ALIBABA CLOUD

阿里云

云安全中心（态势感知）

快速入门

文档版本：20201112

阿里云

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
危险	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。	危险 重置操作将丢失用户配置数据。
警告	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。
注意	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。
说明	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	命令或代码。	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.配置任务

试用企业版（限试用7天）的用户可以免费使用云安全最佳实践配置任务，快速提升您资产的整体安全水位。建议您在开通试用版后，快速完成最佳实践配置任务，充分利用免费试用资源，全方位排查出您资产中的安全隐患，并对相关安全风险进行处理。

前提条件

您已开通企业版（试用），非试用版暂不支持该功能。

操作步骤

1. 登录云安全中心控制台。
2. 单击右下角 图标，
3. 在云安全最佳实践配置任务页面，根据页面的提示信息，依次完成任务1、任务2和任务3。完成不同的配置任务后，您可以获得对应的奖励，包括：延长企业版试用天数、申请代金券等。

> **说明** 完成不同的任务后，您的云安全中心安全分对应模块的分数也会相应提升。建议您及时完成配置任务，提升资产安全分值（安全分值表）。

2.新手入门

云安全中心作为一个实时识别、分析和预警安全威胁的统一安全管理系统，为您提供安全态势总览、防勒索、防病毒、防篡改、合规检查等安全能力，全方位检测和防护您的服务器和Web应用安全。

适用范围

本文档作为快速入门参考，适用于有以下需求的读者对象：

- 想要了解如何开通使用云安全中心服务。
- 想要了解云安全中心各版本功能。
- 想要了解云安全中心授权接入资产的安全状态。

前提条件

Agent插件是云安全中心提供的本地安全插件，您必须在要防护的服务器上安装该插件才能使用云安全中心的服务。安装Agent的详细指导操作，请参见安装Agent或金融云和VPC用户安装Agent。

> **说明** 在购买ECS实例时，选择**安全加固**即可自动安装Agent并开通云安全中心基础版，无需您手动安装Agent。

快速入门流程

参照以下步骤快速防护您资产的安全。

1. 云安全中心自动为您的服务器资产开通**基础版**功能。**基础版**仅提供主机异常登录检测、漏洞检测、云产品安全配置项检测。

   如需更多高级威胁检测、漏洞修复、病毒查杀等功能，前往云安全中心购买页，购买您需要的版本。

   i. 首先了解云安全中心基础杀毒版、高级版和企业版功能详情。具体内容，请参见功能特性。

   ii. 根据您对资产安全的需求，选择并购买需要的版本。详细操作请参见购买云安全中心。

2. 购买云安全中心服务后，您可以在云安全中心控制台的**总览**页面，查看您资产当前的安全得分。您可根据您的安全得分扣分项严重程度以及扣分项对应的待处理风险，对您资产上的弱点及安全事件进行处理，提升您服务器的整体安全性。详细内容请参见提高安全评分最佳实践。

   > **说明** 资产安全状态通过云安全中心Agent插件收集和检测得出。
   >
   > - 如果您在创建ECS实例时选中了**安全加固**，会自动加载云安全中心基础版本，即自动为该ECS服务器开启Agent插件。这种情况下，您可以直接使用云安全中心为您提供的服务。
   > - 您在创建ECS实例时未选中**安全加固**，实例创建完成后，如果您还需云安全中心为该ECS服务器提供安全防护，您需要先安装云安全中心Agent。详细操作请参见安装Agent。
   > - 您可根据被防护服务器的保护状态确认云安全中心Agent的在线或离线状态。服务器的客户端状态为**开启**，说明Agent在线；服务器的客户端状态为**关闭**，说明Agent离线，您可以排查Agent离线原因，恢复对服务器的安全防护。Agent离线排查的详细内容，请参见Agent离线排查。

3. 购买云安全中心服务后，您可以在云安全中心**总览**页面查看当前阿里云账号下的服务器安全状态，以及安全告警事件、主机漏洞扫描结果、系统配置风险情况。详细内容请参见总览。

我当前的系统是否安全以及如何提升系统安全评分？

我如何使用云安全中心精准防御病毒？

> **说明** 云安全中心**基础版**不支持病毒自动防御，建议升级到**高级版**或**企业版**。

如何使用云安全中心的漏洞修复功能？