ALIBABA CLOUD

阿里云

云安全中心（态势感知）
资产中心

文档版本：20220712

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。

版本限制

云安全中心所有版本用户都可使用该功能。各版本支持的功能详情，请参见功能特性。

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。

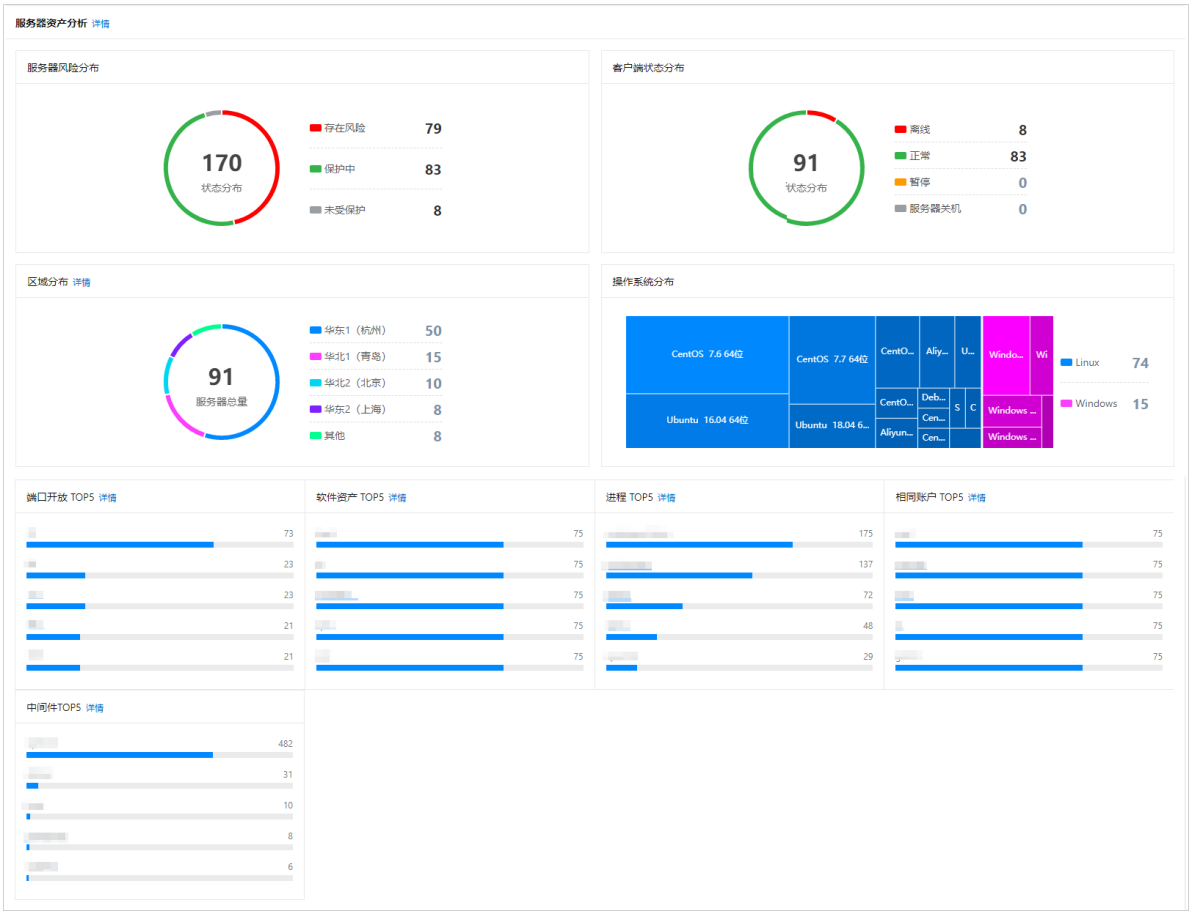
为便于对资产信息进行管理，资产中心提供了资产分组和标签分类功能。您可以将资产分组，以组别的维度查看安全事件；也可以通过资产标签筛选具有相同属性的资产。更多信息，请参见管理服务器的分组、重要性及标签和管理资产标签。

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，请参见查看服务器信息。
- 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，请参见查看服务器信息。
- 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，请参见查看云产品信息。

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

2.资产暴露分析

资产暴露分析支持自动分析您的ECS服务器在互联网上的暴露情况，可视化呈现ECS与互联网的通信链路，并集中展示您暴露在公网的ECS的漏洞信息，帮助您快速定位资产在互联网上的异常暴露情况并提供相应漏洞的修复建议。本文介绍如何使用云安全中心资产暴露分析功能。

版本限制

仅云安全中心的企业版和旗舰版支持该功能，其他版本不支持。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。

支持的服务器类型

资产暴露分析功能仅统计您的ECS服务器在互联网上的暴露情况，不支持统计非阿里云服务器在互联网上的暴露情况。

统计数据说明

资产暴露分析结果会每天自动刷新。**资产暴露分析**页面为您展示资产在互联网暴露情况的统计数据和详细信息列表。下表为统计数据的说明。

统计项	说明
暴露资产/公网IP数	暴露在互联网上的ECS服务器总数量和IP地址总数量。
网关资产	暴露在互联网上的网关资产（负载均衡、NAT网关）总数量。单击相应数值打开**网关资产**面板，可查看网关资产的列表。在**网关资产**面板，单击网关资产名称可跳转至对应资产详情页面。
暴露端口	暴露在互联网上的端口总数量。单击相应数值打开**暴露端口**面板，可查看暴露端口的列表。在**暴露端口**面板，单击暴露端口名称查看存在该暴露端口的资产列表。
暴露组件	暴露在互联网上的您ECS服务器的系统组件（例如OpenSSL、OpenSSH）总数量。单击相应数值打开**暴露组件**面板，可查看暴露组件的列表。在**暴露组件**面板，单击暴露组件名称查看存在该暴露组件的资产列表。
可被利用漏洞	暴露在互联网上可被黑客利用的漏洞总数量及高危、中危、低危漏洞数量。单击表示高危、中危、低危漏洞数量的数字可跳转至**漏洞修复**页面。不同类型的漏洞使用不同颜色表示： • 高危：红色。此类漏洞会对您的资产安全较大的威胁，建议您重点关注并及时修复。 • 中危：橙色。此类漏洞对您的资产会产生一定的危害，建议您及时修复。 • 低危：灰色。此类漏洞对您的资产安全危害较小，您可以延后修复。
弱口令	暴露在互联网上的您ECS服务器弱口令的总数量。单击相应数值，可查看存在弱口令的暴露ECS服务器列表。

前提条件

资产暴露分析功能依赖于资产指纹采集功能获取的中间件相关信息，您需要将**中间件**的采集周期设置为**每1小时采集一次**、**每3小时采集一次**、**每12小时采集一次**或**每天采集一次**。如果您关闭了自动采集或设置的采集周期过长（例如采集周期设置为**每7天采集一次**），资产暴露分析功能将无法每天刷新检测结果。具体操作，请参见采集资产指纹。

查看资产暴露详情

1. 登录云安全中心控制台，在左侧导航栏，单击**资产暴露分析**。
2. 在**资产暴露分析**页面，查看资产暴露信息。
   - **查看资产暴露总览数据**

     在**资产暴露分析**页面上方总览区域，您可以资产暴露的总体情况，包括**弱口令**、**可被利用漏洞**等总览数据。单击下方数字，可查看对应数据的详情。
   - **筛选查看暴露情况**

     您可使用页面提供的搜索组件从有无漏洞、资产分组、端口等维度筛选查看资产暴露情况。
   - **查看暴露详情**

     单击要查看的资产**操作**列的**暴露详情**，资产的暴露详情面板，查看资产暴露通信链路拓扑图、链路详情、弱口令和漏洞信息。
     - 在**弱口令**页签下，查看检测出的弱口令详情。您可以单击检测出的弱口令风险名称，跳转到该资产的**基线检查**页签下，查看该资产上检测出的所有基线风险。黑客可能会利用您ECS服务器上的弱口令进行非法登录，窃取服务器数据或破坏服务器，建议您及时修复弱口令风险。
     - 在**可被利用漏洞**、**全部漏洞**页签下，单击漏洞链接，可跳转漏洞详情页面，您可以查看漏洞信息并根据漏洞修复建议手动修复相应漏洞。建议您及时修复高危漏洞。
     - 如果您的ECS服务器可以通过多种方式访问互联网，通信链路拓扑图会为您展示多条访问互联网的路径。例如您的ECS服务器可以通过NAT网关和负载均衡访问公网，通信链路拓扑图将为您展示访问互联网的两条通信链路。单击不同访问路径上的资产图标，可以切换到该路径，查看该路径详情。

       > **说明** 资产暴露通信链路拓扑图颜色和资产中存在的漏洞的等级的对应关系如下：
       > - 红色：资产中存在弱口令风险或可被黑客通过互联网利用的高危漏洞。
       > - 橙色：资产中存在可被黑客通过互联网利用的中危漏洞。
       > - 灰色：资产中存在可被黑客通过互联网利用的低危漏洞。
       > - 绿色：资产中不存在弱口令风险或可被黑客通过互联网利用的漏洞。
       >
       > 以上拓扑图颜色和漏洞等级的对应关系仅对您的资产生效，不对网络链路图的其余部分（例如互联网）生效，互联网图标默认为灰色。
   - **导出资产暴露数据**

     您可以单击暴露资产列表右上角图标，将暴露资产的详细信息统一导出并保存到本地。导出的文件为Excel格式。

3.管理服务器

3.1. 查看服务器信息

资产中心页面提供了已接入云安全中心的所有服务器的信息，例如服务器的服务商、所在地域、所属VPC、风险状况、资产指纹等信息。本文介绍如何查看服务器的相关信息。

查看服务器信息

同步资产信息

查看服务器信息之前，需要先完成最新资产同步的操作，以确保将新接入的服务器同步到资产列表中。

1. 登录云安全中心控制台，在左侧导航栏，单击**资产中心**。
2. 在**服务器**页签的**服务器**子页签下，单击**同步最新资产**，拉取最新的服务器资产信息，刷新服务器列表。

> **说明** 同步最新资产信息需要1分钟时间，请您耐心等待。

查看服务器信息

1. 登录云安全中心控制台，在左侧导航栏，单击**资产中心**。
2. 在**服务器**页签的**服务器**子页签下，查看服务器的信息。
   - 查看单个服务器的信息

