ALIBABA CLOUD

阿里云

云安全中心（态势感知）
资产中心

文档版本：20201109

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.资产中心总览

您可以通过资产中心的总览页面全面了解云安全中心已防护的资产的安全状态和统计信息。

背景信息

资产中心总览页面从资产的类型、地域分布、防护状态、风险状态等维度分别展示资产的对应信息。

为便于对资产信息进行管理，资产中心提供了资产分组和标签分类功能。您可以将资产分组，以组别的维度查看安全事件；也可以通过资产标签筛选具有相同属性的资产。相关内容请参见管理资产分组和管理资产标签。

总览介绍

云安全中心控制台资产中心**总览**页面提供以下资产统计信息：

- **保有资产分析**：展示受云安全中心保护的云上资产分布和资产安全状态分布情况。

  

- **服务器资产分析**：展示服务器风险分布、客户端状态分布、区域分布、操作系统分布、端口开放TOP5、软件资产TOP5、进程TOP5和相同账户TOP5信息。

  

  - 单击**服务器资产分析**区域的**详情**，可跳转到**资产中心 > 服务器**页面查看服务器详情。详细内容请参见查看服务器安全状态。
  - 单击**区域分布**区域的**详情**，可跳转到**资产中心 > 服务器 > 服务器地域**页面查看服务器地域信息。详细内容请参见查看服务器安全状态。
  - 单击**端口开放TOP 5**、**软件资产TOP 5**、**进程TOP 5**、**相同账户TOP 5**、**中间件TOP 5**的**详情**，可跳转到**资产指纹调查**页面查看对应的指纹详情。详细内容请参见资产指纹调查概述。

- **云产品风险分布**：展示云产品的数量和安全状态分布情况。

  

  单击**存在风险**或**安全**的统计数据，可跳转到**资产中心 > 云产品**页面，查看**存在风险**或**安全**状态的云产品信息。详细内容请参见查看云产品安全状态。

  > **说明** 当**存在风险**或**安全**统计数据为0时，不支持单击跳转到对应的页面。

2.查看服务器安全状态

云安全中心的资产中心页面提供了所有服务器的安全状态相关信息，例如服务器的防护状态、分组、地域、专有网络VPC等统计信息。本文档介绍如何通过筛选功能查看指定服务器的安全状态，并对搜索条件和显示信息进行设置。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。
3. 在**服务器**页面，查看服务器安全状态。您可以根据需要执行以下操作：
   - **根据服务器状态进行筛选**
     - 在**所有服务器**功能项，您可以查看**所有服务器**数量、**存在风险的服务器**数量、**未受保护的服务器**数量、**未启动的服务器**数量和**新增服务器**数量，查看所有服务器安全状态。

       

       以下是不同服务器分类的说明：
       - **所有服务器**：受云安全中心防护的所有服务器，包括所有阿里云服务器和已安装云安全中心Agent的非阿里云服务器。
       - **存在风险的服务器**：存在漏洞、基线风险、告警等安全风险的服务器。
       - **未受保护的服务器**：Agent客户端状态为**关闭**或**暂停保护**的服务器，云安全中心无法对该类型服务器提供安全防护。
       - **未启动的服务器**：已关机的服务器。

       单击需要查看服务器的名称或其**操作**栏的**查看**或**修复**，可查看该服务器的详细信息。更多详细内容请参见查看单个资产详情。
     - 单击**存在风险的服务器**、**未受保护的服务器**、**未启动的服务器**或**新增服务器**，查看对应服务器的安全状态。

       
   - **根据服务器组进行筛选**
     - 单击**服务器组**，您可以查看**服务器组**数量及各分组的**包含服务器数量**、服务器**存在风险数量**和**未保护数量**。

       

       云安全中心支持**管理**和**删除**服务器分组，具体操作指导请参见管理资产分组。
     - 单击目标分组下**包含服务器数量**、**存在风险数量**或**未保护数量**，查看目标分组下服务器安全状态。例如，单击**服务器组**为*2008*的**存在风险数量**下的数字，显示**检索项**为**是否存在风险：有风险**和**分组名称：2008**下的服务器安全状态。

       
   - **根据服务器所在地域进行筛选**
     - 单击**服务器地域**，您可以查看**服务器地域**数量及各地域下的**包含服务器数量**、服务器**存在风险数量**和**未保护数量**。

       

- 单击目标地域下**包含服务器数量**、**存在风险数量**或**未保护数量**，查看目标地域下服务器安全状态。例如，单击**服务器地域**为**华北3（张家口）**的**包含服务器数量**下的数字，显示**检索项**为**地域：华北3（张家口）**下的服务器安全状态。

- **根据专有网络VPC实例ID进行筛选**
  - 单击**专有网络VPC**，您可以查看**专有网络VPC**数量及各VPC下的**包含服务器数量**、服务器**存在风险数量**和**未保护数量**。

  - 单击目标专有网络VPC下**包含服务器数量**、**存在风险数量**或**未保护数量**，查看目标VPC下服务器安全状态。例如，单击**专有网络VPC**为*nocloudEcs*的**包含服务器数量**下的数字，显示**检索项**为**所属VPC ID：**noncloudEcs下的服务器安全状态。

