安骑士

用户指南

用户指南

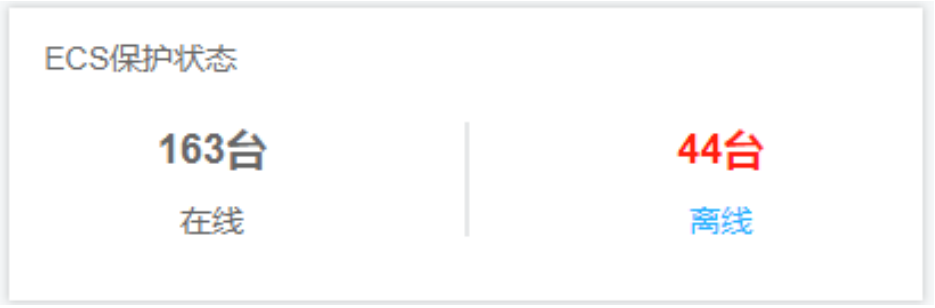
Agent 插件

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 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。

安骑士 Agent 包含以下两个主要进程：

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\aegis\aegis_client
- **Windows 64位系统**： C:\Program Files (x86)\Alibaba\aegis\aegis_client
- **Linux 系统**： /usr/local/aegis/aegis_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\aegis\aegis_update
- **Windows 64 位系统**： C:\Program Files (x86)\Alibaba\aegis\aegis_update
- **Linux 系统**： /usr/local/aegis/aegis_update

资源占用

安骑士Agent仅占用您服务器少量资源：

- **业务优先模式**： 安骑士Agent占用不超过1%CPU及50MB内存。
- **防护优先模式**： 安骑士Agent占用不超过10%CPU及80MB内存。

注意：

如果占用资源超过防护优先模式峰值，安骑士Agent将会暂停工作。CPU占用下降到合理范围内后Agent会自动重启。

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：

阿里云服务器，直接安装即可。

对于通过internet通信的非阿里云服务器，安装后如果出现离线情况请参考Agent离线排查

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

操作步骤

1. 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/卸载**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

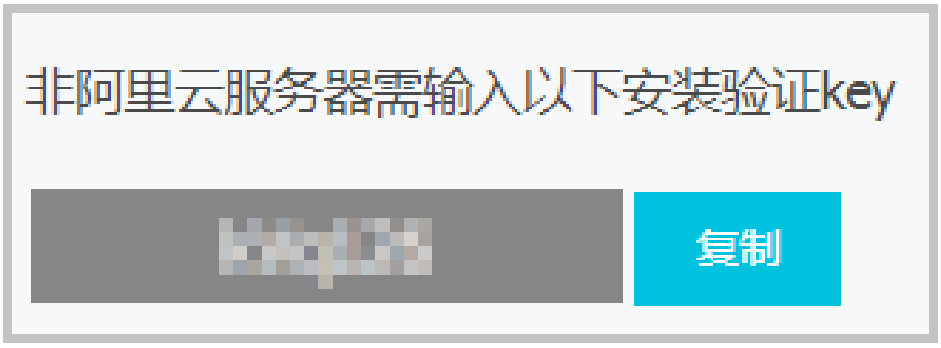
a. 在安装安骑士Agent页面，单击**点击下载**下载最新版本安骑士Agent插件安装文件到本地计算机。

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。

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。



注意：

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。

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。

完成安装。

单击**立即查看**打开资产列表，查看资产在线状态。

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，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。

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。

   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。

i. 140.205.140.0/24 Port: 80
ii. 106.11.68.0/24 Port: 80
iii. 106.11.248.0/24 Port: 80 443
iv. 106.11.250.0/24 Port: 80 443
v. 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：

