

# 云安全中心

## 操作指南





【版权声明】

©2013-2025 腾讯云版权所有

本文档(含所有文字、数据、图片等内容)完整的著作权归腾讯云计算(北京)有限责任公司单独所有,未经腾讯云事先明确书面许可,任何主体不 得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯,腾讯云将依法采取措施追究法律责任。

【商标声明】

## 🕗 腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算(北京)有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标,依法由权利人所有。未经 腾讯云及有关权利人书面许可,任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为,否则将构成对腾讯云及有关权利人 商标权的侵犯,腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况,部分产品、服务的内容可能不时有所调整。 您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定,除非双方另有约定,否则,腾讯云对本文档内容不做任何明 示或默示的承诺或保证。

#### 【联系我们】

我们致力于为您提供个性化的售前购买咨询服务,及相应的技术售后服务,任何问题请联系 4009100100或95716。



操作指南

## 文档目录

资产中心 云资源配置风险 安全体检 功能简介 操作指引 添加白名单 IP 评分详情 热点问题 云边界分析 功能简介 查看统计面板 查看边界列表 检索暴露路径 查看扫描结果 云 API 异常监测 功能简介 云 API 密钥安全使用方案 统计面板 资产列表 告警 风险 策略管理 DNS 威胁监测 功能简介 统计面板 全部请求 恶意请求 异常基线 策略管理 用户行为分析(UEBA) 大模型态势管理 日志投递(支持多账号多产品多日志) 多云多账号管理 多云接入 多账号管理 阿里云账号权限说明 访问权限管理



## 操作指南 资产中心

最近更新时间: 2024-08-28 18:57:11

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					
		云服务器 CVM				
	腾讯云	轻量应用服务器 Lighthouse				
主机资产		边缘计算器				
	甘他云	亚马逊云服务器 AWS EC2				
	HUA	微软云服务器 Azure VMs				
	容器					
	本地镜像					
		CCR 镜像				
		TCR 镜像				
	仓库镜像	Harbor 镜像				
		亚马逊云镜像 AWS ECR				
		微软云镜像 Azure ACR				
	主机节点	CVM				
容器资产		Lighthouse				
		超级节点				
		托管集群				
		独立集群				
	集群	边缘集群				
		弹性集群				
		自建K8s集群				
		自建Openshift集群				
	Pod					
公网 IP 资产	公网 IP					
	高可用虚拟	IP				
	弹性 IP					
	弹性 IPv6					



	anycast IP					
	非腾讯云 IP					
は夕次立	域名					
以石页厂	非腾讯云上域名					
		NAT 网关				
		VPN 网关				
		负载均衡 CLB				
	정문	NAT 防火墙				
	网大	探针 Probe				
网络资产		亚马逊云负载均衡 ELB				
		本地网络 Local Network				
		虚拟网络 Virtual Network				
	弹性网卡 EI	NI				
	私有网络 VPC					
	子网					
		云数据库 MySQL				
		云数据库 Redis				
	腾讯云	云数据库 MariaDB				
		云数据库 PostgreSQL				
- ** urt		云数据库 MongoDB				
<b>云</b>		亚马逊云 DynamoDB				
		亚马逊云OpenSearch				
	其他云	微软云 Postgre				
		微软云 MySQL				
		微软云 Redis				
其他云资源	云硬盘 CBS					
	对象存储 CC	DS				
	文件存储					
	消息队列					
	Elasticsea	arch Service				
	密钥管理系统	充 KMS				
	操作审计 CloudAudit					



API 网关 API Gateway
SSL 证书
安全组 SecurityGroup
其他证书

## 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。

() <b>说明:</b> 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 。	
资产更新 🕜 🔗	接入多云资产     手动	添加资产 收集外部资产		近24小时 7天 30天
资产统计概况				
主机资产 🕠	公网IP资产	域名资产	4 主机资产监控 容器资产监控 公网IP资产监控	域名 论 ▶ 入向峰值带宽 TOP5 ▼
$\uparrow$	$\uparrow$	$\uparrow$		
未防护主机	未防护公网IP	未防护域名		
风险主机	风险公网IP	风险域名	and the second se	
容器资产	网关资产	数据库资产		
$\uparrow$	个	$\uparrow$		

## 搜索资产

• 在 资产中心页面,支持按照资产类型,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。

─ 按资产分组 ─ 按资产类型	① 按服务类型 只看	<b>雪新增</b> 只看核心	只看未防护		多个关键字用竖线 "	" 分隔,多个过滤标签用@	回车键分隔	Q Ø
<b>主机资产(107)</b> 容器资产(537	3) 公网IP资产(131)	域名资产(502)	网络资产(224)	数据库资产(1)	其他云资源(220)			
开启防护标记为核心资产	标记为非核心资产						<b> </b>	Ŧ
资产实例ID/名称	IP地址 ▼	资源标签		资产类型 🔻	地域 🔻	所 防护状态 ▼	操作	
	公网: 内网:	核心资产				• 未防护	开启防护 更多 ▼	

● 在 资产中心页面,支持按照资产分组,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。



<b>三</b> 按资产分组	① 按服务类型						
<b>网络结构</b> 资源标签							
网络结构				93) 33)	个关键字用竖线 " " 分隔,多个过	滤标签用回车键分隔	Q Ø
▼ 全部资产 366	资产实例ID/名称	IP地址	资产类型	地域 ▼	所属私有网络	端口 \$	漏洞 \$
▶ 上海自动 1		公网:	-				
		内网:	公网资产			0	0

• 在 资产中心页面,支持按照服务类型,查询不同 Web 服务下,分别有哪些 VPC,每个 VPC 内分别关联哪些资产。

按资产分组 🗄 按资	资产类型 ① 按服务类型 只看新增	只看核心 只看未防护		多个关键字用竖线 " " 分隔,多个:	·过滤标签用回车键分隔	Q	φ
Web服务							
添加服务标记为	核心资产 标记为非核心资产 删除				☆ 自定	义列表字段 ▲	
服务地址	资源标签	服务类型 👅	内网IP	所属私有际云防	5火墙防护 🍸 操作		
	核心资产	公网服务		• 7	<mark>卡防护</mark> 开启防护	' 更多 ▼	
	核心资产	公网服务		• オ	<mark>卡防护</mark> 开启防护	'更多▼	

## 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。

按资产分组 🗄 按资产类型	① 按服务类型 只	看新增只看核心	只看未防护		多个关键字用竖线	:"!" 分隔,多个过滤标签用	回车键分隔(	2
<b>主机资产(107)</b> 容器资产(537	'3) 公网IP资产(131)	域名资产(502)	网络资产(224)	数据库资产(1)	其他云资源(220)			
开启防护标记为核心资产	标记为非核心资产						☆ 自定义列表字段	
资产实例ID/名称	IP地址 ▼	资源标签		资产类型 🍸	地域 ▼	所 防护状态 ▼	操作	
	公网: 内网:	-				• 未防护	开启防护 更多 ▼	
	公网: 内网:	-				<ul> <li>未安装</li> </ul>	标记为核心资产 标记为非核心资产 安装工具包	
	公网: 内网:	核心资产				• 已防护	防护详情 更多 ▼	

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。



三 按资产分组					多个关键字用竖线 " '	回车键分隔	Q Ø	
<b>主机资产(107)</b> 容器资产(5373	3) 公网IP资产(131)	域名资产(502)	网络资产(224)	数据库资产(1)	其他云资源(220)			
开启防护标记为核心资产	标记为非核心资产						自定义列表字段	±
资产实例ID/名称	IP地址 ▼	资源标签		资产类型 👅	地域 ▼	所 防护状态 ▼	操作	
	公网: 内网:	核心资产				• 未防护	开启防护 更多 ▼	
	公网: 内网:	-				• 未安装	标记为核心资产 标记为非核心资产 安装工具包	
	公网: 内网:	核心资产				• 已防护	防护详情 更多 ▼	

• 在 资产中心页面,可以根据防护状态筛选资产。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。

按资产分组 🗄 按资产类型	① 按服务类型 只	看新增 只看核心	只看未防护		多个关键字用竖线 " "	" 分隔,多个过滤标签用回	车键分隔	C
<b>主机资产(107)</b> 容器资产(5373	3) 公网IP资产(131)	域名资产(502)	网络资产(224)	数据库资产(1)	其他云资源(220)			
开启防护标记为核心资产	标记为非核心资产						☆ 自定义列	则表字段
资产实例ID/名称	IP地址 ▼	资源标签		资产类型 ▼	地域 ▼	所 防护状态 🕈	操作	
	公网: 内网:	核心资产			北京	全部 - - 未安装	护更	[3 ▼
	公网: 内网:	核心资产			北京	- - - - -	护 更	13 ▼
	公网: 内网:	核心资产			南京	确定 - - 已版把	重置 防护连桥 更	[3 ▼

🕛 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。



☰ 按资产	Ξ 按资产分组 投资产类型 ① 按服务类型 只看新增 只看核心 只看未防护					字用竖线 " " 分隔,多个过滤标签用	回车键分隔 Q C
主机资	ē产(107) 容器资产(	5373) 公网IP资产(131)	域名资产(502) 网络资产(224)	数据库资产(1)	其他云资》	原(220)	
网关	网卡 私有网络	子网标记为核心资	帝 标记为非核心资产				☆ 自定义列表字段 上
	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	操作
		公网: 内网:	核心资产				标记为核心资产 更多 ▼
		公网: 内网:	核心资产				标记为核心资产 更多 ▼
		公网: 内网:	核心资产				标记为核心资产 更多 ▼

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。

Ξ 按资产分组  ⊟ 按资产类型	① 按服务类型							
网络结构 资源标签								
资源标签					多个关键字用竖线 "!" 分隔,多个过滤	基标签用回车键分隔	Q	φ
▼ 全部资产 366	资产实例ID/名称	IP地址	资产类型	地域 ▼	所属私有网络	端口 \$	漏洞	\$
Þ		公网: 内网:	- 公网资产					
•		公园·	_					
Þ		内网:	内网资产					
Þ		公网:	-					
Þ		内网:	公网资产					

## 添加云外资产

如需管理非腾讯云资产,可以在资<u>产中心页面</u>,选择**接入多云资产、手动添加资产、收集外部资产**。



资产更新 🕚 🗠	🥶 🔡 接入多云资产 手动	添加资产 收集外部资产	近24小时 7天 30天
资产统计概况			
主机资产	公网IP资产	域名资产	✓ 主机资产监控 容器资产监控 公网IP资产监控 域名资 ▶ 入向峰值带宽 TOP5 ▼
$\uparrow$	$\uparrow$	个	
未防护主机	未防护公网IP	未防护域名	
风险主机	风险公网IP	风险域名	
容器资产	网关资产	数据库资产	-
$\uparrow$	$\uparrow$	$\uparrow$	

其中公网 IP 资产、域名资产需经认证后,方可对该资产使用资产中心的功能和操作。

∃ 按资	产分组	□ 按资产类型 ① 按服务类型	只看新增 只看核心 只看未防护	多个关键	字用竖线 " " 分隔,多个过滤标签用	回车键分隔 Q	φ
主机资	受产(15)	容器资产(144) 公网IP资产(26)	<b>域名资产(6)</b> 网络资产(78)	数据库资产(3) 其他云资源(23)			
标记	为核心资产	标记为非核心资产 删除					Ŧ
	域名	解析地址	资源标签	地域 <b>▼</b> Web应用	防火墙防护 ▼ 所属账号 ▼	操作	
			待认证 外部资产 🧪	未知 -	<u>&amp;</u>	认证资产 更多 ▼	
			核心资产 外部资产 C	<b>按照下述内容认证该资产为本企业/集团</b> F 手动认证 〇 人工认证(耗时可能较长)	fī有	更多 ▼	
			<u>外部资产</u> 安 该	主域名服务商平台根据下方字符内容修改 全中心将解析待认证的域名。完成认证后,您可 资产为本账号所属企业所有。	域名的TXT记录 认对该资产使用资产中心的功能和排	,修改后云 操作,请确保 <b>更多 ▼</b>	
			外部资产			更多 ▼	6
			外部资产	承诺该资产归本账号所属企业所有,如资产归 法律责任	属错误,所造成的后果将由本账号归	∃属企业承担 更多 ▼	- <u>C</u>
			认证中外部资产	77 XE KAVE	9X/H V/ NL	更多 ▼	Ξ

• 在接入多云资产弹窗中,填写相关信息完成配置,详细请参考 多云接入。



选择账号类型	🔛 Azure账号 🔤 AWS账号 🙆 腾讯云子账号 🙆 腾讯云账号,前往集团账号配置 🖸	
创建子账号的方式	手动配置 5分钟完成,需要创建"应用注册"与"客户端密码",并绑定"订阅",赋予"读者"权限。 收起配置指引 ▲ 在文档中查看 ℃	
	< 第1/3步 > 请前往 www.azure.com/xxx 🖸 创建一个应用注册,并根据需要选择支持的帐户类型。	
	•         •	
	1. Number (14) (14) (14) (14) (14) (14) (14) (14)	8
「阅ID	请输入	
户ID	请输入	

• 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。

$\odot$	腾讯云
---------	-----

手动添加	资产	• ×
<b>i</b>	支持在资产中心添加云外公网IP、域名资产	×
添加方式	● 手动录入 ○ 文件导入	
地址	1.	
	请输入公网IP地址、Web网站域名、API域名,手动输入使用回车换行,每 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;不 地址,若输入重复IP,后台将自动合并	珩一个; 支持CIDR
承诺查看	添加资产归本账号所属企业所有,如使用他人资产将由本账号归属企业承担没 f详情 确定 取消	去律责任

 在收集外部资产弹窗中,开启外部资产收集开关,开启后,云安全中心将会使用腾讯安全网络空间资产发现和情报信息收集能力,主动获取您所 在企业的外部资产,并自动导入到对应资产列表中;输入企业关键词(为确保收集信息的准确性,建议输入企业或集团的注册公司名称、主站域 名或证书),勾选服务协议,单击确定。

外部资产收集	
企业关键词	请选择
	设置企业关键词后,我们会使用腾讯安全威胁情报的信息收集工 具,在互联网中捕获外部的企业资产,为确保收集信息的准确 性,建议输入企业或集团的注册公司名称、主站域名或证书
云洪东中	*雄河山未叱马统屋个业成去,加持它不恰坐的关键河收已动共取进;
承诺添加新的资产信息	关键词归本账号所属企业所有,如填写不恰当的关键词将导致获取错说 息,所造成的后果将由本账号归属企业承担法律责任
承诺添加非的资产信息	关键词归本账号所属企业所有,如填写不恰当的关键词将导致获取错说 急,所造成的后果将由本账号归属企业承担法律责任 确定 取消



• 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。

资产中心					多账	号管理	• 🛇
资产更新 🕚 🔗 😇	田 接入多云资产     手动添	加资产收集外部资产	请输	入账号名称/账号ID进行打	搜索		Q <sub>天</sub>
资产统计概况				账号名称	账号ID/APPID	所属部门 ▼	
主机资产 ①	公网IP资产	域名资产		8			r
<b>个</b> 未防护主机 风险主机	个 未防护公网IP 风险公网IP	↑ 未防护域名 风险域名		Ø			
容器资产	网关资产	数据库资产					
$\uparrow$	$\uparrow$	$\uparrow$					
三 按资产分组 🔡 按资产	类型 ① 按服务类型	只看新增 只看核心 只看未防护		Ø			¢
主机资产(15) 容器资	产(144) 公网IP资产(26)	<b>域名资产(6)</b> 网络资产(78)		Ø			6
标记为核心资产标识	2为非核心资产 删除				确定取消	Y HAAM	- 2
域名	解析地址	资源标签		地域 ▼	Web应用防火墙防护 ▼ 月	「属账号 ▼ 操作	<b>C</b>
		待认证 外部资产		未知	- 6	8 认证资产 更多 ▼	E
	-	核心资产 外部资产		未知	• 未防护	⊗ 开启防护 更多 ▼	

## 云资源配置风险

最近更新时间: 2025-08-14 10:10:42

## 功能介绍

云资源配置风险是通过对云资源的配置进行检查以发现因配置不当引入的安全风险。

## 访问入口

- 1. 登录 云安全中心控制台,在左侧导览中,单击**漏洞与风险中心**。
- 2. 在**漏洞与风险中心 > 云资源配置风险**中,支持查询云资源配置风险。

云安全中心	漏洞风险	端口风险 弱口令风	俭 内容风险	风险服务暴露 云波	<b>該配置风险</b> 主机基	线风险 容器基线风险
<ul> <li>記 安全概览</li> <li>三 待か事项</li> <li>运营中心</li> </ul>	<ol> <li>您的账号I</li> <li>配置项视角</li> </ol>	E处于新云资源配置检查引擎 资产视角	恢度中,但存在未灰	夏的接入账号,未灰度账号无 <b>;</b>	去展示云资源配置风险数据	8,我们将在两个工作日内完成灰度,您
⑦ 资产中心	① 立即检测	✔ 仅展示高优修复风	睑			最近发现时间 ~ 2025-07-
	云厂商 ℃	配置项名称		检查类型 ⑦	风险等级 丁	风险监测聚合描述
安全场景	CD 阿里云	对象存储未禁用匿名	用户读写权限	鉴权管控	高危	发現 5 个对象存储未禁用匿名用
◎ 云API异常监测	O 阿里云	对象存储未禁用匿名,	用户列桶权限	鉴权管控	高危	发现 2 个对象存储未禁用匿名用
<ul><li>DNS威胁监测</li><li>一 大模型态势管理</li></ul>	🔗 腾讯云	CAM主账号未启用登	录操作保护	账号安全	高危	发现 10 个CAM主账号未启用登
策略配置 ○ 用户行为分析	🔗 腾讯云	存储桶未禁用匿名用所	白读写权限	鉴权管控	高危	发现 15 个存储桶未禁用圈名用
》 《模拟攻击	🔗 腾讯云	容器镜像个人版仓库公	公网未授权访问	网络安全	高危	发现 32 个容器镜像个人版仓库
系统配置	_					

## 风险检测

云资源配置风险检测会跟随您资产的同步周期进行检测,您也可以通过以下方式手动触发检测。

- 1. 登录 云安全中心控制台,在左侧导览中,单击**漏洞与风险中心**。
- 2. 在漏洞与风险中心 > 云资源配置风险中,单击立即检测,即可发起云资源配置风险检测。

3. 鼠标移至**立即检测**上方,您可以看到最近一次检测任务的运行时间。

最近检测时间:20	25-07-31 12:08:14
① 立即检测	✓ 仅展示高优修复风险

## 配置项视角

- 1. 登录 云安全中心控制台,在左侧导览中,单击**漏洞与风险中心**。
- 在漏洞与风险中心 > 云资源配置风险中,选择配置项视角,风险按配置项做了聚合统计,用于解决同类问题。



漏洞风险	端口风险 弱口令风险 内容风险	风险服务暴露 云资源	配置风险 主机基	线风险 容器基线风	险					
配置项视角	资产视角									Ê
① 立即检测	✔ 仅展示高优修复风险			最近发现时间 >	2025-07-30 10:15:33 ~ 2025-08-05 10:15:33	8 🗄	处理状态:未修复		Q	C
云厂商 ⑦	配置项名称	检查类型 了	风险等级 丁	风险监测聚合描述			首次/最近发现时间 ↓	处理状态 了	操作	
🖸 阿里云	对象存储未禁用匿名用户读写权限	鉴权管控	高危	发现 5 个对象存储	未禁用匿名用户读写权限		2025-07-09 16:23:26 2025-08-05 09:52:55	未修复	详情	
🖸 阿里云	对象存储未禁用圈名用户列桶权限	鉴权管控	高危	发现 <mark>2</mark> 个对象存储	未禁用匿名用户列桶权限		2025-05-28 11:48:51 2025-08-05 09:52:55	未修复	详情	
🔗 腾讯云	CAM主账号未启用登录操作保护	账号安全	高危	发现 <mark>10</mark> 个CAM主题	张号未启用登录操作保护		2025-05-30 18:59:12 2025-08-05 08:28:27	未修复	详情	
🔗 腾讯云	存储桶未禁用匿名用户读写权限	鉴权管控	高危	发现 15 个存储桶未	禁用匿名用户读写权限		2025-07-09 17:12:12 2025-08-05 09:07:13	未修复	详情	

- 3. 列表按风险处理的优先级进行了风险排序,您可以按顺序进行风险治理。
- 4. 列表默认勾选了**仅展示高优修复风险**,将隐藏一部分修复优先级较低的风险,若您关注此类风险,可以取消该勾选,查看全部内容。

配置项视角	资产视角
🕓 立即检测	✔ 仅展示高优修复风险

- 5. 页面还支持多种筛选条件:首次发现时间、最近发现时间、处理状态、风险等级、云厂商,您可以根据实际使用需求筛选数据。
- 6. 选择目标数据,单击**详情**,可以看到该条风险的全部详情数据。

云厂商 🔽	配置项名称	检查类型 了	风险等级 了	风险监测聚合描述		首次/最近发现时间 📫	处理状态了	操作
∞ 腾讯云			高危	发	∃用登录操作保护	2025-07-02 14:41:02 2025-08-13 16:40:30	未修复	详情
❷ 腾讯云			高危	发	名用户读写权限	2025-07-09 18:34:30 2025-08-13 17:02:57	未修复	详情

7. 在详情页面,您可以查看风险危害、风险修复建议、风险详情。

多复建议						
1险危害	匿名用户对存储桶的读	写权限可能导致数据泄露、篡改	<b>文和删除,带来严重的安全和隐私</b>	风险。		
1险修复建议	♀ 修复建议					展开 ▼
	1 登录 对象存储 Bucket 新	音控制台,在存储桶列表找到目 <sup>;</sup>	际存储桶,点击存储桶名称进入	管理页面。		
		Kull-12, Statute Line Instantiautonik Lenink, (Hakirak Kulturak Line Internet Instantiautonik Lenink, (Hakirak Kulturak Kullurak Internet Instantiautonik Kullurak Internet Instantiautonik	N         Same         Sa	Notice         Notice<		
<b>以险详情</b> 标记处置	标记忽略		处理状态:未修复		Q	C .
资产Ⅱ	D/名称	公共权限	授权操作	处理状态 了	操作	
		公有读私有写	公共权限	未修复	验证 标记忽略 标识	已处置

8. 在风险详情中,您可以查看该配置风险项的完整风险列表,并对目标数据进行验证、标记忽略或标记处置等操作。

## 资产视角



- 1. 登录 云安全中心控制台,在左侧导览中,单击漏洞与风险中心。
- 2. 在**漏洞与风险中心 > 云资源配置风险中**,选择**资产视角,**风险按配置项和风险做了聚合统计,可以针对资产进行风险查询。

配置项视角								宣 策略配置
① 立即检测		最近发现时间 > 2025-07-	30 16:44:30 ~ 2025-08-05 16	:44:30 📋 🖇	让理状态:未修复		Q	C & 7
资产ID/名称	配置项名称	检查类型 丁	风险等级 丁	首次/最近发现时	间 \$	处理状态 了	操作	
	容器镜像个人版仓库公网未授权访问	网络安全	高危	2025-07-15 22: 2025-08-05 14:	54:47 :20:07	未修复	详情	

- 3. 列表按风险处理的优先级进行了风险排序,您可以按顺序进行风险治理。
- 4. 列表默认勾选了**仅展示高优修复风险**,将隐藏一部分修复优先级较低的风险,若您关注此类风险,可以取消该勾选,查看全部内容。

配置项视角	资产视角
① 立即检测	✔ 仅展示高优修复风险

- 5. 页面还支持多种筛选条件:首次发现时间、最近发现时间、资产id、资产名称、处理状态、风险等级、云厂商,您可以根据实际使用需求筛选数 据。
- 6. 选择目标数据,单击**详情**,可以看到该资产对应风险的全部详情数据。

资产ID/名称	配置项名称	检查类型 了	风险等级 ℃	首次/最近发现时间 ‡	处理状态 了	所属账号 了	操作
主账号		账号安全	高危	202 202	未修复	ø ]	详情
主账号		账号安全	高危	202 202	未修复	Ø	详情
主账号		账号安全	高危	202 202	未修复	<u>@</u>	详情

7. 在详情页面,您可以查看风险危害、风险修复建议、风险详情。



<b>资产配置详情</b>						
<b>》</b> = M	 长号		所属账号 检查项	CAM主账号未启用登录損	操作保护	
多复建议		惑马和强化促始 一日廿土老祭	3.31次制公、按可以任务福佐	业日本资本 动眼日本的资本选品	北在宇	
4.应危害 3.险修复建议	CAM主赋号没有开启 ♀ 修复建议	豆来和探FF床扩,一旦攻击有豆	来到在前口,符可以在总保TF!	赋亏下页/ , 刈赋亏下的页/ 迫/	以心古。	展开 ▼
	1     登录访问管:       2     单击设置默*       身份安全	里控制台 ,在用户 > 用户设置 页 从方式,进入身份安全设置窗口。 ∶ <b>设置</b>	页面,找到设置项身份安全设置	•		
风险详情						
标记处置 用户名和	标记忽略 <b>东</b>	是否可以登录控制台	用户账号	风 处理状态 了	操作	G .
主账号		是	• • • •	操 未修复	验证 标记忽■	格 标记处置
主账号		是		登: 未修复	验证 标记忽日	格 标记处置

8. 在风险详情中,您可以查看该配置风险项的完整风险列表,并对目标数据进行验证、标记忽略或标记处置等操作。

### 策略配置

- 1. 登录 云安全中心控制台,在左侧导览中,单击**漏洞与风险中心**。
- 2. 在漏洞与风险中心 > 云资源配置风险中,单击策略配置,您可以查看风险配置项列表,也可以选择策略进行禁用。

() 策略規	观则的调整 <b>仅对日常检测、标准体检、手</b>	<b>动检测生效,</b> 高级体检(	仍按自定义策略项的	勾选结果进行体检			×
批量启用	批量禁用		多个关键	撑用竖线 " " 分隔,多	个过滤标签用回车银	能分隔 Q	G
	配置项名称	云厂商 ⑦	风险等级 了	处置分类	关联账号	策略开关 了	
	API 网关未授权访问且存储桶未禁…	8	高危	紧急风险治理	1		
	CAM主账号未启用登录操作保护	<u>න</u>	高危	紧急风险治理	1	• 已开启: 1,	/1
Þ	CAM存在恶意账号	Ø	高危	紧急风险治理	1	● 已开启: 1,	/ 1
	Elasticsearch Service公网未授	8	高危	紧急风险治理	1	● 已开启: 1,	/1
	Elasticsearch Service采集器未	8	严重	紧急风险治理	1	● 已开启: 1,	/1
	云数据库 KeeWiDB公网未授权访问	<u>න</u>	高危	紧急风险治理	1	• 已开启: 1,	/1
	云数据库 MongoDB公网未授权访	8	高危	紧急风险治理	1	● 已开启: 1,	/1
	云数据库 SQL Server未禁用管理	Ø	高危	紧急风险治理	1	● 已开启: 1,	/ 1
	云数据库Redis公网未授权访问	6	高危	紧急风险治理	1	• 已开启: 1,	/ 1
	存储桶未禁用匿名用户列桶权限	Ø	高危	紧急风险治理	1	● 已开启:1,	/1



## 支持的云产品列表

云厂商	产品分类	产品名称
腾讯云	计質	云服务器
	۶I <del>/ ۲</del>	轻量应用服务器
		容器服务
		容器镜像服务
	容器与中间件	云函数
		消息队列 CKafka 版
		消息队列 TDMQ 版
		<b>负载均衡</b>
		弹性公网 IP
	网络	弹性网卡
		NAT 网关
		私有网络
	CDN 与边缘	内容分发网络 CDN
	安全	Web 应用防火墙
		云防火墙
		密钥管理系统
		云数据库 MySQL
		云数据库 MariaDB
		云数据库 SQL Server
		云数据库 MongoDB
	物坦应	云数据库 PostgreSQL
	жлла <i>н</i>	云数据库Redis
		云数据库 KeeWiDB
		向量数据库
		TDSQL MySQL 版
		TDSQL-C MySQL 版
		对象存储
	存储	云硬盘
		文件存储
	大数据	Elasticsearch Service



		弹性 MapReduce
	云通信与企业服务	SSL 证书
		访问管理
	开发与运维	操作审计
		腾讯云可观测平台
阿里云	计算	云服务器 ECS
	<del>次</del> 現	容器服务
	谷品	容器镜像服务
		负载均衡 SLB
		内容分发网络CDN
		弹性公网IP
	网络与 CDN	弹性网卡 ENI
		NAT 网关
		任播弹性公网 IP
		私有网络
	大数据计算	检索分析服务 Elasticsearch 版
		大数据开发治理平台
	Serverless	函数计算
	中间件	微服务引擎
		API 网关
		云数据库 RDS
		云数据库 MongoDB 版
		云数据库 Tair(兼容 Redis)
		云数据库 ClickHouse
	数据库	云数据库 OceanBase 版
	хлин <del>т</del>	云原生分布式数据库
		云原生数据仓库 AnalyticDB PostgreSQL版
		云原生数据仓库AnalyticDB MySQL版
		云原生数据库 PolarDB
		数据管理服务 DMS
	存储	对象存储 OSS
	1子1頃	日志服务



		Web 应用防火墙
		云安全中心
	安全	云防火墙
		云身份服务
		堡垒机
	迁移与运维管理	访问控制
	计管	Amazon EC2
	비뷰	AWS Lambda
	交叉	Amazon EKS
	17 FF	Amazon ECR
	存储	Amazon S3
		Amazon EFS
	数据库	Amazon RDS
AW/S		Amazon DynamoDB
AWG		Amazon MemoryDB
		Amazon ElastiCache
	联网和内容分发	Amazon VPC
	前端 Web 和移动应用程序	Amazon API Gateway
	应用程序集成	Amazon SQS
	安全性、身份与合规性	Amazon IAM
	公析	Amazon MSK
	ፓጠ	Amazon EMR



## 安全体检

## 功能简介

最近更新时间: 2024-09-03 10:32:21

## 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。

#### 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	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	V	V	Ś	V
应急漏洞	-	V	Ś	V
漏洞风险	-	$\mathcal{A}$	Ś	V
弱口令风险	-	V	Ś	V
云资源配置风险	-	V	V	V
风险服务暴露	-	-	Ś	V
网站内容风险	-	-	Ś	V
体检配额	端口风险检查不消耗配额	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: 2024-09-05 10:12:51

## 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。

安全体检					0
安全体检任务 体检任务 / 总配额 ① 9/10 介 周期任务2个 进行中 0 个	已用体检次数 / 总配额 / 次 升级购买配额 查看报告	<b>安全体检任务执行记录</b> 体检开始时间	体检名称	体检结束时间	操作 详情 详情
创建安全体检任务 停止任务	删除 全部执行情况 ▼		多个关键字用竖线 " " 分隔,	多个过滤标签用回车键分隔	Q ¢

## 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 。



产品管理     产品证维     安全中心     自定义面板4     □     管理面板       安全体检     上次体检时间:          血          本島臨获得本月1次免費 <u>- 編安全体检</u> 机会 ×        分、超越同行业          的用户           重新体检         ピ 评分详情	対張部导航或首页使用有建议或疑问,请向我们反馈 反馈 ✔ 下 ▼ ・・・ 账号ID APPID
当前评分较低,可前往待办事项为核心资产添加防护措施,消除风险隐患,接重并处置 攻击告誓	<b>安全防线</b>
安全防线建设         业务资产梳理         高危风险发现         高危告警处置           道未防护         个未防护         个         个	第二道防线-Web应用防火墙 **** 旗舰版试用中 Web攻击与BOT访问: 个
可试用 全部资产 全部风险 全部内陸 全部告警	■ 第三道防线-主机安全 *** 旗舰版试用中 待处理风险: 个
安全防线建设	展开更多加固防线(4) ~
✓ 云防火墙(第一道防线)	漏洞情报 产品动态 章者更多 C
✓ Web应用防火墙(第二道防线)	Springboot actuator未投权功问 高命 POC 2023-06-30 15:24:49 影响资产 未修复 未防护
✓ 主机安全(第三道防线)	Apache RocketMQ 远程代码执行漏洞(CVE-2023-33246)
业务资产梳理	当前状态 无风险
	Apache-SkyWalking未授权访问
★防护域名资产 ~   共 个 ⑦ 展开 ▼	当前状态 <b>无风险</b>
未防护主机资产         个 I共 个 IZ         可用授权数         开启防护         展开 ▼	OpenSSL X.509 电子邮件地址可变长度缓冲区溢出漏洞 (           高危         POC         EXP         2022-11-02 02:15:00           影响時年         中445         中550
高危风险发现	
<b>云安全态势</b> 腾讯云为企业安全保驾护航,累计服务超过 <b>100万</b> 用户,平均每年防御 <b>1.5万亿</b> 安全威胁,提供自动化安全与响应体系。	
<b>柔</b> 计守护你的云斑产 全网安全态势 - 派洞攻击趋势 - 互联网暴露面	

