漏洞扫描（CSIP）

产品文档

目录

漏洞扫描（CSIP） 3
- 产品简介 3
  - 产品简介 3
- 快速入门 4
  - 快速入门 4
- 应用场景 5
  - 云上安全预防 5
- 操作指南 6
  - 安全概览 6
  - 资产中心 8
  - 风险中心 17
  - 安全体检 19
    - 功能简介 19
    - 操作指引 21
    - 热点问题 24
  - 报告下载 25
  - 操作日志 27
- 故障处理 28
  - 根据故障反馈关联策略解除权限问题 28

产品简介
产品简介

什么是漏洞扫描

漏洞扫描（Cloud Security Integrated Platform，CSIP）是一站式安全管理平台，通过资产中心、风险中心、安全体检等，帮助用户实现事前威胁检测、事中响应处置、事后溯源分析的安全运营闭环，一键搞定安全问题。

- 资产中心：支持管理主机资产、IP资产、域名资产和网络资产等。
- 漏洞与风险中心：漏洞风险、端口风险、弱口令风险、风险服务暴露等。

产品功能

资产中心

最全资产管理系统，支持自动同步云服务商的主机资产、IP资产、域名资产和网络资产等，手动添加非云服务商 IP、非云服务商域名进行统一管理。

漏洞与风险中心

创建资产体检任务，检测端口风险、漏洞风险、弱口令风险、风险服务暴露等，并将以上风险信息分类进行管理。支持发起定时任务、周期任务，持续监测企业安全情况。

安全体检

管理资产体检任务，对资产体检任务进行编辑、暂停、删除。

报告下载

对于已经完成的资产体检任务，漏洞扫描会自动生成 PDF 格式的安全报告，提供预览或下载。

快速入门
快速入门

步骤1：登录注册

若没有账号，请参考 账号注册教程，进行账号注册。

步骤2：立即体验

账号注册完成，在云产品导航页进入 漏洞扫描控制台，即可使用漏洞扫描，对云上资产安全情况进行盘点，对云上安全产品的安全事件进行统一监测。

步骤3：使用漏洞扫描

开通漏洞扫描高级版 后，即可使用漏洞扫描完整功能，实现云上安全的一站式自动化及可视化安全运营管理。

应用场景
云上安全预防

适用场景

业务上云之后，由于云服务商自身的特点以及业务上频繁的变更可能会带来很多威胁，例如云上服务器直接面向公网开放了 Telnet 访问；又例如云上数据库直接面向公网开放了服务访问，同时还未加密码验证。针对此类问题，需要对云上的各种安全情况进行集中的安全预防与检查。而漏洞扫描则集成了此类功能，可为客户提供完整的云上安全预防能力。

解决方案

漏洞扫描提供端口风险、漏洞风险、弱口令风险、风险服务暴露四类功能对客户云上资源做集中的安全预防管理，分别覆盖关键信息泄露、云上服务暴露、云服务器的漏洞等云上主要安全问题。同时结合集中的云上资产管理能力，可以为客户提供全局的资产风险管理视角。

操作指南
安全概览

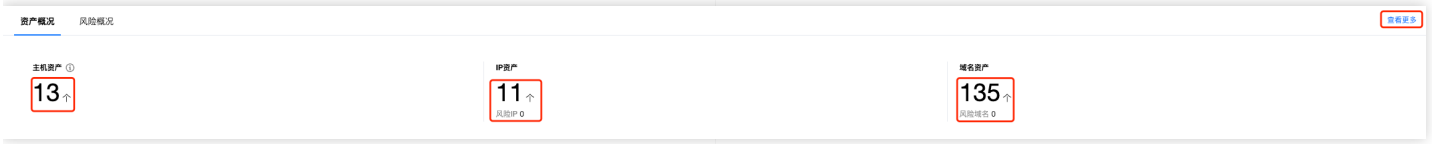
安全概览页面展示了登录漏洞扫描控制台的账号信息、资产概览、风险概览和体检任务概况。

账号信息

账号信息包括账号名称、账号UIN和创建时间。展示该账号累计防护时长，以及预计取消订阅按钮。取消订阅后产品控制台无法访问，请谨慎操作。

资产概况

资产概况展示主机资产数量、IP资产数量、和域名资产数量。点击各资产数据，可跳转资产中心对应的资产列表页面。点击查看更多，跳转资产中心。

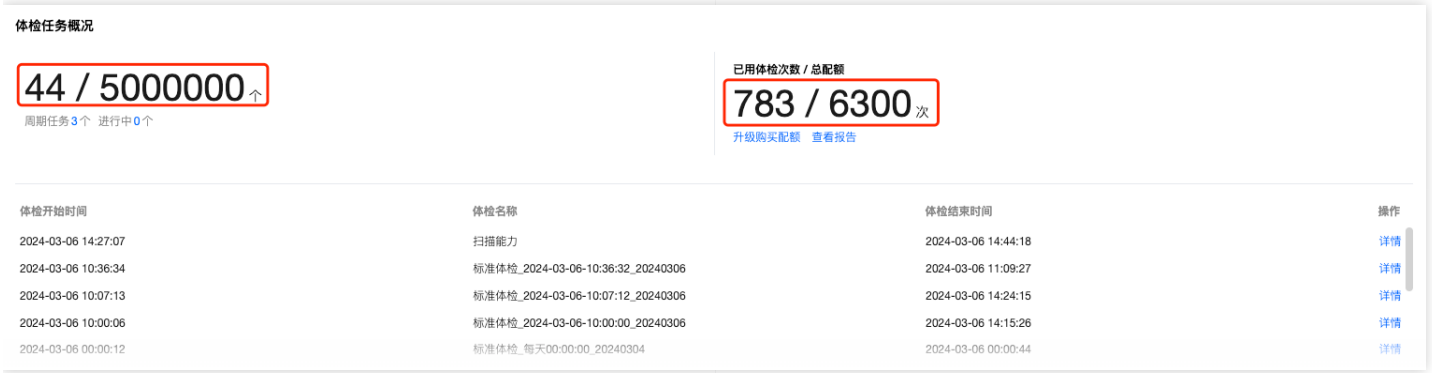


风险概况

风险概况展示端口风险、漏洞风险、弱口令风险和风险服务暴露的数量，以及每类风险的高危风险数量。同时可展示这四类风险近24小时、7天、30天风险趋势图。点击各类风险数据，可跳转风险中心对应风险列表页面。点击查看更多，跳转风险中心。

