

安骑士

用户指南

用户指南

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。

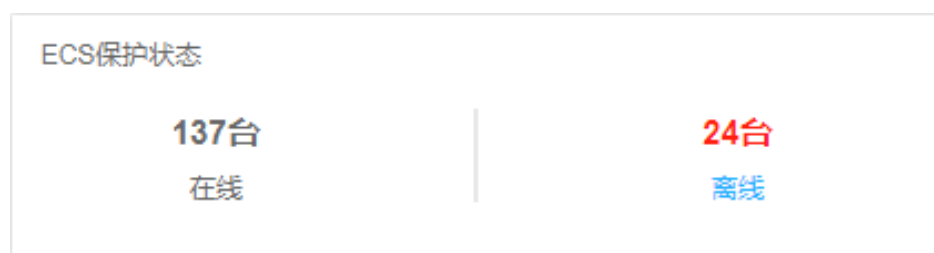
待处理的告警事件数量

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，点击**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

弱点

类型: ☒ 漏洞 ☒ 基线

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

点击**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。

注意：不支持同时取消勾选**漏洞**和**基线**。

TOP弱点主机

TOP弱点主机

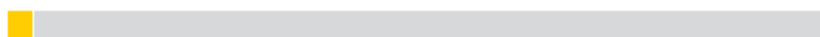
47.93.139.32

17个



30个

59.110.115.63



30个

47.88.27.166



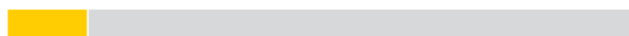
30个

139.196.201.93



24个

47.89.177.108



23个

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：

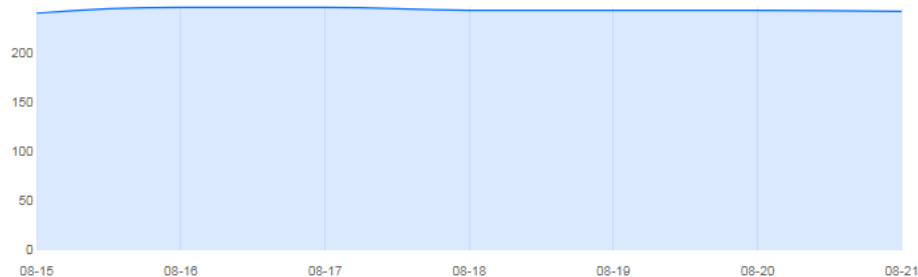
- **红色**：高危弱点
- **黄色**：中危弱点
- **灰色**：低危弱点

事件类型

事件

类型: ☒ 异常登录 ☒ 网站后门 ☒ 主机异常

入侵事件趋势



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：

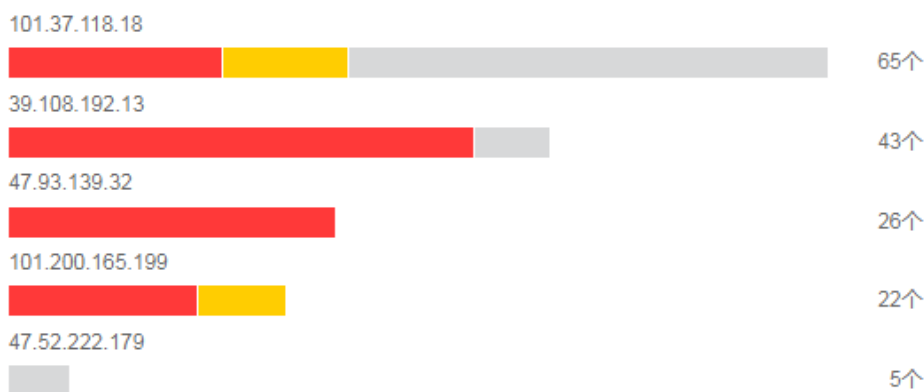
- 异常登录
- 网站后门
- 主机异常

点击事件右侧的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。

注意：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

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

最近重要弱点和事件

【待处理】 2018-08-22 11:43:38

【101.37.118.18 (yundi nessus) 】

主机异常: Windows新增自启动项

【待处理】 2018-08-22 11:30:09

【39.108.192.13 (CentOS6.8x64-testAegis) 】

主机异常: Windows异常帐号创建

【待处理】 2018-08-22 11:30:09

【39.108.192.13 (CentOS6.8x64-testAegis) 】

主机异常: Windows异常帐号创建

【待处理】 2018-08-22 11:30:09

【39.108.192.13 (CentOS6.8x64-testAegis) 】

主机异常: 反弹Shell

【待处理】 2018-08-22 11:30:09

【39.108.192.13 (CentOS6.8x64-testAegis) 】

主机异常: 挖矿进程

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。

点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。

Agent 插件

Agent说明

工作原理

安骑士 Agent 每隔五个小时会主动向安骑士服务器端上报一次在线数据信息。

如果安骑士 Agent 没有按时上报在线信息，安骑士服务器端则在 12 小时后判定该服务器不在线，且在安骑士管理控制台中此服务器的保护状态显示为离线。

相关进程

安骑士 Agent 包含以下两个主要进程：

说明：安骑士 Agent 的进程在 Linux 系统的服务器上以 root 帐号运行，在 Windows 系统的服务器上以 system 帐号运行。

AliYunDun

此进程主要用于与安骑士服务器建立连接。

进程文件所在路径：

- **Windows 32位系统：** C:\Program Files\Alibaba\aeis\aeis_client
- **Windows 64位系统：** C:\Program Files (x86)\Alibaba\aeis\aeis_client
- **Linux 系统：** /usr/local/aeis/aeis_client

AliYunDunUpdate

此进程主要用于定期检测安骑士Agent是否需要升级。

进程文件所在路径：

- **Windows 32 位系统：** C:\Program Files\Alibaba\aeis\aeis_update
- **Windows 64 位系统：** C:\Program Files (x86)\Alibaba\aeis\aeis_update
- **Linux 系统：** /usr/local/aeis/aeis_update

资源占用

安骑士 Agent 仅占用您的服务器非常少的资源：

- **普通状态：** 安骑士 Agent 占用约 1% CPU及 50 MB 内存。

峰值状态： 安骑士 Agent 占用不超过 10% CPU 及 80 MB 内存。

注意： 如果占用资源超过此峰值，安骑士 Agent 将会暂停工作。

安装Agent

服务器安全（安骑士）Agent 插件已集成于公共镜像中。如果您在购买 ECS 实例时选择公共镜像并选择启用 **安全加固** 选项的话，安骑士 Agent 插件一般都已经默认安装在镜像中。



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。

手动安装（支持非阿里云服务器）

注意：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。

注意：安装前请确认您安装安骑士服务器的环境：

1. 服务器在阿里云上，直接安装即可
2. 服务器不在阿里云上，服务器与阿里云通信走internet通信，安装后如果出现离线情况请参考：[离线排查](#)

服务器不在阿里云上，服务器与阿里云通过专线连接走内网通信，需要修改您的DNS配置，指定安骑士服务端DNS 解析地址：

106.11.68.13 jsrv.aegis.aliyun.com

106.11.250.224 update.aegis.aliyun.com

登录 云盾服务器安全（安骑士）管理控制台，单击 **设置**。

单击 **安装安骑士** 进入安装安骑士 Agent 页面。



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

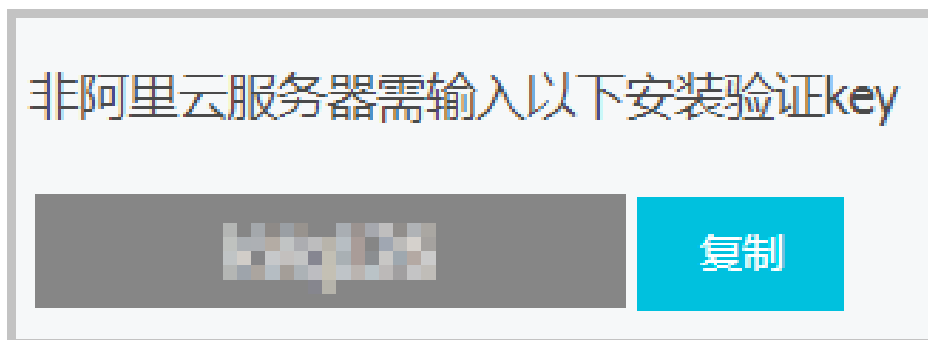
在安装安骑士 Agent 页面，单击 **点击下载** 下载最新版本安骑士 Agent 插件安装文件到本地计算机。

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。

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，完成安装。

注意：安骑士 Agent 插件安装过程中可能会提示您输入安装验证 Key。该安装验证 Key 将用于关联您的阿里云账号，在云盾服务器安全（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。

您可在云盾安装安骑士页面找到您的安装验证 Key。



Linux 系统

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**。

以管理员身份登录您的 Linux 服务器。

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。

执行安装命令即可完成安骑士Agent插件的下载及安装。

注意：该安装命令包含从阿里云站点下载最新的安骑士 Agent 插件，请确认您的服务器已连接公网。

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。关于安骑士 Agent 进程说明，请参考 [Agent说明](#)。