     您可使用服务器列表上方提供的搜索组件，通过该服务器的**实例名称**、**公网IP**、**私网IP**精准查找到该服务器。

     在该服务器的**风险状况**列，可查看到该服务器是否存在安全风险。

     单击服务器**操作**列的**查看**，进入该服务器的详情页面查，看服务器的详细信息。

功能页签	说明

功能页签	说明
基本信息	■ 详细信息 展示了该服务器的基本信息，如服务器的ID、地域、分组、操作系统等。还支持更换该服务器的分组，以及对服务器上云安全中心客户端的异常状态进行一键诊断（客户端问题排查）。 **说明** 如果服务器的基本信息（如MAC地址、内核版本等）缺失，您可以返回资产列表，选中该服务器，在服务器列表下方选择**更多操作** > **资产采集**，一键采集该服务的基本信息。 ■ 防御状态 展示了该服务器的客户端自保护、病毒防御、网络防御这三个功能的开启状态。 ■ 漏洞检测 展示漏洞检测类型，支持为该服务器开启或关闭不同类型的漏洞检测功能。 ■ 防暴力破解 展示该服务器应用的暴力破解防御规则内容，支持修改该服务器应用的暴力破解防御规则。 ■ 登录安全设置 展示该服务器已添加的常用登录地址、登录的IP、时间和账号，支持设置该服务器的相关告警。
漏洞信息	展示该服务器的漏洞检测结果。
安全告警处理	展示该服务器的安全告警信息。
基线检查	展示该服务器的基线检查结果。
资产指纹调查	展示该服务器指纹的详细信息。
云平台配置	展示该服务器云平台配置检查的详细信息。
运维监控	■ 远程运维 展示了该服务器通过云助手进行远程运维的命令列表、命令执行的结果以及文件发送结果。 ■ 性能监控 展示了该服务器的CPU使用率、内存使用率、系统负载、网络流入流出速率、TCP连接数等数据。

- 查看同一分类的服务器的信息

  资产中心提供了**存在风险的服务器**、**未受保护的服务器**、**暴露的服务器**等服务器的分类方式，帮助您对服务器进行分类管理。

分类	说明
所有服务器	可查看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	可查看存在漏洞、基线风险、告警等安全风险的服务器。
未受保护的服务器	可查看Agent客户端状态为**关闭**或**暂停保护**的服务器。 **注意** 云安全中心无法对Agent客户端状态为**关闭**或**暂停保护**的服务器提供安全防护。如果您想开启云安全中心对服务器的保护，具体操作，请参见修改服务器保护状态。
关机的服务器	可查看已关机的服务器。
暴露的服务器	可查看暴露在互联网中的服务器（即可与互联网通信的服务器）。您资产在互联网暴露情况的详情，请参见资产暴露分析。 **说明** ■ 仅企业版和旗舰版支持资产暴露分析功能，其他版本用户需要升级至企业版或旗舰版才能查看暴露在互联网的服务器数量和列表。 ■ **暴露的服务器**右侧显示**未知**表示您当前版本不支持资产暴露分析功能，云安全中心无法提供暴露服务器的数量信息。如果您需要使用资产暴露分析功能，您需要先升级到企业版或旗舰版。具体操作，请参见升级与降配。
新增服务器	可查看最近15天内新购买的阿里云ECS服务器。
服务器组	可查看各服务器组服务器。您可单击目标分组**包含服务器数量**、**存在风险数量**或**未保护数量**列的数字，查看目标分组下对应维度的服务器的安全状态。 **说明** 云安全中心支持**管理**和**删除**服务器分组，具体操作，请参见管理服务器的分组、重要性及标签。
服务器地域	可查看各地域内服务器。您可单击目标地域的**包含服务器数量**、**存在风险数量**或**未保护数量**列的数字，查看目标地域下对应维度的服务器的安全状态。
专有网络VPC	可查看各专有网络VPC下的服务器。你可单击目标专有网络VPC的**包含服务器数量**、**存在风险数量**或**未保护数量**列的数字，查看目标VPC下对应维度的服务器的安全状态。

分类	说明
资产重要性	可查看各资产重要性等级下服务器。您可在**资产重要性**区域，单击**重要资产**、**一般资产**或**测试资产**，查看对应重要性下的服务器的安全状态。 **说明** 云安全中心支持将资产按重要性划分为3个等级。资产重要性需要您根据您业务的实际情况，对您当前账号下的资产按重要等级进行分类，帮助您从资产重要性的维度对资产进行批量管理。
标签	可查看各资产标签下服务器。您可单击**标签**下已添加的资产标签，查看对应标签下服务器的安全状态。 **说明** 云安全中心支持**管理**和**删除**服务器标签，具体操作，请参见管理资产标签。

- 查看满足一个或多个检索条件的服务器的信息

  所有服务器、**存在风险的服务器**、**未受保护的服务器**、**关机的服务器**、**暴露的服务器**、**新增服务器**这几个服务器分类下，还支持设置一个或者多个检索条件，筛选出满足筛选条件的服务器。

  下文以设置同时满足系统类型为Linux系统、存在安全告警、所在地域为华东1（杭州）这3个检索条件的服务器为例，为您介绍如何设置多检索条件筛选目标服务器。

  a. 在**资产中心**的服务器页签下，单击**未受保护的服务器**。

  b. 在检索条件下拉菜单中，对**系统类型**、**是否存在安全告警**、**地域**分别做以下设置。

     - **系统类型**：Linux
     - **是否存在安全告警**：有
     - **地域**：华东1（杭州）

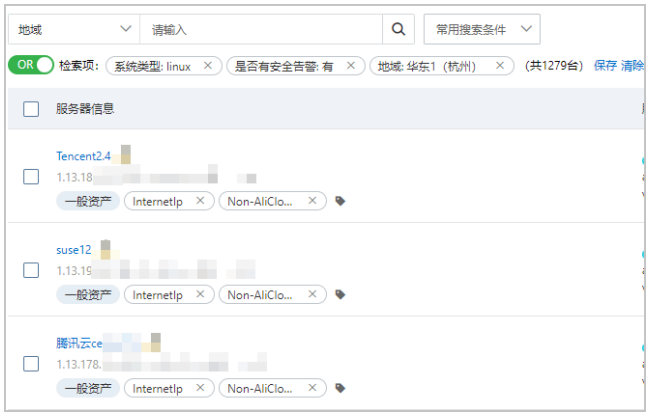
     说明 部分检索条件不支持选择，您可以选择该筛选条件后，在右侧的输入框中输入具体的筛选信息进行设置。

     设置筛选条件后，服务器列表上方的**检索项**中会显示您已设置的检索条件。

c. 单击**检索项**左侧的AND或者OR，可以切换各个检索条件之间的逻辑关系。

- 检索条件设置为**AND**：多个检索项之间是**与关系**。
- 检索条件设置为**OR**：多个检索项之间是**或关系**。

设置完成后，服务器列表中的服务器即为满足这3个检索条件的服务器。



d. （可选）如果您想将以上设置的筛选条件作为**常用筛选条件**，您可以单击检索条件右侧的**保存**。

设置为**常用筛选条件**后，您后续查找服务器，可以使用**常用筛选条件**功能中已保存的筛选条件，快速查找目标服务器。

3.2. 修改服务器保护状态

在服务器上安装云安全中心Agent后，云安全中心会自动开启对服务器的安全防护。您可根据您的业务需要，修改云安全中心对服务器的保护状态。本文介绍如何修改云安全中心对服务器的保护状态。

背景信息

在服务器成功安装Agent后，在**资产中心**页面的服务器列表，服务器的**客户端**列显示图标，表示该服务器已受到云安全中心的安全防护。如果服务器**客户端**列显示图标，则说明该服务器上的未安全云安全中心Agent或者Agnet处于离线状态。Agent离线状态下，云安全中心无法为服务器提供安全防护，请您及时处理Agent离线问题。具体操作，请参见Agent离线排查。

前提条件

请确保已在服务器上安装了云安全中心Agent。具体操作，请参见安装Agent。

操作步骤

1. 登录云安全中心控制台，在左侧导航栏，单击**资产中心**。
2. 在**资产中心**的**服务器**页签下，修改服务器的保护状态。
   - **暂停保护**

     注意 云安全中心无法为**暂停保护**的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。

     如果您确认服务器无需云安全中心的防护，可将服务器的保护状态设置**暂停保护**。选中一个或多个**客户端**列显示图标的服务器，单击列表下方的**更多操作**，在**更多操作**菜单中单击**暂停保护**。

设置成功后，目标服务器**客户端**列的图标会变为图标，表示该服务器已不再受到云安全中心的安全防护。

- **开启保护**

  选中一个或多个**客户端**列显示图标的服务器，单击列表下方的**更多操作**，在**更多操作**菜单中单击**开启保护**。

> **说明** 如果将服务器的保护状态设置为**开启保护**后，服务器**客户端**列仍然显示的是图标，可能是以下原因：
>
> - 该服务器上未安装云安全中心Agent，请为该服务器安装云安全中心Agent，安装Agent后，云安全中心会自动开启对该服务器的安全防护。安装Agent的具体操作，请参见安装Agent。
> - 该服务器上的云安全中心Agent处于离线状态，请您及时处理Agent离线问题。具体操作，请参见Agent离线排查。

3.3. 管理服务器的分组、重要性及标签

资产中心页面提供了服务器组、重要性及标签这三个功能，用于帮助您从不同的维度对服务器进行管理。使用这三个功能对服务器进行管理，能为您后续使用云安全中心的功能提供便利。本文介绍如何使用这三个功能对服务器进行管理。

管理服务器的分组

在使用防勒索、网页防篡改、基线检查、漏洞扫描等云安全中心功能，选择生效的服务器时，如果您提前使用**服务器组**功能对服务器进行了分组，即可按照服务器的分组进行快捷选择，免去一个个选择生效服务器的麻烦。

1. 登录云安全中心控制台，在左侧导航栏，单击**资产中心**。
2. 在**服务器**页签的**服务器**子页签下，通过服务器列表左侧**属性**区域的**服务器组**，对服务器进行分组管理。
   - **查看目标分组**

     在**服务器组**区域，单击目标服务器组的名称，可查看该服务器组下的所有服务器的列表。
   - **新建分组**

     在**服务器组**区域，单击右上角**添加**，在**添加分组**对话框中，填写分组的名称、选择要添加到该分组的服务器，然后单击**确定**。
   - **编辑和删除分组**
     - 编辑分组

