和时间函数。

基于客户端IP的查询分析

日志中warn_ip表示登录日志的登录源IP。

- 登录源国家分布

  对某个设备登录的来源国家分布查询，例如：

```
__topic__: aegis-log-login and uuid: 12344567
| SELECT ip_to_country(warn_ip) as country,
count(1) as "登录次数"
group by country
```

  这里先用函数ip_to_country得到这个登录源IPwarn_ip对应的国家信息。

country	登录次数
柬埔寨	1
新加坡	6
英国	1

  世界地图展示如下：

- 登录者身份分布

  使用函数 ip_to_province获得更详细的基于省份的登录者分布，例如：

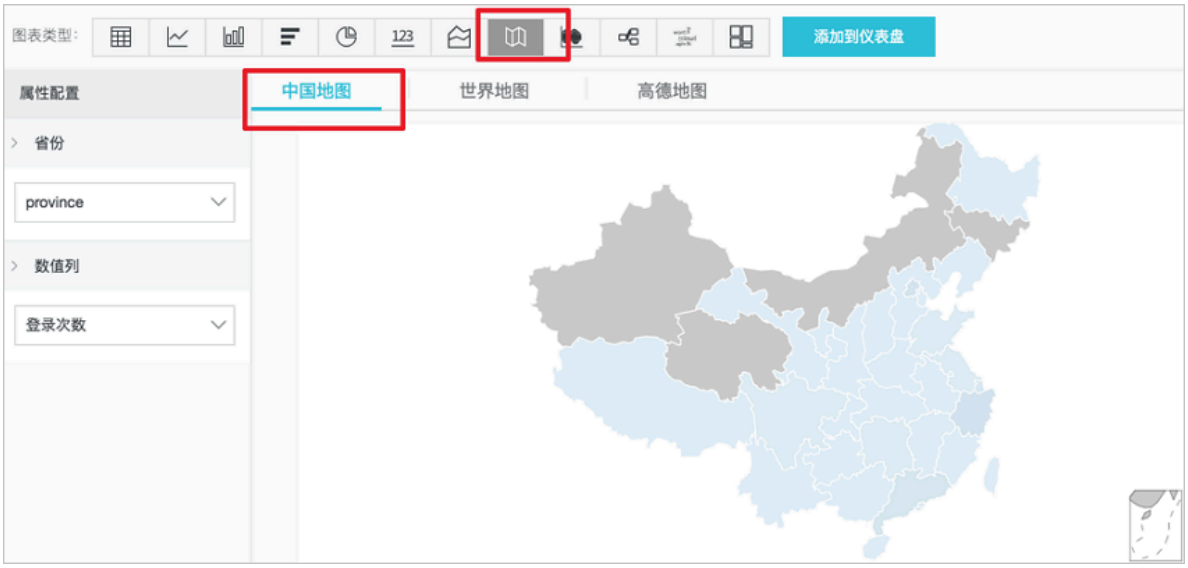
```
__topic__: aegis-log-login and uuid: 12344567
| SELECT ip_to_province(warn_ip) as province,
         count(1) as "登录次数"
```

```
        group by province
```

这里使用了另外一个IP函数`ip_to_province`来获得一个IP的所属省份。如果是中国以外的IP地址，会尝试转化为其国家所属省份（州），但在选择中国地图展示时，会无法展示出来。

province	登录次数
黑龙江省	4
辽宁省	15
俄亥俄州	2
江西省	4
KH_10	1
湖南省	58
US_CO	58
山东省	70
安徽省	6

中国地图方式展示如下：



- **登录者热力分布**

  使用函数`ip_to_geo`获得一张登录者的热力图：

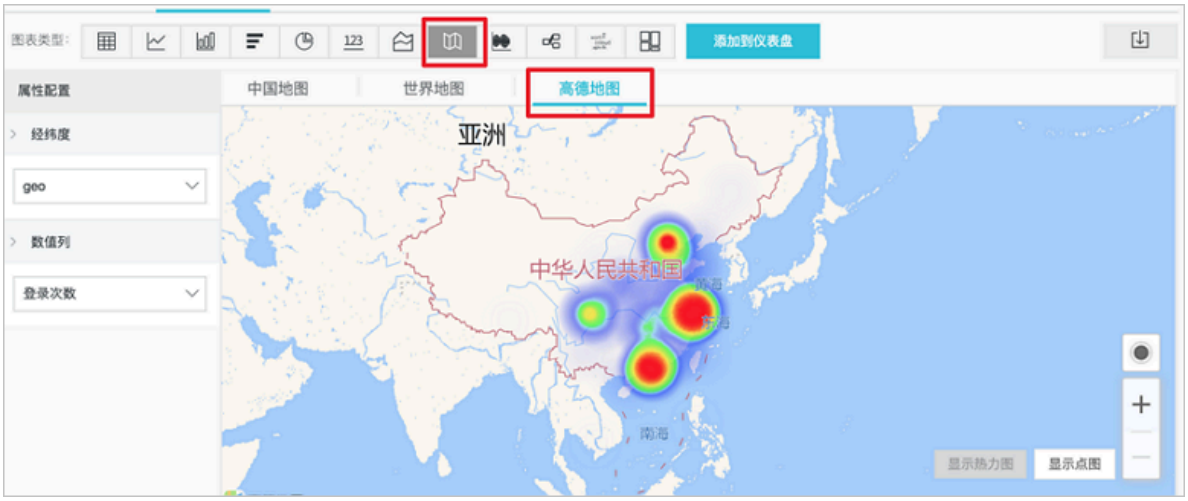
```
__topic__: aegis-log-login and uuid: 12344567
| SELECT ip_to_geo(warn_ip) as geo,
         count(1) as "登录次数"
         group by geo
```

```
    limit 10000
```

这里使用了另一个IP函数`ip_to_geo`来获得一个IP的所在经纬度，并获取前1万条。

geo	登录次数
[redacted]	1
[redacted]	2
[redacted]	1
[redacted]	56
[redacted]	1
[redacted]	1
[redacted]	1

高德地图展示如下：



说明:

