Alibaba Cloud
云安全中心（安骑士）

用户指南

文档版本：20200605

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. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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

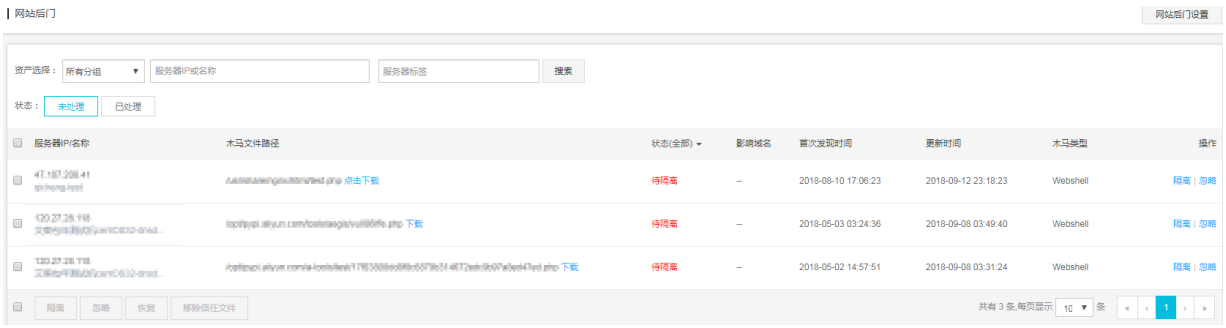
格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止：** 重置操作将丢失用户配置数据。
	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告：** 重启操作将导致业务中断，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意：** 权重设置为0，该服务器不会再接受新请求。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明：** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	单击**设置** > **网络** > **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令。	执行cd /d C:/window命令，进入Windows系统文件夹。
斜体	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。	switch {active|stand}

目录

1 入侵检测

1.1 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。

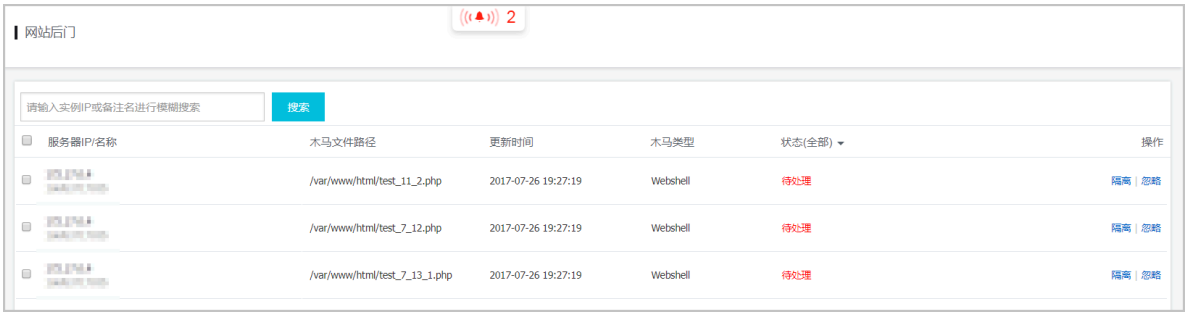
您也可以在安骑士控制台手动添加需要检测的Web目录，详情参见**操作步骤5**。

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。

1.2 主机异常

1.2.1 病毒云查杀

云盾安骑士病毒查杀（以下简称“云查杀”）集成了中国及中国以外地域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。
- **集成中国及中国以外地域主流病毒查杀引擎**：云查杀集成中国及中国以外地域多款优秀的杀毒引擎，可对病毒进行实时更新。
- **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对云查杀结果进行隔离和恢复处理。