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。

注意：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

Agent 离线排查

如果您的安骑士 Agent 处于离线状态，请按照以下步骤进行排查：

登录您的服务器查看安骑士 Agent 相关进程是否正常运行。

如果安骑士 Agent 相关进程无法运行，建议重启您的服务器，或者参考 [安装Agent](#) 重新装安骑士 Agent。

Windows 系统

在任务管理器中查看相关进程是否正常运行。

映像名称	用户名
AliYunDun.exe	SYSTEM
AliYunDunUpdate.exe	SYSTEM

Linux 系统

执行如top命令查看相关进程是否正常运行。

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

如果首次安装安骑士 Agent 的服务器在安装完成后显示安骑士状态不在线，请尝试参考以下方式重新启动安骑士 Agent：

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

注意：将命令中的xx替换为该目录下的最大的数字。

Windows 系统： 在服务项中重新启动以下两个个服务项，选中该服务右键点击重新启动即可。



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、云外机器）

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

服务器无公网 IP（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命令。
- **Linux 系统：** 执行ping jsrv3.aegis.aliyun.com -s 1000命令。

如果解析不通，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。

注意： 请将下列 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。

- 140.205.140.0/24 Port: 80
- 106.11.68.0/24 Port: 80
- 106.11.248.0/24 Port: 80 443
- 106.11.250.0/24 Port: 80 443
- 100.100.25.0/24 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：

在您服务器的 hosts 文件添加以下域名解析记录：

- a. 100.100.25.3 jsrv.aegis.aliyun.com
- b. 100.100.25.4 update.aegis.aliyun.com

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

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

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、h_srv_domain对应的值分别修改为 100.100.25.3 及 100.100.25.4。修改完成后，重启安骑士 Agent 进程。

注意： 修改前请务必备份 network_config 配置文件。

此方法只适用于公网带宽为零且安骑士 Agent 离线的服务器情况。

如果 Ping 命令执行解析成功，再次尝试通过 Telnet 命令连接解析出的域名 IP 的 80 端口（例如，执行telnet 140.205.140.205 80命令），查看是否连通。如果无法连通，请确认防火墙是否存在相关限制。

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。

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。

卸载Agent

如果您决定不再使用云盾服务器安全（安骑士）服务的所有功能，您可以选择以下方式进行卸载安骑士 Agent。

注意： 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。

自动卸载安骑士 Agent

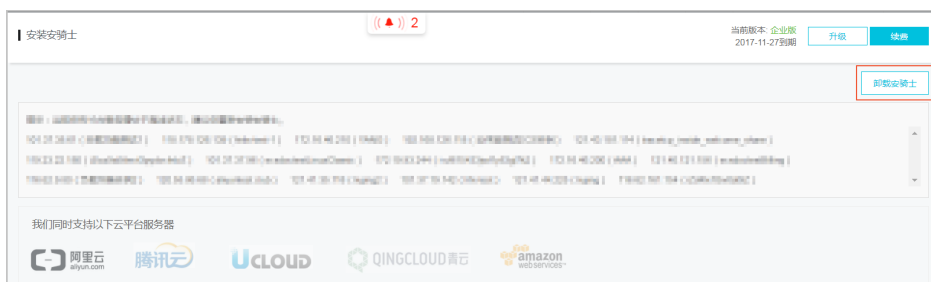
您可以通过以下方式在云盾服务器安全（安骑士）管理控制台中自动卸载安骑士 Agent：

注意：通过该种方式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）。

登录 云盾服务器安全（安骑士）管理控制台，单击 **设置**。

单击 **安装安骑士**，进入安装安骑士 Agent 页面。

单击页面右上方的 **卸载安骑士**。



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，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。

手动卸载安骑士 Agent

您也可以参考以下步骤手动卸载您服务器上的安骑士 Agent。

Linux 系统服务器

1. 登录您的 Linux 系统服务器。

执行以下命令下载安骑士 Agent 卸载脚本。

```
wget http://update.aegis.aliyun.com/download/uninstall.sh
```

依次执行以下命令卸载安骑士 Agent。

```
- chmod +x uninstall.sh  
- ./uninstall.sh
```

Windows系统服务器

登录您的 Windows 系统服务器。

在您的服务器上下载 安骑士 Agent 卸载脚本。

注意：您也可以将安骑士 Agent 卸载脚本文件下载至本地计算机后，通过 FTP 文件传输工具将脚本文件上传至您的服务器后执行卸载。

双击 uninstall.bat 文件执行脚本卸载安骑士 Agent。

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

登录 云盾服务器安全（安骑士）管理控制台。

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。

资产列表

3

当前版本：企业版
2017-11-27到期

续费

服务器IP名称

搜索

分组排序

所有资源 11台

test2 3台

test7 7台

test1 5台

test3 2台

未分组 1台

共11台，在线4台，离线7台立即安装

服务器IP名称	操作系统 (全部)	地域 (全部)	保护状态 (全部)	漏洞 (全部)	基线 (全部)	异常登录 (全部)	网站后门 (全部)	主机异常 (全部)
192.168.1.100	linux	华南 1	离线	无	无	无	无	无
192.168.1.101	linux	华东 2	离线	无	无	无	无	无
192.168.1.102	linux	华东 2	离线	38	2	无	无	无
192.168.1.103	linux	华东 2	离线	25	2	无	无	无
192.168.1.104	linux	华东 2	离线	26	2	无	无	无
192.168.1.105	linux	华东 1	在线	无	4	无	无	无
192.168.1.106	windows	华东 1	在线	无	2	无	无	无

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。



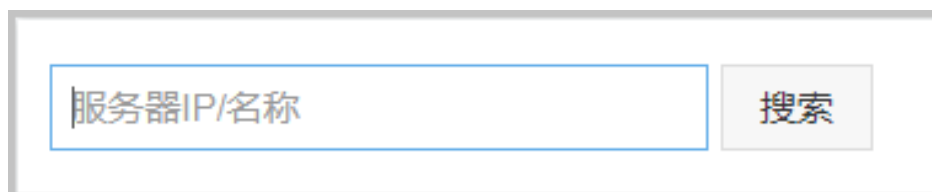
注意：目前，最多可支持三级资产子分组。

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。

注意：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。

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。

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。



漏洞管理

Web-CMS漏洞

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

、快速修复的功能。Web-CMS 漏洞管理功能可以帮助您解决漏洞发现不及时、不会修复漏洞、无法批量进行补丁更新等诸多问题。

注意： 安骑士基础版只提供 Web-CMS 漏洞检测功能；漏洞修复功能需要您升级到安骑士企业版才能使用。

漏洞检测原理

Web-CMS 漏洞功能通过您服务器上的安骑士 Agent 的漏洞扫描和下发更新功能，每天随机进行一次漏洞扫描检测。如果发现您的服务器上存在漏洞，会上报至 服务器安全（安骑士）管理控制台 > 弱点 > 漏洞管理 > Web-CMS漏洞 页面，并为您推送漏洞告警信息。

说明： 同一服务器上的同一漏洞只会在首次发现时为您推送告警信息。当遇到重大漏洞爆发的情况，安骑士将为您多次推送告警信息提示您尽快修复该漏洞。

漏洞修复原理

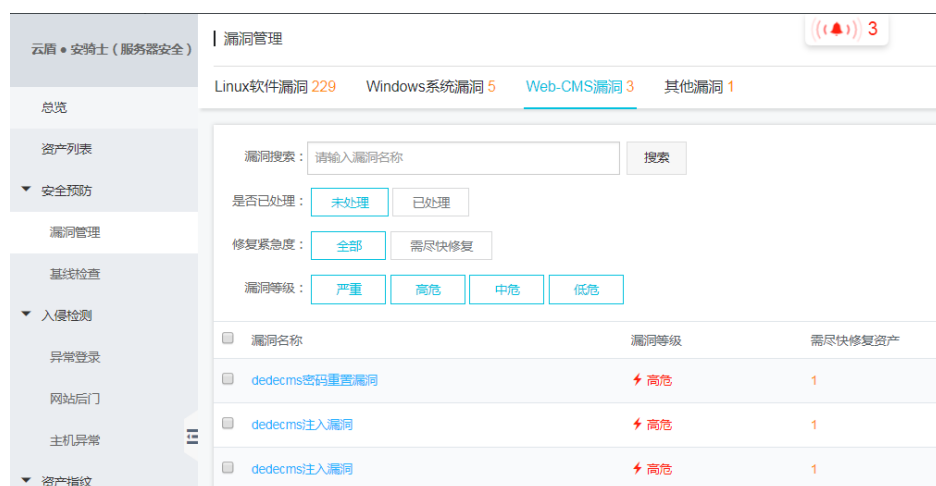
安骑士通过识别存在漏洞的通用 Web 文件的 MD5 值，替换存在漏洞的文件，实现 Web-CMS 漏洞修复。

注意： 如果您服务器上的某些漏洞已经通过手工进行修复，存在漏洞文件的 MD5 值可能没有改变，安骑士仍然会提示您的服务器上存在这些漏洞。这种情况下，请在安骑士管理控制台的 Web-CMS 漏洞管理页面忽略这些漏洞。