基于IP的更多解析功能，例如获得IP所属运营商`ip_to_provider`、判断IP是内网还是外网`ip_to_domain`等，可以参考*IP*地理函数。

7.5 查看日志的时间分布

您可以在日志分析页面查看查询到的日志的时间分布柱状图。

搜索栏下面显示了日志的分布时间和查询到的日志总数。横轴显示时间，纵轴显示查询到的日志数量。

您可在日志时间分布图横轴上滑动以缩小选择的时间范围，并显示对应时间范围内的查询结果。

7.6 查看原始日志

您可通过日志分析功能查看原始日志及其详细信息。原始日志支持下载到本地。

原始日志页面展示了每一条日志的详细内容，包括时间、内容以及日志中的各个字段。

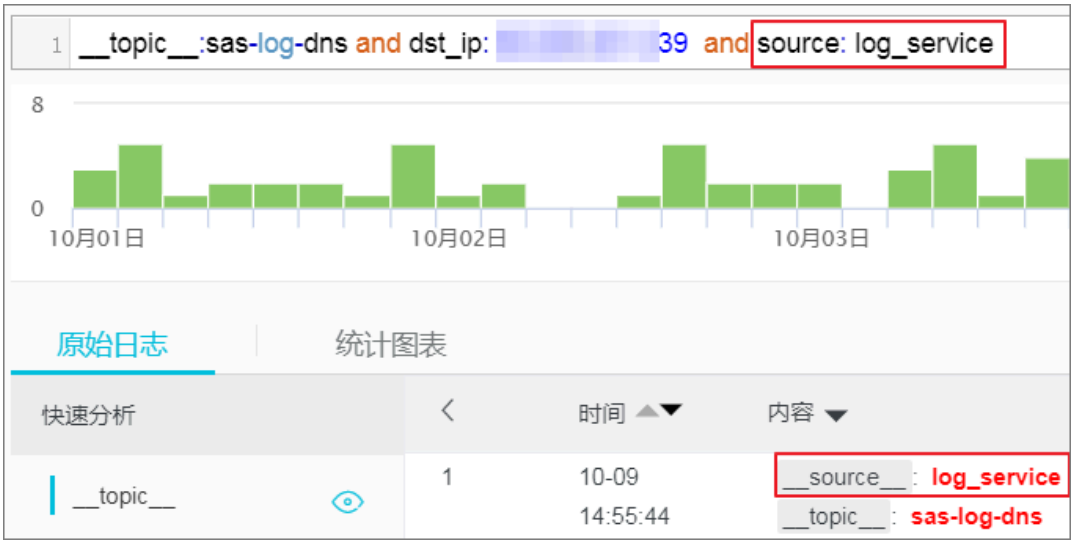
您可对列进行排序、对当前查询结果进行下载，也可以单击齿轮按钮，选择特定的字段进行展示等。

在页面中点击相应字段的值或分词，搜索框中会自动输入相应的搜索条件。

操作步骤

1. 单击日志分析页面的原始日志按钮打开原始日志列表。

2. 在内容栏中单击相应的字段，可将该字段自动加到搜索栏中。如选中log_service，搜索栏中将会加入该字段。

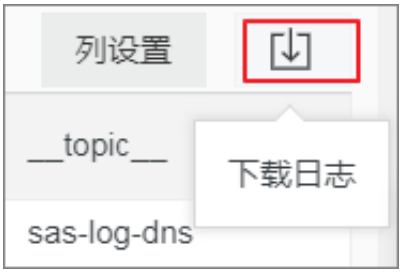


您可在原始日志页面进行以下操作：

- 单击原始日志列表右侧的列设置可将您需要的字段添加到原始日志列表中。

字段添加到列设置后，原始日志列表将以列的形式呈现该字段信息。

- 单击列设置右侧的下载日志按钮打开下载日志对话框。



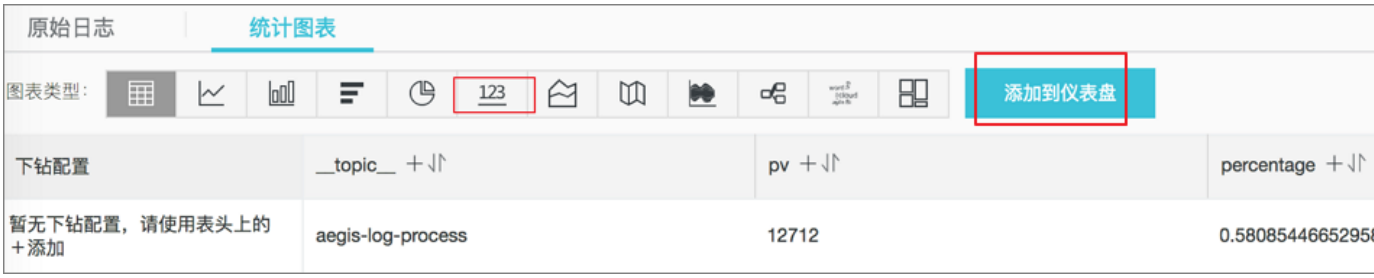
在下载日志对话框中单击下载本页日志或通过命令行工具下载所有日志下载日志。

- 下载本页日志：以CSV格式将本页面的日志到本地。
- 通过命令行工具下载所有日志：使用命令行工具下载所有的日志。详细操作参见导出日志。

7.7 查看统计图表

日志分析服务支持图表形式展示日志分析结果。

您可以在控制台统计图表页面根据需要选择不同的图表类型或将日志统计图表添加到仪表盘。



统计图表类型信息参见图表说明。

7.8 查看日志报表

安骑士日志报表 页面展示了日志服务默认的仪表盘 界面。您可以在当前仪表盘通过修改时间范围、添加过滤条件等操作，查看多种筛选条件下的仪表盘数据。

日志报表页面提供以下两类共6个默认的仪表盘：

- 安全
  - 漏洞中心
  - 基线中心
  - 主机异常中心
- 主机
  - 登录中心
  - 进程中心
  - 网络连接中心

仪表盘各模块说明参见日志报表仪表盘。

> 说明:
> 查看日志报表前请确认日志分析页面右侧的日志状态为开启。日志关闭状态下您将无法查看日志报表。

操作步骤

1. 登录安骑士管理控制台。
2. 单击左侧导航栏日志分析。

3. 在日志分析页面单击日志类型主机日志或安全日志切换到对应的日志报表盘页面。

   您可在日志报表盘页面进行以下操作：

   · 单击报表盘下方的时间选择器按钮 

打开时间设置对话框筛选您指定时间范围内的日志。

   可选择相对时间、整点时间或设置自定义时间。

说明：

设置时间范围后，该页面所有的仪表盘都将显示该时间范围内的数据。

说明：

时间选择器仅在当前页面临时生效，系统不保存该设置。您下次重新打开该报表页面时，仪表盘将恢复到默认时间范围。

- 您可在时间选择器下方的搜索框输入客户端ID、客户端IP、登录源IP和登录类型作为过滤条件，单击查询定位到对应的报表。

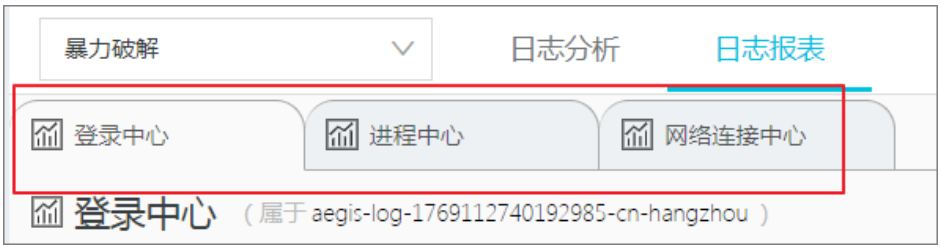
设置过滤条件后，日志列表仪表盘将展示过滤条件范围对应的数据。您可添加多个过滤条件，缩小报表数据展示范围。

