阿里云
安骑士

用户指南

文档版本：20190410

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 什么是安骑士Agent插件?

Agent是安骑士部署到云服务器操作系统中的轻量化进程，主要功能是根据用户配置的安全策略上报服务器存在的安全风险和新增的安全事件数据，同时响应用户和安骑士云端防护中心的指令，实现对云服务器上的安全威胁清除和恶意攻击拦截。

工作原理

安骑士 Agent 每隔5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，安骑士服务器端会及时判定该服务器不在线，且在安骑士管理控制台中该服务器的保护状态会显示为离线。

说明:

- 如果未安装agent，您将无法使用安骑士提供的服务。
- 安骑士Agent与服务端网络连接断开或程序退出都可能导致服务器保护状态离线，详情参见Agent离线排查。

Agent相关进程

安骑士 Agent 进程运行账号:

- Windows：Agent进程在Windows 系统的服务器上以system账号运行。
- Linux：在Linux系统的服务器上以root账号运行。

安骑士 Agent 包含以下两个主要进程:

Agent进程名称	进程功能	进程所在路径
AliYunDun	该进程用于与安骑士服务器建立连接。	· 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	该进程用于定期检测安骑士Agent是否需要升级。	· 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。

您可在安骑士控制台定位到设置 > 安全配置 > Agent插件，在Agent插件模块可查看Agent不同优先模式运行的服务器数量。

单击管理可将您的服务器设置为业务优先模式或防护优先模式。

说明:

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。

1.2 安装Agent

安装安骑士Agent 插件后才能对您的主机提供防护。安骑士目前可支持对离线Agent进行一键自动安装。

一键安装功能无需您单独下载插件或执行任何命令安装Agent。

若您的服务器安骑士 Agent 显示离线状态，请参照本文档描述的内容安装安骑士 Agent 插件。

您可以在安骑士控制台资产列表页面查看您所有服务器的Agent 在线状态，或在 设置 > 安装/卸载 页面查看Agent插件已离线的所有资产情况。

如果出现离线情况请参考*Agent* 离线排查。

前提条件

安装Agent前请确认您安装安骑士服务器的环境：

- **阿里云服务器可直接安装Agent。**
- **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，指定以下任意一个安骑士服务端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`

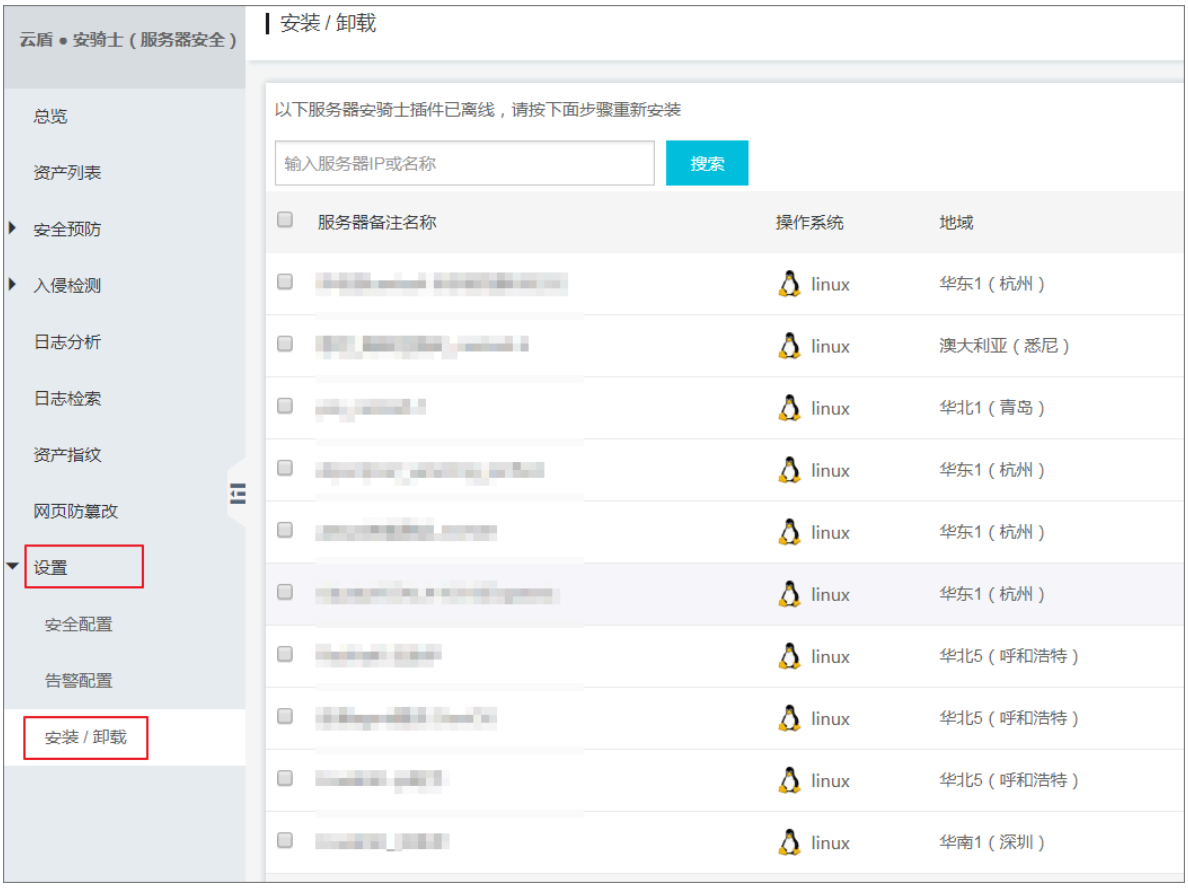
说明:

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。

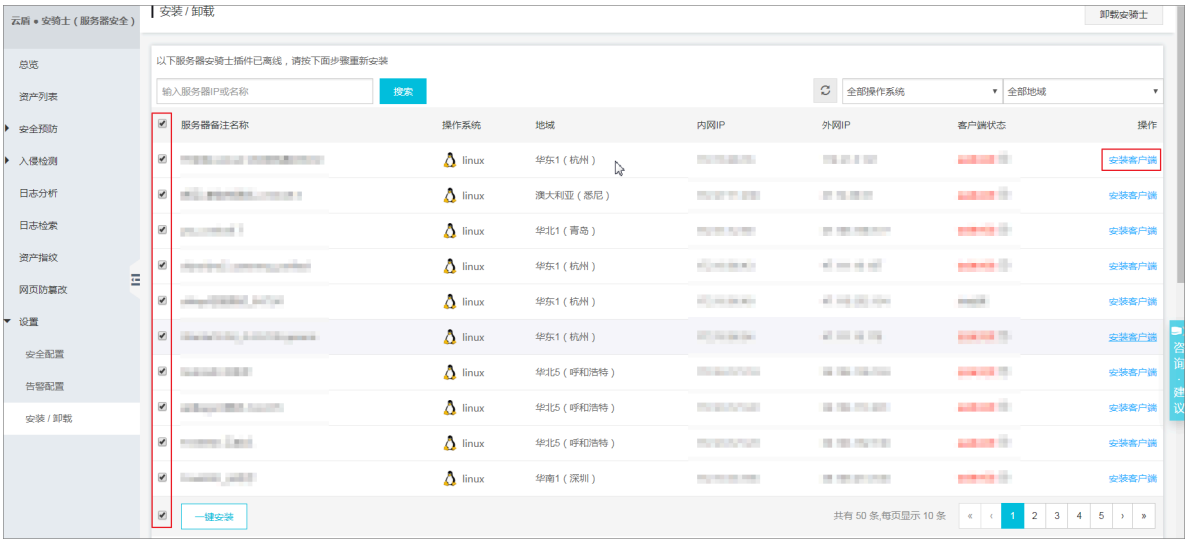
一键安装Agent

安骑士支持对阿里云服务器一键安装Agent，非阿里云服务器需执行手动安装。

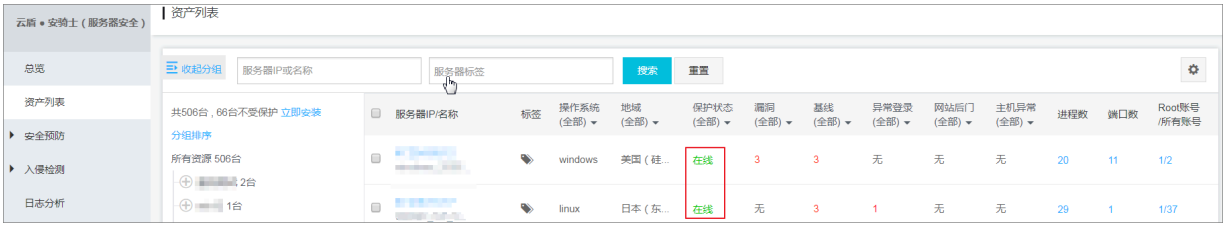
1. 登录云盾安骑士管理控制台。
2. 单击 设置 > 安装/卸载 。



3. 单击操作栏的安装客户端对单个服务器安装Agent或勾选多台服务器名称后单击左下角一键安装对多台服务器执行批量安装Agent。



安骑士 Agent 插件安装完成约五分钟后，您即可在云盾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。