## 创建任务

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



创建安全体核	<b>验任务</b> IP加白提示 ()
任务名称 🚺	
体检模式	💿 快速体检 🔹 💿 标准体检 💿 高级体检(配置较复杂) 🖪
体检计划 🛈	🔷 立即体检 🔹 🔘 周期任务
	每天 💌 00:00:00
体检项目 🛈	免费体检项目 公网IP和域名资产不消耗配额,主机和容器资产请先开通授权
	🔽 端口风险 👔 🛛 🗹 云资源配置风险 👔 🔽 风险服务暴露 👔
	<ul> <li>消耗配额项目 仅公网IP和域名资产消耗,主机和容器资产请先开通授权</li> <li>✓漏洞风险 (i)</li> <li>✓ 弱口令风险 (i)</li> <li>✓ 内容风险 (i)</li> </ul>
体检资产	◆ 全部资产(197) 从现有资产选择 手动填写 文件导入 剔除资产(0)
	(i) 其中 <u>10</u> 台主机、 <u>2</u> 个容器集群、 <u>6</u> 个容器镜像未授权暂不能执 行体检任务,请先授权。
预计耗时	240分钟
单次消耗 🚺	25/资产/次 (消耗对象为已选中体检资产中的 25 个公网IP和域名)
同意并授权	<b>《体检许可协议,查看详情</b>
承诺添加资	产归本账号所属企业所有,如使用他人资产将由本账号归属企业承担法律责任
	确定取消

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	<ul> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
体检计划	<ul> <li>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。</li> <li>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。</li> <li>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。</li> </ul>



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。

## 编辑任务

- 1. 登录 云安全中心控制台,在左侧导览中,单击**安全体检**。
- 2. 在体检任务列表,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。										
任务ID/名称	任务类型 🔻	体检资产 🕏	体检项目 👅	执行时间 🕈	预估耗时	任务执行情况	体检报告	所属账号 ▼	操作	
	周期任务	1	🖸 🚖 유 🖵 🛞 🔅	每天 00:00:00	约 5 分钟	✓ 已完成 215 次 最近完成: 2024-09-03 00:00:50	215	Ø	编辑	删除
	周期任务	1	🖸 遼 乌 🖵 🌐 🍪	每天 16:17:51	约 6 分钟	✓ 已完成 245 次 最近完成: 2024-09-02 16:24:07	245	<u>&amp;</u>	编辑	删除

3. 在编辑资产体检任务弹窗中,修改相关参数,单击确定。

编辑安全体格	金任务 (i)
任务名称 🛈	
体检模式	🔷 快速体检 🔹 🧿 标准体检 👘 高级体检(配置较复杂) 🖸
体检计划 🛈	○ 立即体检 ○ 定时体检 ○ 周期任务
	每天 🔻 00:00:00
体检项目 🚺	<b>免费体检项目</b> 公网IP和域名资产不消耗配额, 主机和容器资产请先开通授权 □ 端口风险 (〕 □ □ <b>□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □</b>
	消耗配额项目 仅公网IP和域名资产消耗,主机和容器资产请先开通授权
	「加利风」(1) 第二令风」(1) 内谷风」(1) 内谷风」(1)
体检资产	<ul> <li>全部资产(874) ● 从现有资产选择 手动填写 文件导入</li> <li>选择资产(1) 全部资产(874)</li> </ul>
预计耗时	5分钟
单次消耗 🚺	0/资产/次
同意并授权	R体检许可协议,查看详情 8产归本账号所属企业所有,如使用他人资产将由本账号归属企业承担法律责任 确定 取消

## 删除任务

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



任务ID/名称	任务类型 🔻	体检资产 💲	体检项目 🔻	执行时间 🕈	预估耗时	任务执行情况	体检报告	所属账号 ▼	操作
	立即体检	1	1 1 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	2024-09-03 10	约9分钟	✓ 已完成 完成时间: 2024-09-03 10:50:16	1	Ø	编辑 删除
	立即体检	1	🏵 🏵 🖓 📮 🛞 🏵	2024-08-30 17	约 8 分钟	✓ 已完成 完成时间: 2024-08-30 17:56:17	1	⊗	编辑 <b>删除</b>

- 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。

一键下载					多个关键字用竖线 " " 分隔,多	个过滤标签用回车键分隔	Q Ø
报告名称	报告类型 ▼	体检资产 \$	风险统计 \$	体检任务ID/名称	生成时间 🕈	所属账号 ▼	操作
	体检报告	1	1		2024-09-03 10:42:09	<mark>⊗</mark>	预览 下载
	体检报告	1	0		2024-09-03 00:00:22	8	预览 下载

#### 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**。

一键下载					多个关键字用竖线 " " 分隔,多	6个过滤标签用回车键分隔	Q	¢
报告名称	报告类型 ▼	体检资产 🗲	风险统计 \$	体检任务ID/名称	生成时间 \$	所属账号 ▼	操作	
	体检报告	1	1		2024-09-03 10:42:09	Ø	预览 下载	
	体检报告	1	0		2024-09-03 00:00:22	Ø	预览 下载	

○ 批量:选择一个或多个报告,单击左上角的**一键下载**。

一银	下载				TRV TRV	5个关键字用竖线 "I" 分隔,多	个过滤标签用回车键分隔		Q	¢
	报告名称	报告类型 ▼	体检资产 💲	风险统计 🗲	体检任务ID/名称	生成时间 \$	所属账号 ▼	操作		
		体检报告	1	1		2024-09-03 10:42:09	Ø	预览	下载	
		体检报告	1	0		2024-09-03 00:00:22	Ø	预览	下载	
		体检报告	1	247		2024-09-02 16:18:10	Ø	预览	下载	
		体检报告	1	0		2024-09-02 00:00:15	8	预览	下载	



## 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: 2025-05-30 15:48:51

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 如下,共84个 IP。

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 43.139.243.246 119.28.101.45 119.28.101.51 150.109.12.53 129.226.197.194 129.226.197.196 129.226.197.199 129.226.197.200 129.226.197.201 129.226.197.204 129.226.197.205 129.226.197.207 129.226.197.209 129.226.197.21 43.134.229.58 101.33.220.146 182.254.192.73 175.178.79.94 106.55.172.224 119.91.226.99 43.139.53.159 106.55.100.23 106.53.104.226 123.207.45.218



43.136.98.102

云安全中心

43.139.150.105 175.178.22.156 122.152.222.70 159.75.140.45 193.112.176.100 43.136.103.134 101.33.244.20 114.132.180.83 159.75.80.121 43.136.56.35 106.52.219.11 42.193.249.24 43.136.123.68 123.207.72.172 43.139.233.146 119.91.227.203 175.178.108.10 43.136.85.179 111.230.104.109 119.91.226.24 119.91.48.196 101.33.203.139 134.175.222.22 175.178.72.188 175.178.90.4 119.29.244.62 123.207.72.179 175.178.79.108 111.230.243.60 43.138.175.184 134.175.53.125 43.139.204.202 122.152.233.202 175.178.176.234 43.139.244.105 43.139.188.254 159.75.154.2 106.52.244.65 43.138.233.4 159.75.110.155 134.175.248.145

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**。

<b>P查询</b> P查询 封	禁查询		v		
() 在这	里,你可以查询某个	'IP的封堵状态,是否在	EIP黑白名单中, <del>;</del>	是否触发了CC,	自定义人机识别等
输入IP		查询			
查询结果					
请输入IP,	并点击查询。				

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。

查询结果		
IP		拦截
域名		
生效时间		
结束时间		
类别	сс	
触发策略名称	人机识别	
加入黑白名单		

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。

	~
类别 💦 黑名单 🔘 白名单	
IP地址	
截至时间• <b>永久生效</b> ▼	
备注	
添加 取消	

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。

黑白名单 IP黑名单	IP白名单	精准白名单	~ 规则白名单				黑白名单操	作指南 🖸
添加±	也址 删除	注地址 <b>全部翻</b>	除 导入数据	导出全部筛选结果	单个域名量多可以添加20000个IP地址,剩余19998个	获取鼠标焦点即可选择过滤属性	Q	C

#### 2. 在添加白名单页面,配置相关参数,单击确定。

<b>添加白名单</b> IP地址 *	₫ 支持任意IP地均	上,例如10.0.0.10	〕或FF05::B5;支持(	CIDR格式地址,例如	(]
	10.0.0.0/16或F	F05:B5::/60,使	用换行符进行分隔,	一次最多添加1001	
生效方式 *	永久生效	定时生效	周粒度生效	月粒度生效	

#### 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100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。

ау(т ц <del>т</del>		
	<b>寺</b> 入	
	点击按钮,选择文件。	
兄明: 1.格式,仅支持.xlsx,.xls,每次只式 2.数量,每次最多可导入 50 条规则, 3.内容,必须包含类别,IP地址,截。 4.截止时间,必须在2033/12/31 00: 5.导入的格式严格按照导出格式填写	支持单个文件上传。 ,如需导入大量规则,请分多次导入。 止时间三列;具体可参考导出数据excel格式。 :00:00之前,格式YYYY/MM/DD HH:MM:SS。 ,详情请看 <b>IP黑名单操作指南</b> 和I <b>P白名单操作指南</b>	
	協수문 ) 重要	

## 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,进入 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。

IP查询 ▼	IP查询操作指南 IZ
IP查询 封禁查询	
⑥ 这里可以查看到正在封堵状态中的IP记录/这里可以查看动态生成的IP封堵记录,例如CC,自定义人机识别等	×
* <b>类型: ALL ▼ 触发策略:</b> 策略名称 IP地址: 输入IP	
记录创建时间: 近5分钟 近10分钟 近30分钟 2024-09-03 14:11:06 ~ 2024-09-03 23:59:59 首	
<b>友放我中时间</b> 。 2024 00 02 1415-06 2024 00 11 1415-06 ⊨■	
- 円×1000 - 2024-03-03 14,10,00 ~ 2024-03-11 14,10,00 Ⅰ	

## 评分详情

最近更新时间: 2024-09-05 10:12:51

云安全中心将结合各类安全场景下的监控数据,对用户的腾讯云风险情况做出整体评价,并助力提升云上安全水位。

评价方法采用100分制,最高分100分。如果用户存在相关的安全风险,可以按照对应得分途径从当前体检分数提升至 100 分。具体风险点与得分途 径如下:

评分维度	风险点	得分途径	得分分值	得分上限	
	云防火墙	云防火墙普惠版、高级版、企业版、旗舰版 防护中或试用中	0道防线未开通:+10分;1 道防		
安全防线建设	Web 应用防火墙	Web 应用防火墙高级版、企业版、旗舰版、 独享版防护中或试用中	线未开通: +8 分; 2 道防线未开 通: +4 分; 3 道防线未开通: +0 分。	10	
	主机安全	主机安全专业版、旗舰版防护中或试用中			
业务资产梳理	公网 IP 资产	公网 IP 已开启互联网边界防火墙的防护	+(1 – 未防护核心资产数量 / 全 部资产数量)*10分;若资产数为 0,则+10分。		
	域名资产已接入 SaaS 型 Web 应用防火墙 实例或负载均衡型 Web 应用防火墙实例		+(1 – 未防护核心资产数量 / 全 部资产数量)*10分; 若资产数为 0,则+10分。	30	
	主机资产	主机资产已授权开通了主机安全专业版或旗 舰版。	+(1 – 未防护核心资产数量 / 全 部资产数量)*10分; 若资产数为 0,则+10分。		
	端口风险	及时处理云上业务潜在的端口风险	+(1 – 有高危风险的资产数量 / 全部资产数量 )*10分;若资产数为 0,则+10分。		
资产风险发现	漏洞风险	及时处理云上业务潜在的漏洞风险	+(1 – 有高危风险的资产数量 / 全部资产数量)*10分;若资产数为 0,则+10分。	30	
	弱口令风险	及时处理云上业务潜在的弱口令风险	+(1 – 有高危风险的资产数量 / 全部资产数量 )*10分;若资产数为 0,则+10分。		
高危告警处置	高危告警	及时处置云上业务的高危告警	+(1 – 有高危告警的资产 / 全部 资产)*30	30	

() 说明

• 每个风险点均设计有最高得分上限。

• 评分解读:

○ 评分低于 60 分时,安全性较差,系统将按照红色呈现安全评分。

- 评分大于等于 60 分,小于 80 分时,风险较为可控,系统将按照黄色呈现安全评分。
- 评分大于等于 80 分,小于 95 分时,风险可控,系统将按照蓝色呈现安全评分。
- 评分大于等于 95 分时,安全性较高,系统将按绿色呈现安全评分。



## 热点问题

最近更新时间:2024-08-28 09:25:01

#### 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 。

#### 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。

#### 安全体检能支持多少企业 IT 资产的扫描?

安全体检依托腾讯云的计算能力,能够做到快速扩容,支持对千万级 IT 资产的扫描。

#### 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。

#### 安全体检有哪些扫描 IP?

安全体检通过公网模拟黑客入侵(无害的攻击)的方式进行安全扫描。如果您的服务器有相关防护措施或者限制了访问的 IP,为保证扫描的正常进 行,建议您将以下 IP 地址加到白名单。

安全扫描节点 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

## 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,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,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	repositor y	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 应该开启自动 备份	数据安全	redis	中危	默认安全规 范,网络安 全等级保护	判定 Redis 数据库的备份功能是否异常, 正常情况下,数据应该至少每天备份一 次。


				三级技术要 求	
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	mongod b	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 MariaDB 数据库不建议对公网 开放访问	网络访问控制	mariadb	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。
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 存储桶应开启服 务端加密	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	存储桶支持在对象级别上应用数据加密的 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 三级技术要 求	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。
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 据库审计保留时间应 满足要求	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	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



				三级技术要 求	也可以满足安全合规等要求。(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。
<del>子账号</del> 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。
协作者不应该同时使 用编程访问与用户界 面访问	基础安全防护	cam	高危	默认安全规 范	协作者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。
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 AP I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。
高风险权限子账号不 建议启用 API 密钥	基础安全防护	cam	低危	默认安全规 范	高权限子账号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。
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。



# 云边界分析 功能简介

最近更新时间: 2025-06-24 11:29:42

云安全中心将展示您云租户互联网边界的整体状态,帮助您进行日常的边界管理。该功能包含了**互联网边界**与**扫描结果**,数据来源于**边界梳理与安全** 体检。

- **互联网边界**:通过分析云上资产关联关系(如 CLB/CDN 绑定关系等),绘制资产面向互联网暴露的路径,同时结合资产状态、安全组策略,得 到资产面向互联网的开放状态,即互联网边界。
- 扫描结果:通过安全体检对您的公网资产进行扫描,获取开放的端口服务、Web 服务,并检查存在的高危端口、风险页面、漏洞、弱口令等风 险。

### 前提条件

已购买 云安全中心旗舰版。

### 边界开放状态

云安全中心,将根据资产的属性、关联关系、访问控制状态等梳理互联网边界。根据网络状态分为:

网络状态	详情
完全开放	互联网所有地址均可访问该端口。
受限访问	云资源设置了访问控制,仅白名单里地址可访问该端口。
无法访问	云资源状态异常或关机,因此无法被访问。

示例:您的负载均衡资产(IP:1.1.1.1)创建了80端口的监听器,监听器的后端服务是两台云服务器。以下不同情况对应不同的开放状态: • 负载均衡的安全组开放了允许0.0.0.0/0访问80端口,两台云服务器均处于正常运行状态。

IP	通口	开放状态
1.1.1.1	80	完全开放

• 负载均衡的安全组开放了允许2.2.2.0/24访问80端口,两台云服务器均处于正常运行状态。

IP	端口	开放状态
1.1.1.1	80	受限访问(白名单: 2.2.2.0/24)

• 负载均衡的安全组开放了允许0.0.0.0/0访问80端口,两台云服务器均处于关机状态。

IP	端口	开放状态
1.1.1.1	80	无法访问

() 说明:

实际上,决定开放状态的因素还包括负载均衡状态、监听器状态、以及云服务器安全组是否允许负载均衡的访问。这些可能的影响因素都被 视为判断开放状态的条件。

### 查看数据

- 1. 登录 云安全中心控制台,在左侧导览中,单击云边界分析。
- 2. 在云边界分析页面,支持查看统计面板、数据详情,其中统计面板包含**云边界统计**和**扫描结果统计**。



云边界统计	300			网络扫描结果统计(近7天)	⊻.		
<b>10</b> 560↑ 近7天新増 ◆ 32				第日服务 204 ↑	web服务 76↑	C	
• 完全开放 ()	04–03 247 ↑ ● 受限访	04-05 © (i) 248 ↑	04-07 ● 无法访问〔) 65 个	<ul> <li>高危端口服务 128</li> </ul>	• 风险Web服务 20	<ul> <li>漏洞风险 65</li> </ul>	<ul> <li>弱口令风险</li> </ul>
互联网边界①	网络扫描结果(345) ①						
边界列表 暴	露路径						
全部端口标签 、 域名/IP	全部 ~ 端口/标签	开放状态(i) 🛙	最近发现时间 ~ 2025-04-09 1 资产ID/名称	17:02:25 ~ 2025-04-10 17:02:25 资产类型 ⑦ 网络扫描结果 ↓	多个关键字用竖线 " " 分隔,	多个过滤标签用回车键分隔 首次所属账号 7	Q C ② 也 操作
119	1-65535 非标端口 高危端口	完全开放	in Éir- t	云服务器 端□: 8 异 Web服务: 7 异	常1 漏洞:3 常2 弱口令:0	202 202	详情 发起扫描
43.1	1-65535 非标端口 高危端口	完全开放	in∈ ⊈3 tk er	云服务器 端口:7 异 Web服务:6 异	常 1 第 2 弱口令: 0	202 202 🙆 🗾	详情 发起扫描
43	1-65535 非标端口 高危端口	完全开放	ins 🗘	云服务器 端口:6 异 Web服务:4 异	常 2 漏洞: 5 常 2 弱口令: 0	202 202	详情 发起扫描
13	1-65535 非标端口 高危端口	完全开放	i X	云服务器 端口:6 异 Web服务:4 异	常 2     漏洞: 5 常 2    弱口令: 0	202 202	详情 发起扫描

### 数据详情的数据内容如下表:

主标题	二级标题	功能简介
互联网边界	边界列表	展示互联网边界数据台账,每个边界端口(或端口范围)关联扫描结果,以便您查询面向互联 网的资源的状况。
	暴露路径	根据输入的资产信息以 <b>树状图</b> 的形式该资产所有面向互联网暴露的路径,展示网络链路前后关 联关系。
	端口服务	展示扫描发现的互联网端口及服务信息。
扫描往田	Web服务	展示扫描发现的 Web 服务及组件信息。
口油石米	漏洞风险	展示扫描发现的漏洞。
	弱口令风险	展示扫描发现的弱口令。

### 3. 在云边界分析页面,单击边界梳理,即可触发边界的梳理任务。

云边界分析					
边界梳理	J	安全体检	综合体检结果	~	

## 安全体检

对互联网地址进行扫描,并将结果与互联网边界的资产进行关联。涉及的体检项目:端口风险、风险服务暴露、漏洞风险、弱口令风险。



- 1. 登录 云安全中心控制台,在左侧导览中,单击云边界分析。
- 2. 在云边界分析页面,单击**安全体检**,弹出对话框进行扫描。若需要了解安全体检的详细内容,可访问<u>文档</u>。

创建安全体格	✿任务 IP加白提示 (i)
任务名称 🛈	100014592178_标准体检_每天00:00:00_20250305
体检模式	🔷 快速体检 🔹 🔿 标准体检 👘 高级体检(配置较复杂)
体检计划 🛈	🔷 立即体检 🔹 💿 周期任务
	每天 🔻 00:00:00
体检项目 🛈	免费体检项目 公网IP和域名资产不消耗配额,主机和容器资产请先开通授权 ✔ 端口风险 (i)
	<ul> <li>消耗配额项目 仅公网IP和域名资产消耗,主机和容器资产请先开通授权</li> <li>✓ 漏洞风险 (i)</li> <li>✓ 弱口令风险 (i)</li> <li>内容风险 (i)</li> </ul>
体检资产	◆ 全部资产(233) 从现有资产选择 手动填写 文件导入 剔除资产(0)
	<ul> <li>其中<u>5</u>台主机、<u>2</u>个容器集群、<u>7</u>个容器镜像未授权暂不能执行体检任务,请先授权。</li> </ul>
预计耗时	240分钟
单次消耗 🚺	40/资产/次 (消耗对象为已选中体检资产中的 40 个公网IP和域名)
同意并授权	《体检许可协议,查看详情
承诺添加资	产归本账号所属企业所有,如使用他人资产将由本账号归属企业承担法律责任
	确定取消

3. 需要使用到的体检项目:端口风险、风险服务暴露、漏洞风险、弱口令风险。页面默认勾选了这四个选项。请阅读体检许可协议后,勾选两个确 认框后,单击**确定**即可发起体检。

## 支持的云产品实例类型

目前,云边界分析已支持以下云产品,产品分类及名称参考云厂商官网文档。

云厂商	产品分类	产品名称	
腾讯云	计管	云服务器	
	비দ	轻量应用服务器	
		负载均衡	
	网络	弹性公网 IP	
		弹性网卡	
		NAT 网关	
	CDN 与边缘	内容分发网络 CDN	



	安全	Web 应用防火墙			
		云数据库 MySQL			
		云数据库 MariaDB			
	***	云数据库 SQL Server			
	剱/茄/ <del>年</del>	云数据库 MongoDB			
		云数据库 PostgreSQL			
		云数据库Redis			
	存储	对象存储			
	大数据	Elasticsearch Service			
	计算	云服务器 ECS			
		负载均衡 SLB			
		内容分发网络CDN			
		弹性公网IP			
	网络与 CDN	弹性网卡 ENI			
		NAT 网关			
<b>应用</b> —		任播弹性公网IP			
判主工	大数据计算	检索分析服务 Elasticsearch 版			
	Serverless	函数计算			
		云数据库 RDS			
	数据库	云数据库 MongoDB 版			
		云数据库 Tair ( 兼容 Redis )			
	存储	对象存储 OSS			
	安全	Web 应用防火墙			



## 查看统计面板

最近更新时间: 2025-04-11 17:39:02

## 暴露统计

- 1. 登录 云安全中心控制台,在左侧导览中,单击**云边界分析**。
- 统计面板左侧即云边界统计。云边界统计的数据取自最近识别时间在24小时内的互联网端口。云安全中心根据云资源的策略及状态将互联网端口的开放状态分为以下三类:

开放状态	状态说明
完全开放	互联网所有地址均可访问该端口。
受限访问	云资源设置了访问控制,仅白名单里地址可访问该端口。
无法访问	云资源状态异常或关机,因此无法被访问。

云边界统计		网络扫描结果统计(近7天) 🜛					
<b>互联网边界</b> ① 560 个 近7天新増↑32	300 200 100 04-03 04-05 04-07 04-09	端口服务 web服务 204 ↑ 近7天新増↑204 近7天新増↑76	0				
• 完全开放 ()	247 ↑     • 愛爾访问 ①     248 ↑     • 无法访问 ①     65 ↑	• 高危端口服务 128 • 风险Web服务 20 • 漏洞风险	65 • 弱口令风险 0				

3. **功能交互**:单击4个统计数据,将在下方**互联网边界−边界列表**内,展示具体的结果。下图是点击**云边界统计**面板中"**受限访问**"对应数字的展示 结果。

<b>互联网边界</b> () 网络	各扫描结果(345) ①						
边界列表 暴露路径	£						
全部端口标签 🖌	全部	l	最近发现时间 > 2025-04-09	17:07:42 ~ 2025-0	4-10 17:07:42 📋 开放状态: 受限访问		Q Q 尊 F
域名/IP	端口/标签	开放状态 访 🝸	资产ID/名称	资产类型 🍸	网络扫描结果 \$	首次 所属账号 ⑦	操作
139.	1-65535 非标端口 高危端口	受限访问 ①	in: 未	云服务器	未扫描	202 202	详情 发起扫描
128 B	1-65535 <u>非标端口</u> 高危端口	受限访问 ①	ii D 2	云服务器	未扫描	202 202	详情 发起扫描
114	1-65535 <u>非标端口</u> 高危端口	受限访问 ①	jn:	云服务器	未扫描	202 202	详情 发起扫描
12:	1-65535 非标端口 高危端口	受限访问 ①	in c	云服务器	未扫描	202 202	详情 发起扫描
106.	1-65535 非标端口 高危端口	受限访问 ①	in. 未f	云服务器	未扫描	202 202	详情 发起扫描
43	1-65535 <u>非标端口</u> 高危端口	受限访问 ①	ins- o tk1	云服务器	未扫描	202 202	详情 发起扫描
43.	1-65535 非标端口 高危端口	受限访问 🛈	in : tk	云服务器	未扫描	202 202	详情 发起扫描

4. 云边界数量趋势图:展示了近7天边界数量的整体趋势。



## 扫描结果统计

- 1. 登录 云安全中心控制台,在左侧导览中,单击云边界分析。
- 2. 统计面板右侧即扫描结果统计。扫描结果取自安全体检中近7天网络扫描的结果,涉及的体检项为端口风险、风险服务暴露、漏洞风险、弱口令风 险。数据统计的性质说明如下表:

统计内容	内容说明
端口服务	通过扫描发现的端口服务。
Web 服务	通过扫描发现的Web服务。
高危端口服务	扫描识别为高危服务的端口服务,如:mysql、redis 等。
风险 Web 服务	扫描识别为高危的 Web 服务,如:Jenkins、phpmyadmin 等。
漏洞风险	扫描发现的漏洞。
弱口令	扫描发现的弱口令,如:ssh 弱口令、Web 后台弱口令。

云边界统计				网络扫描结果统计(近7天) 👌									
<b>互联网边界 ①</b> 560 个 近7天新增↑32	200 200 0 0 0 0 0 0 0 0 0 0 0 0		<b>端口服务</b> 204 <sub>个</sub> 近7天新増↑204		web服务 76 ↑ 近7天新増↑76		0						
• 完全开放 (i)	<b>247</b> ↑	• 受限访问 ()	<b>248</b> ^	● 无法访问 ()	<b>65</b> 个	● 高危端口服务	128	● 风险Web服务	20	• 漏洞风险	65	• 弱口令风险	0

3. **功能交互**:单击**扫描结果统计面板中**的**统计数字**,将在下方**扫描结果**的对应 Tab 页面,展示具体的结果。下图是单击"**高危端口服务**"对应数字 的展示结果。

互联网边界 ① 网络扫描组	<b>詰果(345)</b> ()									
端口服务(204) Web朋	务(76)	漏洞风险(65)	弱口令风险(0)							
标记处置 标记忽略	全部处理状态	~	最近发现时间 >	2025-04-09 17:07:42 ~ 20	025-04-10 17:07:42	<b>自</b> 多个关键字	用竖线 " " 分隔,多个过滤标:	签用回车键分隔	QB	戀 平
域名/IP	端口	服务判定 🍸	资产ID/名称	资产类型 🔽	组件	服务/协议	首次/量 所属账号 🕜	处理状态 (i)	操作	
10'	139	高危服务	in wi	CVM	samba	netbios-ssn tcp	2025- 2025-	未处理	封禁端口 更多、	~
111.	139	高危服务	ins wi	CVM	samba	netbios-ssn tcp	2025- 2025-	未处理	封禁端口 更多、	~
48	139	高危服务	in w	CVM	samba	netbios-ssn tcp	2025- 2025-	未处理	封禁端口 更多、	~

4. 功能交互:单击该导出按钮,可以下载全部扫描结果。



5. 通过调整体检任务,可以查看不通体检任务的结果。综合体检结果即根据所有体检任务的结果进行汇总。体检任务的切换只影响扫描结果,不影响互联网边界的结果。



边界梳理	安全体检	综合体检结果 🛛 🗡					
云边界统计	200	请输入体检报告ID/名称进行搜索			Q	(近7天) ۓ	
互联网边界 🕦	200 -	体检报告ID/名称	体检计划 了	体检资产 💲	所属账号 ⑦	Web服务	$\mathbf{\cap}$
<b>560</b> 个 近7天新增 ↑ 32	100 - 0 -	rpt-7t - 2 高级体 寸	周期任务	429	<mark>⊘</mark> 100	<b>76</b> ↑ 近7天新增↑76	
• 完全开放 ()	<b>247</b> ↑	rpt-e 9d 标准体 78	立即体检	425	2 100	128 • 风险Web服务 20 • 漏洞风险	65 • 弱口令风险 0



## 查看边界列表

最近更新时间: 2025-04-11 17:39:02

## 查询边界列表

1. 登录云安全中心控制台,在左侧导览中,单击云边界分析。

### 2. 在**云边界分析 > 互联网边界 > 边界列表**中,支持查看云上互联网边界的详细列表。

互联网边界 ①	网络扫描结果(65) ①						
边界列表 暴露	露路径						
全部端口标签 🖌	全部 🗸		最近发现时间 > 2025-04-09	9 17:19:52 ~ 2025-04	4-10 17:19:52 📋 开放状态: 完全开放		Q C 🕸
域名/IP	端口/标签	开放状态 访 🕆	资产ID/名称	资产类型 🍸	网络扫描结果 ↓	首次 所属账号 了	操作
42	1-65535 <u>非标端口</u> 高危端口	完全开放	ins-p [auto	云服务器	<ul> <li>端口:4 异常3</li> <li>漏洞:1</li> <li>Web服务:1 正常</li> <li>弱口令:1</li> </ul>	202 202	详情 发起扫描
182.	1-65535 非标端口 高危端口	完全开放	ins-kia [aut	云服务器	<ul> <li>端口:3 异常1</li> <li>通洞:1</li> <li>Web服务:2 正常</li> <li>弱口令:0</li> </ul>	202 202	详情 发起扫描

### 特殊的展示字段说明如下表。

字段名	示例	说明
端口	<ul><li> 1−65535</li><li> 22</li></ul>	端口是根据云资源的访问控制规则获取,如您的安全组如果配置了1~65535的开放策略,那 么1~65535就会被定为一个边界。
端口标签	<ul><li>● 高危端口</li><li>● 非标端口</li></ul>	端口标签直接根据端口号进行判定。定义端口标签是为了帮助您更好的规范网络开放端口。 • 高危端口:以下端口将被视为高危端口:22、23、135、137、139、161、1099、 1433、1521、3306、3389、5432、8000、9200、27017。 • 非标端口:非 80,443的端口将被视为非标端口。
开放状态	<ul> <li>完全开放</li> <li>受限访问</li> <li>无法访问</li> </ul>	开放状态是云安全中心根据资产的属性进行判断的接口,代表您网络策略配置的状态,并不是 指扫描结果。 • 完全开放: 互联网所有地址均允许访问该端口。 • 受限访问: 云资源设置了访问控制,仅允许白名单里地址访问该端口。 • 无法访问: 云资源状态异常或关机,因此无法被访问。
扫描结果	● 未扫描 ● 0	资产经过体检中相关扫描后,即可获取扫描结果。结合扫描结果可以提升治理优先级。 • 0代表扫描未发现端口开放情况。 • 未扫描即该资产未经过扫描,无法获取扫描结果。 • 扫描结果包含:端口服务、Web 服务、漏洞、弱口令。
发现时间	2025-02-28 00:00:00	<ul> <li>首次发现时间:代表首次记录该互联网边界数据的时间。</li> <li>最近发现时间:代表该互联网边界数据最近被更新的时间。每一次对互联网边界进行统计时,若发现该数据,即更新时间。因此,您可以根据最近发现时间判断该边界是否仍存在。</li> </ul>

特殊过滤条件说明如下表:

|--|



端口标签	<ul> <li>● 高危端口</li> <li>● 非标端口</li> <li>● 其他</li> </ul>	如果您期望网络开放按一定的规范进行,那么您可以根据筛选不同的端口标签和开放状态来进 行网络规范治理。				
开放状态	<ul> <li>完全开放</li> <li>受限访问</li> <li>无法访问</li> </ul>	如:除报备的特殊需求场景外,80,443是唯一允许开放至互联网的端口。那您可以过滤完全 开放并且标签为非标端口的边界。				
扫描结果	<ul> <li>端口可访问</li> <li>存在 Web 服务</li> <li>存在高危服务</li> <li>存在风险 Web 页面</li> <li>存在漏洞</li> <li>存在弱口令</li> </ul>	<ul> <li>选项说明:</li> <li>端口可访问:互联网边界端口范围内,扫描发现端口可访问。</li> <li>存在 Web 服务:互联网边界端口范围内,扫描发现 Web 服务。</li> <li>存在高危服务:互联网边界端口范围内,扫描发现高危服务,如 mysql、ssh 等。</li> <li>存在风险 Web 页面:互联网边界端口范围内,扫描发现可能存在风险的 Web 服务,如 jenkins。</li> <li>存在漏洞:互联网边界端口范围内,扫描发现漏洞。</li> <li>存在弱口令:互联网边界端口范围内,扫描发现系统弱口令。如ssh弱口令、网站后台弱口令。</li> <li>您可以根据不同的风险优先级来推进治理工作。</li> </ul>				

### 3. 单击后侧的**导出**按钮,可以将数据进行导出,格式是 Excel。

<b>互联网边界 ①</b> 网	络扫描结果(65) 🛈						
边界列表 暴露路	径						
全部端口标签 🖌 🖌	全部 🖌		最近发现时间 ~ 2025-04-09 1	7:19:52 ~ 2025-04	10 17:19:52 📋 开放状态: 完全开放		र द \$ <del>\$</del> कि
域名/IP	端口/标签	开放状态 访 🝸	资产ID/名称	资产类型 🔽	网络扫描结果 ↓	首次 所属账号 ⑦	操作
42.1	1-65535 非标端口 高危端口	完全开放	ins-r [al	云服务器	<ul> <li>端口:4 异常 3 漏洞:1</li> <li>Web服务:1 正常 弱口令:1</li> </ul>	202 202	详情 发起扫描
182.	1-65535 非标端口 高危端口	完全开放	ins-l [autotest	云服务器	<ul> <li>端口: 3 异常 1 遍洞: 1 </li> <li>Web服务: 2 正常 </li> </ul>	202 202 📀 📕	详情 发起扫描

