阿里云
云安全中心（态势感知）

控制台总览

文档版本：20190917

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

法律声明.....I
通用约定.....I
1 总览..... 1

1 总览

云安全中心总览页作为阿里云云平台的安全运营中心，实时展示了您所有资产的威胁概览信息和安全评分信息、以及您开通的所有云盾安全服务，并提供升级、续费、扩充资产规模、调整接收通知规则等设置功能，帮助您对资产进行统一的安全管控。

您可在总览页面查看您资产的安全概览信息和进行相关操作。

总览页面展示以下模块：

- 升级、续费：云安全中心的版本信息，提供升级高级版、企业版、扩充资产规模和续费操作。

- 安全评分：您资产的安全分值以及受保护/未受保护资产数量。具体评分分值参见安全分值表。

  单击立即处理可展开安全风险处理页面，您可根据页面的提示，参考对应的帮助文档或直接对风险立即处理。安全风险处理包含所有需要您尽快处理的安全风险和威胁，包含以下类别：

  - 待处理告警
  - 待修复漏洞
  - 基线检查
  - 云平台配置检查（云产品安全风险项）
  - 攻击事件等其他风险或威胁

- 资产状态：查看您已安装和未安装Agent插件的资产数量，即已在云安全中心防护范围内的资产和还未受云安全中心防护的资产数量；查看存在风险资产总数量；分别查看存在风险的服务器、网站、云产品数量。

  单击未防护资产下的安装Agent，可以跳转到安装/卸载插件页面，您可以将未受保护的资产接入云安全中心的安全防护内。有关Agent安装的详细操作，参见#unique_4。

- 安全检测及防御能力：提供安全防御引擎、日志容量、病毒库更新时间、系统漏洞扫描时间、精准防御数量和网页防篡改数量等相关信息，帮助您实时掌握安全防御情况，了解资产安全状态。

- 威胁统计：查看威胁统计数据。

  - 待处理告警：显示您资产中的告警总数量和不同危险等级（紧急、可疑、提醒）告警对应的数量。单击待处理告警总数值可跳转到安全告警处理页面。
  - 待修复漏洞：显示您资产中还未修复的漏洞总数和不同漏洞风险等级对应的数量。单击待修复漏洞的总数量可跳转到漏洞修复页面。详见#unique_6。
  - 基线问题：显示您资产中存在的基线风险总数量和不同危险等级的基线风险对应的数量。单击基线问题总数值可跳转到基线检查页面。
  - 攻击次数：显示您资产受到攻击的总次数。单击攻击总次数可跳转到攻击分析页面。
- 云平台配置风险：检测到的云产品基线配置存在的风险。单击查看全部可跳转到云平台配置检查页面。详细操作参见#unique_9。
- 安全运营：展示15天内已处理的告警、漏洞、基线配置数量柱状图和趋势图。

升级企业版、扩充资产规模、续费

云安全中心支持基础版、高级版和企业版，您可在总览页面右上角查看云安全中心的版本信息。基础版、高级版和企业版支持的功能参见#unique_10。

- 基础版：页面右上角显示云安全中心的版本信息和购买按钮。升级到高级版或企业版后可使用基线检查、资产指纹、恶意进程（云查杀）、日志分析等高级功能。

- 高级版/企业版：页面右上角显示云安全中心的到期日期和资产规模（服务器台数），并提供升级和续费操作按钮。

  说明:
  如果当前服务器数量超过购买服务时配置的服务器数量，页面右上角会出现扩充资产规模操作按钮，提示您尽快扩充资产规模。

安全分值表

安全分值	分值说明	字体颜色
95-100	恭喜，您的资产安全状态良好。	绿色
85-94	您的资产存在安全隐患，建议您尽快加固安全防护体系。	黄色
70-84	您的资产存在较多安全隐患，建议您及时加固安全防护体系。	黄色

安全分值	分值说明	字体颜色
69分以下	您的资产防御黑客入侵的能力很弱，建议您尽快加固安全防护体系。	红色

安全评分扣分项目表

安全分扣分项	加固建议
缺少安全运营中心。	建立纵深防御体系。如有疑问请提交工单了解详情。
存在未修复漏洞。	修复漏洞，详见漏洞管理。
存在未处理的告警事件。	对告警事件进行及时处理。详见#unique_12。
主机缺乏安全防护。	开通安骑士企业版。
保护状态为离线（Agent未安装或离线）。	安装Agent。
存在Web-CMS漏洞。	修复#unique_14。
存在系统软件漏洞。	修复#unique_15。
基线检查存在风险。	修复基线检查漏洞。详细操作参见#unique_16。
存在异常登录事件。	查看并处理#unique_17。
存在网站后门威胁。	查看和处理#unique_18文件。
存在主机异常。	对主机异常事件进行处理。

更多信息

如果您需要安全专家帮助提升系统安全性，可使用安全加固服务。在您授权后，专业安全工程师会为您修复安全基线和漏洞、排查系统潜在安全威胁、提升资产安全性。

详细信息参见安全加固。