阿里云
安骑士

最佳实践

文档版本：20190415

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。

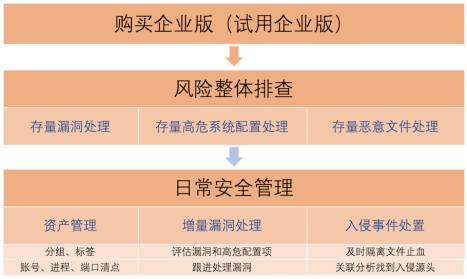
通用约定

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 如何用好安骑士

安骑士最佳实践图



一句话解释什么是安骑士

安骑士是主机安全领域的领导者，已为全球百万级主机提供安全防护服务，具备漏洞智能化管理、基线配置检查、病毒查杀积极防御等功能，是等级保护合规和纵深防御安全体系的必备产品。

实践目标

- **充分了解安骑士产品的功能，可使用安骑士进行日常的安全管理，"看见”并“解决”安全问题，提高工作效率。**
- **学会安全管理技能：漏洞检测和处置方法、风险配置修复、入侵事件排查、进程端口账号等资产管理。**

产品功能

- **精准防御：多病毒检测引擎配合阿里云多年安全经验，支持主流病毒自动查杀。**
- **漏洞管理：全面的漏洞管理，包括漏洞检测和漏洞修复，让您的资产漏洞风险降到最低。**
- **网页防篡改：防止网站被非法植入涉恐涉政、暗链、木马、后门等内容，保障网页信息正常运行。**
- **入侵检测系统（云查杀）：黑客即入侵实时预警，即使被入侵也可快速发现和止血。**
- **基线检查：支持安全配置的全面安全检查，帮助您更好地加固您的主机安全。**
- **资产指纹：进程、端口、账号、软件版本的清点。**
- **主机日志检索：记录主机所有内容。**

为什么要做好服务器安全？为什么服务器安全着重在漏洞管理？

- **所有的黑客攻击最终都会落在主机上，我们的数据、程序都是运行在主机上，只有主机才能最近感知到黑客的动作，安全讲究纵深防御，主机侧安全是必不可少的。**
- **云服务器跟传统PC不同，PC会主动去访问互联网，一不小心上了挂马网站和运行了恶意软件，所以需要的是防病毒产品。而云服务器ECS不同，它只有可能“被”互联网来访问，相当于**

一个黑盒子，那么黑客要入侵，必须要找到“漏洞”才行，所以安骑士着重帮助客户在事前做好漏洞检测和修复工作。

购买企业版或试用

- 当前产品有两种付费模式：包年包月和按量付费（安全点）。包年包月推荐预算固定ECS台数固定的用户购买，按量付费模式推荐ECS弹性变动较大的用户购买。更多详情参见购买说明。
- 您也可以开启企业版试用体验功能，默认为7个自然日。如试用过企业版后还需申请企业版试用，可提交工单。
- 开通后无需进行产品特殊配置，购买或者开启试用后，将自动为您完成配置，您直接使用控制台进行操作即可。
- 开通企业版后，最多需要2天进行安全数据收集和分析处理，系统自动完成，暂不支持手动触发全面安全扫描，所以您开通后在2天后可看到安骑士检测到的全部事件。

解决漏洞问题

如何解决软件漏洞?

- 如果是Windows漏洞：可使用安骑士的一键修复功能进行修复。
- 如果是Web应用漏洞：可根据提示的修复方案进行手动修复，一般都是业务的逻辑漏洞。

如何解决系统软件漏洞?

