ALIBABA CLOUD

Alibaba Cloud

云安全中心（态势感知）

安全运营

文档版本：20220505

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.安全报告 05
2.任务中心 07
2.1. 任务中心概述 07
2.2. 创建任务 07
2.3. 查看任务详情 10
3.容器签名 13
4.多账号安全管控 15

1.安全报告

云安全中心支持安全报告功能。您可通过创建安全报告，定时向您的邮箱发送资产安全报告，及时掌握资产的安全状况数据。本文介绍如何创建安全报告。

版本限制说明

仅高级版、企业版、旗舰版支持该功能，其他版本用户需要升级到高级版、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。各版本支持的功能详情，请参见功能特性。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全运营 > 安全报告**。
3. 在**安全报告**页面，单击**创建新报告**。

   注意　除默认已创建的安全日报，最多支持创建9个安全报告。

4. 在**添加报告**页面，配置安全报告的基本信息。

   安全报告相关配置项说明如下：

参数	说明
报告名称	设置安全报告的名称。
报告类型	选择创建报告的类型，取值： ○ **日报** ○ **周报** ○ **月报** ○ **自定义周期** 选择该项后，您需要在**统计周期**中设置该自定义安全报告统计的周期。
报告发送时间	设置报告发送的**开始时间**和**结束时间**。 **说明**　报告发送的开始时间和结束时间的最小间隔为2小时。
统计周期	设置报告的统计周期。仅报告类型为**自定义周期**时需设置该配置项。可设置的统计周期的时间范围为最近一个月。
选择语言	选择报告内容的语言，可选**简体中文**或**English**。
报告邮件接收人	设置接收报告的邮箱地址。使用Enter键可输入多个邮箱地址。 **说明**　邮箱需要经过验证，未经过验证的邮箱需要按照邮件指引完成激活。

5. 单击**下一步**，进入报告详情页面。
6. 在在报告详情页左侧，选中需要在报告中展示的数据。

   可以选择**安全运营**、**资产**、**告警**、**漏洞**、**基线**、**攻击**相关的统计数据。
7. 单击**保存报告内容**，完成报告的创建。
   您可在**安全报告**页面查看到您新建的报告。报告完成创建后，默认为启用状态。云安全中心会在您设置的**报告发送时间**内，向您添加的报告邮箱地址中发送该安全报告。

相关操作

在**安全报告**页面，您可对目标报告根据需要执行以下操作：

- **立即发送报告**

  自定义周期的安全报告，您可单击**立即发送**，发送自定义周期内的安全报告内容至报告邮件收件人。

  > **说明** 日报、周报和月报不支持立即发送功能。

- **关闭报告的发送**

  报告完成创建后，默认启用。云安全中心会在您设置的**报告发送时间**内，向您添加的报告邮箱地址中发送该安全报告。如果您后续不再需要接收该报告，可在该报告区域单击 图标，关闭该报告的发送。

- **编辑、克隆或删除报告**

  支持对已创建的报告进行编辑、克隆和删除。

  - 单击**编辑**，可修改报告的基础信息和报告内容。

    > **说明** 云安全中心默认创建的安全报告的**报告类型**为**日报**，修改该安全报告的基础信息时不支持修改其**报告类型**。

  - 单击**克隆**，可新增一个和此配置相同的报告。
  - 单击**删除**，可删除该报告。报告删除后不可恢复，请您谨慎操作。

    > **说明** 云安全中心默认创建安全报告不支持删除。

- **导出报告**

  单击**导出**，可以导出该安全报告的HTML文件。

2.任务中心

2.1. 任务中心概述

任务中心提供自动化响应编排能力，将安全事件响应过程中重复性的任务逻辑编排成自动化处置策略，帮助您高效地进行系统安全加固。您创建自动化任务后，任务中心会在您选择的资产上自动化批量执行该任务。本文介绍了任务中心的策略模板和任务管理等模块提供的功能。