## 边界详情

- 1. 登录云安全中心控制台,在左侧导览中,单击**云边界分析**。
- 2. 在**云边界分析 > 互联网边界 > 边界列表**中,选择目标数据,单击**详情**。

互联网边界 ①	网络扫描结果(65) ①						
边界列表 暴	露路径						
全部端口标签 ~	<b>全部</b>	•	最近发现时间 ~ 2025-04	-09 17:19:52 ~ 2025-04-	-10 17:19:52 📋 开放状态: 完全开放		く 5 尊 平
域名/IP	端口/标签	开放状态 🕕 🝸	资产ID/名称	资产类型 🍸	网络扫描结果 ↓	首次 所属账号 冚	操作
42.1	1-65535 非标端口 高危端口	完全开放	ins-p1, [autote	云服务器	<ul> <li>端口:4 异常3     <li>温洞:1     <li>Web服务:1 正常     <li>弱口令:1     </li> </li></li></li></ul>	202 202 🔗	详情发起扫描

3. 在边界详情页面上方提供了互联网边界的详情信息、端口配置建议。



边界详情					发起扫描 ×
42. 1-65500- 非称 高近		开放状态	完全开放		
资产ID ins-, 资产名称 [autote 资产类型 云服务器		首次发现时间 最近发现时间 所属云账号	2025-01-21 11:33:38 2025-04-10 17:13:00 ☎		
♀ 端口配置建议					展开建议 ▼
网络扫描结果 7         暴露路径           端口服务 (4)         Web服务 (1)         漏洞风险 (1)         弱口令风险 (1)					<b>不</b> 會用
标记处置 标记忽略 全部处理状态 🖌	最近发现时间 > 选	择时间	选择时间	多个关键字用竖线 " " 分隔,多个过滤标签用	回车键分隔 Q
域名/IP 端口 服务判定 订	组件	服务/协议	首次/最近发现时间 \$	处理状态 ①	操作
42.18 21 高危服务	vsftpd	ftp tcp	202 202	未处理	封禁端口 更多 >
42.1 22 高危服务	OpenSSH	ssh tcp	202 202	未处理	封禁端口

### 4. 单击**展开建议**,可查看对应的**端口配置建议**。

收起建议 ▲

5. 在边界详情页面,支持通过切换 Tab 页面查看该互联网边界的扫描结果。

网络扫扫	描结果 7	暴露路径							
端口)	服务(4)	Web服务(1) 漏洞风险	(1) 弱口令风险(1)	]				<u>↓</u> €	身出
标记	处置	标记忽略 全部处理状态 🗸		最近发现时间 ~	选择时间	选择时间	多个关键字用竖线 "I" 分隔,多个过滤	际签用回车键分隔 Q	
	域名/IP	端口	服务判定 了	组件	服务/协议	首次/最近发现时间 💲	处理状态 ①	操作	
	42	21	高危服务	vsftpd	ftp tcp	2024 2021	未处理	封禁端口 更多 ~	
	4:	22	高危服务	OpenSSH	ssh tcp	2024 2025	未处理	封禁端口	
	42	515	高危服务	-	unknown tcp	202! 202!	未处理	封禁端口 更多 >	
	41	80	web服务	多个 (2)	http tcp	2024 2025	无需处理〔〕	封禁端口	
共 4 项							10 ~ 条 / 页	⊌ ◀ 1 /1页 ▶	

6. 单击暴露路径,可以查看该公网资产的后端资源信息。有关暴露路径功能的详细信息,请参阅文档。





## 检索暴露路径

最近更新时间: 2025-04-11 17:39:02

## 功能介绍

暴露路径提供了基于资产信息来检索资产暴露路径的功能。如果您购买了主机安全产品,还将展示主机对应的进程信息、漏洞信息、高危基线风险信息。通过暴露路径,您可以输入某个**公网资产**,云安全中心将展示该资产后端挂载服务的映射路径,甚至看到具体的端口进程是什么。您也可以输入 某个**内网资产**,查看其通过哪些网络设备(如:NAT网关、弹性公网、负载均衡、CDN)等面向互联网开放的过程。

## 暴露路径检索

- 1. 登录云安全中心控制台,在左侧导览中,单击云边界分析。
- 2. 在云边界分析 > 互联网边界 > 暴露路径中,支持检索资产暴露路径。

〕 暴露路径需要通过您	输入对应参													
→ 暴露路径需要通过您	給入対応参													
	101/1/12/8	<b>▶数</b> 检索查看,您可以在	下方输入对机	应资产ID、域名或IP,	回车或点击搜	索按钮可以发起	重询。							
请输入资产 ID	Q	请输入域名	Q	请输入IP	Q	请输入端口	C	ξ · · · · ·						+
					· · · · · .		次立のが	口进行本达						
					4	月相八IP, 收石	,页/10,灿	山匹1」트미						

3. 输入资产 ID、域名或 IP 的一个或多个,即可开展检索,输入端口可以得到更精确的路径。页面分为树状图和数据详情列表两个部分。



边界列表 暴露路	₹.								
<ol> <li>暴露路径需要通过您</li> </ol>	<b>输入对应参数</b> 检索查看,您可以在	下方输入对应资产ID、域名或IP,回车或s	ā击搜索按钮可以发起查询。						×
请输入资产 ID	Q 请输入域名	Q 172.16.0.4 🛛	Q 请输入端口 Q						+ -
				ins-		ins			
				11 61:80		172.18.0.4:80			
				/		· · · · · · · · · · · · · · · · ·			
				/		💼 ins-4			
				11 61:22*		172.16.0.4:22			
				(B) ins-		(E) ins			
			· · · · · · · · <u>· ·</u> · · · //·,						
				112 01502	n 💬	172.16.0.4:8081			
			and the second sec						
				ins 3m		ins-			
				118 01:908	0(	172.16.0.4:8080			<ul> <li>完全开放</li> </ul>
				· \ · · · · · · · · · · · · · · · · · ·					<ul> <li>受限访问</li> </ul>
				n ins- n		ins-			● 天法法问
				118. 61:338	•	172.16.0.4:3389			
									◎ 仔住扫描风险
					(	💼 ins 🔛			○ 后端服务节点
				118.	5635	172.16.0.4:1-65535			○ 后端服务节点 (异常)
	后端服务节点(7) 主相	〕列表(2) 主机进程(0) 主	几风险(104)						
互联网节点(7)									
互联网节点(7) 							多个关键字用竖线 "	7 分隔,多个过滤标签用回车键分隔	0 8 🕸 🗄
互联网节点(7) 	端口/标签	开放状态 ① ⑦	资产ID/名称	资产类型 🔽	网络扫描结果 \$		多个关键字用竖线 "P <b>首次/最近发现时间</b> \$	· 分隔, 多个过滤标签用回车键分隔 <b>所属账号</b>	Q C 愈 d
互联网节点(7)	端口/标签 1-65535 <del>非标项口</del>	开放状态 ① <b>マ</b> 完全开放	资产ID/名称 int / \$	资产类型 7 <b>云服务器</b>	网络扫描结果 ‡		多个关键字用竖线 " 管次/最近发现时间 非 2025-03-06 22:01:33 2025-04 40 27:11:42	2 分類、多个过滤标签用回车键分离 所属账号	Q 2 8 2
互联网节点(7) £名/IP 118. 31	端口/标签 1-65535 <del>1-5</del> 535 <b>- 1-</b> 5535 <b>- 1-55</b> <b>- 1- 1- 1- 1- 1- 1- 1- 1</b>	开放状态 ① 〒 完全开放	资产ID/名称 Int ws	资产类型 了 云服务器	网络扫描结果 ↓ 0		多个关键字用竖线"" 首次爆近发现时间 2025-03-06 22:01:34 2025-04-10 17:11:42	2 分開,多个过滤标准用回车键分隔 所属账号	<ul> <li>Q 2 3 4</li> <li>操作</li> <li>后端服务节点详情 发起扫描</li> </ul>
互联网节点(7) 1名/IP 18. 31	端口/振莲 1-65535 北核城口 高危雄口 22	开放状态 ① マ 完全开放	资产ID/名称 Inj · · · · · · · · · · · · · · · · · · ·	资产类型 マ 云蜀秀器	网络扫描结果 : 0		多个关键字用接线"1 蓄沈/最近发现时间 : 2025-03-06 22:01:3 2025-04-10 17:11:42 2025-03-06 22:01:3	· 分類、多个过滤标签用回车键分類 所質账号	Q         2         第         2           操作         后端服务节点详情         发起扫描
互联网节点 (7) 名/IP IB. 31 ٤	罐口/标签 1-65535 (基础) 高危端口 22 (半线) 高度第口	开放状态 ① マ 完全开放 完全开放	资产ID/名称 Inj · · · · · · · · · · · · · · · · · · ·	资产类型 ▽ 云磁务器 云磁务器	网络扫描结果 : 0		多个关键字用接线 11 首次编近发现时间 : 2025-03-06 22:01:34 2025-04-10 17:11:42 2025-03-06 22:01:33 2025-04-10 17:11:42	* 分類,多个过滤器蛋用回车键分類 * 分類,多个过滤器蛋用回车键分類 * ② ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	Q         2         3         4           操作         馬端服务节点详情 发起扫描

## 暴露路径树状图

资产暴露路径将通过树状图的形式进行展示,初始节点为互联网 Internet,面向互联网的节点即为互联网节点,后续所有资产节点为后端服务节点,主机类资产可以关联到进程端口节点。若进程存在漏洞或高危基线风险,则会关联风险节点。以下是节点的状态说明。

节点类型	颜色区分	说明
互联网节点	<ul> <li>红色:完全开放</li> <li>橙色:受限访问</li> <li>灰色:无法访问</li> </ul>	<ul> <li>完全开放: 互联网所有地址均允许访问该端口。</li> <li>受限访问: 云资源设置了访问控制,仅允许白名单里地址访问该端口。</li> <li>无法访问: 云资源状态异常或关机,因此无法被访问。</li> </ul>
后端服务节点	<ul><li>● 蓝色:正常</li><li>● 灰色:异常</li></ul>	<ul> <li>正常:资产处于正常运行、激活等状态。</li> <li>异常:资产处于关机、未激活等异常状态。</li> </ul>

2. 在暴露路径中,将鼠标放置于节点上,可以查看节点的详细信息。



	ns-a71 2 / / / / / / / / / / / / / / / / / /	<b>10.1</b> 65535
	1-65535 扫描风险 2 资产ID ins- <i>i</i> 资产名称 资产类型 云服务器 所属云账号 ② 转发规则 -	
(1) 主机进程(32) 主机风险(3) ① 亚 资产ID/名称	域名     -       lp     132       访问控制类型     白名单       访问控制名单     0.0.0.0/0       首次发现时间     2025-01-12 12:29:00       最近发现时间     2025-01-12 12:29:00	多个关键字

## 数据详情列表

在暴露路径中,云安全中心将根据暴露路径的节点信息提供更详细的数据展示。

• 互联网节点列表: 展示面向互联网的节点的数据信息。

互联网节点(1) /	后端服务节点(1)	主机列表(1)   主机进程	』(31) 主机风险(2)				
					多个关键字用竖线 " " 分隔,多个过	這标签用回车键分隔	く 5 袋 下
域名/IP	端口/标签	开放状态 (i) 了	资产ID/名称	资产类型 🔽	扫描结果 🗅	所属账号	操作
139.155	1-65535 高危端口 非标端口	完全开放	ins- 📩 🏠 fer	云服务器	端口: 3	<mark>⊘</mark> . ■.	后端服务节点详情 重新扫描
共1项						10 ~ 条 / 页   阔 🔌	1 /1页 ▶ ▶

• 后端服务节点列表:展示互联网节点后映射的后端服务的数据信息。

互联网节点(1) 后端服务节点(1)	主机列表(1)   主机进程(31)	主机风险(2)			
				多个关键字用竖线 " " 分隔,多个过滤标签用回驾	F键分隔 Q
资产ID/名称	资产类型 了	端口	域名/IP	实例状态 ℃	所属账号
ir 🕰	云服务器	1-65535	10.195	• 运行中	⊗ 1
共1项				10 🗸 条 / 页 🛛 🔘 🔳	1 /1页 ▶ ▶

• 主机列表: 展示通过主机安全采集到的主机进程信息,以便您了解主机上的应用信息、端口监听情况。



互联网节点(1)  后端服	务节点(1) <b>主机列表(</b>	l) 主机进程(31) 主机风险(2)						
<ol> <li>     数据来源于各个云平台   </li> </ol>	主机安全/安全中心产品,若您未购买	或未开启,则无法获取数据。						×
					多个关键字用竖线" "分隔,	多个过滤标签用回车键分隔	Q	⊻
资产实例ID/名称	IP地址 了	资源标签	资产类型 🔽	地域 了	漏洞风图 所属账号	防护状态 ⑦ 操作	Ē	
ins- 💭	公网: 138 内网: 10.1		CVM	成都	6 🙆	旗舰版防护中防护	▷详情 更多 >	
共1项					1	0 ❤ 条 / 页	/1页	► H

• 主机进程列表: 展示通过主机安全采集到的主机进程信息,以便您了解主机上的应用信息、端口监听情况。

互联网节点(1) 后端服约	务节点(1)    主机列表(1)	<b>主机进程(31)</b> 主机风险(2) 				
<ul> <li></li></ul>	机安全/安全中心产品,若您未购买或未	开启,则无法获取数据。				×
						بة.
资产ID/名称	IP地址	资源标签	进程信息	cmdLine	端口	所属账号
ins- fer.	公网: <mark>139.</mark> 内网: 10.1!	核心资产 undefined	536 systemd- logind	/usr/lib/systemd/systemd-logind	-	<u>&amp;</u>
ins- 🖄 fen:	公网: <mark>139</mark> . 内网: 10.1	核心资产 undefined	407 Ivmetad	/usr/sbin/lvmetad -f	-	<mark>⊗</mark>
ins 🎝 fer	公网: 135 内网: 10. <sup>-</sup>	核心资产 undefined	537 dbus-daemon	/usr/bin/dbus-daemonsystem address=systemd:noforknopidfile systemd-activation	-	۵
ins 🗘 fer	公网: 135 内网: 10.	核心资产 undefined	5941 YDService	/usr/local/qcloud/YunJing/YDEyes/YDService	-	ø

### • 主机风险列表:分为主机漏洞、主机高危基线风险。高危基线风险包含弱口令检查、未授权访问等。

互联网节点(1)  后端服务节点(1)   主机列表(1)	主机进程(31)	主机风险(2) 				
<ol> <li>数据来源于各个云平台主机安全/安全中心产品,若您未购买或未)</li> </ol>	开启,则无法获取数排	据。				×
<b>主机漏洞 (2) 高危基线风险 (0)</b> 标记处置	标记忽略			处理状态:未处理		Q 🕸 🛪
漏洞名称/类型	风险等级 了	资产ID/名称	首次/最近发现时间	所属账号	处理状态 (i) 🍸	操作
▲測到目标服务器启用了OPTIONS方法 配置错误	提示	in fe	2025-03-03 18:21:25 2025-03-04 19:15:18	<u>&amp;</u>	未处理	标记处置 更多 ~
检测到目标服务器没有启用X-Frame-Options选项 配置错误	提示	ins fe	2025-03-03 18:21:25 2025-03-04 19:15:18	8	未处理	标记处置 更多 ~
共 2 项					10 ~ 条 / 页	● 1 /1页 ▶ ▶

## 暴露路径示例解读

下图的路径关系如下:

1. 弹性公网 EIP ( eip-\*\*\*\*, IP:123.\*\*\*.\*\*\* ) 绑定了弹性网卡 ( eni-\*\*\*\* ) 。



- 2. 弹性网卡(eni-\*\*\*\*)绑定了弹性网卡云服务器(ins-\*\*\*)。
- 3. 关联主机安全资产,发现云服务器(ins-\*\*\*)的3个进程监听了22、323、80等三个端口。
- 4. 由于弹性网卡的安全组策略设定了1-65535端口面向0.0.0/0开放,最终导致公网IP(123.\*\*\*.\*\*\*.) 面向互联网开放了1-65535端口。 实际,可访问的端口是22、323、80。



## 应用场景示例

1. 当 CVM 实例 ins−ox\*\*\*\*出现入侵告警时,需要排查可能的入侵路径。您可以在暴露路径输入该实例 ID,即可展示该资产面向互联网开放的场 景。





2. 分析可知,资产通过安全组开放了所有端口,并且配置了公网 IP(129.\*\*\*.\*\*\*)。同时通过负载均衡(139.\*\*\*.\*\*\*)开放了22端口。资 产存在 Linux 系统弱口令,该弱口令可能是入侵的主要原因。可以根据该方向进行排查。



# 查看扫描结果

最近更新时间: 2025-04-11 17:39:02

- 1. 登录 云安全中心控制台,在左侧导览中,单击**云边界分析**。
- 2. 在**云边界分析 > 扫描结果**中,切换 Tab 选项卡,读取不同的结果数据。
  - 端口服务: 查看扫描发现的互联网端口及对应的组件、服务信息。云安全中心会将高危服务进行标注。

互联网边界 ① 网络扫描	结果(346) ()									
端口服务(204) Web	服务(76)	漏洞风险(66)	弱口令风险(0)							
标记处置标记忽略	全部处理状态	~	最近发现时间 ~	2025-04-03 17:31:47 ~ 2	2025-04-10 17:31:47	<b>当</b> 多个关键字》	用竖线 " " 分隔,多个过滤标签	签用回车键分隔	Q	C 🌣 7
域名/IP	端口	服务判定 🍸	资产ID/名称	资产类型 🍸	组件	服务/协议	首次/員 所属账号 🛛	处理状态 ()	操作	
101	139	高危服务	ins wi	СУМ	samba	netbios-ssn tcp	2025- 2025- 🙆 🎙	未处理	封禁端口〔	更多 ~
111	139	高危服务	ins wir	СУМ	samba	netbios-ssn tcp	2025- 2025-	未处理	封禁端口	更多 ~
49.	139	高危服务	in: wi	CVM	samba	netbios-ssn tcp	2025- 2025-	未处理	封禁端口	更多 ~

○ Web 服务: 查看扫描发现的 Web 服务,包括预览页、标题、状态响应码、组件等。云安全中心会将高危 Web 服务进行标注。

互联网边界 ① 网络扫描结果(346) ①								
端口服务(204) Web服务(76) 漏洞风险(66)	弱口	1令风险(0)						
标记处置 标记忽略 全部处理状态 🗸		最近发现时间 > 2025-0	4-03 17:32:37 ~ 2025-0	04-10 17:32:37 📋	多个关键字用竖线 " " 分隔,多个过滤板	ī签用回车键分隔	Q	C 🕸 🛪
服务标题/链接	端口	域名/IP	风险等级 了	资产ID/名称	资产类型 所属账号	处理状态 🛈	操作	
@ http:// 7:11434	11434	10	高危	ins Alj	CVM 📀	未处理	标记处置	标记忽略
MLflow	5000	10£	高危	ins- AI基	CVM 🙆	未处理	标记处置	标记忽略

○ 漏洞风险: 查看扫描发现的漏洞。您可以通过勾选仅展示 POC 扫描发现,来过滤通过 POC 检测的漏洞。



互联网边界① 网络扫描结果(346)①								
端口服务(204) Web服务	(76) 漏	<b>同风险(66)</b> 弱口令风险(0)						
标记处置 标记忽略	全部处理状态	→ 最近发现时间 →	2025-04-03	3 17:34:02 ~ 2025-04-10 17:34:02 📋	多个关键字用竖线 " " 分隔,多1	个过滤标签用回车键分网	8	Q C
1X展示POC扫描发现								ф <u>т</u>
资产ID/名称	资产类型 🔽	漏洞名称/类型	端口	风险等级 了 漏洞标签 了		所属账号 🕜	处理状态 🛈	
↓ ins 大ŧ	CVM	检测到目标服务器启用了OPTIONS方法 🎲 配置错误	5000	提示 -		Ø	未处理	
► Ihin ₩	LH	wp-xmirpc ssrf漏洞 <del>【】</del> 跨站请求伪造	80	中危		8	未处理	

### ○ 弱口令风险:查看扫描发现的应用弱口令或网站后台弱口令。

端口服务(0) Web	服务(0)	漏洞风险(65)	弱口令风险(1)						
标记处置 标记忽略	全部处理状态	~	最近发现时间	ⓐ ∽ 2025-03-01 17:37	:33 ~ 2025-04-10 17:3	<b>37:33 </b> 一 多个关键字月	B竖线 " " 分隔,多个过滤	标签用回车键分隔	Q
域名/IP	端口	弱口令类型	详情	资产ID/名称	资产类型 🔽	首次/最近发现时间	处理状态()	所属账号 冚	操作
42	21	FTP 弱口令	username:ftp password:***	ins-p	CVM	2024-06-04 00:19:40 2025-03-14 11:57:45	未处理	🕹 ;	标记处置 标记

# 云 API 异常监测 功能简介

最近更新时间: 2025-04-22 16:18:12

云安全中心通过实时监测云 API 访问密钥 AccessKey(以下简称:AK)相关信息,梳理 AK 权限配置与调用路径,并基于腾讯云独有的丰富情 报识别**泄露事件、异常调用、权限配置风险**,并进行告警。

# 注意: 建议您及时关注 AK 调用情况与异常告警,并按照相关指引修改权限策略,可帮助您解决 AK 的权限失控、配置错误、泄露响应慢、异常调用难溯源等问题,更好地对 AK 进行管理,减少安全隐患,防止威胁扩散,保障云上安全。



## 功能点梳理

功能板块		功能点	解决问题	操作指引
统计面板 资产概览 & 安全概览		快速了解 AK 资产情况,定位建议关注的异常 AK、待处理告警、待处理风险等。	定位高优问题,了解有多少 AK 需关 注,待处理的问题有多少,近期安全运 营趋势怎样。	统计面板
资产列 表 	AK 资产	基于 AK 资产视角,查看 AK 基本信息、安全建 议、关联告警与风险、调用记录与关联资产。(永 久密钥与临时密钥均支持)	梳理 AK 数量,了解每个 AK 是否在 被调用,这把 AK 被多少个 IP 访问了 哪些接口,调用是否有异常,相关策略 是哪些。	次立列主
	调用源 IP	基于调用源 IP 视角,查看 IP 地域、类型、调用 AK 情况、关联告警、调用记录。	梳理请求了永久 AK 的 IP 数量,IP 是 否为内部资产,IP 属地是哪,调用了 多少 AK,是否有告警,支持客户备注 IP 所属业务。	<b>贝/ 71衣</b>



告警列表		实时监控 AK 泄露与异常调用: • 黑客工具/行云管家/ cos−browser 识别。 • github 泄露(github 合作 + IP检查等)。 • 异常 IP 调用敏感接口等。 基于告警规则视角,查看告警内容(泄露、异常调 用),关联 AK 与异常调用记录,并提供权限策略 配置建议。	<ul> <li>实时告警泄露事件,全面分析并溯 源异常调用;</li> <li>了解泄露地址,了解异常调用链路 (调用IP、访问服务与接口、相关 策略),提供治理建议,引导处 置。</li> </ul>	告警
风险列表		自动化扫描 AK 权限配置, 检查 AK 是否存在高 权限策略,基于风险规则视角,查看配置风险描述 与风险判定证据,并提供权限策略配置建议。	支持事前梳理 AK 的高风险策略配置, 收敛敏感权限,减少安全隐患。	风险
垒政答	告警策略	管理系统告警策略。	答理季季关注的失效笑咳 计其工业名	
理	白名单策 略	管理告警白名单,可对白名单进行增删改查,基于 IP、调用方式、AK、接口等进行加白。	雷廷丽安入庄的百言采唱,开 <b>举了亚</b> 为 需要自定义白名单。	策略管理

## () 说明:

由于 AK 异常检测功能比较敏感,提供 API 后可能暴露更多风险 API 接口,暂不提供 API 接口。



## 云 API 密钥安全使用方案

最近更新时间: 2025-04-22 16:18:12

云 API 密钥 AccessKey(以下简称"AK")是构建腾讯云 API 请求的重要凭证。您的 API 密钥代表您的账号身份和所拥有的权限,使用腾讯 云 API 可以操作您名下的所有腾讯云资源。

AK 包含 SecretId 和 SecretKey,用于您调用 腾讯云 API 时生成签名,查看 生成签名算法 。SecretId 作为用户标识,**SecretKey(必须保** 密) 为验证用户身份的密钥。

### ▲ 注意:

AK 若泄露且被恶意利用,会给用户的云上资源与相关业务带来很大的安全隐患,进一步造成重大损失。

### AK 泄露案例

### 1. 代码仓库硬编码暴露风险

开发者将 SecretId/SecretKey 直接写入业务代码并上传至 GitHub 等开源平台,攻击者通过关键词(如"SecretKey"、"cos.apshanghai"等)搜索即可快速定位敏感凭据。(代码中未使用环境变量或配置中心,凭据以明文形式存在于版本控制历史记录中。)

#### 2. 客户端反编译导致的凭证提取

小程序/APP 开发者将 SecretKey 硬编码在客户端,攻击者通过逆向工程(如反编译 APK、微信小程序源码)提取凭据,直接接管云资源。

### 3. 技术文档与样例代码泄露

技术文档、内部或公开分享材料中包含测试环境 SecretId/SecretKey,攻击者利用其访问生产资源。

#### 4. 临时密钥滥用

开发者在客户端直接生成临时密钥,攻击者在有效期内劫持并利用其发起恶意请求。

#### 5. 日志与监控系统泄露

云函数(SCF)环境变量、云硬盘快照或操作审计日志中残留 SecretKey 明文,攻击者通过权限枚举获取敏感信息。

### 6. 服务器内明文配置的 AK 被攻击者获取

攻击者通过漏洞入侵服务器、任意文件读取漏洞,通过环境变量、配置文件等,窃取到明文 AK/SK。

### AK 安全实践教程

### 避免使用主账号 AK

请尽量不要使用主账号 AK 访问腾讯云,更不要将 AK 共享给他人。一般情况下,应该为所有访问腾讯云的用户创建子账号,同时授权该子账号相应 的管理权限。相关设置请参见 用户类型。

### 请勿在代码中嵌入 AK

嵌入代码中的 AK 凭证容易被人忽视,经验丰富的开发者会将其写入数据库或者独立的文件中,使得其管理起来更方便。 开发者应将 AK 存储在独立加密配置文件或密钥管理系统中(如腾讯云 KMS 白盒密钥 ),而非直接写入业务代码,降低因代码仓库权限管理疏漏或 客户端反编译导致的泄露风险。

#### 定期更新 AK

建议您或 CAM 用户要定期轮换 AK。这样可以让身份凭证泄露情况下的影响时间受限。

#### 删除不需要的权限/AK

- 删除用户不再需要的权限,尽量减少 AK 泄露后带来的安全风险。
- 删除长期不使用的 AK,减少 AK 的暴露面。



### 遵循最小权限原则申请账户

最小权限原则是一项标准的安全原则。即仅授予执行任务所需的最小权限,不要授予更多无关权限。例如,一个用户仅是 COS 服务的使用者,那么 不需要将其他服务的资源访问权限(如 CAM 读写权限)授予给该用户。 另外申请用户时,如果只需要 API,仅申请 API 权限用户即可,不要把控制台和 API 的用户混合。

### 事前 AK 请求情况梳理

在云安全中心 > 云 API 异常监测,实时做好 AK 的资产管理和备注。

- AK 列表: 梳理 AK 资产,了解我有多少把 AK,备注每把 AK 是什么业务在用。
- 调用源 IP: 梳理调用源 IP, 了解每个调用源 IP 属于哪个业务。
- 风险权限收敛: 查看 AK 配置检查结果,梳理是否有不需要的高权限接口。
- 应急响应:当提前掌握好上面的情况后,出现 AK 泄露导致异常调用时,可以快速的完成 AK 替换。

# 统计面板

最近更新时间: 2025-04-22 16:18:12

- 1. 登录 云安全中心控制台,在左侧导览中,单击云 API 异常监测。
- 2. 资产概览:统计当前腾讯云账号下主账号与子账号全部 AK 数量(包含永久密钥与临时密钥)与不同安全建议的 AK 数量。

安全建议	建议说明
立即处理	该 AK 有异常调用告警/泄露事件,请立即关注并处理。
建议加固	该 AK 权限配置存在风险,建议进行关注并收敛权限,完成加固。
暂无异常	该 AK 暂无异常调用告警、泄露事件,权限配置暂无风险。

- 3. 安全概览:统计近7天待处理的告警和风险,与不同类型告警的数量;统计近7天不同安全建议的 AK 变化趋势。
- 4. 单击"关注的字段",下方列表搜索框中自动添加条件并筛选出对应内容。

PI异常!	监测							Ê	] 策略管理	多账号管理		
<del>[</del> 产概览		安全概览(近7天)			近7天安全趋势							
K资产数		待处理告警	待处理风险		建议立即处理AK	2	2	2	2	2	2	2
37.	- 占未字段	<b>15</b>	144	<b>†</b> 0	建议加固AK	30	30	30	30	30	30	30
议立即处		泄露监测 0	配置风险 144		暂无异常AK	5	5	5	5	5	5	5
议立即加	固 30	异常调用 15										
账号AK:	3											
												1
行列表	告警 风险						自动填	充条件				
AK资	产 调用源IP (i)	同步资产 更多 >	自动筛选对原	立内容			2 多个关键字用	]竖线 " " 分隔,多'	个过滤标签用回	百年键分隔	Q	ଛରୁ ମ
	AK名称/备注	账号名称/身份 ℃	安全建议 🛈 🔽	告警 🏾	风险 丁	调用源IP	AK创	建/最近访问时间 💲	: AI	(状态 🛈 🍸 ‡	操作	
	AKIDt -		立即处理	异常行为:2	配置风险: 11	37			• i	己启用	详情	更多 ~
	AKIDc 备注一		立即处理	异常行为: 30	配置风险:1	5			•	己启用	详情	更多 Y
	AKID(		建议加固	-	配置风险:1	0			• 1	己启用	详情	更多 ~
	AKIDr -	<mark>⊘</mark> 子账号(所属主账号:	建议加固		配置风险:12	0			• 1	己启用	详情	更多 ~
	AKID1 -	⊘ 子账号(所属主账号:	建议加固		配置风险:13	0			• 1	己启用	详情	更多 ~
	AKIDr -		建议加固		配置风险: 13	0			• 1	己启用	详情	更多 ~



## 资产列表

最近更新时间: 2025-04-22 16:18:12

## AK 资产

## AK 资产列表

- 1. 登录 云安全中心控制台,在左侧导览中,单击云 API 异常监测。
- 2. 在资产列表 > AK 资产中,基于 AK 资产视角,查看 AK 基本信息、安全建议、关联告警与风险。

()	说明:					
	临时密钥由于数量较多,	不停变化,	所以进行了聚合展示,	临时密钥也包含了控制台的临时密钥,	AK名称为	"临时密钥"

产列表	告警 风险								
AK资产	调用源IP ① 同步资产	更多~					多个关键字用竖线 " " 分隔,多个	>过滤标签用回车键分隔	0 © C +
	AK名称/备注	账号名称/身份 丁	安全建议 ① ⑦	告警 ⑦	风险 丁	调用源IP	AK创建/最近访问时间 💲	AK状态 (i) 〒 💠	操作
	AKID75		立即处理	异常行为:12	配置风险:1	2		• 已启用	详情 更多 >
	AKIDGi		立即处理	异常行为: 21	配置风险:1	29		• 已启用	详情 更多 >
	AKIDoU		立即处理	异常行为:5	配置风险:12	3		• 已启用	详情 更多 ~
	AKIDZF		立即处理	异常行为: 63	配置风险:1	97		• 已启用	详情 更多 ~
	临时密钥 -	<mark>⊘</mark> 主账号	立即处理	异常行为: 61	-	28		• 已启用	详情 更多 >
	临时密钥 -	▲ 主账号	立即处理	异常行为:2	-	12		• 已启用	详情 更多 ~
	临时密钥	▲ 主账号	立即处理	异常行为:53	-	7		• 已启用	详情 更多 ~
	临时密钥 -	▲ 主账号	立即处理	异常行为:8	-	16		• 已启用	详情 更多 ~
	AKID3J -		立即处理	异常行为: 1	-	1		• 已启用	详情 更多 ~
	AKIDKW		建议加固	-	配置风险: 3	8		• 已启用	详情 更多 >
も84 項								10~条/页 阔 🖣	1 /9页 ▶ ₩

字段名	示例	说明
AK 名称/备注	AKID75XXX 部门1AK	AK 名称与自定义备注。 • AK 保留前6位与后11位,中间省略,支持一键复制;单击拉起 <b>AK 详情</b> 抽 屉。 • 备注可自定义编辑,不超过20字符,若备注为空显示""。
账号名称/身份	账号 A 主账号/子账号(所属主账 号:主账号 B)	<ul> <li>AK 所属云厂商与账号,若为子账号展示所属主账号信息。</li> <li>鼠标悬浮查看账号 ID与 APPID;支持筛选主账号/子账号。</li> </ul>