       将鼠标悬停在目标分组，单击图标，在**添加分组**对话框中，修改分组的名称、添加或删除分组中的服务器。

- 删除分组

  将鼠标悬停在目标分组，单击×图标，在**提示**对话框中，单击**确定**。

  > **说明** 默认分组**未分组**不支持删除。

- **更换分组**

  在**服务器组**区域，单击目标分组的名称，进入该分组的服务器列表，选中要更换分组的服务器，单击列表下方的**更换分组**，在**更换分组**对话框中的**新的分组**下拉菜单，选择要更换的分组的名称，然后单击**确定**。

  您也可以在所有服务器列表中，筛选并选中您要更换分组的服务器，单击列表下方的**更换分组**，在**更换分组**对话框中，选择要更换的分组的名称，然后单击**确定**。

管理服务器的重要性

您为服务器设置的重要性，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**，进而影响服务器漏洞修复紧急度最终得分。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。建议您将核心服务器的**重要性**设置为**重要**，云安全中心将根据服务器的重要性提示您尽快修复重要服务器中的漏洞。

下表展示了服务器重要性和资产重要性因子取值的关系。关于漏洞修复优先级的更多信息，请参见漏洞修复优先级。

重要性类型	资产重要性因子	选择建议
重要	1.5	运行您核心业务或存储核心数据的服务器，该类服务器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	1	运行一般业务的服务器，可替代性较高。该类服务器被病毒恶意入侵后对整个系统的影响较小。
测试	0.5	进行业务功能或性能测试的服务器，或其他对您业务影响较小的服务器。

> **说明** 如果您未设置服务器重要性，您所有服务器的重要性标签默认为**一般**，即所有资产重要性因子都为1。

1. 登录云安全中心控制台，在左侧导航栏，单击**资产中心**。
2. 在**服务器**页签的**服务器**子页签下，通过服务器列表左侧的**重要性**区域，管理服务器的重要性。
   - **设置服务器的重要性**

     单击**重要性**区域的**管理**，在**资产重要性管理**对话框中，选择重要性、选择该资产重要性下的要包含的服务器，单击**确认**。
   - **管理服务器的重要性**

     将鼠标悬停在**重要性**区域下的目标重要性（**重要**、**一般**、**测试**）上，单击⚙图标，在**资产重要性管理**对话框中，根据业务需要添加或减少该重要性下的服务器，然后单击**确定**。
   - **管理单个服务器的重要性**

     您可以在服务器列表中，单击目标资产**服务器信息**列的🏷图标，在对话框中选择重要性，然后单击**确定**。

管理服务器标签

使用**标签**功能为服务器自定义标签标识其特殊属性，可方便您筛选具有相同属性的服务器。

1. 登录云安全中心控制台，在左侧导航栏，单击**资产中心**。
2. 在**服务器**页签的**服务器**子页签下，通过服务器列表左侧的**标签**区域，管理服务器的标签。
   - **查看目标标签**

     在**标签**区域，单击目标标签的名称，可查看该标签下的所有服务器的列表。
   - **新建标签**

     在**标签**区域，单击右上角**添加**，在**标签管理**对话框中，填写标签的名称、选择要添加该标签的服务器，然后单击**确定**。
   - **编辑和删除标签**
     - 编辑标签

       将鼠标悬停在目标标签，单击 图标，在**标签管理**对话框中，修改标签的名称、添加或删除包含该标签的服务器，然后单击**确定**。
     - 删除标签

       将鼠标悬停在目标标签，单击 × 图标，在**提示**对话框中，单击**确定**。
   - **管理单个服务器的标签**
     - 添加标签

       您可以在服务器列表中，单击服务器**服务器信息**列的 图标，在对话框中为该服务器选择标签，然后单击**确定**。

       > **说明** 支持为一个服务器添加多个标签。
     - 删除标签

       在服务器列表中，单击服务器**服务器信息**列的标签右侧的 × 图标，在**提示**对话框中，单击**确定**。

3.4. 资产指纹调查

云安全中心提供资产指纹调查功能，支持采集服务器资产的11种资产指纹数据。本文介绍如何使用资产指纹调查功能采集及查看服务器的资产指纹数据。

背景信息

首次使用资产指纹调查功能时，建议您通过设置资产指纹的采集频率，自动采集您所有资产的指纹数据。资产指纹调查的内容，请参见资产指纹调查的内容。

版本限制

仅企业版和旗舰版支持该功能，其他版本用户需要升级到企业版或旗舰版才可使用该功能。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。

采集资产指纹

开通云安全中心企业版或旗舰版后，云安全中心不会自动采集资产指纹数据。您需要设置自动周期性采集或手动立即采集来获取最新的资产指纹数据。

采集方式	描述
周期性自动采集	云安全中心支持自动采集所有资产的资产指纹数据。您可按需求配置自动采集资产指纹的频率。具体操作，请参见设置周期性自动采集资产指纹。
采集所有资产最新指纹数据	如果您想立即查看所有资产的资产指纹数据，您可使用**采集最新数据**功能一键采集所有资产的最新资产指纹数据。具体操作，请参见手动采集所有资产最新指纹数据。
采集单个资产最新指纹数据	如果您想立即查看单个资产的资产指纹数据，您可使用**立即采集数据**功能一键采集该资产的最新资产指纹数据。具体操作，请参见手动采集单个资产最新指纹数据。

1. 登录云安全中心控制台，在左侧导航栏，单击**资产中心**。
2. 在**资产中心**页面的**服务器**页签，采集资产指纹数据。
   - 设置周期性自动采集
     a. 在**服务器**页签的**账户**子页签下，单击**配置管理**。
     b. 在**配置管理**对话框，设置各个资产指纹的采集频率，然后单击**确定**。

     > **说明**
     > - 云安全中心不会自动触发采集任务获取对应资产指纹的最新数据。所有资产指纹的刷新频率均默认为**关闭**。不同的资产指纹可以设置不同的刷新频率。
     > - **中间件**、**数据库**以及**Web服务**这三种资产指纹的采集频率设置，统一在配置项**中间件**中配置。
     > - 如果您正在使用**资产暴露分析**功能，**中间件**的数据采集频率需要设置为**每1小时采集一次**、**每3小时采集一次**、**每12小时采集一次**或**每天采集一次**，不能设置为**关闭**或**每7天采集一次**。更多信息，请参见资产暴露分析。

     完成采集频率设置后，云安全中心会按照设定的采集频率自动触发资产指纹采集任务，记录最新资产指纹数据到**资产中心**的**服务器**页签下的各资产指纹页签，您可以在各资产指纹页签下查看最新指纹数据。更多信息，请参见查看资产的资产指纹数据。
   - 手动采集所有资产最新指纹数据
     a. 在**服务器**页签的**账户**子页签下，单击**采集最新数据**。
     b. 在**采集最新数据**对话框，选中需要采集的资产指纹数据，然后单击**确定**。

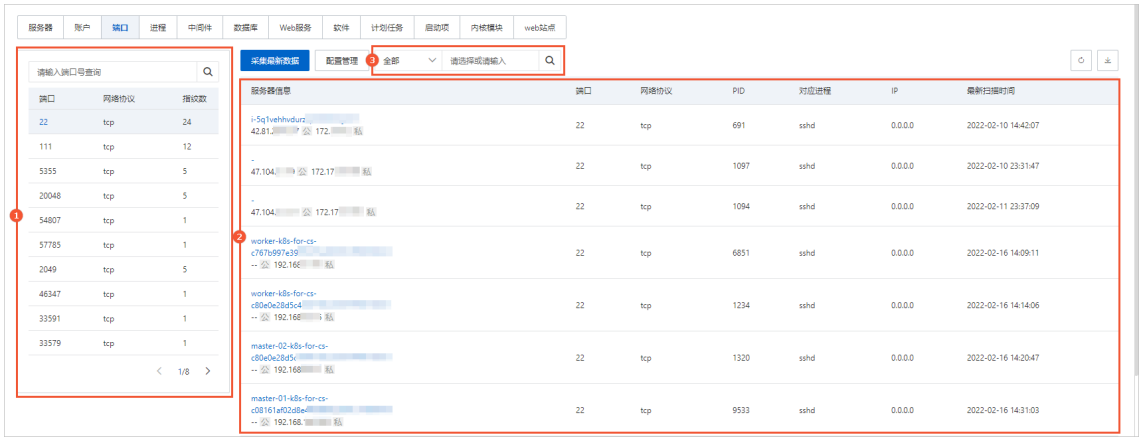
     > **说明** 大约需要1~5分钟可以完成数据采集，请您耐心等待。
   - 手动采集单个资产最新指纹数据
     a. 在**服务器**页签的**服务器**子页签下的服务器列表中，单击需要采集资产指纹的服务器**操作**列的**查看**。
     b. 在该资产详情页面，单击**资产指纹调查**页签，然后单击要采集的资产指纹的对应页签。
     c. 单击右上方的**立即采集数据**，在**采集任务下发成功**对话框中，单击**确定**。

> **说明** 大约需要1~5分钟可以完成数据采集，请您耐心等待。

查看资产的资产指纹数据

1. 登录云安全中心控制台，在左侧导航栏，单击**资产中心**。
2. 在**资产中心**页面的**服务器**页签下，查看资产指纹数据。
   - 查看所有资产的资产指纹