背景信息

目前，任务中心仅支持创建漏洞自动化修复任务。

版本限制说明

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。各版本的功能详情，请参见功能特性。

策略模板

策略模板页签展示了云安全中心提供的**漏洞自动化批量修复策略**模板。该策略支持多主机、自动化批量修复漏洞。在该页签下，您可以基于已有模板快速创建策略。在**操作**列单击**添加到我的策略**，可以创建一个新的策略并将该策略添加到**我的策略**页签中。

我的策略

我的策略页签展示了所有已创建的自动化策略的信息，包括策略名称、类型、执行模式、创建时间、最近更新时间。在该页面，您可以在已有策略模板下创建任务。更多信息，请参见创建任务。

任务管理

任务管理页签展示了所有已创建任务的信息，包括任务名称、执行数、执行模式、创建时间、完成时间和进程状态。在该页签下，您可以查看已有任务的详情。更多信息，请参见查看任务详情。

2.2. 创建任务

任务中心可根据您添加的策略模板来快速创建自动化任务。创建任务后，该任务会在设置的任务执行时间开始时，对已选择的服务器资产自动化批量执行漏洞修复，帮助您提高系统安全加固的效率。本文介绍如何创建任务。

前提条件

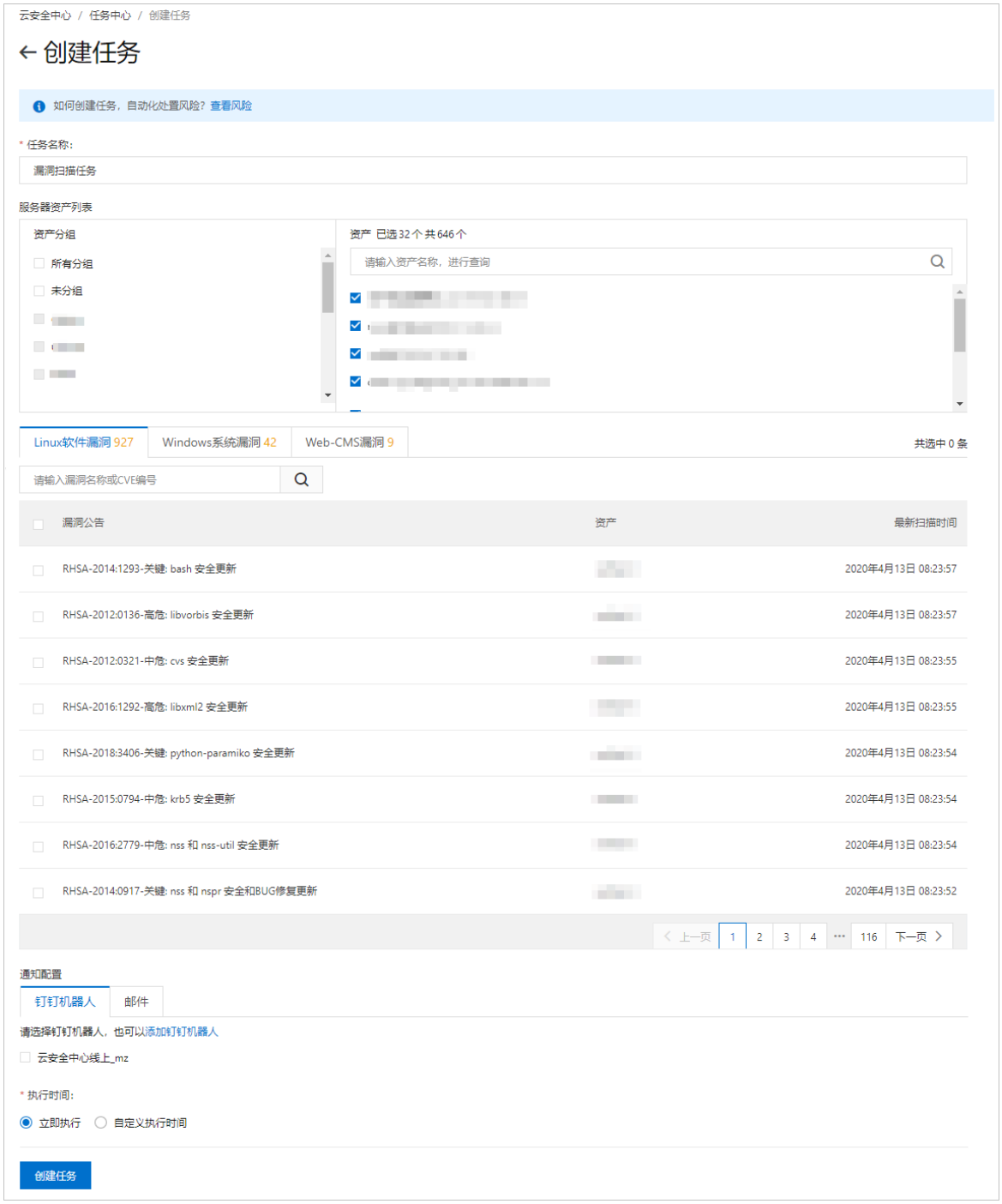
已购买或升级至云安全中心企业版、旗舰版。具体操作，请参见购买云安全中心和升级与降配。各版本支持的功能详情，请参见功能特性。

