云安全中心

操作指南

产品文档

腾讯云

文档目录

操作指南
访问权限管理

最近更新时间：2024-08-02 10:14:18

本文档将指导您如何查看和使用云安全中心特定资源的权限，并指导您使用云安全中心控制台特定部分的策略。

操作场景

您可以通过使用访问管理（Cloud Access Management，CAM）策略，使用户拥有在云安全中心（Cloud Security Center，CSC）控制台查看和使用特定资源的权限。

SOC 的全读写策略

如果您希望用户拥有**管理**云安全中心的权限，您可以对该用户使用名称为：QcloudSSAFullAccess 的策略，该策略通过让用户对云安全中心所有资源都具有操作权限，从而达到目的。可将预设策略 QcloudSSAFullAccess 授权给用户具体操作步骤，请参见 操作步骤。

SOC 的只读策略

如果您希望用户拥有**查询**云安全中心的权限，但是不具有创建、删除、处理的权限，您可以对该用户使用名称为：QcloudSSAReadOnlyAccess 的策略，可将预设策略 QcloudSSAReadOnlyAccess 授权给用户，具体操作步骤，请参见 操作步骤。

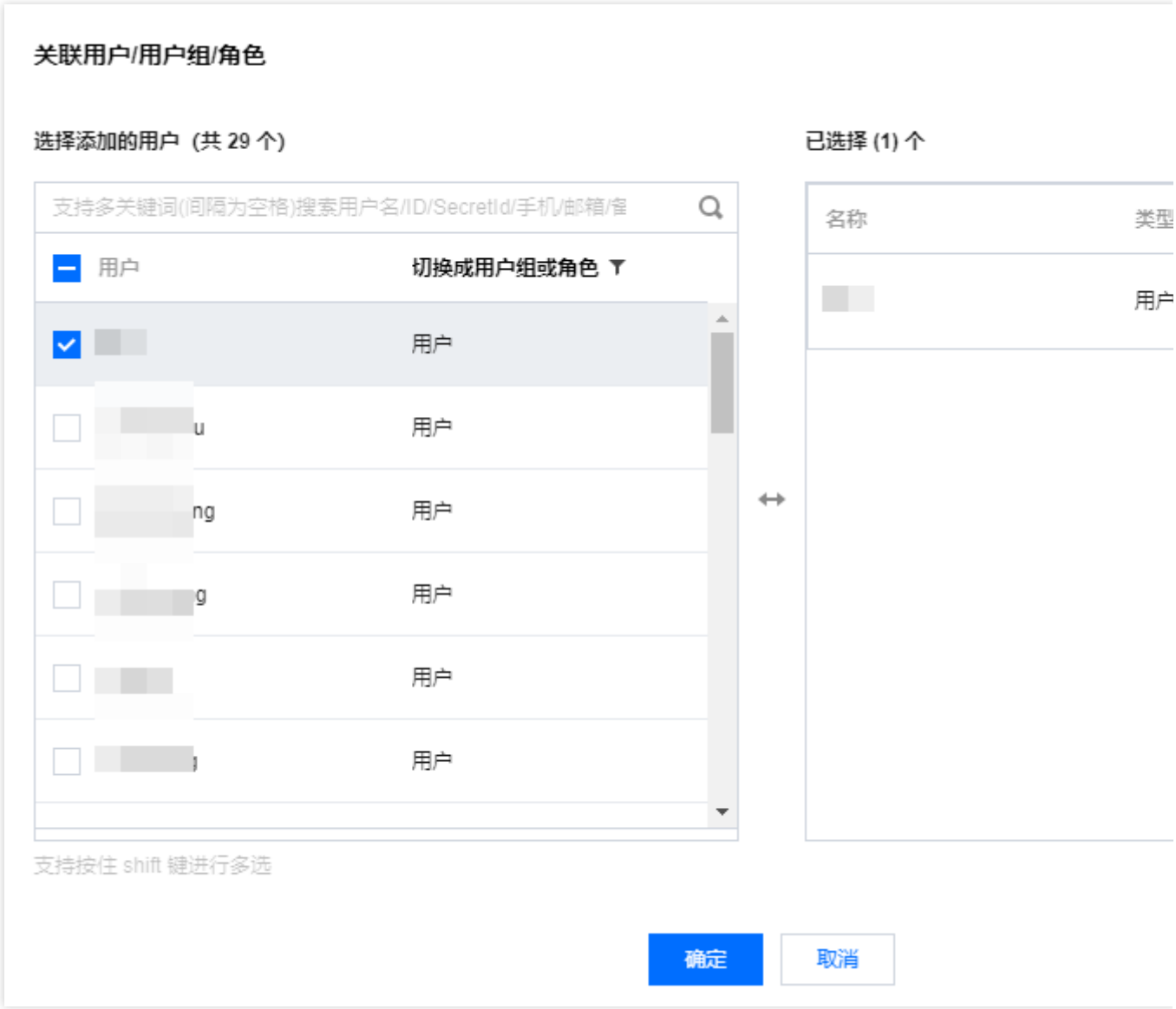
SOC 相关资源的策略

如果您希望用户拥有**使用**云安全中心云资产、合规管理、云安全配置、响应中心及 UBA 的权限，您可以对该用户使用名称为：QcloudAuditFullAccess 的策略。该策略通过让用户对操作审计所有资源都具有操作权限，从而达到目的，可将预设策略 QcloudSSAReadOnlyAccess 授权给用户，具体操作步骤，请参见 操作步骤。

操作步骤

1. 登录 访问管理控制台，在左侧导航中，单击**策略**，进入策略页面。
2. 在策略页面的搜索框中，输入策略名称（根据实际需求搜索），如输入“QcloudSSAFullAccess”进行搜索。
3. 在“QcloudSSAFullAccess”策略的右侧操作栏中，单击**关联用户/组/角色**。

4. 在关联用户/用户组/角色页面，选中需要配置权限的子用户，单击**确定**即可。



多云多账号管理
多云接入

最近更新时间：2024-08-02 10:14:18

功能简介

当用户业务同时部署在腾讯云和第三方云厂商时，支持通过腾讯云云安全中心集中管理多云资源（目前支持亚马逊云 AWS、微软云 Azure）。通过接入多云账号，实现多云安全管理上的透明化与可视化，实时掌握第三方云上业务的安全防护状态、风险等信息。

操作步骤

1. 登录 云安全中心控制台，在左侧导览中，单击**多云多账号管理**。
2. 在多云多账号管理页面，单击**接入多云账号**。

3. 在配置多云、云外、混合云账号页面，选择账号类型为 Azure 账号 或 AWS 账号，并配置相关参数，单击**确定**。

Azure 账号

步骤1：应用注册

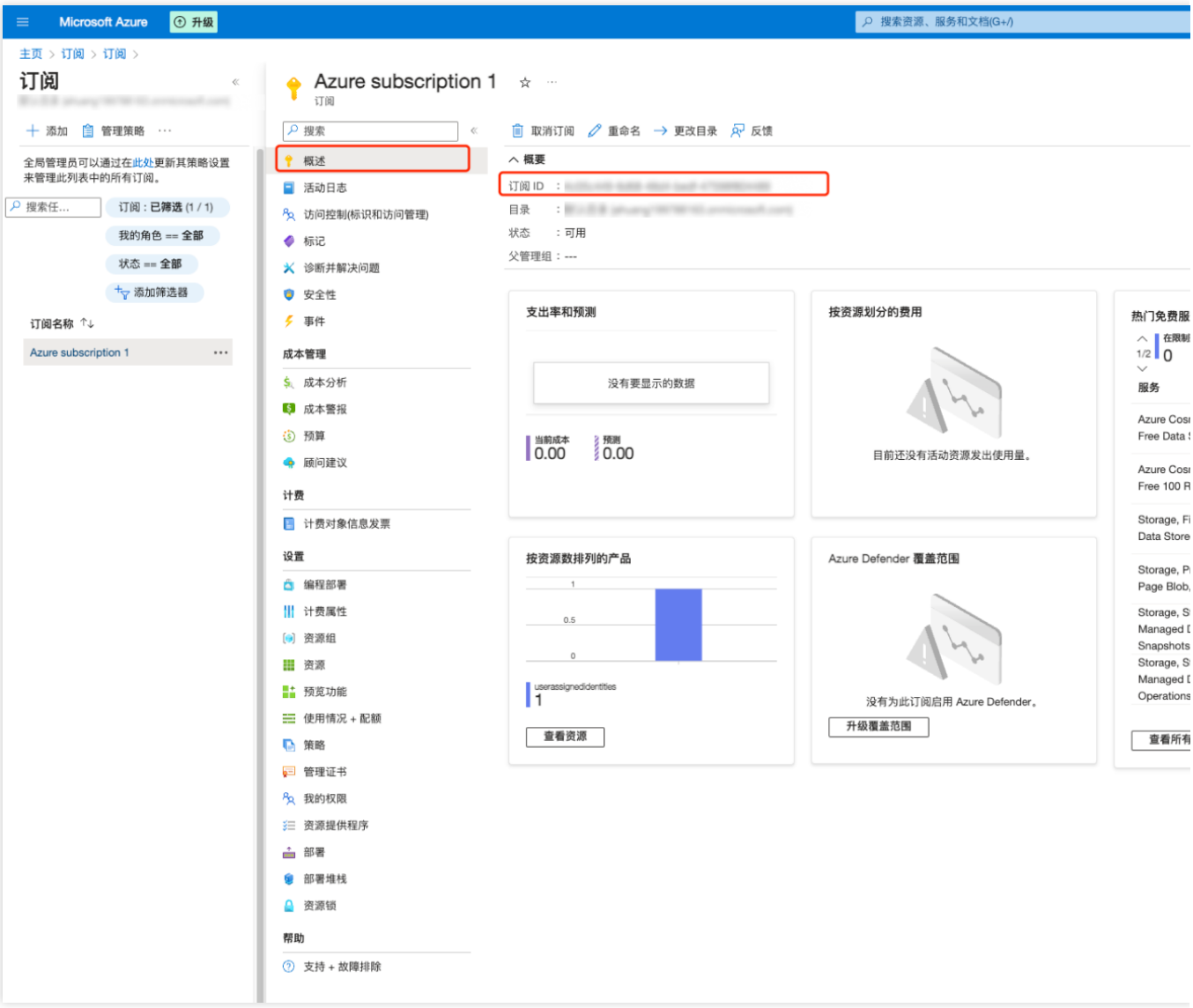
1. 登录 Azure 后前往应用注册页面，单击**新注册**（如果已有应用注册，跳到第二步）。

2. 在注册应用程序页面，填写应用程序“名称”，并根据实际需要选择“受支持的账户类型”，单击**注册**。

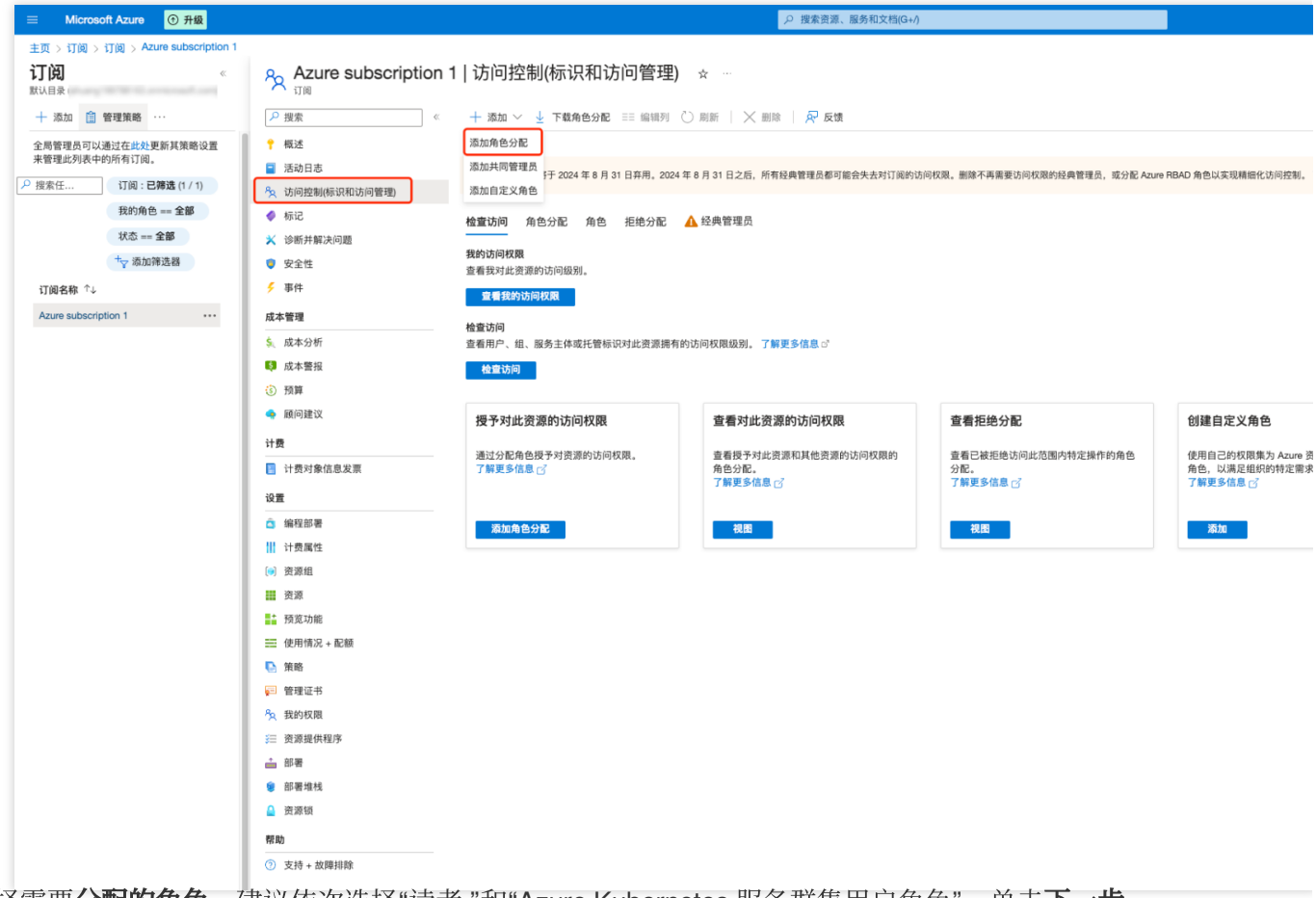
步骤2：获取订阅 ID

1. 在订阅列表页面，选择将要接入的订阅（应用注册可以绑定多个订阅），单击**订阅名称**。

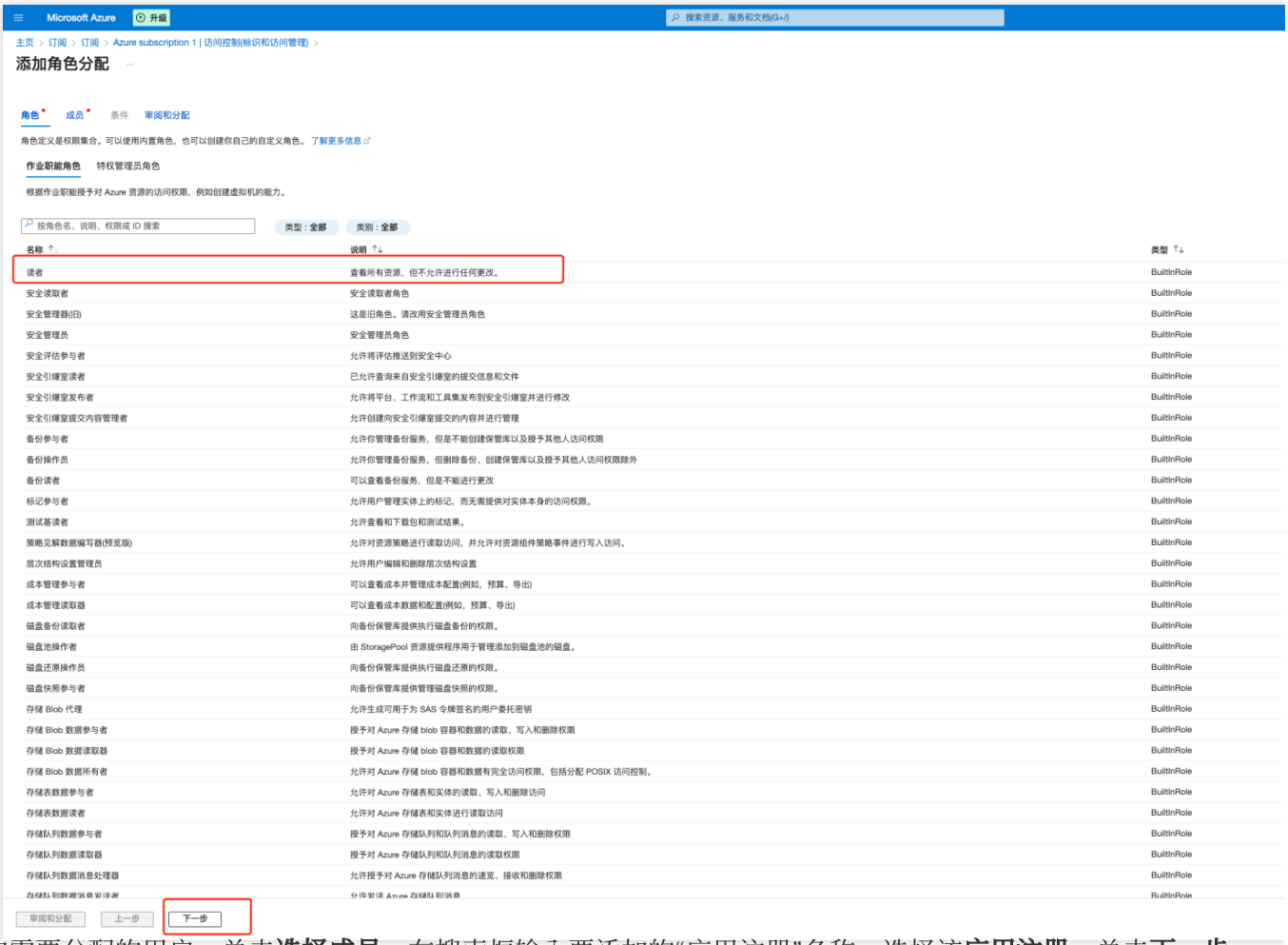
2. 在订阅详情页面，单击**概述**，获取**订阅 ID**。



3. 选择**访问控制**，单击**添加**，选择**添加角色分配**。



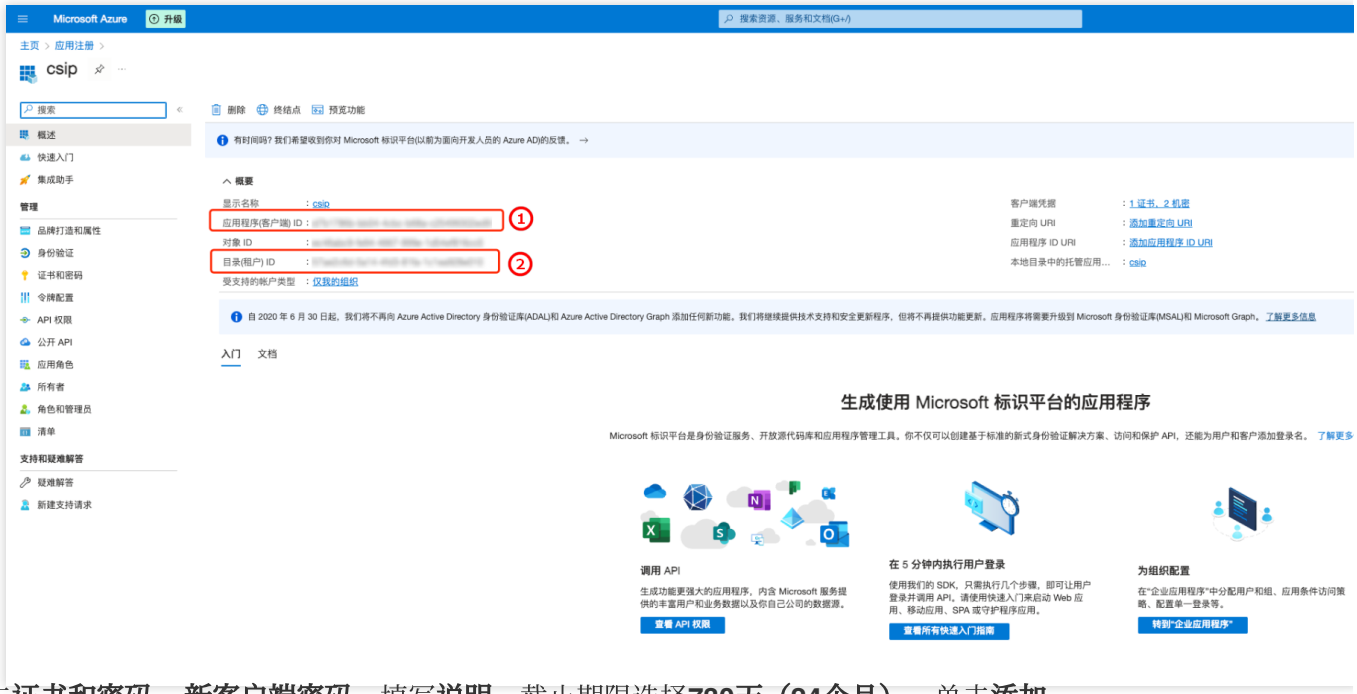
4. 选择需要**分配的角色**，建议依次选择“读者 ”和“Azure Kubernetes 服务群集用户角色”，单击**下一步**。