- **根据资产重要性进行筛选**

  您可以在**资产重要性**区域单击**重要资产**、**一般资产**或**测试资产**，查看对应重要性服务器的安全状态。

- **根据标签项进行筛选**

  您可以单击资产列表左侧已添加的标签项，查看对应标签下服务器的安全状态。

- **多筛选查看**

  使用**所有服务器**、**服务器组**、**服务器地域**、**专有网络VPC**或**标签**功能选项，通过**资产中心**列表上方搜索栏，筛选出指定的服务器。

  - 展示多个筛选子项结果：

    您可以在**资产中心**列表上方搜索栏，选择识别类型（**公网IP**、**私网IP**、**实例名称**、**实例ID**、**所属VPC ID**、**操作系统**、**是否有基线问题**、**是否有漏洞问题**、**是否有安全告警**、**是否存在风险**、**是否在线**、**开机状态**、**标签名称**、**分组名称**、**地域**），并选择或输入指定类型信息，筛选出指定的服务器。

    > **说明**
    >
    > 您可以同时输入多个检索项，并选择多个检索项之间的关系。以下是检索项关系的相关说明：
    >
    > - 检索项之间的关系：
    >   - AND：检索项之间是**与关系**。
    >   - OR：检索项之间是**或关系**。
    > - 展示多个筛选子项结果，需要选择检索项之间的关系为OR。
    > - 需要输入指定信息搜索的检索项，完成输入后，需要单击**搜索**按钮，才能显示对应的检查信息。

    例如，选择检索项之间的关系为**OR**，选中**地域**并选择**华东1**，然后重新选中**地域**并选择**华北1**，可以显示华东1和华北1下的所有资产。

- 展示跨筛选项组合结果：

  同时应用多个筛选项。例如，选中**地域**并选择**华东1**后，选中**开机状态**并选择**开机状态：开机**，选择检索项之间的关系为**AND**，可以显示华东1下的所有开机资产信息。

  

  您也可以在选择了**服务器组**、**服务器地域**、**专有网络VPC**或**标签**功能检查后，通过**资产中心**列表上方搜索栏，筛选出更多指定的服务器。

- **设置常用筛选条件**

  对于已应用的筛选项组合，您可以将其保存为常用筛选条件。单击**保存**，在**保存条件**对话框为该筛选条件命名（例如华东1，开机）后，就可以在搜索栏右侧**常用搜索条件**选择框中直接选用该筛选条件。

  

- **设置显示列**

  单击**资产中心**页面右上角的设置列按钮，可以设置需要显示的列内容。

  

3.查看容器安全状态

云安全中心的资产中心页面提供了所有容器相关资产的安全状态相关信息，主要包括容器应用、集群、容器组、容器、命名空间和镜像的统计数据及风险状态信息。本文档介绍如何通过筛选功能查看目标容器资产的安全状态。

背景信息

云安全中心为您提供检测K8s集群安全风险的能力。您在云安全中心控制台**设置**页面的**容器K8s威胁检测**区域打开**威胁检测**开关后，即可开启该安全能力。更多信息请参见容器K8s威胁检测。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。
3. 在**资产中心**页面单击**容器**页签。
4. 在**容器**页签您可以查看容器安全状态。

   资产中心容器页面

   您可以执行以下操作：

   - **查看所有应用详细信息和风险状态**

     在**容器**页签下单击左侧的**所有应用**，查看您资产中的所有应用信息。您可以进行以下操作：

     - **筛选指定应用**

       您可以在搜索框处选择**是否有漏洞问题**、**是否有安全告警**、**集群ID**等搜索条件，定位到您需要查看的应用。您可以查看所有应用的详细信息，包括所有应用数量、**应用名称**、应用所在**集群**、集群的**创建时间**和**风险状态**。

     - **查看应用详情**

       定位到您需要查看的应用，单击其操作列的**处理**。在该应用详情页面，您可以查看该应用的基本信息、漏洞风险、告警风险和所在容器组信息。

   - **查看存在风险的应用**

     在**容器**页签下单击左侧的**存在风险的应用**，查看您资产中所有存在风险的应用信息。单击指定应用操作列的**处理**可以查看该应用的基本信息、漏洞风险、告警风险和所在容器组信息。

   - **查看集群详细信息和风险状态**

     在**容器**页签下单击左侧的**集群**，查看您资产中的所有集群信息。您可以进行以下操作：

     - **筛选指定集群**

       您可以在搜索框处选择**是否有漏洞问题**、**是否有安全告警**、**集群ID**等搜索条件，定位到您需要查看的集群。您可以查看所有集群的详细信息，包括所有集群数量、**集群名称/ID**、**集群类型**、**地域**、**服务器**数量、集群**创建时间**、**集群状态**和**风险状态**。

     - **查看集群详情**

       定位到您需要查看的集群，单击其操作列的**处理**。在该集群详情页面，您可以查看该集群的基本信息、漏洞风险、告警风险、容器组和服务器信息。

   - **查看容器组详细信息和风险状态**

     在**容器**页签下单击左侧的**容器组**，查看您资产中的所有容器组信息。您可以进行以下操作：

- **筛选指定容器组**

  您可以在搜索框处选择**是否有漏洞问题**、**是否有安全告警**、**实例ID**等搜索条件，定位到您需要查看的容器组。您可以查看容器组的详细信息，包括所有容器组数量、**容器组名称**、**存在风险容器数/总容器数**、**容器组IP**、容器组所在**服务器**、容器组**所属集群**和**风险状态**。