一键安装后如果客户端状态显示为安装失败并提示未安装云助手，请先安装云助手后再重试。

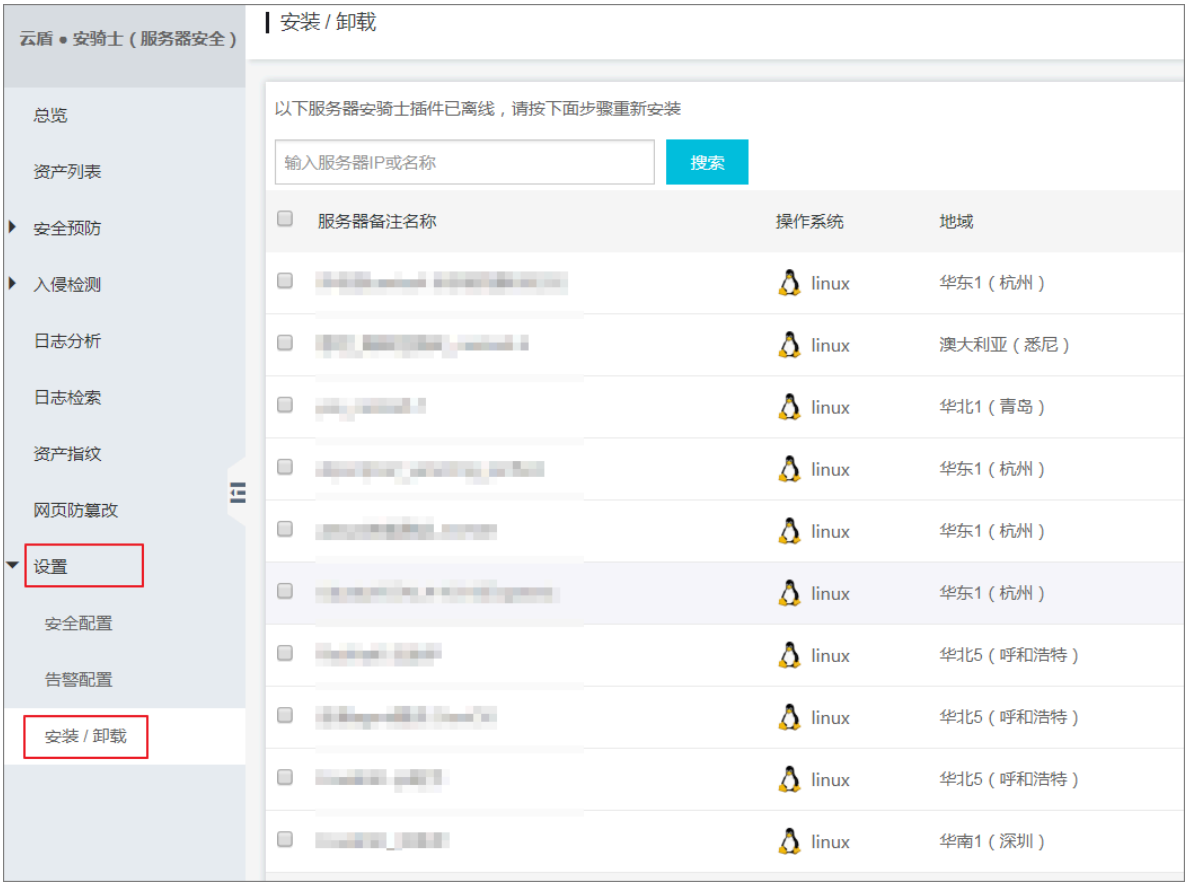
手动安装Agent

以下情况不支持一键自动安装、必须执行手动安装Agent：

- 您的服务器为非阿里云服务器
- 网络类型为经典网络
- ECS不在支持的区域内
- 服务器操作系统为Windows 2008、Redhat、FreeBSD、Coreos
- 未安装云助手
- 服务器未开启

