阿里云
云安全中心（态势感知）

资产管理

文档版本：20190906

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

1 资产中心

云安全中心提供资产管理功能，可帮助您全面了解云安全中心已防护服务器和云产品的安全状态。

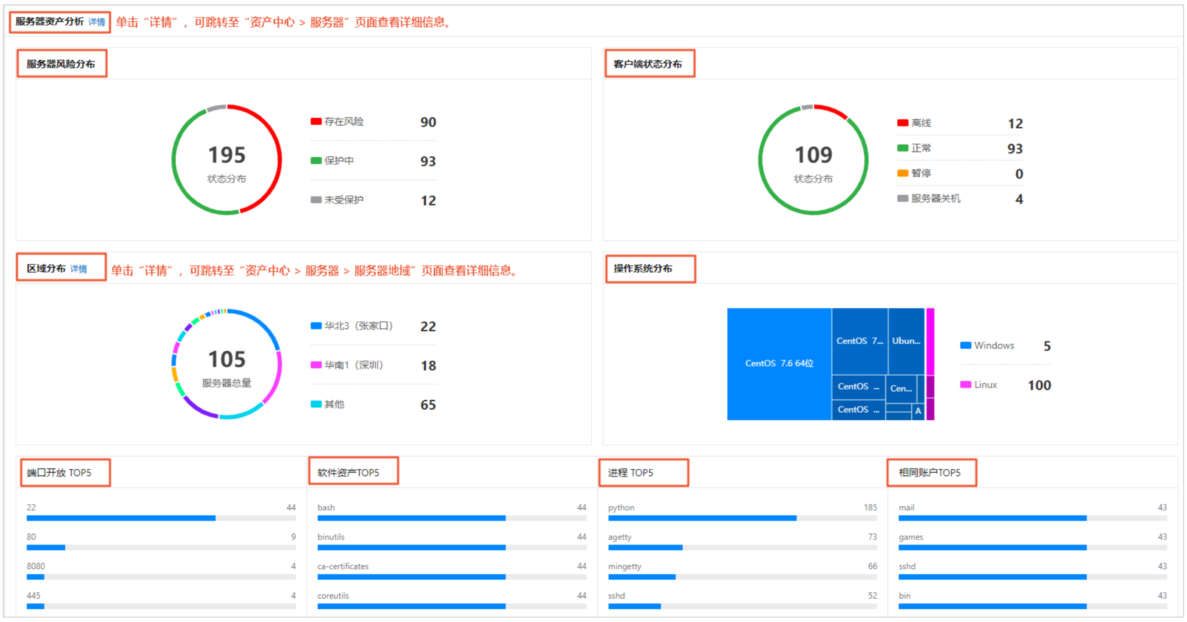
为便于对资产进行安全管控，资产中心提供了资产分组和标签分类功能。您可以将资产分组，以组别的维度查看安全事件；也可以通过资产标签筛选具有相同属性的资产。

总览

云安全中心的总览页面，提供以下资产分析信息。

- 保有资产分析：展示云上资产分布和资产安全状态分布。

- 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。



- **云产品风险分布：展示云产品安全资产数量，和存在风险资产数量。**

2 查看服务器安全状态

本文档介绍如何通过筛选功能定位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。

背景信息

云安全中心的资产中心的服务器页面为您提供了所有服务器的安全状态信息。

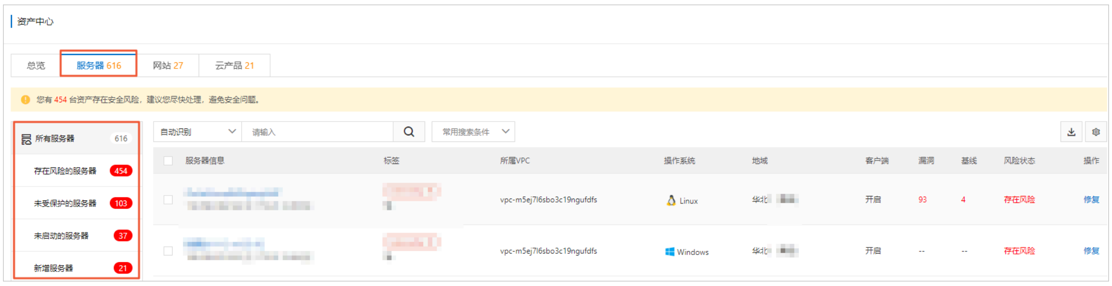
操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击资产中心，然后选择服务器子页面。

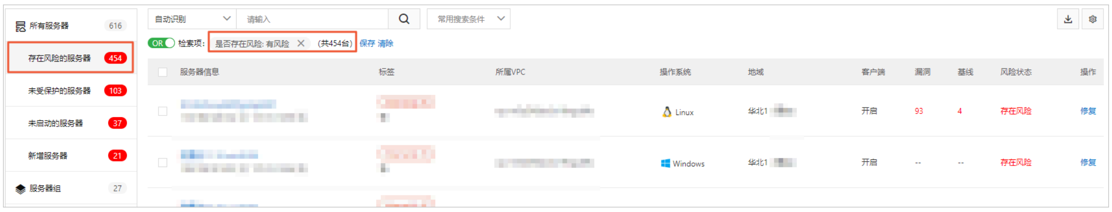
3. 在服务器页面，您可以根据需要执行以下步骤，通过不同的筛选功能，查看服务器安全状态，并设置显示列和常用搜索条件。

   · 根据服务器状态进行筛选

     - 在所有资产功能项，您可以查看所有资产数量、存在风险的资产数量、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。



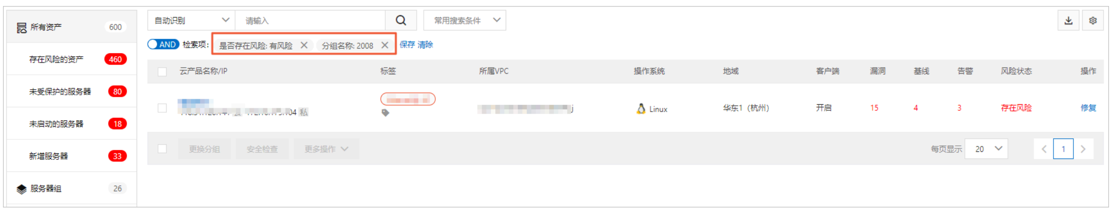
     - 单击存在风险的资产、未受保护的服务器、未启动的服务器或新增服务器，查看对应服务器的安全状态。



   · 根据服务器分组进行筛选

     - 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。

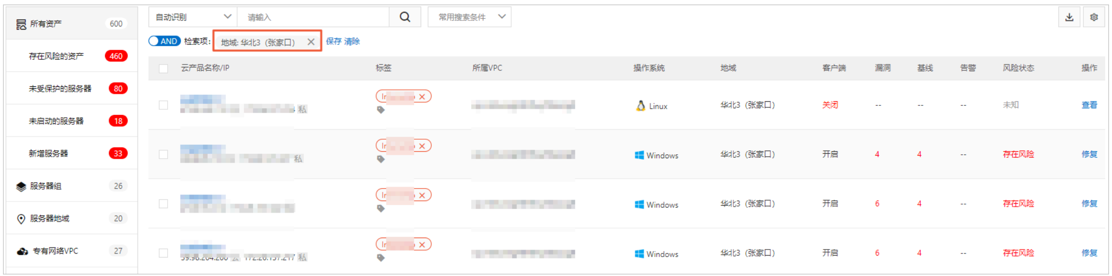
     - 单击某分组下包含服务器数量、存在风险数量或未保护数量，查看某分组下服务器安全状态。例如，单击服务器组为18的存在风险数量下的数字，显示检查项为是否存在风险：有风险和分组名称：18下的服务器安全状态。



