



云安全中心

操作指南

产品文档





【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有,未经腾讯云事先书面许可,任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】



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。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况,部分产品、服务的内容可能有所调整。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。



文档目录

操作指南

访问权限管理 多云多账号管理

多云接入

多账号管理

模拟攻击

日志投递(支持多账号多产品多日志)

资产中心

安全体检

功能简介

操作指引

添加白名单 IP

热点问题

用户行为分析(UEBA)



🔗 腾讯云

操作指南 访问权限管理

最近更新时间:2024-08-02 10:14:18

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

操作场景

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

SOC 的全读写策略

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

SOC 的只读策略

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

SOC 相关资源的策略

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

操作步骤

1. 登录 访问管理控制台,在左侧导航中,单击**策略**,进入策略页面。

2. 在策略页面的搜索框中,输入策略名称(根据实际需求搜索),如输入"QcloudSSAFullAccess"进行搜索。

3. 在"QcloudSSAFullAccess"策略的右侧操作栏中,单击关联用户/组/角色。



新建自定义策略		全部策略 预设策略 自定义策略
策略名	服务类型 ▼	描述
QcloudSSAFullAccess	云安全中心	Full read-write access to Security Situation Awareness(

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	5/ID/SecretId/手机/邮箱/崔	Q		名称	类型
- 用户		切换成用户组或角色 ▼				田户
		用户	Î			,13,
	u	用户				
	ng	用户		↔		
	g	用户				
		用户				
	b	用户				
古法按住 shift 鏈			•			
2X143X17 9000 84	2011 32722					
			确定		取消	



多云多账号管理 多云接入

最近更新时间:2024-08-02 10:14:18

功能简介

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

操作步骤

1. 登录 云安全中心控制台, 在左侧导览中, 单击**多云多账号管理**。

2. 在多云多账号管理页面,单击**接入多云账号**。



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



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	置区
子账号的方式	手动配置 5分钟完成,	,需要创建"应用注册 文档中查看 I2	"与"客户端密码",并绑定	5"订阅",赋予"读者"权限。	
	〈 第1/3步 〉	请前往 www.azure	.com/xxx 🖸 创建一个应用	用注册,并根据需要选择支持的帐户类	型。
	Constant (20) Constant	Elene : 2º 4000 Elene : 4º 400 elene sup Eleneted, Kinekenstere Al 400 (100)	- MARE MANINES	in	8
			AN * THE OWNER AND		
	n Anastran (EEA) 2011年3月1日 2011年3月1日日本 -		• • • • • • • •	- 9 - 5 - 6 (2)	2
ID	请输入				
ID	请输入				
端ID	请输入				
端密钥	请输入				
	为确保账号可用,请为 置)角色分配'读者'权限,	,如账号有效期内发生客府	户端密钥变更,请及时在云安全中心修	改对应配
部门(选填)	请选择	•			
	从腾讯云集团账号获取	?部门信息,为了便于	后续管理,请为当前账号	选择一个部门	

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)。



主页 >	
应用注册 🖉 👘	
+ 新注册 ⊕ 线组成 ∥ 疑惑解释 ◯ 彩新 🛓 下載 🖬 预定功能 🖗 得到反我?	
● 自 2020年6月30日起,我们将不再向 Azure Active Directory 身份恰证商(ADAL)和 Azure Active Directory Graph 添加任何新功能,我们将继续指	提供技术支持和安全更新程序,但将不再提供功能更新,应用程序将需要开级到 Microsoft 身份检证库(MSAL)和 Microsoft Graph, <u>了解更多信息</u>
所有应用程序 握有的应用程序 已删除的应用程序 个人帐户中的应用程序	
	此账户未列为这个目录中任何应用程序的所有者。
	童童自录中的所有应用程序

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	⑦ 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 進能使用此应用程序或访问此 AP!? ④ 仅此组织目录(仅 默认目录 - 单一租户)中的帐户 ● 任何组织目录(任何 Microsoft Entra ID 租户 - 多租户)中的帐户 ● 任何组织目录(任何 Microsoft Entra ID 租户 - 多租户)中的帐户和个人 Microsoft 帐户(例如 Skype、Xbox) ● 仅 Microsoft 个人帐户 幣我选择… 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 	
 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? ④ 仅此组织目录(仅 默认目录 - 单一租户)中的帐户 ● 任何组织目录(任何 Microsoft Entra ID 租户 - 多租户)中的帐户 ● 任何组织目录(任何 Microsoft Entra ID 租户 - 多租户)中的帐户和个人 Microsoft 帐户(例如 Skype、Xbox) ● 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)	
* 名称	
Microsoft Azure ① 升級 E页 > 应用注册 > 生 册 应 用程序 … 名称 生 虚 用程序面向用户的显示名称(稍后可更改)。 名称 比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 能使用此应用程序或访问此 API? ① 仅此组织目录(仅 默认目录 - 单 一租户)中的帐户 ① 仅此组织目录(仅 默认目录 - 单 一租户)中的帐户 ① 任何组织目录(任何 Microsoft Entra ID 租户 - 多租户)中的帐户 ① 仅此 (可选) 正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,但大多数身份强性值。 透择平台	
	Microsoft Azure ④ 升級 エン 第一次回知注册 > 第一次回知注册 > 第一次回知注册 > 第一次回知程序或 … 第本 2月2日 2月2日 第二 2月2日 2月2日 2月2日 2月2日 <
受支持的帐户类型	
谁能使用此应用程序或访问此	API?
Q此组织目录(仅 默认目录)	录 - 单一租户)中的帐户
○ 任何组织目录(任何 Micro	osoft Entra ID 租户 - 多租户)中的帐户
○ 任何组织目录(任何 Micro	osoft Entra ID 租户 - 多租户)中的帐户和个人 Microsoft 帐户(例如 Skype、Xbox)
 主册应用程序 … * 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 雖能使用此应用程序或访问此 API? ④ 仅此组织目录(仅 默认目录 - 单一租户)中的帐户 ● 仅此组织目录(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)中的帐户和个人 Microsoft 帐户(例如 Skype、Xbox) ● 仅 Microsoft 个人帐户 解我选择… 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,但大多数身份豁供值。 遗择平台 ∨ 例如, https://example.com/auth 	
帮我选择	
重定向 LIBI (可选)	
主龙门 Off (52)	喀把身份验证响应该回到此口RI 现在可想需要提供此口RI 日鹅后可再改 但大多数身份验
供值。	
注册应用程序 … * 名称 此应用程序面向用户的显示名称(桶后可更改)。	
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。
	 ● 升級 … 法称(稍后可更改)。 法本(前方可更改)。 法本(前方可更改)。 法本(前方可更改)。 (法本(1)) (本)) (*)) (*))
如果继续,表明你同意 Micros	soft 平台策略 ♂
注册	