- **查看容器组详情**

  定位到您需要查看的容器组，单击其操作列的**处理**。在该容器组详情页面，您可以查看该容器组的基本信息、漏洞风险、告警风险和容器信息。

- **查看容器详细信息和风险状态**

  在**容器**页签下单击左侧的**容器**，查看资产中的所有容器信息。您可以进行以下操作：

  - **筛选指定容器**

    您可以在搜索框处选择**是否有漏洞问题**、**是否有安全告警**、**容器ID**等搜索条件，定位到您需要查看的容器。您可以查看容器的详细信息，包括所有容器数量、**容器ID**、**告警**数量、**漏洞**数量、容器所属**容器组**、容器所属**所属服务器**和**风险状态**。

  - **查看容器详情**

    定位到您需要查看的容器，单击其操作列的**处理**。在该容器详情页面，您可以查看该容器的基本信息、漏洞风险和告警风险。

- **查看存在风险的容器**

  在**容器**页签下单击左侧的**存在风险的容器**，您可以查看您资产中的所有存在风险的容器信息。单击容器操作列的**处理**，可以查看该容器存在的漏洞风险和告警风险详情。

  

- **查看命名空间详细信息和风险状态**

  在**容器**页签下单击左侧的**命名空间**，查看您资产中的所有命名空间信息。您可以进行以下操作：

  - **筛选指定命名空间**

    您可以在搜索框处选择**是否有漏洞问题**、**是否有安全告警**、**集群ID**、**命名空间**等搜索条件，定位到您需要查看的命名空间。您可以查看所有命名空间的详细信息，包括**命名空间名称**、命名空间所在**集群**、命名空间**创建时间**和风险状态。

  - **查看命名空间详情**

    定位到需要查看的命名空间，单击其操作列的**处理**。在命令空间详情页面，您可以查看该命名空间的基本信息、漏洞风险、告警风险、容器组和应用信息。

- **查看镜像详细信息和风险状态**

  在**容器**页签下单击左侧的**镜像**，您可以查看您资产中的所有镜像信息。您可以进行以下操作：

  - **筛选指定镜像**

    您可以在搜索框处选择**是否有漏洞问题**、**是否有安全告警**、**实例ID**、**仓库名称**等搜索条件，定位到您需要查看的镜像。您可以查看镜像的详细信息，包括**镜像地址/标签**、**镜像大小**、**地域**、**最新发现时间**和**风险状态**。

- **查看镜像漏洞详情**

  定位到需要查看的镜像，单击其操作列的**处理**。在漏洞列表页面，您可以查看云安全中心检测出的该镜像上存在的漏洞信息，包括**镜像系统漏洞**、**镜像应用漏洞**和**镜像恶意样本**信息。

  漏洞详情

  在漏洞列表右上角，您可以使用漏洞修复紧急程度过滤漏洞列表，或搜索指定漏洞，查看您关注的信息。

  如果您需要查看某个漏洞的详细信息，您可以单击该漏洞操作列的**详情**，查看该漏洞影响资产、修复命令和影响说明信息。镜像漏洞的更多信息请参见查看镜像安全扫描结果。

  漏洞详细信息

相关文档

容器安全

容器K8s威胁检测

查看镜像安全扫描结果

使用运行时刻安全监控

4.查看网站安全状态

云安全中心的资产中心为您提供资产中所有网站的安全状态信息，并支持进行网站安全体检和查看网站安全报告。本文档介绍如何查看网站对应资产的风险状态和网站安全报告。

查看网站对应资产的风险状态和告警数量

资产中心提供您资产中所有网站的安全状态信息，主要包括网站根域名、子域名及其资产的风险状态和告警数量统计信息。以下步骤介绍如何查看网站对应资产的风险状态和告警数量。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。
3. 在**资产中心**页面单击**网站**页签。
4. 在**网站**页面，查看网站信息。您可以执行以下操作：
   - **查看根网站及对应资产**

     单击**根网站**，您可以查看所有根网站（即根域名）的信息，包括根网站的**网站名称**和**资产IP**。

     
   - **查看子域名及对应资产**

     单击**子域名**，您可以查看所有子域名的信息，包括子域名的**网站名称**和**资产IP**。

     
5. （可选）查看网站对应服务器风险状态和告警数量。

   在**根网站**或**子域名**页面，单击目标网站的**网站名称**或操作列下的**查看**，查看该网站的详细信息。

   
   - 您可以查看网站的**域名**、**根域名**、**风险状态**和**相关资产**信息。**相关资产**信息包括**资产名称/IP**、**资产类型**、**服务器漏洞**数量和**告警**数量。
   - 您可以单击目标资产名称，打开资产列表详情，在该资产**基本信息**页签下查看该资产的**风险状态**。更多信息请参见查看单个资产详情。

     
   - 您可以单击目标资产**服务器漏洞**或**告警**列的数字，查看具体漏洞或告警信息。漏洞处理更多信息请参见漏洞修复概述。告警处理更多信息请参见查看和处理告警事件。

     

查看网站安全报告

云安全中心支持网站安全体检功能，并提供网站安全报告。以下步骤介绍如何查看网站安全报告。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。
3. 在**资产中心**页面单击**网站**页签。
4. 在**安全体检**区域单击**立即体检**。
5. 在**网站安全报告**页面，查看网站的统计数据、存在风险的网站、安全告警、漏洞风险以及安全建议。您可以查看以下内容：
   - **总览**