   · 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。

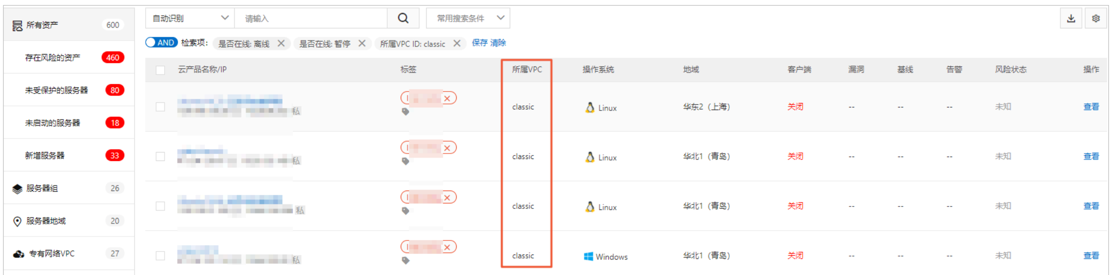
- 单击某地域下包含服务器数量、存在风险数量或未保护数量，查看某地域下服务器安全状态。例如，单击服务器地域为华北3（张家口）的包含服务器数量下的数字，显示检查项为地域：华北3（张家口）下的服务器安全状态。



· 根据专有网络VPC实例ID进行筛选

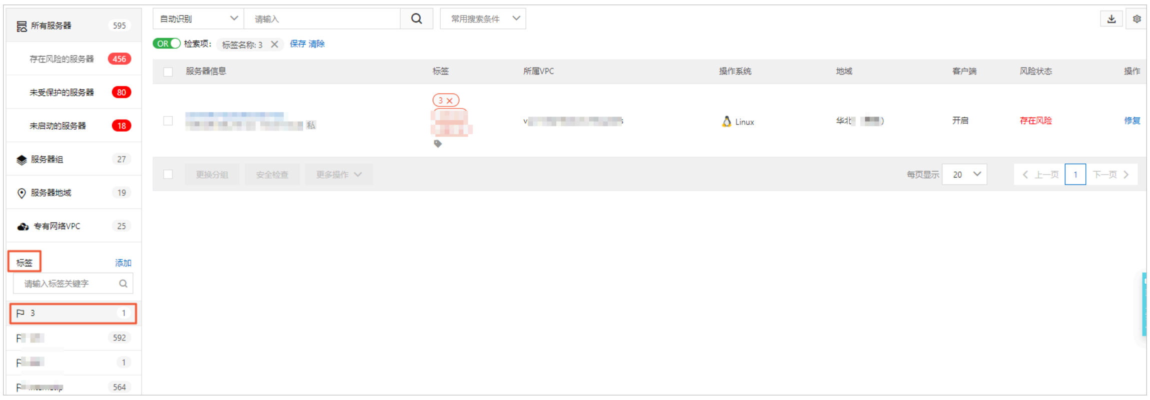
- 单击专有网络VPC，您可以查看专有网络VPC数量及各VPC下的包含服务器数量、服务器存在风险数量和未保护数量。

- 单击某专有网络VPC下包含服务器数量、存在风险数量或未保护数量，查看某VPC下服务器安全状态。例如，单击专有网络VPC为classic的未保护数量下的数字，显示检查项为所属VPC ID：classic下的服务器安全状态。



- **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**

  使用所有资产、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。

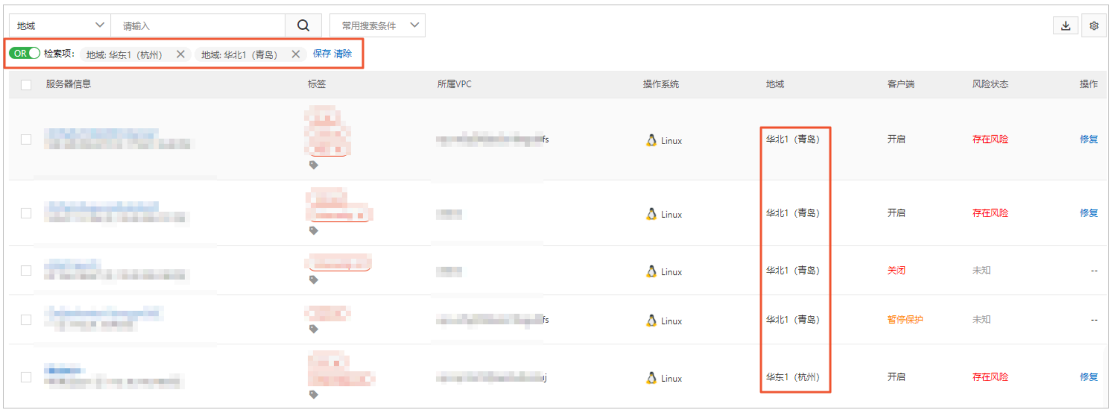
  - **展示多个筛选子项结果：**

    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:**
    >
    > - 检查项之间的关系：
    >   - AND：检查项之间是与关系。
    >   - OR：检查项之间是或关系。
    > - 展示多个筛选子项结果，需要选择检查项之间的关系为OR。

■ 需要输入指定信息搜索的检查项，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。



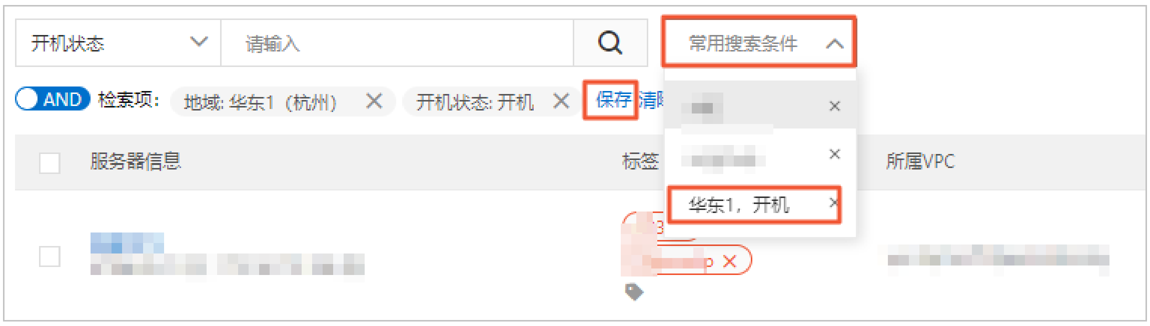
- 展示跨筛选项组合结果：

同时应用多个筛选项。例如，勾选地域并选择华东1后，勾选开机状态并选择开机状态：开机，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条件框中直接选用该筛选条件。