步骤2:获取订阅 ID

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



≡ Micro	rosoft Azure ① 升级		の援	《资源、服务和文档(G+/)		
主页 > 订阅 订阅 承 示加	l> ¢					
全局管理员可 ク 提索任何	可以通过在此处更新其策略设置来管理此列表中 可字段	н的所有订阅。 我的角色 == 全部 状态 == 全部 ¹ ☆ 添加得选器				
订阅名称 个	ru -	itika id ↑↓	我的角色 ↑↓	当前成本	安全功能分数 ↑↓	父管理组 ↑↓
Azure subsc	cription 1	Address and the set of the set	所有者		•	

2. 在订阅详情页面,单击概述,获取订阅 ID。

			》 投系资源、服务相关目(047)	
页 > 订阅 > 订阅 > 「阅 《	Azure subscriptior	11 ☆ …		
🕇 添加 📋 管理策略 \cdots	₽ 搜索 《	📋 取消订阅 🧷 重命名 🔿 更改目录 📈 反馈		
:局管理员可以通过在此处更新其策略设置 :管理此列表中的所有订阅。	 	へ 概要 订阅 ID :		
是索任 订阅: 已筛选 (1 / 1)	♣ 访问控制(标识和访问管理)	目录:		
我的角色 == 全部	♦ 标记	状态:可用		
状态 == 全部	🗙 诊断并解决问题	父管理组:		
+~ 添加筛选器	 安全性 多 事件 	支出率和预测	按资源划分的费用	热门务
Azure subscription 1 ····	成木等理		~	^ 1/2
	· · · · · · · · · · · · · · · · · · ·	沿方西日云的数据		~
	1 成本整提	汉有安亚小时奴据	14.	服务
	(2) 荷質			Azur
	() 所得	当前成本 外憩	目前还没有活动资源发出使用量。	1100
	■ 建築(15)また			Azur Free
	计费			
	🔄 计费对象信息发票			Stora
	设置	按资源数排列的产品	Azure Defender 覆盖范围	Stor
	△ 编程部署	1		Page
	₩ 计费属性	0.5		Stor
	() 资源组			Man Sna
	资源	0	~	Stor
	■ 预览功能	userassignedidentities	没有为此订阅户用 Azure Defender	Ope
	🔜 使用情况 + 配额		升级覆盖范围	
	● 策略	查看资源		查
	🔁 管理证书			
	⁸ ☆ 我的权限			
	※三 资源提供程序			
	部署			
	🧐 部署堆栈			
	🔒 资源锁			
	帮助			

3. 选择**访问控制**,单击**添加**,选择**添加角色分配**。



主页 > 订阅 > 订阅 > Azure subscription 1					
订阅 《 默认目录	Azure subscription 1 روم Azure subscription	访问控制(标识和访问管理)	☆ …		
┼ 添加 🃋 管理策略 ···					
全局管理员可以通过在此处更新其策略设置	↑ 概述	添加角色分配			
来管理此列表中的所有订阅。	PREME RANKENGAGE PREME RANKENGAGE PREME RANKENGAGE PREME RANKENGAGE PREME RANKENGAGE PREME RANKENGAGE PREME RANKENGAGE PREME RANKENGAGE PREME RANKENGAGE PREME RANKENGAGE PREME RANKENGER PREME RANKENGAGE PREME RANKENGE PREME RANKENGE				
♀ 搜索任 订阅:已簿选 (1 / 1)	Sg 访问控制(标识和访问管理)	添加自定义角色	+0月31日之间, 川利兹突着建筑110月南西大五内门所可以		HDAD HIGH SKARHBEIT (VIN) 200
我的角色 == 全部	♦ 标记	检查访问 角色分配 角色 拒绝分配	▲ 经典管理员		
状态 == 全部	🗙 诊断并解决问题				
+▽ 添加筛选器	安全性	我的访问权限 查看我对此资源的访问级别。	♪ R業業業、服务和文化(Go) 和坊内管理) ★ 2012 三 単称列 () 単新 × 目前 戸 & 第 2014 三 単称列 () 単新 × 目前 戸 & 第 2014 三 月 31 日之后、所有社会管理会会与打算的以内代品、新述不具要定以内代品的法理理点、成分社 Auve ROAD 会 LU. KR# Her KURPER. 角色 単位分配 ▲ 社会管理点 HE 等 HER AUX ▲ 社会管理点 HE 等 HER AUX ▲ 社会管理点 HE 等 HER AUX ▲ 社会管理点 E 電子が比淡薄 Sh (Lange Aux Auve ROAD 会 LU. KR# Her KURPER. HE 等 HER AUX ▲ 社会管理点 E 電子が比淡薄 Sh (Lange Aux Auve ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Aux Aux Auve ROAD 会 LU. KR# Her KURPER. HE 等 HER AUX ▲ 社会管理点 E 電子が比淡薄 Sh (Lange Aux Aux Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Aux Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡薄 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子が比淡 Sh (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子 CH (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子 CH (Lange Auxer ROAD 会 LU. KR# Her KURPER. E 電子 CH (
订阅名称 ↑↓	🗲 事件	童看我的访问权限			
Azure subscription 1 ····	成本管理	AA and the Am			15、成分配 Azure RBAD 角色以实现捐偿化访问控制。 創建自定义角色 規作的角色 使用自己的双度集为 Azure 所 角色、以满足组织的特定需求 了解更多点是。() 変加
	ዿ 成本分析	恒宣访问 查看用户、组、服务主体或托管标识对此资源拥有自	り访问权限级别。 了解更多信息 ♂		
	成本警报	检查访问			
	③ 預算				
	🌳 顾问建议	授予对此资源的访问权限	查看对此资源的访问权限	查看拒绝分配	创建自定义角色
	计费				
	计费对象信息发票	通过分配角色授予对资源的访问权限。 了解更多信息 🖸	查看授予对此资源和其他资源的访问权限的 角色分配。 了解更多信息 <2	查看已被拒绝访问此范围内特定操作的角色 分配。 了解更多信息 r2	使用自己的权限集为 Azure 角色,以满足组织的特定需 了解更多信息 CZ
	设置			+/) 物は何収温、振祥不再重要访何权限的投展管理点、成分配 Asure RBAD 角色以及現積低化访问交訊、 雪石 に 文規語 うだ。 「新見 5 信息 ci 一 電 一 一 一 一 一 一 一 一 一 一 一 一 一	
	编程部署	添加角色分配	视图	視图	添加
	计费属性				
	() 资源组				
	资源	 唐金坊區 角色 拒绝分配 ▲ 拒绝分配 ▲ 陸典管理员 年度北防防時限 西北市 組 馬多生体或比管療识对此资源機會的访问权限 (新要多信息 of Action (新要多信息 of Action (Action (Action			
	■ 预览功能				
	☴ 使用情况 + 配额				
	● 策略				
	戸 管理证书				
	⁸ ♀ 我的权限				
	注 资源提供程序				
	部署				
	9 部署堆栈				
	🎴 资源锁				
	帮助				
	⑦ 支持 + 故障排除				
雷田公前的角角	唐沙龙次选择"遗步	× "€Π"Λzuro Kuborp	too 肥冬群隹田白鱼	色"	