在**总览**区域查看您网站的统计信息，包括安全评分、域名总数、存在风险的网站数量、安全告警数量和漏洞风险数量。网站安全评分是云安全中心根据您资产中所有网站的安全状态给出的安全评分。详细的扣分规则请参见网站安全评分扣分项目表。以下是网站安全评分的颜色和分值的对应关系：

- 绿色：90~100分。网站安全评分显示为绿色，表示您的网站资产安全状态良好。
- 黄色：70~89分。网站安全评分显示为黄色，表示您的网站资产存在安全隐患，建议您根据网站安全报告页面的提示尽快处理存在的安全风险。
- 红色：10~69分。网站安全评分显示为红色，表示您的网站资产防御黑客入侵的能力很弱，网站资产存在较大的安全隐患。建议您尽快加固安全防护体系。

- **存在风险的网站**

  在**存在风险的网站**区域，查看存在风险的网站列表。您可以查看网站的域名、漏洞风险数量、安全告警数量和SSL证书配置状态。

  SSL证书（SSL Certificates）可以为网站提供HTTPS保护，对网站流量进行加密，防止数据被窃取。如果您的网站未配置SSL证书，建议您单击**立即配置**，为您的网站配置SSL证书。更多信息请参见SSL证书新手入门。

  需要处理指定域名的安全风险时，您可以单击该域名操作列的**风险处理**跳转到该域名详细信息页面，查看该域名的基本信息、风险状态和相关资产。在**相关资产**区域，单击**服务器漏洞**或**告警**下的数字，跳转到该资产的**漏洞信息**或**安全告警处理**页面，修复服务器上存在的漏洞，处理存在的安全告警。漏洞修复相关信息请参见Web-CMS漏洞和应用漏洞。告警处理相关信息请参见处理告警事件。

- **安全告警**

  在**安全告警**区域，查看您网站服务器中存在的安全告警。您可以查看告警名称、风险级别、受影响资产和最新发生时间。需要处理指定安全告警时，您可以单击该告警操作列的**告警处理**，跳转到**安全告警处理**页面处理该告警。更多信息请参见处理告警事件。

- **漏洞风险**

  在**应用漏洞风险**和**Web-CMS漏洞风险**区域，查看网站资产中的漏洞列表。您可以查看漏洞公告、风险级别和受影响资产。需要处理指定漏洞时，您可以单击该漏洞操作列的**漏洞修复**跳转到**漏洞修复**页面处理该漏洞。更多信息请参见漏洞修复概述。

- **安全建议**

  在**安全建议**区域，查看云安全中心根据安全体检结果为您提供的安全建议。收到建议（例如：**建议开启网页防篡改功能，防止网站被恶意注入外链，被篡改为涉恐涉政等不良信息，造成企业严重的社会负面影响**）时，您可以单击**前去处理**，跳转到**网页防篡改**页面，为您的服务器开启防篡改保护。

网站安全评分扣分项目表

扣分项	单项扣分值	单项扣分上限
存在安全告警	每个告警扣5分	30分
存在安全漏洞	每个漏洞扣5分	40分
存在未配置证书的域名	每个域名扣5分	20分

5.查看云产品安全状态

云安全中心的资产中心页面提供了云产品安全状态的相关信息，包括存在风险云产品信息及云产品分类（负载均衡、NAT网关、RDS数据库和MongoDB数据库）统计等。本文档介绍如何通过筛选功能定位查看目标云产品安全状态，并对搜索条件进行设置。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。
3. 在**资产中心**页面单击**云产品**页签。
4. 在**云产品**页面，查看云产品安全状态。 您可以根据需要执行以下操作：
   - **根据资产状态筛选云产品**
     - 在**所有云产品**区域，您可以查看**所有云产品**数量和**存在风险的云产品**数量，查看所有云产品安全状态。

       
     - 您可以单击**存在风险的云产品**，查看对应云产品的安全状态。

       

     单击需要查看的云产品名称或其操作列的**查看**或**修复**，可查看目标云产品的详细信息。更多详细信息请参见查看单个资产详情。
   - **根据资产类型进行筛选**

     云产品资产类型分为以下4种：
     - **负载均衡**
     - **NAT网关**
     - **RDS数据库**
     - **MongoDB数据库**

     

     在各资产类型功能项，您可以查看对应资产类型的云产品数量。单击**负载均衡**、**NAT网关**、**RDS数据库**或**MongoDB数据库**，查看对应云产品的安全状态。

     
   - **根据标签项进行筛选**

     您可以在**标签**功能项中，查看标签对应资产数量。单击资产列表左侧已添加的标签项，查看对应标签下云产品的安全状态。

     
   - **多筛选查看**

     使用**所有资产**、**负载均衡**、**NAT网关**、**RDS数据库**或**MongoDB数据库**功能选项，通过**资产中心**列表上方搜索栏，筛选出指定的资产。

     例如，选择**所有资产**，进行多筛选查看资产安全状态。

- 展示多个筛选子项结果：

  您可以在**资产中心**列表上方搜索栏，选择识别类型（**公网IP**、**实例名称**、**实例ID**、**是否有安全告警**、**是否存在风险**、**标签名称**、**分组名称**、**地域**），并选择或输入指定类型信息，筛选出指定的资产。