背景信息

任务中心的批量漏洞修复任务支持修复Linux漏洞、Windows漏洞和Web-CMS漏洞。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全运营 > 任务中心**。
3. 在**任务中心**页面，单击**我的策略**页签。
4. 在**我的策略**页面，定位到需要创建任务的策略，单击**操作**列**创建任务**。
5. 在**创建任务**页面，参考以下表格完成任务配置。



配置项	说明
任务名称	填写任务名称。

配置项	说明
服务器资产列表	支持选中单台资产、跨组选中多台资产或者选中资产分组。执行以下操作选择需要执行当前任务的资产： ○ 在**服务器资产列表**中，选中**资产分组**模块中的分组，自动选中该分组下的所有资产。您可在右侧**资产**模块下，对已自动选中的资产取消选中。 ○ 在**资产**模块下输入资产名称（支持模糊查询），单击搜索框的搜索按钮后会为您展示相关资产，您可选中需要执行自动化处理任务的资产。 **说明** 自动化任务仅处理在**资产**模块中选中的资产。
漏洞列表	漏洞列表展示了您在资产列表中已选择的资产中存在的漏洞。选择需要修复的漏洞。您可以单击**Linux软件漏洞**、**Windows系统漏洞**或**Web-CMS漏洞**页签，选择相应类型漏洞。 **说明** 您最多可以选择200个需要修复的漏洞。
通知配置	支持**钉钉机器人**和**邮件**两种通知方式。系统在任务执行完成后，通过您配置的通知方式向您发送通知。以下是通知方式的配置方法： ○ **钉钉机器人**：选中需要发送通知的钉钉机器人。您也可单击**添加钉钉机器人**添加新的钉钉机器人。添加钉钉机器人的操作步骤，请参见配置钉钉机器人通知。 ○ **邮件**：输入您的邮箱地址。如果有多个邮箱地址请使用英文逗号（,）隔开。
执行时间	自动化任务执行的时间支持选择以下方式： ○ **立即执行**：创建任务后，设置的任务将立即被调度并自动执行。 ○ **自定义执行时间**：设置任务调度的**起始时间**和**结束时间**。创建任务后，任务将在设置的**自定义执行时间**（即补丁维护窗口）内进行调度并自动执行。

6. 单击**创建任务**。
   创建任务时，如果**执行时间**选择**立即执行**，任务创建完成后进程状态将为**进行中**；如果**执行时间**选择**自定义执行时间**，任务创建完成后进程状态将为**等待中**。