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		
用色成员 录件 审阅和分配		
角色定义是权限集合。可以使用内置角色,也可以创建你自己的自定义角色。了解	要多信息が	
作业职能角色 特权管理员角色		
按角色名、说明、权限或 ID 搜索 类型:全部	共列:全部	
名称 ↑↓	説明 やよ	类型 ↑↓
读者	查看所有资源 。但不允许进行任何更改。	BuiltInRole
安全读取者	安全谈取者角色	BuiltInRole
安全管理器(旧)	这是旧角色。请改用安全管理员角色	BuiltInRole
安全管理员	安全管理员角色	BuiltInRole
安全评估参与者	允许将评估推送到安全中心	BuiltInRole
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
安全引爆室发布者	允许将平台、工作追和工具集发布到安全引爆室并进行修改	BuiltInRole
安全引爆室提交内容管理者	允许自建向安全引爆室提交的内容并进行管理	BuiltInRole
备份参与者	允许你管理备份服务,但是不能创建保留库以及损予其他人访问权限	BuiltInRole
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
备份读者	可以查看备份服务,但是不能进行更改	BuiltInRole
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
測试基读者	允许重看和下载包和测试结果。	BuiltInRole
策略见解数据编写器(预览版)	允许对贾源策略进行该取访问,并允许对贾源组件策略事件进行写入访问。	BuiltInRole
层次结构设置管理员	允许用户编辑和删除很次结构设置	BuiltInRole
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
成本管理读取器	可以查看成本教課和配置(例如,預算、导出)	BuiltInRole
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
磁盘池操作者	由 StoragePool 资源提供程序用于管理添加到磁盘涂的磁盘。	BuiltInRole
磁盘还原操作员	向备份管管库提供执行磁盘还覆的权限。	BuiltInRole
磁盘快照参与者	向备份保管库提供管理磁盘快照的权限。	BuiltInRole
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
存储表数据参与者	允许对 Azure 存储表和实体的读取、写入和删除访问	BuiltInRole
存储表数据读者	允许对 Azure 存储表和实体进行读取访问	BuiltInRole
存储队列数据参与者	授予对 Azure 存储队列和队列消息的渎职、写入和删除权限	BuiltInRole
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
存储队列数据消息处理器	允许授予对 Azure 存储认列消息的速览、接收和删除权限	BuiltInRole
之確貼·利數提習·意爱送者	小学家後 A7102 互保U 別語教	BuiltInBole
审阅和分配 上一步 下一步		

5. 添加需要分配的用户,单击**选择成员**,在搜索框输入要添加的"应用注册"名称,选择该**应用注册**,单击**下一步**。

6. 确定角色与成员,单击**审阅和分配**。



≡ Microso	ft Azure ① 升级	
主义〉订阅〉		
添加用巴?	づ自己 …	
角色 成员	条件 审阅和分配	
角色	读者	
范围		
成员	名称	对象 ID
道明	干消明	
6443	7G WC4/3	
审阅和分配	上一步下一步	
約:获取租户 ID	、客戶端 ID、客戶端密钥	

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"。



=	Microsoft Azure	① 升级				
主页 >	> 应用注册 >					
	csip 🖈 …					
_						
2搜	索	*	■ 删除 4. 终结点 ≥3 预宽功能			
- 概3	述		👔 有时间吗? 我们希望咳到你对 Microsoft 标识平台(以前为面向开发人员的 Azure AD)的反馈。 →			
📣 快;	速入门					
💉 集日	成助手		へ 概要			
管理			显示名称 : <u>csip</u>		客户端凭据	: <u>1 证书、2 机密</u>
🖬 品牌	牌打造和属性		应用程序(客户端) ID:		重定向 URI	: 添加重定向 URI
④ 身(份验证				应用程序 ID URI	
† 证=	书和密码		回來(他一) D · · · · · · · · · · · · · · · · · ·		本地自从中的九星应用	· 636
() 令#	牌配置					
📀 AP	リ权限		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 3	添加任何新功能。我们将继续提供技术支持和安全更新程	I序,但将不再提供功能更新。应用程序将需要升级到 Microsoft	身份验证库(MSAL)和 Microsoft Graph。 <u>了解更多信息</u>
🙆 公決	开 API					
11 应用	用角色		<u>VI</u> 74			
🔉 所礼	有者					
👗 角包	色和管理员			生成1	使用 Microsoft 标识半台的应用	桂序
□ 清約	单		Microsoft 标识平	平台是身份验证服务、开放源代码库和应用程序管理:	工具。你不仅可以创建基于标准的新式身份验证解决方案、	访问和保护 API,还能为用户和客户添加登录名。 了解更多
支持和	疑难解答					
/> 疑	难解答					
🤰 863	建支持请求		-	N N N	Ö 😰	* *
			×	ा 🔹 🔹 🚺		
			24 田町		在 5 分钟内执行用户登录	为组织配置
			生成功能	- 語更强大的应用程序,内含 Microsoft 服务提	使用我们的 SDK,只需执行几个步骤,即可让用户	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。	室來升调用 API。请使用快速入门米后动 Web 应 用、移动应用、SPA 或守护程序应用。	略、配置单一登录等。
			宣響	API 权限	宣看所有快速入门指南	转到"企业应用程序"

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。

💡 test 证书和密码 🔅	? ···	22400
▶ 搜索 《	₽ 得到反馈?	说明
 職述 ● 快速入门 ✓ 健成助手 	借助凭据,凭据应用程序可以在 Web 可寻址位置(使用 HTTPS 方案)接收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(而不是客	银江舟户区
[*] [*] [*] [*] [*] [*] [*] [*] [*] [*]	① 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 身份验证 	证书(0) 客户端密码(0) 联合凭据(0)	
 ♥ 证书和密码 ① 		
 ()) 令牌配置 → API 权限 ○ () → API 	→ 新客户端密码 ② 说明 截止期限 值 ① 机密 ID	
 公开 API 	尚未为此应用程序创建任何客户端机密。	
🎦 所有者		
🛃 角色和管理员		
1 清单		
支持和疑难解答		
乃 疑难解答		
🧟 新建支持请求		