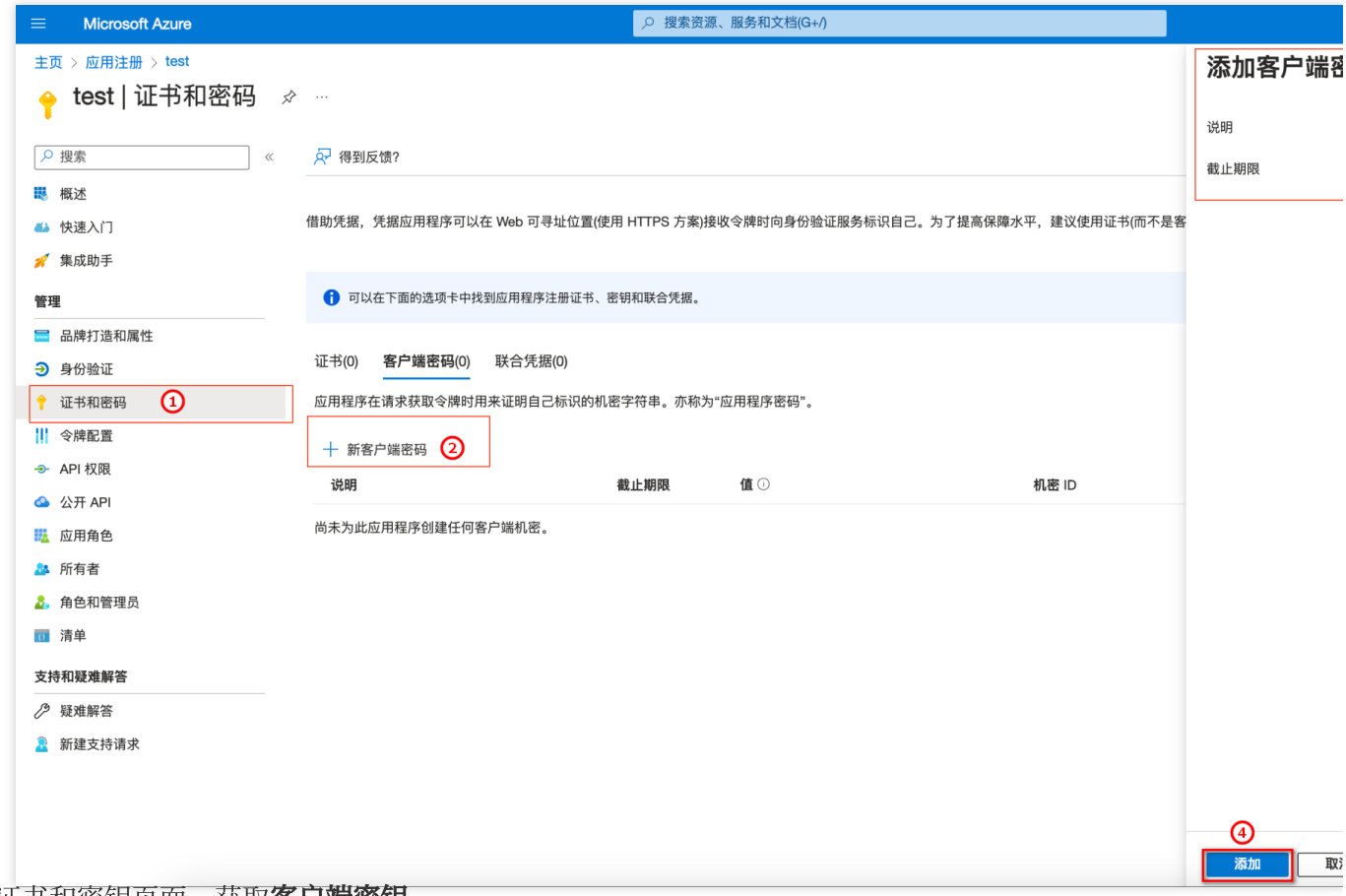
5. 添加需要分配的用户，单击**选择成员**，在搜索框输入要添加的“应用注册”名称，选择该**应用注册**，单击**下一步**。
6. 确定角色与成员，单击**审阅和分配**。

步骤3：获取租户 ID、客户端 ID、客户端密钥

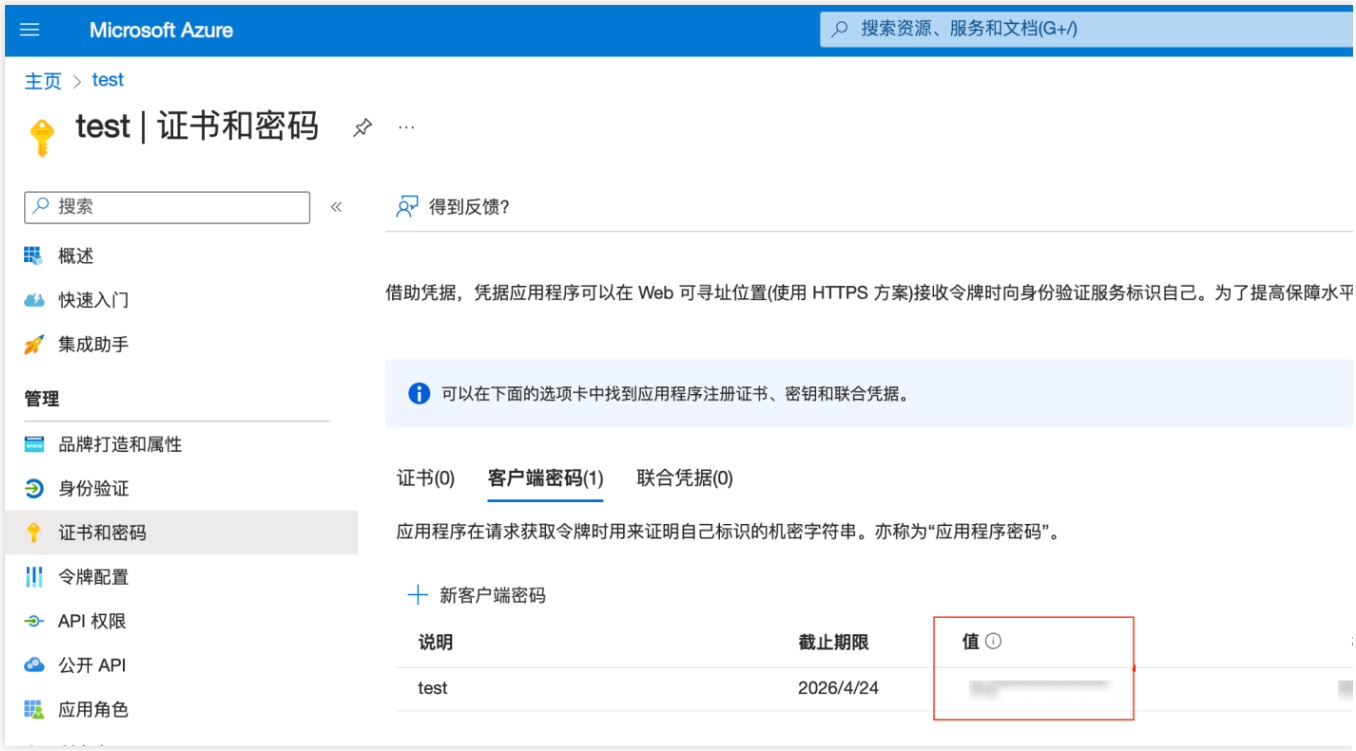
1. 进入刚刚绑定的应用注册页面，单击**概览**，获取“①客户端 ID”与“②租户 ID”。



2. 单击**证书和密码** > **新客户端密码**，填写**说明**，截止期限选择**730天（24个月）**，单击**添加**。



3. 在证书和密钥页面，获取**客户端密钥**。

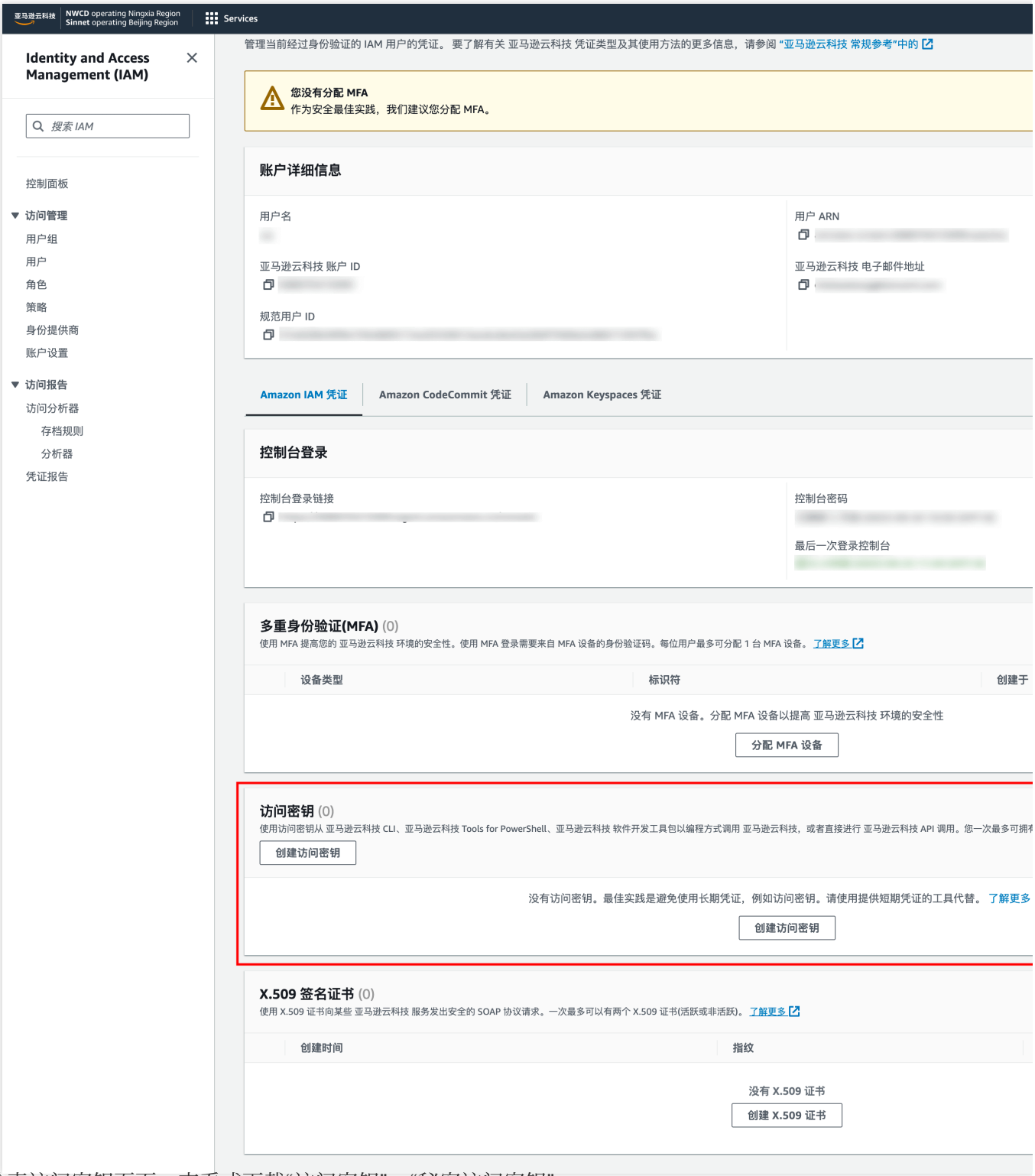


AWS 账号

快速配置

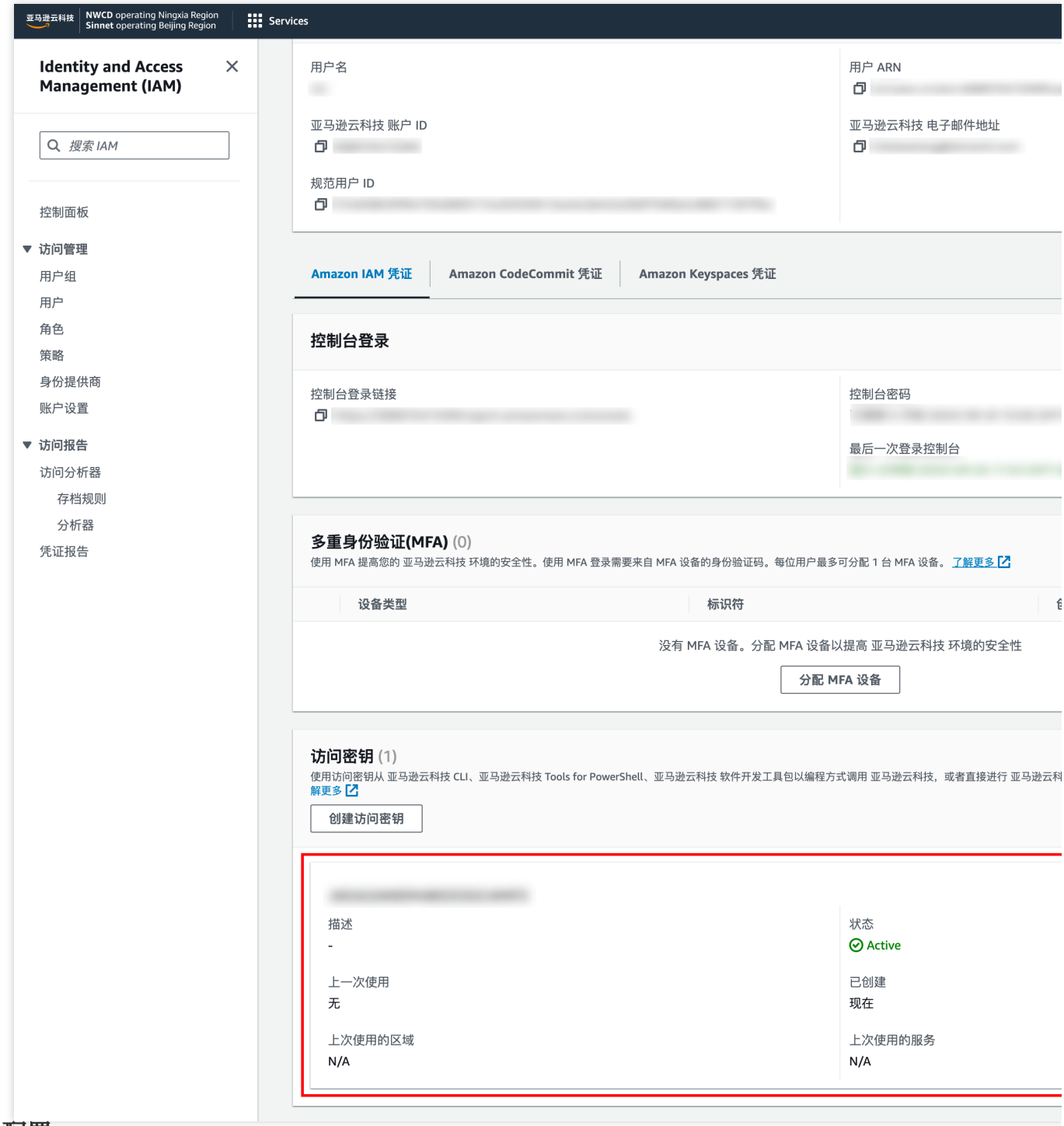
完成时间约为1分钟，但因需要较高权限，需配置主账号的 AK。之后，云安全中心会自动创建一个子账号 AK 以接入资产，并授予对所有资产的只读权限。

1. 请登录 AWS 后前往 安全凭证 页面，单击**创建访问密钥**生成可用于监控或管理亚马逊云科技资源的“访问密钥”、“秘密访问密钥”。



2. 在检索访问密钥页面，查看或下载“访问密钥”、“秘密访问密钥”。

3. 确保“访问密钥”的状态为 Active 后，将“访问密钥”、“秘密访问密钥”填写至“主账号 SecretID”、“主账号 SecretKey”。

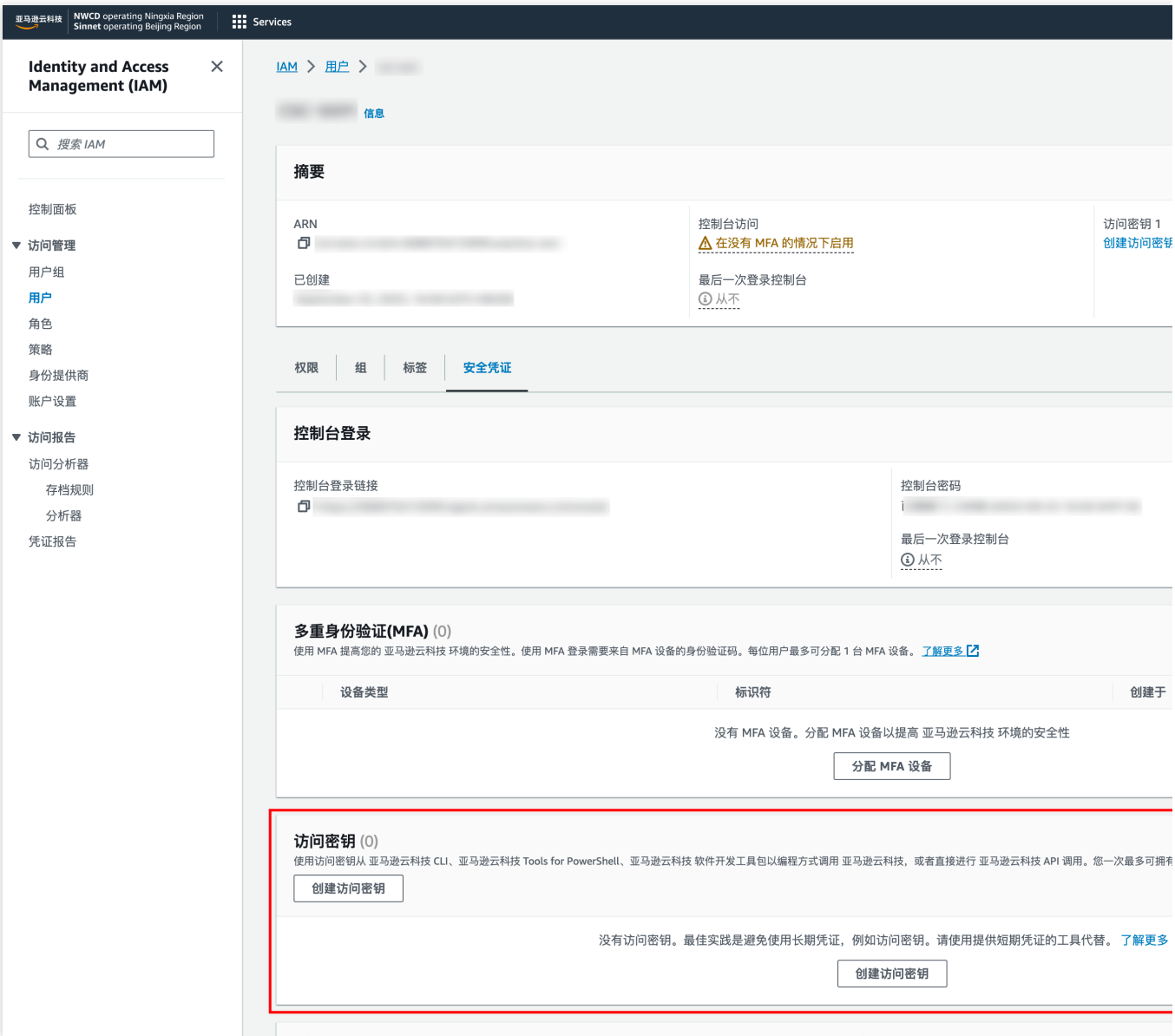


手动配置

完成时间约为5分钟，但权限配置较为复杂，需要为创建好的子账号配置访问密钥（AK），以便更灵活地控制权限范围。

1. 请登录 AWS 后前往 IAM > 用户 页面，单击**创建用户**，创建子账号用于与账户中的亚马逊云科技进行交互。

2. 进入该子用户详情，单击**创建访问密钥**生成可用于监控或管理亚马逊云科技 资源的“访问密钥”、“秘密访问密钥”。

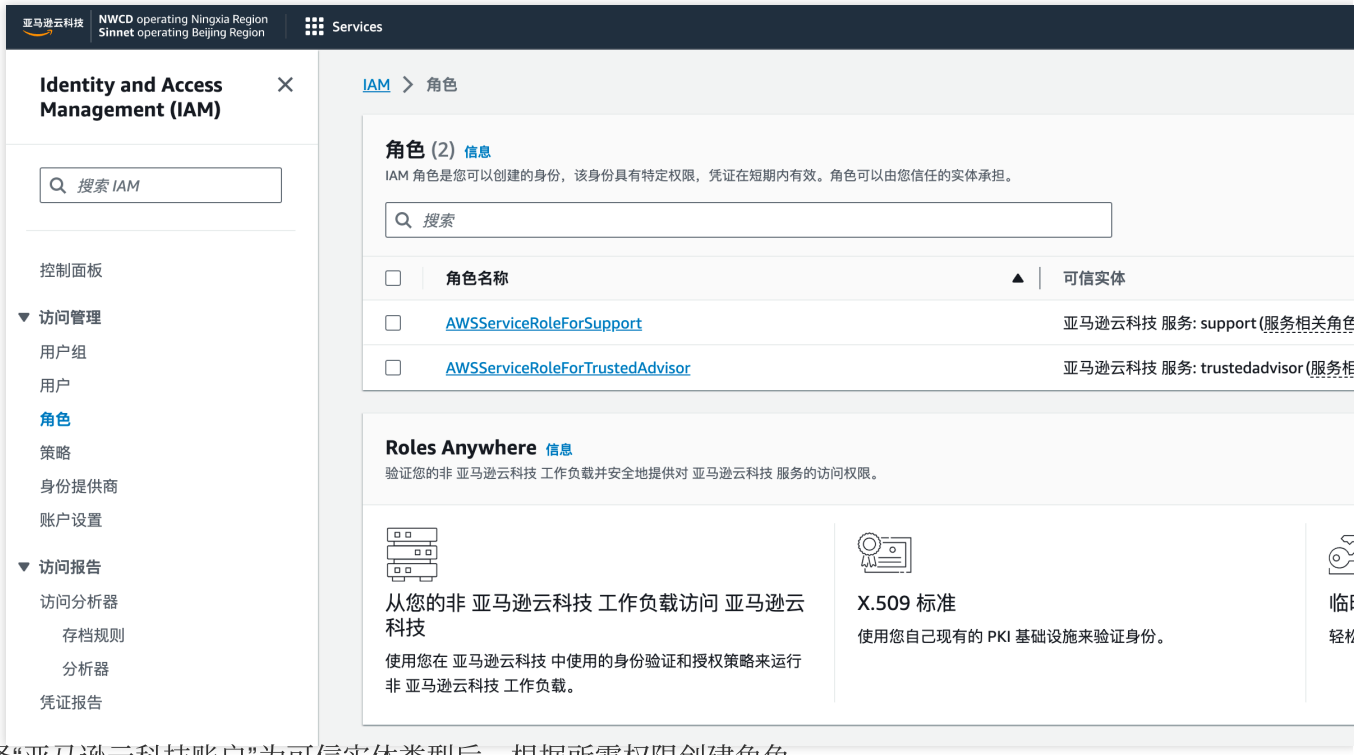


3. 查看或下载“访问密钥”、“秘密访问密钥”，确保“访问密钥”的状态为 Active 后，将“访问密钥”、“秘密访问密钥”填写至“子账号SecretID”、“子账号 SecretKey”。