体检任务概况

展示任务数量和任务配额、已用体检次数和体检总配额、安全体检任务执行记录。点击周期任务和进行中任务数据，可跳转安全体检页面查看任务。点击查看报告，可跳转报告下载页面预览或下载报告。



体检报告概况

展示体检报告数量和待查看体检报告的数量。点击数量，可跳转报告下载页面预览或下载报告。

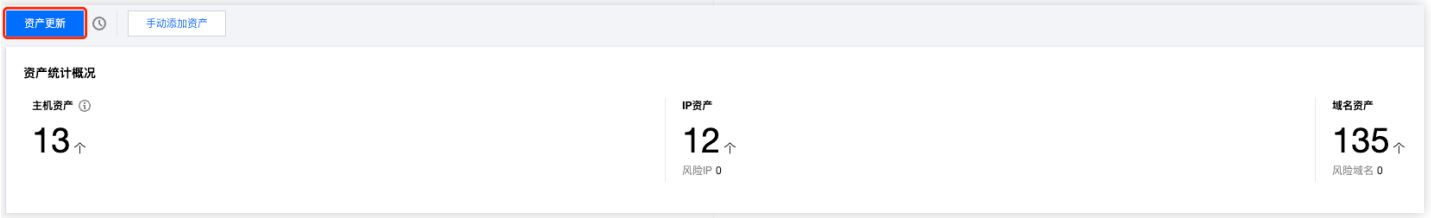
资产中心

资产中心是云服务商上的资产管理系统，可以自动同步云服务商的多种云上资产，手动添加非云服务商 IP、非云服务商域名进行统一管理。可自动同步的云服务商资产详情如下：

资产类型	资产详情
主机资产	云服务商服务器
IP资产	内网、公网、弹性IP、未知
域名资产	CLB-WAF、CLB、SAAS-WAF、未知
网络资产	网卡、私有网络

更新资产

单击左上角的资产更新，漏洞扫描会自动获取云服务商上的资产信息并更新资产列表。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。



更新云外资产

如需管理非云服务商资产，可单击左上角添加云外资产。

支持手动录入或文件导入云外公网IP、内网IP、域名资产。勾选服务协议，单击确定。
选择手动录入时，可输入公网IP地址、内网IP地址、Web网站域名、API域名，手动输入使用回车换行，每行一个；

最多支持输入1000行，外部复制粘贴多个地址，请用英文逗号”,“分隔；内网IP和内网域名请用vpc-所属私有网络 | IP、vpc-所属私有网络 | 域名的格式，例如vpc-h2****** | 10...；*不支持CIDR地址，若输入重复IP，后台将自动合并。*

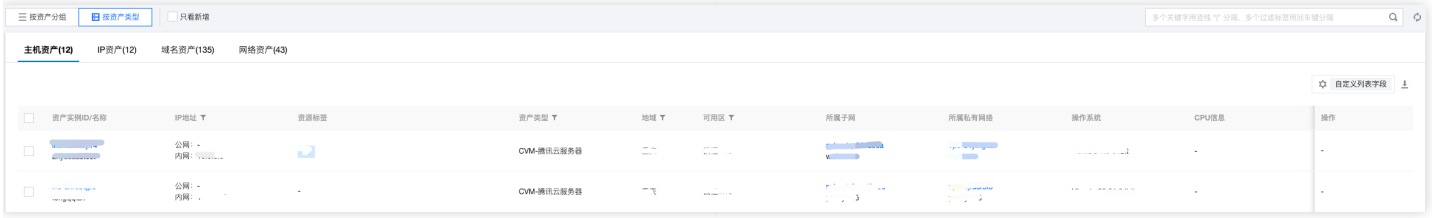
选择文件导入时，文件格式要求如下：

1、请上传xlsx/csv/txt格式文件，大小100M以内；

*2、文件中包含的地址，请使用回车换行，每行一个；内网IP和内网域名请用vpc-所属私有网络 | IP、vpc-所属私有网络 | 域名的格式，例如vpc-h2***** | 10...*；不支持CIDR地址，若输入重复地址，后台将自动合并。