操作步骤

登录 云盾服务器安全（安骑士）管理控制台。

单击 **漏洞管理**，选择 **Web-CMS漏洞**。



单击漏洞名称，可查看该漏洞的详细信息。

单击 **查看详情**，可进入漏洞处理页面进行漏洞处理。



- 单击 **修复**，安骑士将通过替换您服务器上存在漏洞的 Web 文件修复 Web-CMS 漏洞。
注意： 修复 Web-CMS 漏洞前，建议您备份该漏洞相关的 Web 文件。您可参考漏洞处理页面说明栏中的路径，对相关的 Web 文件进行备份。
- 单击 **忽略**，您可忽略该漏洞，安骑士将不再上报并告警此服务器上的这个漏洞。
- 手动修复漏洞后，您可以单击 **验证**，一键验证该漏洞是否已修复成功（如果您未进行手动验证，漏洞修复成功后 48 小时内安骑士会进行自动验证）。
- 对于已修复完成的漏洞，单击 **回滚** 可进行漏洞回滚，将原来的 Web 文件进行还原。

漏洞状态说明

状态	说明
未修复	您的服务器存在 Web-CMS 漏洞需要更新，可一键修复该漏洞（若漏洞的最后发现时间大于七天，建议您先进行漏洞验证，可能该漏洞已不存在）。
修复中	漏洞正在修复中，可能由于异常原因阻断，最长修复时间为 10 分钟。
修复成功	漏洞被成功修复。
修复失败	漏洞修复失败，失败原因可能有多种，请参考 漏洞修复失败可能原因 进行排查。
漏洞文件不存在	存在漏洞的 Web 文件可能已被删除。
回滚成功	已恢复到漏洞未修复的状态。若您未修复该漏洞，周期扫描检测会在第二天再次向您提示该漏洞告警信息。
回滚失败	回滚失败，失败原因可能有多种，请参考 漏洞管理回滚操作失败可能原因 进行排查。
已忽略	漏洞被忽略后，安骑士将不再向您提示该漏洞的告警信息。
文件已修改	存在漏洞的文件已被修改，系统会暂时判定该漏洞文件已不存在。若您未修复该漏洞，周期扫描检测会在第二天再次向您提示该漏洞告警信息。

软件漏洞

系统软件漏洞功能支持检测并修复您服务器上的两大类软件漏洞：

注意： 您需要升级到服务器安全（安骑士）企业版才能使用此功能。

一、Linux软件漏洞（CVE 漏洞）

服务器安全（安骑士）订阅 CVE 官方漏洞源，通过收集和识别您服务器上安装的软件版本信息，为您提供系统软件漏洞的检测。系统软件漏洞功能可检测出您服务器上的 Vim、Bind、及 OpenSSL 等软件漏洞。

检测原理： 通过判断服务器上安装的软件版本是否存在漏洞，并为您推送漏洞消息。

检测周期： 每两天进行一次自动检测（若遇到重大软件漏洞爆发，安骑士会及时对您的服务器进行检测并第一时间为您推送漏洞消息）。

注意： 当前系统软件类型的漏洞无法进行“一键修复”，请按照安骑士提供的修复命令尝试进行修复。修复完成后，可通过安骑士提供的“验证”功能，快速验证漏洞是否修复成功。

操作步骤

登录 云盾服务器安全（安骑士）管理控制台。

单击 **漏洞管理**，选择 **软件漏洞**。



单击 **漏洞分类**，选择 **系统软件漏洞**。

单击漏洞名称，可查看该漏洞的详细信息。
关于漏洞的详细信息参数，请参考 系统软件漏洞各参数说明。

漏洞名称	漏洞等级(全部)	漏洞分类(全部)	最后发现时间	受影响资产数/未处理数	操作
RHSA-2017-0933: kernel security, bug fix, and enhancement update (Important)	高危	系统软件漏洞	2017-09-05 01:17:15	2台 / 2台	查看详情
RHSA-2017-1615: kernel security and bug fix update (Important)	高危	系统软件漏洞	2017-09-05 01:17:15	2台 / 2台	查看详情
RHSA-2016-1025: pcrc security update (Important)	高危	系统软件漏洞	2017-09-05 01:17:15	2台 / 2台	查看详情
RHSA-2017-1095: bind security update (Important)	中危	系统软件漏洞	2017-09-05 01:17:15	2台 / 2台	查看详情
RHSA-2017-1615: kernel security and bug fix update (Important)					×
CVE-2017-2583 高危 CVE-2017-6214 高危 CVE-2017-7477 中危 CVE-2017-7645 高危 CVE-2017-7895 高危					
标题: Linux Kernel权限提升漏洞 (CNVD-2017-01069) CVSS分值: 4.6 CVSS: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H					
披露时间: 2017-02-06 00:00:00 利用难度: LOW POC公开时间: 2017-05-30 06:25:21					
CVEID: CVE-2017-2583					
简介: The load_segment_descriptor implementation in arch/x86/kvm/emulate.c in the Linux kernel before 4.9.5 improperly emulates a "MOV SS, NULL selector" instruction, which allows guest OS users to cause a denial of service (guest OS crash) or gain guest OS privileges via a crafted application.					
解决方案: 请直接在该漏洞处理页面，选择对应服务器和漏洞，生成修复命令后，登录到服务器上运行即可。					
相关链接: git.kernel.org www.kernel.org www.openwall.com www.securityfocus.com bugzilla.redhat.com github.com					

单击 **查看详情**，可进入漏洞处理页面进行漏洞处理。

- 单击 **生成修复命令**，安骑士自动生成修复漏洞的指令。您可登录您的服务器运行该指令进行漏洞修复。如果生成的修复命令为空，请参考 **系统软件漏洞修复命令为空** 进行排查。
注意： 在修复系统软件漏洞时，建议您参考 **系统软件漏洞修复最佳实践** 中的方法进行修复。
 - 单击 **忽略**，您可忽略该漏洞，安骑士将不再上报并告警此服务器上的这个漏洞。
 - 手动修复漏洞后，您可以单击 **验证**，一键验证该漏洞是否已修复成功（如果您未进行手动验证，漏洞修复成功后 48 小时内安骑士会进行自动验证）。
- 如果您确认已完成漏洞修复，但验证后仍提示未修复，请参考 **漏洞修复后手动验证没有反应** 进行排查。

二、Windows 系统漏洞

服务器安全（安骑士）订阅微软的官方补丁更新，如果遇到重大漏洞更新（如“SMB 远程执行漏洞”）安骑士会为您提供自动检测和修复功能。

检测原理： 通过判断服务器上的补丁是否已经更新，并为您推送漏洞消息。
注意： 部分补丁更新后需要重启才能生效，如服务器未重启安骑士仍可能为您推送漏洞消息。

检测周期： 每天进行自动检测（若遇到重大软件漏洞爆发，安骑士会及时对您的服务器进行检测并第一时间为您推送漏洞消息）。

操作步骤

登录 云盾服务器安全（安骑士）管理控制台。

单击 **漏洞管理**，选择 **软件漏洞**。

单击 **漏洞分类**，选择 **Windows系统漏洞**。

单击 **漏洞名称**，可查看该漏洞的详细信息。

单击 **查看详情**，可进入漏洞处理页面进行漏洞处理。

- 单击 **一键修复**，即可修复该漏洞。安骑士会在云端缓存一份 Windows 官方补丁文件，您的 Windows 系统服务器会直接下载安骑士云端的补丁并完成自动更新（支持批量更新）。
- 如果漏洞补丁更新后需要重启服务器才能生效，安骑士不会自动重启您的服务器，您需要单击 **重启服务器** 重启您的服务器。
- 如果您在服务器上已手动更新了漏洞补丁，您可单击 **验证一下**，验证是否该漏洞是否已经修复。

漏洞状态说明

状态	说明
未修复	您的服务器存在系统软件漏洞需要更新，可一键修复或生成修复命令修复该漏洞。
修复中	漏洞正在修复中，可能由于异常原因阻断，最长修复时间为 10 分钟。
验证中	手动验证漏洞是否存在。
修复成功待重启	对于Windows系统漏洞，漏洞补丁已完成更新，等待重启服务器后生效。
修复失败	漏洞修复失败。失败原因可能有多种，请参考 漏洞修复失败可能原因 进行排查。
修复成功	漏洞已修复成功。
漏洞已失效	漏洞已通过其它途径手动修复或已不存在。系统自动检测七天内未发现该漏洞则将该漏洞标记为已失效，如果您手动验证该漏洞，则漏洞状态将更新为修复成功。
已忽略	漏洞已被忽略后，安骑士将不再向您提示该漏洞的告警信息。