7.9 日志报表仪表盘

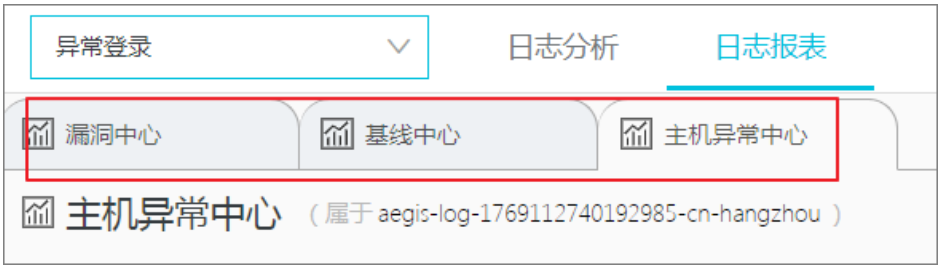
安骑士日志报表 页面为您集中展示安全、主机两部分日志列表仪表盘的相关数据。

安骑士日志分析功能开通后，系统为您自动创建以下6个默认的报表仪表盘页面：

- 主机日志报表仪表盘：



- 安全日志报表仪表盘：



主机日志：登录中心

安骑士可展示主机登录中心仪表盘，为您提供主机上登录信息的全局视图，包括登录源和目标地址地理分布、趋势、登录端口和类型分布等。

登陆中心仪表盘信息说明参见下表：

图表名称	数据类型	默认时间范围	描述	样例
登录次数	单值比较	1小时/同比昨日	总的登录总数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
被登录设备	单值比较	今日（整点）/同比昨日	被登录的独立主机设备的个数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
独立登录源IP	单值比较	今日（整点）/同比昨日	登录设备的独立源个数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
独立登录用户名	单值比较	今日（整点）/同比昨日	登录设备的独立用户名的个数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
终端登录监控趋势	柱状图与线图	今日（整点）	每小时的发生登录事件的设备以及登录次数的趋势图。	-
登录方式趋势	流图	今日（整点）	每小时的登录方式（RDP、SSH等）的趋势图，单位为次/每小时。	-
登录方式分布	饼图	今日（整点）	登录方式（RDP、SSH等）的趋势图的分布。	-
设备分布	地图（全球）	今日（整点）	发生登录事件有外网地址的设备数的地理分布	-
登录来源分布	地图（全球）	今日（整点）	发生有外网地址的设备上登录来源的登录数地理分布	-
独立登录源分布	地图（全球）	今日（整点）	发生有外网地址的设备上独立登录来源数的地理分布。	-

图表名称	数据类型	默认时间范围	描述	样例
登录最多的10个用户	饼图	今日（整点）	登录次数最多的10个用户名。	-
登录最多的10个端口	饼图	今日（整点）	登录次数最多的10个目标端口。	-
激活用户列表	表格	今日（整点）	在设备上可用的前30个账户。	-
登录机器最多30个用户和来源信息	表格	今日（整点）	登录机器最多30个用户和来源，包括来源网络、登录IP、用户名、登录方式、登录的独立设备数以及次数等。	-

主机日志：进程中心

安骑士可展示主机进程中心仪表盘，为您提供主机上进程启动相关的全局视图，包括进程启动趋势、分布，进程类型以及特定bash、java程序的启动分布等。

进程中心仪表盘信息说明参见下表：

图表名称	数据类型	默认时间范围	描述	样例
进程启动次数	单值比较	1小时/同比昨日	进程启动事件总数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
相关设备数	单值比较	今日（整点）/同比昨日	发生进程启动事件的独立主机设备的个数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
独立启动进程名称	单值比较	今日（整点）/同比昨日	启动的独立进程名的个数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%

图表名称	数据类型	默认时间范围	描述	样例
终端设备数	柱状图与线图	今日（整点）	每小时的发生进程启动的设备以及独立进程名个数的趋势图，单位为个/小时。	-
进程启动趋势	线图	今日（整点）	每小时的每台设备平均启动进程数，单位为个/小时。	-
外网设备分布	地图（全球）	今日（整点）	发生进程启动的有外网地址的设备数的地理分布。	-
外网设备上进程启动次数分布	地图（全球）	今日（整点）	发生有外网地址的设备上进程事件数的地理分布。	-
启动次数最多的20个进程	表格	今日（整点）	启动次数最多的20个进程，包括进程名、进程路径、启动次数等。	-
触发Bash最多的前20个进程	表格	今日（整点）	触发Bash最多的前20个进程，包括父进程名、触发总数等。	-
启动进程最多的前30个客户端	表格	今日（整点）	启动进程最多的前30个客户端，包括客户端、总的启动次数、这个客户端上启动次数最多的命令行、对应进程名/次数和占比等。	-

主机日志：网络连接中心

安骑士可展示主机网络连接中心仪表盘，为您提供主机上网络链接变化的全局视图，包括连接趋势、分布，链接目标以及接入的分布与趋势等。

网络中心仪表盘信息说明参见下表：

图表名称	数据类型	默认时间范围	描述	样例
连接事件	单值比较	1小时/同比昨日	设备上网络连接的变化事件总数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
相关设备	单值比较	今日（整点）/同比昨日	发生连接变化事件的独立主机设备的个数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
独立进程	单值比较	今日（整点）/同比昨日	发生网络连接的变化事件独立进程名数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
独立源IP	单值比较	今日（整点）/同比昨日	发生网络连接的变化事件的独立连接源IP的个数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
独立目标IP	单值比较	今日（整点）/同步昨日	发生网络连接的变化事件的独立连接目标IP的个数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
网络连接趋势	双线图	今日（整点）	每小时发生网络连接的设备数以及事件数的趋势图，单位为个/每小时。	-
连接类型趋势	双线图	今日（整点）	每小时发生网络连接变化事件的连接类型（对外、接收）分布的趋势图，单位为个/每小时。	-

图表名称	数据类型	默认时间范围	描述	样例
连接类型分布	饼图	今日（整点）	网络连接变化事件的连接类型（对外、接收）的分布。	-
协议类型分布	饼图	今日（整点）	网络连接变化事件的连接协议（tcp、udp等）的分布。	-
外网设备分布	地图（全球）	今日（整点）	发生网络连接变化事件的设备数的地理分布。	-
外网设备事件分布	地图（全球）	今日（整点）	发生有外网地址的设备上网络连接变化事件数的地理分布。	-
对外连接目标分布	地图（全球）	今日（整点）	网络连接变化事件的对外连接的目标的地理分布。	-
接收连接源分布	地图（全球）	今日（整点）	网络连接变化事件的接收连接的源目标的地理分布。	-
对外连接最多的30个设备	表格	今日（整点）	发生对外连接类型的网络连接变化事件最多的30个设备，包括设备、对外连接事件数、独立的连接目标数、以及样例。	-
接收连接最多的30个设备	表格	今日（整点）	发生接收连接类型的网络连接变化事件最多的30个设备，包括设备、侦听IP、接收连接事件数、侦听端口数，以及样例。	-

图表名称	数据类型	默认时间范围	描述	样例
对外连接目标最多的30个设备	表格	今日（整点）	发生对外连接类型的网络连接变化事件中目标最多的30个设备，包括设备、对外连接事件数、独立的连接目标数、以及样例。	
接收连接最多的30个侦听端口	表格	今日（整点）	发生接收连接类型的网络连接变化事件中最多的30个侦听端口，包括侦听端口、接收连接事件数、以及样例。	-
对外连接最多的30个进程	表格	今日（整点）	发生对外连接类型的网络连接变化事件的最多的30个进程名，包括进程名、对外连接事件数、相关设备数、以及路径样例。	-
接收接收连接最多的30个进程连接最多的30个设备	表格	今日（整点）	发生接收连接类型的网络连接变化事件的最多的30个进程名，包括进程名、对外连接事件数、相关设备数、以及路径样例。	-