     在**服务器**页签下，单击要查看的资产指纹页签，查看对应的资产指纹数据。

     - 图示①：资产指纹列表，主要包括所有资产指纹及其应用的服务器数量。
     - 图示②：资产指纹的详情列表，在左侧资产指纹列表中单击目标指纹（如单击某个端口号），页面右侧的资产指纹列表中会展示目标指纹对应的指纹详情。
     - 图示③：资产指纹搜索功能组件，您可在搜索框中输入相应信息，搜索目标指纹信息，支持模糊搜索。
   - 查看单个资产的资产指纹

     a. 在**服务器**页签的**服务器**子页签下的服务器列表中，单击需要查看资产指纹的服务器**操作**列的**查看**。

     b. 在该资产详情页面，单击**资产指纹调查**页签，然后单击要查看的资产指纹页签，查看资产指纹数据。

资产指纹调查的内容

资产指纹类型	描述

资产指纹类型	描述
账户	服务器的账户。定期采集服务器的账户信息，具体包括以下内容： • **服务器信息**：账户所属的服务器。 • **账号**：账号信息。 • **ROOT权限**：账户是否有root权限。 • **用户名**：账户的名称。 • **用户组**：账户所属的用户组的信息。 • **到期时间**：账户密码的到期时间。 • **密码是否过期**：账户密码是否已过期。 • **密码是否锁定**：账户密码是否已锁定。 • **用户是否过期**：账户状态是否已过期。 • **是否sudo账号**：账户是否拥有sudo权限。 • **是否交互登录账号**：账户是否具备login权限。 • **上次登录**：当前账户上一次登录服务器的时间。 • **最新扫描时间**：云安全中心最近一次采集服务器信息的时间。
端口	监听端口。定期采集服务器的对外端口监听信息，具体包括以下内容： • **服务器信息**：端口所在的服务器信息，包括服务器名称和IP地址。 • **端口**：监听端口号。 • **网络协议**：监听端口使用的网络协议。 • **PID**：监听端口对应服务器的运行进程的标识符。 • **对应进程**：监听端口对应服务器的运行进程。 • **IP**：监听端口绑定的网卡的IP。 • **最新扫描时间**：云安全中心最近一次采集监听端口信息的时间。
进程	运行进程信息。定期采集服务器的进程信息，具体包括以下内容： • **服务器信息**：进程所在的服务器信息，包括服务器名称和IP地址。 • **进程名**：进程的名称。 • **进程路径**：进程的启动路径。 • **启动参数**：进程的启动参数。 • **启动时间**：进程的启动时间。 • **运行用户**：进程的启动用户。 • **运行权限**：进程启动用户的权限。 • **PID**：进程的ID。 • **父进程PID**：进程启动的父进程的ID。 • **文件MD5**：进程文件的MD5值。 • **是否安装包进程**：是否使用安装包内的进程。 • **进程状态**：进程的当前状态。 • **最新扫描时间**：云安全中心最近一次采集服务器信息的时间。

资产指纹类型	描述
中间件	定期采集服务器的中间件信息。中间件是指可独立运行的系统组件，例如MySQL（数据库）、Docker（容器组件）等。具体采集以下内容： • **服务器信息**：中间件所在的服务器信息，包括服务器名称和IP地址。 • **中间件**：中间件的名称。 • **类型**：中间件的所属类型。 • **运行时环境版本**：中间件运行时的环境的版本。 • **版本**：原中间件的版本号。 • **PID**：中间件的启动进程的ID。 • **启动路径**：中间件的启动路径。 • **版本验证信息**：中间件版本的获取方式。 • **父进程PID**：中间件启动的父进程的ID。 • **运行用户**：中间件的启动用户。 • **监听IP**：中间件启动监听的IP地址。 • **监听端口**：中间件启动监听的端口。 • **监听状态**：中间件当前的监听状态。 • **监听端口协议**：中间件当前监听端口的网络协议。 • **启动时间**：中间件的启动时间。 • **进程命令行**：中间件启动执行命令的参数。 • **容器名称**：中间件所在的容器的名称。 • **镜像名称**：中间件所在的镜像的名称。 • **配置路径**：中间件启动配置所在的绝对路径。 • **最新扫描时间**：云安全中心最近一次采集服务器信息的时间。

资产指纹类型	描述
数据库	数据库信息。定期采集服务器上的数据库的信息，具体包括以下内容： • **服务器信息**：数据库所在的服务器信息，包括服务器名称和IP地址。 • **数据库名**：数据库的名称。 • **类型**：数据库的类型。 • **版本**：数据库的版本号。 • **PID**：数据库的启动进程的ID。 • **启动路径**：数据库的启动路径。 • **版本验证信息**：数据库版本的获取方式。 • **父进程PID**：数据库的启动的父进程的ID。 • **运行用户**：数据库的启动用户。 • **监听IP**：数据库启动监听的IP地址。 • **监听端口**：数据库启动监听的端口。 • **监听状态**：数据库当前的监听状态。 • **监听端口协议**：数据库当前监听端口的网络协议。 • **启动时间**：数据库的启动时间。 • **启动命令行**：数据库启动执行命令的参数。 • **容器名称**：数据库所在的容器的名称。 • **镜像名称**：数据库所在的镜像的名称。 • **配置路径**：数据库启动配置所在的绝对路径。 • **最新扫描时间**：云安全中心最近一次采集服务器信息的时间。

资产指纹类型	描述
Web服务	Web服务信息。定期采集服务器上的Web服务的信息，具体包括以下内容： • **服务器信息**：所在的服务器信息，包括服务器名称和IP地址。 • **Web服务名**：Web服务名称。 • **类型**：Web服务的类型。 • **运行时环境版本**：Web服务运行时JDK环境的版本。 • **版本**：Web服务的版本号。 • **PID**：Web服务启动进程的ID。 • **启动路径**：Web服务的启动路径。 • **版本验证信息**：版本的获取方式。 • **父进程PID**：Web服务启动的父进程的ID。 • **运行用户**：Web服务的启动用户。 • **监听IP**：Web服务启动监听IP的地址。 • **监听端口**：Web服务启动监听的端口。 • **监听状态**：Web服务当前的监听状态。 • **监听端口协议**：Web服务当前监听端口的网络协议。 • **启动时间**：Web服务的启动时间。 • **启动命令行**：Web服务启动执行命令的参数。 • **容器名称**：Web服务所在的容器的名称。 • **镜像名称**：Web服务所在的镜像的名称。 • **配置路径**：Web服务启动配置所在的绝对路径。 • **Web目录**：Web配置网页的路径。 • **最新扫描时间**：云安全中心最近一次采集服务器信息的时间。
软件	软件资产。定期采集服务器的软件信息，具体包括以下内容： • **服务器信息**：软件所在的服务器，包括服务器名称和IP地址。 • **软件资产**：软件资产的名称。 • **版本**：软件的版本号。 • **软件启动路径**：软件启动的路径。 • **软件更新时间**：软件版本的更新时间。 • **最新扫描时间**：云安全中心最近一次采集软件信息的时间。
计划任务	定期采集您服务器上周期性执行的任务路径信息。具体采集任务的以下信息： • **服务器信息**：计划任务所在的服务器信息，包括服务器名称和IP地址。 • **执行命令**：计划任务执行的命令行。 • **任务周期**：计划任务的定时周期。 • **MD5**：计划任务进程的HASH。 • **账户名称**：启动任务的账号。 • **最新扫描时间**：云安全中心最近一次采集服务器信息的时间。

资产指纹类型	描述
启动项	启动项信息。定期采集服务器的启动项信息，具体包括以下内容： • **服务器信息**：启动项所在的服务器信息，包括服务器名称和IP地址。 • **启动项路径**：启动服务所在的路径。 • **最新扫描时间**：云安全中心最近一次采集服务器信息的时间。
内核模块	内核模块信息。定期采集服务器的内核模块信息，具体包括以下内容： • **服务器信息**：内核模块所在的服务器信息，包括服务器名称和IP地址。 • **模块名称**：内核模块的名称。 • **模块大小**：内核模块文件的大小。 • **模块文件路径**：内核模块所在的路径。 • **被模块依赖数目**：其他依赖模块的数量。 • **最新扫描时间**：云安全中心最近一次采集服务器信息的时间。
Web站点	Web站点信息。定期采集服务器的Web站点信息，具体包括以下内容： • **服务器信息**：Web站点所在的服务器信息，包括服务器名称和IP地址。 • **域名**：Web站点配置的域名。 • **站点类型**：Web服务使用软件的类型。 • **端口**：Web服务的监听端口。 • **Web路径**：WebHome目录的路径。 • **Web根路径**：Web配置中根目录的路径。 • **用户**：Web服务的启动用户。 • **目录权限**：Web目录的权限。 • **监听协议**：Web启动的监听协议。 • **PID**：进程的ID。 • **启动时间**：Web服务的启动时间。 • **镜像名称**：Web站点所在的镜像的名称。 • **容器名称**：Web站点所在的容器的名称。 • **最新扫描时间**：云安全中心最近一次采集服务器信息的时间。

3.5. 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、中间件）采集。本文介绍如何执行服务器安全检查。

背景信息

仅云安全中心的防病毒版、高级版、企业版、旗舰版支持该功能，免费版不支持。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。

> **注意** 执行一键安全检查后，云安全中心会并发执行漏洞检测、基线检测、网站后门检测和资产指纹采集，会导致该服务器CPU和内存占用率升高，可能会对您服务器上部署的业务产生一定的影响。一键检查一般需要1~5分钟，建议您在业务低峰期执行该操作，避免影响正常业务运行。

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**确定**，执行检查。
8. 在提示对话框中，单击**确定**。

   安全检查预计需要1~5分钟，请您耐心等待，不要重复执行安全检查。

   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、中间件）的最新数据详情，请参见查看资产指纹数据。

3.6. 解绑非阿里云服务器

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绑非阿里云服务器。本文介绍如何解绑非阿里云服务器。

背景信息

如果您的非阿里云服务器已经关机（即处于离线状态），并且该服务器还有待处理的漏洞或告警事件，您可以在资产列表中对该服务器执行解绑操作，避免遗留的待处理风险影响您当前账户的整体安全分。如果您确认无需云安全中心防护这台服务器，您也可以直接执行卸载操作。具体操作，请参见卸载Agent。

> 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（保有服务器台数或计算核数），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，在左侧导航栏，单击**资产中心**。
2. 在**服务器**页签的资产列表中，选中需要解绑的非阿里云服务器，在列表下方选择**更多操作 > 解除绑定**。
3. 在**提示**对话框中，单击**确定**。

   解除绑定后，云安全中心推送卸载指令卸载服务器上的Agent，同时也会从资产列表中移除该服务器，并且将不会再对该服务器提供安全防护。

   如果您直接执行卸载Agent操作，该服务器的Agent进程和文件将完全从您的服务器中清除。您后续要使用云安全中心防护该服务器，您需要为该服务器重新安装Agent。具体操作，请参见安装Agent。

3.7. 客户端问题排查

当云安全中心客户端出现异常离线、安装或卸载失败、进程CPU占有率高等问题时，您可以使用云安全中心提供的客户端问题排查功能进行排查。本文介绍如何使用客户端问题排查功能。