安全建议	<ul> <li>立即处理</li> <li>建议加固</li> <li>暂无异常</li> </ul>	<ul> <li>基于当前 AK 的告警、风险状态,为您提供综合的安全等级,可以按照推荐的处理等级进行处置。</li> <li>支持筛选不同建议管理的 AK。</li> </ul>
告警	<ul> <li>● 异常调用: x</li> <li>● 泄露监测: x</li> </ul>	<ul> <li>近期未处理告警,单击拉起 AK 详情抽屉,定位到告警页签。</li> <li>支持筛选泄露监测/异常行为/无告警</li> </ul>
风险	● 权限风险: ×	近期未处理风险,单击拉起 AK 详情抽屉,定位到风险页签。
调用源IP	6	调用该 AK 的 IP 数量。
AK创建/最近访问 时间	<ul> <li>2025-01-01 18:00:00</li> <li>2025-01-12 18:00:00</li> </ul>	AK 创建与最近访问时间。 • 格式:YYYY-MM-DD HH:MM:SS。 • 支持排序。
AK状态	<ul><li>● 已禁用</li><li>● 已启用</li></ul>	展示 AK 禁用/启用状态。 支持筛选已禁用/已启用。

### 3. 在 AK 资产中,支持进行如下操作:

○ 详情:单击详情,拉起 AK 详情抽屉。

- 更多:单击更多,支持选择检测、API 密钥管理、修改 AK 备注、添加白名单策略。
  - 检测:检查对应 AK 的配置风险。
  - API 密钥管理:跳转至访问管理 > 访问密钥 > API 密钥管理页面。
  - 修改 AK 备注:修改备注信息,单击确定。

修改AK备注					×
AK名称	AI			:1	
备注	测试				
		确定	取消		

○ 添加白名单策略:进入添加白名单策略页面,并填充对应 AK。

## AK 详情

- 1. 登录 云安全中心控制台,在左侧导览中,单击云 API 异常监测。
- 2. 在资产列表 > AK 资产中,选择所需资产,单击详情。



资 <b>产列表</b> 告警 风险	:							
AK资产 调用源IP ()	同步资产 更多 ∨			多个关键字用竖线 "["分	隔,多个过滹标签用	回车键分隔	(	2 © 5 ±
AK名称/备注	账号名称/身份 了	安全建议 🛈 🍸	告警 🔽	风险了	调用源IP	AK创建/最近访问	问时间 ‡	操作
	▲ 授主	立即处理		-		- 202	1	详情 更多 ~
	<mark>⊘</mark> 主账	立即处理	异常行为:	-		- 202!	)6	详情 更多 >

- 3. 在 AK 详情页面,查看 AK 信息关联告警与风险、调用记录与关联资产。
  - 查看 AK 信息

AK详情	检测 更多 ~ ×
AKID75: - Ø	安全建议 <b>立即处理</b> AK状态 • 已启用
基本信息 告警 风险	
基础信息	
账号名称 🔗 🕒	CAM策略 5
账号身份 子 <b>账号</b>	AK创建时间
账号ID/APPID	最近访问时间
所属主账号	

○ 查看 AK 告警信息,默认展示未处理告警,单击**详情**拉起告警详情抽屉,字段解释请参见告警。



AK详情		*	<u>☆</u> 测 更多 → ×
AKID75 - Ø	安全建议 AK状态 •	立即处理 已启用	
基本信息 告警 风险			
标记处置 更多 >	<b>近30天 ~</b> 处理状态:未处理		Ø 懲 ℃ 平
告警名称/类型 了	告警等级 ⑦ 告警时间 ↓	处理状态 了	操作
<b>非控制台方式调用高危接口</b> 异常行为	高危	未处理	详情 更多 ~
非控制台方式调用高危接口 异常行为	高危	未处理	详情 更多 >
非控制台方式调用高危接口 异常行为	高危	未处理	详情 更多 ~
非控制台方式调用高危接口 异常行为	高危	未处理	详情 更多 >

○ 查看 AK 风险信息,默认展示未处理风险,单击**详情**拉起风险详情抽屉,字段解释请参见 风险 。

AK详情		检测	更多
AKID75 - Ø	安全建议 <b>立</b> 民 AK状态 • 已属	<b>以处理</b> 自用	
基本信息  告警 <b>风险</b> ——			
检测 更多 ~	近30天 🖌 处理状态:未处理		○ 唸い上
风险名称/类型 了	风险等级 ⑦ 风险检出时间 💲	处理状态 了	操作
不应该拥有高权限预设策略 配置风险	严重	未处理	详情 更多 ~
共1项		10 ~ 条 / 页 🚺 🔺	1 /1页 🕨 🕨


○ 查看调用记录,查看调用该 AK 的 IP、IP 类型、用什么方式调用了什么服务、调用成功和失败分别的次数、首次/最近调用时间,以及相关 的 CAM 策略。

AK详情				检测	更多
<b>基本信息</b> 告警  风险					
基础信息 账号名称			CAM策略 5 AK创建时间 最近访问时间		
<ul> <li>♀ AK权限策略配置建议</li> <li>1 确认需要收敛权限的AK</li> <li>• 根据调用记录详情,定位</li> </ul>	使用该接口对应CAM策略	0			收起建议 ▲
<ol> <li>禁用或删除 Access Key</li> <li>登录 访问管理 管理控制指</li> <li>删除或禁用对应的 Access</li> <li><b>修改权限策略</b></li> <li>在权限策略中移除相关预</li> <li>验证权限回收效果</li> </ol>	) 会,并进入 访问密钥-API ss Key。 设策略或修改自定义策略	密钥管理。 <b>前往登录</b> ,以收敛接口相关的	<b>记</b> 权限。 <b>查看示意</b>		
• 尝试通过被移除的接口调	用操作,确保访问被拒绝	0			
多个关键字用竖线 " " 分隔,多个过滤标		Q 2	海田培口,即名	CAL4 <sup>9</sup> 空空	业
❷开麻戸2037亩庄 □	账号外 (未备注)	API	DescribeAccountPrivileges	5	详情 更多 >
❷ 中国-四川省-成都市 -	账号外 (未备注)	ΑΡΙ	DescribeAccounts cdb	5	详情 更多 ~
▶ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	账号外 (未备注)	API	DescribeAsyncRequestInfo	5	详情 更多 ~
字段名    示例		说明			

调用源 IP/地域/备 注	1.1.1.1 中国−北京   部门1AK	调用源 IP、所属地域与自定义备注。 • IP 内容支持一键复制。 • 备注可自定义编辑,不超过20字符,若备注为空显示"–"。
IP类型	<ul> <li>账号外(未备注)</li> <li>账号内(未备注)</li> <li>账号外</li> <li>账号内</li> </ul>	<ul> <li>账号内:在云安全中心 IP 资产列表中识别到的调用源 IP,有备注。</li> <li>账号内(未备注):在云安全中心 IP 资产列表中识别到的调用源 IP, 无备注。</li> <li>账号外(未备注):非账号内 IP 且无备注。</li> <li>账号外:非账号内 IP 但有备注。</li> </ul>
调用方式	● API ● 控制台	通过 API 调用 AK 访问服务还是在控制台的操作。
调用接口/服务	DescribeAccountPrivile ges cdb	调用的接口与接口所属服务。
CAM 策略	AdministratorAccess	该 AK 关联的 CAM 策略,多个时显示数字,单击打开 CAM 策略详情弹 窗。
调用状态/次数	<ul> <li>成功 (x次)</li> <li>失败 (x次)</li> </ul>	调用该 AK 成功/失败状态及次数。
首次/最近调用时间	<ul> <li>2025-01-01 18:00:00</li> <li>2025-01-12 18:00:00</li> </ul>	首次与最近调用时间。
IP所属资产(ID/名 称)	ins−xxx 机器1号	展示 AK 所属资产。

4. 在 AK 详情 > 基本信息 > 调用记录页面,选择所需调用源 IP,单击详情/更多。

多个关键字用竖线 "1" 分隔,多个过滤	标签用回车键分隔	Q			4
调用源IP/地域/备注 了	IP类型 (i) 了	AK名称/备注		调用方式 了	调用接口/服务 操作
) 🖸 🔗 中国-广东省-广州市 - 🧷	账号外 (未备注)	F - Ø	ي 7	API	<sup>3</sup> 洋情 更多 ~ 添加白名单策略
❷ 中国-广东省-广州市 -	账号外 (未备注)	AI -		API	管理白名单策略 (

• 详情

> 腾讯云

○ 展示调用信息,调用详情(包含时间、请求 ID、请求体;支持翻页),CAM 策略详情。



调用记录详情				× 调用记录详情		
I用源IP I用源IP地域 I用源IP备注 类型 I所属资产ID I用AK名称 I用AK备注	<ul> <li>○ 中国-四川省-成都市 0</li> <li>- </li> <li>- </li> <li>●</li> <li>- </li> <li>AKID75</li> <li>- </li> </ul>	调用方式 调用接口 调用派务 调用次数 调用状态 首次调用时间 最近调用时间	API DescribeAccountPrivileges cdb 273 • 成功	<pre>17 vpcId: "0", 18 sigMethod: " 19 name: "", 20 action: "Describe 21 uin: ' 22 reqHost: "cdb.1 23 region: "none", 24 accUin: ' 25 timestamp: ' 26 }</pre>	-	
<b>祥情 《</b>	1/273 ►			CAM策略详情(5) 策略名称	策略类型	操作
D	6da			AdministratorAccess	预设策略	策略详情 前往
1 <b>{</b> 2 3	server:		 。 		自定义策略	策略详情 前往(
	ver:			QCIoudFinanceFullAccess	预设策略	策略详情 前往C
	language: "zh-CN", reqSrc: "API",			QcloudWeDataFullAccess	预设策略	策略详情 前往C
	httpMethod: "POST", accountArea: "0",			QcloudWeDataReadOnlyAccess	预设策略	策略详情 前往C

○ 单击**策略详情,**展示其策略代码,支持复制;单击**前往 CAM 查看**,跳转至定位**访问管理 > 策略 > 具体策略详情**。

调用记录详情		
17       vpcId: "0",         18       sigMethod: "'         19       name: "",         20       action: "Describ         21       uin: "         22       reqHost: "cdb.         23       region: "none"		
CAM策略详情		×
<pre>1 { 2 statement: [ 3 { 4 action: "*", 5 effect: "allow", 6 resource: "*" 7 }, 8 ], 9 version: "2.0" 10 }</pre>		凸 复制
QCloudFinanceFullAccess	预设策略	策略详情 前往CAM查看 🖸
QcloudWeDataFullAccess	预设策略	策略详情前往CAM查看 🖸
QcloudWeDataReadOnlyAccess	预设策略	策略详情 前往CAM查看 IZ

• 更多

○ 添加白名单策略:在添加白名单策略页面,填充对应 IP、调用方式、AK、接口、返回码,单击保存。

○ 管理白名单策略:在策略管理页面,定位至**白名单策略**。

# 调用源 IP

### 调用源 IP 列表

1. 登录 云安全中心控制台,在左侧导览中,单击云 API 异常监测。

2. 在资产列表 > 调用源 IP 中,基于调用源 IP 视角,查看调用源 IP 信息、安全建议、关联告警与风险、调用的 AK 与接口。



### 🕛 说明:

- 列表数据聚合逻辑:一天内同一 IP 调用同一账号下的 AK。
- 仅展示永久密钥的 API 请求。

资产列表 告警 风险								
AK资产 调用源IP ① 修改备注	更多 >				近7天 ~	多个关键字用竖线 "J" 分隔,	多个过滤标签用回车键分隔	Q & C ∓
调用源IP/地域/备注 ⑦	IP类型 (i) 了	IP所属资产 (ID/名称)	调用AK	AK所属账号	调用接口	告警 ⑦	最近调用时间 \$	操作
₽	账号外 (未备注)	- Q -	2	۵	59	异常行为: 3		详情 更多 ~
❷ 中国-广东省-广州市 -	账号外 (未备注)	-	2	8	84	异常行为:4		详情 更多 ~
❷ 中国-广东省-广州市 -	账号外 (未备注)	-	2	8	78	异常行为:5		详情 更多 ~
❷ 中国-广东省-广州市 -	账号外 (未备注)	-	2	<b>&amp;</b>	67	异常行为:5		详情 更多 ~
❷ 中国-广东省-广州市 屏蔽	账号外	:	2	۵	61	异常行为:4		详情 更多 ~
❷ 中国-广东省-广州市 -	账号外 (未备注)	:	2	<b>&amp;</b>	69	异常行为:5		详情 更多 ~
❷ 中国-广东省-广州市 -	账号外 (未备注)	:	2	<b>&amp;</b>	83	异常行为:5		详情 更多 ~
❷ 中国-广东省-广州市 -	账号外 (未备注)	-	2	<b>&amp;</b>	91	异常行为:5		详情 更多 ~
Ø 中国-广东省-广州市 -	账号外 (未备注)	-	2	8	74	异常行为:6		详情 更多 ~
❷ 中国-广东省-广州市 -	账号外 (未备注)	-	2		30	-		详情 更多 ~
共 157 项							10 ❤ 条/页	1 /16页 ▶ ₩

字段名	示例	说明
调用源 IP/地域/备 注	<ul><li>● 已隐藏</li><li>● 未隐藏</li></ul>	调用源 IP、所属地域与自定义备注;支持隐藏,可通过字段旁边筛选展示已隐藏/ 未隐藏IP。 • IP内容支持一键复制。 • 备注可自定义编辑,不超过20字符,若备注为空显示""。
IP类型	<ul> <li>账号外(未备注)</li> <li>账号内(未备注)</li> <li>账号外</li> <li>账号内</li> </ul>	<ul> <li>账号内:在云安全中心IP资产列表中识别到的调用源 IP,有备注。</li> <li>账号内(未备注):在云安全中心IP资产列表中识别到的调用源 IP,无备注。</li> <li>账号外(未备注):非账号内 IP 且无备注。</li> <li>账号外:非账号内 IP 但有备注。</li> </ul>
IP 所属资产(ID/ 名称)	ins−xxx 机器1号	展示 AK 所属资产。
调用 AK	AKXXX	多个时显示数字,单击 <b>数字</b> 展示具体 AK 及其所属账号。
AK 所属账号	账号 A	调用 AK 所属的主账号。
调用接口	7	多个时显示数字,单 <b>数字</b> 击打开 <b>调用源 IP 详情</b> 抽屉。
告警	● 异常调用: x	<ul> <li>近期未处理告警,单击拉起调用源 IP 详情抽屉,定位到告警页签。</li> </ul>



	● 泄露监测:x	● 支持筛选泄露监测/异常行为/无告警。
最近调用时间	2025-01-01 18:00:00	最近调用时间。 ● 格式:YYYY−MM−DD HH:MM:SS。 ● 支持排序。

### 3. 在调用源 IP 中,选择所需调用源 IP,单击详情/更多。

资产列表	告警 风险						
AK资产	调用源IP ①	更多 >	近7天	▼ 多个关键字用竖线	" " 分隔,多个过滤标签用回车键	分隔	Ø 総 3 平
调用	源IP/地域/备注 了	IP类型 (i) T	IP所属资产 (ID/名称)	调用AK	AK所属账号	调用接口	: 操作
<b>∞</b>	₽ 中国-广东省-广州市 - 🖉	账号外 (未备注)	- @ -		💩   🧠 🖟	Г	详情 更多 ~
	中国-广东省-广州市 -	账号外 (未备注)	-		۵		修改IP备注 添加白名单策略
	中国-广东省-广州市 🛛 -	账号外 (未备注)	-		❷ 腾 .	L	日理ロム平東哨 隐藏该IP

操作类型		说明
详情		单击拉起 <b>调用源 IP 详情</b> 抽屉。
	修改 IP 备注	修改源 IP 备注,单击 <b>确定</b> 。
	添加白名单策略	单击拉起 <b>添加白名单策略</b> 抽屉,并填充对应 IP。
	管理白名单策略	单击跳转至 <b>策略管理 &gt; 白名单策略</b> 。
更多 隐藏该 IP		单击隐藏该 IP的调用记录,隐藏该调用源 IP 后,后续新增 IP 的调用记录同步隐藏。隐藏后可通过字 段旁边筛选展示已隐藏/未隐藏 IP,隐藏 IP 旁边通过标签标识。
	隐藏该 IP	调用源IP/地域/备注 了
		129. 已隐藏

### 调用源 IP 详情

- 1. 登录 云安全中心控制台,在左侧导览中,单击云 API 异常监测。
- 2. 在资产列表 > 调用源 IP 中,选择所需调用源 IP,单击详情。
- 3. 在调用源 IP 详情页面,查看 IP 信息关联告警、调用记录。
  - 查看 IP 信息



调用源IP详情		修改IP备注	更多 >	×
106 - Ø	IP地域  ◎ 中国-广东省-广州市 @ IP类型  账号外 (未备注)			
基本信息 告警				
基础信息       AK所属账号 <ul> <li>●</li> <li>■</li> <li>■</li></ul>	最近调用时间			

○ 查看该 IP 相关告警信息,默认展示未处理告警,单击详情拉起告警详情抽屉,字段解释请参见告警。

调用源IP详情			修改IP备注	更多 Y X
106       - ク       基本信息	11	P地域 Ø 中国-广东省-广 P类型 账号外 (未备注)	州市 口	
标记处置 更多 >>	近30天 🗸 处理状态: 未	大处理		Ø 輸 ℃ 平
告警名称/类型 🔽	告警等级 ⑦ 告	警时间 🛊	处理状态 了	操作
<b>自动化助手高危操作</b> 异常行为	高危		未处理	详情 更多 >
<b>自动化助手高危操作</b> 异常行为	高危		未处理	详情 更多 ~
非控制台方式调用高危接口 异常行为	高危		未处理	详情 更多 >
<b>自动化助手高危操作</b> 异常行为	高危		未处理	详情 更多 >
共 4 项		10 🗸 务	€/页	1 /1页 🕨 🕨

○ 查看调用记录,查看调用该 AK 的 IP、IP 类型、用什么方式调用了什么服务、调用成功和失败分别的次数、首次/最近调用时间,以及相关 的 CAM 策略。

调用源IP详情	ĵ				修改IP备注	更多 ~   ×
基本信息	告警					
基础信息 AK所属账号 账号ID/APPID IP所属资产ID IP所属资产名称	<ul> <li>20</li> <li>- 0</li> <li>- 0</li> </ul>		<b>a</b>	近调用时间		
♀ АК权	限策略配置建议					收起建议 ▲
1 7			- C A & A 4000 1007			
	恨据调用记求许们	育, 定位使用该接口对应	/CAM束眙。			
<b>2</b> 。 。	禁用或删除 Acce 登录 访问管理 管 删除或禁用对应的	<b>ess Key</b> 理控制台,并进入 访问 妁 Access Key。	密钥-AP 密钥管理。前往登录 C			
3 f	<b>多改权限策略</b> 在权限策略中移降	余相关预设策略或修改自	1定义策略,以收敛接口相关的权	限。 <b>查看示意</b>		
<b>4</b> मु	<b>佥证权限回收效</b> 界	Ŗ				
٠	尝试通过被移除的	的接口调用操作,确保认	访问被拒绝。			
<b>调用记录</b> 多个关键字用	竖线 "!" 分隔,多1	个过滤标签用回车键分网	Q			<del>بر</del>
AK名称/备注		调用方式 🔽	调用接口/服务	CAM策略	调用状态/次数	作
AKID -		ΑΡΙ	DescribeResourceTags tag	2	• 成功 (2968次) <sup>详</sup>	精 更多 >
AKID -		ΑΡΙ	DescribeDBInstances mongodb	2	◦成功 (141次)	結 更多 ≻
AKID			DescribeInstances		• 成功	

字段名	示例	说明
AK 名称/备注	AKID75XXX 部门1AK	AK 名称与自定义备注。 • AK保留前6位与后11位,中间省略,支持一键复制;单击拉起 AK 详情 抽屉。 • 备注可自定义编辑,不超过20字符,若备注为空显示""
调用方式	● API ● 控制台	通过 API 调用 AK 访问服务还是在控制台的操作。
调用接口/服务	DescribeAccountPrivil eges cdb	调用的接口与接口所属服务。
CAM策略	AdministratorAccess	该 AK 关联的 CAM 策略,多个时显示数字,单击打开 CAM 策略详情弹 窗。
调用状态/次数	• 成功 (x次) • 失败	调用该 AK 成功/失败状态及次数。

腾讯云



	( x次 )	
最近调用时间	2025-01-01 18:00:00	最近调用时间。 ● 格式:YYYY−MM−DD HH:MM:SS。 ● 支持排序。
IP 所属资产(ID/ 名称)	ins-xxx 机器1号	展示 AK 所属资产。

### 4. 在基本信息页面,选择所需 AK,单击详情/更多。

调用记录				
多个关键字用竖线" "分隔,	多个过滤标签用回车键分隔	Q		
AK名称/备注	调用方式 ⑦	调用接口/服务	CAM策略	调用状态/次数 操作
ي - 1	API		1	• 成功 ( 次
-	API		1	<ul> <li>         成功         ( 欠)         管理白名单策略     </li> </ul>

#### • 详情:

○ 展示调用信息,调用详情(包含时间、请求 ID、请求体;支持翻页 ),CAM 策略详情。

调用源IP		调用方式	API	17	vpcId: "0",		
调用源IP地域	🔗 中国—四川省—成都市 🗗	调用接口	DescribeAccountPrivileges	19	name: "",		
调用源IP备注	- 19	调用服务	cdb	20 21	action: "Describe uin: '		
IP类型	账号外 (未备注)	调用次数	273	22	reqHost: "cdb.t		
IP所属资产ID	<u>م</u> _	调用状态	• 成功	23	region: "none", accUin: '		
	-	首次调用时间		25	timestamp: '		
调用AK名称	AKID75	最近调用时间		20	1		
调用AK备注	_ /						
调用详情 ◀	1/273 ►			CAM策略	羊情(5)		
<b>调用详情</b> ◀ 调用时间 请求ID	1/273 ► 6dε			CAM策略 策略名称 Administr	详情(5) atorAccess	策略类型 预设策略	操作 策略详情 前往CAM查想
<b>周用详情</b> ◀ 周用时间 青求ID 1 <b>{</b> 2 3	1/273 ► 6de server:		<u>چ</u> م	CAM策略 策略名称 Administ	详情(5) atorAccess	策略类型 预设策略 自定义策略	操作 策略详情 前往CAM查付 策略详情 前往CAM查付
调用详情 ◄ 周用时间 请求ID 1 <b>{</b> 3 4 5	1/273 ► 6de server: assumerUin: "", cliIp: '		<u>چ</u> م 	CAM策略 策略名称 Administr 和 QCloudFi	详情 (5) atorAccess nanceFullAccess	策略类型 预设策略 自定义策略 预设策略	操作 策略详情 前往CAM查试 策略详情 前往CAM查试
<b>周用详情</b> ◄ 同用时间 直示状D 1 { 2 3 4 5 6 7 8	1/273 ► 6de server: assumerUin: "", cliIp: ' ver: module: "cdb", language: "zh-CN", reqSrc: "API",		ይ ያ	CAM策略 策略名称 Administr QCloudFi QcloudW	详情 (5) atorAccess nanceFullAccess eDataFullAccess	策略类型           预设策略           自定义策略           预设策略	/ 操作 策略详情 前往CAM查付 策略详情 前往CAM查付 策略详情 前往CAM查付 策略详情 前往CAM查付

○ 单击**策略详情**,展示其策略代码,支持复制;单击前往 CAM 查看,跳转至访问管理 > 策略 > 具体策略详情。



## • 更多

○ 添加白名单策略: 在添加白名单策略页面,填充对应 IP、调用方式、AK、接口、返回码,单击保存。

○ 管理白名单策略:在策略管理页面,定位至**白名单策略**。



# 告警

最近更新时间: 2025-04-22 16:18:12

# 告警列表

- 1. 登录 云安全中心控制台,在左侧导览中,单击云 API 异常监测。
- 2. 在告警列表中,基于告警规则视角,查看告警内容(泄露、异常调用),关联 AK 与异常调用记录,并提供权限策略配置建议。

标记处	置 更多 ×				<b>近7天 &gt;</b> 处理状态:未处理		Q 🕸 :
	告警名称/类型 🔽	告警等级 ⑦	AK名称/备注	账号名称/身份 丁	告警时间 🗅	处理状态 了	操作
	非控制台方式调用高危接口 异常行为	高危		🐼 pi 子账号		未处理	详情 更多 ~
	非控制台方式调用高危接口 异常行为	高危		<mark>必</mark> pi 子账号		未处理	详情 更多 ~
	非控制台方式调用高危接口 异常行为	高危		<mark>⊘</mark> fe 子账号		未处理	详情 更多 ~
	非控制台方式调用离危接口 异常行为	高危		❷ pi 子账号		未处理	详情 更多 ~
	非控制台方式调用高危接口 异常行为	高危		<mark>⊘</mark> pi 子账号		未处理	详情 更多 ~
	非控制台方式调用高危接口 异常行为	高危		☑ fe 子账号		未处理	详情 更多 ~
	非控制台方式调用高危接口 异常行为	高危		❷ pi 子账号		未处理	详情 更多 ~
	非控制台方式调用高危接口 异常行为	高危		❷ pi 子账号		未处理	详情 更多 ~
	<b>未授权的服务调用</b> 异常行为	提示		<mark>⊘</mark> pi 子账号		未处理	详情 更多 ~
	未授权的服务调用	提示		🖉 pi		未处理	详情 更多 ~

字段名	示例	<b>说明</b>
告警名称/类型	<ul><li>异常行为</li><li>泄露监测</li></ul>	单击拉起 <b>告警详情</b> 抽屉。
告警等级	<ul> <li>严重</li> <li>高危</li> <li>中危</li> <li>低危</li> <li>提示</li> <li>无效</li> </ul>	基于腾讯云安全实践评定告警等级。
AK 名称/备注	AKID75XXX 部门1AK	AK 名称与自定义备注。 <ul> <li>AK 保留前6位与后11位,中间省略,支持一键复制;单击拉起 AK 详情抽屉。</li> <li>备注可自定义编辑,不超过20字符,若备注为空显示"—"。</li> </ul>
账号名称/身份	账号A	<ul> <li>AK 所属云厂商与账号,若为子账号展示所属主账号信息。</li> <li>鼠标悬浮查看账号 ID 与 APPID;支持筛选主账号/子账号。</li> </ul>



	主账号/子账号(所属主 账号:主账号B )	
告警时间	2025-01-12 18:00:00	告警发生时间。 ● 格式:YYYY-MM-DD HH:MM:SS。 ● 支持排序。
处理状态	<ul><li>未处理</li><li>已处置</li><li>已忽略</li></ul>	展示告警处理状态,手动完成标记,处理状态支持筛选。

### 3. 在告警列表中,选择所需告警,单击**详情/更多**。

资产列表 告警 风险						
标记处置 更多 >		近7天	✔ 处理状态:未处理			Q 🕸 🖯 4
告警名称/类型 了	告警等级 🍞 🦷 AK名	3称/备注	账号名称/身份 了	告答时间 ‡	处理状态、	┏ 操作
异常行为	高危 - ⑦	>	▲ i . 0 主账号0	2025	未处理	详情 更多 >
异常行为	高色		<mark>⊘</mark> 主账号	2028 7	未处理	标记处置 标记忽略 法加白夕单等略
异常行为	高危		<mark>る</mark> 主账号	2025	未处理	API密钥管理 [2]

操作类型		说明
详情		单击拉起 <b>告警详情</b> 抽屉。
	标记处置	单击后处理状态变为"已处置"。
百夕	标记忽略	单击后处理状态变为"已忽略"
史多	添加白名单策略	单击拉起 <b>添加白名单策略</b> 抽屉,并填充对应 AK。
	API 密钥管理	单击跳转至 <b>访问管理 &gt; 访问密钥 &gt;</b> API 密钥管理。

# 规则说明

实时监控 AK 泄露与异常调用,监测分为三类:黑客工具/行云管家/cos−browser 识别、github 泄露(github 合作 + IP检查等 )、异常 IP 调 用敏感接口等,具体规则见下表:

规则名称	规则说明
根密钥调用高危接口	主账号访问密钥调用高危接口。 高危接口包含cam、sts、tat、scf、tke、cdb、cvm、cbs 等20+类服务的30+接口,相关示例: cam.ListAccessKeys、cam.DeleteUser…
非控制台方式调用高危接 口	使用非控制台方式(主要是通过 sdk 调用云 API),调用高危接口。
未授权的服务调用	通过 API 调用未授权的服务,需要收敛该账号/角色的权限。



创建密钥操作	有新的密钥被创建。
权限提升行为	通过调用 sts、cam 的部分接口,该用户权限得到提升。
非正常时间段敏感行为	在晚上10点至凌晨6点时间段内,通过控制台或者 API 执行一些敏感操作,例如删除资源等操作。
新增用户调用高危接口	1天内创建的用户调用了高危 API,需要注意。
github密钥确认请求	检查请求是否来源于 GithubAK 回调的出口 IP。 如果命中,代表该 ak 存在于 github 公库/私有库。
黑客工具检测	检查同一个 ak 的行为是否与黑客工具相似。
长期未使用的访问密钥出 现调用	在过去一个月内未曾使用的访问密钥出现了 API 调用,需要注意。
通过cos-browser调用 云API	通过 cos-browser 调用云 API,部分攻击者会使用 cos-browser 进行文件下载,需要判断是否正常使 用。
通过api创建云资源	通过腾讯云 API,创建云资源,例如创建云服务器(CVM )、云数据库(CDB)等。
行云管家行为	这部分调用来源于行云管家的调用,需要关注。 行云管家是一个多云管理平台,可以可视化的管理云上 CVM、网络、镜像等,部分攻击者也会使用。需要梳理 运维人员是否使用行云管家。
自动化助手高危操作	通过调用 tat 的部分接口,直接对机器执行命令。

# 告警详情

- 1. 在告警列表中,选择所需告警,单击**详情。**
- 2. 在告警详情页面, 查看告警信息与异常调用记录。
  - 查看告警信息

告警详情	未处理		标记处置 更多 > > > >
	<b>非控制台方式调用高危接口</b> 异常行为	告警等级 告警时间	高危
AK名称	临时密钥	账号名称 账号身份	<mark>⊘</mark> 主账号

○ 查看异常调用记录,查看命中该告警的是哪个 IP、IP 类型、用什么方式使用了哪个 AK 调用了什么服务、调用成功和失败分别的次数、首次/最近调用时间,以及相关的 CAM 策略;根据 AK 权限策略配置对 AK 进行处置。

♀ AK权限策略配置建议				收	记建议 ▲
1 确认需要收敛权限	的AK				
• 根据调用记录详情	i,定位使用该接口对应CAM策略	ф П о			
2 禁用或删除 Acces	ss Kev				
<ul> <li>登录 访问管理 管:</li> </ul>	理控制台,并进入 访问密钥-API	密钥管理。前往登录 C			
• 删除或禁用对应的	J Access Key。				
3 修改权限策略					
• 在权限策略中移除	相关预设策略或修改自定义策略	,以收敛接口相关的权限。 <mark>1</mark>	查看示意		
4 验证权限回收效果	ł				
• 尝试通过被移除的	]接口调用操作,确保访问被拒绝	1			
2常调用记录					
<b>*常调用记录</b> 多个关键字用竖线 *** 分隔,多个 调用调p/tbtig/命注	·过滤标签用回车键分隔	Q AK 名称/各注	海田方式 立	调用培门/服务 操作	4
<b>2 常调用记录</b> 多个关键字用竖线 "!" 分隔,多个 调用源IP/地域 <b>/</b> 备注	过滤标签用回车键分隔 IP类型 ① 了	Q AK名称/备注	调用方式 ℃	调用接口/服务 操作	<u>.</u>
<ul> <li>常调用记录     <li>多个关键字用竖线 "广分隔,多个     <li>调用源IP/地域/备注     <li>፩ 腾讯云内网 -     </li> </li></li></li></ul>	<ul> <li>过滤标签用回车键分隔</li> <li>IP类型 ① 丁</li> <li>账号外 (未备注)</li> </ul>	Q AK名称/备注	调用方式 API	调用接口/服务 操作 DescribeAccot cdb 详情 更多	<u>*</u>
<ul> <li>*常调用记录</li> <li>多个关键字用竖线 ** 分隔,多个</li> <li>调用源IP/地域/备注</li> <li>         の 読讯云内网 -     </li> </ul>	→过滤标签用回车键分隔 IP类型 ① ℃ 账号外(未备注)	Q AK名称/备注	调用方式 T API	调用接口/服务 操作 DescribeAccot cdb 详情 更多	<u>ب</u>
<ul> <li>*常调用记录</li> <li>多个关键字用竖线 "「分隔,多个</li> <li>调用源IP/地域/备注</li> <li>         の 勝讯云内网 -         <ul> <li></li></ul></li></ul>	·过滤标签用回车键分隔       IP类型 ① 了       账号外 (未备注)       账号外 (未备注)	Q AK名称/备注	调用方式 T API API	<ul> <li>调用接口/服务 操作</li> <li>DescribeAcco. cdb 详情 更多</li> <li>DescribeClust tke 详情 更多</li> </ul>	~ ~
<ul> <li>常调用记录</li> <li>多个关键字用竖线 "广分隔,多个</li> <li>调用源IP/地域/备注</li> <li>         ◎ 腾讯云内网 -     </li> <li>         ◎ 腾讯云内网 -     </li> </ul>	<ul> <li>过滤标签用回车键分隔</li> <li>IP类型 ① 丁</li> <li>账号外 (未备注)</li> <li>账号外 (未备注)</li> </ul>	Q AK名称/备注	调用方式 T API API	<ul> <li>调用接口/服务 操作</li> <li>DescribeAccot cdb</li> <li>DescribeClustr tke</li> <li>ListAccessKey 光振 平常</li> </ul>	~ ~
<ul> <li>*常调用记录</li> <li>多个关键字用竖线 "!" 分隔, 多个</li> <li>调用源IP/地域/备注</li> <li>の 勝讯云内网 -</li> <li>② 勝讯云内网 -</li> <li>③ 勝讯云内网 -</li> </ul>	<ul> <li>・过滤标签用回车键分隔</li> <li>・レスクロン・レン・レン・レン・レン・レン・レン・レン・レン・レン・レン・レン・レン・レン</li></ul>	Q AK名称/备注	iiii iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	<ul> <li>週用接口/服务 操作</li> <li>DescribeAccot cdb</li> <li>DescribeClust tke</li> <li>ListAccessKey 注情 更多</li> </ul>	~ ~
*常调用记录         多个关键字用竖线 "/* 分隔,多个         调用源IP/地域/备注         の 勝讯云内网 -         の 勝讯云内网 -         の 勝讯云内网 -	<ul> <li>过滤标签用回车键分隔</li> <li>ⅠP类型 ① 丁</li> <li>账号外 (未备注)</li> <li>账号外 (未备注)</li> <li>账号外 (未备注)</li> <li>账号外 (未备注)</li> </ul>	Q AK名称/备注	调用方式 マ API API API	· 调用接口/服务 操作 DescribeAcco cdb 详情 更多 DescribeClust tke 详情 更多 ListAccessKey cam 详情 更多	~ ~ ~
<ul> <li>* 常调用记录</li> <li>多个关键字用竖线 "!" 分隔, 多个</li> <li>调用源IP/地域/备注</li> <li>         ・ 勝讯云内网 -         ・     </li> <li>         ・ 勝讯云内网 -         ・     </li> <li>         ・ 勝讯云内网 -         ・     </li> </ul>	<ul> <li>・过滤标签用回车键分隔</li> <li>・レスクロン・レン・レ、レン・レ、レン・レ、レン・レ、レン・レ、レン・レ、レン・レ、レン</li></ul>	Q AK名称/备注	<ul> <li>调用方式 Y</li> <li>API</li> <li>API</li> <li>API</li> <li>API</li> <li>API</li> <li>API</li> </ul>	<ul> <li>週用接口/服务 操作</li> <li>DescribeAccot cdb</li> <li>DescribeClust tke</li> <li>ListAccessKey cam</li> <li>DescribeAccot は情 更多</li> <li>近時 更多</li> <li>近時 更多</li> <li>近時 更多</li> </ul>	. <b>⊻</b> ~ ~
*常调用记录         多个关键字用竖线 "/* 分隔, 多个         调用源IP/地域/备注         の 勝讯云内网 -         の 勝讯云内网 -         の 勝讯云内网 -         の 勝讯云内网 -	·过滤标签用回车键分隔 ·IP类型 ① 丁 账号外 (未备注) 账号外 (未备注) 账号外 (未备注) 账号外 (未备注) 账号外 (未备注)	Q AK名称/备注	iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	调用接口/服务     操作       DescribeAccoot cdb     详情 更多       DescribeClustt tke     详情 更多       ListAccessKey cam     详情 更多       DescribeAccoot cdb     详情 更多       DescribeAccoot cdb     详情 更多	.⊻ ~ ~ ~