安全日志：漏洞中心

提供漏洞相关的全局视图，包括漏洞分布、新增/严重/修复的趋势、状态等。

图表	类型	默认时间范围	描述	样例
相关客户端	单值比较	今日（整点）/同比昨日	发生漏洞问题的独立主机设备的个数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%

图表	类型	默认时间范围	描述	样例
新增漏洞	单值比较	今日（整点）/同比昨日	新增安全漏洞事件数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
验证漏洞	单值比较	今日（整点）/同比昨日	验证安全漏洞事件数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
修复漏洞	单值比较	今日（整点）/同比昨日	修复安全漏洞事件数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
漏洞操作趋势	流图	今日（整点）	每小时的各种漏洞操作（新增、验证等）的趋势图，单位为个。	-
漏洞类型趋势	流图	今日（整点）	每小时的各种漏洞类型（windows漏洞、Linux漏洞、Web漏洞等）的趋势图，单位为个。	-
漏洞状态趋势	流图	今日（整点）	每小时的各种漏洞状态（未修复、已修复）的趋势图，单位为个。	-
漏洞操作方式分布	环图	今日（整点）	各种漏洞操作（新增、验证等）的分布。	-
漏洞类型分布	环图	今日（整点）	各种漏洞级别（windows漏洞、Linux漏洞、Web漏洞等）的分布。	-

图表	类型	默认时间范围	描述	样例
漏洞状态分布	环图	今日（整点）	各种漏洞最新状态（未修复、已修复、修复失败等）的分布，注意：如果一台机器的一个漏洞有多个状态变化，取最新的状态归类。	-
新增漏洞Top10	环图	今日（整点）	在各个设备上新增最多的10个漏洞。	-
验证漏洞Top10	环图	今日（整点）	在各个设备上验证最多的10个漏洞。	-
修复漏洞Top10	环图	今日（整点）	在各个设备上修复最多的10个漏洞。	-
漏洞事件客户端Top20	表格	今日（整点）	前20个发生漏洞事件的设备，包括客户端、漏洞事件数、新增/验证/修复数、各种类别数等。	-

安全日志：基线中心

提供基线检查相关的全局视图，包括检查问题分布、新增/处理的趋势、状态等。

图表	类型	默认时间范围	描述	样例
相关客户端	单值比较	今日（整点）/同比昨日	发生基线问题的独立主机设备的个数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
新增基线	单值比较	今日（整点）/同比昨日	新增基线事件数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%

图表	类型	默认时间范围	描述	样例
验证基线	单值比较	今日（整点）/同比昨日	验证基线事件数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
高优先级基线	单值比较	今日（整点）/同比昨日	发生的高优先级的基线事件的个数，以及与昨日同时段比的一个百分比增加减少状况。	10个 增加10%
基线操作趋势	流图	今日（整点）	每小时的各种基线操作（新增、验证等）的趋势图，单位为个。	-
基线子类型趋势	流图	今日（整点）	每小时的各种基线子类型（系统账户安全、注册表等）的趋势图，单位为个。	-
基线状态趋势	流图	今日（整点）	每小时的各种基线状态（未修复、已修复）的趋势图，单位为个。	-
基线操作方式分布	环图	今日（整点）	各种基线操作（新增、验证等）的分布。	-
基线子类型分布	环图	今日（整点）	各种基线子类型（系统账户安全、注册表等）的分布。	-
基线状态分布	环图	今日（整点）	各种基线最新状态（未修复、已修复、修复失败等）的分布，注意：如果一台机器的一个基线有多个状态变化，取最新的状态归类。	-

图表	类型	默认时间范围	描述	样例
新增基线Top10	环图	今日（整点）	在各个设备上新增最多的10个基线。	-
验证基线Top10	环图	今日（整点）	在各个设备上验证最多的10个基线。	-
基线事件客户端Top20	表格	今日（整点）	前20个存在基线事件的设备，包括客户端、基线事件数、新增/处理、高中优先级数等。	-

安全日志：主机异常中心

提供主机异常事件相关的全局视图，包括检查问题分布、新增/处理的趋势、状态等。

图表	类型	默认时间范围	描述	样例
相关客户端	单值比较	今日（整点）/同比昨日	发生主机异常问题的独立主机设备的个数，以及与昨日同一时间相比的百分比增加/减少状况。	10个 增加10%
新增告警	单值比较	今日（整点）/同比昨日	新增主机异常事件数，以及与昨日同一时间相比的百分比增加/减少状况。	10个 增加10%
处理告警	单值比较	今日（整点）/同比昨日	处理的主机异常事件数，以及与昨日同一时间相比的百分比增加/减少状况。	10个 增加10%
高优先级告警	单值比较	今日（整点）/同比昨日	发生的严重的主机异常事件数，以及与昨日同时段比的百分比增加/减少状况。	10个 增加10%

图表	类型	默认时间范围	描述	样例
告警操作趋势	线图	今日（整点）	每小时各种主机异常操作（新增、处理等）的趋势图，单位为个。	-
告警操作方式分布	环图	今日（整点）	主机异常操作（新增、处理等）的分布。	-
告警级别趋势	流图	今日（整点）	每小时各种主机异常（验证、可疑、提醒等）趋势图，单位为个。	-
告警级别分布	环图	今日（整点）	各种主机异常级别（验证、可疑、提醒等）的分布。	-
告警状态趋势	流图	今日（整点）	每小时各种主机异常状态（未修复、已修复）趋势图，单位为个。	-
告警状态分布	环图	今日（整点）	每小时各种告警最新状态（未修复、已修复、修复失败等）的分布。如果一台主机的一个异常事件有多个状态变化，取最新的状态。	-
新增告警Top10	环图	今日（整点）	新增最多的10个主机异常事件。	-
处理告警Top10	环图	今日（整点）	处理最多的10个主机异常事件。	-
告警事件客户端Top20	环图	今日（整点）	存在主机异常事件数量排名前20的设备。	-