查看资产

可按资产分组和按资产类型查看资产。



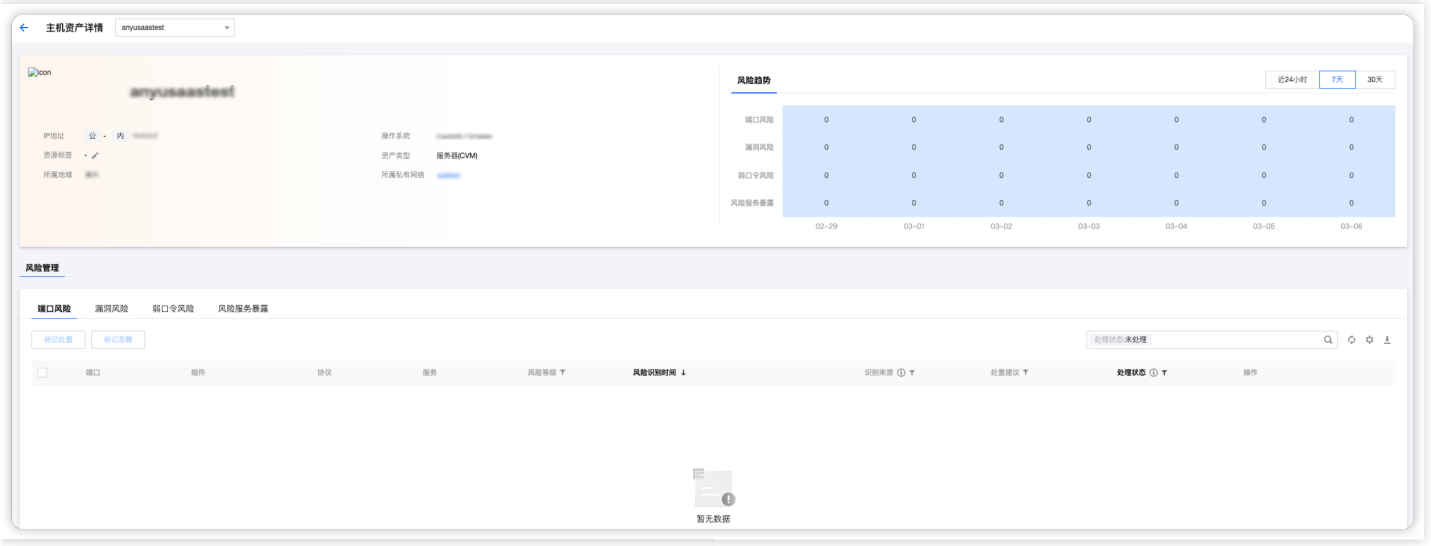
1.按资产类型

按资产类型，可查看主机资产、IP资产、域名资产和网络资产。

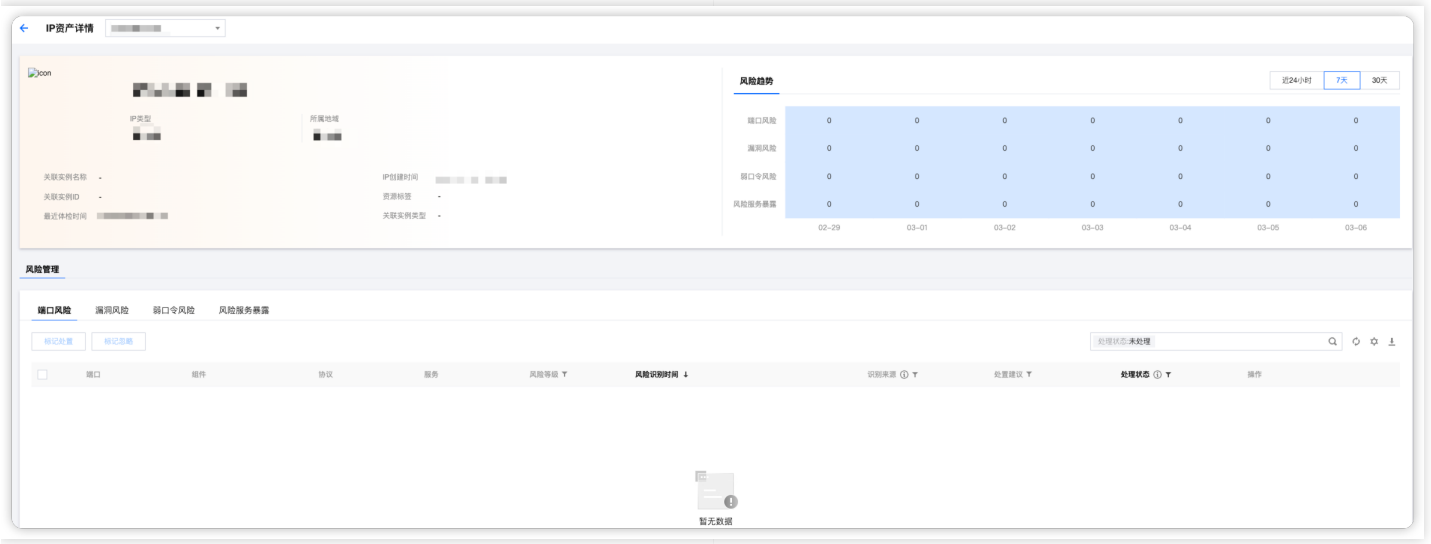
（1）主机资产

展示字段包括资产实例ID/名称、IP地址、资源标签、资产类型、地域、可用区、所属子网、所属私有网络、操作系统、体检任务、端口风险、漏洞风险、时间（最近体检时间、资产创建时间）。