漏洞白名单

如果您需要对某些漏洞彻底忽略，可以将此漏洞添加到漏洞白名单。添加成功后，安骑士将不再对漏洞白名单中的漏洞进行上报并告警。

注意：如果您将某个漏洞从白名单中移除，安骑士将恢复对该漏洞的检测，但无法恢复该漏洞的历史上报记录。

操作步骤

登录 云盾服务器安全（安骑士）管理控制台。

单击 **漏洞管理**，选择 **软件漏洞**。

单击 **漏洞白名单配置**。

输入漏洞名称，单击 **确定**。



关闭 Web 应用漏洞扫描

如果您发现 “Web应用漏洞扫描” 对您的业务有影响，您可以在设置页面关闭相关服务器的远程扫描功能。

操作步骤

登录 云盾服务器安全（安骑士）管理控制台。

单击 **设置**，单击 **安全配置**。



在漏洞管理设置中，单击 **管理**。



选择 **关闭部分** 并添加服务器IP，或选择 **关闭所有服务器**，单击 **确定**。

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。

注意： 您需要升级到服务器安全（安骑士）企业版才能使用此功能。

- **检测原理：** 基线检查功能自动检测服务器上的系统、权限、账号、数据库等配置存在的风险点，并提供修复建议。
- **检测周期：** 默认每天进行一次全面自动检测，自动检测在凌晨0到6点间完成。您可以在在安全设置页面设置检测周期和检测发生时间。
- **注意事项：** 某些检测项，例如：Mysql弱密码检测、sqlserver弱密码检测，会采用尝试登录方式进行检查，会占用一定的服务器资源以及生产较多的登录失败记录，这些项目是默认不开启的。如果需要这些功能，请确认上述风险后，在基线检查设置中勾选这些项目。

基线检查检测内容

分类	检测项	说明
系统	系统自启动项检测 (Windows)	检测 Windows 系统服务器中的注册表项 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogo

		n\Userinit中的键值是否包含可疑的可执行文件。
	系统共享配置检测 (Windows)	检测 Windows 系统服务器中的注册表 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous 中的键值，查看该键值控制是否允许远程操作注册表。
	组策略检测 (Windows)	检测 Windows 系统服务器中以下账号相关的安全策略： - 账号密码长度最小值 - 密码复杂度（数字、大小写字母、特殊字符组合） - 密码更新时必须与原密码不同 - 登录框是否显示上次登录账号 - 登录事件记录是否开启 - 登录过程中事件记录是否开启
	SSH 登录基线检测	检测 Linux 系统服务器中以下 SSH 登录安全策略配置： - 登录端口是否为默认 22 端口 - root 账号是否允许直接登录 - 是否使用不安全的 SSH V1 协议 - 是否使用不安全的 RSH 协议 - 是否运行基于主机身份验证的登录方式
弱密码检测	Linux 系统登录弱口令检测	检测 Linux 系统服务器的登录账号的密码是否为常见弱口令，及 SSH 登录的密码是否常见弱口令。
	SQLServer 登录弱口令检测	检测服务器上 SQLServer 登录账号的密码是否为常见弱口令。
	Windows 系统登录弱口令检测	检测 Windows 系统服务器中系统登录账号的密码是否为常见弱口令，及 RDP 登录的密码是否

		为常见弱口令。
	FTP 匿名登录检测	检测服务器上的 FTP 服务是否开启匿名登录。
	MySQL 弱口令检测	检测服务器上的 MySQL 服务的登录账户是否为常见弱口令。
	PostgreSQL 登录弱口令检测	检测服务器中 PostgreSQL 登录账户的密码是否为常见弱口令。
账号	风险帐号扫描	检测服务器系统中可疑的隐藏账号、及克隆账号。
	密码策略合规检测	检测 Linux 系统服务器中的以下账户密码策略： - 账号密码最大使用期限 - 密码修改最小间隔时间 - 密码最小长度 - 密码到期开始通知时间
	空密码账户检测	检测服务器中密码为空的账号。
	Linux 账号完整性检测	检测 Linux 系统服务器中新增账号的完整性。
数据库	Redis 配置漏洞被利用可疑文件检测	检测服务器上的 Redis 服务是否存在未授权访问漏洞被利用并向系统关键文件写入异常数据的情况。
	Redis 配置漏洞检测	检测服务器上的 Redis 服务是否对公网开放。
CIS基线检测（ 参考链接 ）	Linux-Tomcat7基线检测	按照CIS-Tomcat7最新基线标准进行中间件层面基线检测。
	Linux-Centos7基线检测	按照CIS-Linux Centos7最新基线标准进行系统层面基线检测。

操作步骤

登录 云盾服务器安全（安骑士）管理控制台。

单击 **基线检查**，查看安骑士发现的您服务器上存在的配置风险项。



选择风险项，单击 **查看详情**，进入风险处理页面。

单击风险名称，可查看该风险详情及相关修复建议。



参考修复建议，在您的对应服务器上进行修复。关于风险项修复的更多建议，您可以参考 **基线检查风险项修复建议**。

修复风险后，您可以单击 **验证**，一键验证该风险是否已修复成功（如果您未进行手动验证，风险修复成功后 72 小时内安骑士会进行自动验证）。

说明： 您也可单击 **忽略**，忽略该风险，安骑士将不再上报并告警此服务器上的这个风险项。

基线检查配置

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。

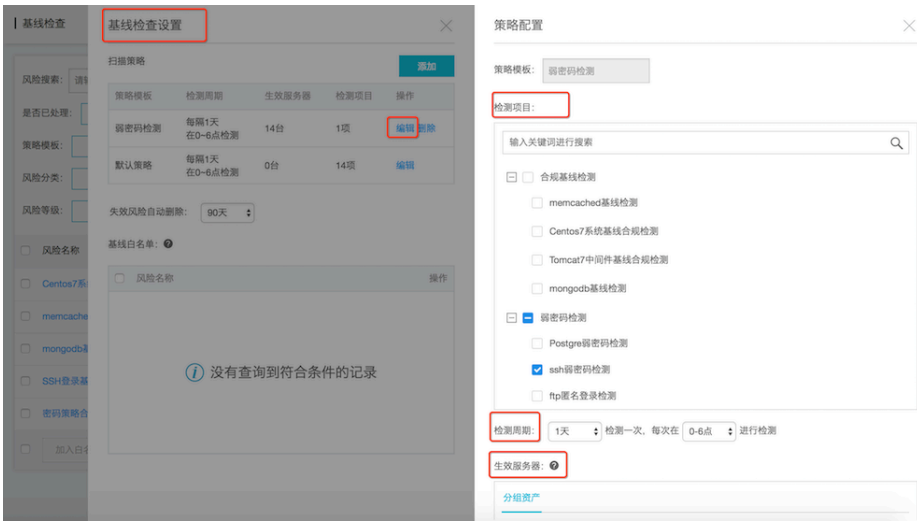
操作步骤

登录 云盾服务器安全（安骑士）管理控制台。

单击 **基线检查**。

单击 **基线检查设置**。

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。



攻略：设置了策略后，可以前往-资产列表，进行一键安全检测快速检测一遍，不用等周期检测哦。

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。

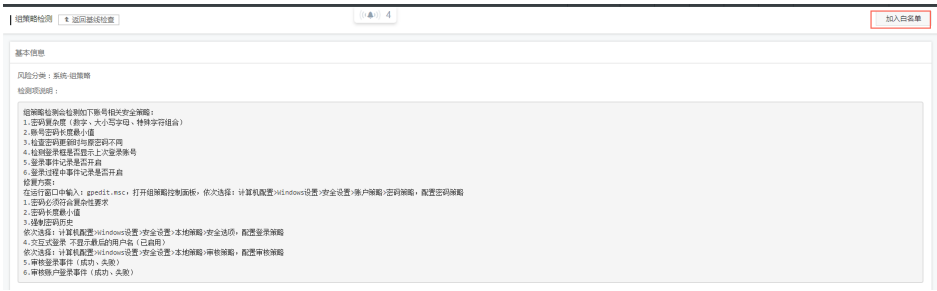
操作步骤

登录 云盾服务器安全（安骑士）管理控制台。

在检测出项目中，点击某个项目进入单击，如下图所示。



进入后点击右上角加入白名单。



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。

异常登录

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。

注意：旧版的正常登录行为不再提供展示，统一转移到日志功能中的登录流水中查询。

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。

当您的服务器第一次接入安骑士时，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成功登录六次或六次以上时，安骑士默认将此IP的地点记录为常用登录地。

注意：异地登录是针对公网IP才有的判断逻辑

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，知道该IP登录满6次会自动把IP的地址记录为常用登录地

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。

注意：您可在 服务器安全（安骑士）管理控制台 > 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）。

操作步骤

登录 服务器安全（安骑士）管理控制台。

定位到 事件 > 异常登录，查看异常登录告警事件。

异常登录

登录安全设置

资产选择：所有分组

服务器IP或名称

服务器IP地址

搜索

告警类型：异地登录

账号登录

非法IP登录

非法账号登录

非法时间登录

状态：

未处理

已处理

服务器IP名称	登录时间	状态	对应用户名	登录类型	登录源IP	告警类型	操作
120.78.85.179 [未处理]	2017-12-06 20:46:17	未处理	root	SSH	杭州市 (121.40.103.116)	非法账号登录	标记为已处理
120.78.85.179 [未处理]	2017-12-06 20:40:14	未处理	root	SSH	杭州市 (121.40.103.116)	非法时间登录	标记为已处理
120.78.85.179 [未处理]	2017-12-06 19:40:45	未处理	root	SSH	杭州市 (121.40.103.116)	非法IP登录	标记为已处理
106.15.127.17 [未处理]	2017-12-06 15:30:27	未处理	yhf	RDP	南京市 (221.228.56.18)	异地登录	标记为已处理
106.15.127.17 [未处理]	2017-12-06 11:14:25	未处理	yhf	RDP	南京市 (221.228.56.18)	异地登录	标记为已处理
106.15.127.17 [未处理]	2017-12-06 08:14:41	未处理	yhf	RDP	南京市 (221.228.56.18)	异地登录	标记为已处理