- 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。

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。

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。

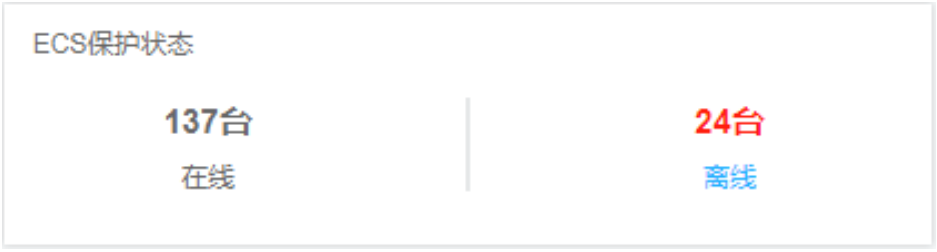
待处理的告警事件数量

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

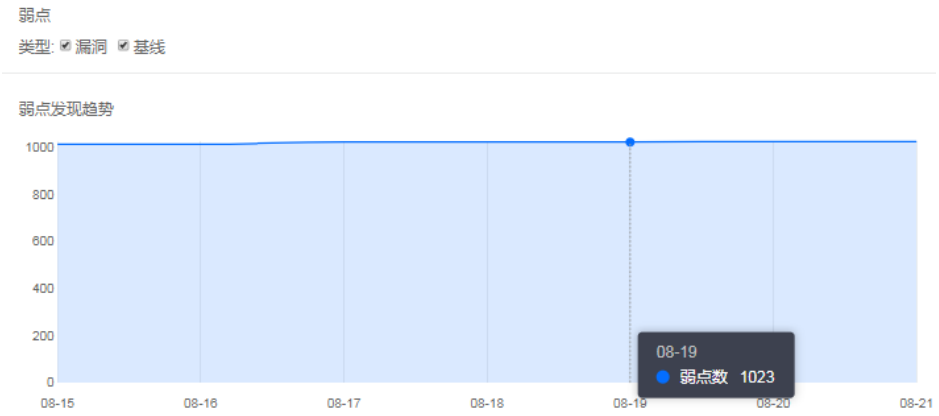
ECS保护状态



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



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）。

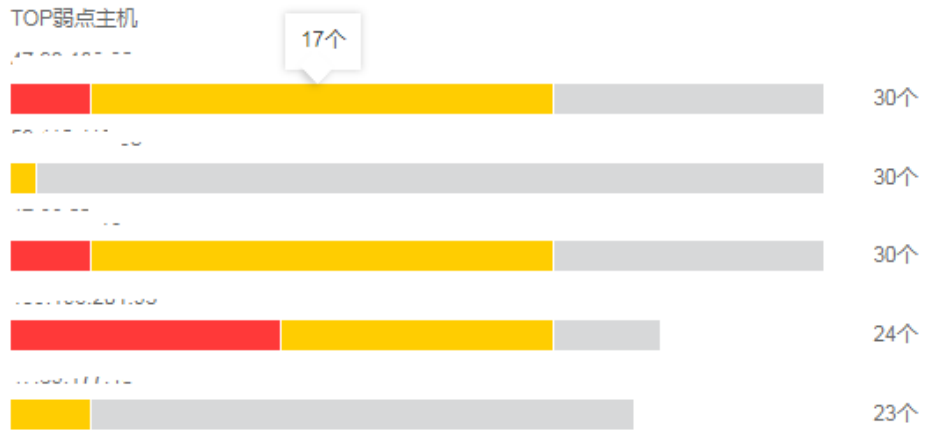
设置弱点类型显示以下弱点发现趋势：

- 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



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）。

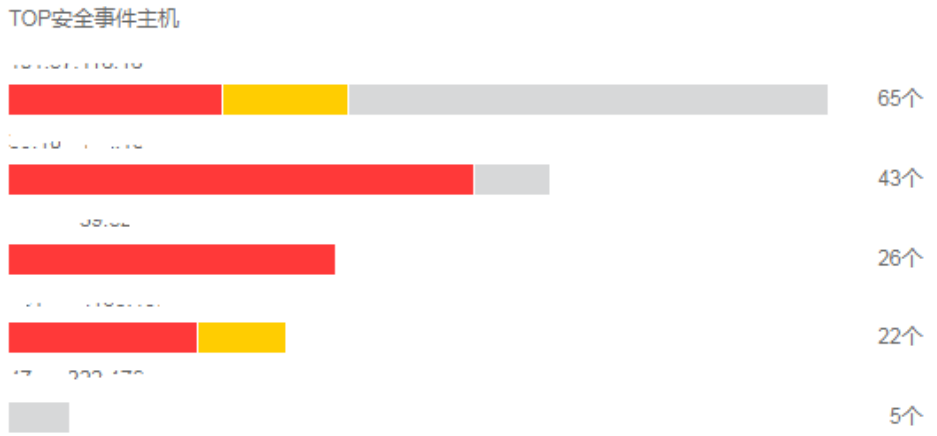
设置事件类型在总览页面显示以下入侵事件趋势：

- 异常登录
- 网站后门
- 主机异常

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



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。

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。

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。

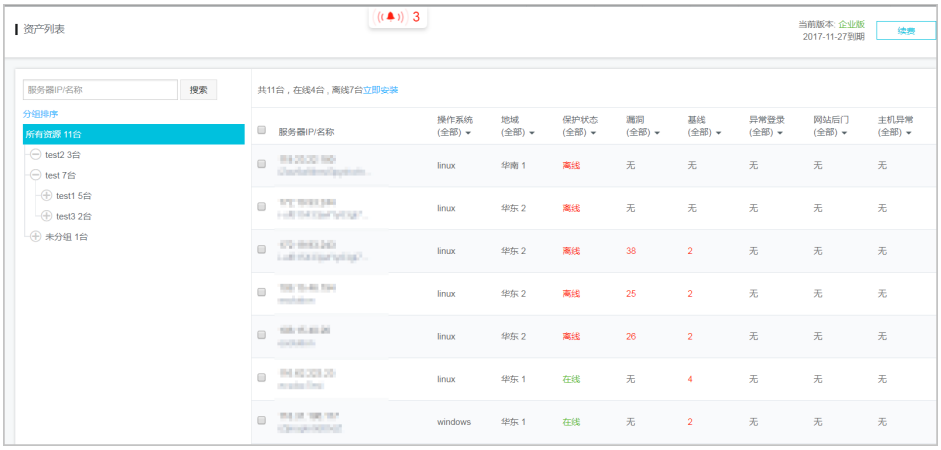
单击 **资产列表**，查看安骑士已防护的服务器的保护状态。

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。

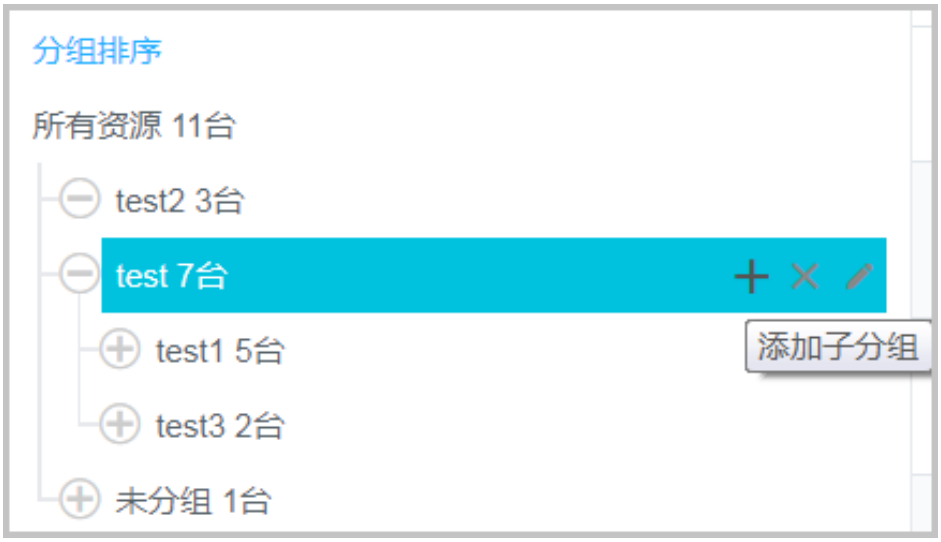


对您的服务器资产进行分组。

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。



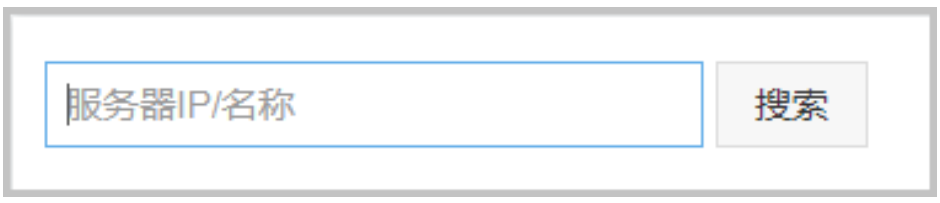
注意： 目前，最多可支持三级资产子分组。

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。



安全预防

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\Winlogon\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\SYS

		TEM\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 登录账号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 监听配置	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，建议您尽快修改配置。
CIS基线检查	Linux-Tomcat7基线检测	基于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	基于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。

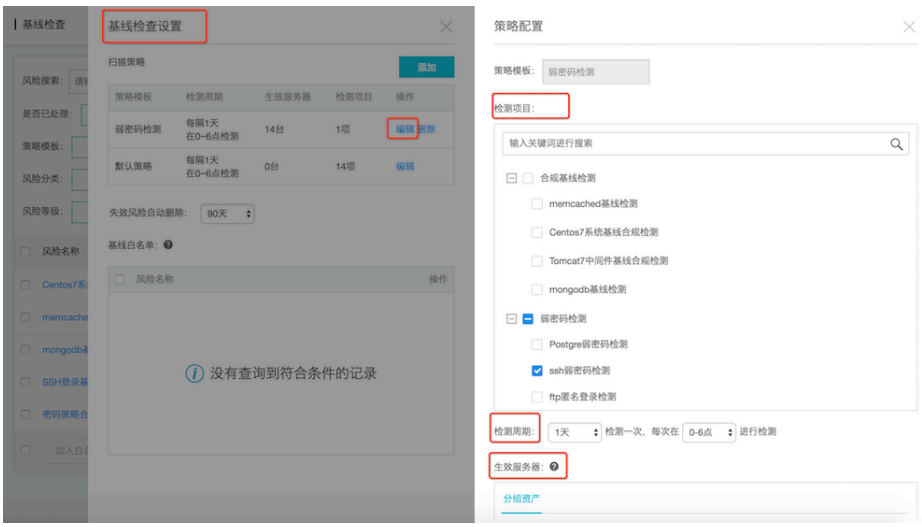
操作步骤

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

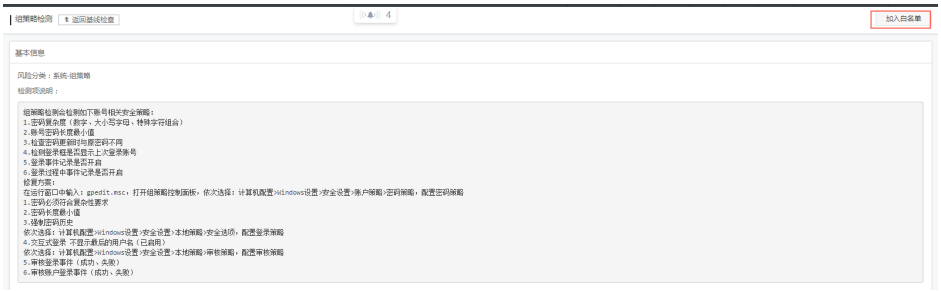
如果您需要对某些基线检查项目彻底忽略，可以将此检测项添加到基线检查白名单。添加成功后，安骑士将不再对基线检查白名单中的检测项目所发现的风险进行上报并告警，加入白名单或忽略操作支持填写备注，以便后续查看。