  > **说明**
  >
  > 您可以同时输入多个检索项，并选择多个检索项之间的关系。以下是检索项关系的相关说明：
  >
  > - 检索项之间的关系：
  >   - AND：检索项之间是**与关系**。
  >   - OR：检索项之间是**或关系**。
  > - 展示多个筛选子项结果，需要选择检索项之间的关系为OR。
  > - 需要输入指定信息搜索的检索项，完成输入后，需要单击**搜索**按钮，才能显示对应的检查信息。

  例如，选择检查项之间的关系为**OR**，勾选**地域**并选择**华东1**，然后重新勾选**地域**并选择**华北1**，可以显示华东1和华北1下的所有资产。

  

- 展示跨筛选项组合结果：

  同时应用多个筛选项。例如，选中**地域**并选择**华东1**后，选中**是否存在风险**选择**是否存在风险：有风险**，选择检查项之间的关系为**AND**或**OR**，可以显示华东1下的所有的有风险资产信息。

  

  > **说明**
  >
  > - 您也可以在选择**负载均衡**、**NAT网关**、**RDS数据库**、**MongoDB数据库**或**标签**功能检查后，通过**资产中心**列表上方搜索栏，筛选出更多指定的资产。
  > - 您也可以在选择**所有资产**、**负载均衡**、**NAT网关**、**RDS数据库**或**MongoDB数据库**功能检查后，通过**标签**项，筛选出更多指定的资产。

- **设置常用筛选条件**

  对于已应用的筛选项组合，您可以将其保存为常用筛选条件。单击**保存**，在**保存条件**对话框为该筛选条件命名（例如华东1，标签1）后，就可以在搜索栏右侧条件框中直接选择该筛选条件。

  

6.查看服务器系统可信状态

云安全中心支持检测服务器的系统可信状态。购买可信ECS实例后，您可以在云安全中心控制台的资产中心页查看ECS服务器的可信信息，并对系统可信告警进行处理。

背景信息

云安全中心遵循国际标准，采用PCR（Platform Configuration Register）值来记录和识别服务器系统启动过程中各环节的状态。PCR是可信安全设备的存储单元，能够可靠地保护系统启动过程中收集的状态信息。PCR中存储的实际度量值与预期的标准值一致，即表示系统启动过程中特定环节符合系统可信的标准。

系统可信仅针对ECS可信实例生效。ECS实例规格以英文字母t（例如：c6t）结尾表示该实例为可信实例。详细介绍，请参见实例规格族。

查看ECS服务器启动状态

默认情况下，云安全中心以您ECS服务器第一次上报的系统启动状态作为标准值，来判断ECS后续的启动情况。即如果某次ECS启动状态与第一次相同，则该次启动会被判定为正常。

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。
3. 在**资产中心**页面单击**服务器**页签。
4. 在**服务器**中定位到目标ECS实例，并单击该实例的名称。单击实例名称可以跳转到该实例的安全详情页面。
5. 在该实例的安全详情页面单击**可信信息**。

   您可以在**可信信息**页签中查看**资产启动概况**。**资产启动概况**即为ECS服务器系统的启动链状态，由10个圆圈组成。圆圈分别代表ECS实例服务器启动过程中的一个特定环节，每个环节对应于**资产中组件可信状态**模块中的PCR0至PCR9中的一行。

   正常情况下所有圆圈均为绿色，表示ECS启动过程正常。此时ECS系统启动中的各个环节组件的状态都符合预期，具体表现为**资产中组件可信状态**中每一行组件的标准值和实际度量值（即系统可信功能收集到的服务器系统实际状态）都一致。

   如果启动过程中某环节出现问题，则对应环节的圆圈颜色将变为红色，同时后续环节对应的圆圈颜色将变为灰色（表示这些环节的状态信息已经无意义）。您可以通过查看安全告警了解问题环节的详细情况和进行相应的处理。

查看可信异常告警

如果ECS启动过程中发生异常，系统可信功能将在该ECS的**安全告警处理**页签下展示**可信异常**类型的告警。可信异常产生的原因可能是您的ECS检测到了安全问题（例如：遭受了BootKit、RootKit攻击），也可能是您的系统进行了某些修改和维护（您或您系统管理员修改了操作系统启动参数）。

云安全中心会对相同的安全告警周期性重复上报。为避免产生过多干扰信息，重复上报的告警不会显示为多条告警信息，仅展示最近一次检测到的告警信息（通过更新**最近发生时间**来实现）。

您可以单击告警事件的**详情**，查看告警的具体情况，并根据实际情况对告警进行处理。

7.查看单个资产详情

云安全中心的资产中心功能提供了所有资产的详细信息，包括基本信息、漏洞信息、安全告警处理、基线检查和资产指纹调查等。本文介绍了查看单个服务器或云产品信息的具体操作。