在上角选择 登录安全设置，可以针对机器自主添加常用登录地。

登录安全设置

×

常用登录地

添加

乍得	生效服务器：105台	编辑 删除
上海市	生效服务器：1台	编辑 删除
包头市	生效服务器：4台	编辑 删除
昆明市	生效服务器：1台	编辑 删除
罗马尼亚	生效服务器：1台	编辑 删除

共有 12 条，每页显示 5 条

«

<

1

2

3

>

»

企业版用户可在上角选择 登录安全设置，可以针对机器自主设置合法登录IP、合法登录时间、合法登录账号。

合法登录IP	非合法登录IP报警：	☒	添加
192.168.0.1/24	生效服务器：1台	编辑	删除
共有 1 条，每页显示 5 条		« < 1 > »	

合法登录时间	非合法登录时间报警：	☒	添加
00:01 - 03:00	生效服务器：1台	编辑	删除
共有 1 条，每页显示 5 条		« < 1 > »	

合法账号	非合法账号登录报警：	☒	添加
test	生效服务器：1台	编辑	删除
共有 1 条，每页显示 5 条		« < 1 > »	

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。

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：安骑士基础版只提供网站后门文件检测功能；隔离、恢复功能需要您升级到安骑士专业版或企业版才能使用。

功能原理

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。

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：

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。

注意：您可在 服务器安全（安骑士）管理控制台 > 设置 > 安全设置 中的 木马查杀 区域，单击 周期检查Web目录 选项右侧的 管理 设置需要进行静态检测的服务器。默认情况下，安骑士防护的所有服务器均开启静态检测。

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 服务器安全（安骑士）管理控制台 > 入侵检测 > 网站后面 页面，单击网站后门设置，手动添加需要检测的Web目录。

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

登录 服务器安全（安骑士）管理控制台。

定位到 事件 > 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。

网站后门

2

当前版本：企业版
2017-11-27到期

升级

续费

请输入实例ID或备注名进行模糊搜索

搜索

☐	服务器IP/名称	木马文件路径	更新时间	木马类型	状态(全部)	操作
☐	10.10.10.10 服务器IP: 10.10.10.10	/var/www/html/test_11_2.php	2017-07-26 19:27:19	Webshell	待处理	隔离 忽略
☐	10.10.10.10 服务器IP: 10.10.10.10	/var/www/html/test_7_12.php	2017-07-26 19:27:19	Webshell	待处理	隔离 忽略
☐	10.10.10.10 服务器IP: 10.10.10.10	/var/www/html/test_7_13_1.php	2017-07-26 19:27:19	Webshell	待处理	隔离 忽略

对发现的木马文件进行处理。

- **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。

注意：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。

日志

功能介绍

日志功能尚处于 Beta 测试阶段。

注意： 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、无需部署，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，免安装免维护，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

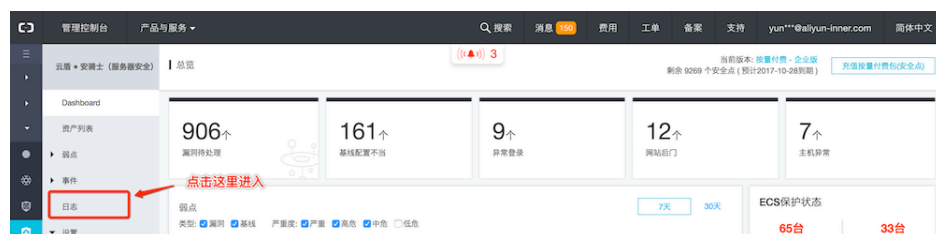
注意：各种日志源支持的字段信息请查看 各日志源字段说明。

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。

操作步骤

登录 云盾服务器安全（安骑士）管理控制台，单击 **日志**，进入日志页面。



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**。

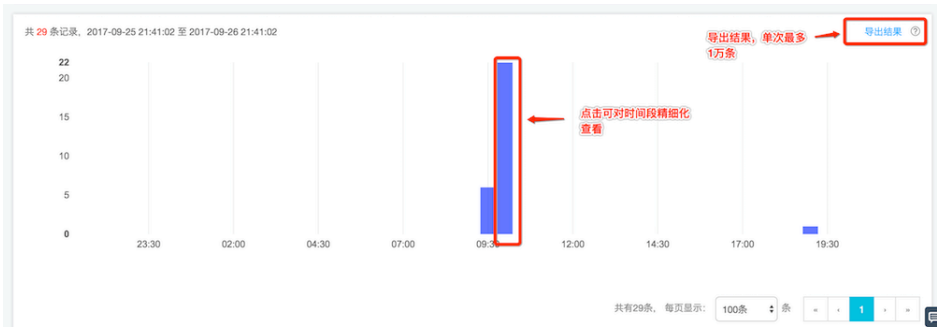
说明：您可以增加多条搜索条件，进行逻辑检索。



根据您的设置搜索条件，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。



您可以根据细粒度的时间维度查看搜索结果，并将数据结果导出。



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）	uuid	客户端编号	uuid	text
	ip	IP地址	ip	text
	pid	进程ID	pid	text
	groupname	用户组	groupname	text
	ppid	父进程ID	ppid	text
	uid	用户ID	uid	text
	username	用户名	username	text
	filename	文件名	filename	text
	pfilename	父进程文件名	pfilename	text
	cmdline	命令行	cmdline	text
进程启动	filepath	进程路径	filepath	text
	pfilepath	父进程路径	pfilepath	text

	time	启动时间		
端口监听快照	src_port	监听端口	src_port	text
	src_ip	监听IP	src_ip	text
	proc_path	进程路径	proc_path	text
	pid	进程ID	pid	text
	proc_name	进程名	proc_name	text
	proto	协议	proto	text
	time	数据获取时间		
网络连接	src_ip	源IP	src_ip	text
	src_port	源端口	src_port	text
	proc_path	进程路径	proc_path	text
	dst_port	目标端口	dst_port	text
	proc_name	进程名	proc_name	text
	dst_ip	目标IP	dst_ip	text
	status	状态	status	text
	proto	协议	proto	text
	time	连接时间		
账号快照数据	perm	是否拥有root权限	perm	text
	home_dir	home目录	home_dir	text
	warn_time	密码到期提醒时间	warn_time	text
	groups	用户属于的组	groups	text
	login_ip	最后一次登录的ip地址	login_ip	text
	last_chg	密码最后修改时间	last_chg	text
	shell	linux的shell命令	shell	text
	domain	windows域	domain	text
	tty	登录的终端	tty	text
	account_expire	账号超期时间	account_expire	text
	passwd_expire	密码超期时间	passwd_expire	text
	last_logon	最后登录时间	last_logon	text
	user	用户	user	text
	status	用户状态：0-禁	status	text

		用、1-正常		
	time	数据获取时间		
进程快照数据	path	进程路径	path	text
	start_time	进程启动时间	start_time	text
	uid	用户ID	uid	text
	cmdline	命令行	cmdline	text
	pname	父进程名	pname	text
	name	进程名	name	text
	pid	进程ID	pid	text
	user	用户名	user	text
	md5	进程文件MD5值 ，超过1MB不计算	md5	text
	time	数据获取时间		
登录流水	warn_ip	登录来源IP	warn_ip	text
	warn_port	登录端口	warn_port	text
	warn_user	登录用户名	warn_user	text
	warn_type	登录类型	warn_type	text
	warn_count	登录次数	warn_count	text
	time	登录时间		
暴力破解	warn_ip	攻击来源IP	warn_ip	text
	warn_port	破解端口	warn_port	text
	warn_user	破解用户名	warn_user	text
	warn_type	类型	warn_type	text
	warn_count	破解次数	warn_count	text
	time	破解时间		

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。
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。

注意： 语法关键词不区分大小写。

已下线功能

主机访问控制

主机访问控制功能运行在Aliyundun进程中，当前支持TCP、UDP以及HTTP协议的自定义访问控制。

- 首次添加服务器到策略组，由于防火墙模块安装需要大概3-5分钟，若显示防护失败，请多重试几次。

支持系统

- 支持系统：CentOS 6.x、CentOS7.0、Windows 2008
- 不支持系统：Windows2003以及其余未提及的linux系统

应用场景

- 四层防护：针对服务器的ip、端口、协议访问控制策略，类似于iptables
- 七层防护（HTTP精准策略）：web应用防护，专门针对http/https进行防护，可以针对具体的某个web页面设置防护策略

资源占用

- 内存：运行时可能会消耗您几M物理内存（一般在6M左右，不会大于10M）。
- CPU：以双核ecs为例，在10MBit/s流量下（满负荷），会消耗8%左右的cpu值。

实现原理

使用了内核技术，接管了一部分网络协议栈的工作，所以当您看到Aliyundun这个进程使用了较大cpu的时候，是因为原来网络协议栈这部分工作内容转嫁到Aliyundun 中，Aliyundun 承担了这部分工作内容而造成了额外的cpu消耗，但是实际上总体性能消耗并没有额外的增加（实际消耗8%左右）