   说明 支持取消进程状态为**等待中**的任务。您可以单击需要取消的任务操作列的**取消**，取消该任务。

执行结果

创建任务成功后，系统会提示**创建成功**，并自动跳转到**任务管理**页面。

后续步骤

任务执行完成后，您可在**任务管理**页面查看该任务详情。查看任务详情的操作步骤，请参见查看任务详情。

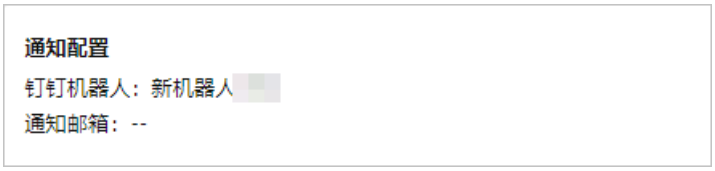
2.3. 查看任务详情

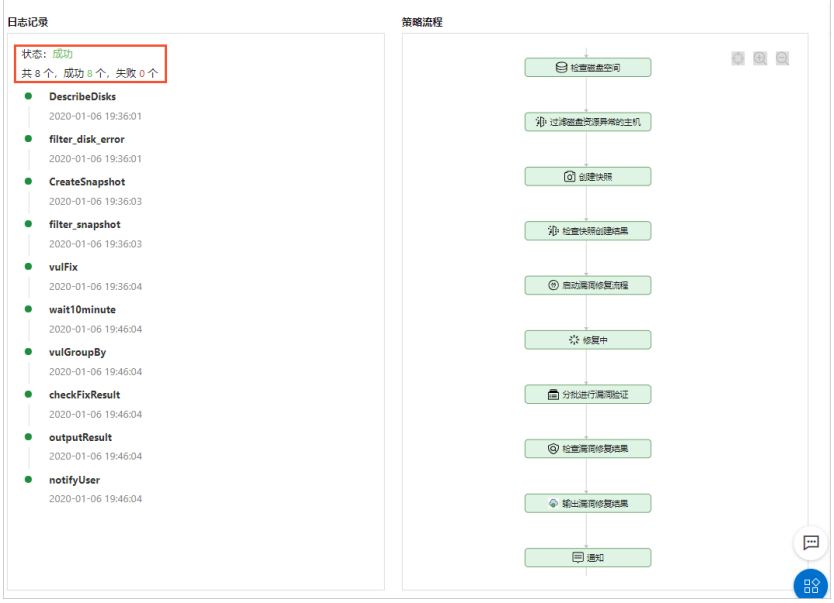
成功创建任务后，通过查看任务详情，您可以查看该任务的服务器资产列表、通知配置和其他信息。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全运营 > 任务中心**。
3. 在**任务中心**页面，单击**任务管理**页签。
4. 在任务列表中，单击目标任务操作栏的**详情**。
5. 在任务详情页面，查看**服务器资产列表**、**通知配置**和**其他**信息。

   单击**服务器资产列表**、**通知配置**或**其他**页签可快速定位到对应模块。各模块的详细说明如下表所示。

模块	说明
服务器资产列表	展示当前漏洞修复任务相关的**资产**、**漏洞名称**和**最新扫描时间**。
通知配置	当前任务的通知方式，包含**钉钉机器人**和**邮件**的详细配置。 

模块	说明
其他	当前任务执行的**日志记录**和**策略流程**信息。 ○ **日志记录**：记录任务执行的状态、进程总数、失败/成功进程数和各步骤执行的详细情况。 ○ **策略流程**：批量修复漏洞任务的流程图。 

3.容器签名

容器签名可实现对容器镜像的可信签名，确保只允许部署您认可的容器镜像，防止未经签名授权的镜像启动，从根本上帮助您提升资产的安全性。

前提条件

使用容器签名功能前，您需要先完成以下操作：

- 已创建了非对称加密算法的KMS密钥。

  有关创建KMS密钥的详细内容，请参见创建密钥。

  > **注意** 由于非对称密钥算法才支持容器签名功能，创建KMS密钥时，**密钥类型**必须选择*RSA_2048*，**密钥用途**必须选择*SIGN/VERIFY*。关于KMS密钥算法的详细内容，请参见KMS支持的算法规格说明。

- 已创建了Kubernetes集群，并且集群已安装了kritis-validation-hook组件。

  创建Kubernetes集群的具体操作，请参见创建Kubernetes专有版集群。

  有关kritis-validation-hook组件的更多信息，请参见kritis-validation-hook组件介绍。

- 首次使用容器签名，需要先完成云资产访问授权。

版本限制说明

仅旗舰版支持该功能，其他版本用户需要升级到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。各版本的功能详情，请参见功能特性。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全运营 > 容器签名**。
3. （可选）在**容器签名 > 证明者**页签中创建证明者。