字段名	示例	说明
调用源IP/地域/备注	1.1.1.1 中国−北京   部门1AK	调用源 IP、所属地域与自定义备注。 • IP 内容支持一键复制。 • 备注可自定义编辑,不超过20字符,若备注为空显示"-"。
IP类型	<ul> <li>账号外(未备注)</li> <li>账号内(未备注)</li> <li>账号外</li> <li>账号内</li> </ul>	<ul> <li>账号内:在云安全中心 IP 资产列表中识别到的调用源 IP,有备注。</li> <li>账号内(未备注):在云安全中心 IP 资产列表中识别到的调用源IP,无备注。</li> <li>账号外(未备注):非账号内 IP 且无备注。</li> <li>账号外:非账号内 IP 但有备注。</li> </ul>
AK名称/备注	AKID75XXX 部门1AK	AK 名称与自定义备注。 • AK 保留前6位与后11位,中间省略,支持一键复制;单击拉起 AK 详情 抽屉。 • 备注可自定义编辑,不超过20字符,若备注为空显示""。
调用方式	● API ● 控制台	通过 API 调用 AK 访问服务还是在控制台的操作。

🔗 腾讯云



调用接口/服务	DescribeAccountPrivi leges cdb	调用的接口与接口所属服务。
用户角色/策略	角色: CSIG_Security 策略: 1	该 AK 关联的角色与 CAM 策略,多个时显示数字,单击打开 CAM 策略详 情弹窗。
调用状态/次数	• 成功 (x次) • 失败 (x次)	调用该 AK 成功/失败状态及次数。
首次/最近调用时间	<ul> <li>2025-01-01 18:00:00</li> <li>2025-01-12 18:00:00</li> </ul>	首次与最近调用时间。 • 格式:YYYY-MM-DD HH:MM:SS。 • 支持排序。
IP 所属资产(ID/ 名称)	ins−xxx 机器1号	展示 AK 所属资产。

3. 在告警详情页面,选择所需调用源 IP,单击详情/更多。

异常调用记录						
多个关键字用竖线" "分隔,多个边	北遠标签用回车键分隔	Q				₹
调用源IP/地域/备注	IP类型 (i) T	AK名称/备注		调用方式 🍸	调用接口/服务 操作	
<mark>の</mark> 勝讯云内网 - 🖉	账号外 (未备注)	- Ø	ā	API	Keys 详情 更多 ~	
🕹 腾讯云内网 -	账号外 (未备注)			API	添加白名单策略 e) 管理白名单策略	

### ● 详情

○ 展示调用信息,调用详情(包含时间、请求 ID、请求体;支持翻页),CAM 策略详情。



调用记录详情				× 调用记录详情		
I用源IP I用源IP地域 I用源IP备注 类型 I所属资产ID I用AK名称 I用AK备注	<ul> <li>○ 中国-四川省-成都市 0</li> <li>- </li> <li>- </li> <li>●</li> <li>- </li> <li>AKID75</li> <li>- </li> </ul>	调用方式 调用接口 调用服务 调用次数 调用状态 首次调用时间 最近调用时间	API DescribeAccountPrivileges cdb 273 • 成功	<pre>17 vpcId: "0", 18 sigMethod: " 19 name: "", 20 action: "Describe 21 uin: ' 22 reqHost: "cdb.1 23 region: "none", 24 accUin: ' 25 timestamp: ' 26 }</pre>	-	
<b>祥情 《</b>	1/273 ►			CAM策略详情(5) 策略名称	策略类型	操作
D	6da			AdministratorAccess	预设策略	策略详情 前往
1 <b>{</b> 2 3	server:		 。 		自定义策略	策略详情 前往(
	ver:			QCIoudFinanceFullAccess	预设策略	策略详情 前往C
	language: "zh-CN", reqSrc: "API",			QcloudWeDataFullAccess	预设策略	策略详情 前往C
	httpMethod: "POST", accountArea: "0",			QcloudWeDataReadOnlyAccess	预设策略	策略详情 前往C

○ 单击策略详情,展示其策略代码,支持复制;单击前往 CAM 查看,跳转至访问管理 > 策略 > 具体策略详情。



• 更多



○ 添加白名单策略:输入对应 IP、调用方式、AK、接口、返回码,填写说明请参见 策略管理。

← 添加日名	1单策略	<b>&amp;</b>	×
○ 策略生交	<b>攻预</b> 览		>> 隐藏说明
当 1.1	2.2. 使用 AK123456 通过 全部调用方式 调用 QueryList1、	QueryList2 ,	
返回码为 🗍	成功 时,均不进行告警监测,且 存量告警的处理状态修改为"已忽略" 。		) (1)
主效范围	增量告警命中策略内加白内容时,均不进行告警 ✔ 修改历史告誓的处理状态为"已忽略"	ייו ייו גלאווי אריין	2
1白内容 🔸	✔ 根据IP加白		返回码
	加白调用源iP 1.1 2.2	Pamero シン 接口 接口	) 
	🔽 调用方式		
	调用方式 <b>全部调用方式 控制台 API</b>		
	✔ 根据AK加白		
	加白AK 从现有AK中选择 <b>●</b> 自定义输入 AK123456		
	✔ 根据接口加白		
	加白接口 QueryList1 QueryList2		
	✔ 返回码		

○ 管理白名单策略:单击拉起策略管理抽屉,跳转至策略管理 > 白名单策略。



# 风险

最近更新时间: 2025-04-22 16:18:12

## 风险列表

- 1. 登录 云安全中心控制台,在左侧导览中,单击云 API 异常监测。
- 2. 在风险列表中,自动化扫描 AK 权限配置, 检查 AK 是否存在高权限策略,基于风险规则视角,查看配置风险描述与风险判定证据,并提供权限 策略配置建议。

是产列表	告誓 <b>风险</b>							
检测	更多 ~				近7天 > 3	处理状态: 未处理		0 © C F
	风险名称/类型 ⑦	风险等级 ⑦	AK名称/备注	账号名称/身份 🔽	证据 (风险配置)	风险检出时间 🗅	处理状态 了	操作
	不应该拥有高权限预设策略 配置风险	严重		⊘ 子账号(所属主账号: 腾讯云	AdministratorAccess		未处理	详情 更多 ~
	应该对访问管理(CAM)的操作权限进行收敛 配置风险	严重	3	⊘ 子账号(所属主账号: 勝讯云	cam:*CollApiKey		未处理	详情 更多 ~
	应该对访问管理(CAM)的操作权限进行收敛 配置风险	严重		⊘ 子账号(所属主账号: 膦讯云	cam:ListUsers		未处理	详情 更多 ~
	不应该拥有高权限预设策略 配置风险	严重		♂ 子账号(所属主账号:腾讯云	AdministratorAccess		未处理	详情 更多 ~
	不应该拥有高权限预设策略 配置风险	严重		ᢙ 子账号(所属主账号:腾讯云	AdministratorAccess		未处理	详情 更多 ~
	不应该拥有高权限预设策略 配置风险	严重		ᢙ 子账号(所属主账号: 腾讯云	AdministratorAccess,QCloudResourceF		未处理	详情 更多 ~
	不应该拥有高权限预设策略 配置风险	严重		☑ 子账号(所属主账号:腾讯云	AdministratorAccess		未处理	详情 更多 ~
	不应该拥有高权限预设策略 配置风险	严重			QCloudResourceFullAccess		未处理	详情 更多 ~
	应该对访问管理(CAM)的操作权限进行收敛 配置风险	严重			cam:AttachRolePolicy,cam:CreateRole,c		未处理	详情 更多 >
	不应该拥有高权限预设策略 配置风险	严重			AdministratorAccess		未处理	详情 更多 ~
共 91 项							10~条/页 🖂 🖣	1 /10页 ▶ ₩

字段名	示例	说明
风险名称/类型	配置风险	单击拉起 <b>风险详情</b> 抽屉。
风险等级	<ul> <li>严重</li> <li>高危</li> <li>中危</li> <li>低危</li> <li>提示</li> <li>无效</li> </ul>	基于腾讯云安全实践评定风险等级。
AK 名称/备注	AKID75XXX 部门1AK	AK 名称与自定义备注。 <ul> <li>AK 保留前6位与后11位,中间省略,支持一键复制;单击拉起 AK 详情抽屉。</li> <li>备注可自定义编辑,不超过20字符,若备注为空显示"—"。</li> </ul>
账号名称/身份	账号A 主账号/子账号(所属主账 号:主账号 B)	<ul> <li>AK 所属云厂商与账号,若为子账号展示所属主账号信息。</li> <li>鼠标悬浮查看账号 ID 与 APPID;支持筛选主账号/子账号。</li> </ul>



风险检出时间	2025-01-12 18:00:00	风险检出时间。 ● 格式:YYYY-MM-DD HH:MM:SS。 ● 支持排序。
处理状态	<ul><li>未处理</li><li>已处置</li><li>已忽略</li></ul>	展示风险处理状态,手动完成标记,处理状态支持筛选。

### 3. 在风险列表中,选择所需风险,单击**详情/更多**。

资产列表	告警风险							
检测	更多 >			近7天	✔ 处理状态:未处理			く 参い下
	风险名称/类型 了	风险等级 了	AK名称/备注		账号名称/身份 了	证据 (风险配置)	处理状态了	操作
	る	严重		l.	<mark>⊘</mark> 子账号 (所属主账号…	3	未处理	详情 更多 ~
	Σ 配置风险	<b>〕</b> … 严重	-		➢ ForCloudMonitor 子账号 (所属主账号	c ,	未处理	详情 更多 ∨

操作类型		说明
详情		单击拉起 <b>告警详情</b> 抽屉,查看风险描述与判定证据。查看风险检测内容以及 AK 对应的配置内容,根据 AK 权限策略配置对 AK 进行加固。
	检测	单击后重新检测该规则。
更多	标记忽略	单击后处理状态变为"已忽略"。
	API 密钥管理	单击跳转至 <b>访问管理 &gt; 访问密钥 &gt;</b> API 密钥管理。

# 规则说明

实时监控 AK 泄露与异常调用,监测分为三类:黑客工具识别、github 泄露(github 合作 + IP检查等 )、异常 IP 调用敏感接口等,具体规则见 下表:

规则名称	规则说明
应该对私有网络(VPC)的操作权限进行收敛	应该对私有网络(VPC)的操作权限进行收敛,不应拥有如下敏感接口权限: CreateCcnRouteTables, CreateNatGatewayDestinationIpPortTranslationNatRule, CreateNatGatewaySourceIpTranslationNatRule, CreateSecurityGroup, CreateSecurityGroupWithPolicies, CreateVpcEndPoint, CreateVpcPeeringConnection
应该对向量数据库的操作权限进行收敛	应该向量数据库的操作权限进行收敛,不应拥有如下敏感接口权限:ModifyAccessKey
应该对容器服务的操作权限进行收敛	应该容器服务的操作权限进行收敛,不应拥有如下敏感接口权限: CreateClusterEndpoint, DeleteEKSCluster, DeleteEKSContainerInstances, DescribeClusterKubeconfig, DescribeClusterSecurity, DescribeEKSClusterCredential



应该对高性能计算平台的操作权限进行收敛	应该高性能计算平台的操作权限进行收敛,不应拥有如下敏感接口权限: ModifyInitNodeScripts
应该对云开发服务的操作权限进行收敛	应该对云开发服务的操作权限进行收敛,不应拥有如下敏感接口权限: CreateCloudUser, DescribeEnvs
应该对腾讯云自动化助手的操作权限进行收敛	应该对腾讯云自动化助手的操作权限进行收敛,不应拥有如下敏感接口权限: CreateCommand, CreateInvoker, EnableInvoker, InvokeCommand, RunCommand
应该对安全凭证服务的操作权限进行收敛	应该对安全凭证服务的操作权限进行收敛,不应拥有如下敏感接口权限:AssumeRole, GetFederationToken
应该对云函数的操作权限进行收敛	应该对云函数的操作权限进行收敛,不应拥有如下敏感接口权限:CreateFunction, Invoke
应该对云数据库(Redis)的操作权限进行收敛	应该对云数据库(Redis)的操作权限进行收敛,不应拥有如下敏感接口权限: ClearInstance, KillMasterGroup, ModifyInstanceAccount, ResetPassword
应该对云数据库(PostgreSQL)的操作权限进 行收敛	应该对云数据库(PostgreSQL)的操作权限进行收敛,不应拥有如下敏感接口权限: ResetAccountPassword
应该对集团账号管理的操作权限进行收敛	应该对集团账号管理的操作权限进行收敛,不应拥有如下敏感接口权限: AddUserToGroup, CreateUserSyncProvisioning
应该对轻量应用服务器的操作权限进行收敛	应该对轻量应用服务器的操作权限进行收敛,不应拥有如下敏感接口权限: CreateKeyPair, ImportKeyPair, ResetInstancesPassword
应该对域名注册的操作权限进行收敛	应该对域名注册的操作权限进行收敛,不应拥有如下敏感接口权限: CreateDomainBatch, RegisterDomain, RenewAgentPay
应该对云解析(DNS)的操作权限进行收敛	应该对云解析(DNS)的操作权限进行收敛,不应拥有如下敏感接口权限: CreateDomainBatch, CreateShareDomains
应该对容器安全服务(TCSS)的操作权限进行 收敛	应该对容器安全服务(TCSS)的操作权限进行收敛,不应拥有如下敏感接口权限: DeleteMachine
应该对主机安全(CWP)的操作权限进行收敛	应该对主机安全(CWP)的操作权限进行收敛,不应拥有如下敏感接口权限: DeleteMachine
应该对操作审计(CloudAudit)的操作权限进 行收敛	应该对操作审计(CloudAudit)的操作权限进行收敛,不应拥有如下敏感接口权限: DeleteAudit, DeleteAuditTrack
应该对云数据库(MySQL)的操作权限进行收 敛	应该对云数据库(MySQL)的操作权限进行收敛,不应拥有如下敏感接口权限: CloseWanService, CreateAccounts, CreateRoInstanceIp, DescribeAccounts, DescribeBackups, DescribeBinlogs, ModifyAccountPassword, ModifyDBInstanceSecurityGroups, OpenWanService
应该对访问管理(CAM)的操作权限进行收敛	应该对访问管理(CAM)的操作权限进行收敛,不应拥有如下敏感接口权限:AddUser, AddUserToGroup,AttachRolePolicy,AttachUserPolicy, CreateAccessKey,CreateApiKey,CreateCollApiKey,CreateOIDCConfig, CreateRole,CreateSAMLProvider,CreateServiceLinkedRole, CreateUserOIDCConfig,CreateUserSAMLConfig,EnableApiKey, GetProjectKey,ListAccessKeys,ListUsers,UpdateAccessKey, UpdateCollPassword,UpdateUser
应该对黑石物理服务器(BM)的操作权限进行 收敛	应该对黑石物理服务器(BM)的操作权限进行收敛,不应拥有如下敏感接口权限: BuyDevices, CreateSpotDevice, ReloadDeviceOs, ResetDevicePassword,



应该对云服务器(CVM)的操作权限进行收敛	应该对云服务器(CVM)的操作权限进行收敛,不应拥有如下敏感接口权限: CreateKeyPair, ExportImages, ImportKeyPair, InquirePriceCreateInstances, InquiryPriceRunInstances, ModifyImageSharePermission, ModifySecurityGroupPolicys, ResetInstancesPassword, RunInstances, Adduser, UpdateUser
应该删除长期未使用AK密钥	应该删除长期未使用AK密钥,即使AK被禁用了也应该删除
不应该拥有高权限预设策略	AK不应该有AdministratorAccess、QCloudResourceFullAccess、 QcloudCamFullAccess、QCloudFinanceFullAccess高权限预设策略



# 策略管理

最近更新时间: 2025-04-22 16:18:12

### 告警策略

- 1. 登录 云安全中心控制台,在左侧导览中,单击云 API 异常监测。
- 2. 单击右上角的**策略管理**,进入告警策略页面,对告警策略进行管理,目前支持开启/关闭具体的告警策略、快速定位命中策略的告警。

策略管理					多账号管理	<mark>න</mark> :	~ ×
<b>告警策略</b> 白名单策	5略						
				多个关键字用竖线" "分	隔,多个过滤标签	用回车键分隔	Q D
策略名称/类型 了	策略来源 🔽	策略内容	命中次数	创建时间 ↓	开关 🔽	所属账号 ①	'操作
<b>访问密钥泄露(如github)…</b> 泄漏监测	系统策略	腾讯云对该密钥进…	0	2025-03-25 20:07:15		B	编辑 删除
<b>根密钥调用高危接口</b> 异常行为	系统策略	用户使用根密钥方…	0	2025-03-25 20:07:15		Ø	编辑 删除
<b>可疑IP调用高危接口</b> 异常行为	系统策略	在过去6个月未曾	1	2025-03-13 22:07:15		Ø	编辑 删除
<b>黑客工具检测</b> 异常行为	系统策略	该API使用方式与…	0	2025-03-13 22:07:15		Ø	编辑 删除
<b>非正常时间段敏感行为</b> 异常行为	系统策略	在晚上10点至凌晨…	0	2025-03-13 22:07:15		Ø	编辑 删除
<b>通过api创建云资源</b> 异常行为	系统策略	通过腾讯云API,…	0	2025-03-13 22:07:15		Ø	编辑 删除
<b>通过cos-browser调用…</b> 异常行为	系统策略	通过cos-browser	1	2025-03-13 22:07:15		Ø	编辑 删除
<b>长期未使用的访问密钥…</b> 异常行为	系统策略	在过去一个月内未…	0	2025-03-13 22:07:15		Ø	编辑 删除
<b>新增用户调用高危接口</b> 异常行为	系统策略	在今天创建的用户…	0	2025-03-13 22:07:15		Ø	编辑 删除
<b>未授权的服务调用</b> 异常行为	系统策略	通过API调用未授…	32	2025-03-13 22:07:15		Ø	编辑 删除
共 16 项					10 🖌 条 / 页	⊌ ◀ 1	/2页 ▶ ▶

## 白名单策略

- 1. 登录 云安全中心控制台,在左侧导览中,单击云 API 异常监测。
- 2. 单击右上角的策略管理 > 白名单策略,对白名单策略进行管理,支持基于调用源 IP、调用方式、AK、接口、返回码进行加白,并指定生效范围。



<b>策略管理</b> 告警策略 白名单策略			多账	号管理 🔗		× X
添加策略    删除			多个关键字用竖线" "分隔,多	3个过滤标签用回车等	建分隔	Q B
策略名称	加白内容	备注	更新时间 ↓	所属账号	▼ 操作	
	IP     全部       AK        接口     全部	-		Ø	编辑	删除
	IP 全部 AK 接口 全部	-		Ø	编辑	删除
共 2 项			10	✔ 条 / 页	◀ 1	/1页 ▶ ▶

### 3. 单击**添加策略**,配置相关参数,单击**保存**。

← 添加白名	单策略		🙆 ~ X	← 添加白	名单策略		
基本信息 1 策略名称•	↓ <b>填写白名</b> 请输入规则名称	<b>单策略基本信息</b> , 不超过20个字符		♀ 策略生 当 1.1 返回码为	2.2. 使用 / 成功 时,均不进行	XX123456〕 截江 【全部调用方式】 専用 【QueryList1、QueryList2】, 方音繁显满,且 【存量音音的处理状态传动为"已忽略"】。	(* ####* (* ####* (* ####*
备注 告 <b>警策略内容</b>	请输入文本,不	题过100个字符 题记		生效范围 加白内容・	增量告警命中策 学修改历史告警	能内加白内容时,均不进行音誉 的处理或态力"已思想"	
<ul> <li>○ 策略生交</li> <li>当 全部调け</li> <li>全部返回</li> </ul>	w 预览 3 査	<b>昏白名单策略生效预览</b> MK 通过 全部调用方式 调用 全部接口 , 返回码为 繁盛高,且 存量告爱的处理状态修改为"已忽略" 。	◎ manor (P) (P) (P)		加白调用源IP	11 22	Ринесо Ринесо ЯК
2 填3	写白名单策略	的容			🔽 调用方式		
生效范围	增量告警命中策略	内加白内容时,均不进行告警	und 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		调用方式	● 全部调用方式 控制台 API	
	✔ 修改历史告警的	的处理状态为"已忽略"			✓ 根据AK加自	3	
加白内容•	✓ 根据IP加白		AK 送回時		加白AK	○ 从现有AK中选择 ○ 自定义输入	
	加白调用源IP	遺输入需要加白的调用源P。手动输入后使用使用回车换行,每行一 个,最多支持输入1000 行;不支持CIDR地址,若输入重复IP,后台 将自动合并	Ремис ВС В В			AK123456	
			<u>18 LI 18 LI 18 LI</u>		✔ 根据接口加	伯	
	☑ 调用方式 调用方式	● 全部调带方式 控制台 API			加白接口	QueryList1 QueryList2	
	✓ 根据AK加白						
	加白AK	● 从现有AK中选择 选择AK(0) 自定义输入			✓ 返回码 返回码	✔ 成功 ○ 失敗	
保存	取消			保存	取消		

	内容名称	说明	示例
--	------	----	----



生效范围	<ul> <li>默认为增量告警命中策略内加白内容时,均不进行告警。</li> <li>可选择是否修改历史告警的处理状态为"已忽略"。</li> </ul>	-
根据 IP 加白	勾选该文本框后,自定义需加白的调用源 IP;不勾选默认全部 IP;填写规则: • 多个 IP 换行隔开,每行一个。 • 最多支持输入1000行;不支持 CIDR 地址,若输入重复 IP,后台将自动合并。	1.1.1.1 2.2.2.2
调用方式	勾选该文本框后,选择需加白的调用方式;不勾选默认全部 IP。 • 全部调用方式。 • 控制台。 • API。	-
根据 AK 加白	勾选该文本框后,选择或自定义需加白的 AK;不勾选默认全部 AK;填写规则: • 多个 AK 换行隔开,每行一个。 • 最多支持输入 1000 行。	AK1 AK2
根据接口加白	勾选该文本框后,自定义需加白的接口;不勾选默认全部接口;填写规则: <ul> <li>多个接口换行隔开,每行一个。</li> <li>最多支持输入1000 行。</li> </ul>	QueryList1 QueryList2
返回码	勾选该文本框后,选择需加白的返回码;不勾选默认全部。 • 成功。 • 失败。	-

# DNS 威胁监测 功能简介

最近更新时间:2025-05-27 09:24:11

云安全中心基于腾讯云内网 VPC DNS 公网递归解析(腾讯云默认183.60.83.19/183.60.82.98的 DNS 服务器 ),对域名请求行为进行实时威 胁监控,基于腾讯云独有的丰富情报识别**恶意或异常请求行为**,并进行告警。

建议您及时关注账号内主机**请求情况与相关告警**,可帮助您识别**矿池挖掘、恶意 C2、远程桌面工具、偏离基线行为**等,减少安全隐患,保障云上安 全。

## 核心能力

- 海**量情报精准匹配:**基于腾讯安全大数据挖掘能力和攻防经验模型化,提供专业威胁情报库,精准匹配百万情报,为您进行异常请求匹配,获取 威胁信息。
- 恶意请求实时监控: 免部署一键接入,接入后将默认同步您的腾讯云内网 VPC DNS 公网递归解析日志信息,为您进行实时安全监控,更好了 解 DNS 威胁。
- 异常行为基线监测: 重保、护网期间,支持对核心机器设定 DNS 解析行为基线,监测基线外异常行为。

## 功能点梳理

功能板块		功能点	解决问题	操作指引
统计面板-请求概览		快速了解请求情况、待处理的恶意请求与 异常基线告警等。	了解请求情况与异常占比,待处理的问题 有多少,近期安全运营趋势怎样。	统计面板
全部请求		查看全部域名请求情况、关联异常分析。	梳理有多少主机请求了哪些域名,是否有 命中异常。 关键时期可以进行历史全量域名请求记录 的回溯,协助进行溯源排查。	全部请求
	恶意请求	实时监控恶意域名请求,基于系统与自定 义告警规则视角,查看告警内容、机器详 细信息,并提供说明&修复方案。	识别矿池挖掘、远控木马、恶意 C2、远 程桌面工具等,配合主机/容器安全定位进 程,引导处置	恶意请求
告警列表	异常基线	支持设定行为基线策略,编辑监测的主机 与域名范围。当发生行为基线范围外的请 求时,产生异常告警。可查看告警内容、 机器详细信息。	对核心机器设定 DNS 解析行为基线,监 测基线外异常行为。	异常基线
	告警策略	管理系统告警策略。	答册录曲光计的生数等收 计甘工业名录	
策略管理	白名单策略	管理告警白名单,可对白名单进行增删改 查,基于主机、域名进行加白。	自理而安大注的古言來哈,升基于亚穷斋 要自定义白名单。	策略管理

# 统计面板

最近更新时间: 2025-04-24 15:11:02

- 1. 登录 云安全中心控制台,在左侧导览中,单击 DNS 威胁监测。
- 2. 在 DNS 威胁监测页面,请求概览模块分为以下三种:
  - **全部请求:**统计近7天,当前腾讯云账号下主账号与子账号全部请求。
  - **待处理:**统计近7天,当前腾讯云账号下主账号与子账号中处理状态为"待处理"的恶意请求&异常基线数量。
  - 告警趋势:统计近7天,每天新增的恶意请求&异常基线数量。
- 3. 在 DNS 威胁监测页面,单击关注的字段,下方列表搜索框中自动添加条件并筛选出对应内容。

DNS威胁监测 公测						(□) 策略管:	理 🛇 场景教学	多账号管理		~
请求概览(近7天) 全部请求	待处理告警	告鑒約	韵							
<b>19737</b> ^	<b>2329</b> ↑	点击字段 <sup>恶</sup>	意请求 13	7	6	4	7	2	2	
异常命中 2329	恶意请求 41 异常基线 2288	1 异	常基线 1724	116	81	79	131	69	88	
<u>恶意请求</u> 异常基 告誓名称/命中策	线 标记处重 更多 ~ 略 告誓等级 ⑦ 请	求主机口/名称	IP地址	请求域名	近7天 V DNS解析数	£ 2     £ 2	司动填充条件	自动筛 3 7 处理状态 T	先对应内容 。	2
告警名称/命中策	略 告警等级 了 请	求主机ID/名称	IP地址 公网: 内网:	请求域名 upda	DNS解析数 489	首次/最近告警时间 ↓	所属账号	文理状态 了           待处理	操作 详情 更多 ~	
	高危		公网: 内网:	rece	746		8	待处理	详情 更多 >	
	严重		公网: 内网:	upda	527		Ø	待处理	详情 更多 ~	
	高危		公网: 内网:	rece	837		Ø	待处理	详情 更多 ~	E
	高危		公网: 内网:	rece	767		Ø	待处理	详情 更多 ~	Ε
	严重		公网: 内网:	upda	520		8	待处理	详情 更多 ~	



# 全部请求

最近更新时间: 2025-04-24 15:11:02

### 全部请求列表

- 1. 登录 云安全中心控制台,在左侧导览中,单击 DNS 威胁监测。
- 2. 在 DNS 威胁监测 > 全部请求列表中,查看请求内容(主机信息、请求域名)、异常命中判定等。

()	说明:				
	列表数据聚合逻辑:	一天内同一账号下,	同一主机请求同-	-域名聚合为	<b>-</b> 条数据。

全部请求	告誉 (671)								
() 全部	请求中聚合方式为 <b>请求主机+短名</b> , 角	身赤请求下可能关联多个告誓,请知悉。							
添加策略 ·	~						<b>最近请求时间 &gt; 近7天 &gt; </b> 多个关键字用	1竖线 * * 分隔,多个过滤标签用回车罐分前	0 @ C 4
	请求主机ID/名称	IP地址	黄瓢/地域 罕	请求城名	DNS解析数	异常命中	首次/最近请求时间↓	所属账号 🛛	操作
	1000	公网: 内网:	CVM 上淘金融	31	15709		20: 20:		详情 更多 ~
		公明: 内同:	CVM 単庆	tär	2628		20: 20:	ø	洋情 更多 ~
		公网: 内网:	CVM 成都	tir	2632	-	20: 20:	8	洋情 更多 >
		公网: 内网:	CVM I 成都	tin	1488		20: 20:		洋情 更多 ~
		公网: 内网:	CVM 重庆	tin	2621	-	20: 20:	۵	洋情 更多 ~
		公网: 内网:	CVM I 成都	tir	2585		20: 20:	<b>Ø</b>	洋情 更多 ~
		公网: 内网:	CVM 目成都	tir	2629	-	20: 20:	<u>@</u>	洋情 更多 ~
		公网: 内网:	CVM 成都	ti	2627		20: 20:	0	洋情 更多 ~
		公明: 内网:	CVM 成都	tic	2647		20: 20:	8	洋情 更多 ~
		公网: 内网:	CVM 成都	tir	2596		20: 20:		洋情 更多 ~
共 14703 項								10~条/页 国	< 1 /1471页 ▶ H

字段名	示例	说明
请求主机 ID/名称	ins-xxx 主机 A	发起请求的主机,单击新开页面进入 <b>主机资产详情</b>
IP 地址	公网: x.x.x.x 内网: x.x.x.x	发起请求主机的公网与内网 IP 地址
类型/地域	CVM   地域 A	发起请求主机的类型与所属地域,当前仅支持 CVM
请求域名	xxx.com	主机请求的域名
DNS 解析数	-	单击跳转 <b>日志分析</b> ,筛选对应日志
异常命中	异常基线 恶意请求	该请求是否有命中相关
首次/最近请求时间	2025-01-01 18:00:00 2025-01-12 18:00:00	● 格式:YYYY-MM-DD HH:MM:SS ● 支持排序

3. 在全部请求列表中,选择所需请求,单击**详情/更多**。



全部请求	告警 (1064)						
() ≦	全部请求中聚合方式为 请 <b>求主机+域</b>	<b>名</b> ,单条请求下可能关联多个	告警,请知悉。				
添加第	高略 ~		最近请求时间 >	近7天 🗸 🗸	多个关键字用竖线"1"分隔,多个过	慮标签用回车键分隔	Q & D
	请求主机ID/名称	IP地址	请求域名	DNS部	斜折数 异常命中	首次/最近 所属账号	<b>⑦</b> 操作
	im @	公网: 00 内网:	re	p	异常基线: 1	2025-04-2 2025-04-2 🙆 腾讯云:	安 详情 更多 >
	1	公网: 内网:	tin		异常基线: 1	2025-04-2 2025-04-2 🙆 腾讯云:	添加恶意请求策略 <sup>安.</sup> 加入行为基线策略