- 设置显示列

单击资产中心页右上角的设置列按钮，可以设置需要显示的列内容。

3 查看网站安全状态

本文档介绍如何查看网站对应资产的风险状态和告警数量。

背景信息

云安全中心的资产中心的网站页面为您提供了所有网站信息，及网站对应资产的信息。您可以查看各网站下资产的风险状态和告警数量。

操作步骤

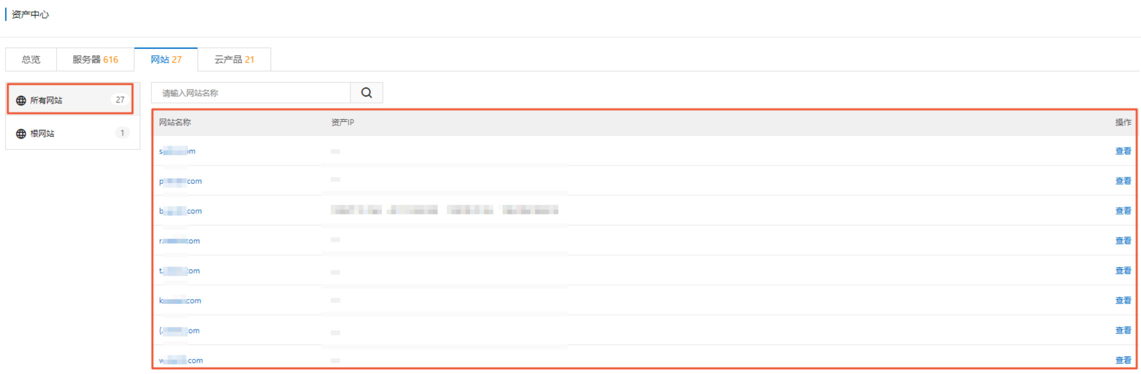
1. 登录云安全中心控制台。
2. 在左侧导航栏，单击资产中心，然后选择网站子页面。

3. 在网站页面，您可以根据需要执行以下操作，查看网站信息。

- 您可以查看所有网站和根网站数量。

- 查看所有网站及对应资产

  单击网站列表左侧筛选功能项所有网站，您可以查看到所有网站，及网站对应的资产IP信息。



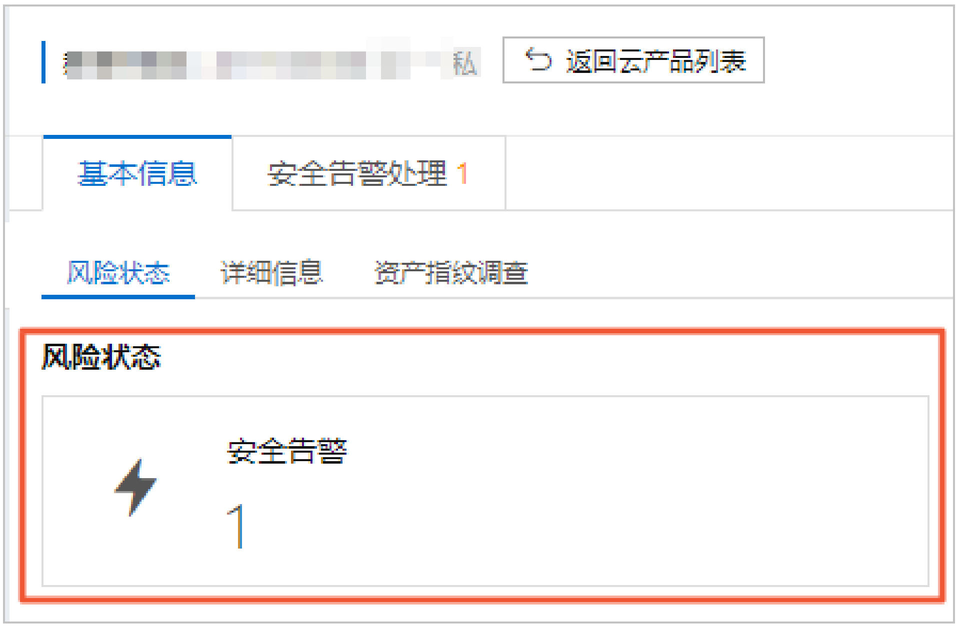
- 查看根网站及对应资产

  单击网站列表左侧筛选功能项根网站，您可以查看到所有根网站，及根网站对应的资产IP信息。

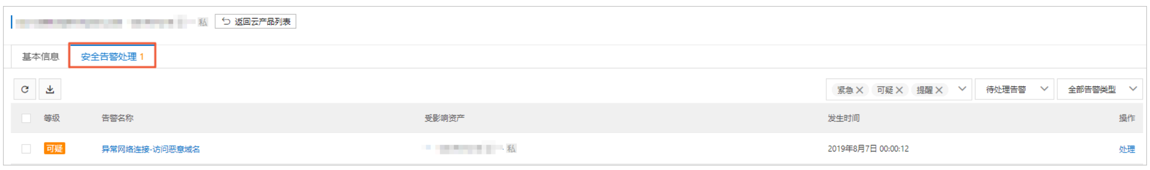
4. 您可以根据需要执行以下步骤，查看网站对应服务器风险状态和告警数量。

   在所有网站或根网站页面，单击网站列表中目标网站的网站名称，或右侧操作下的查看，打开网站列表。

   - 您可以查看到网站的域名、根域名和相关资产信息（资产名称/IP、资产类型和告警数量）。
   - 您可以单击目标资产名称，打开资产列表详情，查看资产基本信息中的风险状态。更多功能管理请参见管理单个资产。



   - 您可以单击目标资产告警列的数字，打开资产列表，查看具体告警信息。告警处理方法请参见#unique_7。



4 查看云产品安全状态

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。

背景信息

云安全中心的资产中心的云产品页面为您提供了所有云产品的安全状态信息。

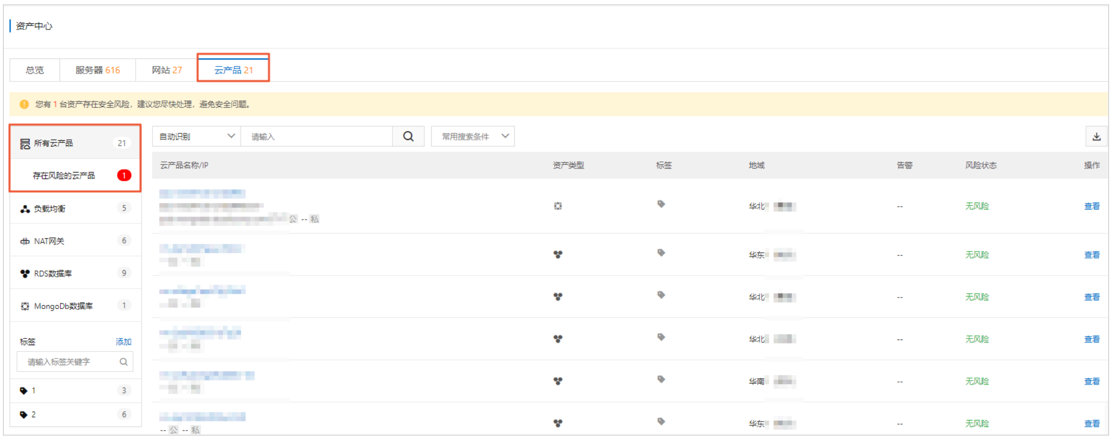
操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击资产中心，然后选择云产品子页面。