		م	搜索资源、服务	和文档(G+/)	
主页 > test					
💡 test 证书和密码 🦻					
∧ 搜索 《	৵ 得到反馈?				
₩ 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 HTTP	S 方案)接收令牌	时向身份验证服务标	示识自己。为了提高保障水平
💉 集成助手					
管理	可以在下面的选项卡中指	戈到应用程序注册证书、密钥和联行	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间	用来证明自己标识的机密字符串	。亦称为"应用稻	昆序密码"。	
令牌配置	→ 新客户端密码				
-→ API 权限	说明	載し期	虎	Û	
🔷 公开 API	test	2026/4	/24	<u> </u>	
12 应用角色	1001	2020/4	67		

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"。



anagement (IAM)			
	您没有分配 MFA		
) 搜索 IAM	←→ 作为安全最佳实践,我们建议您分配 MFA。		
制面板	账户详细信息		
回管理	田户名		用户 ARN
户组			Ð
1	亚马逊云科技 账户 ID		亚马逊云科技 电子邮件地址
3	Ð		0
2	规范用户 ID		
提供商	Ð		
设置			
报告 分析器	Amazon IAM 凭证 Amazon CodeCommit	凭证 Amazon Keyspaces 凭证	
字档规则 分析器	控制台登录		
报告			
	控制台登录链接		控制台密码
			最后一次登录控制台
	使用 MFA 提高忽的 业与遗云科技 环境的安全性。使用 MF	A 登录需要来目 MFA 设备的身份验证码。每位用尸最多可分配 1 台 MF	A 设备。 <u>了解更多【</u> 】
		····································	以堪喜 亚马逊元利技 环谙的安全性
		分配	MFA 设备
	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 fo	or Powersnell、亚马逊云科技 软件并发工具包以骊柱方式调用 亚马逊"	科技,或者且接进行 亚马逊云科技 API 调用。沤一次謆
	使用访问密钥从 亚马逊云科技 CLI、亚马逊云科技 Tools fi 创建访问密钥	or Powersnell、亚马波云科技和叶开友上具已以确在方式调用亚马宽。	科技,或者且按进行 亚马遗云科技 API 调用。芯一次最
	使用访问密钥从 亚马逊云科技 CLI、亚马逊云科技 Tools fi 创建访问密钥	or Powershell、亚马波云科技 软件开发上具包以编程方式调用 亚马波: 没有访问密钥。最佳实践是避免使用长期凭证,例如 创建	KH拉,或者直接並行业与遗云科技API调用。∞一次置 访问密钥。请使用提供短期凭证的工具代替。 了 访问密钥
	使用访问密钥从 亚马逊云科技 CLI、亚马逊云科技 Tools fi 创建访问密钥	or Powershell、亚马波云科技 软叶开友上真包以彌桂方式调用 亚马波 没有访问密钥。最佳实践是避免使用长期凭证,例如 创建	KH技,或者直接进行业与遗云科技 API 调用。谜一次最 访问密钥。请使用提供短期凭证的工具代替。 了 访问密钥
	使用访问密钥从 亚马逊云科技 CLI、亚马逊云科技 Tools fi 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 SO/	or Powershell、亚马波云科技 软件开发上真包以硼程方式调用 亚马波 没有访问密钥。最佳实践是避免使用长期凭证,例如 创建 AP 协议请求。一次最多可以有两个 X.509 证书(活跃或非活跃)。 <u>了解现</u>	KH技,或者直接进行业与遗云科技API调用。湿一次最 访问密钥。请使用提供短期凭证的工具代替。了1 访问密钥
	使用访问密钥从 亚马逊云科技 CLI、亚马逊云科技 Tools fi 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 SO/ 创建时间	or Powershell、亚马波云科技 软件开发上真包以编程方式调用 亚马波 没有访问密钥。最佳实践是避免使用长期凭证,例如 创建 AP 协议请求。一次最多可以有两个 X.509 证书(活跃或非活跃)。了解现 指纹	○ 「「「「「「」」」」、「「」」、「「」」、「「」」、「「」」、「「」」、「「
	使用访问密钥从 亚马逊云科技 CLI、亚马逊云科技 Tools fi 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 SO/ 创建时间	or Powershell、亚马波云科技 软件开发上其包以硼程方式调用 亚马波 没有访问密钥。最佳实践是避免使用长期凭证,例如 创建 AP 协议请求。一次最多可以有两个 X.509 证书(活跃或非活跃)。 <u>了解现</u> 指纹	KH2,或者且接近行业与認広科技API调用。巡一次重 访问密钥。请使用提供短期凭证的工具代替。 了 访问密钥 3.12 4.509 证书

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"。



亚马波五科技 NWCD operating Ningxia Region Sinnet operating Beijing Region Sinnet operating Beijing Region						
O 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	⑦ 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 🖒 安全凭证 🖒 创建访问密钥	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 📖					
步骤 2 - <i>可选</i> 设置描述标签	访问密钥 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					
检察访问密钥						
	访问密钥的最佳实践					
	 切勿以纯文本、代码存储库或代码形式存储访问密钥。 不再需要时请禁用或删除访问密钥。 启用最低权限。 定期轮换访问密钥。 					
	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。					
	下载.csv 文化					