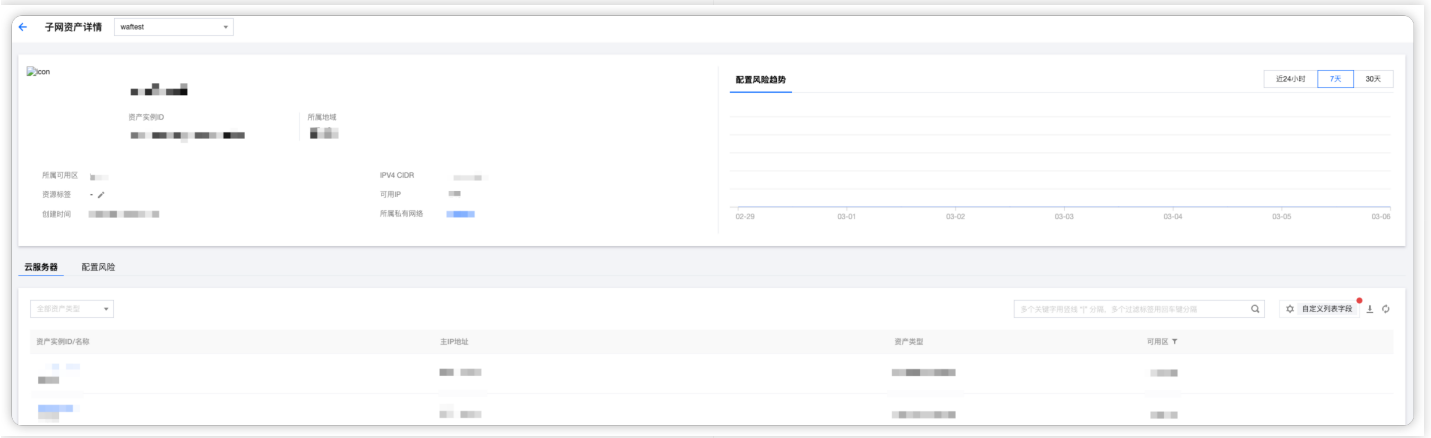
点击资产实例ID，可查看主机资产详情。包括主机详情、风险趋势和风险列表。



点击公网IP，可查看该IP资产详情，包括IP详情、风险趋势和风险列表。

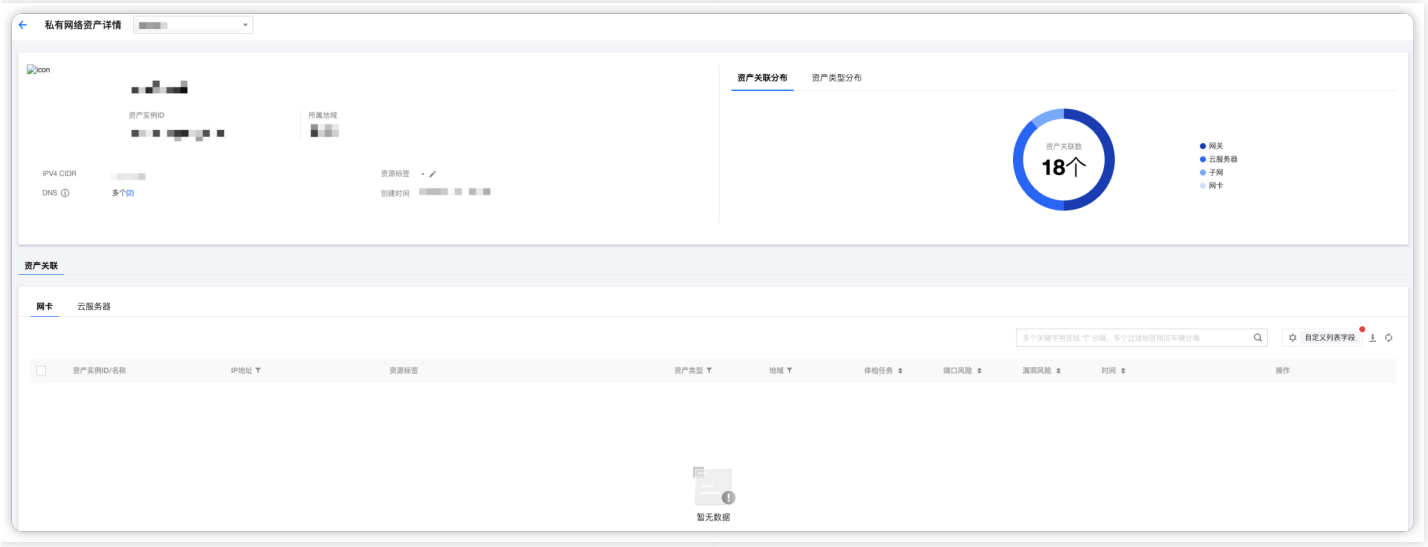


点击所属子网，可查看该子网详情，包括子网信息、配置风险趋势、关联云服务器和配置风险列表。



点击所属私有网络，可查看该私有网络详情，包括私有网络信息、资产关联分布、资产类型分布和资产关联的网络和

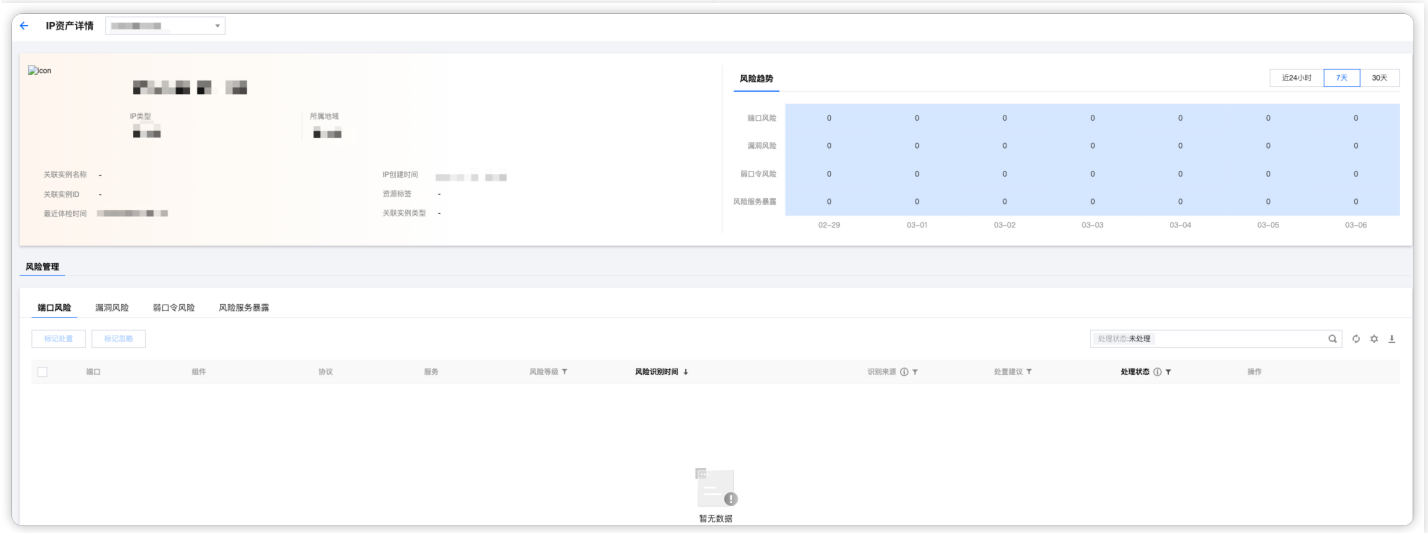
云服务器。



（2）IP资产

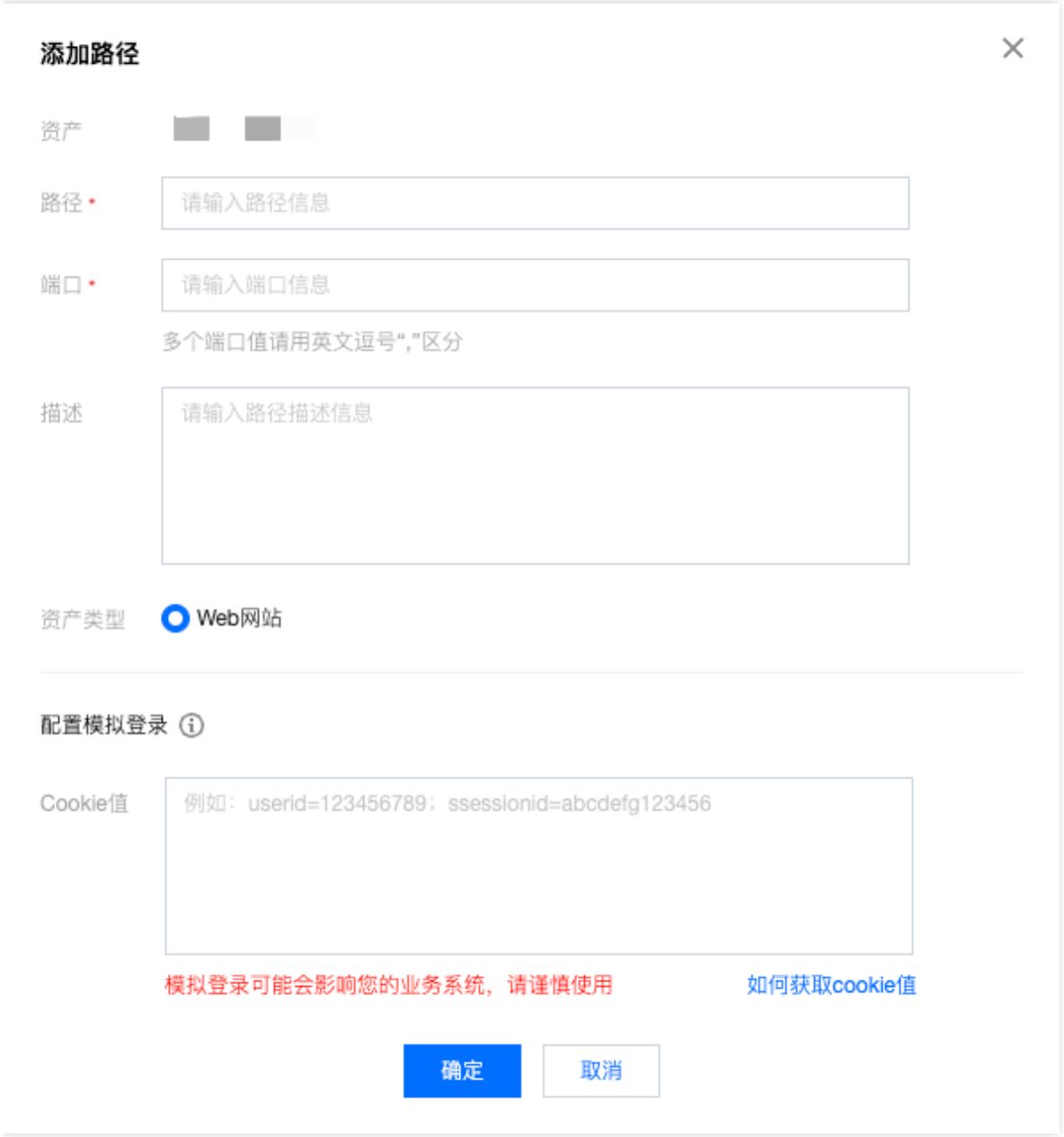