3. 在云产品页面，您可以根据需要执行以下步骤，通过不同的筛选功能，查看云产品安全状态，并设置常用搜索条件。

· 根据资产状态进行筛选

- 在所有资产功能项，您可以查看所有资产数量和存在风险的资产数量，查看所有云产品安全状态。

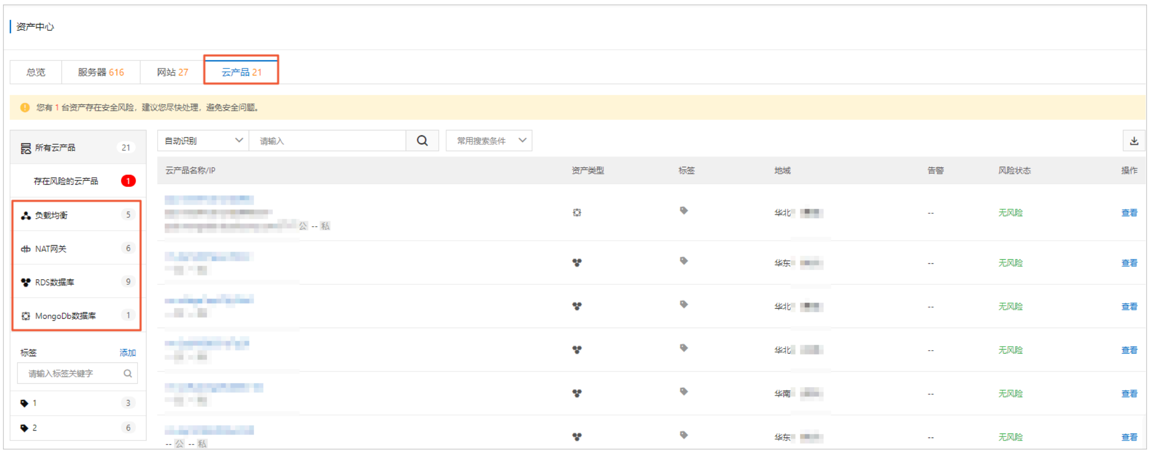


- 您可以单击存在风险的资产，查看对应云产品的安全状态。

· 根据资产类型进行筛选

云产品资产类型分为以下4种：

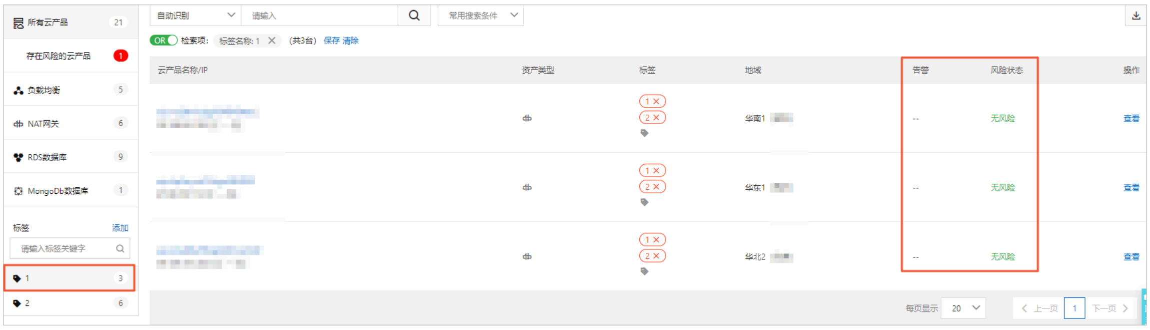
- 负载均衡
- NAT网关
- RDS数据库
- MongoDb数据库



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，查看对应标签下服务器的安全状态。



- 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：

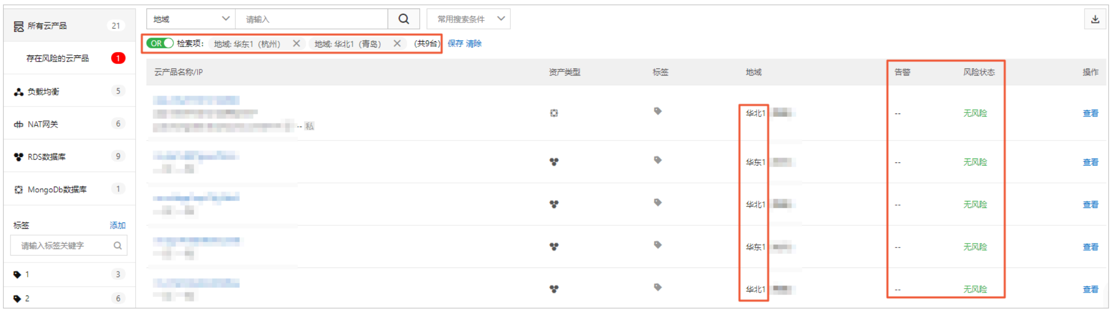
    您可以在资产中心列表上方搜索栏，选择识别类型（公网IP、实例名称、实例ID、是否有安全告警、是否存在风险、标签名称、分组名称、地域），并选择或输入指定类型信息，筛选出指定的资产。

    说明：

    - 检查项之间的关系：
      - AND：检查项之间是与关系。
      - OR：检查项之间是或关系。
    - 展示多个筛选子项结果，需要选择检查项之间的关系为OR。

■ 需要输入指定信息搜索的检查项，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，勾选地域并选择华东1后，勾选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。

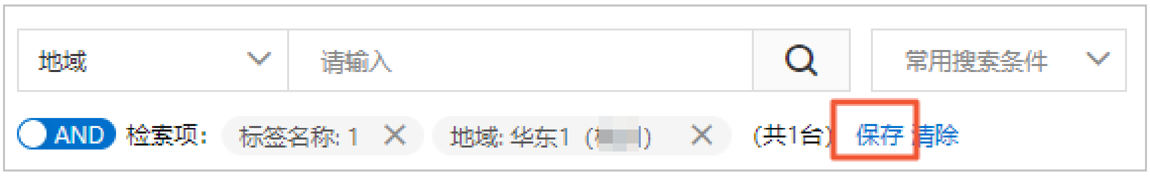
说明:

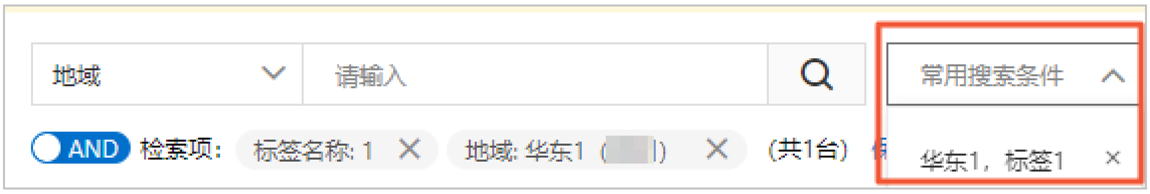
- 您也可以在选择负载均衡、NAT网关、RDS数据库、MongoDb数据库或标签功能检查后，通过资产中心列表上方搜索栏，筛选出更多指定的资产。