背景信息

客户端问题排查的结果信息中会为您展示排查发现的问题并提供针对该问题的解决方案，还支持下载诊断日志，对客户端存在的问题进一步做验证分析。

限制条件

客户端问题排查功能支持的服务器的系统版本：

- Windows Server 2008及以上版本
- Linux 64位系统（CentOS 5及以下版本不支持）

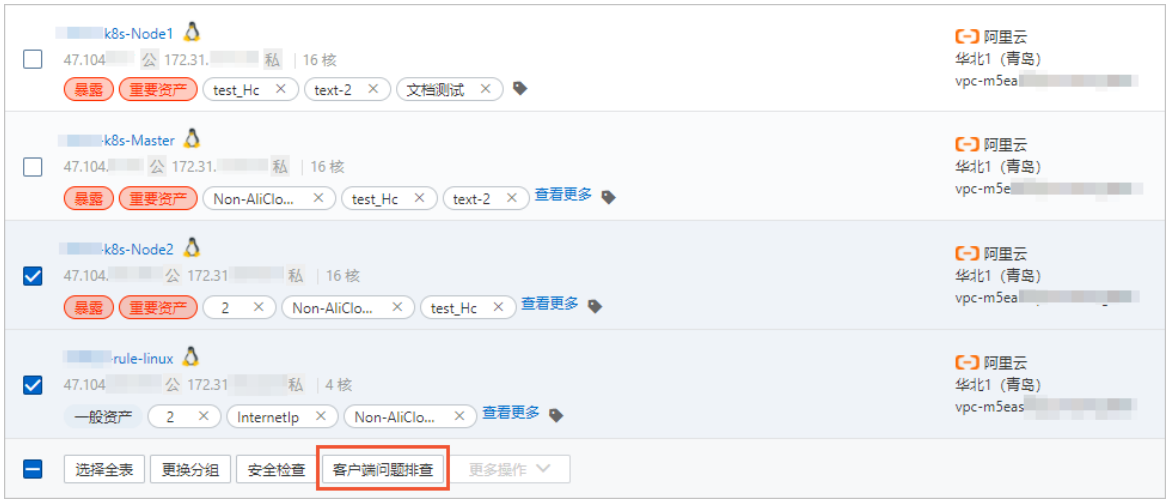
使用场景说明

- 如果您的服务器资产已接入云安全中心，您可以直接使用**资产中心**页面的**服务器**页签下提供的**客户端问题排查**功能，对目标服务器上客户端的问题进行排查。具体操作，请参见服务器资产已接入云安全中心。

- 如果您的服务器资产未接入云安全中心，您可以手动执行aegis_checker命令，对目标服务器上客户端的问题进行排查。具体操作，请参见服务器资产未接入云安全中心。

服务器资产已接入云安全中心

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**。
4. 在**服务器**页签下的服务器列表中，选中您要排查的服务器（可多选），单击列表下方的**客户端问题排查**。



5. 在**客户端问题排查**对话框，选择客户端问题排查的**问题类型**和**模式**。

   配置项说明如下：

配置项	说明
问题类型	选择客户端存在的问题类型。如果您不确认客户端存在的问题，可选择**全面检查**。
模式	选择客户端问题排查的模式，可选择的模式有： ○ **常规模式**：常规模式将采集与客户端相关日志数据上报至云安全中心进行分析，排查需要1分钟左右。 ○ **增强模式**：增强模式将采集与客户端相关的网络、进程、日志等数据上报云安全中心进行分析，排查需要5分钟左右。

6. 单击**开始诊断**。

   > **说明** 客户端问题排查的诊断程序将在该服务器中采集与客户端相关的网络、进程、日志等数据上报云安全中心进行分析。

7. 在**注意**对话框中，单击**确认**，展开**任务管理**面板，查看所有的客户端问题排查任务。

   您也可以在**资产中心**页面，单击右上角的**客户端任务管理**展开**任务管理**面板。

8. 定位到您要查看的客户端排查任务，单击**操作**列的**详情**，展开**执行日志**面板。

   执行日志面板上会展示每个服务器的客户端问题的排查详情。

以下为**执行日志**面板上的执行日志列表中信息的说明：

列表信息	说明
开始时间/结束时间	客户端问题排查任务的开始时间和结束时间。
服务器信息	客户端排查任务中排查的服务器的信息。
状态	客户端排查任务的状态。状态包括： ○ **启动**：表示已经下发客户端问题排查命令。 ○ **超时**：表示下发客户端问题排查命令超过一段时间还没有返回排查结果。 ○ **成功**：表示客户端问题排查结果已生成。
问题	客户端排查任务中排查发现的问题。
结果	客户端排查任务中排查出问题的解决方案。
操作	客户端排查任务的诊断日志。支持下载诊断日志对客户端问题进行进一步做验证分析。

客户端问题排查发现的问题当中，部分问题会在**结果**列给出解决方案，请按照给出的解决方案处理即可。如果在**结果**列没有给出解决方案，请单击**操作**列的**下载诊断日志**，将导出的诊断日志和AliUid给到相关人员进一步做验证分析。

服务器资产未接入云安全中心

如果您的服务器资产未接入云安全中心，你可以根据服务器操作系统不同，在服务器上手动执行相关命令，完成客户端问题排查。

1. 登录目标服务器。

   > **说明**
   > ○ Windows系统需要用管理员权限登录。
   > ○ Linux系统需要用root权限登录。

2. 在服务器上执行以下命令。

   阿里云ECS和非阿里云服务器按照操作系统的不同，客户端问题排查执行的命令也不同。

服务器	操作系统	模式	命令

<table>
<tr><th>服务器</th><th>操作系统</th><th>模式</th><th>命令</th></tr>
<tr><td rowspan="2">阿里云ECS</td><td rowspan="2">Linux系统</td><td>常规模式</td><td>在目标服务器上以root权限执行以下命令：
<pre>wget "http://update2.aegis.aliyun.com/download/aegis_client_self_check/linux64/aegis_checker.bin" && chmod +x aegis_checker.bin && ./aegis_checker.bin</pre>当ECS服务器与云安全中心网络不通时，您需要下载aegis_checker并拷贝到目标服务器后，执行以下命令：
<pre>chmod +x aegis_checker.bin
./aegis_checker.bin</pre>说明 常规模式将采集与客户端相关日志数据上报至云安全中心进行分析，排查需要1分钟左右。</td></tr>
<tr><td>增强模式</td><td>在目标服务器上以root权限执行以下命令：
<pre>wget "http://update2.aegis.aliyun.com/download/aegis_client_self_check/linux64/aegis_checker.bin" && chmod +x aegis_checker.bin && ./aegis_checker.bin -b "ew0KICAgICJ1dWlkIjogIiIsDQogICAgImNtZF9pZHgiOiAiIiwNCiAgICAiaXNzdWUiOiAib3RoZXJfaXNzdWUiLA0KICAgICJtb2RlIjogMywNCiAgICAianNydl9kb21haW4iOiBbXSwNCiAgICAidXBkYXRlX2RvbWFpbiI6IFtdDQp9"</pre>说明 增强模式将采集与客户端相关的网络、进程、日志等数据上报云安全中心进行分析，排查需要5分钟左右。</td></tr>
</table>

<table>
<tr><th>服务器</th><th>操作系统</th><th>模式</th><th>命令</th></tr>
<tr><td rowspan="3">非阿里云服务器</td><td>Windows系统</td><td>常规模式</td><td>在目标服务器上可通过以下两种方式排查客户端问题：
○ 下载aegis_checker程序，然后以管理员权限运行。
○ 以管理员权限在cmd窗口中直接执行如下命令：
<pre>powershell -executionpolicy bypass -c "(New-Object Net.WebClient).DownloadFile('http://update2.aegis.aliyun.com/download/aegis_client_self_check/win32/aegis_checker.exe', $ExecutionContext.SessionState.Path.GetUnresolvedProviderPathFromPSPath('.\aegis_checker.exe'))"; "./aegis_checker.exe"</pre>
说明 Windows操作系统上暂不支持增强模式。</td></tr>
<tr><td rowspan="2">Linux系统</td><td>常规模式</td><td>在目标服务器上以root权限执行以下命令：
<pre>wget "http://aegis.alicdn.com/download/aegis_client_self_check/linux64/aegis_checker.bin" && chmod +x aegis_checker.bin && ./aegis_checker.bin</pre></td></tr>
<tr><td>增强模式</td><td>在目标服务器上以root权限执行以下命令：
<pre>wget "http://aegis.alicdn.com/download/aegis_client_self_check/linux64/aegis_checker.bin" && chmod +x aegis_checker.bin && ./aegis_checker.bin -b "ew0KICAgICJ1dWlkIjogIiIsDQogICAgImNtZF9pZHgiOiAiIiwNCiAgICAiaXNzdWUiOiAib3RoZXJfaXNzdWUiLA0KICAgICJtb2RlIjogMywNCiAgICAianNydl9kb21haW4iOiBbXSwNCiAgICAidXBkYXRlX2RvbWFpbiI6IFtdDQp9"</pre></td></tr>
</table>

服务器	操作系统	模式	命令
	Windows系统	常规模式	在目标服务器上可通过以下两种方式排查客户端问题： ○ 下载aegis_checker程序，然后以管理员权限运行。 ○ 以管理员权限在cmd窗口中直接执行如下命令： `powershell -executionpolicy bypass -c "(New-Object Net.WebClient).DownloadFile('http://aegis.alicdn.com/download/aegis_client_self_check/win32/aegis_checker.exe', $ExecutionContext.SessionState.Path.GetUnresolvedProviderPathFromPSPath('.\aegis_checker.exe'))"; "./aegis_checker.exe"` **说明** Windows操作系统上暂不支持增强模式。

3. 检查完毕后，将生成的log压缩包导出。

   服务器的操作系统不同，log压缩包的存储位置不同。

   - Linux系统

     检查结果log的压缩包在*/root/miniconda2/aegis_checker/output*目录下。

   - Windows系统

     检查结果log的压缩包在当前目录的*./miniconda2/aegis_checker/output*目录下。

   检查结果的log中，以**[root cause]**为前缀的就是aegis_checker检测到客户端存在问题，部分问题会给出已处理或者处理方案的提示，请按照提示处理即可。如果aegis_checker没有给出问题的处理方案提示，请将输出的检查结果截图、log压缩包以及AliUid提供给阿里云技术支持进一步做验证分析。

4.查看容器信息

4.1. 查看容器安全状态

您可在云安全中心的资产中心页面的容器页签下，查看所有容器资产的相关信息。

背景信息

云安全中心旗舰版具备针对容器安全的一体化防护能力，支持在容器运行时针对容器的漏洞、配置合规、攻击入侵等行为进行实时的检测和防御。其中针对K8s的威胁的检测能力需要您开启相关配置。具体操作，请参见开启容器K8s威胁检测。

查看镜像信息

1. 登录云安全中心控制台，在左侧导航栏，单击**资产中心**。
2. 在**资产中心**的**容器**页签下，单击**镜像**页签，查看镜像的相关信息。
   - 查看总览信息

     在页面上方的总览区域，您可以查看**存在风险的镜像仓**的数量、**镜像仓**的总数量、镜像安全扫描的**剩余授权数**，单击**接入**可配置接入私有镜像仓，单击**设置**可设置镜像安全扫描的扫描范围。
   - 同步最新镜像信息