展示字段包括IP、资源标签、IP类型、地域、关联实例ID/名称、关联实例类型、所属私有网络、体检任务、端口风险、弱口令风险、风险服务暴露、时间（最近体检时间、资产创建时间）。

点击IP，可查看该IP资产详情，包括IP详情、风险趋势和风险列表。



点击查看路径，可查看IP路径详情。包括IP基本信息和IP路径信息，如下图所示。在此页面，可针对该IP发起安全体检，也可添加IP路径信息，扫描时支持对具体路径下的内容进行扫描。

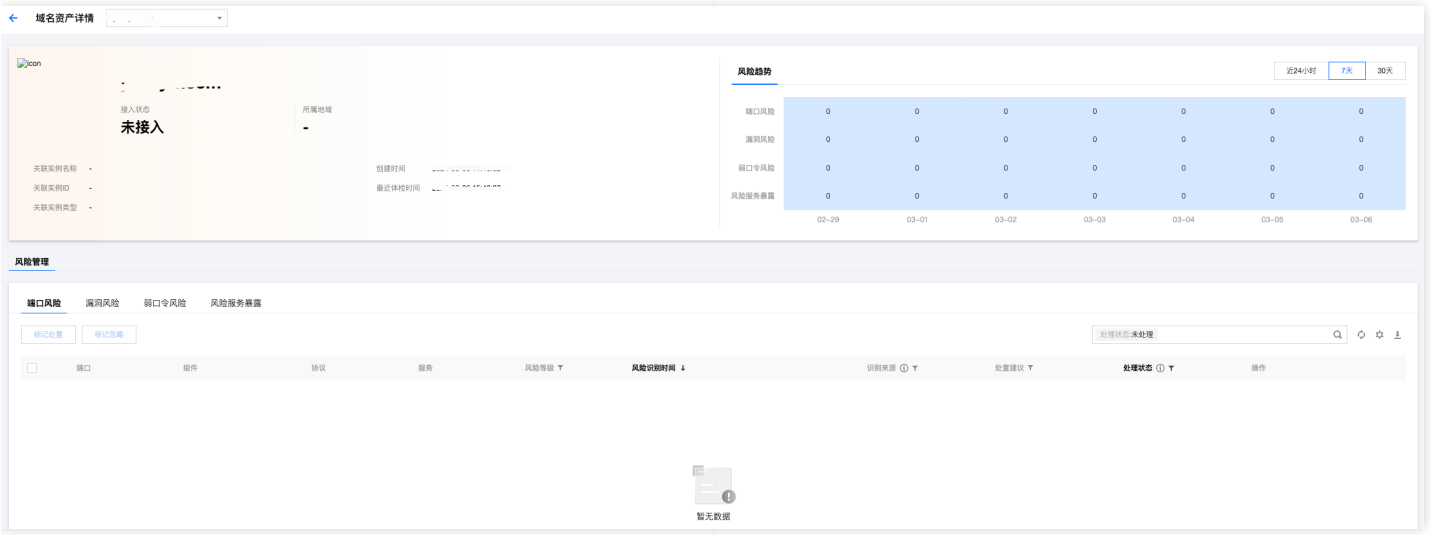

IP路径详情
发起体检
IP基本信息
IP地址
端口 -
所属网络 -
IP类型 未知
url数量 -
IP路径信息
添加路径
请输入路径或描述
路径
端口
类型
体检配置
描述
操作
暂无路径数据，你可以 添加路径
共 0 项
10 条 / 页
1
/ 1 页