操作类型		说明
详情		单击拉起 请求详情 抽屉。
百夕	添加恶意请求策 略	单击打开 <b>添加恶意请求策略</b> 弹窗,并填充对应内容。添加后若命中该策略将产生恶意请求告警。
¥9	加入行为基线策 略	单击打开 <b>加入行为基线策略</b> 弹窗,并填充对应内容。加入后当发生行为基线策略范围外的请求时,产 生异常基线告警。

# 请求详情

在请求详情抽屉页面,查看请求信息、请求详情与关联异常情况。

• 查看请求基本信息

DNS解析数     2565     首次使用时间     2025       是否异常     异常请求     最近使用时间     2025	基本信	息	
是否异常     异常请求     最近使用时间     2025	DNS解析	行数 2565	首次使用时间 2025
	是否异常	异常请求	最近使用时间 2025

 查看请求详情:查看哪些主机访问了指定域名,并提供主机的详细信息。要获取进程、命令行、MD5等更多信息,请升级至主机安全 专业版或 旗舰版。



求详情 请求 ins	主机 详情		请求域名 tir
请求主机详情			
IP地址	公	内	所属网络 vpc 文 D
资产标签		Ø	
资产类型	CVM		① 进程/命令行/MD5等更多信息需开通主机安全专业版/旗舰版获取
地域	成都		

• 查看关联异常:查看恶意请求、异常基线的告警关联情况及其命中策略。

关联异常			
恶意请求告警	0	异常基线告警	1
命中策略	-	命中策略	-



# 恶意请求

最近更新时间: 2025-04-24 15:11:02

### 恶意请求列表

- 1. 登录 云安全中心控制台,在左侧导览中,单击 DNS 威胁监测。
- 2. 在 DNS 威胁监测 > 告警列表 > 恶意请求中,查看告警内容(名称、等级),请求内容(主机信息、请求域名)处理状态等。

## () 说明:

列表数据聚合逻辑:一天内同一账号下,同一告警。

全部请求	告誓 (671)									
恶意请求	そ 异常基线 時記社会 更多 >						近7天	> 处理状态: 得处理		0 @ 8 ±
	告豐名称/命中策略	告誉等级 了	请求主机ID/名称	IP地址	请求域名	DNS解析数	首次/最近告誓时间 ↓	所属账号 🍸	处理状态 冒	操作
	自定义策略	高危	ins pg.	公開: 内開:		424	2025- 2025-	ø	待处理	详情 更多 ~
	自定义策略	严重	ins 截点	公网: 内网:		2	2025- 2025-	۵	待处理	详情 更多 ~
	自定义策略	严重	ins 自ī	公网: 内网:		271	2025- 2025-	8	待处理	洋橋 更多 ~
	自定义策略	高危	ins Pg	公局: 内局:		795	2025- 2025-	8	待处理	洋情 更多 ~
	自定义策略	严重	ins 自主	公网: 内网:		527	2025- 2025-	8	待处理	洋橋 更多 ~
	自定义策略	严重	ins 自ī	公网: 内网:		527	2025- 2025-	8	待处理	洋橋 更多 ~
	自定义策略	高危	ins pg:	公网: 内网:		837	2025- 2025-	۵	待处理	详情 更多 ~
	自定义策略	高危	ins pg:	公网: 内网:		767	2025- 2025-	۵	待处理	详情 更多 ~
	自定义策略	严重	ins 自主	公网: 内网:		520	2025- 2025-	8	待处理	₩₩ 更多 ~ [
	自定义策略	产业	ins wa	公网: 内网:		5061	2025- 2025-	8	待处理	详情 更多 ~
共 31 項									10 🗸 条 / 页	∺ 4 1 /4页 ▶ H

字段名	示例	说明
告警名称/命中策略	<ul><li>系统策略</li><li>自定义策略</li></ul>	单击拉起 <b>告警详情</b> 抽屉
告警等级	<ul> <li>严重</li> <li>高危</li> <li>中危</li> <li>低危</li> <li>提示</li> <li>无效</li> </ul>	基于腾讯云安全实践评定告警等级
请求主机ID/名称	ins-xxx 主机 A	发起请求的主机,单击新开页面进入 <b>主机资产详情</b>
IP地址	公网:x.x.x.x 内网:x.x.x.x	发起请求主机的公网与内网 IP 地址
请求域名	xxx.com	主机请求的域名
DNS解析数	-	单击跳转 <b>日志分析</b> ,筛选对应日志



首次/最近告警时间	2025-01-01 18:00:00 2025-01-12 18:00:00	● 格式:YYYY-MM-DD HH:MM:SS ● 支持排序
处理状态	<ul><li>未处理</li><li>已处置</li><li>已忽略</li></ul>	展示告警处理状态,手动完成标记,处理状态支持筛选

### 3. 在恶意请求列表中,选择所需请求,单击**详情/更多**。

全部请求 告警 (					
恶意请求 异常基线	标记处置 更多 >	近30天 > 多个	Y关键字用竖线 " " 分隔,多个过滤标签用回车	键分隔	Q @ £
告警名称/命中策略	告警等级 了 请求主机ID/名称	IP地址	请求感名所属账号	♥ 处理状态	了探作
育 系统策略	高危 	公网: · · · · · · · · · · · · · · · · · · ·	▶	待处理	详情 更多 >
共1项			10 ∨ 条/]	页 14 4	标记处置 标记忽略 添加白名单策略

操作类型		说明
详情		单击拉起 告警详情 抽屉。
	标记处置	单击后处理状态变为"已处置"。
更多	标记忽略	单击后处理状态变为"已忽略"。
	添加白名单策略	单击拉起 <b>添加白名单策略</b> 抽屉,并填充对应 AK。

# 恶意请求详情

在告警详情抽屉页面,查看告警信息、请求详情与说明&修复方案。

• 查看告警基本信息。

告警详情 待处理		标记处置 更多 ~ X
<b>非法挖矿活动</b> 悪意请求	告警等级 高危 命中策略 系统策略	
DNS解析数 147	首次告警时间 2025 最近告警时间 2025	



 查看请求详情:查看哪些主机访问了指定域名,并提供主机的详细信息。要获取进程、命令行、MD5等更多信息,请升级至主机安全 专业版或 旗舰版。

青求详情	求主机 5 详情	请求域名 tir		
请求主机详情				
IP地址	公内	所属网络 vpc 文 D		
资产标签	Ø			
资产类型	CVM	<ol> <li>进程/命令行/MD5等更多信息需开通主机安全专业版/旗舰版获取 立即开通 IC</li> </ol>		
また	成都			
10436				

#### • 查看说明&修复方案:按照指引处置告警。

### ○ 说明&修复方案 黑客通常会通过弱口令爆破、漏洞攻击等手段攻陷主机,并植入挖矿木马,在用户不知情的情况下利用其计算机的云算力进行挖矿,从而获取利益,挖矿木 告警描述 马会占用CPU等资源,影响用户的正常业务,危害较大。 修复方案 1.在不影响业务的前提下,及时隔离主机/容器,避免部分带有蠕虫功能的挖矿木马进一步在内网进行横向移动; 2.根据cpu占用等信息找到中招机器的挖矿木马 3.若确认为挖矿木马,则进行如下清理操作: (1) 结束挖矿相关进程。 (2) 删除挖矿相关文件。 (3) 查看并清理异常定时任务。 (4) 查看密钥认证文件 删除木马创建的密钥认证文件,如果当前系统之前并未配置过密钥认证,可以直接清空认证存放目录。如果有配置过密钥认证,只需要删除黑客创建的认证 文件即可 4.对系统进行风险排查和安全加固,详情可参考如下链接: [Linux] https://cloud.tencent.com/document/product/296/9604 [Windows] https://cloud.tencent.com/document/product/296/9605



# 异常基线

最近更新时间: 2025-04-24 15:11:02

## 异常基线列表

1. 登录 云安全中心控制台,在左侧导览中,单击 DNS 威胁监测。

2. 在 DNS 威胁监测 > 告警列表 > 异常基线中,查看偏离基线的请求行为(请求内容:主机信息、请求域名),处理状态等。

()	<b>兑明</b> :
	<b>刘表数据聚合逻辑:一天内同一账号下,同一主机请求同一域名聚合为一条数据</b> 。

全部请求	告誓 (676)								
恶意请求	异常基线								
🛞 🕯	<b>宁为基线策略</b> 设置正常行为基线策略,当发生 4.联策略:3条 详情	生行为基础范围外的请求时,将产生一条异常告誓。							
加入行为	夏多~						近7天 × 处理状态: 将	处理	Q @ छ ∓
	请求主机ID/名称	IP地址	请求城名	DNS解析数	恶意请求告誓	首次/最近请求时间↓	前属数号 🙄	处理状态 冒	操作
	ins do	公网: 内网:		2661	0	2025- 2025-	۵.	待处理	详情 更多 ~
	ins as	公网: 内网:		1019	0	2025- 2025-	۵	特处理	洋橋 重多 ~
	ins 未	公网: 内网:		3345	0	2025- 2025-	8	特处理	详情 更多 ~
	ins 未	公网: 内网:		3049	0	2025- 2025-	8	特处理	详情 更多 ~
	ins do	公嗣: 内阙:		3897	0	2025- 2025-	8	待处理	洋橋 更多 ~
	ins 未	公丽: 内丽:		3398	0	2025- 2025-	8	待处理	详情 更多 ~
	ins do	公嗣: 内阙:		3864	0	2025- 2025-	8	待处理	洋情 更多 ~
	ins 来(	公嗣: 内嗣:		2764	0	2025- 2025-	8	待处理	¥情 更多~
	int do	公嗣: 内阙:		3428	0	2025- 2025-	8	待处理	洋楠 更多~
	int as	公嗣: 内例:		1019	0	2025- 2025-	8	待处理	洋橋 更多 ~
共 645 项								10 ~ 😤	д н ∢ 1 /65页 ► н

字段名	示例	说明
请求主机 ID/名称	ins−xxx 主机 A	发起请求的主机,单击新开页面进入 <b>主机资产详情</b>
IP 地址	公网: x.x.x.x 内网: x.x.x.x	发起请求主机的公网与内网 IP 地址
请求域名	xxx.com	主机请求的域名
DNS 解析数	-	单击跳转 <b>日志分析</b> ,筛选对应日志
恶意请求告警	-	该偏离基线行为是否命中情报
首次/最近请求时间	2025-01-01 18:00:00 2025-01-12 18:00:00	<ul><li>● 格式: YYYY-MM-DD HH:MM:SS</li><li>● 支持排序</li></ul>
处理状态	<ul> <li>● 未处理</li> <li>● 已处置</li> <li>● 已忽略</li> </ul>	展示告警处理状态,手动完成标记,处理状态支持筛选

# 🔗 腾讯云

### 3. 在异常基线列表中,选择所需请求,单击**详情/更多**。

加入	行为基线策略 更多 >			近7天	✔ 处理状态: 待处	也理			く 参 5 平
	请求主机ID/名称	IP地址	请求域名	DNS解析	数 恶意请求告警	首次/最近请: 月	所属账号 ⑦	处理状态	了 操作
	þ	公网: 内网:	>	þ	0	2025-04-24 2025-04-24	❷ 腾讯云安	待处理	详情 更多 ∨
		公网: 内网:			0	2025-04-24 2025-04-24	❷ 腾讯云安	待处理	加入行为基线策略 标记处置
		公网: 内网:			0	2025-04-24 2025-04-24	❷ 腾讯云安	待处理	标记忽略 创建告警策略

操作类型		说明
详情		单击拉起 告警详情 抽屉。
	加入行为基线策 略	单击打开 <b>加入行为基线策略</b> 弹窗,并填充对应内容。加入后当发生行为基线策略范围外的请求时,产 生异常基线告警。
百夕	标记处置	单击后处理状态变为"已处置"。
£3	标记忽略	单击后处理状态变为"已忽略"。
	创建告警策略	单击拉起 <b>添加策略-恶意请求</b> 抽屉,并填充生效主机、生效域名。添加后若命中该策略将产生恶意请求 告警。

## 异常基线详情

在请求详情抽屉页面,查看请求信息、请求详情与关联异常情况。

• 查看请求基本信息。

DNS解析数     2565     首次使用时间     2025       是否异常     异常请求     最近使用时间     2025	基本信息			
是否异常     异常请求     最近使用时间     2025	DNS解析数	2565	首次使用时间	2025
	是否异常	异常请求	最近使用时间	2025

 查看请求详情:查看哪些主机访问了指定域名,并提供主机的详细信息。要获取进程、命令行、MD5等更多信息,请升级至主机安全 专业版或 旗舰版。



家详情		
请; in:	求主机 5 详情	请求域名 tir
请求主机详情		
IP地址	公内	所属网络 vpc 文 D
资产标签	ð	
资产类型	CVM	<ul> <li></li></ul>
地域	成都	
所属账号	8	

• 查看关联异常:查看恶意请求、异常基线的告警关联情况及其命中策略。

关联异常			
恶意请求告警	0	异常基线告警	1
命中策略	-	命中策略	-


# 策略管理

最近更新时间: 2025-04-24 15:11:02

## 恶意请求

- 1. 登录 云安全中心控制台,在左侧导览中,单击 DNS 威胁监测。
- 2. 在 DNS 威胁监测页面,单击右上角的**策略管理**。
- 3. 在恶意请求页签,可以对告警策略进行管理,目前支持开启/关闭具体的告警策略、自定义策略、快速定位命中策略的告警。

告警策	<b>传略</b>						
恶意	请求 异常基线	添加策略	删除	多个关键字用竖线 "	"        分隔,多个过滤标签	用回车键分隔	Q
	策略名称	策略来源	策略内容	告警命中	更新时 开关 了	所属账号 ⑦	操作
		自定义策略	域名 资产	1次	2025- 🚺	Ø	编辑删除
		自定义策略	域名 资产	28次	2025-	Ø	编辑删除
		自定义策略	域名 资产	31次	2025- 🚺	Ø	编辑删除
		自定义策略	域名 资产	11次	2025- 🚺	Ø	编辑删除
		自定义策略	域名 资产	0	2025- 🚺	Ø	编辑 删除
5顶					10 文 冬 / 页		/1页 🕨

4. 在恶意请求页签,单击添加策略,配置相关参数,单击**保存**。

← 添加策			
基本信息	填写策略基本信息		
策略名称 •	● 请输入策略名称,不超过20个字符		
策略内容			
<ol> <li>(i) 您可以</li> </ol>	在下方配置 请求的主机及域名 ,后续当检测到对应请求时,将生成一条告警。		
告警名称 •	填写告營相关信息           请输入告警名称,不超过20个字符         2		
告警等级 🔹	● 严重   高危   中危   低危   提示		
生效主机 *	● 全部主机 (103) 剔除资产(0) 自选主机		
生效域名 *	○ 自定义域名 3		
	· · · · · · · · · · · · · · · · · · ·		
	调制八或力/之场力(Xi- www.iZ345.com、:tencent.com等,首个文符ORC),多于对各场关门方圈		
	頃間八蔵石(火城石 (Xi- www.iZ345.com、.ienceniccom等,置小又持ORC),多「丹谷以来1万南		
← 添加策	inmin(或句)/2/43 (xi) www.i2345.com, fieldent.com等, min/240Rc), 多于对各场来127网 格-恶意请求	۵	×
← 添加策 基本信息	infm/(或句//2/或句 (xii- www.iz345.com, filencent.com等, 当小文为ORL), 多于对各以来[1万角 略-恶意请求	<u>ه</u> ~	×
← 添加策器 基本信息 策略名称•	infmi/(或在)/2/或石(xii: www.i2345.com、.tencent.com等,当个交付ORL),多于对各场关门方端 略-恶意请求 策略1	<u>~</u>	×
← 添加策 基本信息 策略名称 •	infm/(或句)/2/43 (xi) www.i2345.com, '.tencent.comy, inf√(xioRc), 少1 /y345(xi)/3/in 略-恶意请求 策略1	Ø ~	×
← 添加策器 基本信息 策略名称 • 策略内容	###/(感音)/2/843 (SE: WWW.12345.COII、'.teiteint.Coility', 当小公内ORE), ⇒1 //345(共)137篇 略-恶意请求 策略1	∠	×
← 添加策略 基本信息 策略名称・ 策略内容 () (第可因)	###/(感音)/2-%子 (知: www.12345.com, .tencent.com等, 当小交用のた), ラーバスなのた), ラーバスなのた), ラーバスないだ), デーバスのた), デーバスのた, デーバスのた, デーバスのた), デーバスのた), デーバスのた, デーバー (デーバン・デーバスのた, デーバー (デーバースのた, デーバスのた, デーバスのた, デーバスのた, デーバーズ(デーバースのた, デーバスのた, デーバスのた, デーバーズのた, デーバーズ(デーバンパーパーズのた, デーバーズ(デーバンパーパーズのた, デーバーズ(デーバンパーズのた, デーバーズ(デーバンパーズ(デーバーズーズ(デーバーズーズ(デーバーズ, デーバーズ(デーバン, デーバーズ(デーバーズ, デーバーズ(デーバーズ, デーバーズ(デーバーズ, デーバーズ(デーバーズ, デーバーズ(デーバーズ, デーバーズ(デーバーズ, デーバーズ(デーバー		×
← 添加策日 基本信息 策略名称・ 策略内容 ① 您可以很小!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!	In 細八成立 // 2-43 (SL)・WWW.12345.COII、「LEICEIIL COIII等, 目小2 (HORC), 多 / P345.CP(1) 5 / / 8 略-恶意请求 策略1 在下方配置 请求的主机及域名 , 后续当检测到对应请求时,将生成一条告警。		×
← 添加策略 基本信息 策略名称・ 策略内容 ① 您可以れ	請書/(截在)/2/434 (Si): WWW.12345.com, 'Aencent.come, art/2/404c), 多十分各块关门方端         略-恶意请求         策略1         在下方配置 请求的主机及域名 ,后续当检测到对应请求时,将生成一条告警。         告警名称A		×
← 添加策II 基本信息 策略名称。 策略内容 ① 您可以很 ① 您可以很 告警名称。	In ##IX(或在)/2-343 (SD· WWW.12345.COII、*.telicent.coIII等, 曾不父母ORC), 多个对各块关门方端           略-恶意请求           策略1           生下方配置 请求的主机及域名 ,后续当检测到对应请求时,将生成一条告警。           告警名称A           ● 严重 高危 中危 低危 提示		×
← 添加策器 基本信息 策略名称・ 策略内容 ① 您可以で 告警名称・ 告警名称・ 告警务级・ 主数主机・	In ##IX(報告)(2243-5 (SI)・WWW.12345(COIII、*.IEIICEIILCOIII等, 目不気用のRC), 多十列各以来[137/# <b>略-恶意请求</b> 第略1         生下方配置 请求的主机及域名 ,后续当检测到对应请求时,将生成一条告誓。         告警名称A         ● 严重 高危 中危 低危 提示         ● 企邸主机 (103) 馴除资产(0) 自选主机		×
← 添加策問 基本信息 基本信息 策略名称・ 策略内容 <ol> <li>您可以れ</li> <li>您可以れ</li> </ol> 告警等级・ 告警等级・ 生效主机・ 主效域名・	Immitted (1/2-43-5 (still: www.i2345.com); *.tencent.com; #14/2404c); #14/240c); #14/240c)		×
← 添加策日 基本信息 策略名称・ 策略内容 ① 您可以很 告警答级・ 告警等级・ 生效主机・ 生效或名・	In ##IX(報告)/2:43-5 (SDF WWW.12345(2011、*.1611CBULLCOUNEY, 当下父母び代力, 当下外会议关门力端          略-恶意请求         第略1         生下方配置 请求的主机及域名 , 后续当检测到对应请求时,将生成一条告警。         告警名称A         严重 高危 中危 低危 提示         全部主机 (103) 剔除资产(0) 自选主机         自定义域名         WWW.123.com		``````````````````````````````````````

# 异常基线

- 1. 登录 云安全中心控制台,在左侧导览中,单击 DNS 威胁监测。
- 2. 在 DNS 威胁监测页面,单击右上角的策略管理。
- 3. 在异常基线页签,对行为基线策略进行管理,目前支持开启/关闭具体的策略、编辑策略。

#### () 说明:

腾讯云

策略说明:一个账号仅支持配置1条行为基线策略,在策略中添加您判定为正常的请求主机及域名,策略生效后进行非白即黑判定,对所 有基线策略外产生的请求生成告警。



<b>古</b> 言 東 哈	白名单策略			多账号管理	6	~
恶意请求	异常基线					
〕 单个云账号	号下仅支持配置1条行为基线策略,	您可以在策略中添加您 <mark>判定为</mark> 」	<b>正常</b> 的请求主机及域名,	策略生效后将对所有基	基线策略外产生的请求	生成告警。
	<b>基线策略                                     </b>	戈范围外的请求时,将产生一条异	常告警。			•
生效主机:3 f 生效域名:1~						

4. 在异常基线页签,单击行为基线策略的 🧷 ,修改生效主机/域名,单击保存。

#### () 说明:

- 选择生效主机:建议选择核心机器设定 DNS 解析行为基线,监测基线外异常行为。
- 选择生效域名:展示在 X 天内请求过的域名,选择需要加入行为基线的域名。建议选择全部未命中情报的域名(命中情报:命中腾讯 云主机安全恶意域名库的域名)。



辑策略-行为基线					<u>&amp;</u>		~	
<ul> <li>         i 当前仅支持配置1条行         ;         </li> </ul>	为基线策略,您	可以在策略中添	加您 <b>判定为正常</b> 的请	求主机及域名,策略生效质	后将对所有基线策略外产生	生的请求生成告	警。	
效主机选择								
效主机 🔹 🔷 全部主	机 (103)	自选主机						
效域名选择								
效域名 * 🔷 从现有	请求域名中选择	自定义域	名					
3天内请求过的域名	~							
择域名(108)				已选择的域名(0)				
请输入搜索内容			Q	请求域名	影响主机 命中情	报 🛈   最近	请求时间	
请求域名	影响主机	命中情报 🛈	最近请求时间					
mi	4	否	2025-					
_h	2	否	2025-		=			
re	1	否	2025-		暂无数据	6		
	2	不	2025	↔				
w	3		2020-					
do	3	否	2025-					
_h	2	否	2025-					
37	1	不	2025-					
共 108 项 <b>10 ~</b> 祭	条/页 №	◀ 1	/11页 🕨 🕨					
				取消全部选择				

# 白名单策略

- 1. 录 云安全中心控制台,在左侧导览中,单击 DNS 威胁监测。
- 2. 在 DNS 威胁监测页面,单击右上角的策略管理 > 白名单策略。
- 3. 在白名单策略页面,对白名单策略进行管理,支持基于资产、域名进行加白。



告警領	策略 <b>白名单策略</b>					
添加	白名单    删除		多个关键	字用竖线 " " 分隔,多个过滤标签	用回车键分隔	Q
	策略名称	加白内容	备注	更新时间 🛟	所属账号 ⑦	操作
		域名 资产		2025	Ø	编辑删除
		域名资产		2025		编辑删除
		域名 资产		2025	<mark>⊗</mark>	编辑删除
3 项				10 ~ 条 / 页	₩ ◀ 1	/1页 ▶ ●

4. 在白名单策略页面,单击添加白名单,配置相关参数,单击**保存**。

← 添加策	略-白名单策略		~ X
基本信息	填写策略基本信息		
策略名称 *	请输入策略名称,不超过20个字符		
备注	请输入备注信息,不超过20个字符		
策略内容			
() 您可以	在下方放通 <b>请求的主机及域名</b> ,后续当检测到对应请求时,将不再生成告警。		
生效主机	● 全部主机 (103) 剔除资产(0) 自选主机 【选择加白策略生效的主机和域名范围】	]	
生效域名	● 自定义域名 2		
	请输入域名/泛域名(如:www.12345.com、*.tencent.com等,暂不支持URL),多个内容以换行分隔		
← 编辑策	略-白名单策略		~ ×
← 编辑策 基本信息	略-白名单策略	8	~ <b>X</b>
<ul> <li>← 编辑策</li> <li>基本信息</li> <li>策略名称・</li> </ul>	略-白名单策略 <sup>策略1</sup>	۵	~ X
<ul> <li>← 编辑策</li> <li>基本信息</li> <li>策略名称・</li> <li>备注</li> </ul>	略-白名单策略 策略1 业务A加白	۵	~ ×
<ul> <li>← 编辑策</li> <li>基本信息</li> <li>策略名称 *</li> <li>备注</li> </ul>	略-白名单策略 策略1 业务A加白		~ X
<ul> <li>← 编辑策</li> <li>基本信息</li> <li>策略名称 •</li> <li>备注</li> <li>策略内容</li> </ul>	略-白名单策略 策略1 业务A加白		<ul> <li>✓ X</li> </ul>
<ul> <li>← 编辑策</li> <li>基本信息</li> <li>策略名称。</li> <li>备注</li> <li>策略内容</li> <li>① 您可以</li> </ul>	<b>略-白名单策略</b> 策略1 业务A加白		× ×
<ul> <li>← 编辑策</li> <li>基本信息</li> <li>策略名称。</li> <li>备注</li> <li>策略内容</li> <li>① 您可以</li> <li>生效主机</li> </ul>	<ul> <li>略-白名单策略</li> <li>策略1</li> <li>业务A加白</li> <li>在下方放通 请求的主机及域名 , 后续当检测到对应请求时,将不再生成告警。</li> <li>● 全部主机 (0) 剔除资产(0) 自选主机</li> </ul>		<ul> <li>✓ X</li> </ul>
<ul> <li>← 编辑策</li> <li>基本信息</li> <li>策略名称・</li> <li>备注</li> <li>策略内容</li> <li>① 您可以</li> <li>生效或名</li> </ul>	<ul> <li>路-白名单策略</li> <li>策略1         <ul> <li>业务A加白</li> </ul> </li> <li>在下方放通 请求的主机及域名 ,后续当检测到对应请求时,将不再生成告警。</li> <li>全部主机 (0) 删除资产(0) 自选主机</li> <li>〕自定义域名</li> </ul>		✓ X
<ul> <li>← 编辑策</li> <li>基本信息</li> <li>策略名称・</li> <li>备注</li> <li>策略内容</li> <li>① 您可以</li> <li>生效主机</li> <li>生效域名</li> </ul>	<ul> <li>第年白名单策略</li> <li>第第1</li> <li>业务A加白</li> <li>本下方放通 请求的主机及域名 , 后续当检测到对应请求时,将不再生成告警。</li> <li>全部主机 (0) 剔除资产(0) 自选主机</li> <li>自定义域名</li> <li>2.com</li> <li>3.com</li> </ul>		× x



# 用户行为分析(UEBA)

最近更新时间: 2025-05-28 18:07:11

腾讯云

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。

① **模块可见范围说明:** 用户行为分析(UEBA)功能仅供存量用户使用,新用户如需相关能力,可以使用 云 API 异常监测功能,相关文档: 云 API 异常监测− 功能简介 。

### 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。

用户行为管理				
<b>用产概况 全部用产 92</b> 个 非常行力用产 0	28年9月月19 92 个 7指9 91	rexap © O↑ Referan	行为概况	NATARE NABATENTES Itte-deskeratentes, karraputaetes, ereitenteseratentesea, e <b>Ine</b> a

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。

日志类型	选择一个日志类型	*
	还没有接入日志,前往	
用户ID	选择一个代表用户ID的字段	•
用户名称	选择一个代表用户名称的字段(可不选)	Ŧ
彙作对象 🛈	请选择	
桑作方式 🛈	请选择	



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**。

行为概况	
	暂无行为数据,请先接入云审计日志
	云安全中心还没有接入云审计日志,无法提供用户行为概览数据,请前往日志分析页面完成云审计日志接入,或 <b>立即接入</b>

3. 在接入日志源对话框中,日志来源可选择操作o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。

<b>妾入日志</b> 》	京						×		
日志来源	云审计					•			
诸时长	7天	30天	60天	90天	180天				
入方式	通过跟踪	集接入				Ŧ			
宗集	请选择跟	踪集				т Ф			
	仅展示可用	且存储到CO:	S的跟踪集, 确定	如已关闭,讠 <b>取消</b>	青先前往开启				
家来源		参数名	称		说明				
审计		存储时	к	1	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。
	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。
自定义日志来源	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。

行为概况							- 昇	常行为(次)	- 异常账号(个)
发现异常行为									
<b>O</b> $\uparrow$									
查看所有行为	05-06	05-07	05-08	05-09	05-09	05–10	05–11	05–12	05–13

# 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。

添加策略 删除策略		多个关键书	P用竖线 IT 分隔,多个过滤标签)	用回车键分隔	Q Ø		
策略ID/名称	策略类型 ▼ 告警等级	₹ 策略内容	开关 ▼	命中次数 🤅 🛊	操作		
可疑IP调用高危接口	系统策略 严重	过去6个月未曾出现过的IP,调用了高危接口		0次	编辑 删除		
root账号进行aksk调用	系统策略 高危	根账号使用aksk进行接口调用		0次	编辑 删除		
长期未使用aksk突发调用	系统策略 高危	长期未使用指一个月内未曾出现过的aksk		0次	编辑 删除		
新用户高危操作	系统策略 高危	新用户指创建时间在最近一天内的用户,高危援 敏感/存在安全隐患的接口列表	操作指调用	0次	编辑删除		
非常用接口突发高频调用	系统策略中危	指在单位时间内某接口调用次数较高,但是其在 内调用蚊少	BUZATA	0次	編輯 删除		
参数名称	说明						
策略 ID	系统默认生	系统默认生成。					
策略名称	系统策略由	产品后台定义;用户自定义策略的	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。

自定义策略		×
策略名称	请输入策略名,不超过20个字符	
用户类型	选择用户类型 ▼ 选择该类型对应的日志类型 ▼	
发生时间	● 毎10分钟 ● 毎小时 ● 毎天 ● 毎周 ● 毎月	
发生事件	● 语句检索 ○ 过滤检索	
	请输入检索语句,支持SQL语句	
告警名称	选择告警名称	
告警等级		
操作者 🛈	请选择	
操作对象 🛈	请选择	
操作方式 🛈	请选择	

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。 <ul> <li>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。</li> <li>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。</li> </ul>
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。



# 大模型态势管理

最近更新时间: 2025-04-01 10:13:13

大模型态势管理为您提供大模型组件资产识别、大模型组件风险识别、网络攻击预警等能力。您可以通过本页面查看云账号下存在的大模型组件,并 了解其可能存在的安全风险及可能正在遭受的网络攻击。资产与风险识别来源于云安全中心体检能力及主机安全的检测能力,网络攻击数据来源于主 机安全。云安全中心将在您购买了主机安全的情况下,读取相关数据。

## 前提条件

已购买 云安全中心高级版。

# 查看功能

- 1. 登录 云安全中心控制台,在左侧导览中,单击大模型态势管理。
- 2. 在大模型态势管理页面,支持查看**大模型组件资产、大模型组件风险、网络攻击**。



3. 在**大模型资产**列表中,您可以查看已识别的组件信息、资产实例信息、识别方式等。选择您关心的数据,单击**详情**可查看具体的组件识别原因、 暴露路径、网络攻击、风险等。



资产详情						重新扫描 ×
•2•	大模型组件			首次发现时间	回 2025-03-24 11:34:25	
- ( • <b>**</b> • )	Ollama			最近发现时	a 2025-03-24 11:34:25	
资产ID	i			域么	-	
资产名称	4			tota tank		
资产类型	CVM			地现	ap-	
(D)	0.	. m.		所属账号	8	
INTERT	22.	+ M-		所属网络	vpc It-VPC	
资产标签	-					
识别方式	主机指纹					
2010/12/9768	("Co.			n(0 <sup>11</sup> )		
いてカリン2平時	1 001			ive /		
显示效众	网络市土 50					
	网络秋山 02	M PM				
						+
						🕞 1/ 🔹 🗋 👘
						21
					/ /	5
					· · · · · · · · · · · · · · · · / · · · · · · · /	😅 🖁 ) • • • •
	(A)		1 1	( 🝙 🖷	(	📻 4 — )
	•	🦳	1 5535	💌 🛯	3	61
					\	<ul> <li>完全开放</li> </ul>
						● 愛限访问
						□ 1 ● 无法访问
					· · · · · · · · · · · · · · · · · · ·	3 存在扫描风险
						○ 后端服务节点
						○ 后端服务节点 (异常)

- 4. 切换至风险标签页,您可以查看识别的大模型组件相关风险,风险包含漏洞风险、基线风险。
  - 漏洞风险:包含网络扫描和主机安全识别的大模型组件相关漏洞。

大模型组件 风险(6) 网络攻击(9424)														
大模型组件漏洞(2)①         大模型组件基线风险(4)①           标记处置         标记忽略         (仅展示POC扫描发现)									多个关键字用引	(线 17 分開,多个过滤	标签用回车键分隔	Q	0 @	ż
漏洞名称	公网IP/域名	关联实例ID/名称	资产类型 丁	端口	組件	风险等级 丁	漏洞类型 丁	CVE编号	cvss ‡	》处理状态 了	所属账号 ℃	操作		4
▶ ollama外部开放将导致算力窃取和数据资源溢	.87		-	11434		提示	其他		0	未处理	<b>⊘</b> γ .	标记处置	更多 ~	د
▶ Open WebUI 路径遍历赢洞(CVE-2024-6707)	218 37		-	7000	-	提示	路径遍历		0	- 未处理	<b>\$</b>	标记处置	更多 ~	E
共 2 项											10~条/页 H 4	1 /	1页 ▶	н