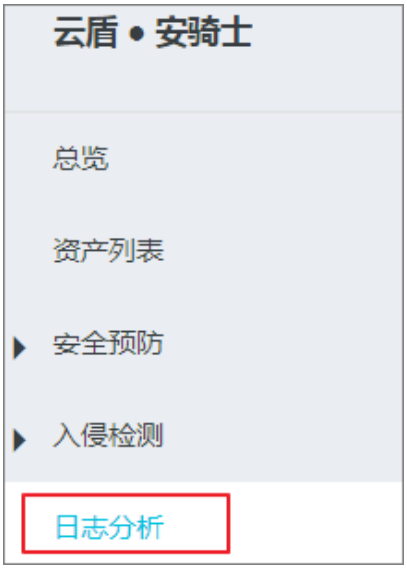
7.10 导出日志

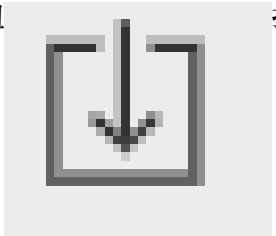
安骑士日志分析服务支持导出日志到本地。

您可下载本页日志（CSV格式）或全部日志（TXT格式）到本地。

操作步骤

1. 登录安骑士管理控制台。
2. 单击左侧导航栏的日志分析。



3. 单击原始日志列表右侧的下载日志按钮  打开日志下载对话框。

4. 在日志下载对话框中下载日志。

- 下载单页日志：

  单击下载本页日志以CSV格式将本页面的日志保存到本地。

- 下载所有日志：

  单击通过命令行工具下载所有日志下载所有日志。

a. 单击下载日志对话框中的命令行工具CLI用户手册，打开命令行安装说明页面。

b. 安装命令行工具。

c. 单击安全信息管理页面链接查看并复制当前用户的秘钥ID和KEY。

d. 单击复制命令行并用当前用户的秘钥ID和KEY替换该命令行中【步骤2中的秘钥ID】和【步骤2中的秘钥Key】。

e. 在CLI命令行工具中执行该命令。

命令执行后，安骑士全部日志将自动下载并保存到运行命令所在目录下的download_data.txt文件中。

7.11 高级管理

安骑士日志分析服务提供高级管理功能，您可使用高级管理功能进行告警与通知、实时订阅与消费、数据投递和对接其他可视化等高级操作。

操作步骤

1. 登录安骑士管理空控制台。
2. 单击左侧导航栏日志分析。
3. 单击日志分析页面右上角的高级设置按钮。

4. 在日志服务高级管理对话框中单击前往打开日志库控制台进行相关操作。

具体高级操作参见：

- 告警与通知
- 实时订阅与消费
- 数据投递
- 对接其他可视化

8 日志

8.1 功能介绍

日志功能尚处于 Beta 测试阶段。您需要升级到服务器安全（安骑士）企业版才能使用此功能。目前，企业版支持检索 30 天内的主机日志。

日志功能介绍

- 主机日志 SaaS 化
  - 无需安装或部署，通过浏览器登录安骑士管理控制台即可查询主机日志。
  - 支持 TB 级数据检索，及 50 种逻辑条件。
  - 秒级展示日志全文检索的结果。
- 主机日志集中化
  - 将散落在各系统中的主机日志进行集中管理。
  - 主机遇到问题时，一站式搜索定位问题根源。

功能特性

- 全 SaaS 化的日志检索平台，免安装和维护，即开即用
- 支持逻辑（布尔表达式）检索，目前支持 50 个维度的数据逻辑组合
- 秒级展示检索结果

可供检索的日志

日志来源	描述	功能上线时间
进程启动日志	主机上进程启动的相关信息	2017-9-27
网络连接日志	主机对外主动连接的日志	2017-9-27
登录流水	系统登录成功的日志记录	2017-9-27

说明:

各种日志源支持的字段信息请查看各日志源字段说明。

典型应用场景

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

8.2 查看和搜索日志

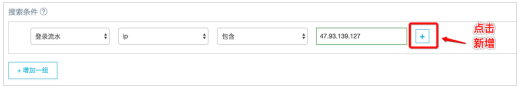
安骑士为用户提供全量日志采集和日志分析回溯，帮助您全面实时了解资产情况和快速定位问题根源。

操作步骤

1. 登录 云盾服务器安全#安骑士#管理控制台，单击日志检索，进入日志页面。

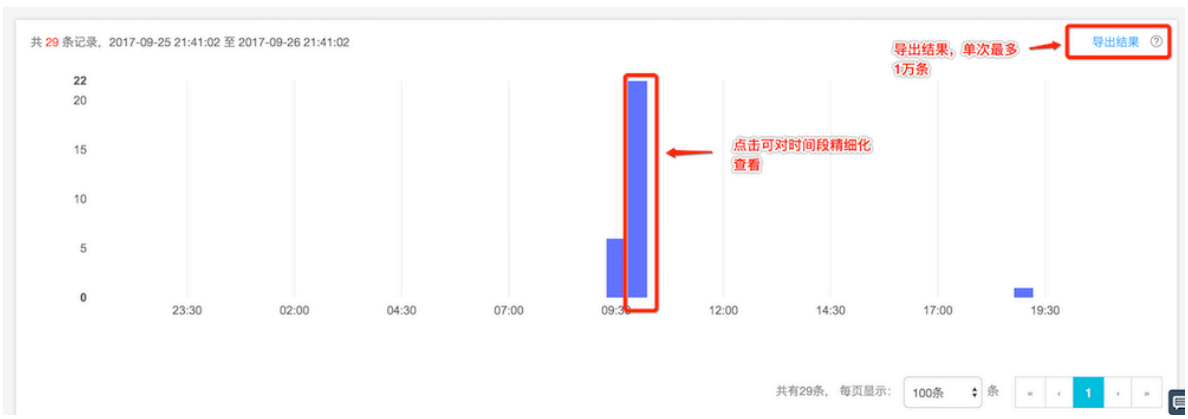
2. 选择日志源、需要检索的日志字段，输入您想要检索的关键词，单击搜索。

> **说明:**
> 您可以增加多条搜索条件，进行逻辑检索。



3. 根据您设置搜索条件，展示精细化的主机日志。同时，您可以在搜索结果中对各字段直接进行进一步检索。

4. 您可以根据细粒度的时间维度查看搜索结果，并单击日志列表右上角导出结果按钮将数据结果导出。



8.3 各日志源字段说明

日志功能尚处于 Beta 测试阶段。安骑士日志功能采集、并可检索的原始日志类型和字段说明如下表。

日志来源	描述	功能上线时间
进程启动日志	主机上进程启动信息	2017-9-27
网络连接日志	主机对外主动连接五元组信息	2017-09-27
系统登录流水	SSH、RDP登录成功日志	2017-09-27

各日志源字段列表

公共字段（以下每种日志类型都有这几个字段）	客户端编号
	IP地址
进程启动	进程ID
	用户组
	父进程ID
	用户ID
	用户名
	文件名
	父进程文件名
	命令行
	进程路径
	父进程路径
	启动时间
端口监听快照	监听端口
	监听IP
	进程路径
	进程ID
	进程名
	协议
	数据获取时间
网络连接	源IP

公共字段（以下每种日志类型都有这几个字段）	客户端编号
	IP地址
	源端口
	进程路径
	目标端口
	进程名
	目标IP
	状态
	协议
	连接时间
账号快照数据	是否拥有root权限
	home目录
	密码到期提醒时间
	用户属于的组
	最后一次登录的ip地址
	密码最后修改时间
	linux的shell命令
	windows域
	登录的终端
	账号超期时间
	密码超期时间
	最后登录时间
	用户
	用户状态：0-禁用、1-正常
	数据获取时间
进程快照数据	进程路径
	进程启动时间
	用户ID
	命令行
	父进程名
	进程名

公共字段（以下每种日志类型都有这几个字段）	客户端编号
	IP地址
	进程ID
	用户名
	进程文件MD5值，超过1MB不计算
	数据获取时间
登录流水	登录来源IP
	登录端口
	登录用户名
	登录类型
	登录次数
	登录时间
暴力破解	攻击来源IP
	破解端口
	破解用户名
	类型
	破解次数
	破解时间

8.4 语法逻辑说明

日志功能尚处于 Beta 测试阶段。多条搜索条件之间支持下表中的语法逻辑。

逻辑名称	描述
and	双目运算符。形式为`query1 and query2`，搜索结果展示`query1`和`query2`查询结果的交集。
or	双目运算符。形式为`query1 or query2`，搜索结果展示`query1`和`query2`查询结果的并集。