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**。



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

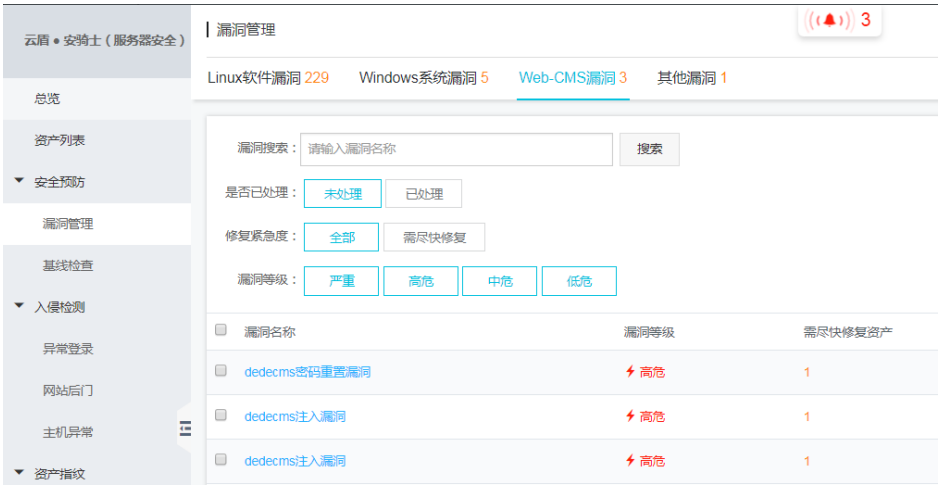
安骑士通过识别存在漏洞的通用 Web 文件的 MD5 值，替换存在漏洞的文件，实现 Web-CMS 漏洞修复。

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。

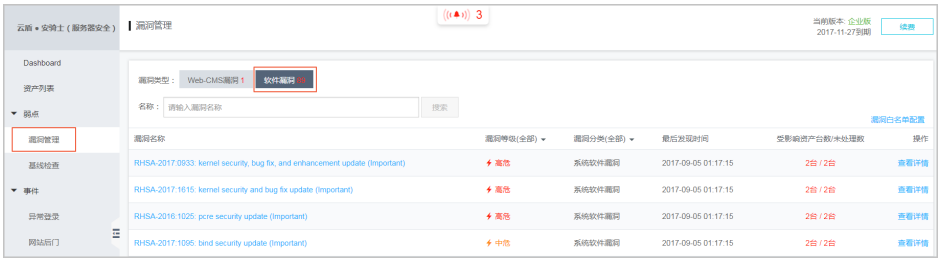
检测周期： 每两天进行一次自动检测（若遇到重大软件漏洞爆发，安骑士会及时对您的服务器进行检测并第一时间为您推送漏洞消息）。

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**。

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**。

入侵检测

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。

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

登录 服务器安全（安骑士）管理控制台。

点击 **事件** > **异常登录**，查看异常登录告警事件。

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。

在**登录安全设置**页面针对服务器自主设置常用登陆地、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。

安骑士病毒云查杀

云盾安骑士病毒查杀（以下简称“云查杀”）集成了国内外多个主流的病毒查杀引擎，并利用阿里云海量威胁情报数据和自主研发的基于机器学习、深度学习异常检测模型，为用户提供全面和实时的病毒检测和防护服务。

目前云查杀每天检测数亿文件，实时服务百万云上主机。

云查杀检测能力

安骑士采用云+端的查杀机制，客户端负责采集进程信息，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，支持用户一键处理，如停止进程、隔离文件等。

- **深度学习检测引擎（自主研发）**
  云盾深度学习检测引擎，使用深度学习技术，基于海量攻防样本，专门打造的一款适用于云环境的恶意文件检测引擎，智能识别未知威胁，是传统病毒查杀引擎的有力支撑。
- **云沙箱（自主研发）**
  真实还原云上环境，监控恶意样本攻击行为，结合大数据分析、机器学习建模等技术，自动化检测和发现未知威胁，提供有效的动态分析检测能力。
- **集成国内外主流病毒查杀集群**
  安骑士集成国内外多款优秀的杀毒引擎，病毒病实时更新。
- **威胁情报检测**
  基于云盾威胁情报数据，配合主机异常行为检测模型，实现多维度检测异常进程和恶意行为。

云查杀覆盖的病毒类型

云查杀是阿里云安全技术与攻防专家经验融合的最佳实践，从数据的采集、脱敏、识别、分析、隔离到恢复已形成安全闭环，同时支持用户在云盾控制台中进行一键处理（隔离、恢复）。

云查杀覆盖以下病毒类型：

病毒类型	病毒描述
挖矿程序	非法占用服务器资源进行虚拟货币挖掘的程序。
蠕虫病毒	利用网络进行复制和传播的恶意程序，能够在短时间内大范围传播。
勒索病毒	利用各种加密算法对文件进行加密，感染此病毒一般无法解密，如WannaCry等。
木马程序	特洛伊木马，可受外部用户控制以窃取本机信息或者控制权、盗用用户信息等的程序，可能会占用系统资源。
DDOS木马	用于控制肉鸡对目标发动攻击的程序，会占用本机带宽攻击其他服务器，影响用户业务的正常运行。
后门程序	黑客入侵系统后留下的恶意程序，通过该程序可以

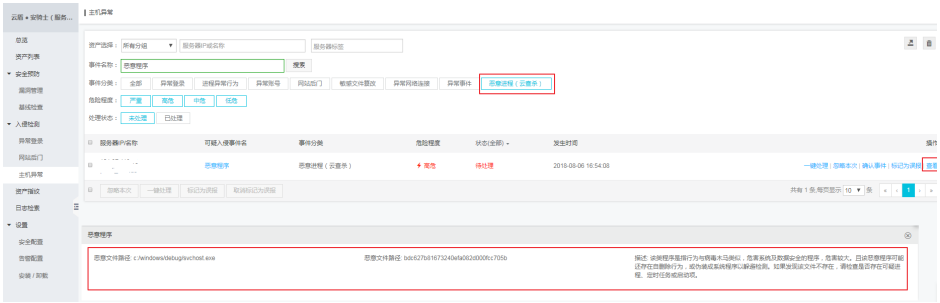
	随时获得主机的控制权或进行恶意攻击。
感染型病毒	运行后感染其他正常文件，将可能携带有感染能力的恶意代码植入正常程序，严重时可能导致整个系统感染。
恶意程序	其他威胁系统和数据安全的程序，比如黑客程序等。

云查杀的优势

- **自主可控**
  基于自主研发的深度学习、机器学习能力及大数据攻防经验，并结合多引擎检测能力，为用户提供全面、实时的病毒检测服务。
- **轻量**
  云查杀服务仅占用约1%的CPU、50MB内存，对业务影响小。
- **实时**
  获取进程启动日志，实时监控病毒程序的启动。
- **统一管理**
  云盾控制台支持对所有主机进行统一管理，实时查看所有主机的安全状态。

云查杀应用案例

检测



隔离

恢复

暴力破解

暴力破解拦截

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将攻击源 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

登录 服务器安全（安骑士）管理控制台。

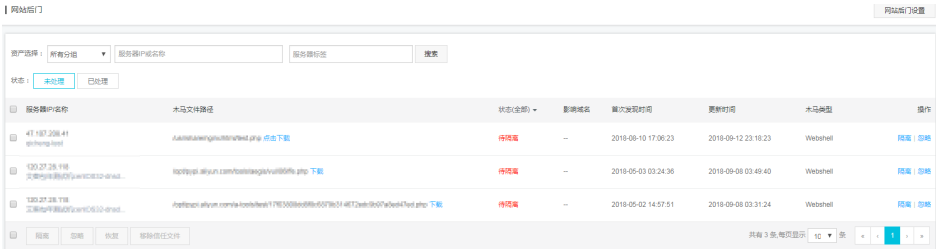
定位到 **事件** > **异常登录**，选择 **暴力破解拦截**，查看您的安骑士已防护的服务器上三天内的暴力破解拦截记录。