背景信息

云安全中心的**资产中心**页面，提供了所有资产的基本信息。

下表罗列云安全中心的**资产中心**页面提供的服务器与云产品详情的功能差异，其中用到的标识：

- X：表示不包含在服务范围中。
- √：表示包含在服务范围中。

功能项	功能项描述	服务器	云产品
基本信息	风险状态：展示该资产风险的数量统计，包括以下类型： • **漏洞** • **安全告警** • **基线检查** • **云平台配置**	√	√（仅支持安全告警处理和云平台配置功能）
	详细信息：展示该资产的配置和保护状态等信息，支持配置该资产的分组和标签。	√	√（不支持资产分组功能）
	资产指纹调查：展示该资产指纹（端口、软件、进程、账户和中间件）的统计信息。	√	√
	漏洞检测：展示漏洞检测类型，支持为该资产开启或关闭不同类型的漏洞检测功能。	√	X
	防暴力破解：展示该资产应用的暴力破解防御规则内容，支持修改该资产应用的暴力破解防御规则。	√	√
	登录安全设置：展示该资产已添加的常用登录地址、登录的IP、时间和账号，支持设置该资产的相关告警。	√	X
漏洞信息	展示该资产的漏洞检测结果。	√	X
安全告警处理	展示该资产的安全告警信息。	√	√
基线检查	展示该资产的基线检查结果。	√	X
资产指纹调查	展示该资产指纹的详细信息。	√	X
云平台配置	展示该资产云平台配置检查的详细信息。	√	√

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。

3. 在**资产中心**页面单击**服务器**、**容器**、**网站**或**云产品**页签。
4. 在**服务器**、**容器**、**网站**或**云产品**页面，定位到目标资产并单击其名称。
5. 查看单个资产详情。

   在当前资产详情页面，单击**基本信息**、**漏洞信息**、**安全告警处理**、**基线检查**、**资产指纹调查**或**云平台配置**页签查看资产信息。

   

   以下介绍了该资产的相关信息：

   - **基本信息**：选择各功能页签查看和管理资产相关信息。
     - **风险状态**：查看漏洞、安全告警、基线检查的检测结果统计信息。单击对应统计数值可跳转至对应页面查看详细信息。

       

     - **详细信息**：查看资产配置和保护状态等信息，并管理资产标签和分组。

       

       - **更换分组**

         单击**更换分组**，在**更换分组**对话框，选择新的分组，并单击**确定**。

         

       - **设置标签**

         单击  ，在**添加标签**对话框，选择标签并单击**确定**。

         

         单击已有标签右侧的删除按钮  ，可删除资产所属标签。

     - **资产指纹调查**：查看资产指纹的统计信息。单击对应统计数值可跳转至**资产指纹调查**页签查看指纹详细信息。

       

     - **漏洞检测**：查看该资产已开启或关闭的漏洞检测功能项，您可根据需要为该资产开启或关闭不同类型的漏洞检测功能，覆盖的漏洞类型包括：Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞和应急漏洞。

       

     - **防暴力破解**：查看该资产应用的防御规则内容，您可根据需要**修改**资产的暴力破解防御规则，并**保存**。如何添加防暴力破解规则请参见安全告警设置。

       

       

     - **登录安全设置**：设置**常用登录地**和高级登录（IP、时间、账号）报警功能；**开启或关闭**非合法登录（IP、时间、账号）报警功能；为目标资产添加常用登录的IP、时间和账号。

       

   - **漏洞信息**：查看目标资产下漏洞检测结果，具体处理方法请参见漏洞修复。

     

- **安全告警处理**：查看目标资产下安全告警检测结果，具体处理方法请参见查看和处理告警事件。

  

- **基线检查**： 查看目标资产下基线检查结果，具体处理方法请参见执行基线检查。

  

- **资产指纹调查**：查看并采集目标资产下指纹（端口、进程、软件、账户、中间件）调查统计信息。

  

  您可手动触发资产指纹数据的采集，获取目标资产指纹的最新数据。

  a. 选择**端口**、**软件**、**进程**、**账户**、**计划任务**或**中间件**页签，并单击页面右上方**立即采集数据**。

  b. 在**采集数据任务下发成功**对话框中，单击**确定**。

  

  采集数据任务下发成功后，需要1~5分钟才能完成指纹数据的采集。任务结束后，您可查看到目标资产的最新指纹数据。资产指纹数据的更多详细信息，请参见资产指纹调查。

- **云平台配置**：查看目标资产的云平台配置检查结果。更多信息请参见查看和处理云平台配置检查结果。

  

8.开启和关闭服务器保护状态

安装Agent后，云安全中心开启对服务器的保护。您可根据您的业务需要，修改服务器的保护状态。本文档介绍如何开启和关闭资产的保护状态。

前提条件

您的服务器已安装了云安全中心Agent。安装云安全中心Agent后才可修改服务器的保护状态。安装Agent详细内容，请参见安装Agent。

背景信息

- 服务器成功安装Agent后，您可在**资产中心**页面查看到服务器的**客户端**实时防护状态为**开启**。
- 如果Agent离线，会导致服务器保护状态变为**关闭**。如果您确认该服务器需要云安全中心提供的防护，需及时为该服务器开启保护。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。
3. 在**资产中心**页面单击**服务器**页签。
4. 在**服务器**页面中，为指定服务器开启或关闭保护。
   - **开启保护**

     选中一个或多个客户端实时防护状态为**关闭**的目标服务器，并单击**更多操作 > 开启保护**。

     

     防护状态开启后，目标服务器的客户端实时防护状态变为**开启**。
   - **关闭保护**

     如果您确认服务器无需云安全中心的防护，可以为服务器关闭保护。选中一个或多个**客户端**实时防护状态为**开启**的目标服务器，并单击**更多操作 > 暂停保护**。

     > **说明** 服务器关闭防护后，云安全中心将无法再为服务器提供安全防护，包括漏洞检测、安全告警等。建议您谨慎操作。

     