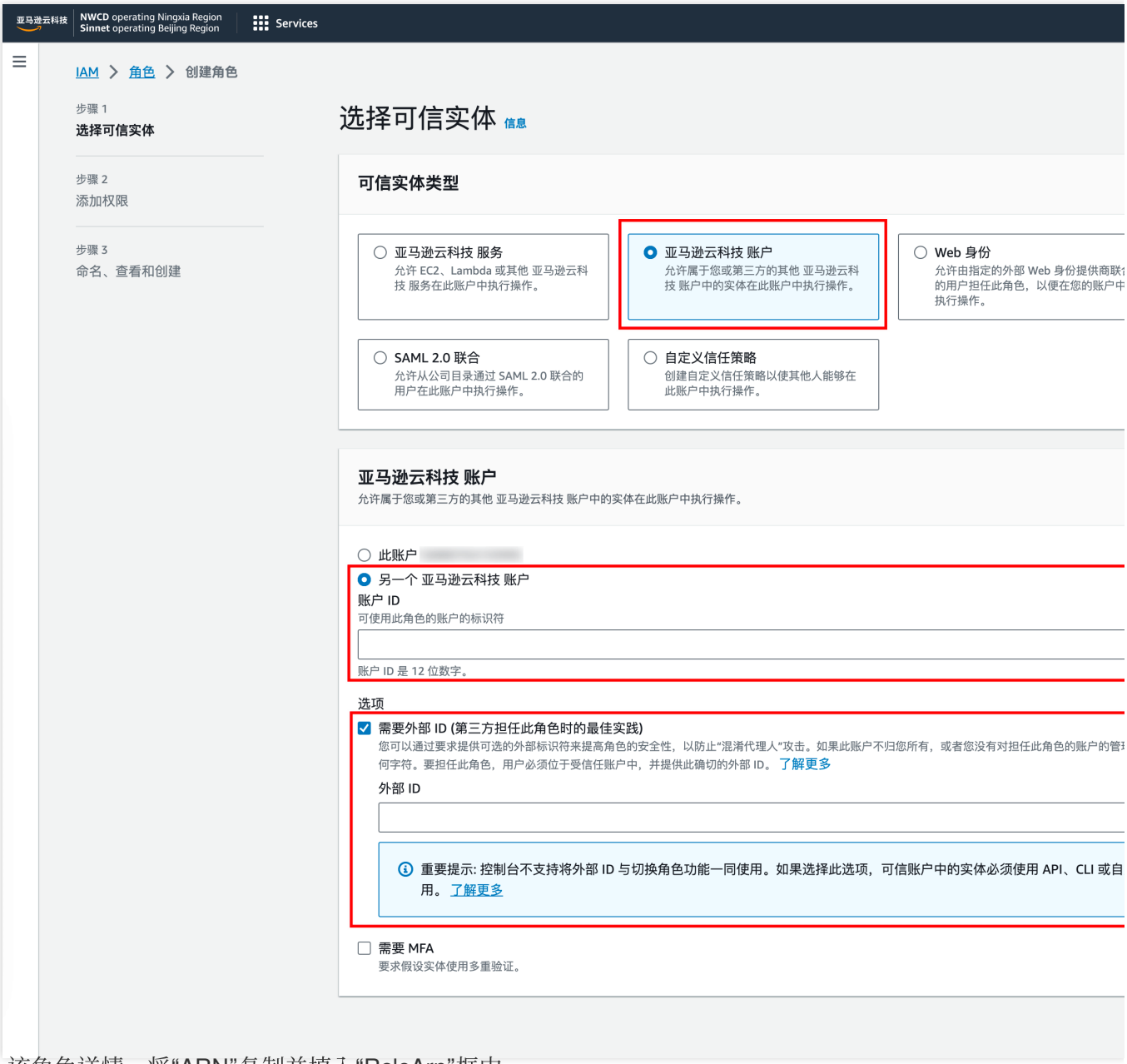
高级配置

较为复杂，但权限范围和期限可控。请按照我们提供的 RoleArn 在 AWS 创建角色，并授权指定 ARN 且带有 uuid 的账号调用 sts:AssumeRole 接口。该接口用于创建账号的临时访问角色。

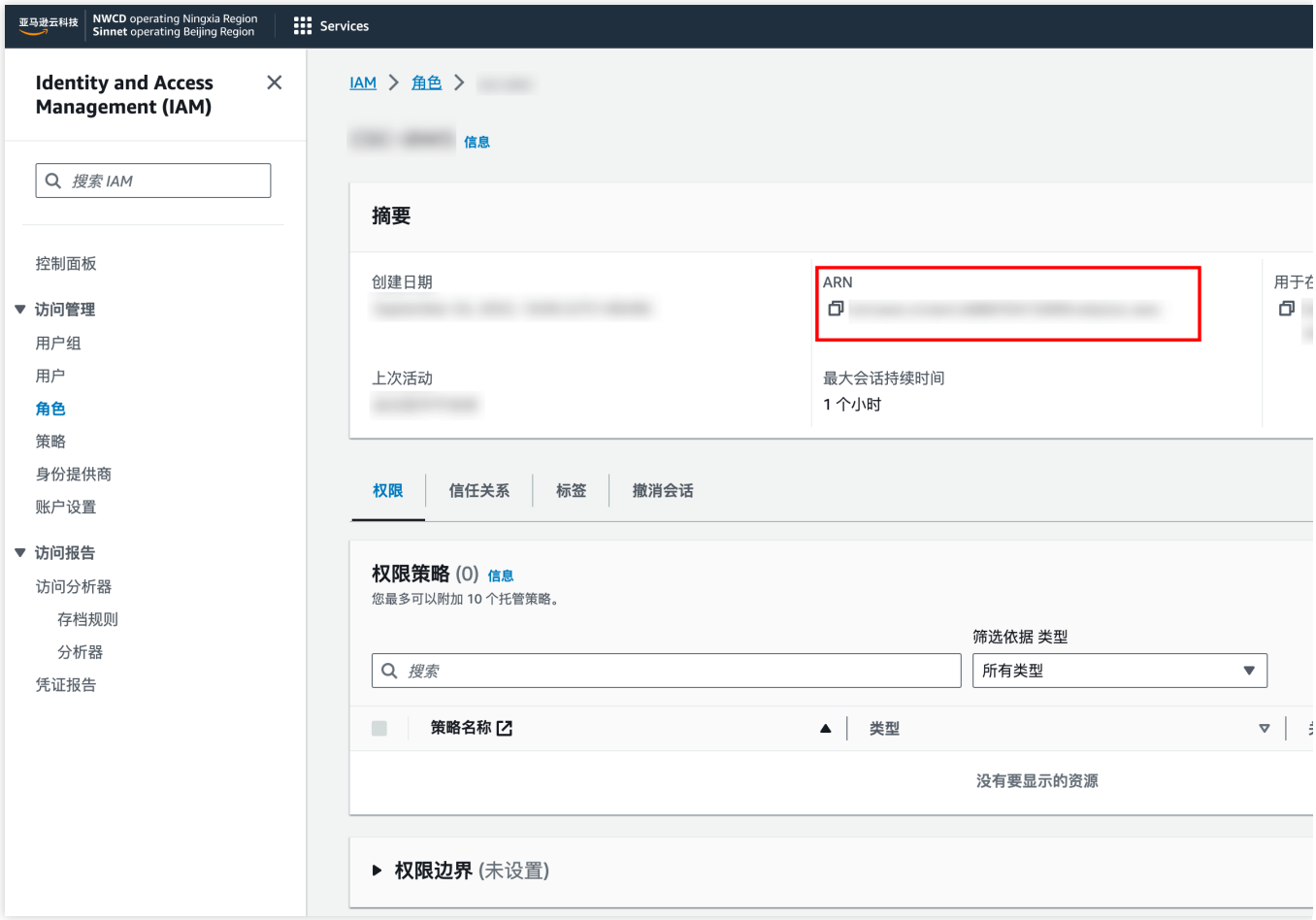
1. 请登录 AWS 后前往IAM > 角色 页面，单击**创建角色**，该身份具有特定权限，凭证在短期内有效。角色可以由您信任的实体承担。



2. 选择“亚马逊云科技账户”为可信实体类型后，根据所需权限创建角色。



3. 进入该角色详情，将“ARN”复制并填入“RoleArn”框中。


亚马逊云科技
NWCD operating Ningxia Region
Sinnet operating Beijing Region
Services
Identity and Access Management (IAM)
搜索 IAM
控制面板
访问管理
用户组
用户
角色
策略
身份提供商
账户设置
访问报告
访问分析器
存档规则
分析器
凭证报告
IAM > 角色 >
信息
摘要
创建日期
ARN
上次活动
最大会话持续时间
1 个小时
权限
信任关系
标签
撤消会话
权限策略 (0) 信息
您最多可以附加 10 个托管策略。
筛选依据 类型
搜索
所有类型
策略名称
类型
没有要显示的资源
权限边界 (未设置)

多账号管理

最近更新时间：2024-08-12 17:26:36

功能简介

用户拥有多个腾讯云主账号且各账号间独立计费，通过多账号管理切换登录各账号、集中管理各账号。集团管理者有效掌握集团安全信息，实现集团安全管理上的透明化与可视化，实时掌握各成员账号云上业务的安全防护状态、风险等信息。

操作场景

切换登录账号

支持一键切换成员账号登录，满足高效且安全的免密码切换。

集中管理账号

无需部署，集中管理集团所有账号，各成员账号安全防护状态透明化，支持设置账号的安全管理权限。
支持对集团多账号云上业务风险处理闭环，可以对任一成员账号的云上资产进行一键扫描以排查潜在风险。

一、集团账号管理

您需在集团账号管理中创建集团组织后，方可使用云安全中心多账号管理。根据当前登录账号不同状态区分，您可以挑选账号状态相符的步骤开始进行操作。

注意

未企业实名认证的个人账号、已加入到其他集团组织的企业账号、之前集团组织创建的账号无法创建集团组织。详情请参见 集团组织设置。

步骤1：未企业实名认证的个人账号

在 多云多账号管理页面，单击**完成实名认证**前往 账号中心控制台，按照步骤完成企业实名认证。详情请参见 变更个人认证信息-变更为企业实名认证。

步骤2：未创建集团组织的企业账号

在 集团账号管理页面，单击**创建**，即创建一个集团组织。在该集团组织下，创建成员账号或邀请账号加入集团组织。

步骤3：使用多账号管理

已开通多账号管理的企业账号，可开始使用多账号管理。

二、如何灵活的切换账号登录

授权访问成员账号

登录 集团账号管理控制台，授权管理员子账号登录管理成员账号的权限。详情请参见 授权访问成员账号。

切换登录成员账号

1. 在 多云多账号管理页面，选择对应成员账号，单击**登录账号**。

2. 在登录账号弹窗中，选择所需的权限名称、策略名称，并单击对应**登录成员账号**，即切换登录成功。

注意

管理员主账号、未进行授权的管理员子账号不能切换登录、被邀请进集团组织的成员账号不支持授权登录。

三、如何高效的集中管理账号

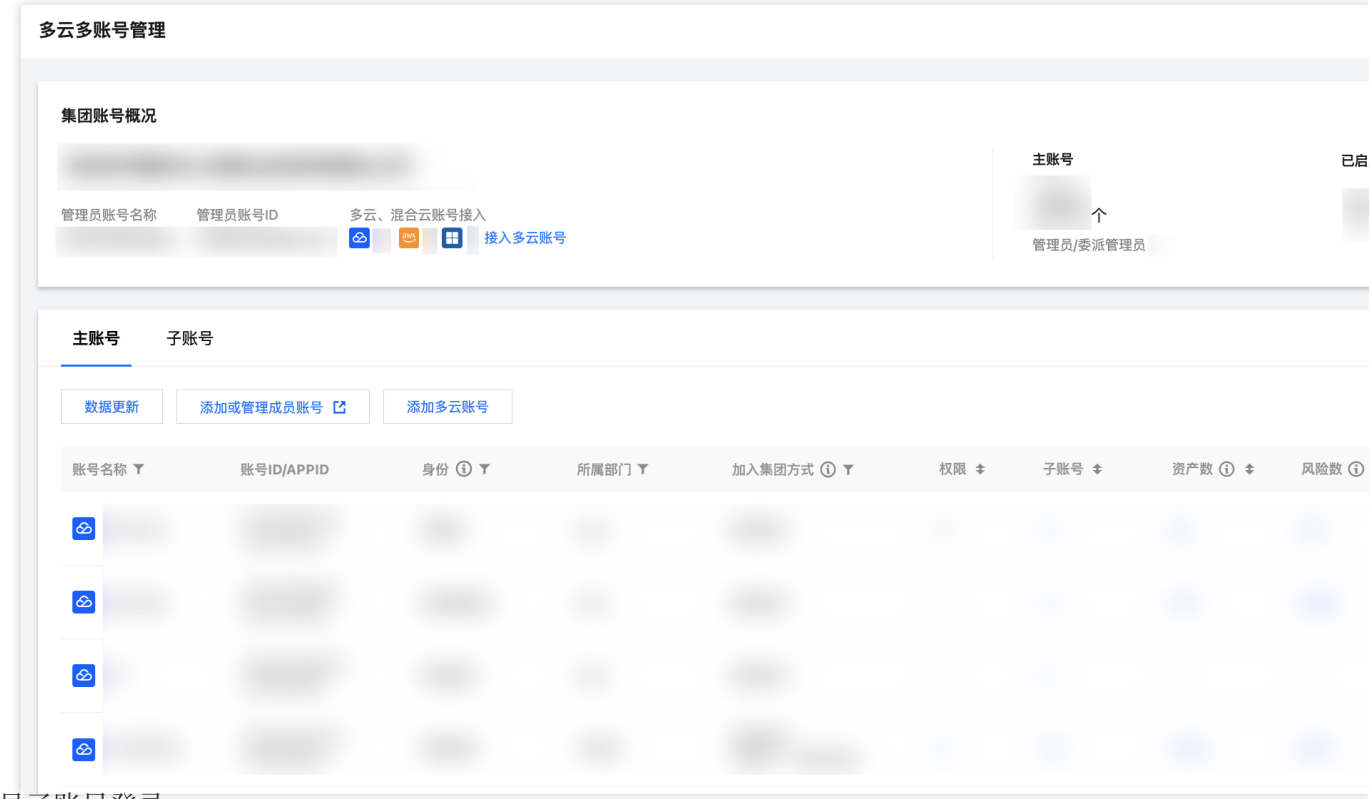
使用管理员主账号、子账号登录 云安全中心控制台后，支持查看集团安全信息，实现集团安全管理上的透明化与可视化，实时掌握各成员账号云上业务的安全防护状态、风险等信息。
在资产中心、风险中心、扫描任务、报告下载等功能模块已适配多账号管理模式，进行跨账号操作以保证集团云上业务资产的安全。

账号切换

在各功能模块右上角，单击**多账号管理**，下拉筛选框后，可以通过输入**账号名称/账号 ID/APPID** 进行搜索，选中成员账号后单击**确定**，功能模块内数据将切换至该账号所有数据。

系统设置-多账号管理

在 多云多账号管理页面，无需部署集中管理集团所有账号，各成员账号安全防护状态透明化，支持一键切换成员账号登录，满足高效且安全的免密码切换。不同方式登录后效果如下所示：
管理员主账号登录



管理员子账号登录

成员主账号、子账号登录

资产中心

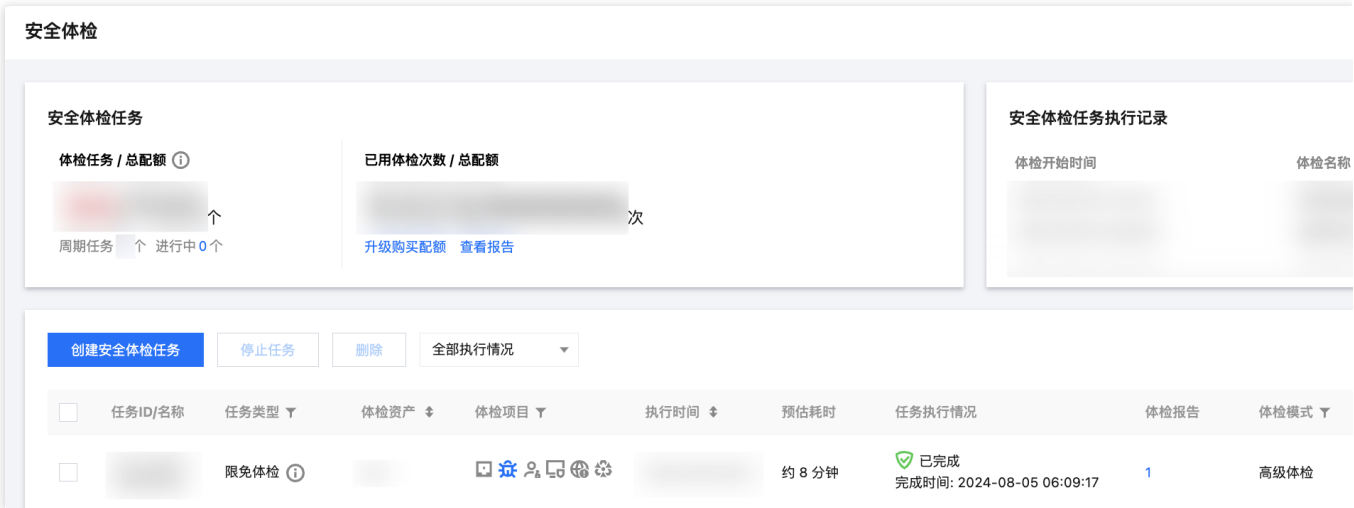
在 资产中心页面，管理员账号可以跨账号管理云上业务资产，掌握各资产安全防护状态，对任一账号的云上资产进行一键扫描以排查潜在风险。

漏洞与风险中心

在 漏洞与风险中心页面，联动各产品能力一站式管控云上业务的端口、漏洞、弱口令、配置、内容等资产风险，管理员账号可以跨账号处理云上业务资产的潜在风险。

安全体检

在 安全体检页面，可视化集团组织下所有账号所有扫描任务的信息并实时反馈各扫描任务执行情况，管理员可以跨账号高效管理各资产扫描任务，支持管理员跨账号对各账号的扫描任务进行编辑、删除、停止任务等操作。



报告下载

在 报告下载页面，联动漏洞扫描服务，管理员可以跨账号下载各扫描任务对应的报告，管理员关注服务号可以随时随地接收报告。

四、常见问题

多账号管理之后的计费标准？

未来新版云安全中心的计费标准请实时关注产品动态。

存量用户的数据情况

云安全中心将在限时免费体验结束前一个月告知用户体验结束，未付费用户的数据将被清除，付费用户的数据将接入新版云安全中心。

如何实现多账号管理，是否需要调整网络架构？

安全产品的系统层数据上打通以实现多账号管理，不需要调整网络架构。

使用过程中，有问题如何联系?

感谢您对腾讯云的信赖与支持，若在使用产品过程中有任何问题可以 提交工单 联系我们处理，我们将尽快为您核实处理！

模拟攻击

最近更新时间：2024-08-02 10:14:18

功能背景

通过模仿黑客的思考和工作方式，基于 MITRE ATT&CK 框架自动化模拟战技、战术，从攻击视角看待各种云上安全威胁，用户可以识别可能被攻击的不同路径和最具影响力的安全威胁，发现安全防护产品的不足及对应安全策略是否配置得当，合理利用安全资源最大程度降低云上风险。

应用场景

高效的渗透化测试

通过自动化执行模拟攻击任务，广泛测试大量已知攻击，操作简便实用，减轻运维人员工作量。系统默认提供以 MITRE ATT&CK 框架作为基准的渗透测试剧本，剧本包含信息收集、漏洞探测、漏洞利用、权限维持、横向渗透等攻击战术，模仿恶意黑客的行为方式及现实世界的对手。