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。

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。

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 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。

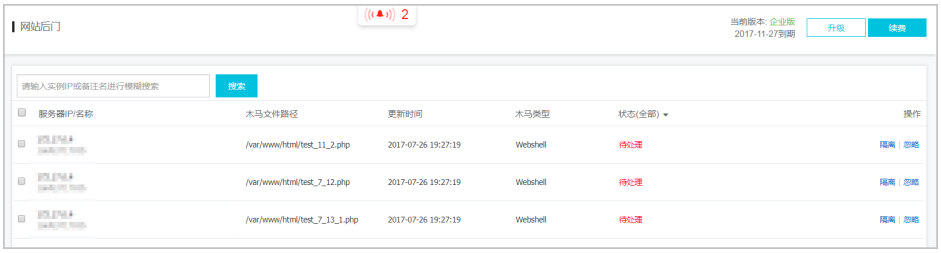
您也可以在安骑士控制台手动添加需要检测的Web目录，详情参见**操作步骤5**。

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

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。



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。

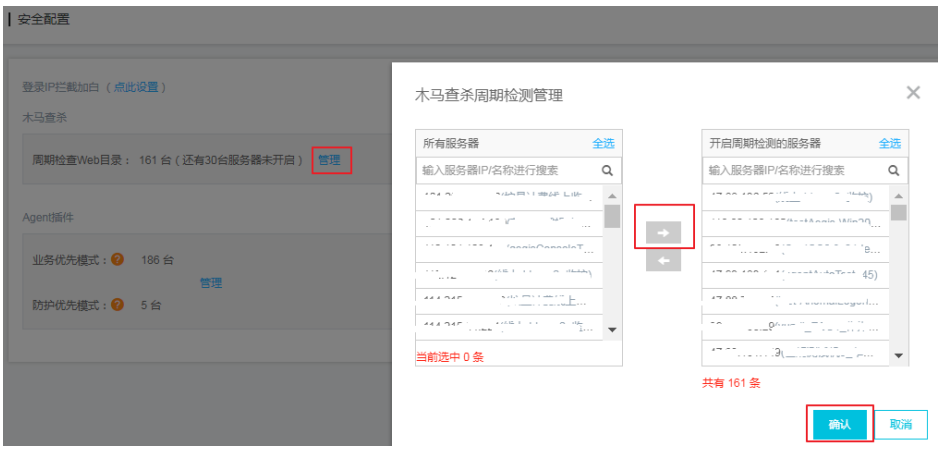
  忽略： 忽略该后门文件后，安骑士将不再对此文件提示风险告警。

  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。

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。



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。

资产指纹

监听端口

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。

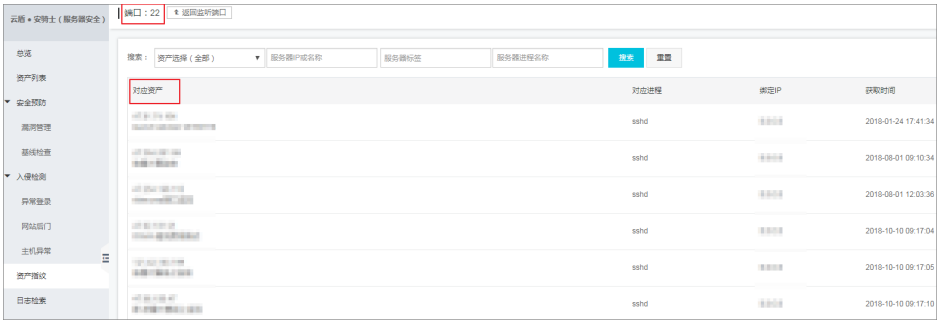
目前监听端口的数据收集为**每小时**收集一次。

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：

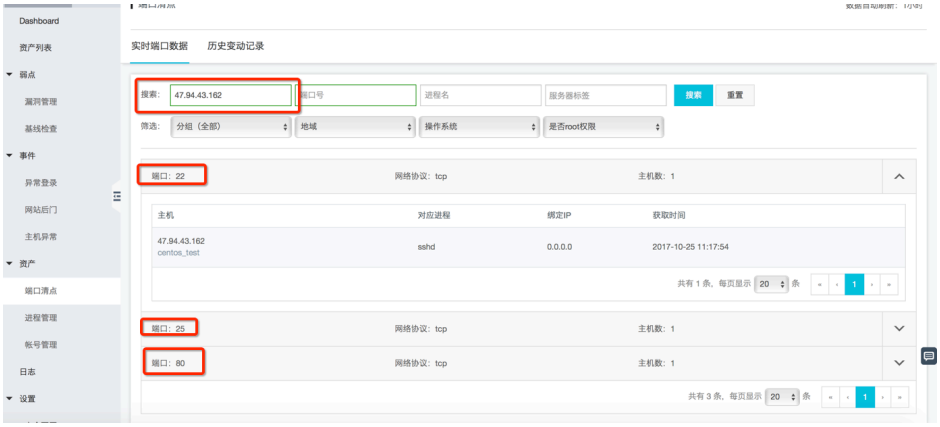
- 监听单个端口的所有服务器信息。
- 一台服务器开放的所有端口信息。
- 异常监听端口的历史变动信息，可通过历史记录查看监听时间等信息。