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"。



dentity and Access	×	用户名	用户 ARN
Management (IAM)			đ
		亚马逊云科技 账户 ID	亚马逊云科技 电子邮件地址
Q 搜索 IAM		Ø	Ø
		规范用户 ID	
空制面板		Ð	
方问管理			
用户组		Amazon IAM 凭证 Amazon CodeCommit 凭证 Amazon Keyspa	aces 凭证
月户			
角色			
 		控制台登录	
份提供商			
长户设置		控制台登录链接	控制台密码
		D .	
方问报告			最后一次登录控制台
方问分析器			
存档规则			
心证 按 百		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 设备类型 杨诚	労验证码。每位用户最多可分配 1 台 MFA 设备。 <u>了解更多</u>
		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
		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
		没有 MFA 设 访问密钥 (1) 使用访问密钥从亚马逊云科技 CLI、亚马逊云科技 Tools for PowerShell、亚马逊云科技 架 解更多 ^[2] 创建访问密钥	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 效件开发工具包以编程方式调用 亚马逊云科技,或者直接进行 亚马
		没有 MFA 设 访问密钥 (1) 使用访问密钥从 亚马逊云科技 CLI、亚马逊云科技 Tools for PowerShell、亚马逊云科技 朝 解更多 ^[2] 创建访问密钥	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
		没有 MFA 设 访问密钥 (1) 使用访问密钥从亚马逊云科技 CLI、亚马逊云科技 Tools for PowerShell、亚马逊云科技 新 解更多 ^[2] 创建访问密钥	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
		没有 MFA 设 访问密钥 (1) 使用访问密钥从亚马逊云科技 CLI、亚马逊云科技 Tools for PowerShell、亚马逊云科技 繁 解更多 ご 创建访问密钥 描述 -	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
		没有 MFA 设 访问密钥 (1) 使用访问密钥从 亚马逊云科技 CLI、亚马逊云科技 Tools for PowerShell、亚马逊云科技 乳 解更多 ☑ 创建访问密钥 描述 - ⊢一次使用	各。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 次件开发工具包以编程方式调用 亚马逊云科技,或者直接进行 亚耳状态 仪态 ♥ Active 口创建●
		没有 MFA 设 访问密钥 (1) 使用访问密钥从 亚马逊云科技 CLI、亚马逊云科技 Tools for PowerShell、亚马逊云科技 靴 解更多 創建访问密钥 描述 - 上一次使用 无	 · 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 · 次配 MFA 设备 · 次配 MFA 设备 · 次配 MFA 设备 · 次配 MFA 设备 · · · · · · · · · · · · · · · · · · ·
		没有 MFA 设 访问密钥 (1) 使用访问密钥从 亚马逊云科技 CLI、亚马逊云科技 Tools for PowerShell、亚马逊云科技 朝 解更多 ^[2] 创建访问密钥 - 上一次使用 无	 奋。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 效件开发工具包以编程方式调用 亚马逊云科技,或者直接进行 亚³ 次件开发工具包以编程方式调用 亚马逊云科技,或者直接进行 亚³ 次件开发工具包以编程方式调用 亚马逊云科技,或者直接进行 亚³
		没有 MFA 设 访问密钥 (1) 使用访问密钥从 亚马逊云科技 CLI、亚马逊云科技 Tools for PowerShell、亚马逊云科技 智 解更多 ^[2] 创建访问密钥 描述 - 上一次使用 无 上次使用的区域	 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 次配 MFA 设备 次件开发工具包以编程方式调用 亚马逊云科技,或者直接进行 亚耳尔 水态 ○ Active 已创建 现在 上次使用的服务

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。



亚马逊云科技 NWCD operating Ningxia Region Sinnet operating Beijing Region Sinnet operating Beijing Region	iervices				
Identity and Access ×	IAM > 用户				
Q. 搜索 IAM	用户 (1) 信息 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。]
控制面板	日用户名	▲ 路径	▼ 组	▼ 上次活动	▽ MFA ▽ 密码期
▼ 访问管理					
用户组					
用户					

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"。

亚马逊云科技 NWCD operating Ningxia Region Sinnet operating Beijing Region	Services	
Identity and Access > Management (IAM)	< IAM > 用户 > 信息	
Q 搜索 IAM	摘要	
控制面板 ▼ 访问管理 用户组 用户	ARN 控制台访问 □ ▲ 在沒有 MFA 的情况下启 已创建 最后一次登录控制台 ① 从不	防问密钥 1 创建访问密钥
用色 策略 身份提供商 账户设置	权限 组 标签 安全凭证	
 ▼ 访问报告 访问分析器 存档规则 分析器 凭证报告 	控制台登录 控制台登录链接 □	控制台密码 i 最后一次登录控制台 ④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。每位用户最多可分配	1 台 MFA 设备。 <u>了解更多</u> [2]
		回難于 FA 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) 使用访问密钥从 亚马逊云科技 CLI、亚马逊云科技 Tools for PowerShell、亚马逊云科技 软件开发工具包以编程方式调用 1 创建访问密钥	亚马逊云科技,或者直接进行 亚马逊云科技 API 调用。您一次最多可拥有
	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。了 <mark>解更多</mark> 创建访问密钥

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



 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 > <u>用户</u> > > > 创建	1;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>可选</i> 设置描述标签	访问密钥 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 检索访问密钥	访问密钥 秘密访问密钥
	访问密钥的最佳实践
	 切勿以纯文本、代码存储库或代码形式存储访问密钥。 不再需要时请禁用或删除访问密钥。 启用最低权限。
	• 定期轮换访问密钥。
	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。
	• T

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 Sinnet operating Beijing Region	ervices	
Identity and Access ×	IAM > 角色	
Q. 搜索IAM	角色(2)信息 IAM 角色是您可以创建的身份,该身份具有特定权限,凭证在短期内有效。角色可以由您们 Q、搜索	信任的实体承担。
控制面板	□ 角色名称	▲ 可信实体
▼ 访问管理 用户组 用户	AWSServiceRoleForSupport AWSServiceRoleForTrustedAdvisor	亚马逊云科技 服务: support (服务相关角色 亚马逊云科技 服务: trustedadvisor (服务相
角色 策略 身份提供商 账户设置	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。	
 ▼ 访问报告 访问分析器 存档规则 分析器 凭证报告 	 小 小 小 小 小 小 小 小 い い	标准 临 自己现有的 PKI 基础设施来验证身份。 轻标

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。



步骤 1 选择可信实体	选择可信实体 🛤
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 技服务在此账户中执行操作。
	○ SAML 2.0 联合 允许从公司目录通过 SAML 2.0 联合的 用户在此账户中执行操作。 ○ 自定义信任策略 创建自定义信任策略以使其他人能够在 此账户中执行操作。
	 允许属于您或第三方的其他 亚马逊云科技 账户中的实体在此账户中执行操作。 ○ 此账户 ○ 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
	C D 是 12 位数字。
	还坝 ✓ 需要外部 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选的外部标识符来提高角色的安全性,以防止"湿滞代理人" 攻击。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 何字符。要担任此角色,用户必须位于受信任账户中,并提供此确切的外部 ID。了解更多
	外部 ID
	外部 ID ④ 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 用。 <u>了解更多</u>