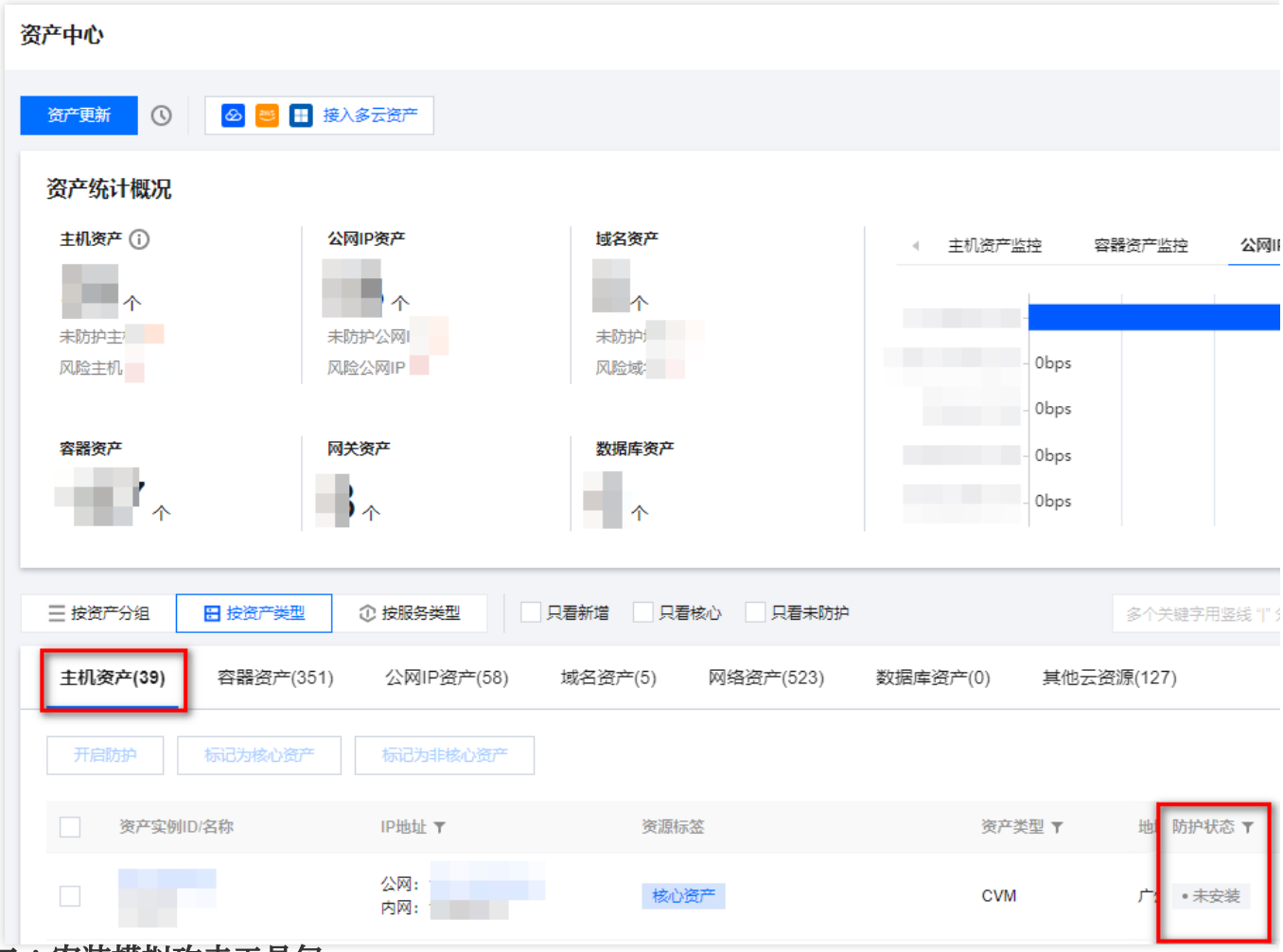
准确对比安全防护产品可靠性

在目标系统上模拟攻击后，前往已拥有的安全防护产品上查看对应告警信息，对比多款安全防护产品的检出率，检验安全防护产品的可靠性。

安装模拟攻击工具包

步骤一：查询资产对应工具包安装状态

1. 登录 云安全中心控制台，在左侧导览中，单击**资产中心**。
2. 在资产中心页面，选择**主机资产**，查看该资产的模拟工具包安装状态。



步骤二：安装模拟攻击工具包

针对未安装模拟攻击工具包的资产，可参照以下三个安装方式进行安装：

方式1：手动执行命令

登录目标服务器后执行对应命令下载、运行模拟攻击工具包。

方式2：通过腾讯云自动化助手执行命令下载并运行模拟攻击工具包

仅支持已安装腾讯云自动化助手客户端的资产，通过自动化助手执行命令后，将在服务器上下载并运行模拟攻击工具包 。

方式3：通过主机安全 Agent 执行命令下载并运行模拟攻击工具包

仅支持已安装主机安全 Agent 的资产，通过主机安全 Agent 执行命令后，将在服务器上下载并运行模拟攻击工具包。

在资产中心页面，选择目标主机资产，单击操作列的**更多 > 安装工具包**。

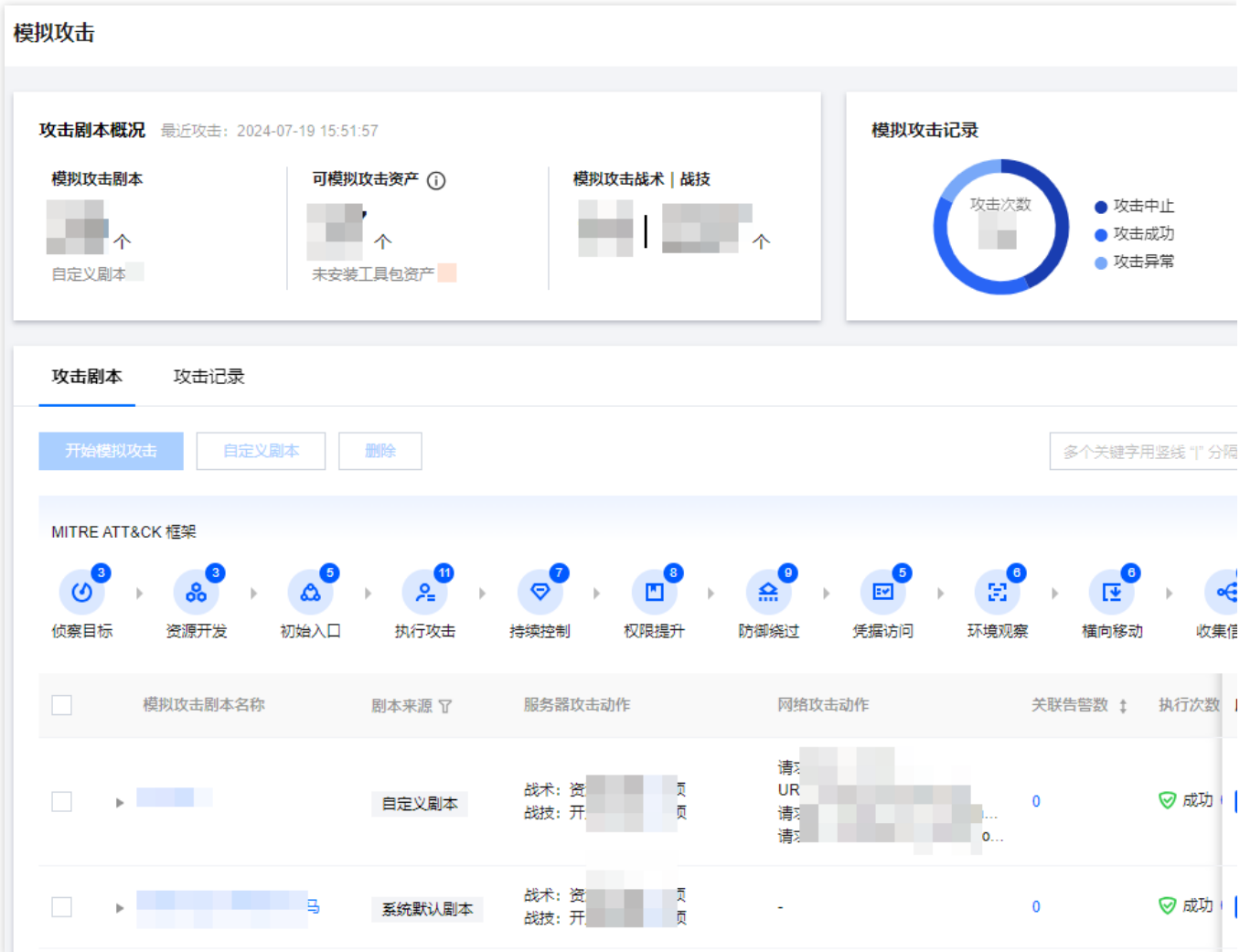
注意：

当前暂仅支持腾讯云内操作系统为 Linux 系统的服务器。

步骤三：如何高效的渗透化测试

查看渗透测试剧本

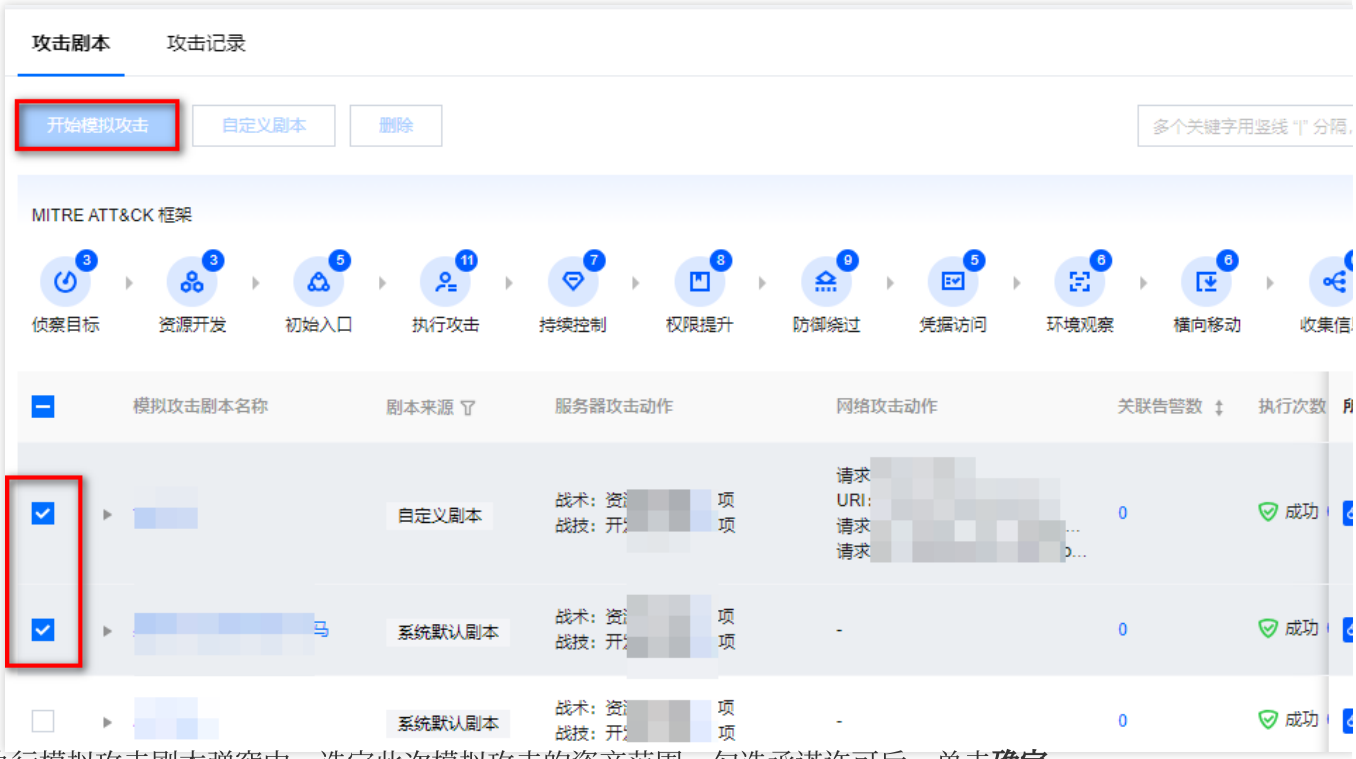
在 模拟攻击页面，查看渗透测试剧本，系统默认提供多个包含信息收集、漏洞探测、漏洞利用、权限维持、横向渗透等攻击战术的渗透测试剧本，以模仿恶意黑客的行为方式及现实世界的对手。



在 模拟攻击页面，单击右上角 **ATT&CK 模拟攻击矩阵**了解单个剧本关联的战术、战技，或了解某个战术、战技所关联的剧本。

选择剧本及模拟攻击资产范围

1. 在 模拟攻击页面，选择一个或多个剧本后，单击**开始模拟攻击**。



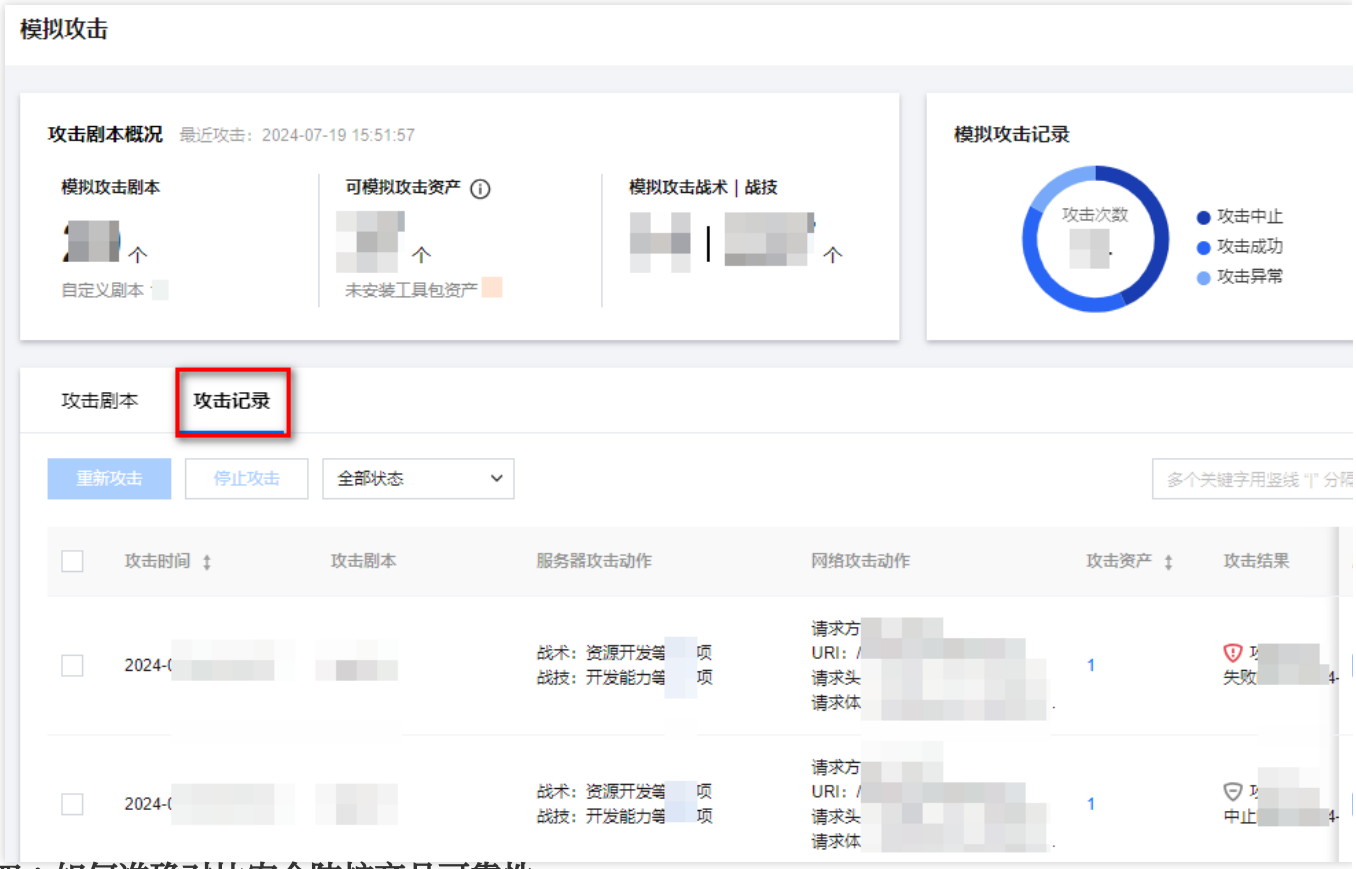
2. 在执行模拟攻击剧本弹窗中，选定此次模拟攻击的资产范围，勾选承诺许可后，单击**确定**。

说明：

仅可对已安装工具包的资产执行模拟攻击剧本。

查看剧本模拟攻击记录

在 模拟攻击 > **攻击记录**页面，通过剧本的执行情况查看当前剧本执行结果（成功、异常、中止），可以停止正在执行中的模拟攻击、重新模拟攻击等操作。



步骤四：如何准确对比安全防护产品可靠性

剧本模拟攻击成功后，可前往已有的安全防护产品查看模拟攻击对应的执行结果，例如 T-Sec 主机安全(CWP)，通过查看安全防护产品已检出的告警内容，发现安全防护产品的不足及对应安全策略是否配置得当。通过多个安全防护产品已检出的告警数量及告警内容的准确性，对比多个安全防护产品的可靠性。

常见问题

为何安装模拟攻击工具包失败？

防火墙拦截：建议防火墙策略放过云安全中心后台服务器访问地址，公网域名 bas.tencentcs.com、csc-1300616671.cos.ap-guangzhou.myqcloud.com，公网端口8001、443。
网络问题：建议检查网络连接是否正常，尝试使用其他网络。模拟攻击工具包需要从互联网下载文件，如果网络不稳定或者下载速度过慢，可能会导致安装失败。
权限问题：建议使用管理员账户登录系统，或者使用“以管理员身份运行”选项下载/运行模拟攻击工具包。下载/运行模拟攻击工具包需要管理员权限，如果当前用户没有足够的权限，可能会导致安装失败。
系统兼容性问题：查看模拟攻击工具包的系统要求，确保当前操作系统和其他软件版本符合要求。模拟攻击工具包可能不兼容当前操作系统或其他软件，导致运行失败。

系统默认剧本依据来源是？

系统默认剧本基于ATT&CK中的战术阶段，可参考 MITRE ATT&CK 进行学习了解。MITRE ATT&CK是一个全球可访问的基于现实世界观察的对手战术和技术知识库。ATT&CK 知识库被用作私营部门、政府以及网络安全产品和服务社区开发特定威胁模型和方法的基础。

系统默认剧本（持续更新）

剧本名称	剧本内容
Python base64命令攻击	模拟黑客使用 Python 解码经过 base64 编码的文本字符串，用来执行恶意代码或窃取敏感信息。
密码复杂性策略检查	模拟黑客检查 Linux 系统上控制台的密码复杂性策略，以便了解密码的要求和限制，可能会被用来破解密码或者获取系统的访问权限。
Shiro 反序列化攻击	模拟黑客利用 Shiro 反序列化漏洞获取目标系统的远程命令执行权限，通过执行恶意命令来获取系统的访问权限或者窃取敏感信息。
DNS 日志信息收集	模拟黑客通过 DNS 日志获取访问者的 IP 地址，用来检测目标用户的活动或者进行其他恶意行为。
端口转发攻击	模拟黑客通过收集目标系统的信息了解目标系统的弱点和漏洞，在目标系统上安装恶意软件或利用漏洞维持对目标系统的访问权限，利用 Netcat 工具使用端口转发技术来绕过防火墙和其他安全防护产品以便在目标系统上执行命令或传输文件。
内网横向移动攻击	模拟黑客收集主机 SSH 信息以了解目标系统的 SSH 配置和安全性，使用 Exploit Writing Toolkit（EW）工具通过利用已经攻破的一台目标系统，进一步攻击其他系统，以便在内网中获取更多的敏感信息或控制更多的系统。
用户权限维持攻击	模拟黑客将目标系统中的敏感数据传输到模拟者控制的服务器或其他地方，以获取非法利益或造成损失，当读取敏感信息后将恶意代码写入以维持对目标系统的访问权限，清除目标系统中的各种历史记录，以隐藏攻击痕迹或误导调查人员。
恶意文件执行攻击	模拟黑客将恶意代码写入文件中并执行该文件来实现攻击，通过收集目标系统上 SUID 信息并在目标系统上执行 Python 反弹 shell 脚本，当模拟者收到目标系统的连接后进行 Prox 横向移动获取更多的系统权限，随后篡改文件的时间戳来隐藏攻击痕迹或误导调查人员。
NC 反弹 shell 攻击	模拟黑客通过收集目标系统上主机安全进程信息以尝试杀掉主机安全相关进程，利用 NetCat 工具在目标系统上执行反弹 shell 命令，将目标系统的 shell 连接到模拟者的机器上，模拟者收到目标系统的连接后可以执行命令或获取系统权限。
Python 反弹 shell 攻击	模拟黑客通过收集目标系统的信息了解目标系统的弱点和漏洞，在目标系统上通过执行 Python 反弹 shell 脚本，将目标系统的 shell 连接到模拟者的机器上，模拟者收到目标系统的连接后可以执行命令或获取系统权限。

恶意横向移动	模拟黑客通过收集目标系统的信息了解目标系统的弱点和漏洞，模拟者利用iox恶意工具进行端口流量转发后控制目标系统，然后利用该目标系统的权限和功能，进一步攻击其他系统，并最终获取更多的敏感信息或控制更多的系统。

日志投递（支持多账号多产品多日志）

最近更新时间：2024-08-12 17:28:05

功能背景

将接入云安全中心的多款产品日志集中并归一化后通过控制台投递至消息队列，便于存储数据或联合其它系统消费数据，助力挖掘日志数据价值，满足用户日志运维诉求。启用日志投递后，将采集到的日志投递至对应的消息队列。

应用场景

日志存储

根据《中华人民共和国网络安全法》、《信息安全等级保护管理办法》等相关法律法规的规定，企业需要对网络安全事件进行记录和存储，并且日志存储时长不少于6个月。这是为了保障企业的信息安全和网络安全，防止安全事件的发生和滋生。

离线分析

将日志投递至 Kafka/CLS 后，企业可以接入其他系统进行离线分析，进一步管控原始日志，协助企业对安全事件进行深入分析和研究，发现安全事件的根本原因和漏洞，提高安全事件的处理能力和水平。

日志投递至 Kafka

在日志分析页面，您可配置云安全中心接入的不同日志类型分别投递到指定 Ckafka 实例的不同 Topic 中。

前提条件：

为了将日志投递至消息队列，需要先购买云安全中心旗舰版，并将相关产品的日志接入云安全中心。如果需要使用 Ckafka 公网域名或 Ckafka 支撑环境接入两种网络接入方式之一，需要先前往创建腾讯云消息队列 CKafka 实例。

Ckafka 公网域名接入

1. 登录 云安全中心控制台，在左侧导览中，单击**日志分析**。
2. 在日志分析页面，单击**日志投递 > 投递至 kafka。**
3. 在投递至 kafka页面，云安全中心自动获取账号的腾讯云消息队列 Ckafka 实例、已接入云安全中心的日志来源，选择 **Ckafka 公网域名接入**，配置相关参数。

参数名称	说明
网络接入方式	Ckafka 公网域名接入。
TLS 加密	选择是否开启 TLS 加密。
消息队列所属账号	投递目标所属账号。

消息队列实例	云安全中心自动获取账号的腾讯云消息队列 Ckafka 实例、选择所需消息队列实例。
公网域名接入	选择所需公网域名。
用户名	请输入所选消息队列实例的用户名。
密码	请输入所选消息队列实例的密码。
日志来源	支持选择主机安全、云防火墙、Web 应用防火墙、云安全中心、DDoS 防护、SaaS 化堡垒机、云审计、网络蜜罐的日志。
日志类型	根据所选的日志来源不同则日志类型也有所不同。
Topic ID/名称	选择所需 Topic。
操作	新增：单击**新增日志投递配置**，支持新增多个日志来源。 删除：单击目标日志操作列的**删除**，经过二次确认后，支持删除该日志来源对应日志类型的日志投递任务。 编辑：如非首次配置日志投递，则支持在日志投递页面，单击**修改配置**，修改相关日志投递。

4. 确认无误后，单击**确定**，即可将采集到的日志投递至对应的消息队列。
5. 在日志投递页面，支持查看同步接入方式、接入对象、消息队列状态、用户名等消息队列详情，以及日志来源、日志类型、账号来源（多账号下）、Topic ID/名称、Topic 投递状态、投递开关等信息，允许修改消息队列、Topic 配置等信息，查看消息队列和各 Topic 状态。

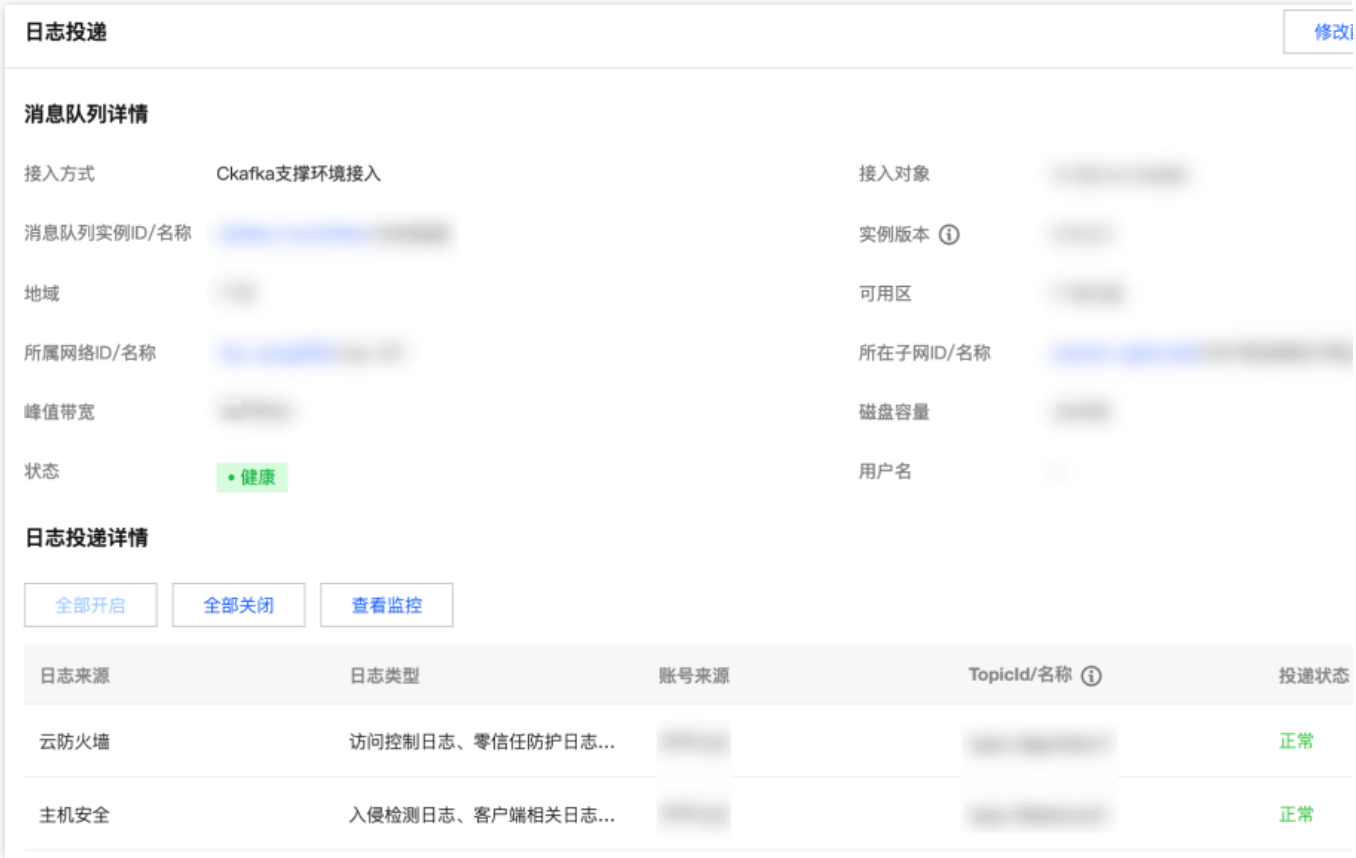
Ckafka 支撑环境接入

1. 登录 云安全中心控制台，在左侧导览中，单击**日志分析**。
2. 在日志分析页面，单击**日志投递 > 投递至 kafka**。
3. 在投递至 kafka 页面，云安全中心自动获取账号的腾讯云消息队列 Ckafka 实例、已接入云安全中心的日志来源，选择 **Ckafka 支撑环境接入**，配置相关参数。