     单击**同步最新资产**，可以同步最新的镜像信息。
   - 查看镜像仓列表

     镜像仓列表中展示了所有已接入资产中心的镜像仓。您可在镜像仓列表中查看镜像仓的名称、所在地域、镜像仓的类型以及风险状态等信息。
     - 搜索目标镜像仓

       您可使用镜像仓列表上方提供的搜索组件，通过镜像仓的**实例ID**、**命名空间**、**镜像类型**等信息查找目标镜像仓。
     - 查看目标镜像仓

       单击目标镜像仓的名称或者操作列的**查看**，进入该镜像仓的详情页面，可以查看该镜像仓中的所有镜像的镜像仓名称、版本、大小、风险状态等信息。

       单击某个镜像**操作**列的**扫描**，可立即对该镜像执行镜像安全扫描，也可选中多个镜像，单击列表下方的**批量扫描**，对选中的镜像进行批量镜像安全扫描。

       单击目标镜像**操作**列的**处理**，进入该镜像的详情页面，可查看该镜像中存在的镜像系统漏洞、镜像应用漏洞、镜像基线检查以及镜像恶意样本。
     - 查看任务管理

       在镜像仓详情页面，单击右上角的**任务管理**，可查看镜像安全扫描以及镜像修复任务的状态。

查看集群信息

1. 登录云安全中心控制台，在左侧导航栏，单击**资产中心**。
2. 在**资产中心**的**容器**页签下，单击**集群**页签，查看集群的相关信息。
   - 查看总览信息

在页面上方的总览区域，您可以查看**集群总数**、**存在风险的集群**。单击**自建集群接入**可配置接入K8s自建集群。接入K8s自建集群的具体操作，请参见接入K8s自建集群。

- 同步最新集群信息

  单击**同步最新资产**，可以同步最新的集群信息。

- 查看集群列表

  集群列表中展示了所有集群的信息。您可在集群列表中查看集群的名称、所在地域、集群的类型以及风险状态等信息。

  - 搜索目标集群

    您可使用集群列表上方提供的搜索组件，通过镜像仓的**集群ID**、**集群名称**、**集群类型**等信息查找目标集群。

  - 查看目标集群

    单击目标镜集群的集群名称或者**操作**列的**查看**，进入该集群的详情页面。集群详情页面使用**集群**、**节点Node**、**应用**、**命名空间**等不同页签，从不同维度为您展示了该集群的详细信息。您可在不同页签下，从不同维度查看该集群的信息以及处理集群中存在的安全风险。

相关文档

容器安全概述

容器网络拓扑

容器K8s威胁检测

容器签名

查看镜像安全扫描结果

使用运行时刻安全监控

4.2. 接入K8s自建集群

您可以在资产中心将K8s自建集群接入云安全中心进行统一管理。本文介绍如何接入K8s自建集群。

版本限制

仅云安全中心的旗舰版支持该功能，其他版本不支持。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。

限制条件

- 您最多可接入10个K8s自建集群。
- 自建K8s集群网络类型为VPC时，仅支持接入华东1（杭州）、华北2（北京）、华东2（上海）、华南1（深圳）和中国香港地域。

> **说明** 自建K8s集群网络类型为公网时，无地域限制。

接入K8s自建集群

如果您的K8s集群是通过混合云的方式部署，且公网不可直接访问，那么您需要先进行网络配置，确保网络连通后再进行集群接入。配置流量转发规则具体操作，请参见接入非阿里云自建集群的网络配置。

1. 登录云安全中心控制台，在左侧导航栏单击**资产中心**。

2. 在**资产中心**页面，单击**容器**页签，然后单击**集群**页签。
3. 在**集群**页签，单击**自建集群接入**。
4. 在**自建集群接入**面板，单击**自建集群接入**，配置要接入的K8s自建集群的相关信息，然后单击**确定**。

参数	说明
集群名称	输入自建K8s集群的名称。名称可包含大小写字母、数字和下划线（_）、短划线（-）。
自建K8s集群版本	选择自建K8s集群的版本。
集群所在地域	选择自建K8s集群所在的地域。
网络类型	选择自建K8s集群的网络类型。
集群所在VPC	选择自建K8s集群所在VPC。
ApiServerIp	输入自建K8s集群API Server的地址。
K8s配置信息	上传K8s配置文件。您需要在服务器上生成K8s配置文件后，才能上传该配置文件。生成K8s配置文件的具体操作，请参见生成K8s配置文件。

完成K8s自建集群接入后，您可以在**自建集群管理**面板查看已接入集群的信息。

生成K8s配置文件

在生成K8s配置文件前，您的服务器需要满足以下前提条件：

- 已在服务器上搭建K8s集群。具体操作，请参见从零搭建K8s集群。
- 已安装Docker。具体操作，请参见安装Docker。
- 如果您的集群设置了访问控制策略，请确保已将容器所在地域的地址池IP加入到了访问控制的白名单中。

地域	公网IP	私网IP
华东1（杭州）	121.41.35.192、121.41.39.7、121.41.39.39、121.41.39.153、121.41.38.32	100.104.177.0/26
华东2（上海）	47.103.62.83、47.103.60.134、47.103.58.177、47.103.54.252、47.103.49.93	100.104.7.192/26
华北1（青岛）	47.104.111.68	100.104.87.192/26
华北2（北京）	123.57.55.56、123.57.55.21、123.57.55.18、123.57.55.7、123.57.55.6	100.104.20.128/26
华北3（张家口）	39.99.229.195	100.104.187.64/26
华北5（呼和浩特）	39.104.147.68	100.104.36.0/26
华南1（深圳）	47.106.245.198、47.107.237.185、47.107.237.182、47.107.237.170、47.107.237.152	100.104.9.192/26

地域	公网IP	私网IP
中国香港（香港）	47.106.245.198、47.107.237.185、47.107.237.182、47.107.237.170、47.107.237.152	100.104.111.128/26
亚太东北1（东京）	47.74.24.20	100.104.69.0/26
亚太东南1（新加坡）	47.74.238.176、47.74.238.61、47.74.237.201、47.74.237.166、47.74.237.91	100.104.41.128/26
美国西部1（硅谷）	47.254.39.224	100.104.145.64/26
美国东部1（弗吉尼亚）	47.252.4.238	100.104.36.0/26
德国（法兰克福）	47.254.158.71	172.16.0.0/20
英国（伦敦）	8.208.14.12	172.16.0.0/20
印度尼西亚（雅加达）	149.129.238.99	100.104.193.128/26

1. 使用root用户登录K8s集群所在服务器。
2. 创建用户。
   i. 执行以下命令创建ClusterRole。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
    name: ${userName}-cluster-reader
rules:
- apiGroups:
  - ""
  resources:
  - "*"
  verbs:
  - get
  - list
  - watch
```

ii. 执行以下命令创建ClusterRoleBinding。

> 注意 执行本步骤及以下所有步骤中的命令时，您需要将 `<UserName>` 替换成您的用户名称。

```
apiVersion: rbac.authorization.k8s.io/v1beta1
kind: ClusterRoleBinding
metadata:
    name: ${userName}-read-all
roleRef:
    apiGroup: rbac.authorization.k8s.io
    kind: ClusterRole
    name: ${userName}-cluster-reader
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: User
  name: ${userName}
```

更多信息，请参见K8s集群创建用户账号。

3. 创建证书。

i. 执行以下命令创建User私钥。

```
openssl genrsa -out <UserName>.key 2048
```

ii. 执行以下命令创建证书签署请求。

```
openssl req -new -key <UserName>.key -out <UserName>.csr -subj "/O=K8s/CN=<UserName
>"
```

iii. 执行以下命令签署证书。

```
openssl x509 -req -in <UserName>.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out
<UserName>.crt -days 365
```

4. 创建集群配置文件。

i. 执行以下命令创建集群配置。

```
kubectl config set-cluster k8s --server=
https: //192.168.XX.XX:6443 --certificate-authority=ca.crt --embed-certs=true --kub
econfig=/root/<UserName>.conf
```

ii. 执行以下命令创建用户配置。

```
kubectl config set-credentials <UserName> --client-certificate=<UserName>.crt --cli
ent-key=<UserName>.key --embed-certs=true --kubeconfig=/root/<UserName>.conf
```

iii. 执行以下命令创建context配置。

```
kubectl config set-context <UserName>@<ClusterName> --cluster=k8s --user=<UserName>
--kubeconfig=/root/<UserName>.conf
```

> 注意 执行本步骤及以下所有步骤中的命令时，您需要将 `<ClusterName>` 替换成您的集群名称。

iv. 执行以下命令切换context。

```
kubectl config use-context <UserName>@<ClusterName> --kubeconfig=/root/<UserName>.c
onf
```

v. 执行以下命令查看config文件。

```
kubectl config view --kubeconfig=/root/<UserName>.conf
```

5. 执行以下命令验证*kubeconfig*文件是否可用。

```
mkdir -p /home/<UserName>/.kube
cp <UserName>.conf /home/<UserName>/.kube/config
kubectl get pod -n kube-system
```

上述命令执行完成后，如果命令窗口可以正常显示Pod的信息，说明云安全中心可以访问该集群，即生成的*kubeconfig*文件是可用的。否则说明*kubeconfig*文件不可用。

接入非阿里云自建集群的网络配置

如果您的K8s集群是通过混合云的方式部署，且公网不可直接访问，那么您需要先进行网络配置，确保网络连通后再进行集群接入。

1. 指定一台ECS服务器，将其访问流量转发到第三方K8s集群API Server所在的IDC服务器上。

示例

将执行转发任务的ECS服务器10.0.XX.XX中A端口的流量，转发至第三方K8s集群API Server所在的IDC服务器192.168.XX.XX的B端口。

- CentOS 7命令：
  - 使用firewallcmd：

```
firewall-cmd --permanent --add-forward-port=port=<A端口>:proto=tcp:toaddr=<192.168.
XX.XX>:toport=<B端口>
```

  - 使用iptables：
    a. 开启端口转发。

```
# echo "1" > /proc/sys/net/ipv4/ip_forward
```

    b. 设置端口转发。

```
# iptables -t nat -A PREROUTING -p tcp --dport <A端口> -j DNAT --to-destination
<192.168.XX.XX>:<B端口>
```

- Windows命令：