   如果您已创建过证明者，可直接进入步骤4。

   您可在**证明者**页签中单击**创建证明者**，完成配置后并单击**确定**，完成证明者的创建。

   创建证明者的配置说明如下。

参数	描述
证明者名称	配置容器签名安全策略时需要选择证明者，用于对您的目标容器进行可信授权。建议输入便于识别的名称。
选择证书	在证书列表中选择您已创建的KMS密钥。 **说明** 由于非对称密钥算法才支持容器签名功能，创建KMS密钥时，**密钥类型**必须选择*RSA_2048*，**密钥用途**必须选择*SIGN/VERIFY*。关于KMS密钥算法的详细内容，请参见KMS支持的算法规格说明。
描述	输入该证明者的备注信息。

4. 创建安全策略。

   您可在**安全策略**页签中，单击**添加策略**，完成配置后并单击**确定**，完成策略的创建。

   添加策略的配置说明如下。

参数	描述
策略名称	配置签名安全策略时需要选择证明者，用于对您的目标集群进行可信授权。 建议输入便于识别的名称。
证明者	在证明者列表中选择您已创建的证明者。 具体操作，请参见步骤3。
应用集群	单击需要进行容器签名的集群分组后，选中目标**集群命名空间**。
策略开启状态	单击开关，创建策略后策略会立即启用。 **说明** 默认不开启策略。策略如果未开启将不会生效。
备注	输入安全策略的备注信息。

后续步骤

成功创建并启用容器签名安全策略后，已开启安全策略的容器镜像会标识为**可信的镜像**。

说明 目前暂不支持展示可信标签。

4.多账号安全管控

您可以使用多账号安全管控功能，对您企业的多个云账号和资源账号进行统一管控，即实现对您企业的各个成员账号进行统一的安全防护配置，实时检测各个成员账号的安全风险状况。本文介绍如何使用多账号安全管控功能。

前提条件

- 已开通资源目录。具体操作，请参见开通资源目录。
- 已在资源目录中创建成员或邀请成员。具体操作，请参见创建成员、邀请阿里云账号加入资源目录。

背景信息

基于阿里云资源管理提供的可信服务功能，云安全中心支持将多个阿里云账号集合到一个资源目录内，通过结构化的方式对多个账号进行统一管理。

您可以通过设置企业管理账号或委派管理员账号，并将企业内其他阿里云账号添加为成员账号，实现对多个账号的集中管理。

您将企业中的某个阿里云账号设置为**委派管理员账号**后，委派管理员账号将获得所在企业管理账号的授权，并且可以获得在云安全中心中访问和管理资源目录中的组织、成员信息以及查看成员账号安全风险的权限。更多信息，请参见企业管理账号、管理委派管理员账号。