1. 登录云盾安骑士管理控制台。

2. 单击 设置 > 安装/卸载 。


云盾 • 安骑士（服务器安全）
总览
资产列表
安全预防
入侵检测
日志分析
日志检索
资产指纹
网页防篡改
设置
安全配置
告警配置
安装 / 卸载
安装 / 卸载
以下服务器安骑士插件已离线，请按下面步骤重新安装
输入服务器IP或名称
搜索
服务器备注名称
操作系统
地域
linux 华东1（杭州）
linux 澳大利亚（悉尼）
linux 华北1（青岛）
linux 华东1（杭州）
linux 华东1（杭州）
linux 华东1（杭州）
linux 华北5（呼和浩特）
linux 华北5（呼和浩特）
linux 华北5（呼和浩特）
linux 华南1（深圳）

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。

e. 完成安装后，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。

一键安装功能支持的地区

表 1-1: 支持的地区

支持的地区	地区名称
亚太	华东 1（杭州）
	华东 2（上海）
	华东 2 金融云
	华北 1（青岛）
	华北 2（北京）
	华北 3（张家口）
	华北 5（呼和浩特）
	华南 1（深圳）
	香港
	新加坡
	澳大利亚（悉尼）
	马来西亚（吉隆坡）
	印度尼西亚（雅加达）
	日本（东京）
欧洲与美洲	德国（法兰克福）
	英国（伦敦）
	美国（硅谷）
	美国（弗吉尼亚）
中东与印度	印度（孟买）

支持的地区	地区名称
	阿联酋（迪拜）

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：

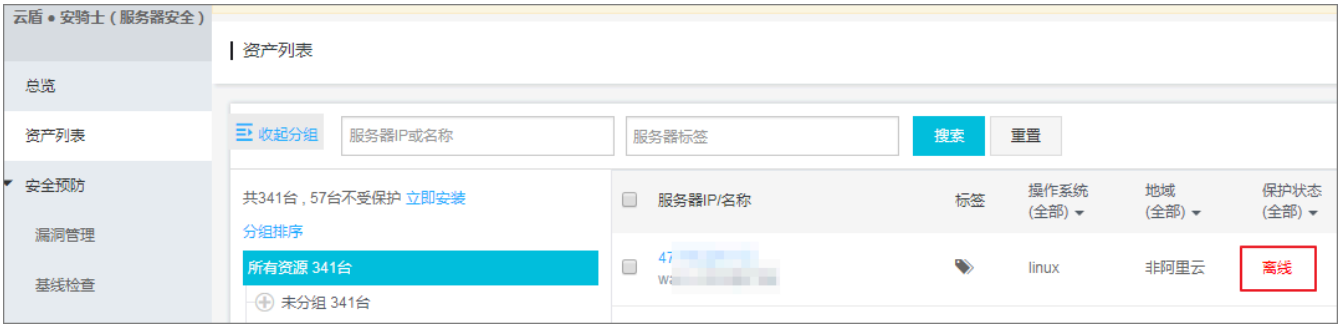
- Windows：C:\Program Files (x86)\Alibaba\Aegis
- Linux：/usr/local/aegis

1.3 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。

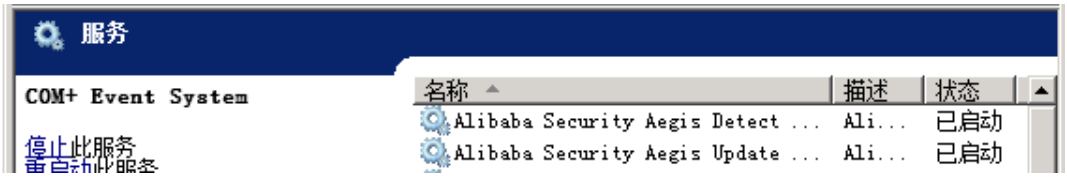
映像名称	用户名	CPU	内存(专用工作集)
AliYunDun.exe *32	SYSTEM	00	6,648 K
AliYunDunUpdate.exe *32	SYSTEM	00	1,000 K

   - 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。

2 安全预防

3 入侵检测

3.1 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. 点击入侵检测 > 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。