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。

病毒类型	病毒描述
病毒型感染	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，例如黑客程序等。

云查杀的优势

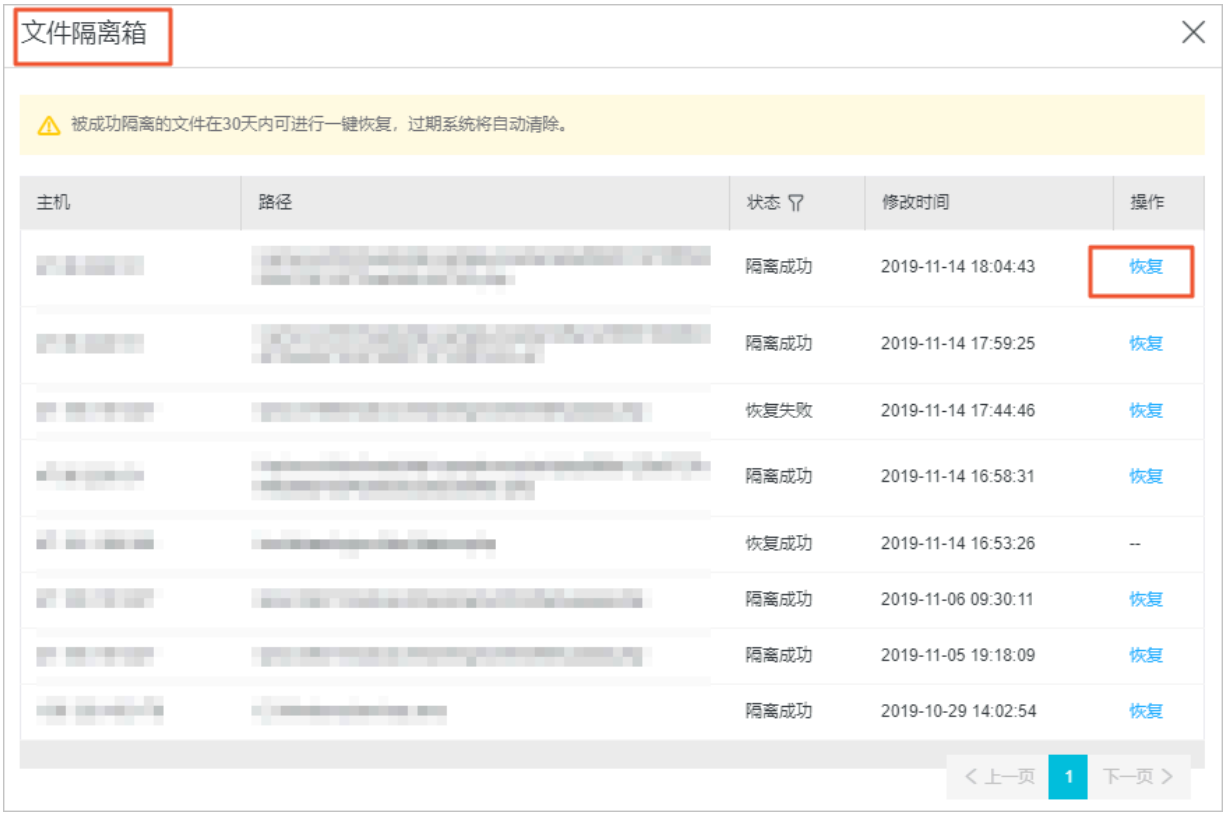
- **自主可控**：基于自主研发的深度学习、机器学习能力及大数据攻防经验，并结合多引擎检测能力，为用户提供全面、实时的病毒检测服务。
- **轻量**：客户端服务仅占用1%的CPU、50MB内存，不影响业务的运行。
- **实时**：获取进程启动日志，实时监控病毒程序的启动。
- **统一管理**：云盾控制台支持对所有主机进行统一管理，实时查看所有主机的安全状态。

云查杀应用案例

检测

隔离

恢复


文件隔离箱
被成功隔离的文件在30天内可进行一键恢复，过期系统将自动清除。
主机
路径
状态
修改时间
操作
隔离成功 2019-11-14 18:04:43 恢复
隔离成功 2019-11-14 17:59:25 恢复
恢复失败 2019-11-14 17:44:46 恢复
隔离成功 2019-11-14 16:58:31 恢复
恢复成功 2019-11-14 16:53:26 --
隔离成功 2019-11-06 09:30:11 恢复
隔离成功 2019-11-05 19:18:09 恢复
隔离成功 2019-10-29 14:02:54 恢复
< 上一页
1
下一页 >