版本限制说明

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。

添加委派管理员账号

添加成员账号前，您需要先将您企业的某个阿里云账号设置为委派管理员。

1. 使用企业管理账号登录资源管理控制台。
2. 在**资源目录 > 可信服务**页面中，为云安全中心添加委派管理员账号。

   当成员账号设置为委派管理员后，该账号在指定可信服务中（即云安全中心），将作为企业管理账号执行相关管理操作。

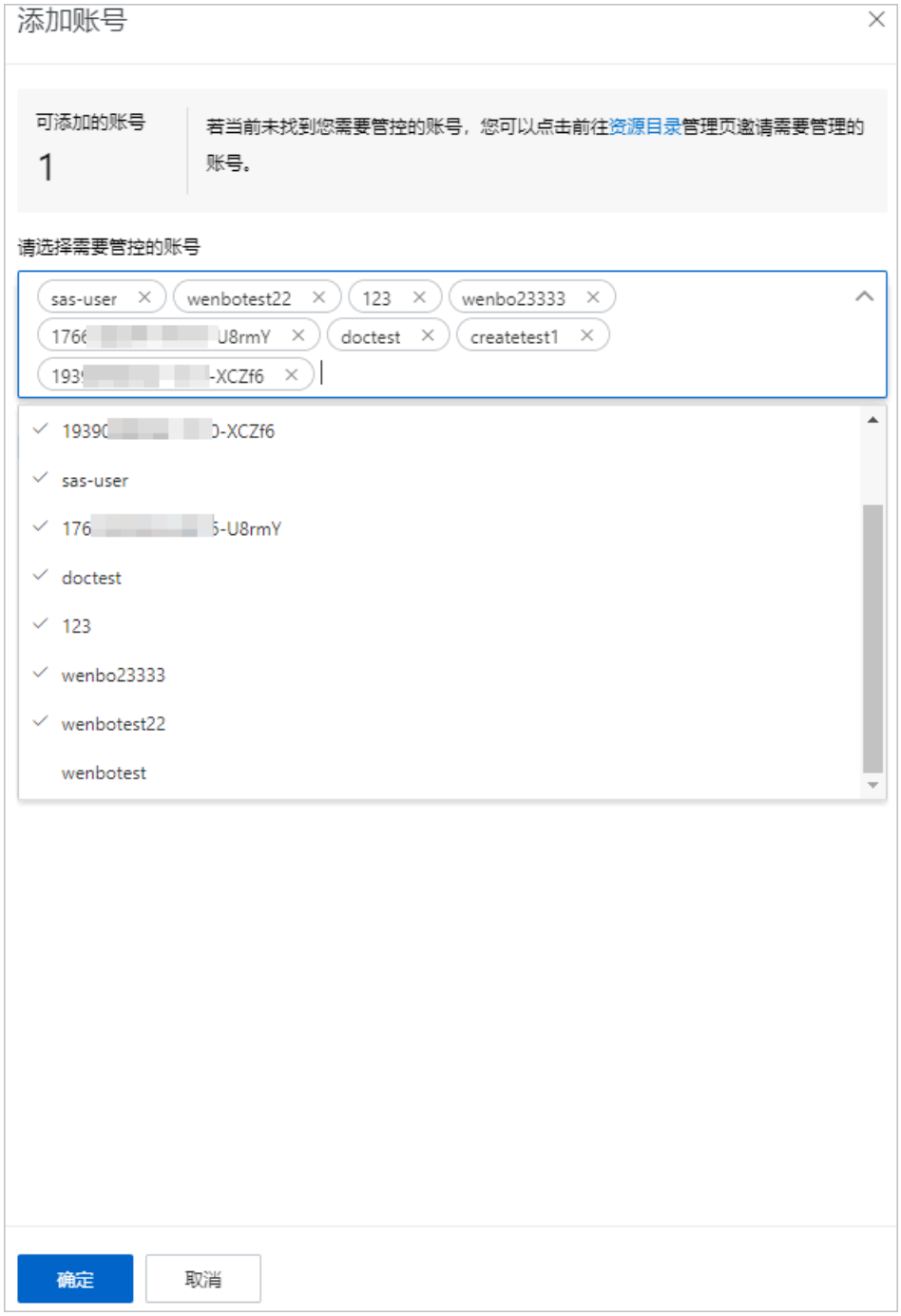
   具体操作，请参见添加委派管理员账号。

> **说明** 云安全中心最多支持添加5个委派管理员账号。

添加成员账号

您可以使用企业管理账号或委派管理员账号将需要统一管控的其他账号添加为成员账号。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全运营 > 多账号安全管控**。
3. 在**多账号安全管控**页面，单击**添加账号**。
4. 在**添加账号**面板上的**请选择需要管控的账号**下拉列表中，选择需要进行安全管控的账号。



说明 企业管理账号和委派管理员账号维护的成员账号列表为同一个列表，使用这两种账号维护成员账号列表均可达到相同的目的。

5. （可选）选择**当有新增账号时，默认添加至管控列表**，将新增的账号自动同步到成员账号列表中。
6. 单击**确定**。
   您可以在**多账号安全管控**页面的成员账号列表中查看已添加的成员账号。