3. 进入该角色详情,将"ARN"复制并填入"RoleArn"框中。



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



多账号管理

最近更新时间:2024-08-12 17:26:36

功能简介

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

操作场景

切换登录账号

支持一键切换成员账号登录,满足高效且安全的免密码切换。

集中管理账号

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

一、集团账号管理

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

注意

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

步骤1:未企业实名认证的个人账号

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



2		
您好,欢迎使用多账号 <mark>管</mark>	管理功能	City City City City City City City City
创建集团组织架构, 集团管理者有效掌握集团安 上业务的安全防护状态、风险等信息。	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
1 企业实名认证 • 暂未认证 创建或加入组织,需完成企业实名 认证,请无成实名认证	>	2 集团组织创建 创建前请先提交工单,创建后不能加入其他集团 账号管理,直到集团组织被删除
提交工单了解更多		

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	
③ 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。	
2010-0-0-00000-0000-00-0-0-0-0000-000	
集团账亏官埋奀型: (2) 3) 3) 3) 3) 3) 3) 3) 3) 3) 3) 3) 3) 3)	账亏、资源、资用官埋型组织
● → 3 → 5 → 4 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	原
○ 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]	
oltze	

步骤3:使用多账号管理

已开通多账号管理的企业账号,可开始使用多账号管理。



二、如何灵活的切换账号登录

授权访问成员账号

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

切换登录成员账号

1. 在 多云多账号管理页面,选择对应成员账号,单击登录账号。

主账号	子账号						
数据更新	添加或管理成员账号 🖸	添加多云账号					多个关键引
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
<u>&</u>		普通成员			1	0	-

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

注意

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





三、如何高效的集中管理账号

使用管理员主账号、子账号登录 云安全中心控制台后,支持查看集团安全信息,实现集团安全管理上的透明化与可 视化,实时掌握各成员账号云上业务的安全防护状态、风险等信息。

在资产中心、风险中心、扫描任务、报告下载等功能模块已适配多账号管理模式,进行跨账号操作以保证集团云上业务资产的安全。

账号切换

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



系统设置-多账号管理

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



						主账号		
會理员账号名称	管理员账号ID 多元 ②	○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	云账号			个 管理员/委派管理	员	
主账号 子财	长号							
数据更新	添加或管理成员账号 🖸	添加多云账号						
数据更新 账号名称 ▼	添加或管理成员账号 乙 账号ID/APPID	添加多云账号 身份 ③ ▼	所属部门 ▼	加入集团方式 ① 🔻	权限 ✿	子账号 \$	资产数 🛈 🗲	
数据更新 账号名称 ▼	添加或管理成员账号 【 账号ID/APPID	添加多云账号 身份 ③ ▼	所属部门 🔻	加入集团方式 ① 👅	权限 ◆	子账号 ✿	资产数 ① 🕈	
数据更新 账号名称 ▼ ②	添加或管理成员账号 C 账号ID/APPID	添加多云账号 身份 ③ ▼	所属部门 🍸	加入集团方式 ① 🔻	权限 ◆	子账号 \$	资产数 ① \$	

管理员子账号登录

耒 团账号概况								
						主账号		
管理员账号名称	管理员账号ID 多云	、混合云账号接入	云账号			个 管理品/委派管理	日	
主账号 子则	胀号							
主账号 子贝		沃加文于叱己						
主账号 子贩 数据更新	张号 添加或管理成员账号 【】	添加多云账号						
主账号 子り 数据更新 账号名称 Y	胀号 添加或管理成员账号 ^{【2} 账号ID/APPID	添加多云账号 身份 ③ ▼	所属部门 ▼	加入集团方式 ① ▼	权限 ◆	子账号 \$	资产数 ① \$	
主账号 子り 数据更新 账号名称 T	张号 添加或管理成员账号 『 账号ID/APPID	添加多云账号 身份 ③ ▼	所属部门 ▼	加入集团方式 🕄 🔻	权限 ◆	子账号 \$	资产数 ① 💲	
主账号 子師 数据更新 账号名称 ▼	K号 添加或管理成员账号 C 账号ID/APPID	添加多云账号 身份 ④ ▼	所属部门 🍸	加入集团方式 ① 🝸	权限 ✿	子账号 ◆	资产数 ① \$	
 主账号 子り 数据更新 账号名称▼ 公 	K号 添加或管理成员账号 【 账号ID/APPID	添加多云账号 身份 ③ ▼	所属部门 👅	加入集团方式 🛈 🍸	权限 \$	子账号 \$	资产数 ① \$	
 主账号 子師 数据更新 账号名称 ▼ ② 	K号 添加或管理成员账号 C 账号ID/APPID	添加多云账号 身份 ④ ▼	所属部门 ▼	加入集团方式 ① 👅	权限 ◆	子账号 \$	资产数 ① \$	

成员主账号、子账号登录



多云多账号管理				
集团账号概况			士配具	-
管理员账号名称	管理员账号ID	多云、混合云账号接入	个 管理员/委派管理员	

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。

⁼中心						
∩ (0) Ø	■ 接入多云资产					
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
\uparrow	\uparrow		۲			
未防护主机	未防护公网IP 1	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				
~	~	^				
					1	
		新悦 口看核心 口看去防护				
🗄 按资产分组	◎ び 按服劳失空 只有					
主 按资产分组 日 按资产类型 主机资产 容器资产		域名资产 网络资产	数据库资产	其他云资源		
三 按资产分组 田 按资产类型 主机资产 容器资产 标记为核心资产 标记为	① 按成为关望 入有 公网IP资产 書除	域名资产 网络资产	数据库资产	其他云资源		
 	 	域名资产 风省资产 资源标签	数据库资产	其他云资源 关联实例ID/名称	关联实	列类型 ▼
 	 · 仅服为实业 · 人類 · 人 · 人 · 人	域名资产 八百人的 资源标签	数据库资产 地域 ▼	其他云资源 关联实例ID/名称	关联实	列类型 ▼

漏洞与风险中心

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



产风险概况	0			重新检测 详情 ~			
漏洞风险		端口风险	551	口令风险	风险趋势		
	$\hat{\mathbf{r}}$	\uparrow		\uparrow	漏洞风险		
高危		高危	高加	危	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	云资源配置风险	and the second sec	
\uparrow		\uparrow		\uparrow	风险服务暴露		
高危		高危	高)	危			

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。

E 14 作业						
安全体检任务				安全体检任务	执行记录	
体检任务 / 总配额 访	已用体检次数 / 总配额			体检开始时间		体检名称
\uparrow		次				
周期任务 个 进行中0个	升级购买配额 查看报告					
创建安全体检任务 停止任务	删除 全部执行情况 ▼					
 创建安全体检任务 停止任务 任务ID/名称 任务类型 ▼ 	全部执行情况 ▼ 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	体检模式 ▼

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								
报告概况 报告数量 个 待查看 个	报告欄板 个 前往创建					报告下载	己录 印 任务名称	报告类型
报告下载 报告模板 一键下载								
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 🕈	
		体检报告						

四、常见问题

多账号管理之后的计费标准?