- 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）

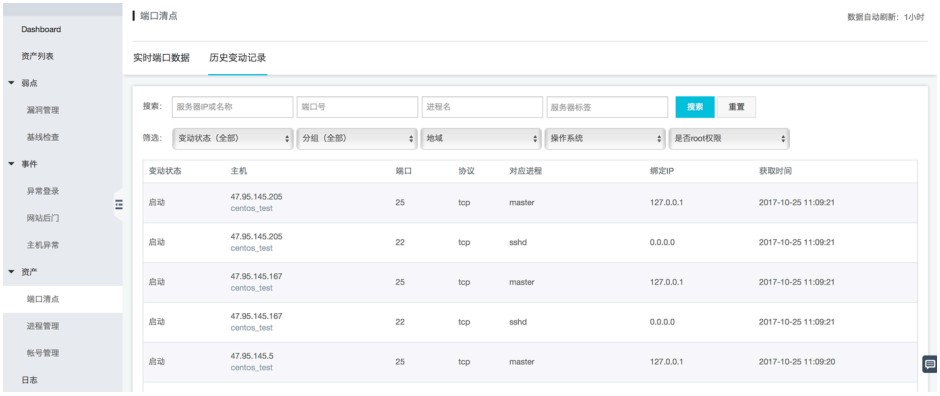
查看监听单个端口的所有服务器信息



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

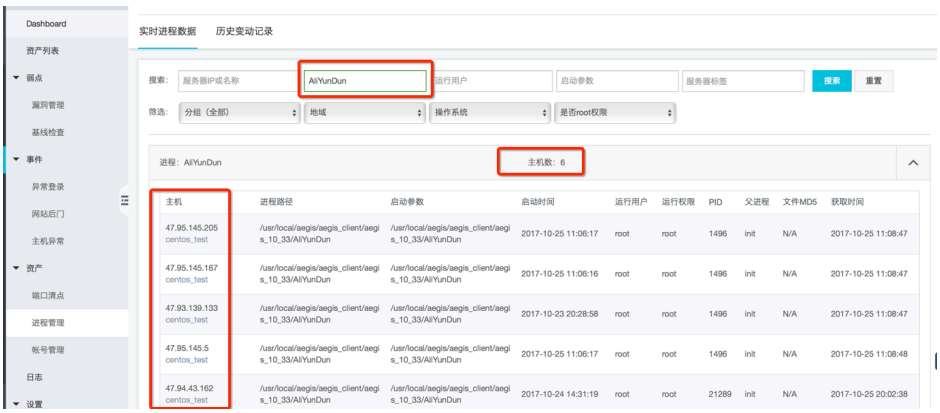


运行进程

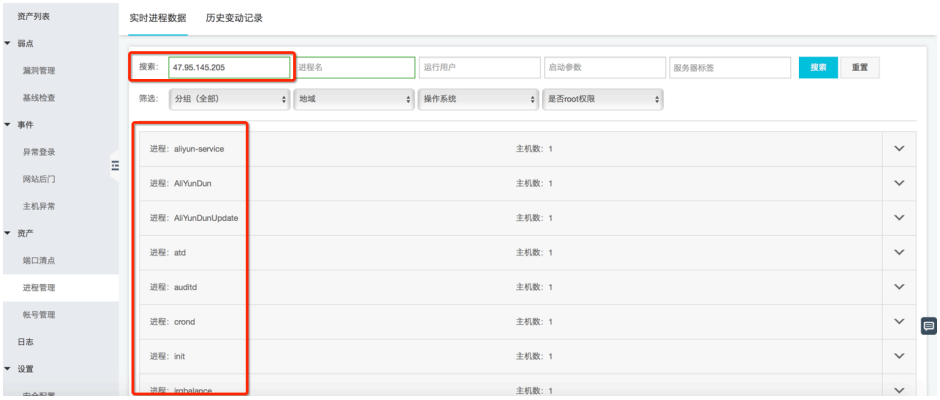
运行进程

- 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）

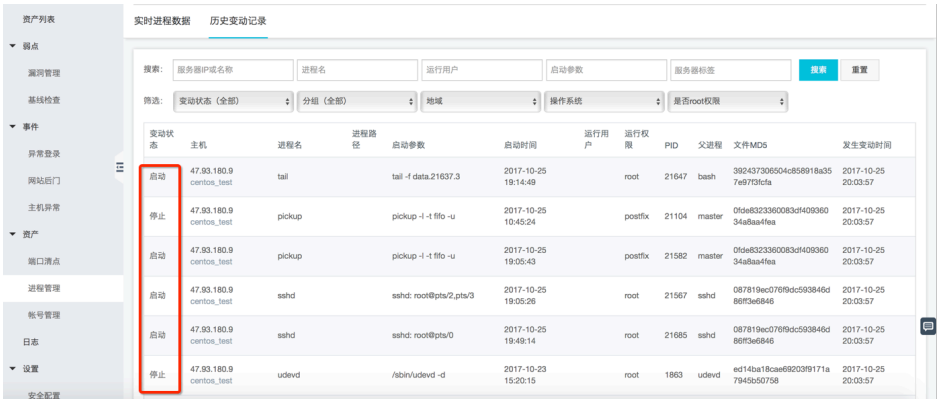
清点一个进程有多少服务器在运行



清点一台服务器运行了多少个进程



进程历史变动



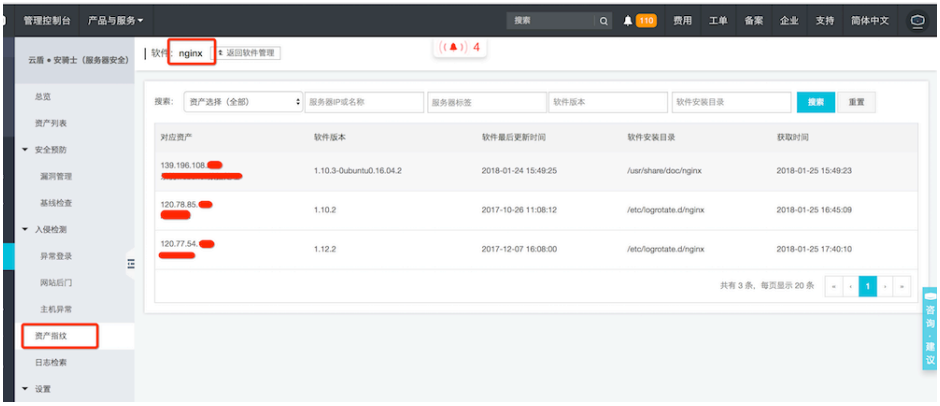
软件版本管理

软件版本管理

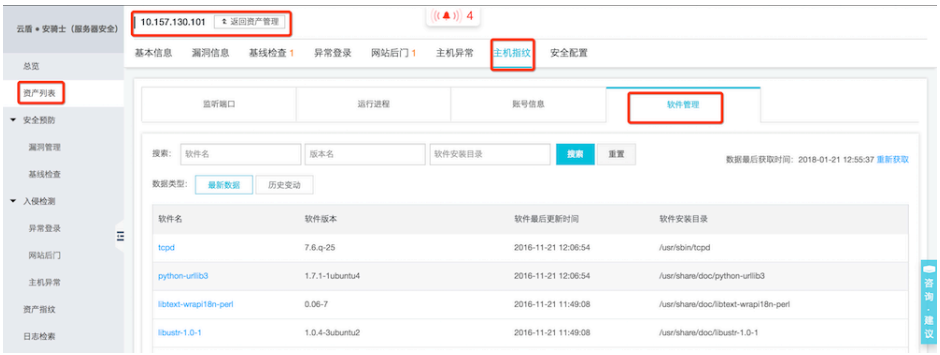
- 功能版本：企业版

- 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

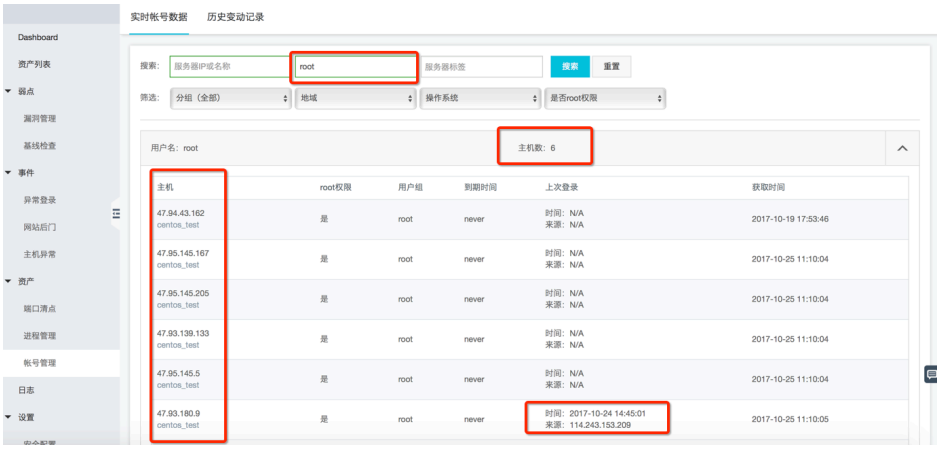


账号信息

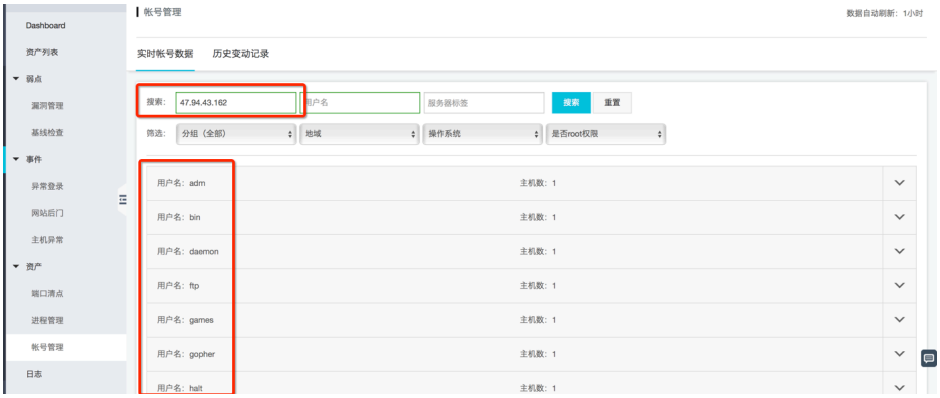
账号管理

- 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）

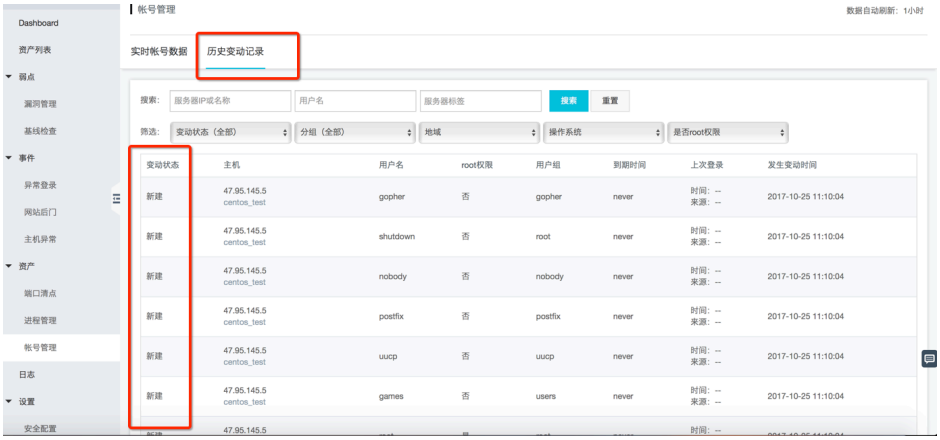
清点一个账号有多少服务器创建了



清点一台服务器创建了多少账号



账号历史变动



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

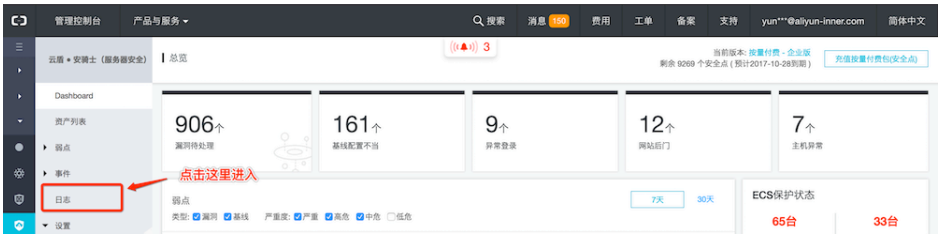
- **安全事件分析**： 主机发生安全事件后，通过日志功能进行调查，评估资产受损范围和影响。
- **操作审计**： 对主机的操作日志进行审计，对高危操作和严重问题进行细粒度排查。

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