- 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用该筛选条件。





5 开启和关闭服务器保护状态

本文档介绍如何管理资产的保护状态。

背景信息

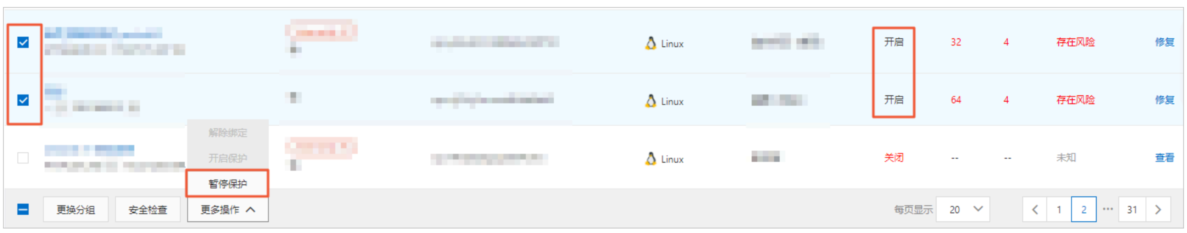
安装云安全中心Agent后才可为您的服务器提供安全防护。安装Agent后，您可在资产中心页面查看到服务器的客户端实时防护状态为开启。

开启服务器保护

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击资产中心，然后选择服务器子页面。
3. 在服务器页面中，勾选一个或多个客户端实时防护状态为关闭的目标服务器，并单击资产中心下方的更多操作 > 开启保护。

关闭服务器保护

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击资产中心，然后选择服务器子页面。
3. 在服务器页面中，勾选一个或多个客户端实时防护状态为开启的目标服务器，并单击资产中心下方的更多操作 > 暂停保护。



6 一键安全检查

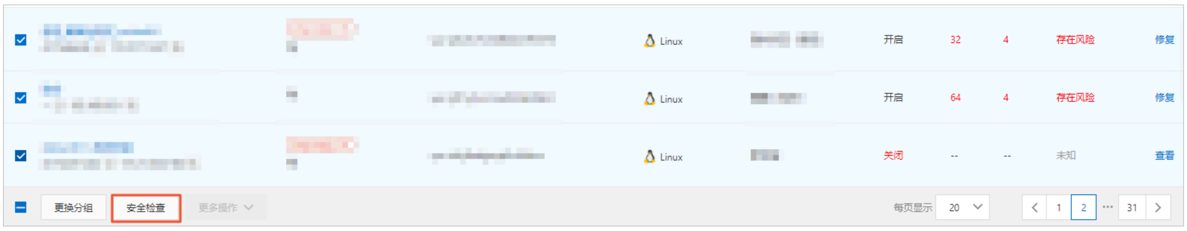
本文档介绍云安全中心下资产中心的安全检查功能。

背景信息

在资产中心页面使用安全检查功能，可以对指定服务器立即执行安全扫描，更新其漏洞信息、基线配置风险信息、及资产指纹信息。

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，然后选择服务器子页面。
3. 在服务器页面中，勾选一个或多个目标服务器。
4. 单击列表下方的安全检查。



5. 在安全检查对话框中，勾选需要执行的检查项目。

6. 单击确认，执行检查。

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对应页面。

7 管理资产分组

本文介绍了服务器分组管理功能。

添加分组

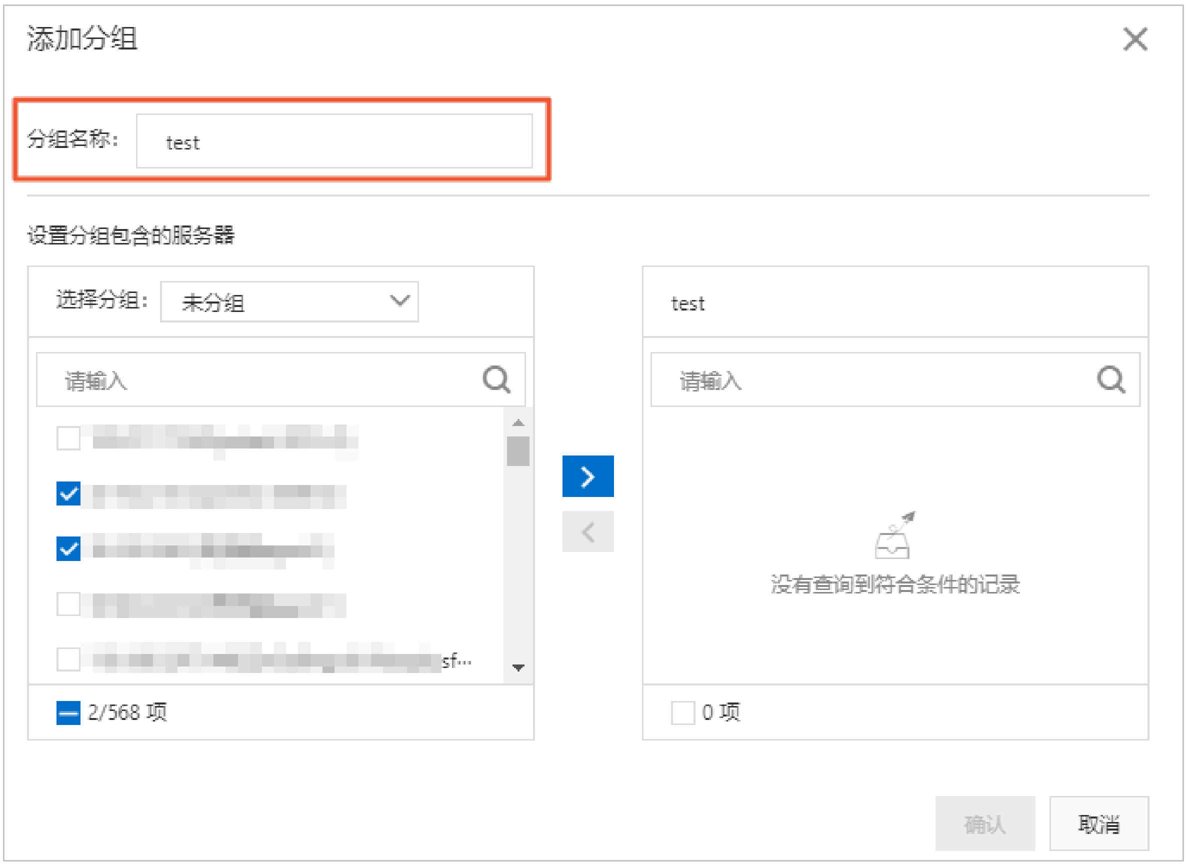
如果您的账号在资产中心下存在多台资产，为方便您快速定位到多个对象或对多个对象执行批量操作，建议您使用分组功能为同类型的资产创建一个分组。

您可以参照以下步骤，创建资产分组：

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击资产中心，然后选择服务器子页面。
3. 在服务器页面，单击服务器组，进入服务器组列表页。