未来新版云安全中心的计费标准请实时关注产品动态。

存量用户的数据情况

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

如何实现多账号管理,是否需要调整网络架构?

安全产品的系统层数据上打通以实现多账号管理,不需要调整网络架构。

使用过程中,有问题如何联系?

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



模拟攻击

最近更新时间:2024-08-02 10:14:18

功能背景

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

应用场景

高效的渗透化测试

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

准确对比安全防护产品可靠性

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

安装模拟攻击工具包

步骤一:查询资产对应工具包安装状态

1. 登录 云安全中心控制台, 在左侧导览中, 单击资产中心。

2. 在资产中心页面,选择**主机资产**,查看该资产的模拟工具包安装状态。



资产中心				
资产更新	🛛 😅 🔳 接入多云资产			
资产统计概况				
主机资产 () 不 未防护主 风险主机	公阿IP资产 个 未防护公网I 风险公网IP	域名资产 个 未防护 风险域:	✓ 主机资产监控 - - - Obps	容器资产监控
容器资产	网关资产 个	数据库资产	- Obps - Obps - Obps	
三技资产分组	交资产类型 ① 按服务类型	日本 日	末防护	多个关键字用竖线 " "
主机资产(39) 容	器资产(351) 公网IP资产(58)	域名资产(5) 网络资产(52	23) 数据库资产(0) 其他云	资源(127)
开启防护标记	防核心资产标记为非核心资产			
资产实例ID/名称	IP地址 ▼	资源标签	资产类型 ▼	地门防护状态 🔻
	公网: 内网:	核心资产	CVM	广: • 未安装

步骤二:安装模拟攻击工具包

针对未安装模拟攻击工具包的资产,可参照以下三个安装方式进行安装:

方式1:手动执行命令

登录目标服务器后执行对应命令下载、运行模拟攻击工具包。

方式2:通过腾讯云自动化助手执行命令下载并运行模拟攻击工具包

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

方式3:通过主机安全 Agent 执行命令下载并运行模拟攻击工具包

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

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

注意:

当前暂仅支持腾讯云内操作系统为 Linux 系统的服务器。



资产总览		资产	列表			服务梳理			
网络结构 资源标签	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	Web服务			
全部防护状态 🔹	全部失陷状态 ▼ 全部	的建时间 🔻		多个关键字用	竖线 " " 分隔,多个过滤标题	密用回车键分隔	Q,	τ¢¢	櫗
资产实例ID/名称 ▼	IP地址 ▼	资产类型 ▼	地域 🔻	所属子网	所属私有网络 ▼	资源标图主机安全防	护	模拟攻击工具	包
	公网:	联闭二眼友	L Vie	s	4u			- + 수생	
	内网: 1	增加/24加25	工内	D	;	• 茎虹版木	19/31/14	• 木文表	
i.	公网:		2 111	s					
ti	内网: '	腾讯云服务…	7 211	N		• 基础版末	地方护	 禾安装 	

步骤三:如何高效的渗透化测试

查看渗透测试剧本

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



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



吹击剧本概況 張近吹击: 2024-07-19 15:51:57 模拟攻击资产① 模拟攻击战术 战技 ・ ・ ・ ・ ・	● 攻; ● 攻; ● 攻;
· · · · · · · · · · · · · · ·	● 攻; ● 攻; ● 攻;
中 自定义風本1 中 大安装工具包资产 大安装工具包资产 中 大安装工具包资产 大安装工具包资产 大安装工具包资产 大安装工具包资产 大安装工具包资产 大安装工具包资产 大安装工具包资产 大安装工具包资产 大安装工具包资产 大安装工具包资产 大安装工具名资产 大安装工具名资产 大安装工具名、 大安装工具 大安美工具 大安美工 大安美工	● 次: ● 攻:
自定义劇本1 未安装工具包资产 攻击剧本 攻击记录 全部劇本内容 攻击战技: 引导或登录自动启动执行 关联劇本 4 位際目标 3 風本 上获得更高级别的特权。操作系统问能具有在系统启动或登录期间自动执行程序,以保持持久性或在受感染系统上获得更高级别的特权。操作系统可能具有在系统启动或登录期间自动执行程序,以保持持久性或在受感染系统的影响。这些机制可能包括自动机均特化。操作系统可能具有在系统启动或帐户登录时自动运行程序的机制。这些机制可能包括自动机均特化。操作系统可能是有在系统启动或登录期间自动执行程序,或者由存储配置信息的存储库引用,例如 权限提表	• 攻:
攻击剧本 攻击记录 全部剧本内容 全部剧本内容 位原目标 3 副本 2/10战技 攻击者可能会将系统设置配置为在系统启动或登录期间自动执行程序,以保持持久性或在受感染系统上获得更高级别的特权。操作系统可能具有在系统启动或帐户登录时自动运行程序的机制。这些机制可能包括自动执行程序,这些性参位于专门指定的目录中,或者由存储配置信息的存储库引用,例如	
攻击剧本 攻击记录 全部副本内容 女部副本内容 女击战技: 引导或登录自动启动执行 关联剧本 4 侦察目标 3 副本 2/10战技 双比技技: 引导或登录自动启动执行 关联剧本 4 0 政力 2/10战技 0	
全部劇本内容 攻击战技:引导或登录自动启动执行 关联剧本 4 侦察目标 3 副本 2/10战技 攻击者可能会将系统设置配置为在系统启动或登录期间自动执行程序,以保持持久性或在受感染系统上获得更高级别的特权。操作系统可能具有在系统启动或帐户登录时自动运行程序的机制,这些机制可能包括自动执行程序,这些程序位于专门指定的目录中,或者由存储配置信息的存储库引用,例如 8/13战	
全部剧本内容 攻击战技:引导或登录自动启动执行 关联剧本 4 侦察目标 3 刷本 达技描述 攻击者可能会将系统设置配置为在系统启动或登录期间自动执行程序,以保持持久性或在受感染系统 上获得更高级别的特权。操作系统可能具有在系统启动或帐户登录时自动运行程序的机制。这些机制 权限提 8 刷 2/10战技 可能包括自动执行程序,这些程序位于专门指定的目录中,或者由存储配置信息的存储库引用,例如 8/13战	
侦察目标 政士者可能会将系统设置配置为在系统启动或登录期间自动执行程序,以保持持久性或在受感染系统 权限提 3 副本 上获得更高级别的特权。操作系统可能具有在系统启动或帐户登录时自动运行程序的机制。这些机制 8 副 2/10战技 可能包括自动执行程序,这些程序位于专门指定的目录中,或者由存储配置信息的存储库引用,例如 8/13战	多个
3 副本 上获得更高级别的特权。操作系统可能具有在系统启动或做产登录时自动运行程序的机制。这些机制 8 副 2/10战技 可能包括自动执行程序,这些程序位于专门指定的目录中,或者由存储配置信息的存储库引用,例如 8/13战	提升
2/10战技 可能包括目动现行程序,这些程序位于专门指定时目录中,或者由存储和宣信息的存储库引用,例如 8/13战	∥本
Willows 注册表。对于可以通过修改现象使我的功能未实现们同时目标。	肢
主动扫描(2) 子战技 注册表运行键/启动文件夹、身份验证包、时间提供者、Winlogon Helper DLL、安全支持提供商、内 (4)	是升控制机制
核模块和扩展、重新打开的应用程序、LSASS 驱动程序、快捷键修改、端口监视器、打印处理器、 收集受害者≠ XDG 自动启动条目、活动设置、登录项	
(1) 关联剧本	令牌操作
模拟攻击剧本名称 关联子战技 操作 引导率	或登录自动启动
○ 加載中	4)
收集受害者网 共0项 5 √ 条/页 № 4 1 /1页 ▶ № (3)	
	或登录初始化關