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。

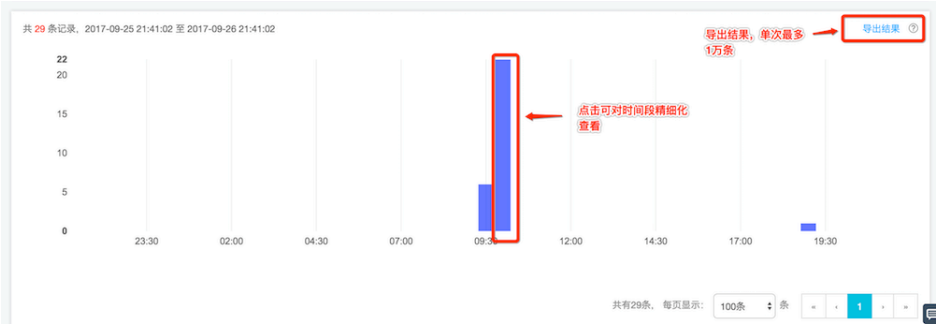


选择日志源、需要检索的日志字段，输入您想要检索的关键词，单击 **搜索**。

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，并单击日志列表右上角**导出结果**按钮将数据结果导出。



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）	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
	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
	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

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。

网页防篡改

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。

注意：

- **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。

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。

注意：

- **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

登录阿里云**安骑士管理控制台**。

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。

在安骑士包年包月购买页面**网页防篡改**区域框单击**开启**。

选择您所需开启网页防篡改服务的服务器数量。

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。

单击**立即购买**并完成支付。

注意：

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**扩大授权数**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**。