逻辑名称	描述
not	双目运算符。形式为`query1 not query2`，搜索结果展示符合`query1`并且不符合`query2`的结果，相当于`query1-query2`。如果只有`not query1`条件，将从全部日志中选取不包含`query1`的结果进行展示。

说明:

语法关键词不区分大小写。

9 网页防篡改

9.1 概述

网络攻击者通常会利用被攻击网站中存在的漏洞，通过在网页中植入非法暗链对网页内容进行篡改等方式，进行非法牟利或者恶意商业攻击等活动。网页被恶意篡改会影响用户正常访问网页内容，还可能会导致严重的经济损失、品牌损失甚至是政治风险。

安骑士企业版支持网页防篡改功能，可实时监控网站目录并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入恐怖威胁、色情等内容。

说明:

- 包年包月企业版开通网页防篡改功能后可使用该功能；安骑士按量付费企业版暂不支持网页防篡改功能。
- 基础版用户开通网页防篡改服务的同时需要购买安骑士企业版。

9.2 开通服务

网页防篡改功能为增值服务，需单独购买，费用为980元/台/月。使用网页防篡改功能前需要先购买开通该服务。

背景信息

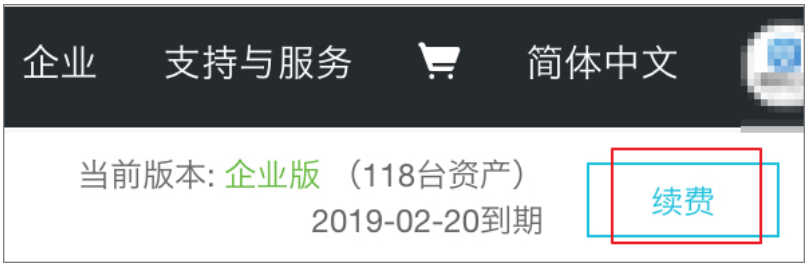
说明:

- 包年包月企业版开通网页防篡改功能后可使用该功能；安骑士按量付费企业版暂不支持网页防篡改功能，具体需求请提交工单。
- 基础版用户开通网页防篡改服务的同时需要购买安骑士企业版，费用为60元/台/月。

操作步骤

1. 登录云盾服务器安全#安骑士#管理控制台。

2. 单击控制台总览页面右上角的续费进入安骑士包年包月购买页面。



3. 在安骑士包年包月购买页面网页防篡改区域框单击开启。

4. 选择您所需开启网页防篡改服务的服务器数量。

5. 在订购时长区域框向右拖动滑块选择需要的订购时间范围。

订购时长在1年以上折扣优惠信息见当前购买页面右侧配置费用区域。

6. 单击立即购买并完成支付。

> **说明:**
> 如果对服务器开启网页防篡改保护的时候提示开启机器数已到上限，您需要在安骑士控制台网页防篡改页面右上角单击扩大授权扩充授权网页防篡改的服务器数量。详细信息参见扩充授权数。

9.3 开启网页防篡改保护

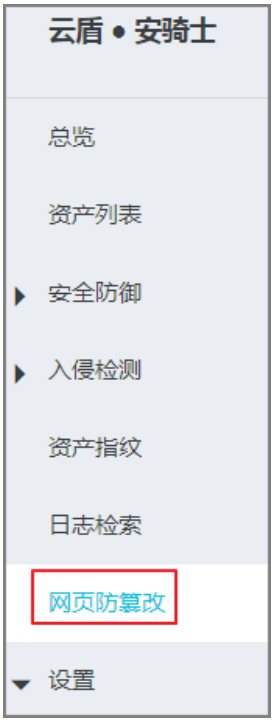
安骑士企业版可对主机开启网页防篡改防护，全面保护您网站的安全。

> **说明:**
> 在网页防篡改页面添加主机后，主机的网页防篡改防护是默认关闭状态的。您需要开启目标主机的防护状态，网页防篡改功能才会生效。详见步骤三 开启防护。