访问控制模块使用内核技术在本机上实现了透明代理，无需重启服务器和web服务，无需修改任何参数和配置，即可使用，即插即用，并支持防御策略的实时热更新。

匹配顺序

超级白名单 > 超级黑名单 > 自定义策略 > 云盾协同防御策略 > 默认策略

支持内容

- TCP、UDP：入方向
 - 允许所有IP访问：即对所有外部过来访问该服务器指定端口的IP均放行
 - 不允许所有IP访问：即对所有外部过来访问该服务器指定端口的IP均拦截
 - 只允许特定IP访问：该端口只开放给特定IP来访问，其余过来访问的IP均拦截
 - 不允许特定IP访问：该端口只对某些IP拦截，其余IP过来访问均放行
 - 超级白名单：超级白名单中的IP，不区分端口，所有请求均放行
 - 超级黑名单：超级黑名单中的IP，不区分端口，所有请求均拦截
 - 默认规则：即匹配完所有策略后，若未命中任何一条策略采取的动作
- TCP、UDP：出方向
 - 允许主动对外访问所有服务器该端口：即该台服务器允许主动外连所有服务器的指定端口（如需设置该台服务器需要上所有的http web网站，则设置：允许主动对外访问所有服务器的 80 端口）
 - 不允许主动对外访问所有服务器该端口：即该台服务器不允许主动外连其他服务器的指定端口
 - 不允许对外访问以下服务器的该端口：即不允许对特定服务器的特定端口进行访问，其余对外请求特定端口均放过
 - 只允许对外访问以下服务器的该端口：即只对外访问特定服务器的特定端口进行放行，其余对外访问特定端口的请求均拦截
 - 默认规则：即匹配完所有策略后，若未命中任何一条策略采取的动作

HTTP精准策略：对协议为http且开启精准策略开关的端口，才会生效http策略

- 访问控制支持全部
method : get , head , trace , delete , options , lock , mkcol , copy , move , post , put
- 支持大多数header : cookie , host , from , referer , expect , te , content-type , user-agent , accept , accept-encoding , accept-charset , accept-language , authorization , proxy-authorization , x-forwarded-for , x-remote-ip , max-forwards , range , if-range , if-match , if-none-match , if-modified-since , if-unmodified-since , request_uri , uri_dir , uri_file
- 支持字符串搜索和正则两种匹配算法

操作步骤

新建主机访问策略组。

添加策略组

策略组名:

添加策略组后，您可以去配置详细的规则策略，并指定相关服务器生效该策略

确认

取消

配置端口和详细访问规则。

策略组: bbbb

返回主机防火墙

策略开关: ☒

入方向

出方向

策略匹配顺序: 超级白名单 > 超级黑名单 > 自定义策略 > 云盾协同防御策略

端口	协议	动作	精准策略自定义	协同防御	操作
90	tcp	允许所有IP访问	--	☐	编辑 删除
8080	http	允许所有IP访问	☐	☐	编辑 删除

+新增规则

默认拦截模式: ☒ 不阻断 ☐ 阻断

入方向建议设置为默认阻断，将需要开放的端口及对应阻断规则添加在上方或超级白名单中

超级白名单

超级黑名单

HTTP精准策略

提示: 对协议为http且开启精准策略开关的端口，才会生效以下策略

新增规则

规则名称	规则条件	拦截动作	操作
没有查询到符合条件的记录			

选择需要生效的服务器。



查看拦截日志。

安全运维

注意：

安全运维功能需要升级安骑士 Agent 版本。

购买服务器安全（安骑士）企业版后，请先绑定好需要开通该功能的服务器。系统将自动触发升级，绑定完成10分钟后，该功能可正常使用。

概述

安全运维功能是基于服务器安全（安骑士）企业版 Agent 长连接命令通道，提供给用户的一个批量进行运维的功能。如需使用该功能，您需要购买服务器安全（安骑士）企业版并绑定到相应服务器。

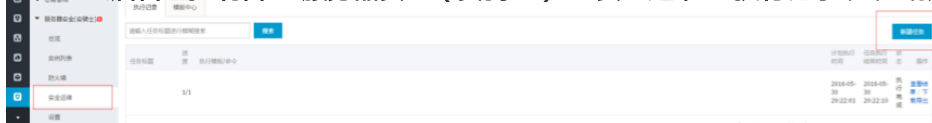
原理

安全运维功能采用分布式 Agent 进行远程脚本执行，并反馈运行结果。可以同时多个您指定的远程主机执行系统脚本。针对不同的目标主机，脚本主要分两类：

- **Shell 命令**：如果选择的目标系统为 Unix 或者 Linux 类型主机，则可以对您指定的多台主机进行远程 shell 命令执行。
- **DOS 命令**：如果您选择的目标主机类型为 Windows，则可以对您指定的多台主机进行远程 dos 命令执行。

操作步骤

定位到云盾管理控制台 > 服务器安全（安骑士）> 安全运维 > 执行记录，单击新建任务。



在新建远程命令任务界面输入任务标题，提交所需要执行的命令并选择需要执行命令的服务器列表。

新建远程命令任务

任务标题：

选择需要运行命令的服务器：

所有服务器（当前选中0条）全选

请选择分组：全部

输入服务器IP/名称进行搜索

已选择服务器（共有1条）全选

输入服务器IP/名称进行搜索

192.168.221.167 (localhost.localdo...

命令：

☐ 使用模板

☒ 将命令保存为模板

☒ 使用系统权限运行

计划执行时间：☒ 立即执行 ☐ 其他时间

确认

取消

注意： Agent 默认使用系统权限执行命令（在 Windows 系统中使用 System 账号，在 Linux 中使用 root 账号）。若需要使用其他账号执行，可以取消使用系统权限运行选项，并在右侧的输入框中填写您想使用的账号。

40



使用模板 命令

☐ 使用系统权限运行 请输入运行账号 账号对应组名，默认为账户名组

计划执行时间：☒ 立即执行 ☐ 其他时间

确认以上所有信息后单击**确认**。系统将根据设置，立即或在您指定的时间执行该命令。

下发到服务器后，所有命令将会作为脚本执行。运行目录为安骑士 Agent 目录。

待任务执行完成后，单击**查看结果**直接查看执行结果，或者单击**下载导出**将执行结果导出。

返回状态

- **下发成功**：命令已下发，安骑士 Agent 执行还未返回结果。
- **下发失败**：命令下发失败，安骑士 Agent 可能未在线，请稍后重试。
- **执行完成**：命令下发执行成功并已返回结果。
- **执行失败**：命令下发成功，但执行失败。
- **目标用户未找到**：命令下发成功，但未找到执行该命令所需要的账号或运行时的环境。

注意事项

- 所有命令超时时间是一分钟。一分钟后若命令仍未结束，将会返回当前已获取的结果，并结束命令进程。
- Windows 2003 不支持通过账号组方式启动进程。
- Windows 下默认在 System 账号下执行命令。
注意：界面相关的进程在 System 账号下执行会存在系统库相关的问题。
- Windows 下指定账号执行命令时需要有通过该账号创建的进程存在，否则会失败。

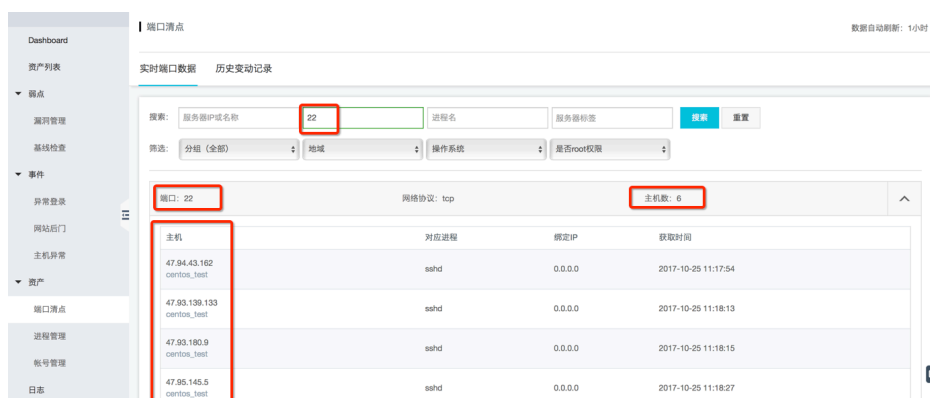
资产管理

端口清点

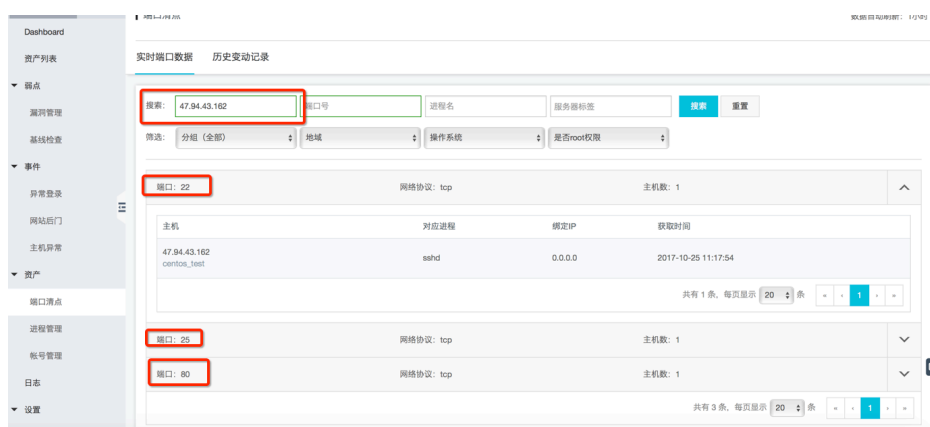
端口清点

- 功能版本：企业版
- 功能介绍：定期收集服务器的对外端口监听信息，并对变动信息进行记录，便于端口清点和历史端口变动查看
- 数据收集周期：每小时
- 使用场景
 - 清点一个端口，有多少服务器监听了
 - 清点一台服务器，开了多少端口
 - 发现了异常监听端口，通过历史记录可查看到监听时间
- 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）