开启网页防篡改保护

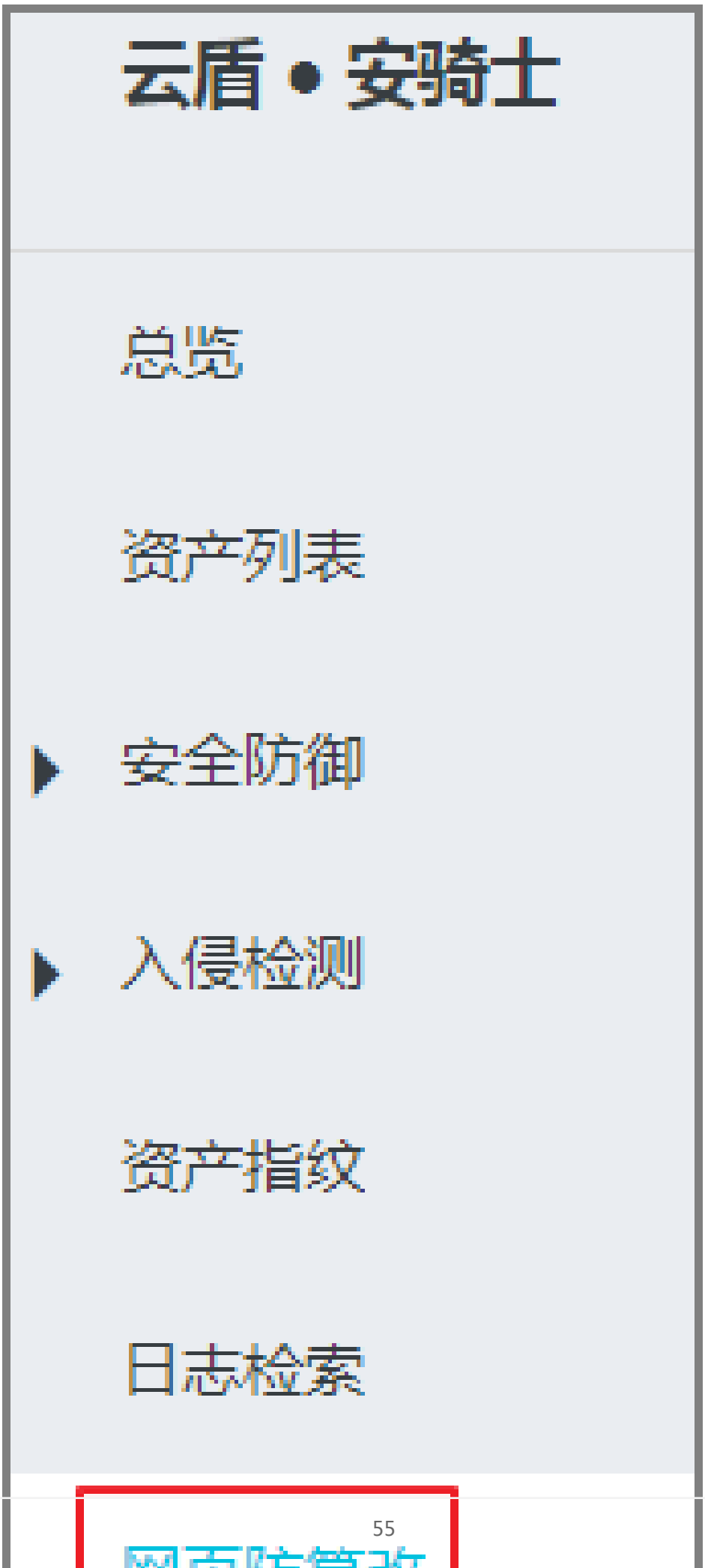
安骑士**企业版**可对主机开启网页防篡改防护，全面保护您网站的安全。

注意：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

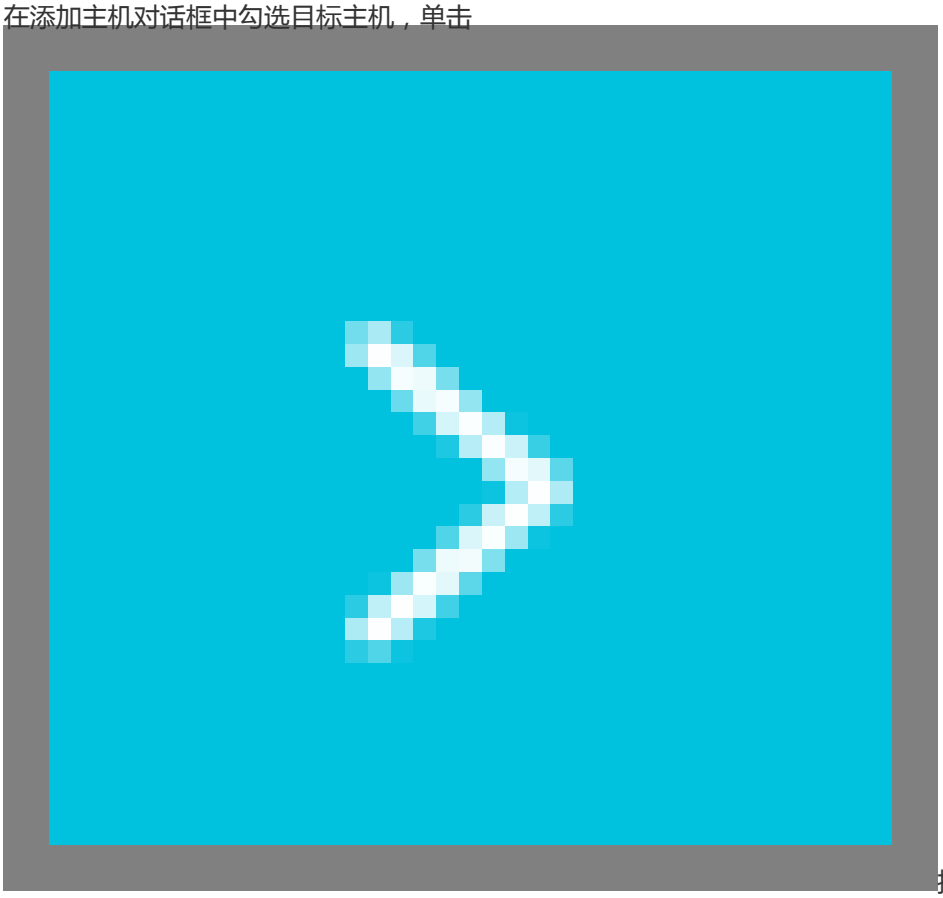
登录阿里云安骑士管理控制台。

在左侧导航栏单击**网页防篡改**。


云盾 • 安骑士
总览
资产列表
安全防御
入侵检测
资产指纹
日志检索

在网页防篡改页面单击左上角**添加主机**。

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。

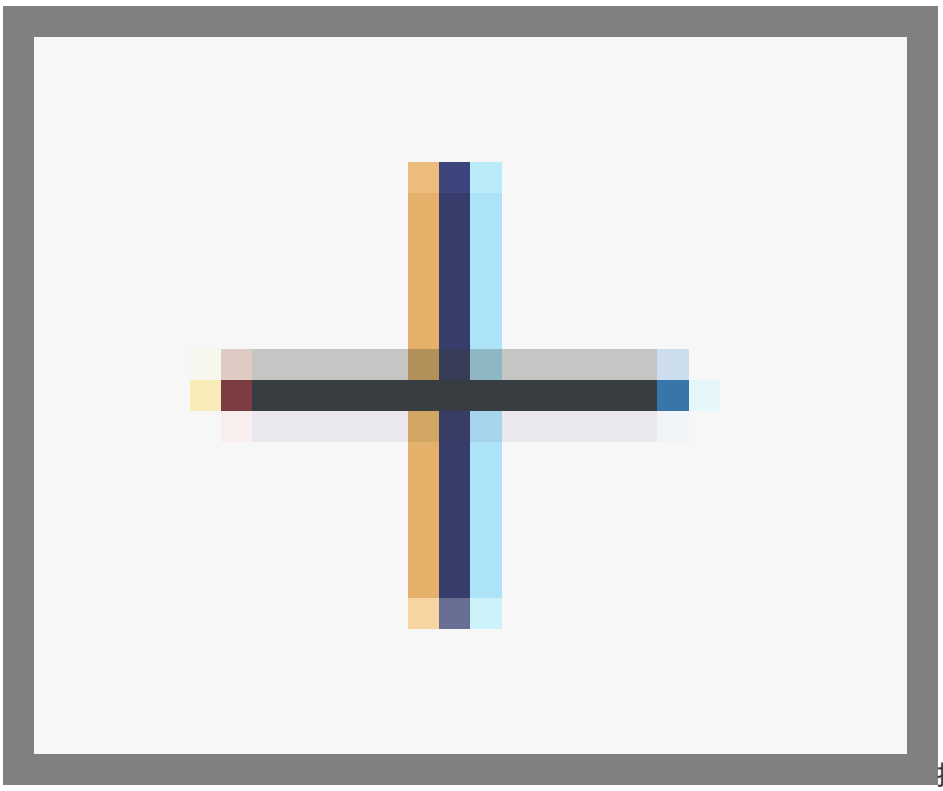
单击对话框右下角的**添加**，将目标主机添加到网页篡改防护列表中。

注意：

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

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。

单击**添加**打开**添加防护目录**对话框。

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。

注意：

- 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。

单击**确定**，保存防护目录配置。

注意：

每台服务器最多可添加10个防护目录；单个防护目录大小不超过3G；单个防护目录下的文件夹数量不超过4000个、防护目录文件夹层级少于20个。

建议您开启防护前检查是否有文件夹目录层级超过20，文件夹个数是否超过4000个，整个防护目录大小是否大于3G。

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

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**。

注意：

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。

防护服务状态列表

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。	-
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**。