参数名称	说明
网络接入方式	Ckafka 支撑环境接入。
TLS 加密	选择是否开启 TLS 加密。
消息队列所属账号	投递目标所属账号。

消息队列实例	云安全中心自动获取账号的腾讯云消息队列 Ckafka 实例、选择所需消息队列实例。
支撑环境接入	选择所需支撑环境。
日志来源	支持选择主机安全、云防火墙、Web 应用防火墙、云安全中心、DDoS 防护、SaaS 化堡垒机、云审计、网络蜜罐的日志。
日志类型	根据所选的日志来源不同则日志类型也有所不同。
Topic ID/名称	选择所需 Topic。
操作	新增：单击**新增日志投递配置**，支持新增多个日志来源。 删除：单击目标日志操作列的**删除**，经过二次确认后，支持删除该日志来源对应日志类型的日志投递任务。 编辑：如非首次配置日志投递，则支持在日志投递页面，单击**修改配置**，修改相关日志投递。

4. 确认无误后，单击**确定**，即可将采集到的日志投递至对应的消息队列。
5. 在日志投递页面，支持查看同步接入方式、接入对象、消息队列状态、用户名等消息队列详情，以及日志来源、日志类型、账号来源（多账号下）、Topic ID/名称、Topic 投递状态、投递开关等信息，允许修改消息队列、Topic 配置等信息，查看消息队列和各 Topic 状态。



其他 Kafka 公网接入

1. 登录 云安全中心控制台，在左侧导览中，单击**日志分析**。

2. 在日志分析页面，单击**日志投递 > 投递至 kafka**。
3. 在投递至 kafka 页面，选择**其他 Kafka 公网接入**，配置相关参数。

参数名称	说明

网络接入方式	其他 Kafka 公网接入。
TLS 加密	选择是否开启 TLS 加密。
公网接入	根据实际需求填写公网信息。
用户名	请输入所选消息队列实例的用户名。
密码	请输入所选消息队列实例的密码。
日志来源	支持选择主机安全、云防火墙、Web 应用防火墙、云安全中心、DDoS 防护、SaaS 化堡垒机、云审计、网络蜜罐的日志。
日志类型	根据所选的日志来源不同则日志类型也有所不同。
Topic 名称	输入所需 Topic 名称。
操作	新增：单击**新增日志投递配置**，支持新增多个日志来源。 删除：单击目标日志操作列的**删除**，经过二次确认后，支持删除该日志来源对应日志类型的日志投递任务。 编辑：如非首次配置日志投递，则支持在日志投递页面，单击**修改配置**，修改相关日志投递。

4. 确认无误后，单击**确定**，即可将采集到的日志投递至对应的消息队列。

5. 在日志投递页面，支持查看同步接入方式、接入对象、消息队列状态、用户名等消息队列详情，以及日志来源、日志类型、账号来源（多账号下）、Topic 名称、Topic 投递状态、投递开关等信息，并且允许修改消息队列、Topic 配置等信息。

日志投递至 CLS

在日志分析页面，您可配置云安全中心接入的不同日志类型分别投递到指定 CLS 的不同日志主题中。

1. 单击左上角的**日志投递**，打开日志投递配置弹窗，首次若未开通 CLS 服务，须先单击 前往授权，同意服务授权且创建服务角色后才可进行更多日志投递配置。

说明：

云安全中心支持将日志投递到 CLS，实现日志采集、日志存储到日志检索等全方位的日志服务。当前账号授权访问CLS服务和开启日志投递到 CLS 后，将为您自动 在 CLS 服务中创建后付费的存储空间，同时也会生成后付费账单。详情请参见 CLS计费详情。

2. 完成上述授权后，可对要进行投递的日志配置不同的日志主题（不进行投递的日志类型，可以不进行配置）。

参数名称	说明
投递所属账号	投递目标所属账号。

日志来源	支持选择主机安全、云防火墙、Web 应用防火墙、云安全中心、DDoS 防护、SaaS 化堡垒机、云审计、网络蜜罐的日志。
日志类型	根据所选的日志来源不同则日志类型也有所不同。
日志来源账号	选择的日志源对应的多账号名称。
目标地域	请输入将要投递的目标地域。
日志集操作	选择投递至已有日志集还是新建日志集进行投递。
日志集	输入新建日志集名称/选择已有日志集。
日志主题操作	选择投递至已有日志主题还是新建日志主题进行投递。CLS 仅支持投递到在云安全中心创建的日志主题。
日志主题	输入新建日志主题名称/选择已有日志主题。

3. 确认无误后，单击**确定**，即可将采集到的日志投递至对应的日志主题。
4. 在日志投递页面，支持查看账号名称/ID、所属部门，以及日志来源、日志类型、来源账号（多账号下）、日志主题、投递状态、投递开关等信息，并且允许编辑已投递任务、（批量）删除任务、（批量）开启/关闭任务、（批量）刷新、日志检索。

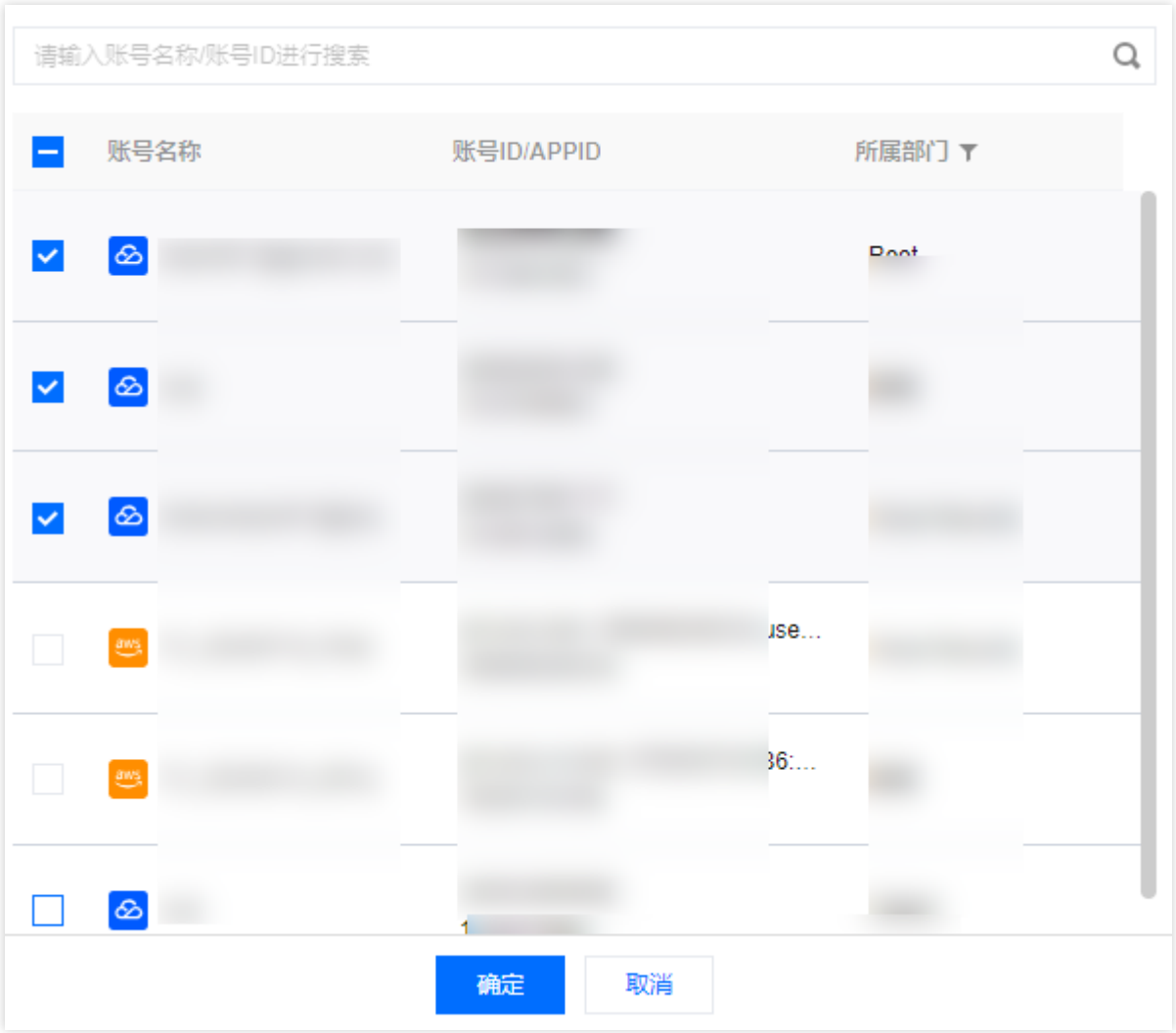
投递及被投递对象

多账号管理

开通 多账号管理 功能后，支持多账号多产品日志投递。

1. 登录 云安全中心控制台，在左侧导览中，单击**日志分析**。
2. 在日志分析页面，单击右上角的**多账号管理**。

3. 在多账号管理页面，选择所需账号，单击**确定**。



场景说明	未配置	配置完成
管理员/委派管理员将全部账号多产品日志统一投递到同一个 Kafka 中。	右上角选中全部账号后配置日志投递，在 Ckafka 公网域名接入、Ckafka 支撑环境接入两种网络接入方式下将自动获取**管理员**的 Ckafka，可选所需腾讯云消息队列。	展示管理员的消息队列状态、用户信息等消息队列详情，同步已配置的日志来源、日志类型、账号来源、投递状态等日志投递详情。
管理员/委派管理员管理其他账号日志，即配置其他账号多产品日志投递。	右上角选中其他账号后配置日志投递，在 Ckafka 公网域名接入、Ckafka 支撑环境接入两种网络接入方式下将自动获取**其他账号**的 Ckafka，可选所需腾讯云消息队列。	展示其他账号的消息队列状态、用户信息等消息队列详情，同步已配置的日志来源、日志类型、投递状态等日志投递详情。
管理员/委派管理员管理当前账号（管理员/委派管理员）日	右上角选中当前账号（管理员/委派管理员）后配置日志投递，在 Ckafka 公网域名接入、Ckafka 支	展示当前账号（管理员/委派管理员）的消息队列状态、用户信息等消息队列详情，同步已配置的日志

志，即配置当前账号多产品日志投递。	撑环境接入两种网络接入方式下将自动获取**当前账号（管理员/委派管理员）**的 Ckafka，可选所需腾讯云消息队列。	来源、日志类型、投递状态等日志投递详情。

单账号管理

仅支持对当前账号进行多产品日志投递。

未配置：在配置日志投递，在 Ckafka 公网域名接入、Ckafka 支撑环境接入两种网络接入方式下将自动获取当前账号的 Ckafka，可选所需腾讯云消息队列。

注意：

若当前账号被管理员/委派管理员管理，则管理员/委派管理员可能编辑当前账号的日志投递配置。

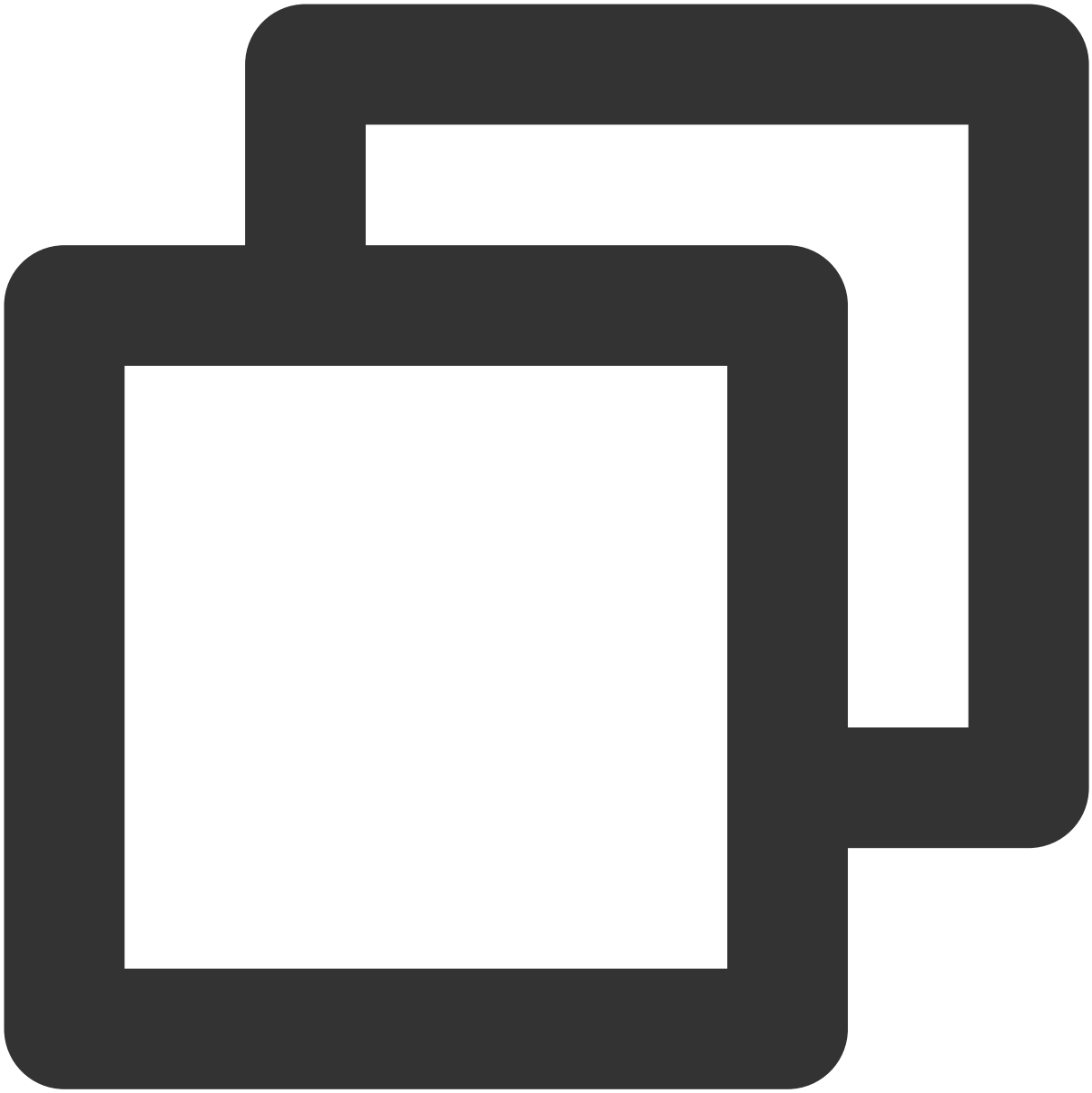
配置完成：展示当前账号的消息队列状态、用户信息等消息队列详情，同步已配置的日志来源、日志类型、投递状态等日志投递详情。

常见问题

日志投递如何收费？

日志投递为云安全中心旗舰版专属，可前往购买日志投递。

公网日志投递出口 IP 白名单



```
106.55.200.0/24
106.55.201.0/24
106.55.202.0/24
81.71.5.0/24
134.175.239.0/24
193.112.130.0/24
193.112.164.0/24
193.112.221.0/24
111.230.173.0/24
111.230.181.0/24
129.204.232.0/24
```

```
193.112.129.0/24
193.112.153.0/24
106.52.11.0/24
106.55.52.0/24
118.89.20.0/24
193.112.32.0/24
193.112.60.0/24
106.52.106.0/24
106.52.67.0/24
106.55.254.0/24
42.194.128.0/24
42.194.133.0/24
106.52.69.0/24
118.89.64.0/24
129.204.249.0/24
182.254.171.0/24
193.112.170.0/24
106.55.207.0/24
119.28.101.0/24
150.109.12.0/24
```

日志投递支持哪些产品哪些日志类型？

产品	日志类型	日志类型
云防火墙	访问控制日志	云防火墙基于用户在互联网边界防火墙、NAT 边界防火墙、VPC 间防火墙和企业安全组间配置的访问控制规则所生成的规则命中记录日志。
	零信任防护日志	云防火墙中用户远程运维登录、Web 服务访问、数据库访问三个模块的零信任防护日志，包括登录与访问服务详情。
	入侵防御日志	云防火墙基于“观察模式”和“拦截模式”所产生和记录的所有安全事件，有“外部入侵，主机失陷，横向移动，网络蜜罐”四个列表，分别查看入站和出站的安全事件详细情况。
	流量日志	云防火墙中互联网边界防火墙和 NAT 边界防火墙基于出站和入站所产生的南北向流量以及 VPC 间的东西向流量情况。
	操作日志	云防火墙中基于该账号内，用户针对安全策略以及开关页所进行的所有操作行为以及操作详情。
Web 应用防火墙	攻击日志	Web 应用防火墙提供攻击日志，记录攻击产生的时间、攻击源 IP、攻击类型及攻击详情等信息。
	访问日志	Web 应用防火墙防护记录域名的访问日志信息。
主机安全	入侵检测日志	主机安全提供木马、高危命令、本地提权及所有登录行为事件等多维度入

		侵检测的安全日志。
	漏洞管理日志	主机安全中漏洞安全事件详细情况的安全日志。
	高级防御日志	主机安全中基于Java 内存马、攻击检测等高级防御的日志。
	客户端相关日志	主机安全检测到客户端异常离线且长达24小时以上未重新上线、客户端被卸载（仅针对 Linux 系统的服务器）的日志。

资产中心

最近更新时间：2024-08-02 10:14:18

资产中心是公有云上的资产管理系统，可以自动同步腾讯云的多种云上资产，手动添加非腾讯云 IP、非腾讯云域名进行统一管理。可自动同步的腾讯云资产详情如下：

资产类型	资产详情
主机资产	云服务器 CVM
	非腾讯云服务器
	轻量应用服务器 Lighthouse
	边缘计算器
容器资产	容器
	本地镜像
	仓库镜像
	主机节点
	集群
	Pod
公网 IP 资产	IP
	高可用虚拟 IP
	弹性公网 IP
	非腾讯云 IP
	弹性 ipv6
	anycast IP
域名资产	域名
	非腾讯云上域名
网络资产-网关	NAT 网关
	VPN 网关

	负载均衡 CLB
	NAT 防火墙
	探针
网络资产-网卡	弹性网卡
私有网络	私有网络 VPC
	子网
云数据库	云数据库 MySQL
	云数据库 Redis
	云数据库 MariaDB
	云数据库 PostgreSQL
	云数据库 MongoDB
其他云资源	云硬盘 CBS
	对象存储 COS
	文件存储
	消息队列
	Elasticsearch Service

更新资产

在 资产中心页面，单击左上角的**资产更新**，云安全中心会自动获取腾讯云上的资产信息，并展示在下发列表；如果资产较多，该过程可能需要3~5分钟，如需更新容器资产需要更长时间。

说明：

资产更新可以自动同步腾讯云上的资产，非腾讯云上资产，请参见 添加云外资产。

搜索资产

在 资产中心页面，支持按照资产分类查询该账号下的主机资产、容器资产、域名资产和公网 IP 资产等情况。

在 资产中心页面，支持在网络结构的视角，查询每个地域下，分别有哪些 VPC，每个 VPC 内分别有哪些资产。

标记核心资产

资产中心会自动识别一部分核心资产，我们也建议您根据自己的业务进行梳理，对关键系统所在的业务，标记为核心资产。

在 资产中心页面，选择目标非核心资产，单击**更多 > 标记为核心资产**。为该资产打上标签，标签会显示在资产名称的右侧。

在 资产中心页面，选择目标核心资产，单击**更多 > 标记非核心资产**。

在 资产中心页面，可以筛选关注核心/非核心资产。云安全中心会自动同步展示资产的防护情况，对应关系为：

主机资产，使用腾讯云主机安全防护。

IP 资产，使用腾讯云防火墙防护。

域名资产，使用腾讯云 Web 应用防火墙防护。

说明：

我们建议您关注自己的核心资产，确保核心资产都得到防护。

添加自定义资产标签

1. 在 资产中心页面，选择目标资产，单击资源标签列下的

，可以添加自定义产品标签。

2. 在编辑标签弹窗中，选择标签键和标签值，单击**确定**。

3. 添加标签后，单击**资源标签**，可以按照自定义标签分类查看资产。

添加云外资产

1. 如需管理非腾讯云资产，可以在 资产中心页面，单击左上角**手动添加资产**。

2. 在手动添加资产弹窗中，输入云外公网 IP、域名资产，勾选服务协议，单击**确定**。

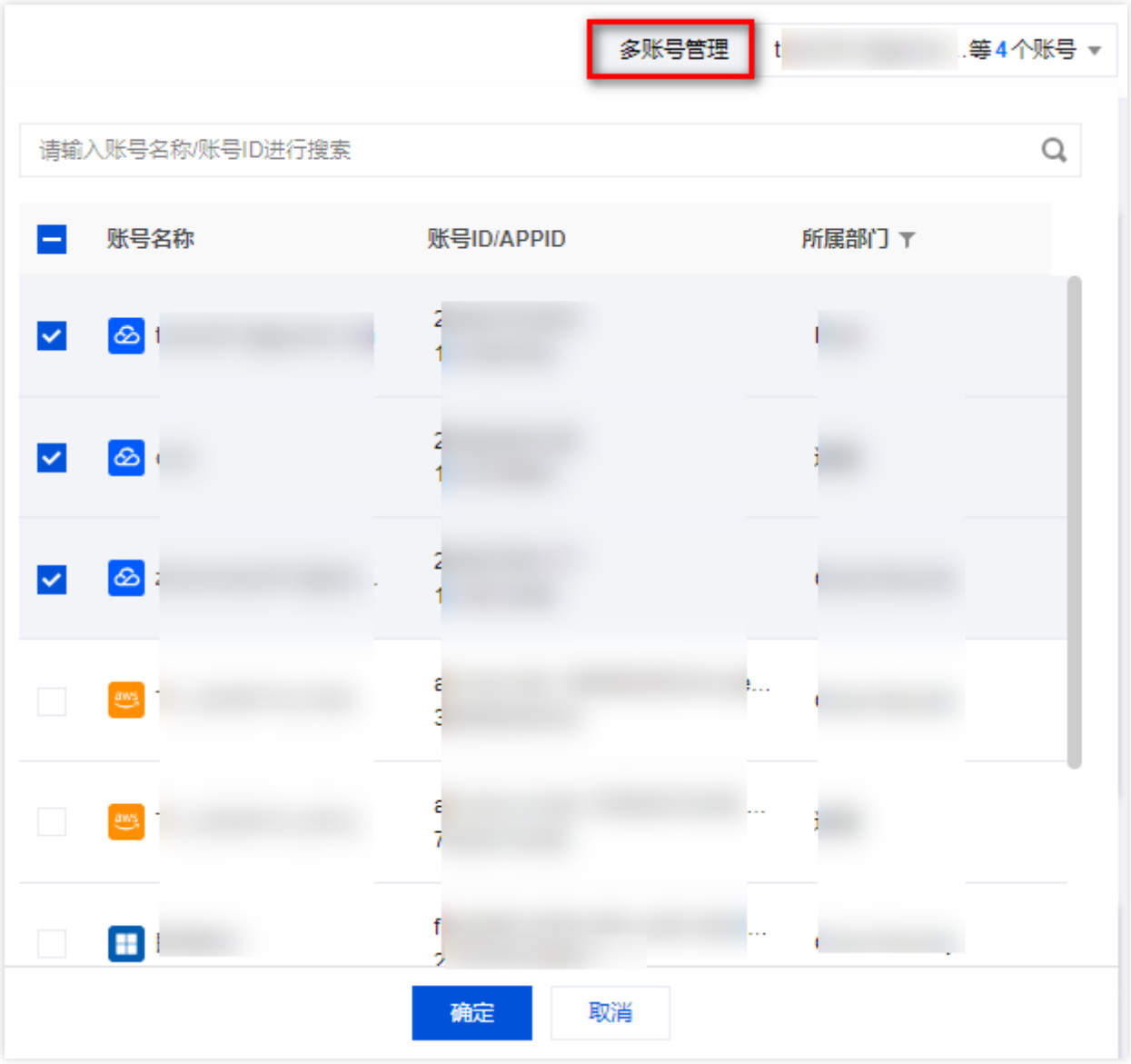
注意：

如需添加云外资产，请 提交工单 联系我们。

请勿添加非本账号所有的资产，如使用他人资产将由本账号归属企业承担法律责任。

管理多账号资产

使用云安全中心 多账号管理功能 后，可以在资产中心查看其他账号的资产。单击左上角**多账号管理**，可以切换账号，或选择所有账号进行查看。


多账号管理
等4个账号
请输入账号名称/账号ID进行搜索
账号名称
账号ID/APPID
所属部门
确定
取消

安全体检
功能简介

最近更新时间：2023-09-21 17:32:10

功能背景

随着网络攻击和数据泄露等安全事件的频繁发生，企业面临着越来越多的安全威胁和风险，并且企业需要落实相关法规政策的要求、不断提升自身的安全能力建设。因此云安全中心提供一键安全体检功能，帮助企业发现云上业务资产6大潜在安全威胁。