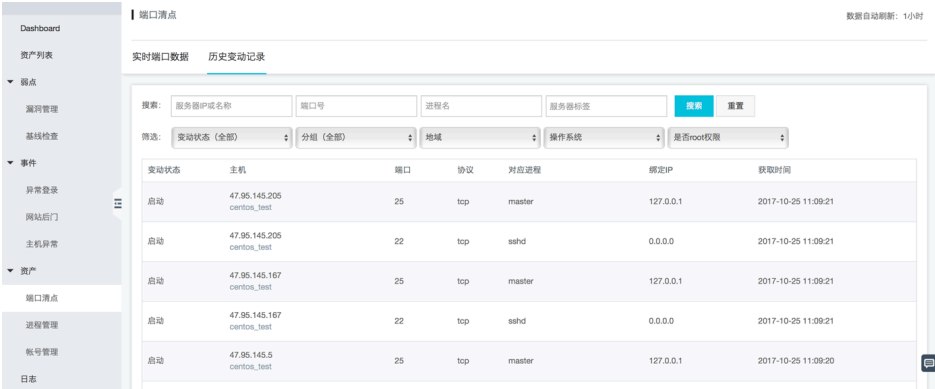
清点一个端口有多少服务器在监听



清点一台服务器开放了多少端口



端口历史变动



进程管理

进程管理

- 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

Dashboard

资产列表

▼ 资产

漏洞管理

基线检查

▼ 事件

异常登录

网站后门

主机异常

资产

端口清点

进程管理

帐号管理

日志

▼ 设置

实时进程数据

历史变动记录

搜索: 服务器IP或名称 47.95.145.205 运行用户 启动参数 服务器标签 搜索 重置

筛选: 分组 (全部) 地域 操作系统 是否root权限

进程: 47.95.145.205 主机数: 6

主机	进程路径	启动参数	启动时间	运行用户	运行权限	PID	父进程	文件MD5	获取时间
47.95.145.205 centos_test	/usr/local/nginx/nginx_client/aeg	/usr/local/nginx/nginx_client/aeg	2017-10-25 11:06:17	root	root	1496	init	N/A	2017-10-25 11:06:47
47.95.145.167 centos_test	/usr/local/nginx/nginx_client/aeg	/usr/local/nginx/nginx_client/aeg	2017-10-25 11:06:16	root	root	1496	init	N/A	2017-10-25 11:06:47
47.93.139.133 centos_test	/usr/local/nginx/nginx_client/aeg	/usr/local/nginx/nginx_client/aeg	2017-10-23 20:28:58	root	root	1496	init	N/A	2017-10-25 11:06:47
47.95.145.5 centos_test	/usr/local/nginx/nginx_client/aeg	/usr/local/nginx/nginx_client/aeg	2017-10-25 11:06:17	root	root	1496	init	N/A	2017-10-25 11:06:48
47.94.43.162 centos_test	/usr/local/nginx/nginx_client/aeg	/usr/local/nginx/nginx_client/aeg	2017-10-24 14:31:19	root	root	21289	init	N/A	2017-10-25 20:02:38

清点一台服务器运行了多少个进程

资产列表

▼ 资产

漏洞管理

基线检查

▼ 事件

异常登录

网站后门

主机异常

资产

端口清点

进程管理

帐号管理

日志

▼ 设置

实时进程数据

历史变动记录

搜索: 47.95.145.205 进程名 运行用户 启动参数 服务器标签 搜索 重置

筛选: 分组 (全部) 地域 操作系统 是否root权限

进程: 47.95.145.205 主机数: 1

进程名	主机数
进程: aliyun-service	主机数: 1
进程: AliYunDun	主机数: 1
进程: AliYunDunUpdate	主机数: 1
进程: atd	主机数: 1
进程: auditd	主机数: 1
进程: crond	主机数: 1
进程: init	主机数: 1
进程: rcbalance	主机数: 1

进程历史变动

资产列表

▼ 资产

漏洞管理

基线检查

▼ 事件

异常登录

网站后门

主机异常

资产

端口清点

进程管理

帐号管理

日志

▼ 设置

实时进程数据

历史变动记录

搜索: 服务器IP或名称 进程名 运行用户 启动参数 服务器标签 搜索 重置

筛选: 变动状态 (全部) 分组 (全部) 地域 操作系统 是否root权限

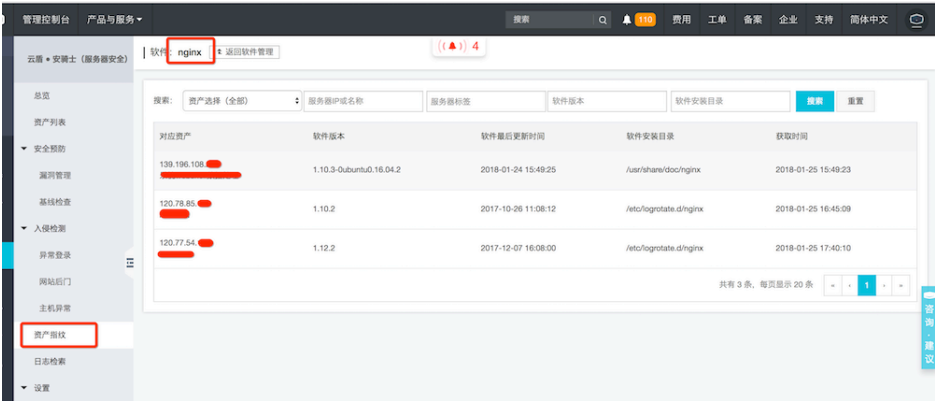
变动状态	主机	进程名	进程路径	启动参数	启动时间	运行用户	运行权限	PID	父进程	文件MD5	发生变动时间
启动	47.93.180.9 centos_test	tail	tail -f data.21637.3		2017-10-25 19:14:49	root	21647	bash	392437306504c858918a357e9773cfa		2017-10-25 20:03:57
停止	47.93.180.9 centos_test	pickup	pickup -i -t ffo -u		2017-10-25 10:45:24	postfix	21104	master	0f5e8323390083d40396034a8aa4f6a		2017-10-25 20:03:57
启动	47.93.180.9 centos_test	pickup	pickup -i -t ffo -u		2017-10-25 19:05:43	postfix	21582	master	0f5e8323390083d40396034a8aa4f6a		2017-10-25 20:03:57
启动	47.93.180.9 centos_test	sshd	sshd: root@pts/2,pts/3		2017-10-25 19:05:26	root	21567	sshd	087819ec0789dc593846d86f93e6846		2017-10-25 20:03:57
启动	47.93.180.9 centos_test	sshd	sshd: root@pts/0		2017-10-25 19:49:14	root	21685	sshd	087819ec0789dc593846d86f93e6846		2017-10-25 20:03:57
停止	47.93.180.9 centos_test	udev	/sbin/udev -d		2017-10-23 15:20:15	root	1863	udev	ed14ba18cae692039171a7840650758		2017-10-25 20:03:57