1. 评估危害（重要）：对于Linux系统，会报出很多软件漏洞，您要进行仔细评估后决策是否修复（例如A漏洞为高危漏洞，需要利用10端口进行远程入侵，但是当前对外未开放10端口，那么此时您就可以忽略该漏洞；还有一些内核，标题中带kernel的漏洞，可能会造成业务影响，也请仔细评估，或者通过搜索引擎查询更加全面的方案）。
2. 生成修复命令：产品支持一键生成修复命令，帮助您快速修复。
3. 验证：修复完成后，可以快速进行修复成功的验证操作（不主动验证，系统也将在48小时内自动验证）。
4. 忽略或加白：如果您确认该漏洞不会对您的系统安全造成威胁、不想再关注该漏洞，您可对漏洞进行忽略或加入白名单。

> 说明:
>
> - 在执行系统及软件漏洞的修复时候，建议您进行快照备份后再操作，即使修复后对业务造成影响，也可以快速回滚。
> - 实在不知道如何评估，请联系大客户经理找云盾专家支持，或者直接购买“安全管家”服务，由安全专家来评估和指导您需要修哪些漏洞。

如何解决Web_CMS漏洞?

- 您可查看漏洞详情或危害，使用安骑士的立即修复功能进行修复即可。
- 如果您觉得漏洞不会对主机安全构成危害，可对漏洞进行忽略。

解决系统高危配置问题

- 开通或试用企业版后需要24小时候才会启动扫描，安骑士才会显示相关数据。
- 当前安骑士检测的配置项包括：弱口令、密码长度不够、注册表配置不当、数据库配置不当等。
- 如果基线提示有需要解决的项目？

  1. 评估影响：查看项目等级和内容，您需要评估该风险项对业务的影响（例如您公司对密码长度有要求，那么就可以检测出配置不当的机器，若无要求，您可以采取忽略操作）。
  2. 查看控制台修复建议，根据修复建议进行修复。
  3. 验证：修复完毕后，可快速验证是否修复完成（若不立即验证，系统在48小时内会自动验证）。

  对于无需修复的基线提示，可选择忽略。

发生安全事件处置方法

服务器有异常登录？

- 服务器被异常登录了将会给您提醒，建议您确认是否为公司员工行为，如在非常用地址登录行为。
- 建议您在日志模块关联搜索下该用户的登录详情，时间，以及登录后这个用户运行了哪些命令行、启动了哪些进程。
- 若事件为“暴力破解成功”，此时要引起高度重视，黑客已经猜中了密码并且登录了ECS，您急需要进行改密码操作，并且排查是否有入侵后的资损。

服务器发现了有网站后门？

- 针对网站的脚本文件扫描，也是我们常说的Webshell、挂马文件，黑客利用该文件可进行页面篡改、SEO暗链、数据窃取等操作。
- 文件是脚本文件，脱离web目录是无法运行的没有危害，所以安骑士也只会监测web目录的文件变动。
- 一旦发现该类型文件会给您推送告警，此时您登录控制台只获知到文件的路径，您可确认下是否为正常的业务文件，如果非正常业务文件，直接操作隔离即可。
- 若发现有误报，也可以进行忽略或者联系我们来进一步排查。

服务器有其他入侵异常事件？

- 包括病毒查杀、进程异常行为、恶意源下载，当前都是可以实时检测到的。
- 一旦发生，可登录控制台进行查看和处理。

做好资产管理和清点

分组和标签

- 当ECS台数多，安全事件和告警也会随之增多，借助分组和标签系统，在处理事件的时候，可以快速捞出来那些重要机器优先处理。

端口、进程、账号清点

- 定期收集服务器的对外端口监听、进程运行、账号信息，并对变动信息进行记录，便于资产清点和历史变动查看。
- 可使用搜索栏到达如下效果：
  - 清点一个端口（或一个进程、一个账号），有多少台服务器正在监听（或运行、创建）。
  - 清点一台服务器，监听了多少端口（或运行了多少进程、创建了多少账号）。
  - 清点一台服务器，端口监听（进程情况、账号情况）的历史变动信息。
  - 建立端口基线（进程基线、账号基线），发现非法的端口开启（非法的进程启动、非法的账号创建）。

进阶1：使用日志功能还原安全事件

- 如发生了入侵事件，可根据线索还原出入侵链路，举例：
  - ECS的CPU占用高，系统业务有影响。
  - 登录安骑士控制台发现报告了“异常事件-挖矿进程”。
  - 日志检索：根据进程名检索出，挖矿进程的启动。
  - 日志检索：通过启动的用户名，再检索登录流水，发现了时间基本吻合。
  - 日志检索：通过网络连接，发现了挖矿进程连接“矿池IP”的行为。
  - 查看基线检查，发现用户名存在弱口令告警。
  - 还原完成：弱口令被黑客登录入侵种植挖矿程序，通过终止进程、修复弱口令问题解决。
- 不仅仅要解决入侵事件，更要找到入侵的源头并解决，治标且治本。