应用场景

日常安全体检

为了及时了解安全状况、定期监测网络安全状况，用户可以根据企业的业务状况、安全需求和安全风险，发起安全体检来评估企业的安全状况。安全体检可以帮助企业在早期发现潜在的安全问题，并采取相应的措施来提高企业的安全水平。

功能详情

体检项目

体检项目	项目内容	识别来源
端口风险	针对公网 IP、域名的业务，由云安全中心、云防火墙提供的端口暴露检测能力。	云安全中心
漏洞风险	多年的安全能力建设积累了丰富而全面的漏洞规则库，覆盖 OWASP TOP 10的 Web 漏洞，例如：SQL 注入、跨站脚本攻击（XSS）、跨站请求伪造（CSRF）、弱密码等。同时，系统还具备专业高效的 0Day/1Day/NDay 漏洞检测能力。	云安全中心、联动主机安全和容器安全
弱口令风险	针对主机资产、公网 IP、域名的通用业务，由云安全中心、主机安全提供的弱口令检测。	云安全中心、联动主机安全
云资源配置风险	提供云资源配置风险的自动化检查评估功能，覆盖云服务器、容器、对象存储、云数据库及负载均衡等多种云资源。	云安全中心、联动主机安全和容器安全

风险服务暴露	针对云上向互联网暴露的资产，提供互联网攻击面测绘功能，快速识别云上资产的暴露端口、暴露服务及暴露组件等潜在攻击面。	云安全中心
网站内容风险	快速准确识别敏感图片、文字信息等网站风险内容，针对网站进行挂马、暗链、垃圾广告、矿池等风险的多维度智能检测。	云安全中心

说明：

当识别来源为云安全中心时，我们可以推断出可能存在的漏洞、弱口令和风险服务暴露内容，但需基于端口扫描获取目标系统上开放的端口和服务信息。例如，如果目标主机开放了80端口（HTTP 服务），则可能存在 Web 应用程序漏洞的风险。

体检资产

体检资产	体检项目
云服务器、轻量应用服务器、边缘计算器	漏洞、弱口令、云资源配置风险
已授权的本地镜像、仓库镜像	漏洞风险
组件运行正常的集群	漏洞、云资源配置风险
公网 IP、域名资产	端口、漏洞、弱口令、网站内容风险
负载均衡、子网、MySQL、Redis、MariaDB、PostgreSQL、MongoDB、云硬盘 CBS、对象存储 COS、Elasticsearch Service	云资源配置风险

注意：

风险服务暴露为云安全中心企业版、旗舰版专属能力，不会消耗体检配额；目前检测子网、云硬盘 CBS 的云资源配置风险也不消耗体检配额。

体检消耗

体检资产	体检项目	消耗体检配额
公网 IP、域名资产	漏洞、弱口令、网站内容风险	1次体检消耗体检配额 = 体检资产数
云服务器、负载均衡、MySQL、Redis、MariaDB、PostgreSQL、MongoDB、Elasticsearch Service、对象存储 COS	云资源配置风险	

云安全中心版本功能对比

体检项目	免费版	高级版	企业版	旗舰版
端口风险	✓	✓	✓	✓
应急漏洞	✓	✓	✓	✓
漏洞风险	-	✓	✓	✓
弱口令风险	-	✓	✓	✓
云资源配置风险	-	✓	✓	✓
风险服务暴露	-	-	✓	✓
网站内容风险	-	-	✓	✓
体检配额	20次	400次/月，可扩展	1200次/月，可扩展	4800次/月，可扩展
任务配额	1个	10个	20个	50个，可扩展至不限制

按照表格所述内容，云安全中心将根据版本提供不同体检项目，体检配额、任务配额进行每次安全体检的校验。

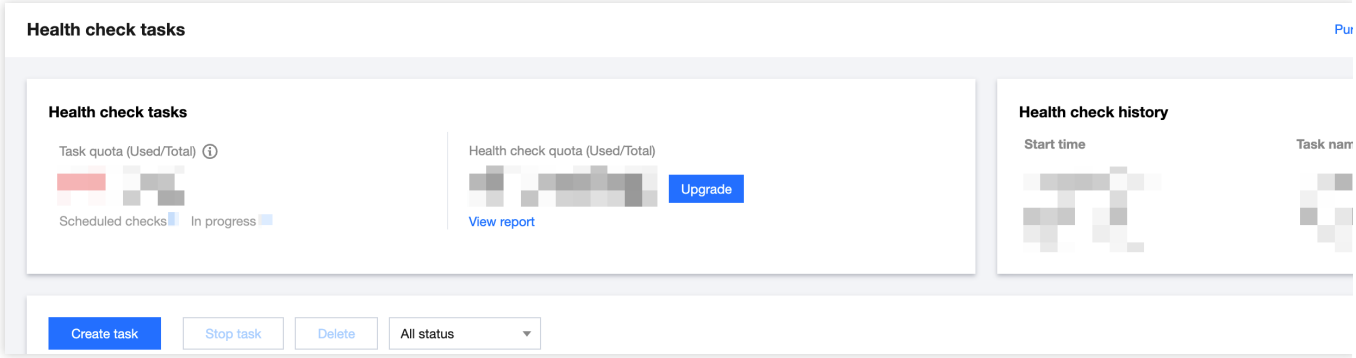
操作指引

最近更新时间：2023-09-21 17:32:59

安全体检入口

安全体检

在 安全体检页面，排查用户云上业务暴露在外的端口、敏感信息及服务，发现潜在漏洞、弱口令、云资源配置等安全威胁，支持多种体检模式选择，安全体检将联动云安全中心、主机安全、容器安全三款产品。



总览体检

在 总览体检页面，涵盖防线建立、资产梳理、风险发现和告警统计四个模块，一站式解决开启试用、资产授权、风险处理和告警处置的问题。

立体防护-应急漏洞

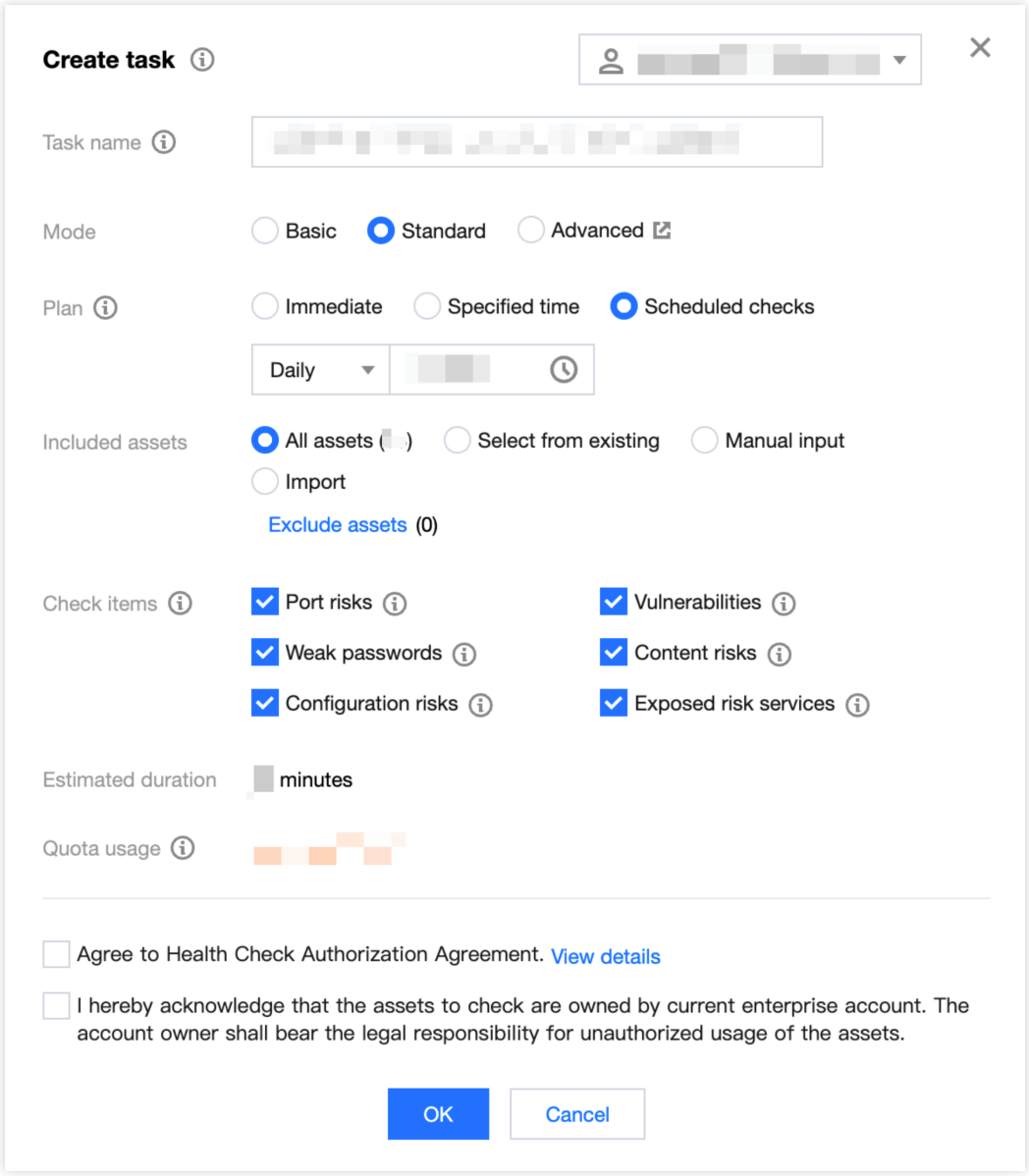
在 云立体防护页面，针对公网 IP、域名资产，由云安全中心提供的应急漏洞风险检测，并梳理互联网漏洞暴露面。

说明：

单个应急漏洞限免2次扫描。

创建任务

1. 登录 云安全中心控制台，在左侧导览中，单击**体检任务**。
2. 在体检任务页面，单击**创建任务**。
3. 在创建资产体检任务弹窗中，配置相关参数，单击**确定**。



参数名称	说明
任务名称	在风险中心中可以直接使用任务名称检索体检结果。
体检模式	快速体检：一键快速发起对端口风险、应急漏洞风险、风险服务暴露进行扫描。 标准体检：支持对端口风险、漏洞风险、弱口令风险、云资源配置风险、风险服务暴露、网站内容风险等6种风险进行选择性扫描。 高级体检：通过创建高级体检任务自定义配置体检项，允许用户手动录入或文件导入方式添加离散端口进行暴露端口检测。针对不同的安全问题进行扫描和检测，及时发现和处理安全漏洞和威胁，提高组织的安全性，排查更加细致和深入的安全风险指标，提高体检的全面性和深度。
体检计划	立即体检：在出现安全问题或有明显安全威胁时进行的体检。这种体检是为了及时了解安全状况、发现安全漏洞或问题，并采取相应的修复措施。立即体检通常是根据安全事件或安全威胁来决定，可以随时进行。

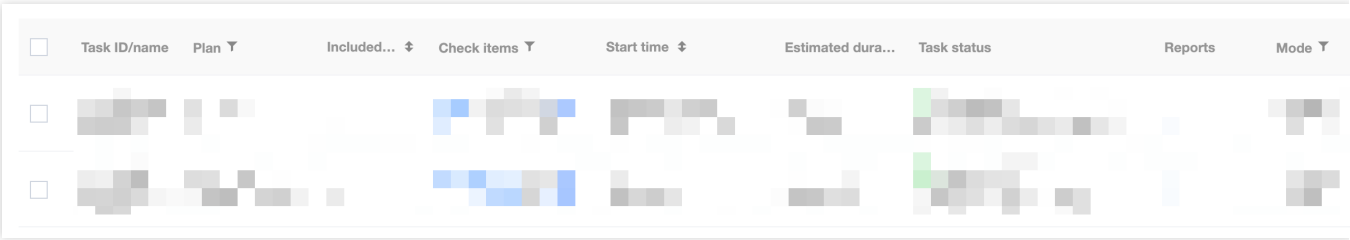
	定时体检：按照设定时间进行的体检，无论是否有明显安全威胁。这种体检是为了定期监测网络安全状况，早期发现潜在的安全问题，并采取预防措施。定时体检的时间间隔可以根据企业的业务状况、安全需求和安全风险来确定。 周期体检：按照一定的周期进行的体检，通常是在特定的时间段或安全生命周期中进行。这种体检是为了全面评估网络安全状况，筛查潜在的安全风险，并采取相应的预防和修复措施。周期体检的时间间隔和内容可以根据不同的安全标准和安全建议来确定。
体检资产	根据实际需求选择。
体检项目	基于端口扫描获取目标系统上开放的端口和服务信息，推断出可能存在的漏洞、弱口令和风险服务暴露内容。例如，如果目标主机开放了 80 端口（HTTP 服务），则可能存在 Web 应用程序漏洞的风险。

编辑报告

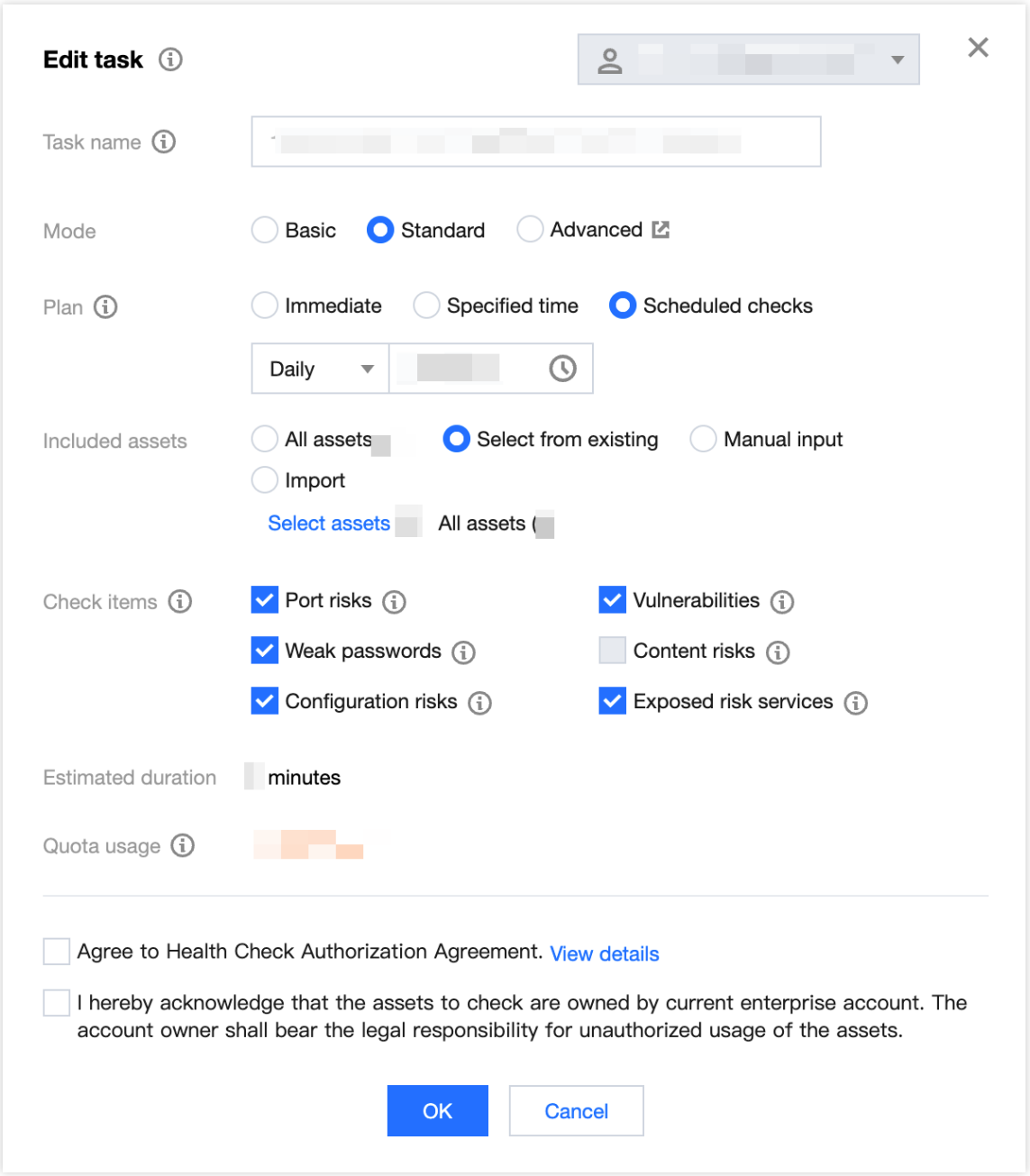
1. 登录 云安全中心控制台，在左侧导览中，单击**体检任务**。
2. 在体检任务页面，选择目标任务，单击**编辑**。

注意：

不支持编辑立即执行的任务、待开始的非周期任务、正在进行中的周期和定时任务。

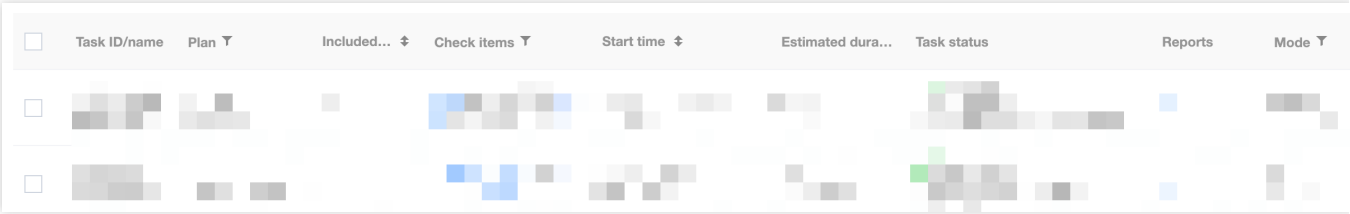


3. 在编辑资产体检任务弹窗中，修改相关参数，单击**确定**。



删除任务

1. 登录 云安全中心控制台，在左侧导览中，单击**体检任务**。
2. 在体检任务页面，选择目标任务，单击**删除**。



3. 在确认删除弹窗中，单击**确定**，即可删除该任务。

注意：

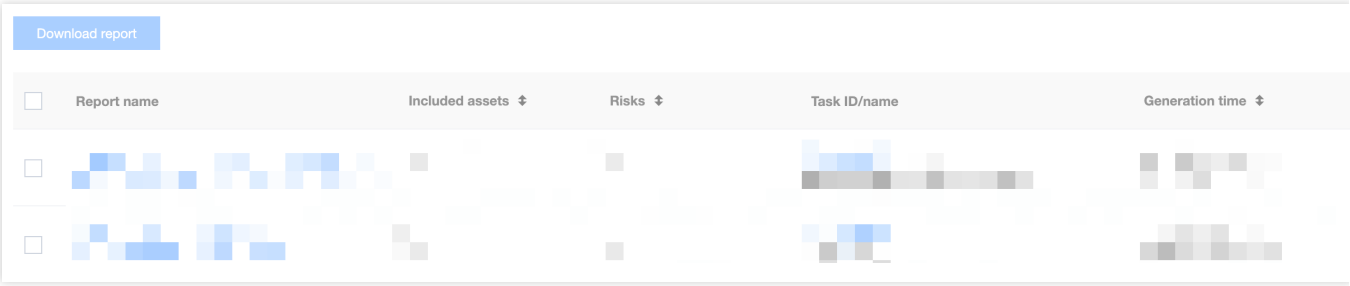
删除任务不可恢复，但会保留任务生成的扫描报告。

不支持删除正在进行中的任务。

下载报告

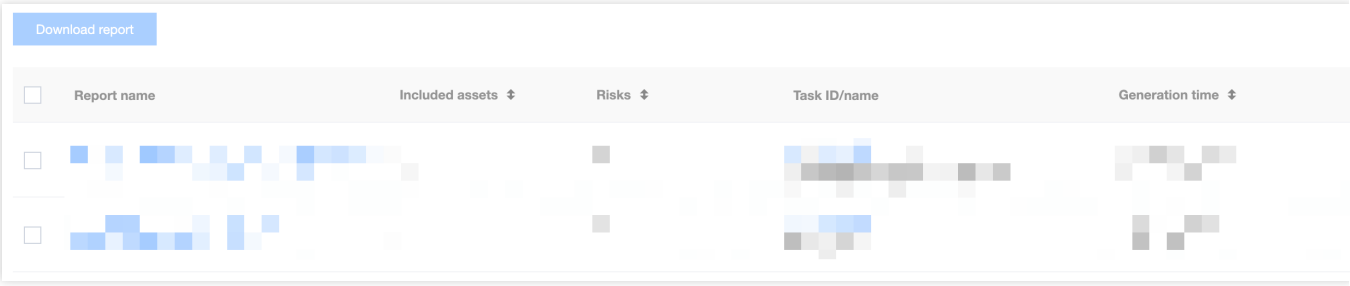
当安全体检任务完成后，云安全中心会自动生成 PDF 格式的安全报告，并提供预览或下载。此外，用户还可以通过关注服务号来随时随地接收报告。