步骤一 添加主机

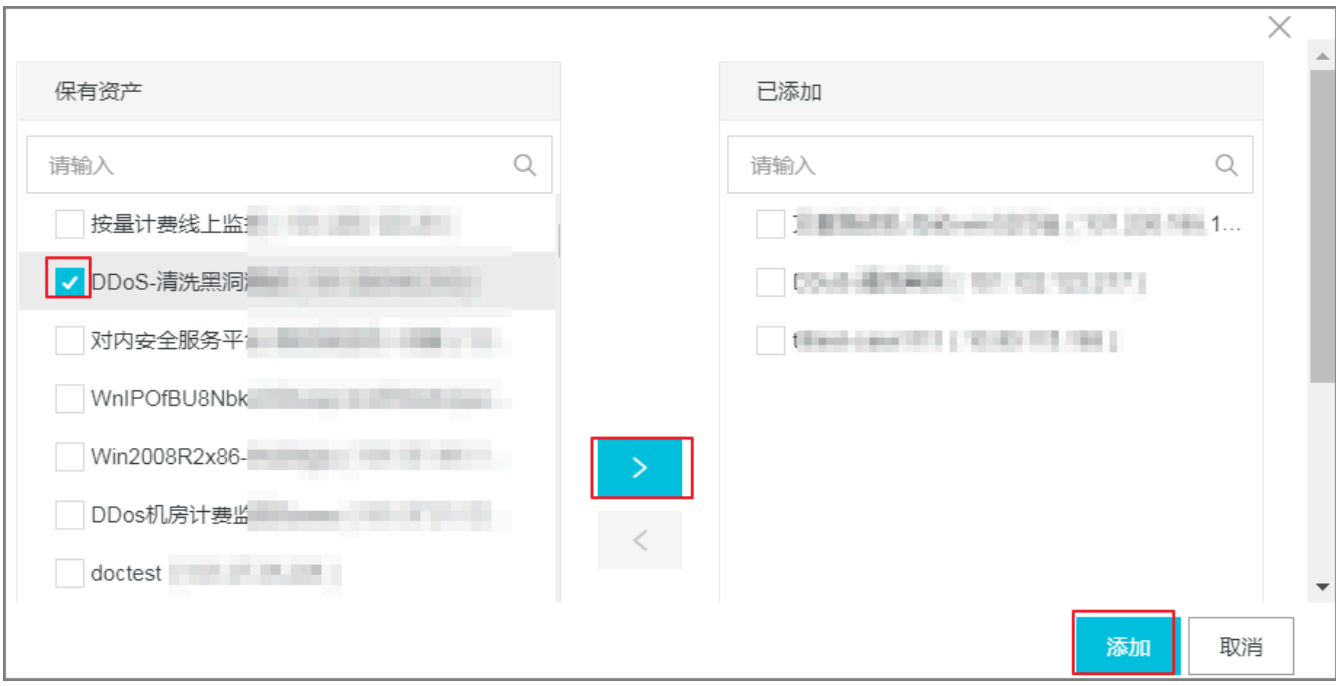
1. 登录云盾服务器安全#安骑士#管理控制台。

2. 在左侧导航栏单击网页防篡改。



3. 在网页防篡改页面单击左上角添加主机。

4. 在添加主机对话框中勾选目标主机，单击 按钮将目标主机添加到右侧的已添加列表中。

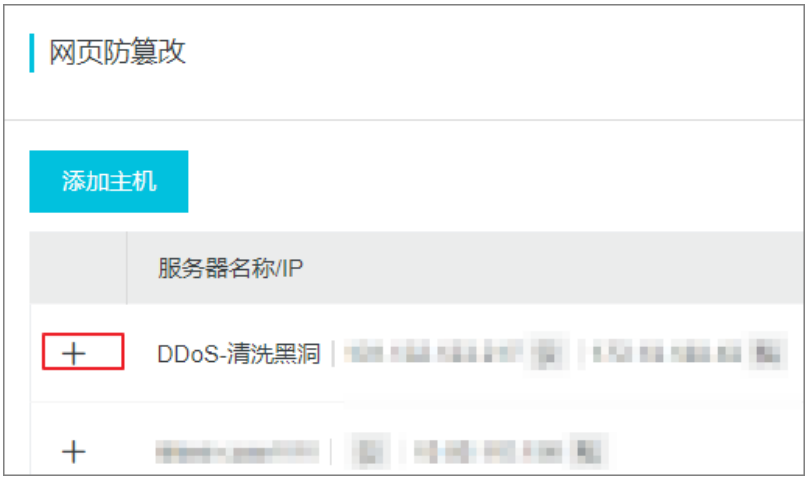


5. 单击对话框右下角的添加，将目标主机添加到网页篡改防护列表中。

> **说明:**
> 添加主机后，主机的网页防篡改防护是默认关闭状态的。您需要在网页防篡改页面开启目标主机的防护状态。

步骤二 添加防护目录

1. 在网页防篡改页面单击目标服务器左侧的 按钮打开防护目录列表。



2. 单击添加打开添加防护目录对话框。

3. 配置添加防护目录对话框。

- 防护目录：需要开启网页防篡改的目录地址。可以手动输入防护目录，也可以在下拉列表中选择目标目录。
- 排除子目录：无需开启网页防篡改的子目录地址。手动输入，多个目录之间用半角分号隔开。
- 排除文件类型：无需进行网页防篡改检测的文件名称。手动输入，多个文件类型之间用半角分号隔开。
- 本地备份目录：显示默认的本地备份目录地址。建议不要修改本地备份目录。

说明：

- 添加的目录都必须是包含文件的、真实和独立存在的目录。
- 两个防护目录不可以互为备份目录。

4. 单击确定，保存防护目录配置。

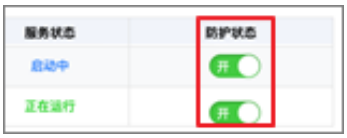
说明：

- 每台服务器最多可添加10个防护目录。
- Window系统单个防护目录大小不超过20G；单个防护目录下的文件夹个数不超过20000个；防护目录文件夹层级不超过20个；单文件大小不超过3MB。Linux系统单个防护目录大小不超过20G；单个防护目录下的文件夹个数不超过3000个；防护目录文件夹层级不超过20个；单文件大小不超过3MB。
- 建议您开启防护前检查文件夹目录层级、文件夹个数和防护目录大小是否超过限制。

- 建议您排除 log、png、jpg、mp4、avi、mp3等无需进行防护的文件类型（多个文件类型之间用分号隔开）。
- 如需删除不必进行网页防篡改检测的目录，可在防护目录列表页面单击目标目录最右侧删除，删除该防护目录及配置信息。

步骤三 开启防护

1. 在网页防篡改页面单击目标主机最右侧防护状态下的开关，开启防护服务。



首次开启防护时，目标主机的服务状态将会显示为启动中。请耐心等待数秒，启动成功后服务状态将会显示为正在运行。

说明:
当防护服务状态为异常时，在目标主机服务状态栏单击异常，显示异常状态的详细原因并单击重试。详见防护异常状态处理。

防护异常状态处理

服务状态	说明	建议
启动中	网页防篡改防护状态正在开启。	首次开启防护时，目标主机的服务状态将会显示为启动中。请耐心等待数秒。
正在运行	防护状态已成功开启，并正常运行中。	-

服务状态	说明	建议
异常	防护开启异常。	在目标主机服务状态栏单击异常，查看发生异常的原因并重试。详细原因参见防护异常状态处理。
未启动	防护状态为未开启。	需将防护状态设置为开。

网页防篡改防护开启发生异常时，您需要在入侵检测 > 主机异常页面对异常事件进行查看和处理。

操作步骤

1. 登录云盾服务器安全#安骑士#管理控制台。
2. 在左侧导航栏单击入侵检测 > 主机异常。

3. 在主机异常页面事件分类区域单击网页防篡改打开网页防篡改事件列表。

4. 单击目标服务器右侧操作栏的查看打开异常事件的详情页面，根据页面的解决方案进行处理。

5. 异常事件处理完成后，在网页防篡改页面单击右侧服务状态栏目标服务器的状态信息，单击重试。

9.4 扩充授权数

开启每台服务器的网页防篡改功能就会消耗1个网页防篡改授权数（网页防篡改服务器台数）。您可在网页防篡改页面右上角查看您已购买的授权数和已使用的授权数。

背景信息

如果需要开启网页防篡改的服务器数量大于已购买的服务器台数，网页防篡改页面会提示开启机器数已到上限。您需要扩充授权网页防篡改的服务器数量。

操作步骤

1. 登录云盾服务器安全#安骑士#管理控制台。
2. 在左侧导航栏单击网页防篡改。

3. 在网页防篡改页面右上角单击扩充授权。

4. 在变配页面选择需要新增授权服务器的数量。

5. 勾选右下角的服务协议并完成支付。

10 设置

10.1 安装/卸载

安骑士Agent插件安装/卸载操作详见安装Agent、卸载Agent。

10.2 告警配置

安骑士企业版通过短信、邮件或站内信的方式提供告警通知的功能。

告警通知界面如下图所示：

通知项目	发送规则	发送频率	通知方式	通知时间
漏洞管理	以周报发送，存在还未处理的漏洞	每7天提醒一次	短信 邮件 站内信	每周一发送
基线检查	以周报发送，存在还未处理的基线风险	每7天提醒一次	短信 邮件 站内信	每周一发送
主机异常	高危及以上的可疑安全事件（含云查杀）	单台ECS一天最多1条 单账号一天最多5条	短信 邮件 站内信	24小时 仅8:00-20:00

您可通过控制台 > 设置 > 告警配置来查看资产的告警通知发送规则、发送频率、通知方式和通知时间，并配置通知方式和通知时间。

> 说明：
> 企业版用户才可以接收通知或配置告警通知方式和通知时间；基本版用户如需接收告警通知或配置告警方式和通知时间请先升级至企业版。

漏洞管理

对未处理的漏洞进行通知。

通知发送频率：每周一通知一次。

基线检查

对未处理的基线风险进行通知。

通知发送频率：每周一通知一次。

主机异常

对高危以上的可疑安全事件（含云查杀）进行通知。

通知发送频率：单台ECS每天最多1条通知；单个账号每天最多5条通知。

通知方式

通过控制台 > 设置 > 告警配置来设置您需要的以下通知方式：

- 短信
- 邮件
- 站内信（控制台站内信）

通知时间

通过控制台 > 设置 > 告警配置来设置以下通知时间：

- 24小时
- 仅8:00-20:00

说明：
仅主机配置项可设置告警时间。

10.3 安全配置

10.3.1 登录IP拦截加白

设置登录IP拦截加入白名单

为避免安骑士对您的正常登录行为进行拦截（例如，多次输入密码错误；或办公网采用统一 IP 作为出口的环境中，多次输入密码错误触发的误拦截等），您可将此类 IP 添加至登录IP拦截白名单中。加入白名单后，安骑士暴力破解拦截功能将不会对来自登录 IP 白名单中的 IP 登录行为进行拦截。