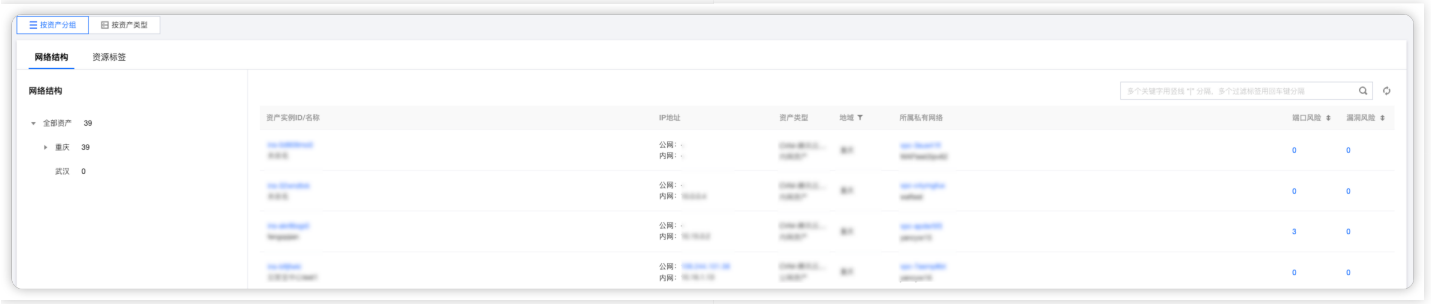
参数名称	参数说明
路径	具体路径目录。
端口	路径访问端口。
描述	对添加路径的自定义描述。
资产类型	支持 Web 网站。
Cookie 值	当资产类型选择 Web 网站时，若网站部分或全部页面、功能需要登录才能访问，建议设置 Cookie 模拟登录网站进行全面扫描，以获得全面的漏洞扫描结果。

（3）域名资产

展示字段包括域名、解析地址、资源标签、地域、关联实例ID/名称、关联实例类型、所属私有网络、体检任务、端口风险、漏洞风险、弱口令风险、风险服务暴露、时间（最近体检时间、资产创建时间）。
点击域名，可查看域名详情，包括域名信息、风险趋势和风险列表。



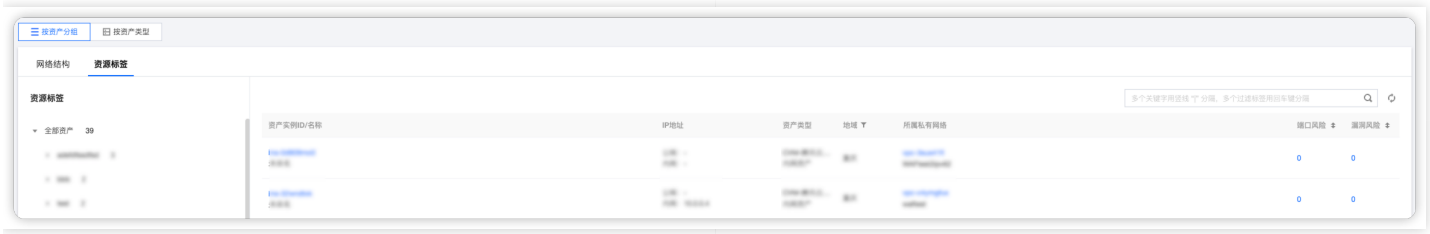
点击查看路径，可查看域名路径详情。包括域名基本信息和域名路径信息，如下图所示。在此页面，可针对该域名发起安全体检，也可添加域名路径信息，扫描时支持对具体路径下的内容进行扫描。
（4）网络资产
包括网络和私有网络。点击网络时，展示字段包括资产实例ID/名称、IP地址、资源标签、资产类型、地域、所属私有网络、体检任务、端口风险、漏洞风险、时间（最近体检时间、资产创建时间）。
点击私有网络时，展示字段包括资产实例ID/名称、IPV4 CIDR、资源标签、地域、DNS、云服务器、时间。
2.按资产分组
可通过网络结构和资源标签查看资产。



添加自定义资产标签

1.选择目标资产，点击资源标签下的　　，可自定义资源标签。
2.在标签标签弹窗中，选择标签键和标签值，单击确定。

3.添加标签后，按资产分组查看资产时，单击资源标签，可以按照自定义标签分类查看资产。



风险中心

风险中心模块展示了现有资产的风险数据，支持检测的风险类型包括端口风险、漏洞风险、弱口令风险、风险服务暴露。统计了当前风险概况，有助于快速定位具体风险，进行风险处理。

查看风险概况

1.在左侧导航中，单击风险中心。
2.查看风险概况，支持按照资产与扫描任务进行筛选。选择风险类型，单击数字，页面下方切换显示对应的风险类型详情。单击高危数字，页面下方切换显示对应的高危风险类型详情。

3.风险趋势栏可查看不同时间段内的风险数量，鼠标悬浮在图中数字上，可显示扫描时间、风险数量。
4.支持以资产名称与扫描报告结果对风险情况进行筛选，显示对应资产在某次扫描任务结果中，检测出的风险详情。

查看不同类型风险详情

漏洞扫描服务支持对端口风险、漏洞风险、弱口令风险、风险服务暴露的检测。在风险中心页面，单击页面下方的风险类型选项，查看不同类型的风险详情，默认显示未处置的风险。单击条件筛选框可重置筛选条件，显示所有风险内容。

> 说明
>
> 以漏洞风险为例。

查看资产的漏洞风险，包括漏洞名称、影响资产、风险等级、端口组件、漏洞类型、CVE 编号、扫描时间、处理状态。
按键说明：

- 单击漏洞风险列表表头关键字中的按钮，支持以关键字内容对漏洞风险进行筛选。
- 单击漏洞名称旁边的按钮，查看漏洞详情。
- 支持切换显示视角。
  - 资产视角：以资产为单位显示每个资产的漏洞风险。
  - 漏洞视角：以漏洞为单位显示每种漏洞影响的资产数量与端口，单击影响资产数栏的数字，跳转至资产视角中该漏洞风险所影响的资产信息。

风险管理

筛选风险

单击筛选框，以关键字对风险进行筛选定位。

标记状态

标为已处置

建议使用云防火墙和主机安全，对安全风险进行封禁等防御措施。防御处置后的风险可以标为已处置，处理状态更改为已处置，当下次扫描任务中仍然检测到此风险，则处理状态重新变回未处理。