> **说明:**
> 未进行资产分组时，所有的资产都在未分组中。

4. 单击添加分组，打开添加分组对话框。



5. 输入分组名称。
6. 添加资产到创建的新分组。

   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新分组中。

   在选择分组选择未分组或一个已分组，勾选分组下资产，单击向右箭头，添加到创建的新分组中。
7. 单击确认。

管理和删除分组

如果需要对某个分组进行管理（例如：为分组命名或修改分组下的服务器）或删除，可参见以下步骤：

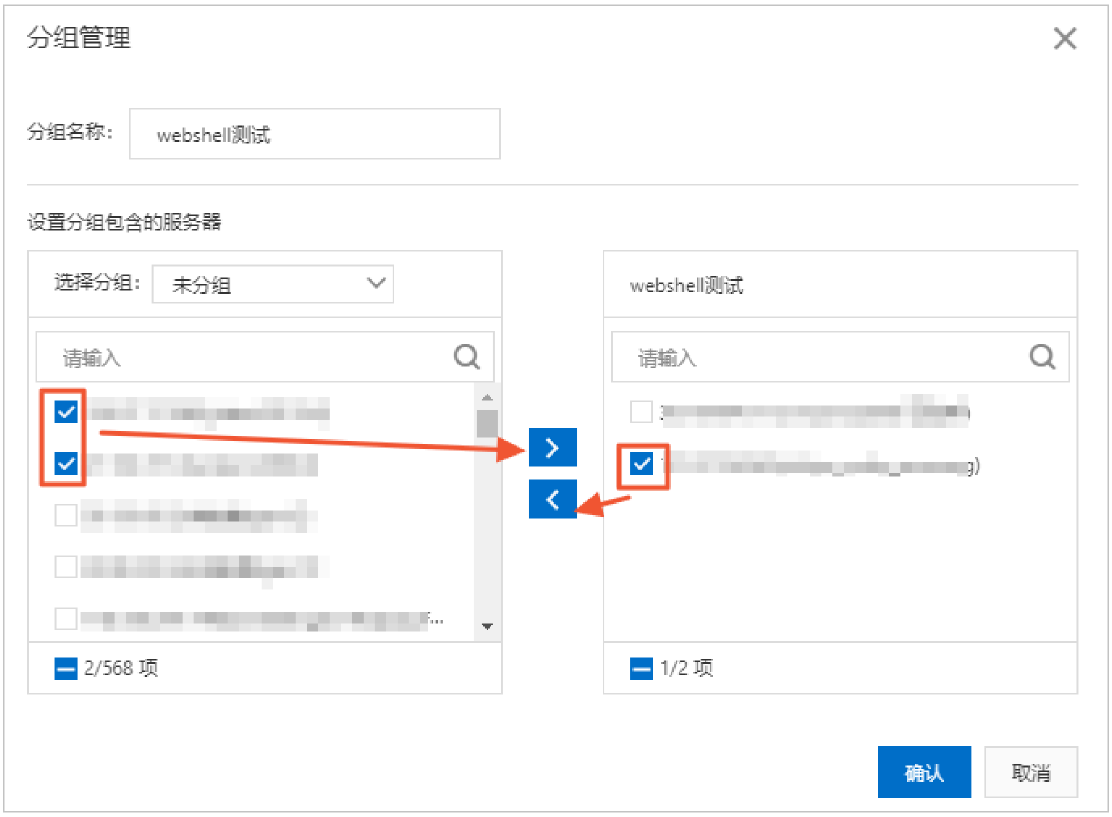
1. 登录云安全中心控制台。
2. 在左侧导航栏，单击资产中心，然后选择服务器子页面。

3. 在服务器页面，单击服务器组，进入服务器组列表页。执行以下操作管理或删除分组。

- 管理分组

  a. 单击未分组或一个已分组右侧操作列下的管理，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，在右侧指定分组下选择资产，单击左向箭头，添加到已选分组中，或在左侧已选分组下选择资产，单击右向箭头，添加到指定分组中。



  c. 单击确认，完成服务器分组。

- 删除分组

  您可以单击一个分组右侧操作列下的删除，然后单击确认，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。

8 管理资产标签

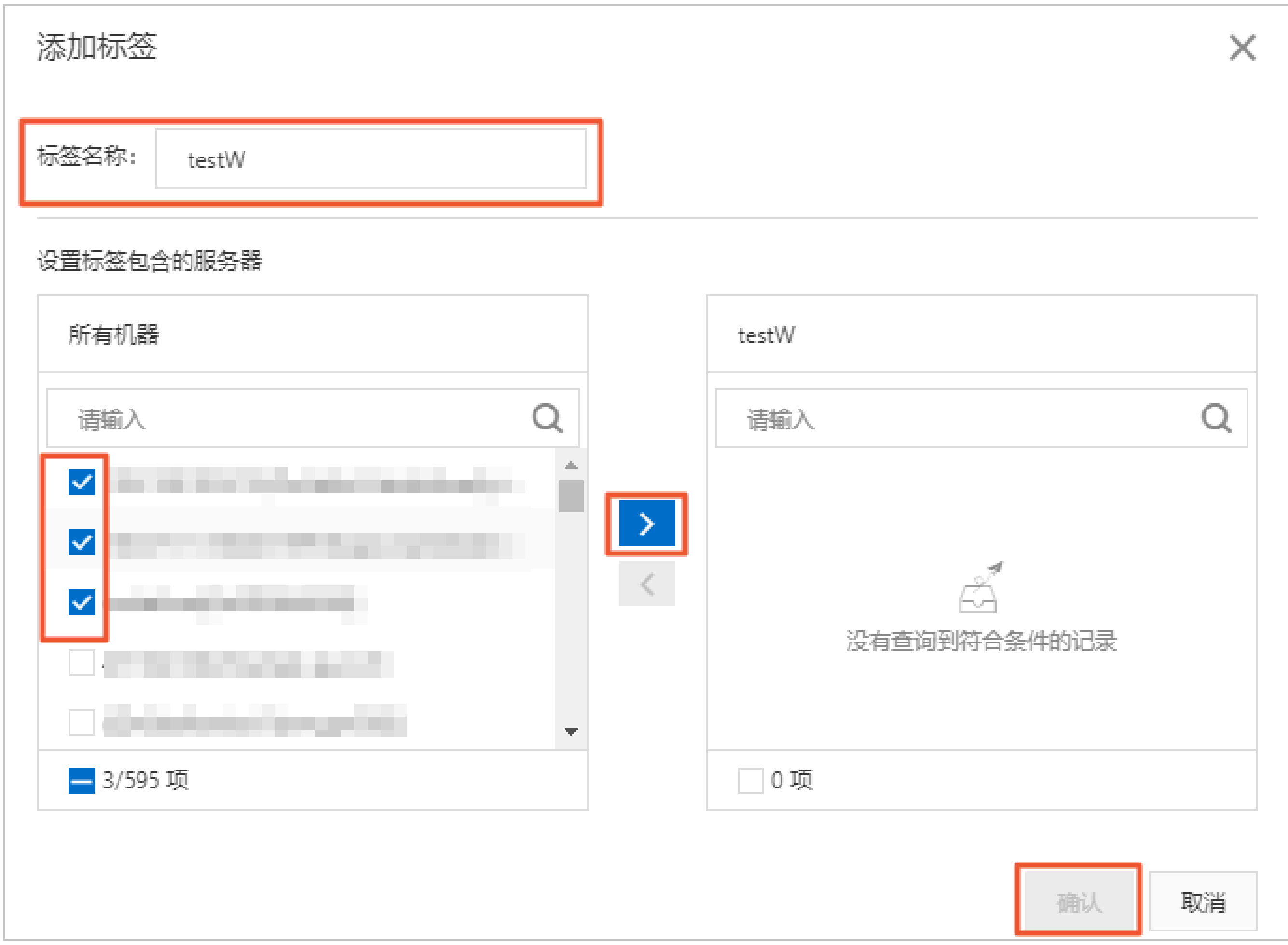
本文介绍了服务器和云产品的标签管理功能。

背景信息

为资产添加标签能够标识其特殊属性，也可用于筛选具有相同属性的资产。

添加标签

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。
4. 在添加标签对话框中输入标签名，并在左侧选择资产服务器，单击向右箭头，将资产添加至已创建的标签。