○ 切换至**基线风险**,可查看通过主机基线检测发现的风险,基线风险是指通过主机安全检测的大模型组件配置不当等风险。

大模型组件漏洞(2)① 大模型	組件基线风险(4) ①								
标记处置标记忽略							多个关键字用竖线 1° 分隔,多	个过滤标签用回车键分隔	Q <i>C</i> 🕸
风险配置项 V	检查类型 了	公网IP/域名	实例/账号ID&名称	风险等级 丁	资产/账号类型 ⑦	风险识别时间 ↓	处理状态 ① 〒	所属账号 🔽	操作
▶ MLflow未提权访问	AI墨线	3	腾讯云服务器(CVM): 实例名称:	高危	CVM	最近: 2025-03-26 15:11:50 首次: 2025-03-26 15:11:50	未处理	8	标记处置 标记忽略
▶ Ollama未授权访问	AI墓线	3	腾讯云服务器(CVM): 实例名称:	高危	CVM	最近: 2025-03-26 15:11:50 首次: 2025-03-26 15:11:50	未处理	<u>@</u>	标记处置 标记忽略
▶ MLflow未授权访问	AI基线	4	腾讯云服务器(CVM): 实例名称:	高危	CVM	最近: 2025-03-26 14:13:08 首次: 2025-03-26 14:13:08	未处理	<u>@</u>	标记处置 标记忽略
▶ Ollama未授权访问	AI墨线	4	腾讯云服务器(CVM): 实例名称:(	高危	CVM	最近: 2025-03-26 14:13:08 首次: 2025-03-26 14:13:08	未处理	<mark>⊗</mark> .	标记处置 标记忽略
共 4 项								10 ~ 条/页 🛛 🛏	< 1 /1页 ►

5. 切换至网络攻击标签页,您可以查看资产正在遭受 AI 类漏洞攻击的详情。选择目标的数据,单击详情,可以查看网络攻击的详细数据。



标记处置 标记包格	全部攻击状态 ¥	BERG	The R. W. Wardshield		请选择时间 5	(送採时间 色)	多个关键字用	· · · · · · · · · · · · · · · · · · ·	8标签用回车输分隔	0.06
i \$	公開:	80	A CERCENTIAL S	Cilana	建用位标 dick1983(chatont 解各器建造实伪造 (SSBF)	·····································	1	(2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	HTIMERY'S E	
	内周:		<b>ξ</b> φ	(H) one in	and conjunction and an and a second second				_	
	内局: -	80	হক	-	ChatGPT-Next-Web服务器路请求伪造 (SSRI	🕞 尝试攻击	1	未处理	ø	详情 更多 >
	公開: 内開:	80	1 (市	M Ollama	ChatGPT-Next-Web服务器稿请求伪造 (SSRI		1	未处理	60	详情 更多 >
\$	公网: - 内词: -	8080	īđ		ChatGPT-Next-Web服务器编请求负遣 (SSRI		1	未处理	۵	详情 更多 >
【击详情 未处	<b>上理</b>						杤	记处置	标记忽	略 ×
<b>计</b> 图4	各攻击告警				攻击状态 G 最近攻击时间 2	9 尝试攻击 025-03-24 0	5:24:45			
击次数	1次				漏洞名称 dirk1983	chatgpt 服务	器端请求任	为诰 (SSRF)	漏洞(CVE-2	024-27564)
击源IP	1 3				漏洞CVE编号 CVI	E-2024-2756	4	/ <u>//2</u> (00111)		024 27004,
<b>文</b> 击源地址	中国 江苏省 南京市				漏洞全网攻击热度 🍐 (					
务进程	nginx: n				ginx					
常行为	-									
x击数据包	GET									of-
	User								L	ustom-
影响	向主机				• ?• 大模型	资产				
<b>V</b>					ollarr	a				
资产类型	CVM				地域 广	·/•				
域名	-				所属账号	<b>3</b> j				
IP地址	公: 1	1内			所属网络					



# 日志投递(支持多账号多产品多日志)

最近更新时间: 2024-08-05 14:26:42

### 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。



日志投递				×								
投递至kafka 投递到	ĒCLS			前往消息队列控制台 2								
<ol> <li>1. 购买消息队列</li> <li>2. 根据消息队列</li> <li>3. 按照本页面中</li> </ol>	① 1.购买消息队列Ckafka实例,推荐按照需要投递的日志量来选购对应Ckafka实例规格     ×       2.根据消息队列Ckafka文档指引,开通白名单实现公网域名接入或支撑环境接入       3.按照本页面中以下指引完成日志投递配置,仅支持使用同一消息队列用户进行投递											
配置消息队列												
网络接入方式	O Ckafka公网域名接入 ○ Ckafka	a支撑环境接入 🦳 其他Kafka公网接入										
TLS加密												
消息队列所属账号 🛈	¥											
消息队列实例	请选择 🖌 🖌	S										
公网域名接入	请选择 🖌 🖌											
用户名 (j)	请输入用户名											
密码	请输入密码											
配置日志投递												
日志来源	日志类型	账号来源	Topic ID/名称 (i)	操作								
云防火墙	< ✓ 全部日志类型	✔ 全部账号 ✓	请选择Topic名称 ✔	删除								
Web应用防火墙	✓ 全部日志类型	✔ 全部账号 ✓	请选择Topic名称 V	删除								
主机安全	~ 全部日志类型	✔ 全部账号 ~	请选择Topic名称 🛛 🗸	删除								
云安全中心	▶ 全部日志类型	✔ 全部账号	请选择Topic名称 🗸 🗸	删除								
云审计	▶ 全部日志类型	✓ 全部账号	请选择Topic名称 ✔	删除								
● 新增日志投递配置												

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。

	<ul> <li>新增:单击新增日志投递配置,支持新增多个日志来源。</li> </ul>
操作	<ul> <li>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。</li> </ul>
	● 编辑:如非首次配置日志投递,则支持在日志投递页面,单击 <b>修改配置</b> ,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。

日志投递				修改配置	t 前往消	息队列控制台 🖸	×
消息队列详情							
接入方式	Ckafka公网域名接入		接入对象				
消息队列实例ID/名称			实例版本 🛈				
地域			可用区				
所属网络ID/名称			所在子网ID/名称				
峰值带宽			磁盘容量				
状态			用户名				
日志投递详情							
全部开启	全部关闭 查看监控						φ
日志来源	日志类型	账号来源	TopicId/名称 (j	投递状态	投递开关	操作	
云防火墙	访问控制日志、零信任防护日志			正常		编辑 查看监持	空 一
Web应用防火墙	攻击日志、访问日志			正常		编辑 查看监持	호
主机安全	入侵检测日志、客户端相关日志			正常		编辑 查看监持	Ŷ

### Ckafka 支撑环境接入

腾讯云

- 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。



日志投递								×
投递至kafka 投	递至CLS						i	前往消息队列控制台口
<ol> <li>1. 购买消息</li> <li>2. 根据消息</li> <li>3. 按照本页</li> </ol>	即从列Ckafka实例 即入列Ckafka文林 页面中以下指引身	列,推荐按照需要投递的日志 当指引,开通白名单实现公网 气成日志投递配置,仅支持使	:量来选购)  域名接入!  用同一消!!	对应Ckafka实例规格 或支撑环境接入 息队列用户进行投递				×
配置消息队列								
网络接入方式	Ckafe	ka公网域名接入 🛛 🔵 Ckafk	a支撑环境	接入 🦳 其他Kafka	公网接入			
TLS加密								
消息队列所属账号 🤇		Ŷ						
消息队列实例	请选择	~	S					
支撑环境接入	请选择	~						
配置日志投递								
日志来源		日志类型		账号来源		Topic ID/名称()		操作
云防火墙	~	全部日志类型	~	全部账号	~	请选择Topic名称	~	删除
Web应用防火墙	~	全部日志类型	~	全部账号	~	请选择Topic名称	~	删除
主机安全	~	全部日志类型	~	全部账号	~	请选择Topic名称	~	删除
云安全中心	~	全部日志类型	~	全部账号	~	请选择Topic名称	~	删除
云审计	~	全部日志类型	~	全部账号	~	请选择Topic名称	~	删除
€ 新增日志投递配置								
参数名称		说明						
网络接入方式	<u>-</u> U	Ckafka 支撑环场	镜接入。					

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	<ul> <li>新增:单击新增日志投递配置,支持新增多个日志来源。</li> <li>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。</li> <li>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。</li> </ul>



- 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。

日志投递					修改配置	前往消息	息队列控制台 🖸	×
消息队列详情								
接入方式	Ckafka支撑环境接入		接入对象					
消息队列实例ID/名称			实例版本 🛈					
地域			可用区					
所属网络ID/名称			所在子网ID/名称					
峰值带宽			磁盘容量					
状态	•健康		用户名					
日志投递详情								
全部开启	全部关闭 查看监控							Φ
日志来源	日志类型	账号来源	Topiclo	山名称	投递状态	投递开关	操作	
云防火墙	访问控制日志、零信任防护日志				正常		编辑查看监	控
主机安全	入侵检测日志、客户端相关日志				正常		编辑 查看监	腔

## 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。



日志投递				×
投递至kafka 投递至Cl	LS			前往消息队列控制台 🛛
<ol> <li>1. 购买消息队列Ck</li> <li>2. 根据消息队列Ck</li> <li>3. 按照本页面中以</li> </ol>	afka实例,推荐按照需要投递的日志量来选购加 afka文档指引,开通白名单实现公网域名接入函 下指引完成日志投递配置,仅支持使用同一消息	寸应Ckafka实例规格 成支撑环境接入 即队列用户进行投递		×
配置消息队列				
网络接入方式	Ckafka公网域名接入 Ckafka支撑环境	接入 🛛 其他Kafka公网接入		
TLS加密 (				
公网接入	请输入			
用户名 (j)	请输入用户名			
密码	请输入密码			
配置日志投递				
日志来源	日志类型	账号来源	Topic名称()	操作
云防火墙	✓ 全部日志类型 ✓	全部账号 >	请输入Topic名称	删除
Web应用防火墙	✓ 全部日志类型 ✓	全部账号 >	请输入Topic名称	删除
主机安全	▶ 全部日志类型 ▶	全部账号 >	请输入Topic名称	删除
云安全中心	◇ 全部日志类型 ◇	全部账号 >	请输入Topic名称	删除
云审计	✓ 全部日志类型 ✓	全部账号 >	请输入Topic名称	删除
● 新增日志投递配置				
参数名称	说明			

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	<ul> <li>新增:单击<b>新增日志投递配置</b>,支持新增多个日志来源。</li> <li>删除:单击目标日志操作列的<b>删除</b>,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。</li> <li>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。</li> </ul>

- 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						修改配置	前往消息	息队列控制台 🖸	×
消息队列详情									
接入方式 其他Kafka2	公网接入		接入对象						
状态 • 健康			用户名		test				
日志投递详情									
全部开启 <b>全部关闭</b>									Φ
日志来源	日志类型	账号来源		Topic名称 (j)		投递状态	投递开关	操作	
云防火墙	入侵防御日志、流量日志、操作					正常		编辑	

# 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。
- 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。

日志投递	×
投递至kafka <b>投递至CLS</b>	前往日志服务控制台 🖸
<ul> <li>         投递至CLS(日志服务) ● 已开通         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服务中创建后付费的存储空间,同时也会生成后付费账单。CLS计费详情 <sup>2</sup> </li> <li> <b>介通日志服务</b>          )         2         配置日志投递      </li> </ul>	CLS后,将为您自动
<ul> <li>说明:</li> <li>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 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;</li> </ul>	JCLS服务和开启日志 十费详情 。

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)。



日志投递		
投递至kafka	投递至CLS	前往日志服务控制
(1) 运行		
	T后口心汉速到CL3后,特为芯白幼在CL3服务中创建后的贫助仔储工间,问时也去主成后的贫效单。	
投递账号		
投递所属账号	请选择账号    ▼	
投递内容		
日志来源	请选择日志来源    ▼	
日志类型	请选择日志类型     ▼	
日志来源账号	请选择	
投递目标 🛈		
目标地域	请选择目标地域    ▼	
日志集操作	● 选择已有日志集   ◯ 创建日志集	
日志集	请输入日志集名称	
日志主题操作	选择已有日志主题 🔷 创建日志主题	
日志主题	·请给 \ 日末 + 聊 < 称	
确定	取消	
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、Sa 蜜罐的日志。	aS 化堡垒机、云审计、际
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。

日志投递		×
投递至kafka <b>投递至CLS</b>	前往日志服务	控制台 🖸
<b>投递账号信息</b> 账号名称/ID 所属部门		
日志投递详情       新增投递     批量开启     批量关闭     日志检索     删除     刷新		
✓ 日志来源 日志类型 来源账号 日志主题 ③	投递状态 投递开关 操作	
✓ Web应用防 多个 (2) 多个 (15)	• 正常            编辑 更多	•
共1项	10 ▼ 条 / 页	• •

# 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**。

日志分析					多账号管理	I等4个账号 ▼
日志概况						
接入日志源	日志投递	已使用日志容量		<b>日志趋势</b> 近7天 >	<b>-</b> 读取(次数)	— 写入(MB)
一个 配置日志接入	U ↑ 日志投递	GB /	前往扩容			
		■ 主机安全 ■ 云防火塘 ■ 云审计 ■ 云安全中心	> ■ 其他	07-14 07-1	6 07-18	07-20

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 <b>管理员</b> 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 <b>其他账</b> 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)日志,即配置当前账号 多产品日志投递。	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 支撑环境接入两种网络接入方 式下将自动获取 <b>当前账号(管理员/委派管理</b> 员)的 Ckafka,可选所需腾讯云消息队 列。	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 已配置的日志来源、日志类型、投递状态等 日志投递详情。

#### 单账号管理

腾讯云

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
	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。
云防火墙	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。
	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。
主机安全	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。



# 多云多账号管理

多云接入

最近更新时间: 2025-08-15 17:12:22

# 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(目前支持阿里云、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**。

多云多账号管理			
集团账号概况			
深いた時	化过量机系统	有限公司	
管理员账号名称	管理员账号ID	多云、混合云账号接入 ❷ 5  0 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 阿里云账号、 Azure 账号 或 AWS 账号,并配置相关参数,单击确定。



择账号类型	🖸 阿里云账号 🔢 Azure账号 🤤 AWS账号 🔗 腾讯云子账号	
	➢ 腾讯云账号,前往集团账号配置 □	
建子账号的方式	<b>手动配置</b> 5分钟完成,但权限配置较为复杂,需要配置创建好的子账号AK,更加灵活的控制权限范围	
	收起配置指引 🔨	
	< 第1/4步 > 请登录阿里云控制台后前往RAM访问控制-创建用户 I <sup>2</sup> ,选择"使用永久 AccessKey 访问"。	
	ter 2 2000	
	BP         Mm         C         MMM         MMM           APM         + RAD*         -          <	
	607         A         00 MARKETS have DMs           607         00 MARKETS have DMs         00 MARKETS have DMs           607         00 MARKETS have DMs         00 MARKETS have DMs           607         00 MARKETS have DMs         00 MARKETS have DMs           607         00 MARKETS have DMs         00 MARKETS have DMs           607         00 MARKETS have DMs         00 MARKETS have DMs           607         00 MARKETS have DMs         00 MARKETS have DMs	
	KR# ∧ ID     TH     KR#     KR#	
	Andread and and a second and a se	
	• • •	
账号SecretID	请输入	
账무CoorotKov	清給 λ	

# 阿里云账号

1. 登录阿里云控制台后,前往 RAM 访问控制-创建权限策略,选择**脚本编辑**。

RAM 访问控制		RAM 访问控制 / 权限策略 / 创建权限策略	关于权限策略
概览		← 创建权限策略	
设置		可視化编辑 脚本编辑 司 导入策略 优化策略	Action 与 NotAction 需要更多输入 策略文档长度 63 / 6144 个字符
身份管理	~		
权限管理 授权	^	1 { 2 "Version": "1", 3 "Statement": [ 4 ]	, in the second se
权限策略		5 "Effect": "Allow", 6 "Action": [].	
权限诊断		7 "Resource": [], 8 "Condition": {}	
集成管理	^	9	
SSO 管理		10 ] 11 }	
OAuth 应用(公测	)		
多账号身份权限(:	云 sso)		

2. 在策略脚本编辑框中,填写下方内容,可访问 文档 了解所需权限的具体原因及参考的系统策略。





	"*:BatchQuery*",
	"hbr:CheckRole",
	"resourcecenter:ExecuteSQLQuery",
	"resourcecenter:ExecuteMultiAccountSQLQuery",
	"ecs:ModifySecurityGroupPolicy",
	"ecs:RevokeSecurityGroupEgress",



3. 单击确定,填写策略名称后,再单击确定。推荐命名为"腾讯云CSIP策略",便于理解使用场景。



	9 10	"Re "E1	esource": "*", fect": "Deny"				
	11 12	}, {		创建权限策略	ł		×
	13 14 15	"Ac	<pre>:tion": [     "*:Describe     "*:List*",</pre>	* 策略名称			
	<ul><li></li></ul>		"*:Get*" "*:Read*"	腾讯云CSIP等			•
	18       19       20       21       22		"*:BatchGet "*:BatchDes "*:Ouerv*".	<sup>東昭石</sup> が主 3 円 备注	10月 120 千子位,又拉夹文、	奴子、庄子何 - 。	
			"*:BatchQué "actiontrai 各注至多可设计		1024 个字符。		
	23 24 25		"dm:Desc*", "dm:SenderS			确定	取消
	26 27 28		"ram:Genera "cloudsso:C "notification	ns:Read*",			
	❸ 错误 0	安全警告 0	● 警告 0	♥ 建议 8			
	Statement	t 2, Action 1	Wildcard in	service name	避免在服务名称中使用通配符	(*, ?),这将会无意中授	予其他具有类似名称的服
	Statement	t 2, Action 2	Wildcard in	service name	避免在服务名称中使用通配符	(*, ?),这将会无意中授	予其他具有类似名称的服
	Statement	t 2, Action 3	Wildcard in	service name	避免在服务名称中使用通配符	(*, ?),这将会无意中授	予其他具有类似名称的服
	确定	返回					

4. 登录阿里云控制台后前往 RAM 访问控制-创建用户 ,选择使用永久 AccessKey 访问,推荐使用 tencent\_csip 作为名称,便于理解账号用 途。

RAM 访问控制		RAM 访问控制 / 用户 / 创建用户		
概览		← 创建用户		
设置		用户账号信息		
身份管理	^	* 登录名称 ⑦ 显示者	名称 ②	标签
用户		tencent_csip	讯云云安全中心	未绑定标签 🖉
用户组		+ 添加用户		
角色		访问方式 ②		
权限管理 授权	^	● 优先考虑使用 STS Token 进行访问 访问密钥(AccessKey)是一种长期有效的程序访问凭证。AccessKey 泄露会威/	\$胁该账号下所有资源的安全。建议优先采用 STS Token 临时凭	证方案,降低凭证泄露的风险。 查看方案详情
权限策略		□ 控制台访问 用户使用账号密码访问云控制台		
权限诊断		✔ 使用永久 AccessKey 访问 创建 AccessKey ID 和 AccessKey Secret,支持通过	± API 或其他开发工具访问	
集成管理	^	《 确定 返回		
SSO 管理				
OAuth 应用(公测)				

5. 复制或下载 AccessKey ID 和 AccessKey Secret。

← 创建用户										
● 若开通 O	- 若开通 OpenAPI 调用访问,请及时保存 AccessKey 信息,页面关闭后将无法再次获取信息。									
用户信息 下载 CSV 文	件									
	□登录名称	状态	启用控制 台登录	登录密码	AccessKey ID	AccessKey Secret	操作			
ten	icent_csi .coi	创建用户: 🗸 成功 m 开启 OpenAPI 调用访问: 🗸 成功	否	无	□ 复制	□ 复制	□ 复制			
[] 添加	加到用户组 添加权限									

6. 勾选账号,单击**添加权限**。



# ← 创建用户

用户信息									
下载(	CSV 文件								
	用户登录名称			状态	启用控制 台登录	登录密码	AccessKey ID	AccessKey Secret	操作
	tencent_csir		.com	创建用户: 🗸 成功 开启 OpenAPI 调用访问: 🖌 成功	否	无	□ <b>复制</b>	凸 <b>复制</b>	♂ <b>复制</b>
	添加到用户组	添加权限							

7. 搜索前面步骤创建的策略"腾讯云CSIP策略",勾选并单击确认新增授权。

新增授权					
<ul> <li>✓ 资源范围</li> <li>● 账号级别</li> <li>● 资源组级别 ⑦</li> <li>✓ 授权主体</li> <li>已选择授权主体</li> </ul>					
tencent_csip@	.com				
▼ 权限策略 腾讯云CSIP	Q 所有策略类型	~	٥	已选择权限策略	>>>
✓ 策略名称	策略类型	描述		<b>自定义策略 (1)</b> 腾讯云CSIP策略	×
Mit	自定义策略				
每页	显示 10 🗸	く 上一页   1/1	下一页 >		
确认新增授权取消					

8. 在 多云多账号管理 的配置页面,将 AccessKey ID和AccessKey Secret 填写至子账号 SecretID、子账号 SecretKey,并注明账号名称,单击确定。



配置多云、云外、	混合云账号	×
创建子账号的方式	手动配置 5分钟完成,但权限配置较为复杂,需要配置创建好的子账号AK,更加灵活的控制权限范围 收起配置指引 ▲ 在文档中查看 □	
	Class     A real     M real     M real     M real     M real       and mark     A real     A real     A real     A real       and mark     A real     A real     A real       and mark     A real     A real     A real       and mark     A real     A real     A real	
	Al     Def Composition       RET     Def Composition       RET	
	0 0 0	
子账号SecretID	请输入	
子账号SecretKey	请输入	
	为确保账号可用,请按推荐策略为子账号配置权限 <b>文档链接 <sup>12</sup></b> ,如账号有效期内发生SecretKey变更,请及时在云 安全中心修改对应账号配置	<u>-</u>
主账号名称	请填写该阿里云账号的名称,方便您区分账号	
配置子账号权限	前往阿里云控制台配置 [2]	
所属部门(选填)		
	MI\$P\$\$P\$175757575759999111111111111111111111111	

# 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)。

	,○ 搜索资源、服务和文档(G+/)	e 🖓 🕸 🖓 🦉 🖉
±页 > <b>应用注册</b>		×
+ 新注册 ⊕ 终结点 ∥ 税増新苦 () 刷新 土 下載 (15) 税工功能   № 例知反馈?		
● 目 2020年6月30日起,我们将不再向 Azure Active Directory 身份检证库(ADAL)和 Azure Active Directory Graph 混乱的	何刻功能。我们消磁機證與技术支持相安全更新相序,但将不再通供功能更新,因用相序将需要升级到 Microsoft 身份做过靠(MSAL)和 Microsoft Graph, <u>了其更多信息</u>	×
所有应用程序 調查的应用程序 已删除的应用程序 个人地户中的应用程序		
户 开始键入显示名称或应用程序(客户编) ID 以神选这些结果     ★    ★    ★    ★    ★    ★    ★		
	此成产未外为这个自录中任何应用程序的特式者。 至于且各学校系统和网络 重要个人类产并实际有应用程序	

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。

☰ Microsoft Azure ③ 升级
主页 > 应用注册 >
注册应用程序
* 名称
此应用程序面向用户的显示名称(稍后可更改)。
受支持的帐户类型
谁能使用此应用程序或访问此 API?
<ul> <li>● 仅此组织目录(仅 默认目录 - 单一租户)中的帐户</li> </ul>
○ 任何组织目录(任何 Microsoft Entra ID 租户 - 多租户)中的帐户 ○ 任何组织目录(任何 Microsoft Entra ID 租户 - 多租户)中的帐户和会人 Microsoft 帐户/倒彻 Slance - Xhou)
○ 仅 Microsoft 个人帐户
帮我选择 重定向 URI (可选)
在成功验证用户身份后,我们将把身份验证响应返回到此 URI。现在可视需要提供此 URI,且稍后可更改,但大多数身份验证方案都要求提 供值。
选择平台 🗸 例如, https://example.com/auth
在此处注册你要使用的应用。通过从企业应用程序中添加,可以从组织外部集成库应用和其他应用。 如果继续,表明你同意 Microsoft 平台策略 🗗

## 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**。

		戶 搜索资源、服务和文档(G+/)			a 🖉 © R 🚺 🧶
主页 > 订阅 > <b>订阅</b> ター・・ <sup>取以目录</sup>					×
*** 道加 全局管理员可以通过在此处更新其集略设置未管理此列表中的所有订阅。 /> 限素任何字段	状态 — 全部				
订刷名称 ウム ゴロロ ウム Acure subscription 1	<b>我的角色</b> ↑↓ 所有者	当前成本	安全功能分数 ↑↓ -	父養理組 ♀↓	秋郎 ↑↓ ● 可用

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。



			d 🖉 🐵 🖉 🖉 🥌
主页 > 1788 > 1788 > Azure subscription 1   访问控制(HSRRIG)(的管理) > 添加角色分配 …			×
R.B.         S.F.         WERCHE           ROSILERADING         TOURRADING         TOUR         TOUR <td>348-7</td> <td></td> <td></td>	348-7		
一 投角色名、说明、权限或 ID 投索	<b>奥别:金部</b>		
名称「→	後期 14	黄型 ℃→ 黄服	/ 1 详细信息
读者	靈着所有资源,但不允许进行任何更改。	BuiltinRole 常知	1 4283
安全读取者	安全波取者角色	BuiltinRole 😤	.性 税图
安全管理器(日)	这是旧角色,请政用安全管理员角色	BuiltinRole 👳	.性 税图
安全管理员	安全管理员用色	BuiltinHole 323	15 8.8
安全评估参与者		BuiltinKcie 323	.15 8.8
安全引爆室读者	已允许查询来自安全引爆室的提交信息和文件	BuiltinRole 👳	推 税图
安全引爆至发布者	允许若平台、工作常和工具集发布到安全引爆至并进行修改	BuiltinHole 923	.112
安全引爆室提交内容管理者	允许创建向安全引爆室提交的内容并进行管理	BuiltinRole 安当	.性 親問
备份参与者	允许你管理备份服务,但是不能创建保管库以及授予其他人访问权限	BuiltinRole 存指	(一一一根因
备份操作员	允许你管理备份服务,但删除备份、创建保管库以及授予其他人访问权限除外	BuiltinRole 存指	( 税出
备份读者	可以查看备份服务,但是不能进行更改	BuiltinRole 存缩	( 税因
标记参与者	允许用户管理实体上的标记,而无需提供对实体本身的访问权限。	BuiltinRole 管理	(和治理 視出
测试基读者	允许查看和下载但和游试结果。	BuiltinRole 无	視問
策略见解数据编写器(预克级)	允许对抗源策略进行读取访问,并允许对资源组件策略事件进行写入访问。	BuiltinRole 预3	i #889
层次结构设置管理员	允许用户编辑和删除层次结构设置	BuiltinRole 管罚	(和治理 視問
成本管理参与者	可以重看成本并管理成本配置(例如) 预算、导出)	BuiltinRole 警罚	(和治理 視問
成本管理读取器	可以查看成本数据和配置(例如,预算、号出)	BuiltinRole 管利	1和治理 視問
磁盘备份读取者	向备份保管库提供执行磁盘备份的权限。	BuiltinRole II th	3 税間
磁盘池操作者	由 StoragePool 资源提供程序用于管理源加到磁盘地的磁盘。	BuiltinRole 无	视图
磁盘还原操作员	向备份保管库提供执行磁盘还原的权限。	BuiltinRole 其他	3 税田
磁盘快聚参与者	向备份保管库提供管理磁盘快照的权限。	BuiltinRole 其他	3 税間
存储 Blob 代理	允许生成可用于为 SAS 令牌签名的用户委托密钥	BuiltinRole 存在	」 ・ 戦 戦
存储 Blob 数据参与者	授予对 Azure 存储 blob 容器和数据的读取、写入和删除权限	BuiltinRole 存在	」 ・ 親題
存储 Blob 数据读取器	授予对 Azure 存储 blob 容器和数据的读取权限	BuiltinRole 存住	」 ・ 親題
存储 Blob 数据所有者	允许对 Azure 存储 blob 容器和数据有完全访问权限。包括分配 POSIX 访问控制。	BuiltinRole 存在	1 税間
存储表数据参与者	允许对 Azure 存储表和实体的读取、写入积删除访问	BuiltinRole 存在	1 税田
存储表数据读者	允许对 Azure 存储表和实体进行读取访问	BuiltinRole 存在	1 税因
存储队列数据参与者	授予对 Azure 存储队列和队列消息的读取、写入和删除权限	BuiltinRole 存缩	4
存储队列数据读取器	授予对 Azure 存储队列和队列消息的读取权限	BuiltinRole 存在	よ 税間
存储队列数据消息处理器	允许授予对 Azure 存储队列消息的速宽、接收和删除权限	BuiltinRole 存在	4 税間
244以初時增速県分送線 	在海塘港 Annes 岩積與制治費	BuiltinRole 2x4	2 20 MI
审阅和分配 上一步 <b>下一步</b>			☆ 反馈

- 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**。

	● ① 升級			▶ 搜索
主页 > 订阅 > 订阅 >	Azure subscription 1   访问控制(标识和访问管理) >			
添加角色分配				
角色 成员 条件	审阅和分配			
角色	读者			
范围				
成员	名称	对象 ID	类型	
	100.000	CONTRACTOR OF A DECEMBER	应用	
说明	无说明			
审阅和分配	上一步			

# 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"。


	♀ 搜索资源、服务和文档(G+f)		
主页 > 应用注册 >			
🔣 csip 💉 🗉			×
0.00	S NA & Gar S S North		
- 50.5K	B BINA UP SCHONE BEN TREE-UNE		
R 40.22	🚺 有时间码? 我们希望收到你对 Microsoft 标识平台(以前为面向开发人员的 Azure ADI的反馈。 →		
■ (KE/(1))	. 478		
A HOWAGT	へ 開発 目前交換 : Alin	安户道任道 1	征服 含類部
112 1	应用程序信户询 ID: 1	重定向 URI : 蓋	<u>Non-Conte</u> Stom定向 URI
■ 品牌打造机属性	対象 ID :	应用程序 ID URI : 🧟	5加应用程序 ID URI
340/8212	目录電介 Ю : 2	本地目录中的托管应用 : 😭	sia.
1 12-194U0399	要支持的帐户类型 : 仅数的组织		
ADI 1778	● 自 2020年 6 月 30 日起。我们将不再向 Azure Active Directory 身份验证库(ADAL)和 Azure Active Directory Graph 添加任何能功能。我们得继续提供技术支持和安全更新程序,但将不再进行	供功能更新。应用程序将需要升级到 Microsoft 身份验	全证用(MSAL)和 Microsoft Graph, 了解更多信息 ×
<ul> <li>От арі</li> </ul>			
1 应用角色	入口 文档		
🎎 所有者			
為 角色和管理员	生成便用 Mic	rosoft 标识平台的应用程序	予
■ 清单	Microsoft 标识平台是身份验证服务、开放源代码库和应用程序管理工具。你不仅可1	以创建基于标准的新式身份验证解决方案、访问和	0保护 API,还能为用户和客户添加登录名。 了解更多信息 (3)
支持和疑难解答			
⊘ 疑地解答			
🤰 新建支持请求	🚽 🔍 🔊 🔊 👘	O D	4 🔊 •
	× 🔹 🔹 🔂	► <b>1</b>	
	调用 API 在 5 分钟内:	执行用户登录	为组织配置
	生成功能更强大的应用程序,内含 Microsoft 服务提 使用我们的 S	DK,只需执行几个步骤,即可让用户 20. 清使思维速)口来总改 Web 应	在"企业应用程序"中分配用户和组、应用条件访问策
	供的丰富用户和业务数据以及你自己公司的数据源。    用、移动应用	I、SPA或守护程序应用。	略、配置单一型录等。
	室着 API 权限 查看所有达	快速入门指南	<u>转到,而而而同时起。</u>

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。

	,○ 搜索资源、服务和文档(G+/)	E 🗘	) 🕸 🚱 🖉	
主页 > 应用注册 > test		添加客户端密码 ③		×
	на н			
•		说明	test	
	☆ 得到反馈?	截止期限	730 天(24 个月)	$\sim$
₩ 概述				
📣 快速入门	值即咒惩,咒惩应用程序可以在 Web 可寻亚位置(使用 HTIPS 万案)接收令牌时间身份验证服务标识自己。为了提高保障水平,建议使用证书(而不是	₿		
💉 集成助手				
管理	可以在下面的选项卡中找到应用程序注册证书、密钥和联合凭据。			
🔜 品牌打造和属性				
Э 身份验证	业书(0) 著戶躊躇醫(4)(0) 联合凭据(0)			
📍 证书和密码 🚺	应用程序在请求获取令牌时用来证明自己标识的机密字符串。亦称为"应用程序密码"。			
● 令牌配置	十 新客户端密码 ②			
→ API 权限				
💁 公开 API				
12 应用角色	ロットノットシュアリオキノアとのオキレージェア、制造りです。			
🎎 所有者				
4 角色和管理员				
100 清里				
支持和疑难解答				
⊘ 疑难解答				
🧟 新建支持请求				
		4		
		添加取消		