1. 支持单个或批量将风险状态标为已处置。
   单个：选择目标风险，单击操作列的标记已处置。
   批量：选择一个或多个风险，单击左上角的标记已处置。
2. 在确认窗口中，单击确定，即可将目标风险标记为已处置。

标记为忽略

当扫描误报产生风险误报时或认为该风险无需处理时，可将该风险忽略，后续扫描任务中该风险将被过滤。

1. 支持单个或批量将风险状态修改为忽略。
   单个：选择目标风险，单击操作列的忽略。
   批量：选择一个或多个风险，单击左上角的忽略。
2. 在确认窗口中，单击确定，即可将目标风险状态修改为忽略。

取消标记

当已处置或已忽略风险时，选择目标风险，可单击操作列的取消标记处置或取消标记忽略，进行取消操作。

下载数据

单击下载按钮，可选择需要导出的行和列中的内容，导出至本地。

安全体检
功能简介

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。因此漏洞扫描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。

等保合规检测

为了帮助用户满足安全合规要求，安全产品提供了安全体检功能，可以检测云上资产的安全状况，并根据检测结果提供相应的加固建议，用户可以根据自己的需求对云上资产的合规风险进行持续监测和评估。

功能详情

体检项目

体检项目	项目内容
端口风险	针对公网 IP、域名的业务，由漏洞扫描提供的端口暴露检测能力。
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。
弱口令风险	针对主机资产、公网 IP、域名的通用业务，由漏洞扫描提供的弱口令检测。
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。

> 说明：
>
> 当识别来源为漏洞扫描时，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。

操作指引

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、服务暴露等安全威胁，支持多种体检模式选择。包括安全体检任务额度查看、体检次数查看、安全体检任务执行记录、体检任务列表和体检引擎实例。

创建任务

1. 登录漏洞扫描控制台，在左侧导览中，单击安全体检。
2. 在安全体检页面，单击创建安全体检任务。
3. 在创建体检任务弹窗中，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	- 标准体检：支持对端口风险、漏洞风险、弱口令风险、风险服务暴露等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，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。 - 端口风险：针对IP、域名的业务，由漏洞扫描提供的端口暴露检测能力，基于该能力可进行漏洞风险、弱口令风险和风险服务暴露能力检测。 - 漏洞风险：针对IP、域名相关资产，由漏洞扫描服务提供的漏洞风险检测，并梳理互联网漏

参数名称	说明
	洞暴露面。 - 弱口令风险：针对IP、域名的Web业务，由漏洞扫描提供的弱口令检测。 - 风险服务暴露：由安全专家摸排服务并全面梳理云上业务资产暴露面、潜在风险，给云上业务资产提供针对性的加固建议。
体检引擎	内网资产体检需使用对应地域的体检引擎，如体检资产包括公网资产，则需单独的公网引擎。
单次消耗	每执行一次任务消耗的体检次数。

编辑任务

1. 登录 漏洞扫描控制台，在左侧导览中，单击安全体检。
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 漏洞扫描控制台，在左侧导览中，单击安全体检。
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

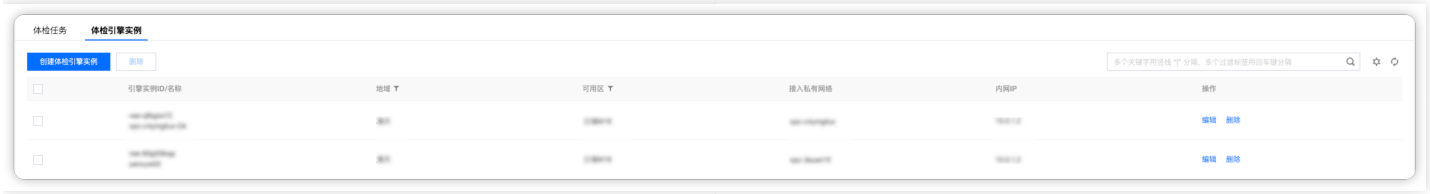
当安全体检任务完成后，漏洞扫描会自动生成 PDF 格式的安全报告，并提供预览或下载。

1. 登录 漏洞扫描控制台，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。

体检引擎实例

内网资产体检需使用对应地域的体检引擎，需配置；如体检资产包括公网资产，则有默认的公网引擎供使用，无需配置。



点击创建体检引擎实例按钮，需配置引擎名称、地域和接入私有网络完成内网体检引擎的配置。

点击体检引擎列表操作列的编辑按钮，可对已配置的体检引擎进行更改；点击删除，删除完成后则相应的内网资产无法进行安全体检，请谨慎操作。

热点问题

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。

安全体检是否会影响业务运行？

不会，安全体检模拟真实用户的访问，同时有精准的速率控制，不会影响业务的正常运转。

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。

报告下载

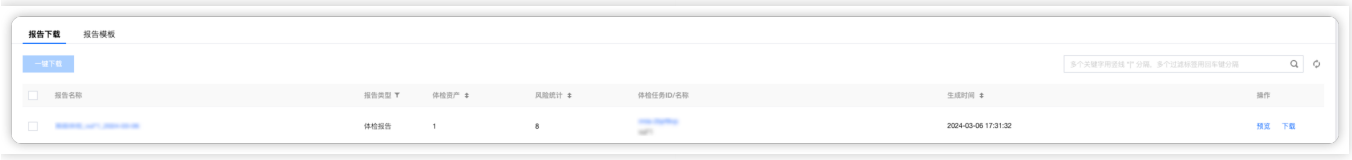
报告下载模块统计了当前扫描任务完成情况，以文档的形式多角度总结扫描任务结果，并提供专业修复建议，更清晰地分析资产安全现状，可直接在线预览，也支持下载到本地保存。