5. 单击确认，完成添加。

   您可以在资产列表，单击目标资产标签栏的添加标签按钮，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。

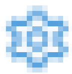
管理和删除标签

如果需要对某个标签进行管理（例如：为标签命名或修改标签所属的服务器）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。

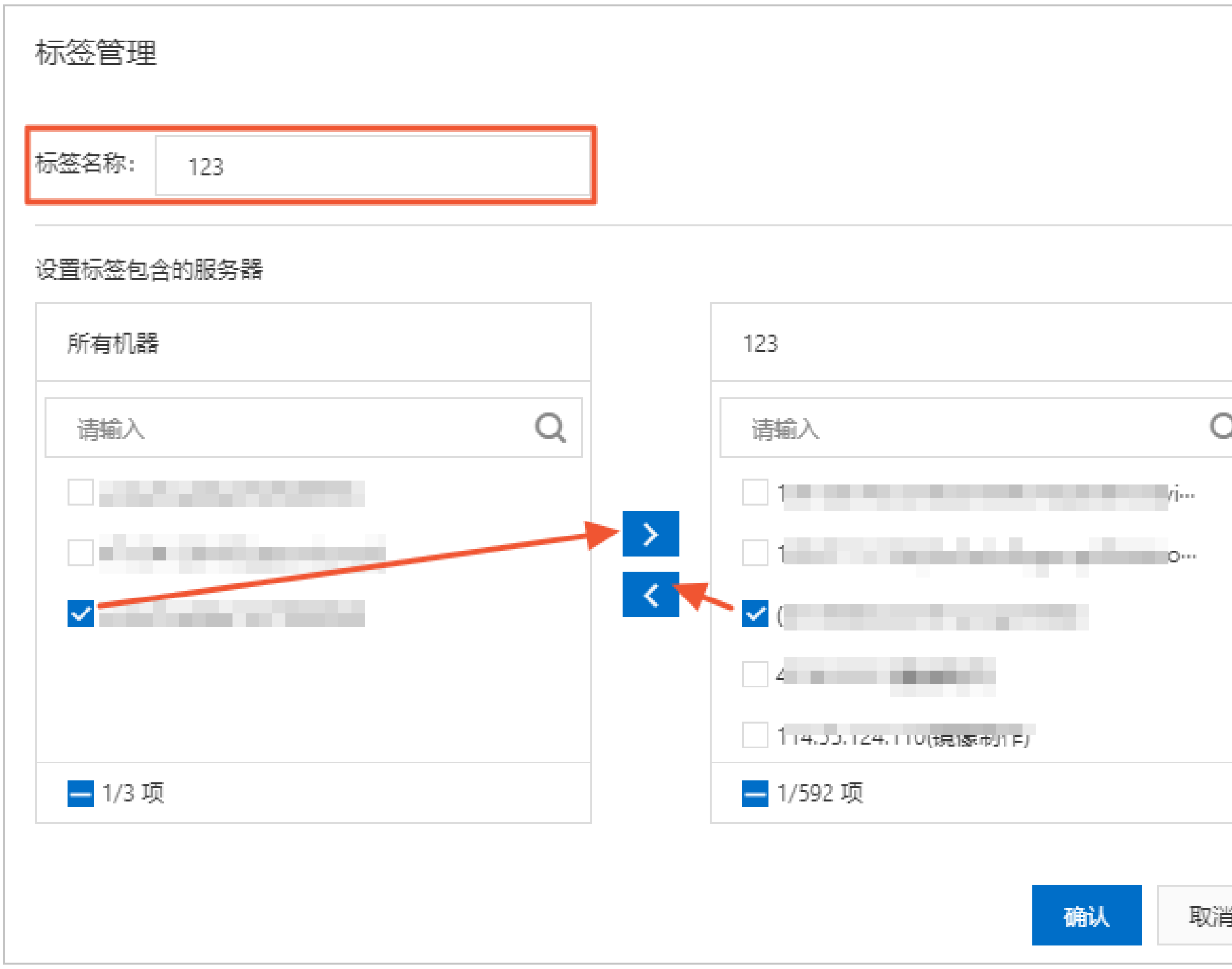
3. 在服务器或云产品页面，执行以下操作管理或删除标签。

- 管理标签

  a. 如果需要管理单个标签，可将鼠标移动至该标签栏中，单击显示的标签管理按钮  ，打开标签管理对话框。

  b. 您可以在标签管理对话框，修改标签名称，添加或删除标签下的服务器。

  c. 单击确认，完成标签管理。

- 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，单击显示的删除按钮 ，并单击确认，可删除标签。

9 删除非阿里云机器

本文档介绍如何删除非阿里云机器。

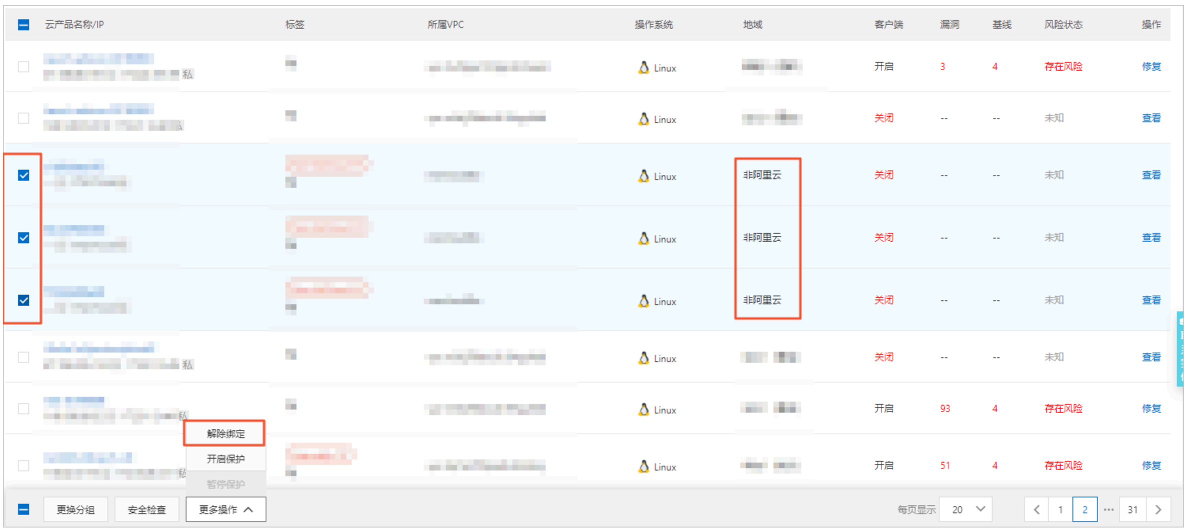
背景信息

如果您不希望云安全中心继续防护您的非阿里云主机，您可以在资产列表中对该非阿里云主机解除绑定。 解除绑定非阿里云主机后，该主机的Agent将被自动卸载，并且云安全中心将不会再对该主机提供安全防护。