3.2 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。

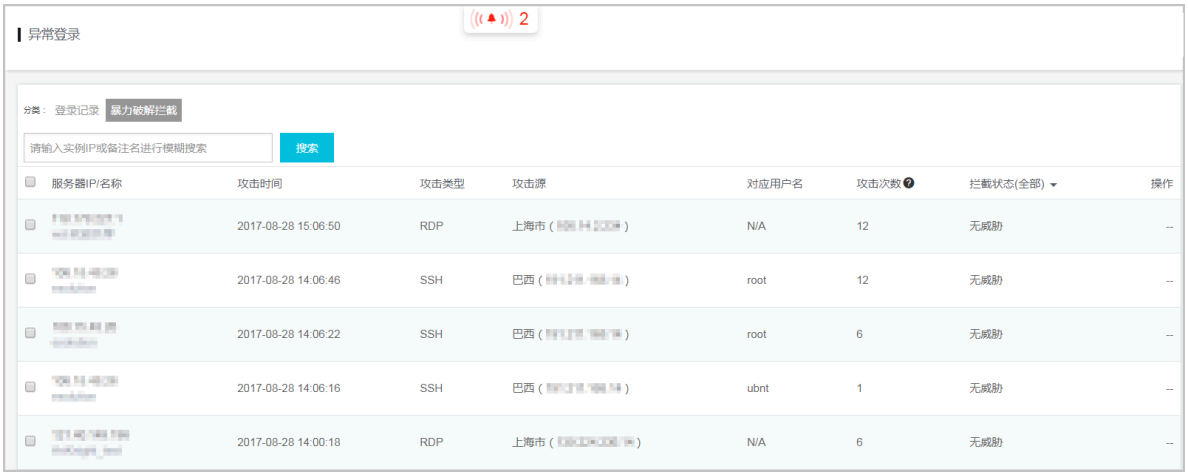
暴力破解拦截功能原理

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

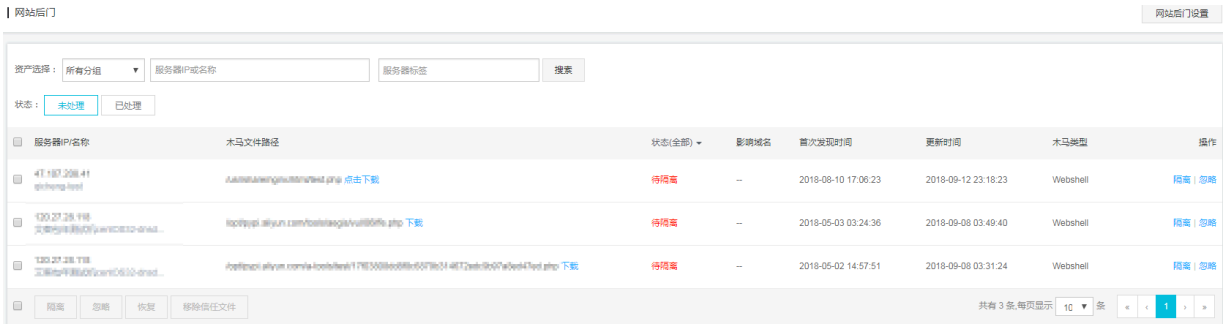
1. 登录 服务器安全#安骑士#管理控制台。
2. 定位到 入侵检测 > 异常登录，选择 暴力破解拦截，查看您的安骑士已防护的服务器上三天内的暴力破解拦截记录。



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。

3.3 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。

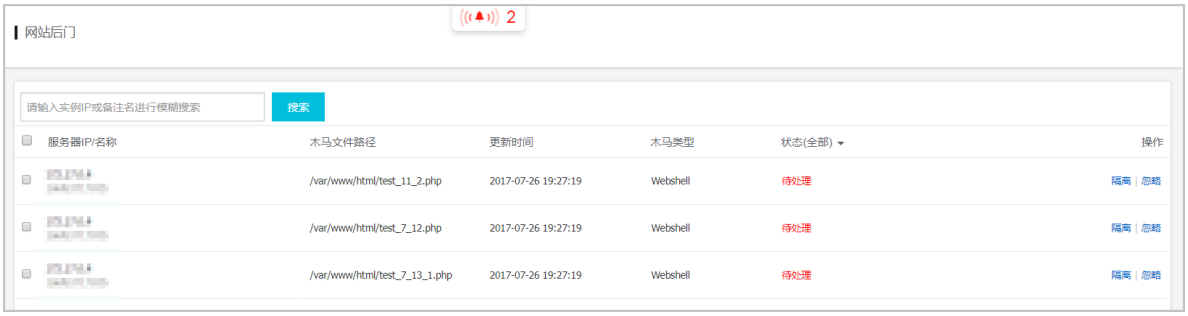
您也可以在安骑士控制台手动添加需要检测的Web目录，详情参见操作步骤5。

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。

3.4 主机异常