操作步骤

1. 登录云盾服务器安全#安骑士#管理控制台。

2. 定位到设置 > 安全配置，在安全配置页面单击登录IP拦截加白选项右侧的点此设置，打开访问白名单页面。

3. 在访问白名单页面单击白名单列表右上角的添加，打开添加对话框。

4. 在源IP输入框中输入访问来源IP地址。

说明:

设置某源IP加入访问白名单后，该IP对您加入白名单的主机访问将不受任何限制，请谨慎操作。

5. 选中需要添加到登录IP拦截白名单中的主机IP地址，单击移动按钮将该主机添加到已选区域。

说明:

如果您希望新购的资产自动添加到登录IP拦截白名单中，可勾选当有新主机购入时，自动共享当前设置选项。该设置将于一天后生效。

6. 单击确认，安骑士暴力破解功能将不再对您选定的IP地址登录行为进行拦截。

取消登录IP拦截白名单设置

如果您需要对主机解除登录IP拦截白名单设置，可单击访问白名单页面操作栏的失效按钮，对目标IP取消登录IP拦截加白的设置。

失效操作支持批量处理。

10.3.2 病毒自动隔离

安骑士企业版病毒自动隔离（即病毒自动查杀）功能为您提供精准防御能力。目前已支持主流勒索病毒、DDOS木马、挖矿和木马程序、恶意程序、后门程序和蠕虫病毒等类型。

所有支持自动隔离的病毒都经过了阿里云安全专家的测试和验证，确保零误杀。建议您启用该功能，加固主机安全防线。

说明:

- 病毒自动隔离服务只有在安骑士企业版中才提供；基础版用户需升级至企业版才可使用病毒自动隔离功能。企业版和基础版功能差异详见功能详情列表。
- 开启病毒自动隔离功能后，安骑士中新购的服务器将默认自动开启该功能。

风险说明

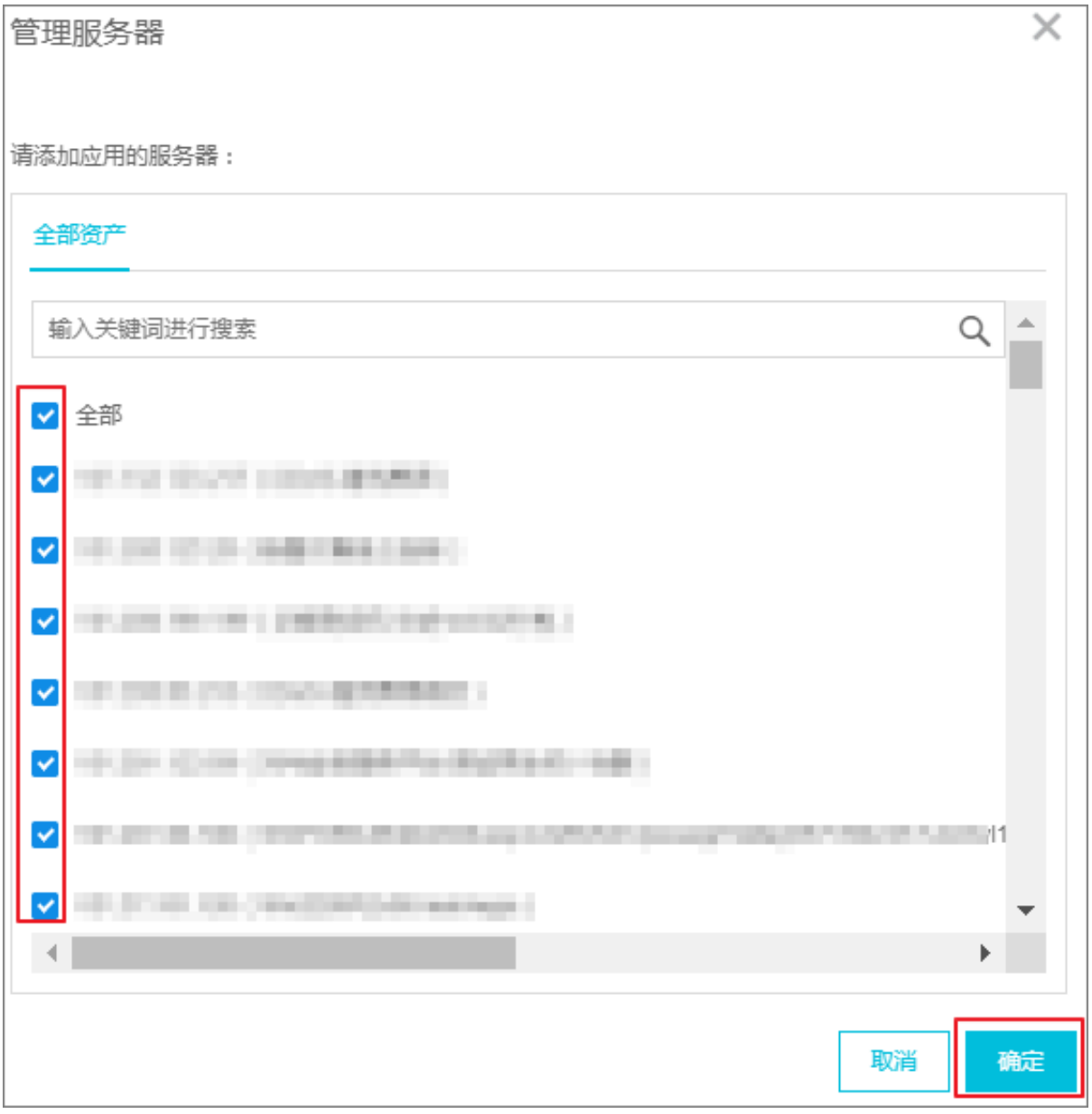
- 安骑士实时自动更新病毒库，但为保证对用户业务影响降到最低，所有支持自动隔离的病毒和路径都会经过查杀引擎验证后才会执行，保证隔离准确性。
- 病毒自动隔离服务开通后，可能会存在部分程序误报或未隔离成功的情况。

  误报的事件和从文件隔离箱中恢复。

  您可在安骑士控制台主机异常功能中对未隔离成功的病毒进行手动隔离。

操作步骤

1. 登录安骑士管理控制台。
2. 在左侧导航栏单击设置 > 安全配置，打开安全配置页面。
3. 在病毒查杀模块单击管理，打开管理服务器对话框。



4. 在管理服务器对话框中勾选服务器并单击确定/取消，对服务器开启/关闭病毒自动隔离功能。

   注意：

   管理服务器对话框打开后默认勾选您的所有资产。

   您可在对话框中通过关键词搜索单个资产名称或勾选单个资产对单个资产开启自动隔离。建议对全部资产开启病毒自动隔离服务。