> **说明:**
> 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。

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，然后选择服务器子页面。
3. 在资产列表中，勾选一个或多个非阿里云服务器。
4. 单击资产列表下方的更多操作 > 解除绑定。



5. 单击确认，系统会自动卸载安装在您服务器上的Agent插件，并将目标服务器从资产列表中移除。

10 管理单个资产

本文介绍了如何管理单个服务器或云产品。

背景信息

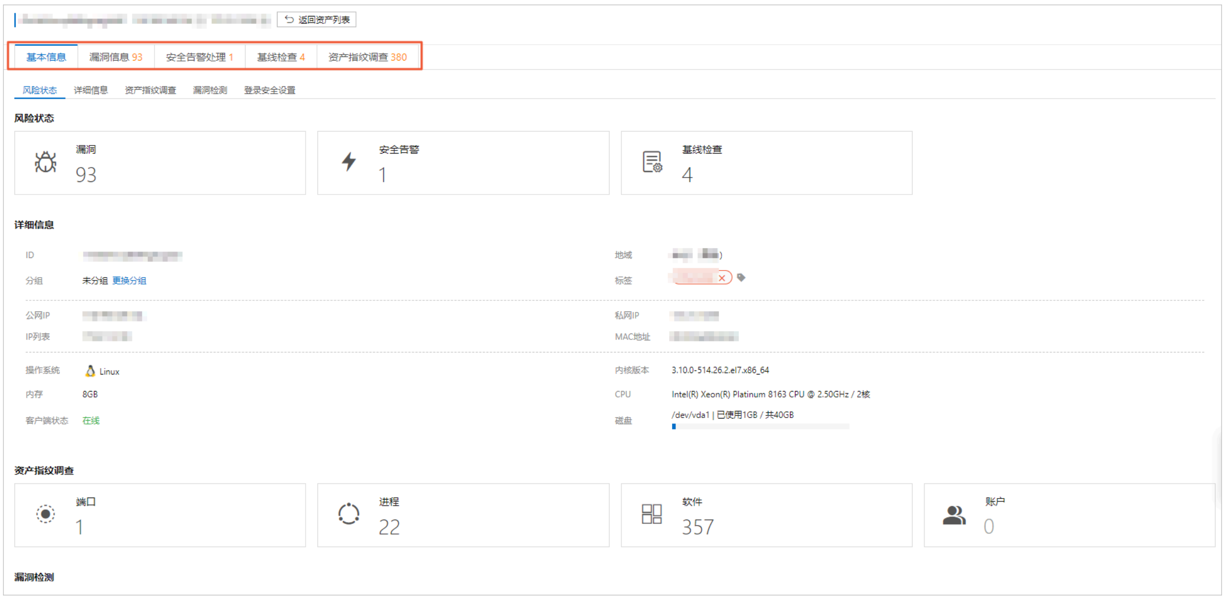
云安全中心的资产中心页面，提供了所有资产的基本信息。根据资产类型不同，对服务器和云产品提供的管理功能是不同的。

步骤一：定位目标资产

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、网站或云产品页面，定位并单击目标资产名称，进入目标资产页面。

步骤二：管理目标资产

在资产信息页面，您可以查看到资产的基本信息、漏洞信息、安全告警处理、基线检查和资产指纹调查。



- 基本信息

  您可以在基本信息页面，查看和管理资产相关信息。

  - 风险状态：您可以查看漏洞、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。

> **说明:**
> 云产品仅支持查看安全告警信息。

  - 详细信息：您可以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

> **说明:**

该功能应用于服务器资产，云产品不支持。

您可以单击更换分组，在更换分组对话框，选择新的分组，并单击确认。

- 管理标签：您可以单击 ，在添加标签对话框，选择标签并单击确认。

您可以单击已有标签右侧的删除按钮 ，删除资产所属标签。

- 资产指纹调查

您可以在此页面，查看到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。

- SQL注入威胁检测（Beta）

说明:

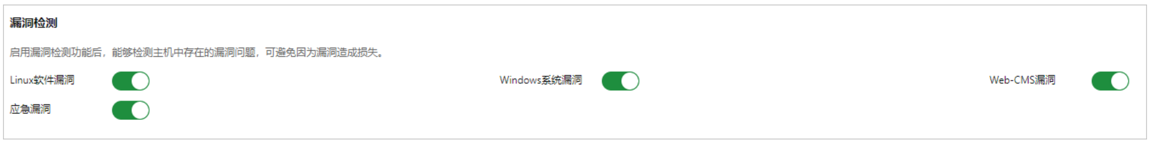
该功能仅应用于RDS数据库云产品。

您可以在此页面查看RDS SQL注入威胁检测的统计结果，具体请参见#unique_14。

- 漏洞检测：

> **说明：**
> 该功能应用于服务器资产，云产品不支持。

您可以在漏洞检测页面，设置该资产的漏洞检测项开启或关闭。



- 登录安全设置：

> **说明：**
> 该功能应用于服务器资产，云产品不支持。

您可以在登录安全设置页面，设置常用登录地和高级登录（IP、时间、账号）报警功能。

您可以开启/关闭非合法登录（IP、时间、账号）报警功能，并为目标资产添加合法登录的IP、时间和账号。

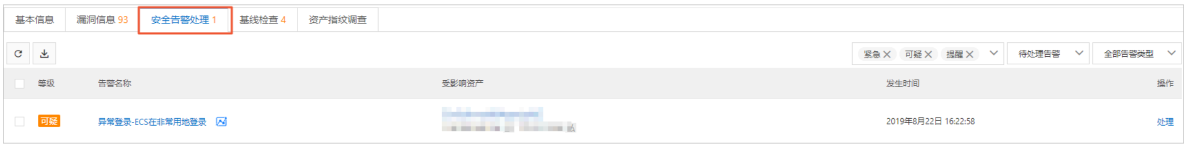
- 漏洞信息：

> **说明：**
> 该功能应用于服务器资产，云产品不支持。

您可以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

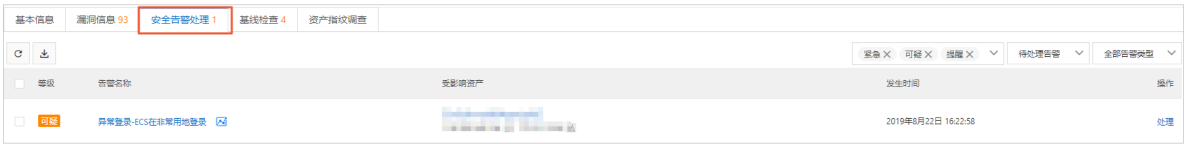
您可以查看目标资产下安全告警检测结果，具体处理方法请参见#unique_7。



- 基线检查：

> **说明：**
> 该功能应用于服务器资产，云产品不支持。

您可以查看目标资产下基线检查结果，具体处理方法请参见#unique_16。



- 资产指纹调查：

> **说明：**
> 该功能应用于服务器资产，云产品不支持。

您可以查看目标资产下指纹（端口、进程、软件、账户）调查统计信息。更多信息请参见#unique_17。