```
netsh interface portproxy add v4tov4 listenport=<端口A> listenaddress=* connectaddress
=<192.168.XX.XX> connectport=<端口B> protocol=tcp
```

2. 在云安全中心将ECS服务器10.0.XX.XX以VPC的方式接入自建集群。

4.3. CI/CD

4.3.1. CI/CD概述

云安全中心CI/CD功能，支持在Jenkins或GitHub的项目构建阶段发现镜像中存在的高危系统漏洞、应用漏洞、恶意病毒、Webshell、恶意执行脚本、配置风险以及敏感数据进行检测和识别，并提供漏洞修复建议，帮助您更便捷地检测出镜像中存在的安全风险。

版本限制

仅高级版、企业版、旗舰版和仅采购增值服务的用户支持使用此功能，其他版本用户需要升级高级版、企业版、旗舰版或仅采购增值服务才可使用该功能。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。各版本的功能详情，请参见功能特性。

CI/CD原理

使用CI/CD功能无需您将镜像资产同步到云安全中心，只需要将CI/CD插件（即云安全中心镜像安全扫描插件）与Jenkins工具或GitHub集成，完成集成配置之后，当您在Jenkins工具或GitHub中构建项目时，会同时触发镜像安全扫描任务，扫描项目中是否存在镜像安全风险，并在云安全中心的**CI/CD**页签下展示扫描结果。您可根据扫描结果，及时处理镜像中存在的安全风险。

应用场景

云安全中心的CI/CD功能适用于以下场景。

- Jenkins-Freestyle模式
- Jenkins-Pipeline模式
- GitHub Actions

环境要求

请确保您的服务器满足最小的配置要求，以免出现镜像安全扫描过慢的情况。

- 最小配置
  - CPU：1核
  - 内存：2 GB
  - 存储：60 GB
  - 网络：可连接公网，支持访问阿里云服务（sas.aliyuncs.com）。
- 最佳配置
  - CPU：4核
  - 内存：8 GB
  - 存储：100 GB
  - 网络：可连接公网，上行带宽大于10 Mbps，支持访问阿里云服务（sas.aliyuncs.com）。

4.3.2. 接入配置

在Jenkins或者GitHub中集成云安全中心的镜像安全扫描插件时，需要填写云安全中心的CI/CD插件的Token和阿里云账号或RAM用户的AccessKey。本文为您介绍如何创建CI/CD插件并获取接入Token，以及创建云安全中心镜像安全扫描专用的RAM用户。

获取接入Token

1. 登录云安全中心控制台，在左侧导航栏，单击**资产中心**。
2. 在**资产中心**的**容器**页签下，单击**CI/CD**，然后单击**接入配置**。
3. 在**接入配置**面板，单击**新增token**，输入插件名称（长度不超过64个字符），然后单击**确定**。
   新增的插件会显示在**接入配置**面板的插件列表中，您可以在**Token**列查看并获取接入Token。

创建及授权RAM用户

1. 创建用于云安全中心镜像扫描的RAM用户。具体操作，请参见创建RAM用户。

   > **说明** 创建RAM用户的**访问方式**请选择为**OpenAPI调用访问**。

2. 创建用于云安全中心镜像扫描的专用权限策略。具体操作，请参见通过脚本编辑模式创建自定义权限策略。

   通过脚本编辑模式创建自定义权限策略的脚本如下：

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "yundun-sas:CreateJenkinsImageScanTask",
        "yundun-sas:ListImageAnalysisRuleProject",
        "yundun-sas:SubmitImageAnalysisOutput",
        "yundun-sas:UpdateJenkinsImageScanTaskStatus",
        "yundun-sas:UploadAnalyzerRuntimeLog",
        "yundun-sas:CreateBatchUploadURL"
      ],
      "Resource": "*"
    }
  ]
}
```

3. 为新增的RAM用户授予新建的权限策略。具体操作，请参见为RAM用户授权。

4.3.3. Jenkins-Freestyle模式集成

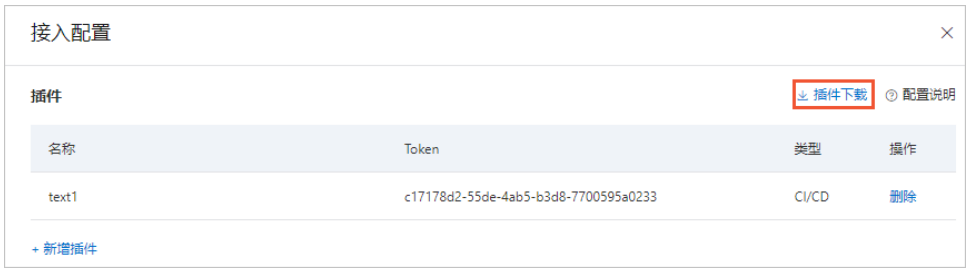
将云安全中心的CI/CD插件与Jenkins-Freestyle模式集成，云安全中心会在您进行项目构建的同时，启动镜像安全扫描任务。本文为您介绍如何将云安全中心的CI/CD插件与Jenkins-Freestyle模式集成。

Jenkins版本限制

请确保您使用的是Jenkins（1.625.3）及以上版本。

下载插件

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**页签下，单击**CI/CD**。
5. 单击**接入配置**。
6. 在**接入配置**面板上，单击右上角的**插件下载**。



云安全中心的CI/CD插件会以HPI格式下载到本地。下载的插件名称为**sas-jenkins-plugin**。

集成插件

1. 登录Jenkins工具。
2. 在左侧导航栏，单击**系统管理**。
3. 在**管理Jenkins**页面，单击**插件管理**。
4. 在**插件管理**页面， 单击**高级**页签。
5. 在**上传插件**区域，单击**选择文件**。

   选择下载到本地的文件名称为**sas-jenkins-plugin**云安全中心CI/CD插件。
6. 单击**上传**。

> 注意 插件sas-jenkins-plugin安装完成后，需要重启Jenkins才能生效。

配置镜像安全扫描

1. 登录Jenkins工具。
2. 定位到要配置镜像安全扫描的项目，单击Jenkins-Freestyle模式的项目名称。
3. 在左侧导航栏，单击**配置**。
4. 在**构建**区域的下拉菜单中，选中**镜像安全扫描**。
5. 在镜像安全扫描区域进行配置，完成云安全中心CI/CD插件与Jenkins-Freestyle模式的集成。

   配置参数说明如下：

参数	说明
准入ID	填写阿里云账号或RAM用户的AccessKey。 **说明** 建议RAM用户的AccessKey。
准入秘钥	填写阿里云账号或RAM用户的AccessKeySecret。 **说明** 建议RAM用户的AccessKeySecret。
令牌	阿里云云安全中心CI/CD插件的接入Token。获取CI/CD接入Token的具体操作，请参见接入配置。
镜像ID/仓库标签	输入您要执行镜像安全扫描的镜像的ID或者镜像所在仓库的标签。
域地址	此参数无需填写。
镜像仓地址	镜像仓的URL。 **注意** 扫描远程镜像仓中镜像时，此参数必填。
镜像仓登录用户名	镜像仓登录用户名。 **注意** 扫描远程镜像仓中镜像时，此参数必填。
镜像仓登录密码	镜像仓登录密码。 **注意** 扫描远程镜像仓中镜像时，此参数必填。

6. 单击**保存**。

集成配置完成后，您在构建项目时，会同步执行镜像安全扫描任务，扫描您项目的镜像是否存在安全风险。

后续步骤

您可以在资产中心的**容器**页签下，查看镜像安全扫描结果。具体操作，请参见查看镜像扫描结果。

4.3.4. Jenkins-Pipeline模式集成

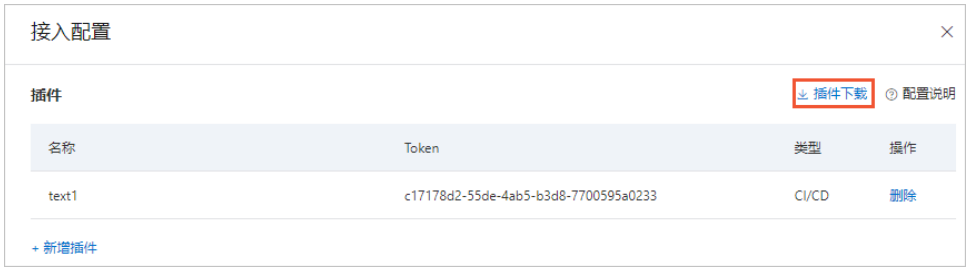
将云安全中心的CI/CD插件与Jenkins-Pipeline模式集成，云安全中心会在您进行项目构建的同时，启动镜像安全扫描任务。本文为您介绍如何将云安全中心的CI/CD插件与Jenkins-Pipeline模式集成。

Jenkins版本限制

请确保您使用的是Jenkins（1.625.3）及以上版本。

下载插件

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**页签下，单击**CI/CD**。
5. 单击**接入配置**。
6. 在**接入配置**面板上，单击右上角的**插件下载**。



云安全中心的CI/CD插件会以HPI格式下载到本地。下载的插件名称为**sas-jenkins-plugin**。

集成插件

1. 登录Jenkins工具。
2. 在左侧导航栏，单击**系统管理**。
3. 在**管理Jenkins**页面，单击**插件管理**。
4. 在**插件管理**页面， 单击**高级**页签。
5. 在**上传插件**区域，单击**选择文件**。

   选择下载到本地的文件名称为**sas-jenkins-plugin**云安全中心CI/CD插件。
6. 单击**上传**。

> 注意 插件sas-jenkins-plugin安装完成后，需要重启Jenkins才能生效。

配置镜像安全扫描

1. 登录Jenkins工具。
2. 定位到要配置镜像安全扫描的项目，单击Jenkins-Pipeline模式的项目名称。
3. 在左侧导航栏，单击**配置**。
4. 在流水线区域，完成云安全中心CI/CD插件与Jenkins-Pipeline模式集成的配置。