1. 登录 云安全中心控制台，在左侧导览中，单击**报告下载**。
2. 在报告下载页面，选择目标报告，单击操作列的**预览**，可以在线查看报告。

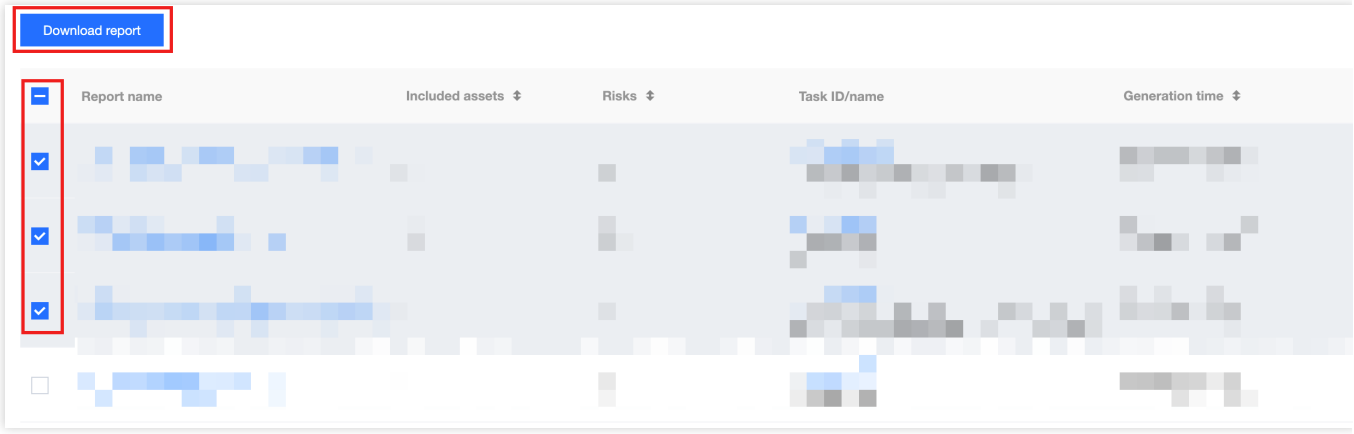


3. 在报告下载页面，支持通过如下两种方式下载报告：

单个：选择目标报告，单击操作列的**下载**。



批量：选择一个或多个报告，单击左上角的**下载报告**。



多账号模式

在多账号模式下，管理员可以指定集团组织下的某个账号为安全体检任务体检消耗配额方，管理员、委派管理员可以为集团组织下任意账号下发安全体检任务，体检配额消耗对象为指定配额方，任务配额占用对象为安全体检任务对应账号。

编辑任务

管理员创建的安全体检任务允许管理员进行编辑操作，委派管理员创建的任务允许管理员、委派管理员进行编辑操作，成员创建的任务允许成员进行编辑操作。由于集团组织下可能存在多个委派管理员，允许进行编辑任务操作的委派管理员应为创建该任务的委派管理员。

删除任务

管理员创建的安全体检任务允许管理员、委派管理员、被创建的成员进行删除操作，委派管理员创建的任务允许管理员、委派管理员、被创建的成员进行删除操作，成员创建的任务允许成员 进行删除操作。由于集团组织下可能存在多个委派管理员，允许进行删除任务操作的委派管理员为所有委派管理员。

添加白名单 IP

最近更新时间：2024-08-02 10:14:18

本文档将为您详细介绍如何将腾讯云安全中心的监测 IP 加入到白名单。

操作场景

云安全中心通过公网进行资产发现和风险监测时会使用模拟黑客入侵攻击的方式。如果您的服务器有安全防护或监控部署（例如 WAF），建议您将腾讯云云安全中心的监测 IP 加入到白名单中，开启扫描访问权限，保证监控服务正常运行，云安全中心扫描节点 IP 为：

129.211.162.110
129.211.162.87
129.211.163.253
129.211.164.19
129.211.166.123
129.211.167.182
129.211.167.200
129.211.167.70
129.211.162.158
129.211.162.23
129.211.166.134
129.211.167.108
129.211.167.181
129.211.166.142
129.211.166.163
129.211.167.128
129.211.167.166
43.139.244.231
43.139.243.246

若您的网站需登录才可以访问，则需要先解除安全策略（即确保所有 IP 都能访问），待您的 cookie 有效性验证通过后再恢复限制。

操作步骤

说明

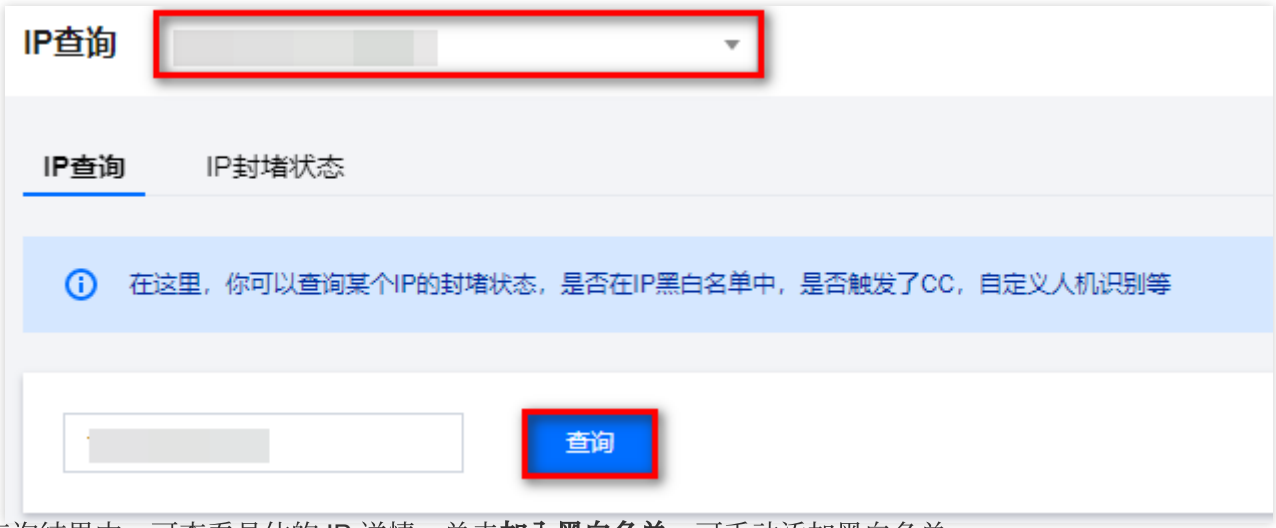
适用于腾讯云 Web 应用防火墙，如果您使用的是其他 WAF 产品，请自行添加。

已购买 Web 应用防火墙。

完成防护域名的添加及正常接入，当前域名处于正常防护，且开启 BOT 管理规则总开关，详情请参见 快速入门。

方式1：通过 IP 查询添加白名单

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，单击 **IP 查询**。
2. 在 IP 查询页面，左上角选择需要防护的域名，输入需要查询的 IP，单击**查询**。



3. 在查询结果中，可查看具体的 IP 详情，单击**加入黑白名单**，可手动添加黑白名单。

4. 在添加黑白 IP 页面，可手动添加白名单。配置相关参数，单击**添加**，即完成白名单添加。

5. 参数说明：

类别：选择**白名单**。

IP 地址：填写需要添加到白名单的地址。

截止时间：填写白名单有效期的截止时间。

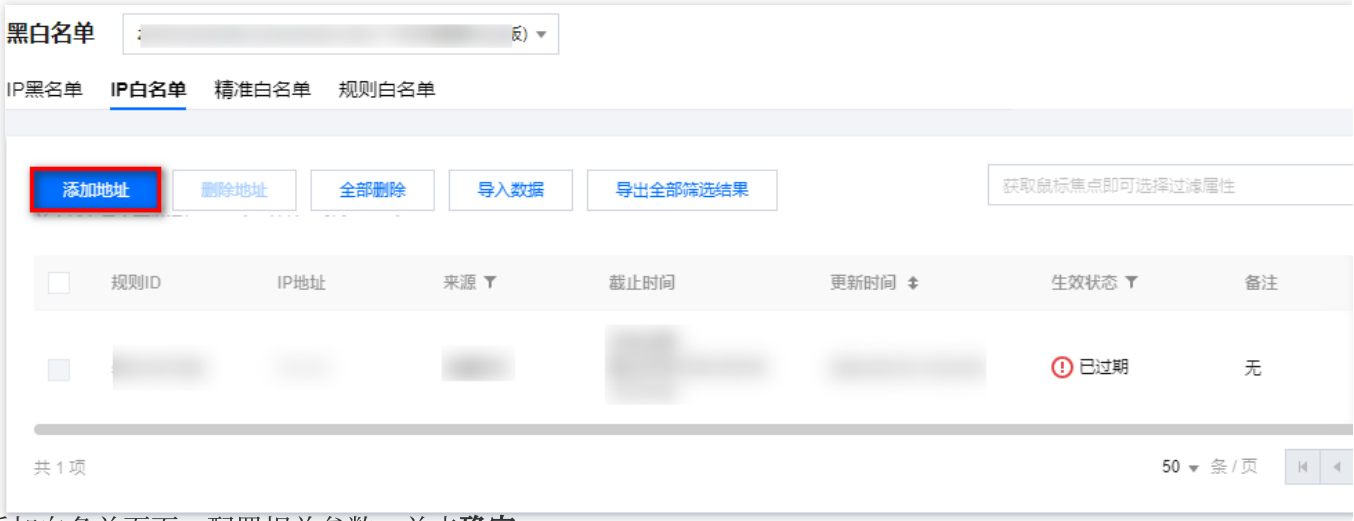
备注：自定义描述。

方式2：直接添加 IP 白名单

登录 Web 应用防火墙控制台，在左侧导航栏中，单击**配置中心 > 黑白名单**，左上角选择需要防护的域名，单击 **IP 白名单**，进入 IP 白名单页面。

手动添加白名单

1. 在 IP 白名单页面，单击**添加地址**，进入添加白名单页面。



2. 在添加白名单页面，配置相关参数，单击**确定**。

字段说明

IP 地址：支持任意 IP 地址，例如10.0.0.10或 FF05::B5；支持 CIDR 格式地址，例如10.0.0.0/16或 FF05:B5::/60，使用换行符进行分隔，一次最多添加20个。

说明

选择域名为 ALL 时，添加的 IP 地址或 IP 段为全局的白名单。

各个版本每个域名规格限制为：高级版1000条/域名、企业版5000条/域名、旗舰版:20000条/域名，每个 IP 地址或者 IP 段占用一条额度。

截止时间：永久生效或限定日期。

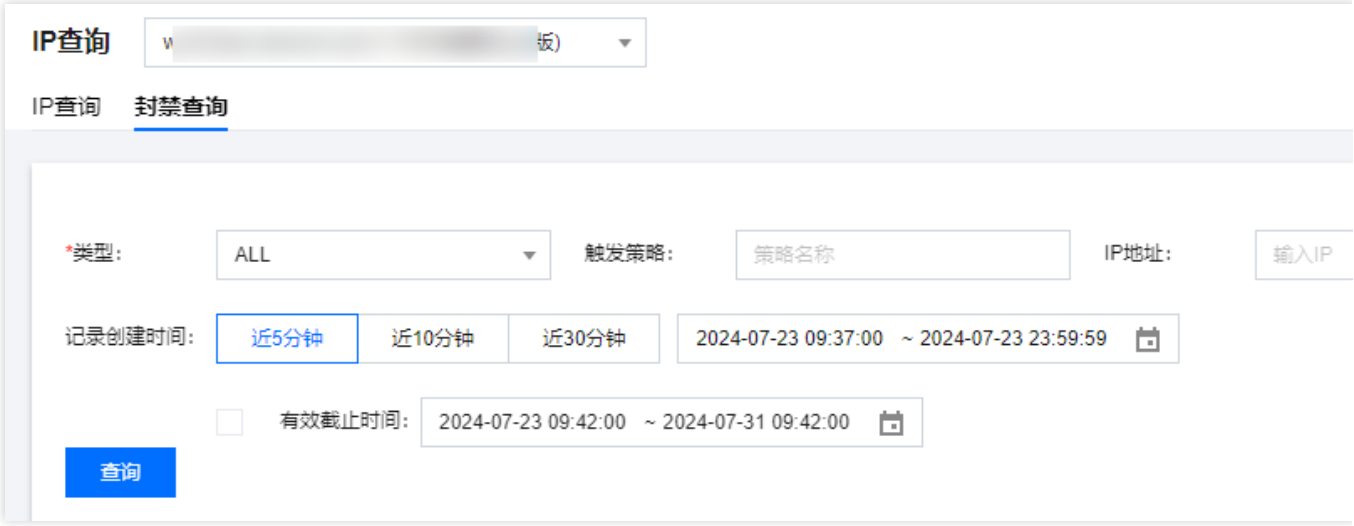
备注：自定义，50个字符以内。

批量导入白名单

1. 在 IP 白名单页面，单击**导入数据**，将弹出“导入 IP 名单”窗口。
2. 在“导入 IP 名单”窗口中，单击**导入**，选择导入白名单文件，上传完成后，单击**确认导入**即可。

方式3：将已封堵 IP 添加白名单

1. 登录 Web 应用防火墙控制台，在左侧导航中，选择 **IP 查询** > **封禁查询**。
2. 在封禁查询页面，输入相关信息，单击**查询**，可以查询云安全中心的相关 IP 信息，即可对已封堵 IP 进行加白操作。



热点问题

最近更新时间：2023-08-29 15:59:14

如何选购体检配额？

为降低资产安全风险，建议每月进行4次自动检测和1次手动全面检测，请根据您的云上资产数量计算购买的资产体检数。

计算消耗体检配额公式

一次安全体检中，选定1个域名、1个 IP 资产分别消耗1个体检配额，共计2个体检配额；若选定云资源配置风险体检项目时，消耗的体检配额为已勾选的云资源数。

体检时间过长是否有异常？

安全体检任务如涉及检测 Web 网站，需要根据您的授权利用爬取技术对您指定的 URL进行内容识别分析，并且执行体检过快容易给业务带来影响，因此体检时间较慢为正常现象。

体检任务被中止后是否还有报告生成？

若安全体检任务被中止则不生成报告，但风险中心中存在已被检测出的风险，可以根据报告 ID 查询到已发现的风险。

体检任务异常是否会消耗体检、占用任务配额？

若安全体检任务无法执行，则占用任务配额但不消耗体检配额；若安全体检任务开始执行，则执行时立即消耗体检配额并占用任务配额。

除了主机和容器之外，配置风险检测还包括哪些云资源的配置检测项？

检查项名称	检查类型	检查对象	风险等级	所属规范	配置风险说明
TDSQL MySQL 版不应该开放公网访问	数据安全	tdmysql	中危	默认安全规范	数据库直接面向公网暴露，可能导致数据库中的敏感数据泄露，安全风险较高；本检查项会检查TDSQL MySQL 版，如果启用了公网访问，则不满足要求。
网络 ACL 不应存在全部放通的入站规则	网络访问控制	subnet	高危	默认安全规范	网络 ACL 是子网粒度的访问控制攻击，如使用全部放通的入站规则，即：入站方向源为0.0.0.0/0，动作为允许的规则，则可能导致该子网开放范围过大，资产产生非必要暴露，本检查项会检查网络 ACL 服务

					入站规则，如存在来源地址为0.0.0.0/0，端口为所有，动作为允许的规则，则不满足要求。
网络 ACL 不建议存在非业务端口全部放通的入站规则	网络访问控制	subnet	高危	默认安全规范	网络 ACL 是子网粒度的访问控制攻击，如使用非业务外（默认：80,443）全部放通的入站规则，即：入站方向源为0.0.0.0/0，端口为80/443以外的端口，动作为允许的规则，则可能导致该子网开放范围过大，资产产生非必要暴露；本检查项会检查网络 ACL 服务入站规则，不应该存在来源地址为0.0.0.0/0，端口为所有或者为非业务端口（默认：80,443），动作为允许的规则。
SSL 证书应在有效期内	数据安全	ssl	中危	默认安全规范	检查 SSL 证书是否超出有效期，证书到期前需及时续费或更换新证书，否则您将无法继续使用 SSL 证书服务，导致数据安全风险，目前检查范围为全部 SSL 证书，您需要根据证书是否关联资源、域名是否还需使用判断是否应修复或删除不再使用的证书。
镜像仓库权限应合理设置	数据安全	repository	中危	默认安全规范，网络安全等级保护三级技术要求	仓库分为公有仓库和私有仓库。 公有仓库可以允许所有互联网中用户进行访问和下载镜像。 如果镜像内部有敏感信息，建议配置成私有仓库，防止信息的泄漏。
云数据库 Redis 应该禁用高危命令	数据安全	redis	中危	默认安全规范	数据库往往安全保护级别较高，若未禁用高危命令（默认：flushall、flushdb、keys、hgetall、eval、evalsha、script），容易出现应用阻塞，数据误删等风险；本检查项会检查 Redis 实例禁用命令配置，若高危命令未禁用（默认包括：flushall、flushdb、keys、hgetall、eval、evalsha、script ），则不符合要求。
Nosql 数据库-Redis 应该开启	数据安全	redis	中危	默认安全规范，网	判定 Redis 数据库的备份功能是否异常，正常情况下，数据应该至少

自动备份				络安全等级保护三级技术要求	每天备份一次。
Nosql 数据库-Redis 不应该对全部网段开放	网络访问控制	redis	高危	默认安全规范，网络安全等级保护三级技术要求	判定 Redis 数据库的服务端口是否对全IP开放访问，正常情况下，数据库服务端口应该只针对可信 IP 或范围开放。
Nosql-Redis 应该位于中国大陆 region	基础设施位置	redis	低危	网络安全等级保护三级技术要求	等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。
云数据库 PostgreSQL 数据库不建议对公网开放访问	网络访问控制	postgres	高危	默认安全规范	数据库直接面向公网暴露，可能导致数据库中的敏感数据泄露，安全风险较高。
关系型数据库-PostgreSQL 应该启用备份	数据安全	postgres	中危	默认安全规范，网络安全等级保护三级技术要求	判定 PostgreSQL 数据库的备份功能是否异常，正常情况下，数据应该至少每天备份一次。
关系型数据库-PostgreSQL 数据库应该位于中国大陆 region	基础设施位置	postgres	低危	网络安全等级保护三级技术要求	等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。
Nosql-MongoDB 应该位于中国大陆 region	基础设施位置	mongodb	低危	网络安全等级保护三级技术要求	等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。
云数据库 MariaDB 应该限制高危命令使用	数据安全	mariadb	中危	默认安全规范	数据库往往安全保护级别较高，若所有账号都拥有全局命令权限 drop、delete，容易出现数据误删除或恶意删除风险，本检查项会检查 MariaDB，如果所有用户都未禁止 drop、delete命令，则不满足要求。
云数据库	网络访问	mariadb	高危	默认安全	数据库直接面向公网暴露，可能导

MariaDB 数据库不建议对公网开放访问	控制			规范	致数据库中的敏感数据泄露，安全风险较高。
云数据库 MariaDB 不应对全部网段开启访问	网络访问控制	mariadb	高危	默认安全规范	云数据库如果对全部网段开启访问，则增大了该数据库的攻击面，增加了数据库被攻击、数据泄露的风险。
关系型数据库-MariaDB 应该启用备份	数据安全	mariadb	中危	默认安全规范，网络安全等级保护三级技术要求	判定 MariaDB 数据库的备份功能是否异常，正常情况下，数据应该至少每天备份一次。
关系型数据库-MariaDB数据库应该位于中国大陆 region	基础设施位置	mariadb	低危	网络安全等级保护三级技术要求	等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。
Elasticsearch 集群不应该开放公网访问	数据安全	es	高危	默认安全规范	Elasticsearch 集群往往存储数据，如开放公网访问，则可能导致不必要的攻击面暴露，产生数据完整性、机密性、可用性风险。
Elasticsearch 集群的 Kibana 组件不应该开放公网访问	数据安全	es	高危	默认安全规范	Elasticsearch 集群往往存储数据，可以通过 Kibana 组件进行数据访问与命令控制，如开放公网访问，则可能导致不必要的攻击面暴露，产生数据完整性、机密性、可用性风险。
安全组不应放通全部网段任何端口	网络访问控制	cvm	高危	默认安全规范，网络安全等级保护三级技术要求	安全组是一种虚拟防火墙，建议根据最小粒度原则，配置防火墙策略。添加服务端口的可信 IP 白名单访问。
CVM 应该位于中国大陆 region	基础设施位置	cvm	中危	网络安全等级保护三级技术要求	等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。
CVM 应使用密钥对登录	身份认证及权限	cvm	中危	默认安全规范	检查 CVM 是否利用 SSH 密钥进行登录，相对于传统的密码登录，

					SSH 密钥登录方式更为方便，且安全性更高。（仅检查 Linux 系统机器）
CVM 上的主机安全代理应正常运行	基础安全防护	cvm	高危	默认安全规范，网络安全等级保护三级技术要求	腾讯云主机安全提供木马查杀、密码破解拦截、登录行为审计、漏洞管理、资产组件识别等多种安全功能。未安装主机安全客户端会面临网络安全，数据泄露的风险。
COS 存储桶建议开启存储桶复制	数据安全	cos	中危	默认安全规范，网络安全等级保护三级技术要求	跨地域复制是针对存储桶的一项配置，通过配置跨地域复制规则，可以在不同存储区域的存储桶中自动、异步地复制增量对象。启用跨地域复制后，COS 将精确复制源存储桶中的对象内容（如对象元数据和版本 ID 等）到目标存储桶中，复制的对象副本拥有完全一致的属性信息。此外，源存储桶中对于对象的操作，如添加对象、删除对象等操作，也将被复制到目标存储桶中。建议进行跨区域复制以提升您的数据容灾能力。
COS 存储桶应配置合理的桶策略	数据安全	cos	高危	默认安全规范，网络安全等级保护三级技术要求	存储桶策略是指在存储桶中配置的访问策略，允许指定用户对存储桶及桶内的资源进行指定的操作。应依据“最小化权限”原则来配置，不推荐对任意用户开放读取操作权限，有遍历文件名或文件被下载的风险。
COS 存储桶应该位于中国大陆 region	基础设施位置	cos	低危	网络安全等级保护三级技术要求	等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。
COS 存储桶应开启防盗链功能	数据安全	cos	中危	默认安全规范，网络安全等级保护三级技术要求	为了避免恶意程序使用资源 URL 盗刷公网流量或使用恶意手法盗用资源，给您带来不必要的损失。建议您通过控制台的防盗链设置配置黑/白名单，对存储对象进行安全防护。
COS 存储桶应	数据安全	cos	中危	默认安全	存储桶支持在对象级别上应用数据