进阶2：日常的安全管理

- 多维度安全管理：
  - 单台ECS维度：在资产列表可针对特殊机器，快速检索和统一查看当前未处理的漏洞和事件。
  - 功能维度：漏洞管理、基线检查，根据项目排查，如弱口令统一清点，到底有多少台服务器存在此类高危问题。

2 快速掌握 ECS 安全态势

安骑士是一款经受200万+主机稳定性考验的主机安全加固产品，拥有自动化实时入侵威胁检测、病毒查杀、漏洞智能修复、基线一键核查等功能，是构建主机安全防线的统一管理平台。

安骑士企业版和基础版功能详情参见功能特性。

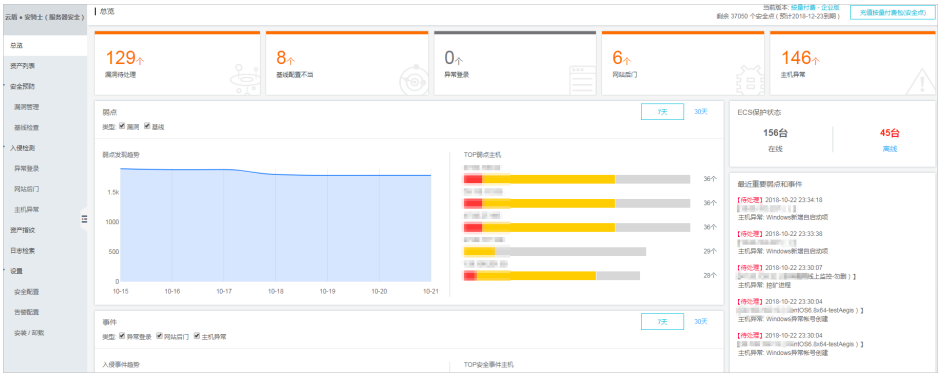
安骑士功能优势参见产品优势。

安骑士企业版提供病毒自动隔离服务，可对目前部分主流勒索病毒（如WannaCry和Globelmposter）、DDOS木马（如XorDDos和BillGates）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。详见安骑士开启病毒查杀自动隔离。

您可以打开ECS控制台概览页面，单击安全概览模块下面的阿里云云盾图标跳转到安骑士总览页面，查看ECS的安全详情。

跳转到安骑士控制台总览页后，您可在总览页面查看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、已处理事件的数量等信息。

详细信息参见控制台总览。



单击待处理告警事件可进入对应的功能进行快速处理：

- 漏洞待处理
- 基线配置不当

- 异常登录
- 网站后门
- 主机异常

详细信息参见安骑士用户指南。

查看ECS实例安全详情

您可以打开ECS控制台实例页面，单击实例列表中的阿里云云盾图标 跳转到安骑士控制台资产列表页面，查看单个ECS实例的安全详情。

跳转到安骑士控制台后，在资产列表页面查看单个ECS实例的安全详情。

ECS实例的安全详情包含：

- 基本信息：

  包括ECS实例名称、ID、所在地区、公网/内网IP地址、主机操作系统、安骑士保护在线状态和分组信息等。

- 漏洞信息：

  检测ECS实例的系统漏洞和Web-CMS漏洞。

- 基线检查：

  检测ECS的系统、数据库、账号配置存在的风险点。

- 异常登录：

  检测ECS上的登录行为，对于在非常用登录地的登录行为提供告警。

- **网站后门：**

  检测ECS上是否存在Webshell后门文件。

- **主机异常：**

  检测ECS上是否存在异常事件并对异常事件进行处理。

- **主机指纹：**

  检测ECS上包含监听端口号、网络协议、对应进程和绑定监听IP等信息。

- **安全配置：**

  对漏洞管理、基线检查和登录安全设置进行配置。

详细信息参见安骑士用户指南。