   以下为您提供了Jenkinsfile的声明式和脚本化的流水线语法样例，请您根据需要选择一种语法样例完成配置。

   - 脚本式Pipeline样例

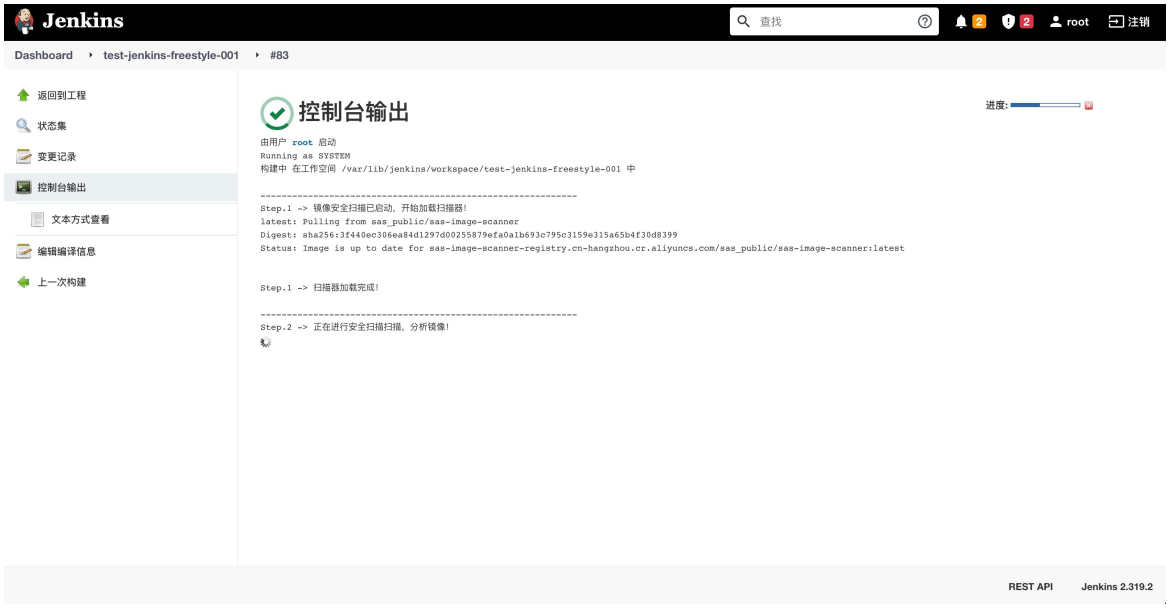
   ```
   node {
       sas(accessKeyId: '$AK', accessKeySecret: '$SK', token: '$TOKEN', imageId: '$IMAGE
   ', domain: '$DOMAIN', registryUrl: '$REGISTRY_URL', registryUsername: '$REGISTRY_USER
   NAME', registryPwd: '$REGISTRY_PWD')
   }
   ```

   - 声明式Pipeline样例

   ```
   pipeline {
       agent any
       environment {
           ACCESS_KEY_ID = '$AK'
           ACCESS_KEY_SECRET = '$SK'
           IMAGE_ID = '$IMAGE'
           TOKEN = '$TOKEN'
           DOMAIN = '$DOMAIN'
           REGISTRY_URL = null
           REGISTRY_USERNAME = null
           REGISTRY_PWD = null
       }
       stages {
           stage('Build') {
               steps {
                   sas(accessKeyId: env.ACCESS_KEY_ID, accessKeySecret: env.ACCESS_KEY_S
   ECRET, imageId: env.IMAGE_ID, token: env.TOKEN, domain: env.DOMAIN, registryUrl: env.
   REGISTRY_URL, registryUsername: env.REGISTRY_USERNAME, registryPwd: env.REGISTRY_PWD)
               }
           }
       }
   }
   ```

5. 单击**保存**。

   集成配置完成后，您在构建项目时，会同步执行镜像安全扫描任务，扫描您项目的镜像是否存在安全风险。



后续步骤

您可以在资产中心的**容器**页签下，查看镜像安全扫描结果。具体操作，请参见查看镜像扫描结果。

4.3.5. GitHub Actions集成

云安全中心提供的CI/CD插件支持对GitHub中构建的镜像进行自动化安全扫描。使用该功能前，您需要在GitHub中集成CI/CD插件。本文为您介绍如何将云安全中心的CI/CD插件集成到GitHub。

操作步骤

1. 登录GitHub。
2. 单击右上角头像，在下来菜单中选中**Your repositories**。
3. 在**repositories**页签下，单击您要集成CI/CD插件的**repository**。
4. 单击**Actions**页签。
5. 在All workflows列表中，定位到要集成CI/CD插件的workflows流水线文件，单击其**Actor**列的...。
6. 在下拉菜单中，选择**View workflow file**。
7. 在**Workflow file for this run**中按照以下样例进行集成配置。

```
name: Docker build and scan security issue by sas-image-scanner
on:
  push:
    branches: [ main ]
  pull_request:
    branches: [ main ]
env:
  REPO_TAG: your_docker_image_repo:your_docker_image_tag
jobs:
  build:
    runs-on: ubuntu-latest
    steps:
    - uses: actions/checkout@v2
    - name: Build the Docker image
      run: docker build . --file Dockerfile --tag ${{ env.REPO_TAG }}
    - name: Scan image by sas-image-scanner
      run: >
          docker run --rm -v /var/run/docker.sock:/var/run/docker.sock --network=host
          sas-image-scanner-registry.cn-hangzhou.cr.aliyuncs.com/sas_public/sas-image-s
canner:latest
          --accessKeyId=${{ secrets.ACCESSKEYID }} --accessKeySecret=${{ secrets.ACCESS
KEYSECRET }}
          --token=${{ secrets.SAS_TOKEN }} --imageId=${{ env.REPO_TAG }}
```

相关配置参数说明如下：

参数	是否必填	参数说明
accessKeyId	是	建议通过GitHub的secrets变量注入阿里云账号或RAM用户的AccessKey。 **注意** 强烈建议使用RAM用户的AccessKey。阿里云账号的AccessKey是您访问阿里云API的密钥，具有账户的完全权限，请您妥善保管并且不要以任何方式公开到外部渠道，避免被他人利用造成安全威胁。建议您遵循阿里云安全最佳实践，使用RAM用户的AccessKey进行API调用。
accessKeySecret	是	建议通过GitHub的secrets变量注入阿里云账号或RAM用户的AccessKey Secret。 **注意** 强烈建议使用RAM用户的AccessKey Secret。阿里云账号的AccessKey是您访问阿里云API的密钥，具有账户的完全权限，请您妥善保管并且不要以任何方式公开到外部渠道，避免被他人利用造成安全威胁。建议您遵循阿里云安全最佳实践，使用RAM用户的AccessKey进行API调用。
token	是	阿里云云安全中心CI/CD插件的接入Token。获取CI/CD接入Token的具体操作，请参见接入配置。

参数	是否必填	参数说明
imageId	是	待扫描镜像标识。默认支持本地扫描。 ○ 本地镜像支持传入ImageId或Repo:Tag。 ○ 远程镜像需传入RegistryUrl或Repo:Tag，并需填写镜像仓凭证。 注意 如果要扫描远程镜像仓中的镜像，您需要正确填写远程镜像的RegistryUrl、RegistryUsername、RegistryPassword的这三个参数。
domain	否	云安全中心接入点。请填写：sas.aliyuncs.com。
registryUrl	否	镜像仓的URL。 注意 扫描远程镜像仓中的镜像时，此参数必填。
registryUsername	否	镜像仓登录用户名。 注意 扫描远程镜像仓中镜像时，此参数必填。
registryPwd	否	镜像仓登录密码。 注意 扫描远程镜像仓中镜像时，此参数必填。

集成配置完成后，您在构建项目时，会自动同步执行镜像安全扫描任务，扫描您项目的镜像是否存在安全风险。

后续步骤

您可以在资产中心的**容器**页签下，查看镜像安全扫描结果。具体操作，请参见查看镜像扫描结果。

4.3.6. 查看镜像扫描结果

在Jenkins和GitHub中集成云安全中心CI/CD插件（云安全中心镜像安全扫描插件）之后，云安全中心可帮助您在项目构建阶段发现镜像中存在的安全风险，请您及时查看扫描结果，并根据云安全中心提供修复建议处理镜像中存在的安全风险。本文介绍如何查看镜像安全扫描结果。

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**页签下，单击**CI/CD**。
5. 在CI/CD插件列表中，单击目标CI/CD插件**操作**列的**查看**。

6. 在**容器**页签下的镜像列表中查看按照镜像扫描的结果。

   您可以在容器镜像列表中查看最近扫描的镜像，可以使用镜像ID或者镜像标签搜索目标镜像。

7. 定位到需要处理安全风险的镜像，单击其**操作**列的**处理**，进入镜像详情页面。
   - 在镜像详情页面，您可以查看该镜像中存在的安全漏洞，包括镜像**系统漏洞**、**镜像应用漏洞**、**镜像基线检查**和**镜像恶意样本**信息。在漏洞列表左上角，您可以通过漏洞修复**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**查看**，查看该漏洞影响资产、修复命令和影响说明信息。

5.查看网站信息

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，并支持对网站进行安全体检和查看安全报告。本文介绍如何查看网站对应资产的风险状态和网站安全报告。

操作步骤

1. 登录云安全中心控制台，在左侧导航栏，单击**资产中心**。
2. 在**资产中心**的**网站**页签下，查看网站信息。
   - **查看网站对应资产的风险状态和告警数量**
     - 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**。
     - 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，请参见查看服务器信息。
       - 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**

     a. 在**安全体检**区域，单击**立即体检**。

b. 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。

- **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。

  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：被篡改为涉恐涉政等不良信息、防止网站被恶意注入外链等）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

6.查看云产品信息

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。本文介绍如何通过筛选功能定位查看目标云产品安全状态。

操作步骤

1. 登录云安全中心控制台，在左侧导航栏，单击**资产中心**。
2. 在**资产中心**的**云产品**页签下，查看云产品信息。
   - **根据资产状态筛选云产品**
     - 在页面左侧的**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。
     - 您可以单击**存在风险的云产品**，查看对应云产品的信息。

     单击需要查看的云产品名称或**操作**列的**查看**或**修复**，可查看目标云产品的详细信息。
   - **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**

     单击对应资产类型，可以查看对应资产类型的云产品数量以及云产品的详细信息。
   - **根据标签项进行筛选**

     在**标签**区域，查看标签对应资产数量。单击已添加的标签项，查看对应标签下云产品信息。
   - **多筛选查看**

     您可在云产品列表上方搜索栏中，选择识别类型（**公网IP**、**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：
     >
     > - 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**，才能显示对应的检查信息。

     例如，在识别类型下拉框中，选择**地域 > 华东1（杭州）**，然后再次选择**地域 > 华北1（青岛）**，设置检索项之间的关系为**OR**，即可筛选显示这两个地域的所有资产。

     对于已应用的筛选项组合，您可以单击右侧**保存**，在**保存条件**对话框为该筛选条件命名，然后单击**确定**，将其保存为常用筛选条件。后续筛选资产时，您可在常用搜索条件下拉框中直接使用该搜索条件。

7.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。更多信息请参见解绑非阿里云服务器。

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
>
> -
> - 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。