防护异常状态处理

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

登录阿里云安骑士管理控制台。

在左侧导航栏单击**入侵检测 > 主机异常**。


云盾 • 安骑士（服务器安全）
总览
资产列表
安全预防
入侵检测
异常登录
网站后门
主机异常

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。

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。

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**。

扩充授权数

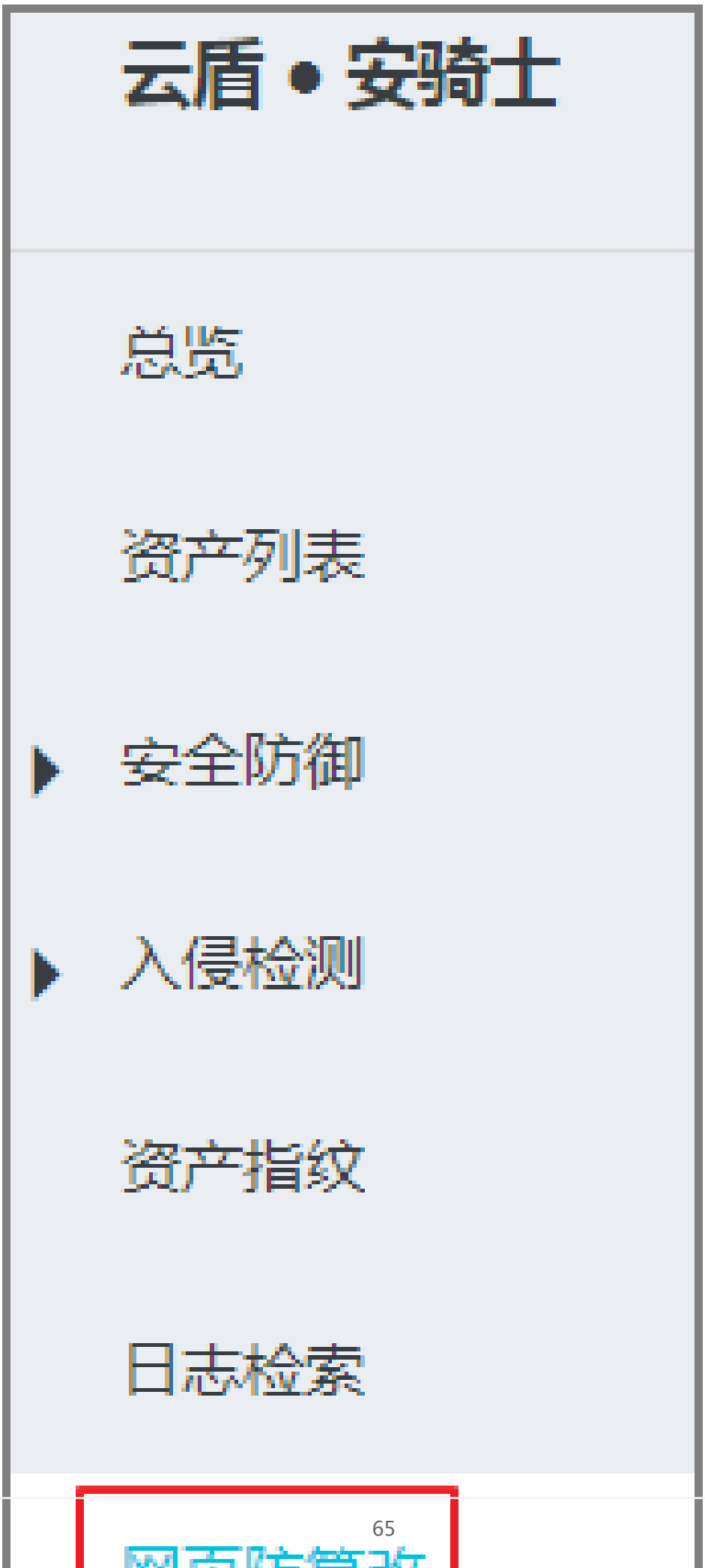
开启每台服务器的网页防篡改功能就会消耗**1个**网页防篡改授权数（网页防篡改服务器台数）。您可在**网页防篡改**页面右上角查看您**已购买的授权数**和**已使用的授权数**。

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

登录阿里云安骑士管理控制台。

在左侧导航栏单击**网页防篡改**。


云盾 • 安骑士
总览
资产列表
安全防御
入侵检测
资产指纹
日志检索

在网页防篡改页面右上角单击**扩充授权数**。

在变配页面选择需要新增授权服务器的数量。

勾选右下角的**服务协议**并完成支付。

设置

安全配置

登录 IP 白名单设置

为了避免安骑士对您的正常登录行为进行误报（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，多次输入密码错误可能会触发误拦截等），您可将此类 IP 添加至登录 IP 白名单中，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 的登录行为进行拦截。

登录 服务器安全（安骑士）管理控制台。

定位到 **设置** > **安全配置**，在 **登录安全** 区域，单击 **常用IP白名单** 选项右侧的 **添加**。

输入要添加至登录白名单的 IP，并选择对应的服务器，单击 **确认**，即可为您选定的服务器添加登录白名单 IP。

病毒自动隔离

安骑士**企业版**病毒自动隔离服务目前支持针对部分主流勒索病毒、DDOS木马进行主动防护和主动隔离。后续将陆续支持更多病毒类型，建议您启用该功能，加固主机安全防线。

注意：

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。详见**功能详情**。

病毒自动隔离功能详细说明参见**功能详情功能列表**。

开启病毒自动隔离功能后，新购的ECS会默认开启该功能。

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。

  您可参考**安骑士云查杀**功能对误报的事件进行处理或从**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. 登陆安骑士管理控制台。

   在控制台弹出的**病毒自动隔离功能已上线**的温馨提示对话框中勾选**开通自动隔离**，并单击**确定**，开通病毒自动隔离服务。

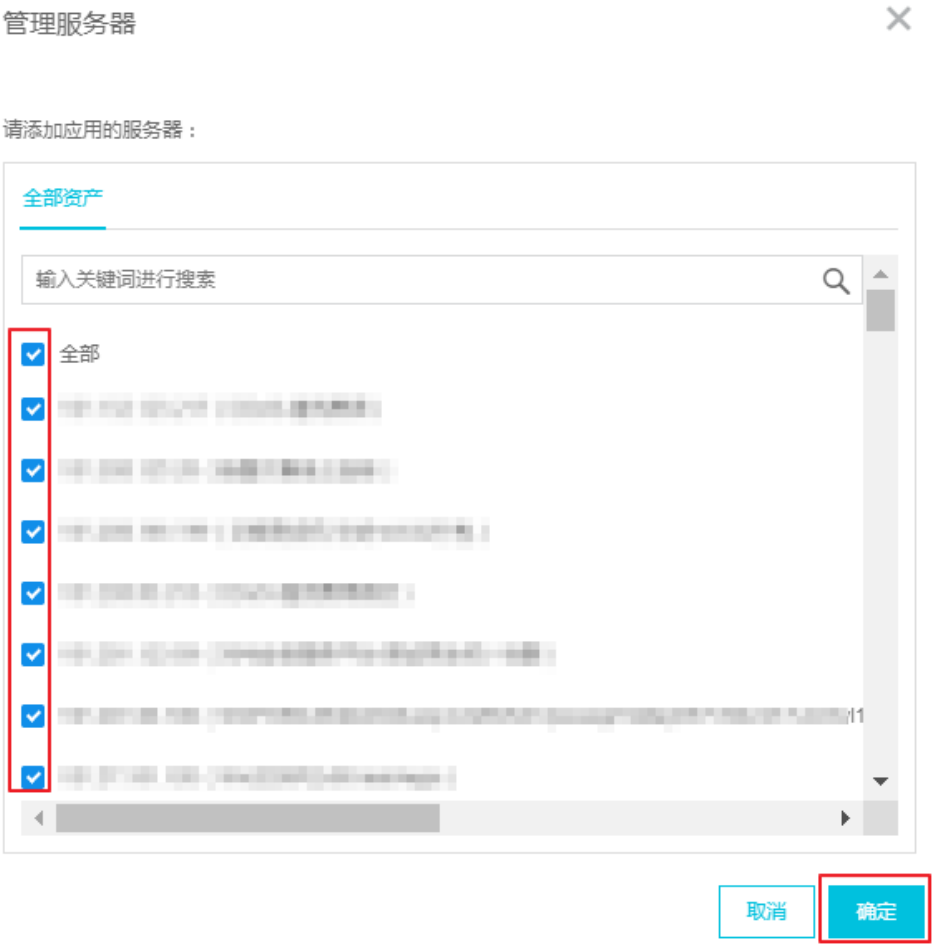
   注意：

   病毒查杀功能上线后，企业版用户首次登陆安骑士控制台会弹出温馨提示。该提示7天内弹出一次，勾选开通**自动隔离**功能后该温馨提示将自动关闭。

   如未勾选**开通自动隔离**，该功能将不会被开启。建议您开启该功能，加固主机安全。

3. 在左侧导航栏单击**设置** > **安全配置**，打开**安全配置**页面。

   在病毒查杀模块单击**管理**，打开**管理服务器**对话框。



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。

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。

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

对高威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。

安装/卸载

安骑士Agent插件安装/卸载操作详见安装Agent、卸载Agent。