成员账号安全防护配置

您无需使用成员账号登录云安全中心，通过使用企业管理账号或者委派管理员账号登录云安全中心后，即可对成员账号的客户端、漏洞扫描、基线检查策略进行统一配置。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全运营 > 多账号安全管控**。
3. 在**多账号安全管控**页面的成员账号列表中，单击成员账号**操作**列的**设置**。
4. 在**设置**面板上，为指定的成员账号配置安全防护策略。
   i. **客户端管理**

   配置项说明如下表：

配置项	说明	相关文档
主动防御	云安全中心的主动防御功能可为您自动拦截常见病毒、恶意网络连接和网站后门连接，并设置诱饵捕获勒索病毒。	主动防御
网站后门查杀	网站后门查杀功能会定期检测网站服务器、网页目录中的网站后门及木马程序。只有为服务器开启网站后门查杀后，云安全中心安全告警才会触发网站后门检测，并向您展示相关告警记录。	网站后门查杀
容器K8s威胁检测	容器K8s威胁检测功能实时为您检测正在运行的容器集群安全状态，帮助您及时发现容器集群中的安全隐患和黑客入侵行为。	容器K8s威胁检测
自适应威胁检测能力	开启自适应威胁检测功能后，如果服务器发生高危入侵事件，云安全中心会自动为您服务器的Agent开启重大活动保护模式。该模式开启所有安全防护规则和安全引擎，可以更全面地检测黑客的入侵行为。	自适应威胁检测能力
告警聚合开关	自动化告警关联分析功能帮助您自动关联同一黑客入侵活动产生的多条告警，即聚合来自同一IP、同一服务和同一个用户的恶意告警。开启该能力后，您可以一键处理具有同一类型特征的告警，提升告警处理的效率。	自动化告警关联分析
防护模式管理	云安全中心Agent是云安全中心提供的本地插件，您必须在服务器操作系统上安装云安全中心Agent插件，才能使用云安全中心提供的安全防护服务。防护模式管理功能提供多种Agent运行模式，可以满足您不同应用场景下的安全需求。	防护模式管理
客户端自保护	客户端自保护功能可以主动拦截恶意卸载云安全中心Agent的行为，保障云安全中心防御机制稳定运行。	客户端自保护
客户端引擎	客户端引擎开启后，云安全中心将仅使用端上引擎能力对网页后门、病毒进行检测，建议仅在云外主机网络受限的情况下使用。	无

   ii. 单击**下一步**。

iii. **漏洞管理**

您可通过漏洞管理设置开启或关闭不同类型漏洞的自动检测、有选择性地对指定服务器开启漏洞检测、设置漏洞扫描周期和扫描方式、对已失效漏洞设置自动删除周期。相关文档，请参见漏洞管理设置。

iv. 单击**下一步**。

v. **基线检查**

您可以使用基线检查功能配置成员账号的基线检查策略，通过执行基线检查策略来检查成员账号的资产的基线配置是否存在风险。相关文档，请参见设置基线检查策略。

5. 配置完成后，单击下方**确定**。
云安全中心将根据您的配置，开启成员账号客户端的相关功能，并根据您的配置对成员账号下拥有的资产进行漏洞扫描和基线检查。

查看成员账号的安全风险

您可以使用企业管理账号或者委派管理员账号在**多账号安全管控**页面的成员账号列表中，查看成员账号的安全风险和管理成员账号。

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**安全运营 > 多账号安全管控**。
3. 在**多账号安全管控**页面的成员账号列表中，查看成员账号的安全风险和管理成员账号。
   - 查看成员账号的安全风险

     您可以在成员账号列表中查看成员账号**安全分**、**安全告警处理**、**漏洞修复**、**基线检查**等安全风险信息。

   - 管理成员账号
     - 单击**前往查看**，跳转到**资源管理**控制台的**资源目录**页面。您可以在**资源目录**页面查看所有资产目录信息、新建成员、邀请成员、将资源账号升级为账号。
     - 单击**删除**，将该账号从成员账号列表中删除。