软件版本管理

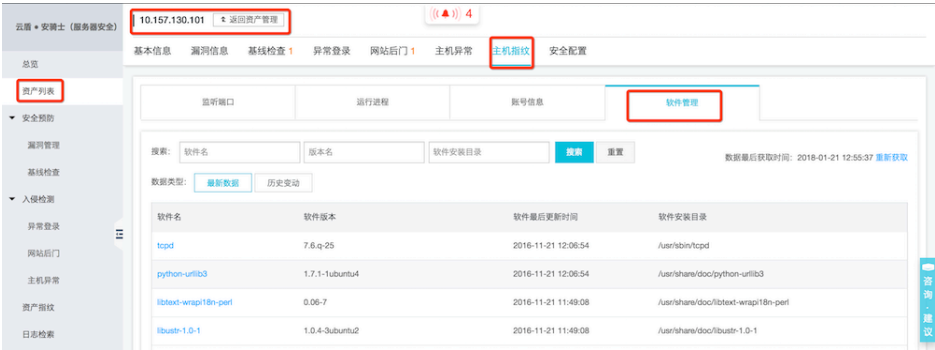
软件版本管理

- 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

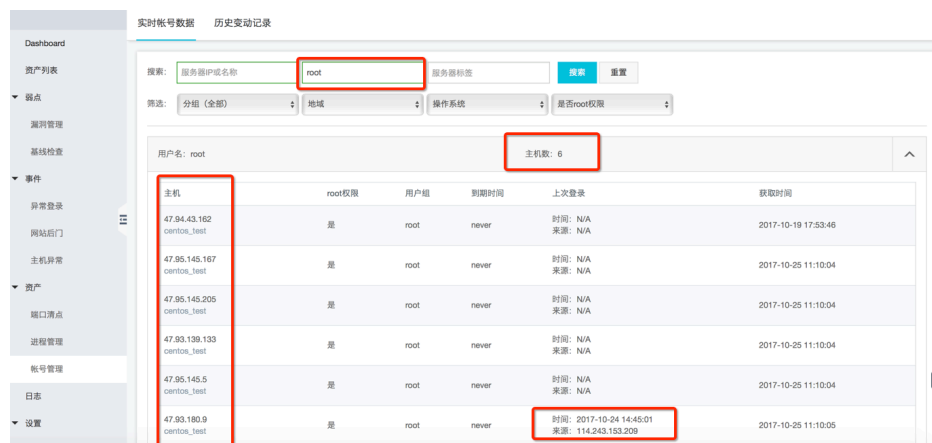


账号管理

账号管理

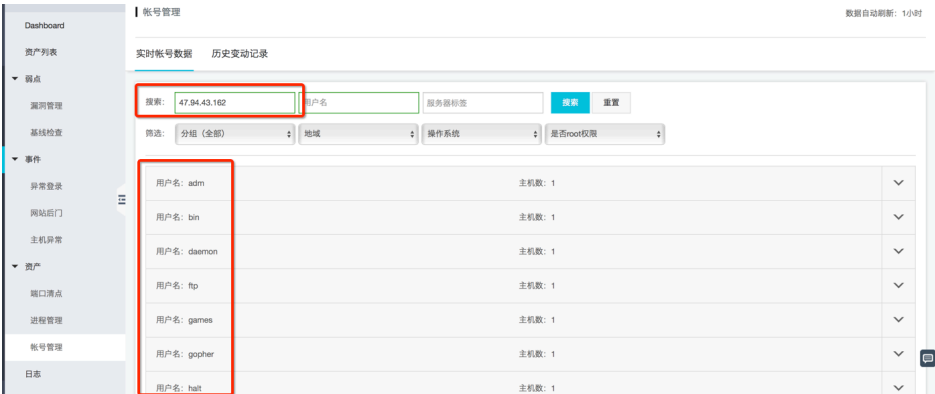
- 功能版本：企业版
- 功能介绍：定期收集服务器的账号信息，并对变动情况进行记录，便于账号清点和历史账号变动查看
- 数据收集周期：每小时
- 使用场景
 - 清点一个账号，有多少服务器创建了
 - 清点一台服务器，创建了多少个账号
 - 发现了非法账号，通过历史记录可查看到变动的的时间
- 账号详情
 - 账号名
 - 是否root权限
 - 用户组
 - 到期时间
 - 上次登录情况（登录时间、登录来源）
- 变动历史说明
 - 变动状态：新建（上次未发现，本次数据收集发现新建了）、删除（上次数据收集有，本次没有了）、修改（账号名没变，但是root权限、y用户组、到期时间变动了）
 - 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

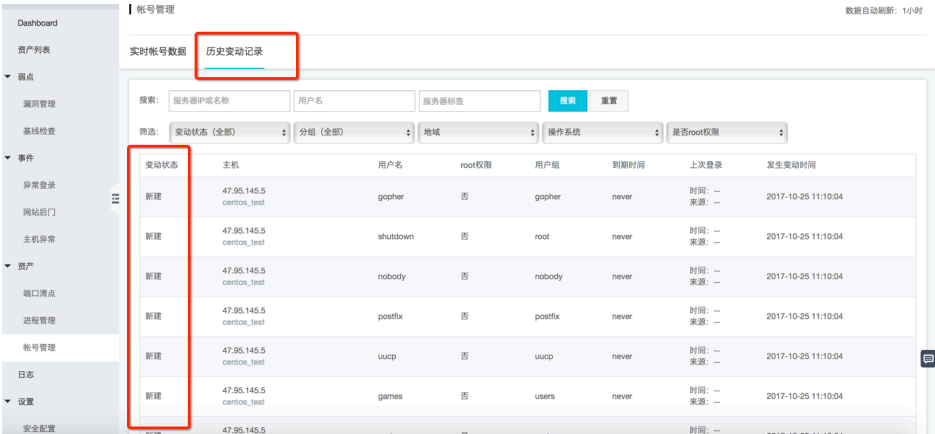


主机	root权限	用户组	到期时间	上次登录	获取时间
47.94.43.162 centos_test	是	root	never	时间: N/A 来源: N/A	2017-10-19 17:53:46
47.95.145.167 centos_test	是	root	never	时间: N/A 来源: N/A	2017-10-25 11:10:04
47.95.145.205 centos_test	是	root	never	时间: N/A 来源: N/A	2017-10-25 11:10:04
47.93.139.133 centos_test	是	root	never	时间: N/A 来源: N/A	2017-10-25 11:10:04
47.95.145.5 centos_test	是	root	never	时间: N/A 来源: N/A	2017-10-25 11:10:04
47.93.180.9 centos_test	是	root	never	时间: 2017-10-24 14:45:01 来源: 114.243.153.209	2017-10-25 11:10:05

清点一台服务器创建了多少账号



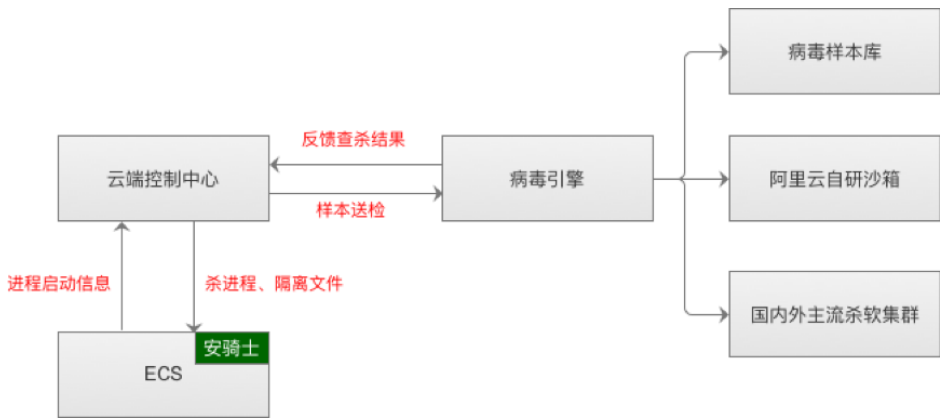
账号历史变动



病毒云查杀

一、 实现方案

采用云+端的查杀机制，客户端负责捕获进程启动信息，上报到云端控制中心进行病毒样本检测，若判断为恶意进程，客户可进行恶意进程的处置：停止进程、隔离文件等。



二、功能满足

- 1、检测出病毒及变种等恶意进程的运行；
- 2、一键杀死病毒进程、隔离病毒源文件；

三、优势

- 轻量

- 云服务器资源非常宝贵，客户需要更多地将资源用来运转业务，安骑士占用资源非常少，仅有50MB

- 实时

- 安骑士采用在应用态获取进程启动信息，对于病毒程序启动可以非常实时地监控

- 少打扰

- 病毒程序不启动，实际上对服务器没有影响，安骑士为保证服务器资源不被过多占用，只对产生危害的病毒程序进行检测，减少客户打扰

- 业务优先

- 云服务器跟传统终端有所不同，可以让客户选择性是否继续运行某些“可疑进程”，一定程度将误报转嫁给客户，但云服务器由于没有客户介入确认，所以仍采用“主动隔离”将给客户业务造成不可预期的风险，故安骑士目前的方案是，对于查杀的部分由客户自主介入进行操作

四、部分截图

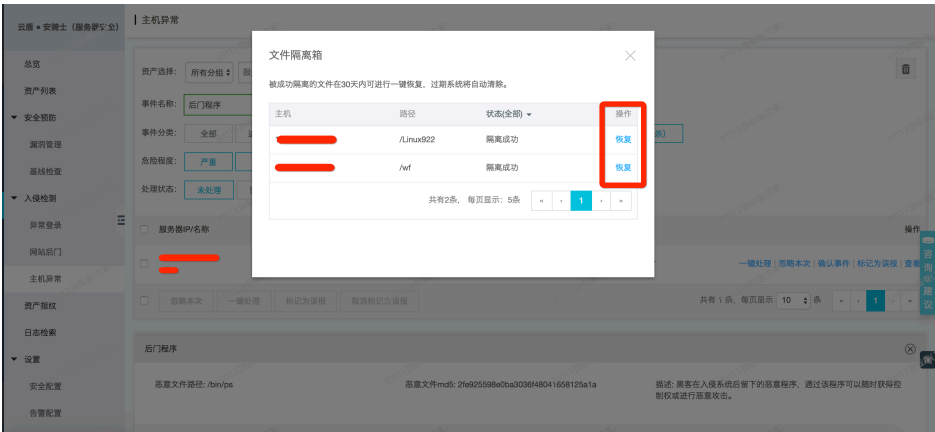
检测



隔离



恢复



告警通知

安骑士企业版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。

注意：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。

通知项目

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

注意：仅主机配置项可设置告警时间。