     关闭成功，目标服务器的**客户端**实时防护状态变为**关闭**。

9.一键安全检查

云安全中心资产中心页面的服务器页面提供了安全检查功能，支持对指定服务器下发安全扫描任务，包括漏洞检测、基线检测、网站后门检测、资产指纹（端口、软件、进程、账号）采集。本文档介绍了服务器安全检查功能的具体操作。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。
3. 在**资产中心**页面单击**服务器**页签。
4. 在**服务器**列表中，选中一个或多个需要执行安全检查的服务器。
5. 单击列表下方的**安全检查**。

   
6. 在**安全检查**对话框中，选中需要执行的检查项目。

   

7. 单击**确认**，执行检查。
8. 在提示对话框中，单击**确定**。

   

   一键安全检查结束后，最新的检查结果会自动更新到云安全中心控制台该资产的详情页面。

   

后续步骤

您需要根据选择的检查项，前往对应页面查看更新后的检查结果。

- 各类型漏洞检测结果详情，请参见以下内容：
  - Linux软件漏洞
  - Windows系统漏洞
  - Web-CMS漏洞
  - 应用漏洞
  - 应急漏洞
- 基线检查结果详情，请参见查看和处理基线检查结果。
- 网站后门检测结果详情，请参见查看和处理告警事件。
- 资产指纹（进程数据、端口数据、软件资产、账号数据）的最新数据详情，请参见查看资产指纹数据。

10.管理资产分组

云安全中心的资产中心页面提供了服务器分组功能。为方便您快速定位到多个资产对象或对多个资产对象执行批量操作，建议您使用分组功能为同类型的资产创建一个分组。本文介绍了服务器分组功能的添加、修改、删除、更换的具体操作。

添加分组

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。
3. 在**资产中心**页面单击**服务器**页签。
4. 在服务器列表左侧，单击**服务器组**。

   

   > **说明** 未进行资产分组时，所有的资产默认在**未分组**中。

5. 单击**添加分组**。
6. 在**添加分组**对话框，完成新分组的设置。

   

   您可以参考以下子步骤配置分组的参数。

   i. 在**分组名称**文本框输入分组名称。

   ii. 添加资产到新创建的分组。

   您可以将未分组或已分组下的资产添加或转移至新创建的分组中。在**选择分组**选择**未分组**或其他分组，选中分组下的资产，单击 图标，将选中的分组添加到新创建的分组中。

7. 单击**确定**。
   在服务器分组列表，您可以看到新创建的分组记录。

   

修改和删除分组

如果需要对某个分组进行修改（例如，修改分组名称或分组下的服务器）或删除，可参见以下步骤：

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。
3. 在**资产中心**页面单击**服务器**页签。
4. 在服务器列表左侧，单击**服务器组**。
5. 定位到需要修改或删除的分组，单击**管理**或**删除**。 您可以根据需要进行以下操作。
   - **修改分组**
     a. 单击需要修改分组操作列下的**管理**，打开分组管理对话框。

b. 在**分组管理**对话框的左侧**选择分组**选择一个分组，在右侧当前分组下选择资产，单击 图标，将选中的当前分组的资产添加到左侧已选分组中。在左侧已选分组下选择资产，单击 图标，将选中资产添加到当前分组中。

c. 单击**确定**，完成服务器分组修改。

- **删除分组**

  您可以单击一个分组右侧操作列下的**删除**，然后单击**确定**，即完成分组的删除。

  > **说明** 当您删除某个分组时，该分组中的资产默认被移入**未分组**中。

更换服务器分组

您可以将多个同类型资产添加到一个分组中，便于对这些资产执行批量操作。如在配置基线检查策略模板时，按组别配置生效服务器；在资产列表页面，使用组别筛选并查看特定资产。

参照以下步骤，将资产添加到指定服务器分组中：

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。
3. 在**资产中心**页面单击**服务器**页签。
4. 在服务器列表页，选中一个或多个服务器资产并单击资产列表下方的**更换分组**。
5. 在**更换分组**对话框，选择新的服务器分组。
6. 单击**确定**。

11.管理资产标签

云安全中心的资产中心页面提供了资产标签功能，支持为资产添加重要性或自定义标签标识其特殊属性，方便您筛选具有相同属性的资产。本文介绍了服务器资产重要性标签的添加和自定义标签的添加、修改和删除的具体操作。

背景信息

云安全中心提供以下表格中的资产重要性标签，方便您根据重要性快速对资产进行分类。您可以为您的资产选择相应的重要性标签。

您为资产设置的重要性标签决定了漏洞修复紧急度得分计算方法中的**资产重要性因子**。**资产重要性因子**会影响资产的漏洞修复紧急度得分。根据漏洞修复紧急度得分您可以判断一个漏洞是否被优先修复。建议您为核心资产设置重要性标签，云安全中心将根据资产重要性提示您尽快修复重要资产中的漏洞。以下表格展示了资产重要性标签和资产重要性因子取值的关系。漏洞修复优先级更多信息请参见漏洞修复优先级。

重要性标签类型	资产重要性因子	选择建议
重要资产	1.5	运行您核心业务或存储核心数据的资产，该类资产被病毒恶意入侵会对业务系统造成较大影响并导致重大的业务损失。
一般资产	1	运行一般业务的资产，可替代性较高。该类资产被病毒恶意入侵后对整个系统的影响较小。
测试资产	0.5	进行业务功能或性能测试的资产，或其他对您业务影响较小的资产。