开启服务端加密				规范，网络安全等级保护三级技术要求	加密的保护策略，并在访问数据时自动解密。加密和解密这一操作过程都是在服务端完成，这种服务端加密功能可以有效保护静态数据。建议您对敏感数据类型开启此项配置。
COS 存储桶应开启日志记录	数据安全	cos	中危	默认安全规范，网络安全等级保护三级技术要求	日志管理功能能够记录对于指定源存储桶的详细访问信息，并将这些信息以日志文件的形式保存在指定的存储桶中，以实现对存储桶更好的管理。日志管理功能要求源存储桶与目标存储桶必须在同一地域，目前支持北京、上海、广州、成都、多伦多地域。如果所在区域支持日志管理功能，建议开启此项功能。
COS 存储桶 ACL 公共权限不应该设置为公共读写	数据安全	cos	高危	默认安全规范，网络安全等级保护三级技术要求	存储桶的公有读和公有写权限可以通过匿名身份直接读取和写入存储桶中的数据，存在一定的安全风险。为确保您的数据安全，不推荐将存储桶权限设置为公有读写或公有读私有写，建议您选择私有读写权限。
CLB 绑定的证书应该在有效期内	监控告警	clb	中危	默认安全规范	检查同 CLB 绑定的证书是否过期，如果过期则需要进行替换，以免影响业务正常使用。
CLB 后端服务器组的健康检查状态应保持正常	监控告警	clb	低危	默认安全规范	检测负载均衡 CLB 服务的健康状态，用以判定 CLB 的后端服务是否异常。
CLB 不应转发高危端口	网络访问控制	clb	高危	默认安全规范，网络安全等级保护三级技术要求	应依据“最小服务”原则来设定 CLB 转发策略，只对必要的公共服务端口（如：80、443等）做转发，其他端口不应该进行转发。
CLB 不应对全部网段开启非业务端口访问	网络访问控制	clb	高危	默认安全规范，网络安全等级保护三	检查 CLB 负载均衡实例访问控制配置，对非业务端口开放0.0.0.0/0存在潜在的安全风险，建议对非 http/https 服务启用访问控制。

				级技术要求	
云数据库 MySQL 应该开启数据库审计	数据安全	cdb	中危	默认安全规范	数据库往往存储重要性较高数据，若不开启数据库审计，如发生误操作、恶意操作等问题，难以回溯，发现源头，本检查项会检查 MySQL 数据库是否开启了数据库审计，如果没有开启，则不符合要求。
云数据库 MySQL 网络类型应使用私有网络	数据安全	cdb	中危	默认安全规范	私有网络可基于租户需求，进行不同网络间隔离，数据库往往存储重要性较高的数据，如使用非私有网络，需要维护较为精确的访问控制规则，如果漏维护、错维护，则可能会导致您的数据库产生不必要的暴露，本检查项会检查 MySQL 数据库类型，如果为私有网络，则满足要求，否则不满足。
云数据库 MySQL 数据库应该为管理员账户设置密码	网络访问控制	cdb	高危	默认安全规范	云数据库 MySQL 是数据库服务，如您未对数据库管理员配置账号密码，则该数据库可能被恶意登录，导致数据泄露。
云数据库 MySQL 数据库应该创建非 root 用户使用	数据安全	cdb	中危	默认安全规范	数据库往往存储重要性较高数据，而数据库若只存在 root 账号，没有其他应用账号，说明权限过大，存在误操作或恶意操作影响数据安全的风险，本检查项会检查 MySQL 已经完成初始化的主实例数据库用户列表，如果除了 root 用户以及腾讯云默认创建的 mysql.*以外没有其他用户，则不符合要求。
云数据库 MySQL 数据库实例应在不同可用区进行部署	数据安全	cdb	低危	默认安全规范	云数据库 MySQL 提供多种高可用的架构，选择主备可用区不同时（即多可用区部署），可保护数据库以防发生故障或可用区中断，本检查项会检查 MySQL 数据库，同一个数据库主备实例如果在同一个区域同一个可用区内，则不满足要求。
云数据库 MySQL 数据库	数据安全	cdb	中危	默认安全规范	数据库往往存储重要性较高数据，基于合规要求，数据库审计日志至

审计保留时间应满足要求					少应保留6个月及以上，本检查项会检查 MySQL 数据库审计保留时间，如果保留时间小于审计时间（默认180天），则不符合要求。
云数据库 MySQL 数据库建议限制非 root 用户高危命令权限	数据安全	cdb	中危	默认安全规范	数据库非 root 账号应该进行权限控制，若应用账号拥有高危命令权限，如 drop、delete 等，容易出现数据误删除或恶意删除风险，本检查项会检查Mysql数据库（检查主实例，不检查只读实例和灾备实例），检查 root 用户以外用户的配置，如果配置中允许执行命令：drop，delete，则不满足，对于不存在非 root 用户的实例，本检查项满足，采用其他检查项进行合规检查。
云数据库 MySQL 数据库不建议对公网开放访问	网络访问控制	cdb	高危	默认安全规范	云数据库 MySQL 是数据库服务，数据库直接面向公网暴露，可能导致数据库中的敏感数据泄露，安全风险较高。
关系型数据库-MySQL 应该启用备份	数据安全	cdb	中危	默认安全规范，网络安全等级保护三级技术要求	判定 MySQL 数据库的备份功能是否异常，正常情况下，数据应该至少每天备份一次。
关系型数据库-MySQL 数据库应该位于中国大陆 region	基础设施位置	cdb	低危	网络安全等级保护三级技术要求	等保2.0中8.2.1.1要求应保证云计算基础设施位于中国大陆。
关系型数据库-MySQL 不应该对全部网段开放	网络访问控制	cdb	中危	默认安全规范，网络安全等级保护三级技术要求	判定 MySQL 数据库的服务端口是否对全 IP 开放访问，正常情况下，数据库服务端口应该只针对可信 IP 或范围开放。
CBS 数据盘应该设置为加密盘	数据安全	cbs	中危	默认安全规范，网络安全等级保护三	检查云硬盘的数据盘是否为加密盘。加密盘不仅可以提供更好的数据保密性，同时也可以满足安全合

				级技术要求	规等要求。（仅支持检查非系统盘）
CBS 应开启定期快照功能	数据安全	cbs	中危	默认安全规范，网络安全等级保护三级技术要求	检查云硬盘是否开启了自动定期快照的功能。定期创建快照，可以提高数据的安全性，实现业务的低成本和高容灾。
子账号应使用 MFA 进行登录保护	基础安全防护	cam	中危	默认安全规范	子账号未绑定 MFA 设备，则在登录保护或操作保护中无法使用 MFA 进行二次验证，存在风险，本检查项会检查子账号，是否绑定了 MFA 设备，如果没有绑定，则不满足要求。
子账号应使用 MFA 进行操作保护	基础安全防护	cam	中危	默认安全规范	子账号未绑定 MFA 设备，则在登录保护或操作保护中无法使用 MFA 进行二次验证，存在风险，本检查项会检查子账号，是否绑定了 MFA 设备，如果没有绑定，则不满足要求。
子账号密码应定期更换	基础安全防护	cam	中危	默认安全规范	子账号密码是用户访问的主要凭据，长期(90天)不更换密码，会导致密码泄露的可能性增加。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
应删除废弃的子账号	基础安全防护	cam	高危	默认安全规范	子账号长期(30天)不登录使用，可能该账户已经被废弃，废弃账户可能被不再属于您组织的成员使用，导致您的资产不可用或数据泄露。
应该删除子账号废弃的 API 密钥	基础安全防护	cam	高危	默认安全规范	子账号 API 密钥长期(30天)不使用，可能该 API密钥已经被废弃，废弃 API 密钥可能被不再属于您组织的成员使用，导致您的资产不可用或数据泄露。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
应该删除废弃的协作者 API 密钥	基础安全防护	cam	高危	默认安全规范	协作者的 API 密钥长期(30天)不使用，可能该 API 密钥已经被废弃，废弃 API 密钥可能被不再属于您组织的成员使用，导致您的资产不可

					用或数据泄露。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
应该定期更换子账号的 API 密钥	基础安全防护	cam	中危	默认安全规范	子账号 API 密钥是编程访问的主要凭据，长期(90天)不更换密钥，会导致密钥泄露的可能性增加。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
应定期更换协作者的 API 密钥	基础安全防护	cam	中危	默认安全规范	协作者 API 密钥是编程访问的主要凭据，长期(90天)不更换密钥，会导致密钥泄露的可能性增加。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
协作者应使用 MFA 进行登录保护	基础安全防护	cam	中危	默认安全规范	协作者未绑定 MFA 设备，则在登录保护或操作保护中无法使用 MFA 进行二次验证，存在风险；本检查项会检查协作者，是否绑定了 MFA 设备，如果没有绑定，则不满足要求。
协作者应使用 MFA 进行操作保护	基础安全防护	cam	中危	默认安全规范	协作者未绑定 MFA 设备，则在登录保护或操作保护中无法使用 MFA 进行二次验证，存在风险；本检查项会检查协作者，是否绑定了 MFA 设备，如果没有绑定，则不满足要求。
协作者应开启登录保护	基础安全防护	cam	中危	默认安全规范	协作者账号不归属于您的账号管控体系中，账号安全风险不可控，如协作者账号泄露，可能会导致该协作者有权限的资产被破坏或者数据泄露，开启登录保护后，对协作者登录进行二次校验，降低协作者账号泄露导致的风险。
协作者应开启操作保护	基础安全防护	cam	中危	默认安全规范	协作者账号不归属于您的账号管控体系中，账号安全风险不可控，如协作者账号泄露，可能会导致该协作者有权限的资产被破坏或者数据泄露，开启操作保护后，对协作者敏感操作进行二次校验，降低协作者账号泄露导致的风险。
协作者不应该同	基础安全	cam	高危	默认安全	协作者账号具备两种访问方式，如

时使用编程访问与用户界面访问	防护			规范	同时开启，则可能导致一个账号的暴露面增加，且可能导致机器账号与人工账号混用，增加账号被恶意使用的可能性。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
具备高风险权限的协作者应开启登录保护	基础安全防护	cam	高危	默认安全规范	协作者账号不归属于您的账号管控体系中，账号安全风险不可控，且高权限协作者具有超级管理员权限，如协作者账号泄露，您的云上资产会面临非常高的安全风险，开启登录保护后，对协作者登录进行二次校验，降低协作者账号泄露导致的风险。
具备高风险权限的协作者应开启操作保护	基础安全防护	cam	高危	默认安全规范	协作者账号不归属于您的账号管控体系中，账号安全风险不可控，且高权限协作者具有超级管理员权限，如协作者账号泄露，您的云上资产会面临非常高的安全风险，开启操作保护后，对协作者敏感操作进行二次校验，降低协作者账号泄露导致的风险。
建议子账号的API 密钥不超过1个	基础安全防护	cam	低危	默认安全规范	一个子账号维护多个 API 密钥，会增大密钥的暴露面，增加密钥泄露的风险。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
高风险权限子账号应该开启登录保护	基础安全防护	cam	高危	默认安全规范	高权限子账号具备超级管理员权限，如果高风险子账号被恶意登录，您云上的资产会面临非常高的风险，登录保护为您的子账号提供账号登录的二次校验，降低高风险子账号被恶意登录的可能性。
高风险权限子账号应该开启操作保护	基础安全防护	cam	中危	默认安全规范	高权限子账号具有超级管理员的权限，主账号误操作或被盗用后恶意操作，可能会影响您云上的所有资产，操作保护为您的敏感操作提供二次校验，降低误操作或恶意操作的风险。
高风险权限子账	基础安全	cam	低危	默认安全	高权限子账号具有超级管理员的权

号不建议启用 API 密钥	防护			规范	限，而 API 密钥是账号编程访问的身份凭证，通常会被写入配置中，易泄露，如果 API 密钥泄露，攻击者可利用该密钥操控您在云上的所有资产，风险较高。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
不能同时为子账号开启编程访问与用户界面访问	基础安全防护	cam	中危	默认安全规范	子账号具备两种访问方式，如同时开启，则可能导致一个账号的暴露面增加，且可能导致机器账号与人工账号混用，增加账号被恶意使用的可能性。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。
主账号应使用 MFA 进行登录保护	基础安全防护	account	中危	默认安全规范	主账号默认拥有账号下腾讯云所有资源，具有超级管理员的权限，如果主账号被盗用，您的云资产会面临非常高的安全风险，MFA（Multi-Factor Authentication）即多因子认证，是一种简单有效的安全认证方法，它可以在用户名和密码之外，再增加一层保护，登录保护可使用腾讯云虚拟 MFA 设备，降低主账号被恶意登录的可能性。
主账号应使用 MFA 进行操作保护	基础安全防护	account	中危	默认安全规范	主账号默认拥有账号下腾讯云所有资源，具有超级管理员的权限，主账号误操作或被盗用后恶意操作，可能会影响您云上的所有资产，MFA（Multi-Factor Authentication）即多因子认证，是一种简单有效的安全认证方法，它可以在用户名和密码之外，再增加一层保护，操作保护中启用虚拟 MFA，可为您的敏感操作提供二次校验，降低误操作或恶意操作的风险。
主账号应开启登录保护	基础安全防护	account	高危	默认安全规范	主账号默认拥有账号下腾讯云所有资源，具有超级管理员的权限，如果主账号被盗用，您的云资产会面临非常高的安全风险，登录保护为您的账号登录提供二次校验，降低主账号被恶意登录的可能性。

主账号应开启操作保护	基础安全防护	account	中危	默认安全规范	主账号默认拥有账号下腾讯云所有资源，具有超级管理员的权限，主账号误操作或被盗用后恶意操作，可能会影响您云上的所有资产，操作保护为您的敏感操作提供二次校验，降低误操作或恶意操作的风险。
主账号建议开启异地登录保护	基础安全防护	account	低危	默认安全规范	主账号默认拥有账号下腾讯云所有资源，具有超级管理员的权限，如果主账号被盗用，您的云资产会面临非常高的安全风险，异地登录保护为您的账号登录提供登录地校验，如发现异地登录，则会进行二次校验，降低主账号被恶意登录的可能性。
主账号不应该启用 API 密钥	基础安全防护	account	高危	默认安全规范	主账号默认拥有账号下腾讯云所有资源，具有超级管理员的权限，而API 密钥是账号编程访问的身份凭证，通常会被写入配置中，易泄露，如果API 密钥泄露，攻击者可利用该密钥操控您在云上的所有资产，风险较高。本检查项涉及的账号信息同步可能存在延时，建议检查间隔4小时以上。

用户行为分析（UEBA）

最近更新时间：2024-08-02 10:14:18

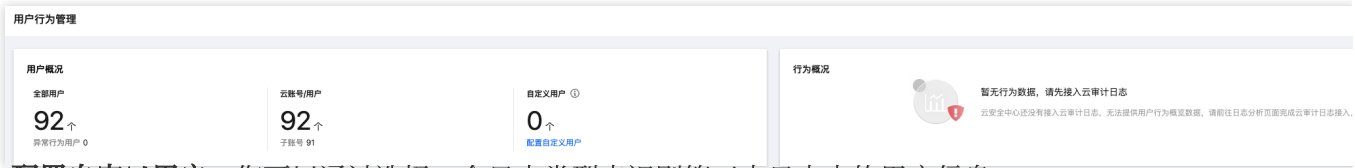
用户行为分析（UEBA）功能提供了对云用户操作行为和云 API 调用的可视化审计与监控，能够针对 AKSK 异常调用、高风险接口调用、用户高风险操作、未授权服务使用、权限提升等风险行为进行检测和告警，识别因用户异常行为和风险 API 调用等引起的安全风险。

功能特性

审计日志接入：通过多云多账户功能模块，可以获取云账户对应的用户列表和云外用户信息。通过操作审计日志，可以获取所有云用户的行为记录，并识别用户行为字段。此外，还能对云用户的操作行为和云 API 调用日志进行可视化监控和实时审计。
风险检测：对 AKSK 异常调用、高危接口调用、用户高危操作、未授权服务使用、权限提升等风险行为进行检测和告警。同时，支持用户自定义启用或禁用检测规则，并自定义添加检测策略。
安全可视化：从异常行为和异常账号等方面展示近7天内检测到的风险数据，客户可以通过对比数据快速了解风险趋势，并及时进行风险管理。

用户概况

1. 登录 云安全中心控制台，在左侧导览中，单击**用户行为分析（UEBA）**。
2. 在用户行为分析（UEBA）页面，支持对您所有用户的行为分析，用户包括您的主账号、子账号、协作者。



3. 单击**配置自定义用户**，您可以通过选择一个日志类型来识别第三方日志中的用户信息。

注意：

此操作需要 配置日志接入 才能进行。

4. 在自定义用户对话框中，配置日志类型、用户 ID 等参数。

参数名称	说明
日志类型	在完成 配置日志接入 后，用户可以在此部分选择要为其添加策略的自定义用户，以审计所需的日志类型。 日志类型包括云防火墙的访问控制日志、操作日志、流量日志、入侵防御日志、零信任防护日志，Web 应用防火墙的攻击日志、访问日志，主机安全的客户端上报日志、云安全中心的内容风险日志、风险服务暴露日志、弱口令风险日志、配置风险日志、漏洞风险日志，SaaS 化堡垒机的资产登录日志、产品登录日志，或其他的自定义日志。
用户 ID	选择代表用户 ID 的字段。
用户名称	选择代表用户名称的字段，可不选。
操作对象	请在当前的日志字段中，选择最多3个字段用于体现用户行为操作的对象，建议选择服务、产品、资源、实例、接口等信息，允许为空。
操作方式	请在当前的日志字段中，选择最多3个字段用于体现用户行为操作的方式，建议选择密钥、AKSK 等信息，允许为空。 配置完成之后，自定义用户部分的用户数据会根据配置信息进行刷新。

5. 单击**确定**，配置完成之后，自定义用户部分的用户数据会根据配置信息进行刷新。

行为概况

1. 登录 云安全中心控制台，在左侧导览中，单击**用户行为分析（UEBA）**。
2. 在行为概况模块中，使用功能之前，需先接入日志，单击**立即接入**。

3. 在接入日志源对话框中，日志来源可选择操作和自定义日志来源。

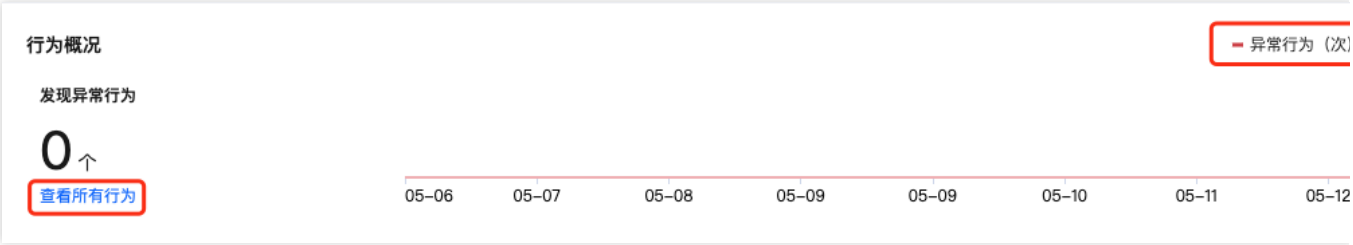
说明：

如果在日志分析已经已经接入了这两类日志，则在用户行为分析（UEBA）功能模块可免去此部分的配置工作，直接添加策略。

日志来源	参数名称	说明
云审计	存储时长	默认为180天，可选择7天、30天、60天、90天或180天。
	接入方式	默认为通过跟踪集接入。
	跟踪集	仅展示可用且存储到 COS 的跟踪集，如已关闭，请先前往 COS 产品开启。
自定义日志来源	日志来源名称	需自定义日志来源名称。
	存储时长	可选择7天、30天、60天、90天或180天。
	接入方式	默认为通过自有 COS 桶接入。
	COS 存储桶	将所需接入的日志写入所选的 COS 存储桶，并配置权限，允许云安全中心服务角色进行读取。云安全中心将自动定时读取日志文件。还可以通过 提交工单 来定制读取方式，或前往 COS 产品页面创建一个新的存储桶。
	存储目录	为提升读取性能，建议在选定的目录下，进一步按照 yyyy/mm/dd 的格式组织日志文件路径，我们会根据日历自动读取对应自然日的文件；日志格式支持 J格式，用‘/n’分割行，支持 gzip 压缩。
	日志样例	建议您输入日志样例供系统参考。系统会根据输入的样例进行字段解析，您可以进一步查看并选择指定字段及排序操作，这将提升日志的读取性能及解析的正确性。

	时间戳	选择日志样例及其对应的时间戳格式。

4. 单击**确定**后，系统将完成日志接入。接下来，系统策略和用户自定义策略会根据实时接入的日志，对异常行为和异常账号进行审计。如果发现异常行为，将更新下图中的异常行为数据和趋势图。单击**查看所有行为**，可跳转至日志分析查看日志详情。



查看策略

1. 登录 云安全中心控制台，在左侧导览中，单击**用户行为分析（UEBA）**。
2. 在用户行为分析（UEBA）列表中，提供系统策略来检测异常行为和异常账号，可针对 AKSK 异常调用、高危接口调用、用户高危操作、未授权服务使用、权限提升等风险行为进行检测告警。

参数名称	说明
策略 ID	系统默认生成。
策略名称	系统策略由产品后台定义；用户自定义策略由用户定义。
策略类型	包括系统策略和自定义策略。
告警等级	包括严重、高危、中危、低危和提示。

策略内容	解释策略的检测内容。
开关	用户可自定义开启或关闭此条策略。
命中次数	统计近7天的策略命中纪录。单击可跳转告警中心查看告警详情，告警来源为用户行为分析（UEBA）。
操作	系统策略不允许编辑和删除。用户自定义策略可编辑或删除策略。

添加策略

1. 登录 云安全中心控制台，在左侧导览中，单击**用户行为分析（UEBA）**。
2. 在用户行为分析（UEBA）页面，单击**添加策略**，可自定义用户行为分析策略。
3. 在自定义策略页面，配置相关参数，单击**确定**。

参数名称	说明

策略名称	用户自定义策略名称，不超过20个字符。
用户类型	云账号或自定义用户。 选择云账号时，可选择的日志类型包括云审计读操作日志和云审计写操作日志。 选择自定义用户时，可选择的日志类型即自定义用户中配置的日志类型。
发生时间	选项包括每10分钟、每小时、每天、每周、每月。
发生事件	可按语句检索或过滤检索进行配置。
告警名称	可选用户异常行为。
告警等级	包括严重、高危、中危、低危和提示。
操作者	请在当前的日志字段中，选择最多3个字段用于体现操作者的信息，建议选择 IP、账号、用户相关字段，不允许为空。
操作对象	请在当前的日志字段中，选择最多3个字段用于体现用户行为操作的对象，建议选择服务、产品、资源、实例、接口等信息，允许为空。
操作方式	请在当前的日志字段中，选择最多3个字段用于体现用户行为操作的方式，建议选择密钥、AKSK等信息，允许为空。