3. 在证书和密钥页面,获取**客户端密钥**。



		▶ 搜索资源、制	服务和文档(G+/)		
主页 > test					
<pre>     test   证书和密码</pre>	•				
	৵ 得到反馈?				
職 概述					
📣 快速入门	借助凭据,凭据应用程序可以在 Web 可寻址位置(使用	目 HTTPS 方案)接收令	令牌时向身份验证服务标	识自己。为了提高保障水平,建议使用证书(而不是	是客户端密码)作为凭据。
💉 集成助手					
管理	可以在下面的选项卡中找到应用程序注册证书、密	钥和联合凭据。			×
💳 品牌打造和属性					
Э 身份验证	证书(0) 客户端密码(1) 联合凭据(0)				
📍 证书和密码	应用程序在请求获取令牌时用来证明自己标识的机密	§字符串。亦称为"应)	用程序密码"。		
令牌配置	→ 新客户端密码				
→ API 权限		裁 i L 期限	值①	机密ID	
🔷 公开 API	toot 2	2026/4/24			r 💼
🐱 应用角色	1051 2	2020/4/24			

# 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"。



agement (IAM)	管理当削殓过身份撤证的 IAM 用户的凭证。 要了解有天 业与遗云科技:	光址关型及具使用力法的更多信息,请参阅"业与虚云科技"常规参考"中的」	·
御史ににに (IAM) 変素 IAM	▲ 您没有分配 MFA 作为安全最佳实践,我们建议您分配 MFA。		分配 MFA
145	账户详细信息		更新电子邮件地址
理	用户名	用户 ARN	
		đ	
	亚马逊云科技 账户 ID	亚马逊云科技 电子邮件地址	
供商	规范用户 ID		
(1)			
告	Amazon IAM 凭证 Amazon CodeCommit 凭证 Amazo	on Keyspaces 凭证	
当规则 千器	控制台登录		更新控制台密码
告			
	控制台登录链接	控制台密码	
	B	目に 小照月校創ム	
	多重身份验证 <b>(MFA)</b> (0)		删除 重新同步 分配 MFA 设备
	使用 MFA 提高您的 亚马逊云科技 环境的安全性。使用 MFA 登录需要来自 MFA	A 设备的身份验证码。每位用户最多可分配 1 台 MFA 设备。 <u>了解更多 🎦</u>	
	设备类型	标识符	创建于
		没有 MFA 设备。分配 MFA 设备以提高 亚马逊云科技 环境的安全	性
		分配 MFA 设备	
	访问密钥(0)		
	19世が同志的AILでもないない。 創建访问密钥	波云科交 软件开及上具已以确性力式调咐 亚句波云科文,或者直按定门 亚句波云科文 AF	NUH4。NG — KU 129 · U 20 · U
	没有访问器	密钥。最佳实践是避免使用长期凭证,例如访问密钥。请使用提供短期凭证的	工具代替。 了解更多 🖸
		创建访问密钥	
	X.509 签名证书 (0) 使用 X.509 证书向某些 亚马逊云科技 服务发出安全的 SOAP 协议请求。一次量	1多可以有两个 X.509 证书(话跃或非话跃)。 <u>了<b>能更多 [</b>]</u>	操作 ▼ <b>上载</b> 创建 X.509 证书
	创建时间	指纹	状态

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"。

포马逊국科	NWCD operating Ningxia Region     Sinnet operating Beijing Region     Services		Ş	0	Global 🔻	
≡ ⊘	D创建访问密钥 这是唯一一次可以查看或下载秘密访问密钥的标	1.会。您以后将无法恢复它。但是,您可以随时创建新的访问密钥。				
	IAM > 安全凭证 > 创建访问密钥					
	步骤 1 访问密钥最佳实践和替代方案	检索访问密钥 📖				
	<b>步骤 2 - <i>可</i>进</b> 设置描述标签	<b>访问密钥</b> 如果您丢失或遗忘了秘密访问密钥,将无法找回它。您只能创建一个新的访问密钥并使旧密钥处于非活跃状态。				
	步骤 3	访问密钥 秘密访问密钥				
	122.5% MJ (*) 125 123					
		访问密钥的最佳实践				
		<ul> <li>切勿以纯文本、代码存储库或代码形式存储访问密钥。</li> <li>不再需要时请禁用或删除访问密钥。</li> <li>启用最低权限。</li> <li>定期轮换访问密钥。</li> <li>定期轮换访问密钥。</li> <li>有关管理访问密钥的更多详细信息,请参阅管理 亚马逊云科技 访问密钥的最佳实践。</li> </ul>				
		下載 .csv 文件 日完成				



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"。

名 逊云科技 账户 ID 用户 ID zon IAM 凭证 Amazon Keyspaces 凭证	用户 ARN 口 亚马逊云科技 电子邮件地址 口
逊云科技 账户 ID 司户 ID zon IAM 凭证 Amazon CodeCommit 凭证 Amazon Keyspaces 凭证	亚马逊云科技 电子邮件地址
평가 ID zon IAM 凭证 Amazon CodeCommit 凭证 Amazon Keyspaces 凭证	
zon IAM 凭证 Amazon CodeCommit 凭证 Amazon Keyspaces 凭证	
zon IAM 凭证 Amazon CodeCommit 凭证 Amazon Keyspaces 凭证	
台登录	更新控制台密码
台登录链接	控制台密码
	最后一次登录控制台
[身份验证(MFA)(0) #A 提高您約 亚马逊云科技 环境的安全性、使用 MFA 登录需要来自 MFA 设备的身份验证码。每	
设备类型标识符	创建于
没有 MFA 设备。分配 M	MFA 设备以提高 亚马逊云科技 环境的安全性 分配 MFA 设备
密钥 (1)  问密钥从 返马逊云科技 CLI、亚马逊云科技 Tools for PowerShell、亚马逊云科技 软件开发工具   2   建访问密钥	1包以编程方式调用 亚马逊云科技,或者直接进行 亚马逊云科技 API 调用。您一次最多可擁有两个访问密钥(活跃或非活跃)。 了
N#	操作 ▼
ist:	Active
一次使用 ;	已创建 现在
次使用的区域 <b>(A</b>	上次使用的服务 N/A

#### 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。

亚马激云科技 NWCD operating Ningxia Region Sinnet operating Beijing Region	Ser	vices					∲ () Global ▼
Identity and Access	×	IAM > 用户					
Q 搜索 IAM		<b>用户 (1) 信息</b> IAM 用户是具有长期凭证的身份, Q、 搜索	用于与账户中的 亚马逊云科技 进行交	互。		]	C 删除 创建用产 < 1 > ③
控制面板		日用户名	▲ 路径	▼ 组	▽ 上次活动	▽ MFA ▽ 密码期限	▽ 控制台上次登录 ▽ 访问密钥
▼ 访问管理 用户组 <b>用户</b>					-		

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"。



itity and Access ×	IAM 〉 用户 〉			
	信息			删除
搜索 IAM	摘要			
面板	ARN	控制台访问	访问密钥 1	
理	B	▲ 在沒有 MFA 的情况 下启用	创建访问公钥	
	已创建	最后一次登录控制台 ③ 从不		
是供商	权限 组 标签 安全凭证			
置 	位則ム発言			ממי דינט אלא וליון לא 5- איז איז מט
告	控制百宣求			管理控制台访问权限
当规则	控制台登录链接	控制	台密码	
折器	ð			
战告 		載后 ① 人	一次登录控制台 从不	
	多重身份验证(MFA)(0) 使用 MFA 提高您的 亚马逊云科技 环境的安全性。使用 MFA 登	录需要来自 MFA 设备的身份验证码。每位用户量多可分配 1 台 MFA 设备。」	<b>ブ解要を【】</b>	全日
	设备类型	标识符	创建于	
		没有 MFA 设备。分配 MFA 设备以提高:	亚马逊云科技 环境的安全性	
		分配 MFA 设行	2 H	
	访问密钥(0) 使用访问密钥从亚马逊云科技 CLI、亚马逊云科技 Tools for Po 创建访问密钥	werShell、亚马逊云科技 软件开发工具包以编程方式调用 亚马逊云科技,或	诸直接进行 亚马逊云科技 API 调用。您一次量多可拥有两个访问密钥(记	跃成非活跃). 了 <b>解更多 [2]</b>
		没有访问密钥。最佳实践是避免使用长期凭证,例如访问密钥	]。请使用提供短期凭证的工具代替。 <b>了解更多 🖸</b>	
			-	

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"。

포马汝군	科技 NWCD operating Ningxia Region Services Sinnet operating Beijing Region		¢	0	Global 🔻	
٦	已创建访问密钥 这是唯一一次可以查看或下载秘密访问密钥的	机会。您以后将无法恢复它。但是,您可以随时创建新的访问密钥。				
	IAM > 用户 > ) 创建访问密钥					
	步骤1 访问密钥最佳实践和替代方案	检索访问密钥 📖				
	步骤 2 - <i>可迭</i> 设置描述标签	<b>访问密钥</b> 如果您丢失或遗忘了秘密访问密钥,将无法找回它,您只能创建一个新的访问密钥并使旧密钥处于非活跃状态。				
	步骤 3 14年1十四四日	访问密钥 秘密访问密钥				
	恒系访问查册					
		访问密钥的最佳实践				
		<ul> <li>切勿以纯文本、代码存储库或代码形式存储访问密钥。</li> <li>不再需要时请禁用或删除访问密钥。</li> <li>启用最低权限。</li> <li>定期轮换访问密钥。</li> <li>定期轮换访问密钥。</li> <li>有关管理访问密钥的更多详细信息,请参阅管理 亚马逊云科技 访问密钥的最佳实践。</li> </ul>				
		下载 .csv	文件 已完成			

## 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。



亚马逊云科技 NWCD operating Ningxia Region Sinnet operating Beijing Region ### 1	Services		
Identity and Access $ imes$ Management (IAM)	IAM > 角色		
Q 搜索IAM	<b>角色 (2) 信息</b> IAM 角色是愈可以创建的身份,该身份具有特定权限,凭证在短期内有效。 Q. 提 <i>索</i>	角色可以由您信任的实体承担。	ご     制除     創建角色       く     1     >     ③
控制面板		▲ 可信实体	
▼ 访问管理	AWSServiceRoleForSupport	亚马逊云科技 服务: support (周	服务相关角色)
用户组	AWSServiceRoleForTrustedAdvisor	亚马逊云科技 服务: trustedad	visor(服务相关角色)
<b>角色</b> 策略 身份提供商	Roles Anywhere 信息 验证您的非 亚马逊云科技工作负载并安全地提供对 亚马逊云科技 服务的访	问权限。	管理
账户设置 ★ 访问报告 访问分析器 存档规则 分析器 凭证报告	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	② X.509 标准 使用您自己现有的 PKI 基础设施来验证身份。	<ul> <li>         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>

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。

are product	
选择可信实体	选择可信头体 🛤
步骤 2 添加权限	可信实体类型
步骤 3 命名、查看和创建	○ 亚马逊云科技 服务 允许 EC2、Lambda 或其他 亚马逊云科 技 账户 按 服务在此账户中执行操作。
	<ul> <li>○ SAML 2.0 联合 が洋小公司目录通过 SAML 2.0 联合的 用户在此账户中执行操作。</li> <li>○ 自定义信任策略 创建目至义信任策略 が膨中中执行操作。</li> </ul>
	<ul> <li>○ 另一个 亚马逊云科技 账户</li> <li>账户 ID</li> <li>可使用此角色的账户的标识符</li> </ul>
	● 另一个 亚马逊云科技 账户 账户 ID 可使用此角色的账户的标识符
	<ul> <li>○ 另一个 亚马逊云科技 账户 账户 ID 可使用此角色的账户的标识符 </li> <li>○ 第更分部 ID (第三方担任比角色时的最佳实践) 您可以通过要求提供可适的外部标识符来提高角色的安全性,以防止"湿滑代理人"吸击,如果此账户不归您所有,或者您没有对担任此角色的账户的管理访问权限,建议您这样做。外部 ID 可以包含您选择的任 何字符,要担任此角色,用户必须位于受信任账户中,并提供此编切的外部 ID。了解更多 外部 ID</li> </ul>
	<ul> <li>● 另一个 亚马逊云科技 账户 账户 ID 可使用此角色的账户的标识符 正户 ID 是 12 位数字。 </li> <li>         这项             ご             愛愛外部 ID (第三方担任此角色时的最佳实践)             您可以通过要求提供可透给外部标识符来提高角色的安全性,以防止"湿滑代理人"攻击。如果此账户不归意所有,或者您没有对担任此角色的账户的管理访问权限,建议您这样做。外部 ID 可以包含您选择的任何字符,要担任此角色,用户必须位于受信任账户中,并提供此编切的外部 ID。了解更多             外部 ID              </li> <li>             重要提示:控制台不支持将外部 ID 与切换角色功能一同使用。如果选择此选项,可信账户中的实体必须使用 API、CLI或自定义联合代理来进行跨账户 iam:AssumeRole 调             用, <u>了解更多          </u></li> </ul>

3. 进入该角色详情,将"ARN"复制并填入"RoleArn"框中。



変马避云科技 NWCD operating Ningxia Region Sinnet operating Beijing Region	Services		\$	⑦ Global ▼
Identity and Access $ imes$ X Management (IAM)	IAM > 角色 >			mino
Q 搜索 IAM	信息			(1) 10 mm 1
控制面板	创建日期	ARN	用于在控制台中切换角色的链接	7999 455
▶ 访问管理 用户组		٥	Ø	
用户 <b>角色</b> 策略	上次活动	最大会话持续时间 1个小时		
身份提供商 账户设置	权限 信任关系 标签 撤消会话			
7 访问报告 访问分析器	<b>权限策略 (0) 信息</b> 您最多可以附加 10 个托管策略。		日本 「 「 人 人 人 人 人 人 人 人 人 人 人 人 人 人 人 人 人	删除 添加权限 ▼
分析器 凭证报告	Q. 搜索	筛选依据 类型           所有类型	•	< 1 > ©
	策略名称 🖸	▲ 类型	▽ │ 关联实体	$\nabla$
		没有要显示的资源		
	▶ <b>权限边界</b> (未设置)			



# 多账号管理

最近更新时间: 2025-08-15 14:42:31

## 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,集中管理集团内外所有账号,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。 支持对集团内外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<mark>完成实名认证</mark>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。



基本信息	集团账号管理使用说明文档 岱
① 当您创建一个集团组织后,您不能加入其它的集团账号管理中,直到此集团组织	被删除。
The set of the second set of the second set	
	集团账号管理类型:账号、资源、费用管理型组织
	⊘ 多账号管理 创建集团组织架构,将账号成员分类管理
	⑦ 资源共享管理 创建共享单元,为成员账号共享资源
	○ 集团财务管理 查看集团财务概览,支持查看成员账单、消费明细,为成员划拨资金、共享优惠等
	更多集团账号管理内容了解详情 2
	<u>ésisa</u>

## 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、集团外账号管理

## 步骤1: 接入集团外账号

1. 在 多云多账号管理页面,单击**接入多云账号**。

2. 在配置多云、云外、混合云账号页面,选择账号类型为**腾讯云子账号**,按照选择的创建子账号方式进行相关配置,单击**确定**完成接入。



	🖸 阿里云账号	📒 Azure账号	🔤 AWS账号	❷ 腾讯云子账号	
	🔗 腾讯云账号	,前往集团账号配置 🖸			
创建子账号的方式	○ 快速配置 1分報 有资	中完成,但权限较大,需要 产的只读权限	配置主账号AK,云安	R全中心将自动创建子帐号AK接入资产	•,并获取所
	● 手动配置 5分	钟完成,但权限配置较为复	杂,需要配置创建好	的子账号AK,更加灵活的控制权限范	
	高级配置 较为 ARN	复杂,但权限范围、期限5 I并且带有uuid的账号调用s	完全可控,按照我们提 ts:AssumeRole接口	是供的RoleArn在腾讯云创建角色,并 」,该接口用于创建账号的临时访问角1	授权来自指定 色
	收起配置指引 🔺				
	〈 第1/2步 〉	请登录腾讯云后前往 <mark>访</mark> 资源的SecretId、Secr	问管理>安全凭证 Ľ etKey。	点击"新建密钥"生成可用于监控或管	理 腾讯云
		2014年 - 2012年0 2月1日1日	88	-1.5%. Q 🔗 089 🗹 Satas- da IA- BEAN-	21 API (211211) 12
	12 65.2 2. A/P ·	<b>9288</b> • SIN AN SURFACEMENT OF MERICANON, CONTRACT AND     • ST TEMPO ADDRESS, AND ADDRESS AN	LURYESTRANSLER. HAT DEGENALISER.		
		BREAN TA DESCRIPTION AND APPECAR, BOX     TOTALEMENTE (ANS) ABBREA-SEPARES, BYE	N TL\$12.50(188) 28. (#478-40052)***********************************		
	C #25%744 ·	Contract Contract of State Back State State State     Contract State Stat	LINGSER BELEVILLE GRANNERSERESE, GRANNERSERE	98%.	
	<	APPO EX	0.000	805049700 000 849	
			•		
主账号SecretID	请输入				
十 III B Cooxot Kov	请输入				
土城与Secretkey	为防止主账号AK泄	露,请在云安全中心创建完	子账号自动接入资产	流程结束后删除以下AK	
土 <u>赋</u> 亏Secletkey					
主账号Secretkey 配置子账号权限	主机资产-读, 容器	器资产–读, 公网IP资产–读, :	域名资产-读, 数据库	资产-读, 其他云资产-读, 账号基本	~
配置子账号权限 所属部门(选填)	主机资产-读, 容器 请选择	器资产−读, 公网IP资产−读, : ~	域名资产-读, 数据库	资产-读, 其他云资产-读, 账号基本	~
主账号Secterkey 配置子账号权限 所属部门(选填)	主机资产-读, 容器 请选择 从腾讯云集团账号刻	<b>聲资产−读, 公网IP资产−读,</b> ~	<b>域名资产-读, 数据库</b> 读管理,请为当前账	<b>资产-读, 其他云资产-读, 账号基本</b> 号选择一个部门	~
王赋号Secterkey 配置子账号权限 所属部门(选填) 资产同步频率	<b>主机资产-读, 容器</b> <b>请选择</b> 从腾讯云集团账号载 请选择	<b>啓資产−读, 公网IP资产−读,</b> ~	<b>域名资产-读, 数据库</b> 续管理,请为当前账	<b>资产-读, 其他云资产-读, 账号基本…</b> 号选择一个部门	~
主派号Secterkey 配置子账号权限 所属部门(选項) 资产同步频率 其他设置	主机资产-读,容器 请选择 从腾讯云集团账号系 请选择 配置完成后立即 同步完成后发起	留资产-读,公网IP资产-读, 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	<b>或名资产-读, 数据库</b> 续管理,请为当前账	<b>资产-读, 其他云资产-读, 账号基本</b> 号选择一个部门	~
主派号3960161469 配置子账号权限 所属部(1)(选填) 资产同步频率 其他设置	主机资产-读,容器 请选择 从腾讯云集团账号载 请选择 配置完成后立即 同步完成后文起	書资产-读,公网IP资产-读, 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	<b>域名资产-读, 数据库</b> 续管理, 请为当前账	<b>资产-读, 其他云资产-读, 账号基本…</b> 号选择一个部门	~

# 步骤2: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。



#### 多云多账号管理

团账号概况							前	前往管理集[	团账号 🖸 了解更多	8 G
理员账号名称 管理	迟账号ID 多군 <mark>소</mark>	、混合云账号接入 13 🚾 5 🔛 2 🖸 4 接.	∖多云账号	±) 2 管理	<b>账号</b> 【 <b>4</b> 个 理员/委派管理员 2	已启用(已版 <b>23  </b> 5	9买账号数 ① 无上限	<b>子账号</b> 180 个 异常账号 -		
主账号 <b>子账号</b>									0	
数据更新 管理	■腾讯云子账号 🖸	全部主账号 >	全部子账号 >			多个关键字用竖线" "分	隔,多个过滤标签用回车	键分隔	Q	
子账号名称 ⑦	子账号ID/APPID	所属主账号	所属主账号ID/APPID	可访问服务 ‡	可访问接口/操作 ↓	可访问资产数 💲	访问/行为日志 🛈 💲	权限	操作	
2		声声乌龙		0	0	0	-	-	行为日志 更多 🗸	
2		幽兰拿铁		408	0	56	0	0	行为日志 更多 ~	
Ø		声声乌龙		66	0	622	-	0	行为日志 更多 ~	5
8		3458898399		0	0	0	-	-	行为日志 更多 🗸	

# 三、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**。

主账号 子!	K4									
数据更新	添加或管理成员账号 🖸	添加多云账号			8	个关键字用竖线 " " (	分隔,多个过滤标签	用回车键分隔	Q	φ
账号名称 🔻	账号ID/APPID	身份 🛈 🔻	所属部门 ▼	加入集团方式 访 🔻	权限 \$	子账号 🗲	资产数 🕏	风险数 🛊	操作	
8		管理员	Root	集团账号	0			0	登录账号更多	¥ 👻
————							10 ▼ 条/页		1 /1页	▶

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。



登录账号			×
() 子账号	导可以通过被授予的访问权	Q限快速登录到成员账号控	制台。 <b>查看详情</b>
成员账号	China State	添加子账号授权 🖸	
访问权限	权限名称	策略名称	操作
			登录成员账号
	2017	-polymer -	登录成员账号
	41	augustan.	登录成员账号

## 四、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**成员账号名称/成员账号 ID** 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。

资产中心					多账号管	<b></b>	× 😒
资产更新 🕜 🙆 🧧	接入多云资产 手动添加资产 收集	外部资产		请输入账号名称/账号ID进行搜	2		Q <sub>X</sub>
资产统计概况				- 账号名称	账号ID/APPID	所属部门 ▼	
主机资产 🛈	公网IP资产	域名资产	主机资产监控 容器资				,
<b>个</b> 未防护主机, 风险主机	个 未防护公网IP 风险公网IP	<b>个</b> 未防护域名 风险域名	Obps	<b>⊘</b>			
容異资产	园生资产	数据库资产	Obps	<u>&amp;</u>			
Υ Υ	↑	÷	0bps 0bps				
三 按资产分组 🛛 按资产	◎类型 ① 按服务类型 只看新增 5	2番核心 只看未防护					φ
主机资产 容器资	产 公网IP资产 域名资产	网络资产 数据库资产	其他云资源				
开启防护标记为核	心资产 标记为非核心资产				确定取消	7 DA.A.V	X77X -

#### 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



多云多账号管理											
<b>集团账号概况</b> 管理员账号名称	管理反販号ID 多云 の	、混合云账号接入 2	云账号			<b>主账号</b> 个 管理员/委派管理/	5	已启用丨已	购买账号数 ① 无上限	前 子 <b>账号</b> 异常账号	±管理集団账号 ピ 了解更多 ピ 个
主账号 子 数据更新	账号 添加或管理成员账号 [2]	添加多云账号						[	多个关键字用竖线 "!" 分	}篇,多个过滤标签用回车链	分隔 Q Φ
账号名称 ▼	账号ID/APPID	身份 🕄 🔻	所属部门 🔻	加入集团方式 🛈 🍸	权限 ≄	子账号 \$	资产数 (i) \$	风险数 (j) \$	告警数 \$	启用状态 ▼	操作 -
Ø											登录账号 <b>更多 ▼</b>
8											登录账号 更多 ▼
Ø											登录账号 <b>更多 ▼</b>

#### • 管理员子账号登录

团账号概况										前	注管理集团账号 🖸 了解更
员账号名称	管理员账号ID 多云 G	、混合云账号接入	云账号			主账号 个 管理员/委派管理	ž	已启用   已	购买账号数 ① 无上限	<b>子账号</b> 异常账号	Ŷ
· <b>账号</b> 子! 	<b>张号</b> 添加或管理成员账号 【	添加多云账号							多个关键字用竖线 "1" 分	隔,多个过滤标签用回车银	纷隔 Q
号名称 ▼	账号ID/APPID	身份 🛈 🔻	所属部门 🔻	加入集团方式 🕃 🍸	权限 \$	子账号 \$	资产数 🛈 💲	风险数 🛈 💠	告警数 \$	启用状态 ▼	操作
ð										-	-
5											登录账号 <b>更多 ▼</b>
5											登录账号 更多 ▼
										_	

• 成员主账号、子账号登录

多云多账号管理					
集团账号概况					前往管理集团账号 🖸 了解更多 🗹
			主账号	已启用   已购买账号数 🚯	子账号
管理员账号名称	管理员账号ID	<b>多云、混合云账号接入</b>	个 管理员/委派管理员	一一无上限	个 异常账号

# 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。



资产中心								多账号管理			• 😒
0 🛛 🔤 🗉	接入多云资产								近24小时	7天 :	30天
资产统计概况											
主机资产 ①	公网IP资产	域名资产		主机资产监控	容器资产监控	公网IP资产监控	域名资产监控	网关资产监控	入向峰值	植带宽 TOP5	Ŧ
$\uparrow$	$\uparrow$	$\uparrow$							38.22Mbps		
未防护主机	未防护公网IP	未防护域名						35.3	34Mbps		
MARKE 19	1/14/25.24 (PS11*	1994 MIL 1997 Tol				17.1	2Mbps				
容器资产	网关资产	数据库资产				16.46	Mbps				
$\uparrow$	$\uparrow$	$\uparrow$				15.21Mb	ps				
按资产分组     按资产类型	① 按服务类型 只看新增	只看核心 只看未防护					多个关键字用竖	线 "[" 分隔,多个过滤	标签用回车键分隔	Q	φ
主机资产 容器资产	公网IP资产 与	<b>记名资产</b> 网络资产	数据库资产	其他云资源							
标记为核心资产标记为非	核心资产 删除								☆ 自定义	列表字段	Ŧ
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 ▼	Web应用防火墙	防护 🕇 👘 所属账号	▶▼ 操作		
	-	待认证外部资产	未知	-	-			Ø	认证资产 3	更多 ▼	

#### 漏洞与风险中心

在 <mark>漏洞与风险中心页面</mark>,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。

漏洞与风险中心							○1个任务正在扫描	多账号管理		0
安全体检全部资产	▼ 综合体检结果 ▼								近24小时 7天	30天
资产风险概况 🕕		重新检测详情、	,							
漏洞风险	端口风险	弱口令风险		J	风险趋势					
↑	个高危	个高危			漏洞风险 端口风险					
					弱口令风险					
内容风险	云资源配置风险	风险服务暴露			内容风险 云资源配置风险 风险服务暴露	-				
高危	高危	高危								
<b>漏洞风险</b>	弱口令风险 内容风险 云资源配置风险	风险服务暴露								
影响我的漏洞 全网漏洞	资产视角 ▼ 处理漏洞 ▼ 只看必修漏)	月 只看应急漏洞					处理状态: <b>未处理</b>		Q Ø	¢ Ŧ
漏洞名称	公网IP/域名	关联实例ID/名称	资产类型 🔻	端口	组件	风险等级 🔻	漏洞类型 ▼ CVE1 处理状态 ▼	所属账号 ▼	操作	
			CVM	-	-	严重	· • 未处理	Ø	标记处置 更多	•

# 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。



安全体检						多账号管理		• 📀
安全体检任务 体检任务 / 总配额 ① 同期任务 个 进行中 0 个	已用件检次数 / 总配额 次 升级购买配额 查看报告		<b>安全体检任务执行记录</b> 体检开始时间	体检名称		体检结束时间		操作 详情 详情
创建安全体检任务 停止任务	■除 全部执行情况 ▼				多个关键字用竖线 " " 分隔,	多个过滤标签用回车键分隔	Q	¢
任务ID/名称 任务类型 ▼	体检资产 ◆ 体检项目 ▼ 执行时间 ◆	預估耗时 任务执行情况	体检报告	体检模式 ▼	体检来源 ▼	创刻 所属账号 ▼	操作	
限免体检 ①	🖸 🏂 ် 🗟 🌐 🌐	約 8 分钟 完成时间: 2024-1	08-05 06:09:17	高级体检	立体防护	202 🙆 🕽	编辑 删除	

# 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。

报告下载					多账号管理 🕹 腾讯云	安全体验账号	•
报告概況 报告数量 援告模板 个 ↑ 待查看 ↑ 前往創建	关注服务号,随时随地接收报告 腾讯云为开发者提供移动管理工 发者在手机上快捷管理云资源和 效管理	具, 報助开 云账户, 高	<b>报告下载记录</b> 振告生成时间 9 202 9 202 9	任务名称	报告类型 报告名称 体检报告 体检报告 体检报告		<b>操作</b> 详情 详情
报告下载 报告模板 一键下载				多个关键字用竖线 鬥分	3篇,多个过滹标签用回车键分隔	(	ζφ
报告名称 报告	言类型▼ 体检资产 \$	风险统计 🗲	体检任务ID/名称	生成时间 🕏	所属账号 ▼	操作	

# 五、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!



# 阿里云账号权限说明

最近更新时间: 2025-06-26 16:48:52

# 权限说明

腾讯云安全中心调用阿里云账号需要的权限和说明如下:

产品	参考的系统策略	配置项	说明
费用与成本 (BSS)	AliyunBSSFullAcce ss 管理费用与成本 (BSS)的权限	{ "Action": [ "bss:", "bssapi:" ], "Resource": "*", "Effect": "Deny" }	拦截所有费用与成本相关的访 问,避免访问用户费用清单。
所有	ReadOnlyAccess 只读访问所有阿里云资 源的权限	<pre>{     "Action": [     "Describe",     ":List",     ":Get",     ":Read",     ":BatchGet",     ":BatchDescribe",     ":Query",     ":BatchDescribe",     ":Query",     ":BatchQuery",     "actiontrail:Lookup*",     "actiontrail:Check*",     "dm:Desc*",     "dm:Desc*",     "dm:Desc*",     "dm:SenderStatistics*",     "ram:GenerateCredentialReport",     "cloudsso:Check*",     "notifications:Read*",     "selectdb:Check*",     "hbr:Search*",     "hbr:BatchCountTables",     "hbr:BatchCountTables",     "hbr:PreCheckSourceGroup",     "nis:Count*",     "nois:Count*",     "nis:Is*",     "sr:HasRole",     "resourcecenter:ExecuteSQLQuery",     "resourcecenter:ExecuteSQLQuery",     "Clickhouse:Check*"     ],     "Resource": "*",     "Effect": "Allow" } </pre>	只读访问所有阿里云资源



消息队列 RocketMQ 版	_	{     "Action": [         "mq:OnsRegionList",         "mq:OnsInstanceInServiceList",         "ons:OnsRegionList",         "mq:OnsInstanceInServiceList"     ],     "Resource": "*",     "Effect": "Allow" }	读取消息队列 RocketMQ 版 的Region和服务列表
云安全中心 ( SAS )	AliyunYundunSASF ullAccess 管理云安全中心 (SAS)的权限	<pre>{     "Action": [         "yundun-sas:",         "yundun-aegis:",         "sasti:"     ],     "Resource": "",     "Effect": "Allow" }, {     "Action": "ram:CreateServiceLinkedRole",     "Resource": "*",     "Effect": "Allow",     "Condition": {         "StringEquals": {             "ram:ServiceName": [             "sas.aliyuncs.com",             "cloudsiem.sas.aliyuncs.com",             "cspm.sas.aliyuncs.com"         ]      } }</pre>	阿里云云安全中心管理权限, 未来可能用于漏洞修复、告警 确认等场景,变更动作均由用 户通过控制台触发,云安全中 心仅主动触发查询操作。
云盾应用防火 墙(WAF)	AliyunYundunWAF FullAccess 管理云盾应用防火墙 (WAF)的权限	{ "Action": "yundun-waf:", "Resource": "", "Effect": "Allow" }	应用防火墙(WAF)管理,变 更动作均由用户通过控制台触 发,云安全中心仅主动触发查 询操作。
云盾云防火墙 (CloudFir ewall)	AliyunYundunClou dFirewallFullAcces s 管理云盾云防火墙 (CloudFirewall)的 权限	<pre>{     "Action": [         "yundun-cloudfirewall:*",         "sasti:Get*",         "sasti:Describe*",         "sasti:Query*",         "sasti:List*",         "sasti:Grant*",         "bss:QueryAvailableInstances",         "bssapi:QuerySavingsPlansInstance" ],     "Resource": "*",     "Effect": "Allow" }</pre>	云防火墙(CloudFirewall) 管理,变更动作均由用户通过 控制台触发,云安全中心仅主 动触发查询操作。

# 权限脚本配置

"*:BatchQuery*",
"hbr:CheckRole",









# 访问权限管理

最近更新时间: 2024-07-22 10:44:31

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。

<b>程自定义策略</b> 删除		全部策略 预设策略 自定义策略	QcloudSSAFullAccess	<b>Q</b> Q
策略名	服务类型 ▼	描述	上次修改时间	操作
QcloudSSAFullAccess	云安全中心	Full read-write access to Security Situation Awareness(SS,	A) 2024-03-06 11:06:16	关联用户/组/角色
已洗0项 共1项			10 - 冬/页 14 - 1	/1页 ▶ ▶

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。



关联用户/用户组/角色						×
选择添加的用户 (共 29 个)				已选择 (1) 个		
支持多关键词(间隔为空格)搜索用户;	名/ID/SecretId/手机/邮箱/智	Q,		名称	类型	
■ 用户	切换成用户组或角色 🍸				用户	ß
	用户	Â				
u	用户					
ng	用户		$\Leftrightarrow$			
g	用户					
	用户					
	用户					
支持按住 shift 键进行多选		*				
<b>确定</b> 取消						