> **说明** 如果您未设置资产重要性标签，您所有资产的重要性标签默认为**一般资产**，即所有资产重要性因子都为1。

添加资产重要性标签

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。
3. 在**资产中心**页面单击**服务器**页签。
4. 在资产列表左侧**资产重要性**区域，单击**添加**。
5. 在**资产重要性**管理页面，设置需要选择的重要性并选择标签应用的服务器。

   > **说明** 一个资产只能添加一个资产重要性标签。

6. 单击**确定**。添加完成后，重要性标签将显示在服务器名称下。如果需要修改单个资产的重要性或自定义标签，您可以单击目标资产右侧的 图标，并在**添加标签**对话框中选择自定义标签和资产重要性标签。

添加自定义标签

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。
3. 单击**服务器**或**云产品**页签。
4. 在**服务器**或**云产品**页面，单击资产列表左侧筛选功能**标签**右侧的**添加**。
5. 在**添加标签**对话框中输入标签名，并在左侧选择服务器，单击 图标，将资产添加至新创建的标签。

   

6. 单击**确定**。 您可以在资产列表，单击目标资产**标签**栏的 图标，将该资产添加至已创建的标签。

   > **说明** 一个资产支持添加多个标签，每个资产的所属标签都会在资产列表的**标签**栏显示。

修改和删除自定义标签

如果需要对某个标签进行修改（例如：修改标签名称或修改标签添加的服务器）或删除，可参见以下步骤：

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。
3. 单击**服务器**或**云产品**页签。
4. 在**服务器**或**云产品**页面，修改或删除标签。 您可以参考以下步骤修改或删除标签：
   - **修改标签**
     a. 如果需要修改单个标签，可将鼠标移动至该标签栏中，单击显示的 图标。

     

     b. 在**标签管理**对话框中修改**标签名称**，或添加、删除标签下的服务器。

     

     c. 单击**确定**。
   - **删除标签**

     如果需要删除某个标签，可将鼠标移动至该标签栏中，单击显示的 图标，并单击**确定**，删除标签。

     

12.删除非阿里云服务器

云安全中心支持绑定并防护非阿里云服务器，您可以根据实际场景需求解除绑定（即卸载）非阿里云服务器。本文档介绍如何删除云安全中心已绑定的非阿里云服务器。

前提条件

- 需要删除的非阿里云服务器Agent已暂停保护或已卸载云安全中心Agent（客户端状态为**关闭**）。更多信息请参见开启和关闭服务器保护状态和卸载Agent。
- 需要删除的非阿里云服务器已关闭客户端自保护。更多信息请参见客户端自保护。

背景信息

如果您不希望云安全中心继续防护您的非阿里云服务器，您可以在资产列表中对该服务器解除绑定。 解除绑定后，该服务器的Agent将被自动卸载，云安全中心将从资产列表中移除该服务器，并且不会再对该服务器提供安全防护。

> **说明**
>
> - 只有非阿里云服务器才需要执行解除绑定的操作。阿里云ECS服务器无需执行解除绑定操作。对于阿里云ECS服务器，即使您卸载了Agent插件，该服务器仍将以离线状态出现在资产管理列表中，而不会从列表中移除。
> - 非阿里云服务器解绑后，该服务器将不再消耗您云安全中心的授权数（保有服务器台数），即解绑后会释放出对应数量的授权数，可以用于防护其他的服务器。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏单击**资产中心**。
3. 在**资产中心**页面单击**服务器**页签。
4. > **说明** 只有Agent客户端状态为**暂停保护**或**关闭**的非阿里云服务器才可执行**解除绑定**操作。如果服务器客户端状态为**开启**，您需要先在**资产中心**页面对该服务器执行**暂停保护**。更多信息请参见开启和关闭服务器保护状态。

   在资产列表中，选中需要删除的非阿里云服务器并单击**更多操作 > 解除绑定**。

   
5. 单击**确定**。
   删除非阿里云机器后，该服务器将从资产列表中移除。

13.常见问题

本文汇总了云安全中心资产中心页面的常见问题。

如何解绑（释放）非阿里云资产？

对于无需防护的非阿里云服务器，您可通过云安全中心手动解除绑定。更多信息请参见删除非阿里云服务器。

对服务器解除绑定后，该服务器将不再受云安全中心的防护，并且您在云安全中心控制台将无法再看到该资产相关的任何数据，包括告警、漏洞、攻击信息等。

> **说明**
>
> - 只有Agent客户端状态为**暂停保护**或**关闭**的非阿里云服务器才可执行**解除绑定**操作。如需释放客户端状态为**开启**的服务器，请先在**资产中心**页面对该服务器执行**暂停保护**。更多信息请参见开启和关闭服务器保护状态。
> - 如果您未对服务器解除绑定，只是暂停或卸载客户端Agent，您仍然可以在云安全中心控制台看到该服务器的信息。

云安全中心如何解绑阿里云ECS服务器？

云安全中心不支持解绑阿里云ECS服务器。您购买的阿里云ECS服务器，即使卸载了Agent插件，该服务器仍将以离线状态出现在服务器列表中，而不会从列表中移除。只有在ECS控制台释放ECS服务器后，该服务器才会从资产中心服务器列表中移除。