查看风险概况

登录漏洞扫描，在左侧导航中，单击报告下载。在报告下载页面的扫描报告概况模块中， 可查看当前产生的扫描报告个数，包含待查看报告个数，以及报告模版。

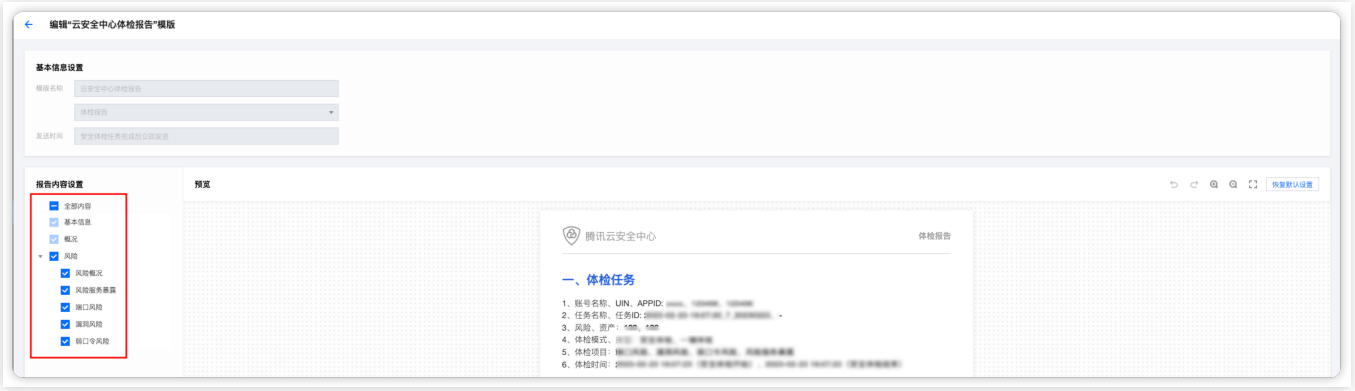
报告下载

在报告下载记录模块中，按时间顺序记录了报告下载的信息，单击详情，在页面下方筛选出对应的扫描报告。
在扫描报告列表模块中，显示了报告名称、报告类型、体检资产数量、风险数量、体检任务ID/名称、生成时间信息，单击任务扫描栏中的体检任务名称，可跳转至安全体检扫描任务页面，查看该报告对应的扫描任务详情。



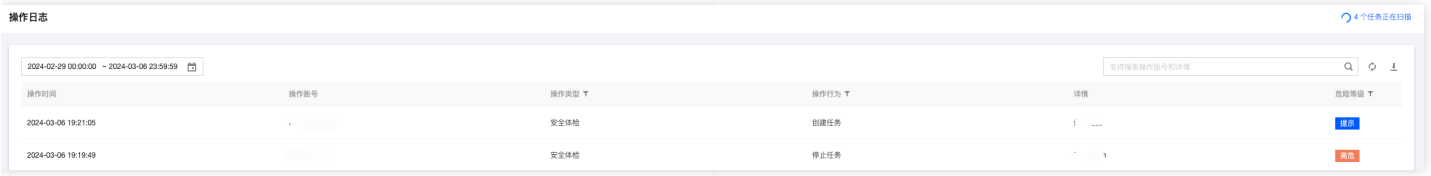
在报告下载页面，单击筛选框，支持以关键字对扫描报告进行筛选。单击，可局部对扫描报告列表进行刷新，保留筛选条件。
在报告下载页面，支持网页预览与本地下载两种查看方式。

- 网页预览：选择目标报告，单击报告名称或操作列的预览，可在网页上预览报告内容。
- 本地下载：选择单个或多个报告，单击左上角下载报告，可批量下载报告到本地；选择目标报告，单击操作列的下载报告，可下载单份报告到本地。
  点击报告名称或预览按钮预览报告时，可对报告模版进行编辑，自定义勾选模版展示的内容。


编辑"云安全中心体检报告"模版
基本信息设置
模版名称
云安全中心体检报告
体检报告
发送时间
安全体检任务完成后立即发送
报告内容设置
全部内容
基本信息
概况
风险
风险概况
风险服务暴露
端口风险
漏洞风险
弱口令风险
预览
恢复默认设置
腾讯云安全中心
体检报告
一、体检任务
1、账号名称、UIN、APPID:
2、任务名称、任务ID:
3、风险、资产:
4、体检模式、
5、体检项目：
6、体检时间：

操作日志

操作日志页面展示了用户登录漏洞扫描的操作行为，包括创建任务、停止任务、编辑任务、删除任务、创建体检引擎、删除体检引擎、标记处置、标记忽略、取消标记处置、取消标记忽略、编辑体检引擎、下载报告、添加路径、添加资产、删除路径、导出列表、删除资产、编辑路径、同步云资产、导出列表。



可根据时间范围、操作类型、操作行为和危险等级对操作记录进行筛选。也可根据操作账号和详情进行关键字检索。

- 操作类型：包括安全体检、风险中心、报告下载、资产管理。
- 危险等级：包括提示、高危、中危、低危。

故障处理
根据故障反馈关联策略解除权限问题

根据故障反馈关联策略解除权限问题

操作场景

本文档介绍如何通过故障反馈关联策略解除权限问题，解除权限问题后，子账号将在新设置的权限范围内管理主账号下的资源。

场景示例1

当子账号访问漏洞扫描时产生如下提示：

如您愿意授权子账号继续进行操作，您可以根据操作指引为其关联以下任意预设策略：

- QcloudSSAFullAccess 安全运营中心服务角色权限（全读写）。
- QcloudSSAReadOnlyAccess 安全运营中心服务角色权限（只读）。
- QcloudWAFReadOnlyAccess Web 应用防火墙服务角色权限（只读）。

场景示例2

当子账号访问漏洞扫描时产生有如下提示：

如您愿意授权子账号继续进行操作，您可以根据操作指引为其关联预设策略：
QcloudAuditFullAccess 操作审计服务角色权限（全读写）。

前提条件

相关服务角色授权需要使用“主账号”或“拥有访问管理读写权限的账号”完成。

> 说明
>
> 主账号拥有访问管理读写权限，同时可以给相应子账号 分配访问管理读写 权限。

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，如“QcloudSSAFullAccess”进行搜索。
3.在“QcloudSSAFullAccess”策略的右侧操作栏中，单击关联用户/组。

4.在关联用户/用户组页面，选中需要配置权限的子用户，单击确定即可。


关联用户/用户组
关联用户
支持多关键词(间隔为空格)搜索用户名/ID/SecretId/手机/邮箱
用户
切换成用户组
用户
用户
用户
用户
用户
用户
用户
已选择(1条)
用户名/组名
类型
用户
支持按住shift键进行多选
确定
取消