1. 在模拟攻击页面,选择一个或多个剧本后,单击**开始模拟攻击**。



	攻击剧本	攻击记录						
	开始模拟	以攻击 自定义剧本	は別除				多个关键字用]竖线 "J" 分隔,
	MITRE AT	T&CK 框架						
	() () () () () () () () () () () () () (● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	▲ ▶ 2 → 丸行攻击		8) 合 9) 分 防御绕过	5 5 受け 5	また、 構 向 移 动	▶ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
		模拟攻击剧本名称	剧本来源 了	服务器攻击动作	网络攻击	动作	关联告警数 🚦	执行次数列
		-	自定义剧本	战术: 资i 战技: 开;	请求 项 URI: 项 请求 请求		0	❷ 成功 🧧
			马 系统默认剧本	战术: 资 战技: 开;	项 		0	☞ 成功 🛛 🧧
2 . 在执	口模拟功	文击剧本弹窗中,	系统默认剧本 选定此次模拟攻击	^{战术:资} ^{战技:开 占的资产范围,}	^项 项 勾选承诺许可后	,单击 确定 。	0	☞ 成功 🛛 🧧

说明:

仅可对已安装工具包的资产执行模拟攻击剧本。

执行模拟攻击剧	· · · · · · · · · · · · · · · · · · ·
模拟攻击剧本	Python base64命令攻击等 2 个剧本
模拟攻击范围 🛈	 ○ 从现有资产选择 ○ 剔除资产 全部资产(738) 选择资产(0)
 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	

查看剧本模拟攻击记录

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


模	拟攻击							
	攻击剧	本概况 最近攻击:2024-0	7-19 15:51:57				模拟攻击记录	
L	模拟攻	击剧本 个 刷本	可模拟攻击资产 () 个 未安装工具包资产	模拟攻	击战术 战技	^	攻击次数	 攻击中止 攻击成功 攻击异常
	攻击層	则本 攻击记录						
	重新	攻击 停止攻击	全部状态 >					多个关键字用竖线 " " 分隔
		攻击时间 🚦	攻击剧本	服务器攻击动作		网络攻击动作	攻击资产	\$ 攻击结果
		2024-(战术: 资源开发等 战技: 开发能力等	项	请求方 URI: / 请求头 请求体	1	<mark>⑦</mark> 兆 失败 4-
		2024-(战术: 资源开发等 战技: 开发能力等	项	请求方 URI: / 请求头 请求体	1	▽ ½ 中止 4-

步骤四:如何准确对比安全防护产品可靠性

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

常见问题

为何安装模拟攻击工具包失败?

防火墙拦截:建议防火墙策略放过云安全中心后台服务器访问地址,公网域名 bas.tencentcs.com、csc-

1300616671.cos.ap-guangzhou.myqcloud.com, 公网端口8001、443。

网络问题:建议检查网络连接是否正常,尝试使用其他网络。模拟攻击工具包需要从互联网下载文件,如果网络不 稳定或者下载速度过慢,可能会导致安装失败。

权限问题:建议使用管理员账户登录系统,或者使用"以管理员身份运行"选项下载/运行模拟攻击工具包。下载/运行 模拟攻击工具包需要管理员权限,如果当前用户没有足够的权限,可能会导致安装失败。

系统兼容性问题:查看模拟攻击工具包的系统要求,确保当前操作系统和其他软件版本符合要求。模拟攻击工具包 可能不兼容当前操作系统或其他软件,导致运行失败。

系统默认剧本依据来源是?



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

系统默认剧本(持续更新)

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



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



日志投递(支持多账号多产品多日志)

最近更新时间:2024-08-12 17:28:05

功能背景

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

应用场景

日志存储

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

离线分析

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

日志投递至 Kafka

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

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

Ckafka 公网域名接入

1. 登录云安全中心控制台,在左侧导览中,单击日志分析。

2. 在日志分析页面,单击日志投递 > 投递至 kafka。

3. 在投递至 kafka页面,云安全中心自动获取账号的腾讯云消息队列 Ckafka 实例、已接入云安全中心的日志来源,选择 Ckafka 公网域名接入,配置相关参数。



日志投递				
投递至kafka 投递到	ĒCLS			前往消息队列控制。
 1. 购买消息队列 2. 根据消息队列 3. 按照本页面中 	JCkafka实例,推荐按照需要投递的日志量来选 JCkafka文档指引,开通白名单实现公网域名接 P以下指引完成日志投递配置,仅支持使用同一;	购对应Ckafka实例规格 入或支撑环境接入 肖息队列用户进行投递		×
配置消息队列				
网络接入方式	○ Ckafka公网域名接入 Ckafka支撑功	际境接入 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 🖌 🗸			
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()	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
● 新憎日志投递配置				

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。
操作	新增:单击 新增日志投递配置 ,支持新增多个日志来源。 删除:单击目标日志操作列的 删除 ,经过二次确认后,支持删除该日志来源对应日志类型 的日志投递任务。 编辑:如非首次配置日志投递,则支持在日志投递页面,单击 修改配置 ,修改相关日志投 递。

4. 确认无误后,单击确定,即可将采集到的日志投递至对应的消息队列。

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

日志投递					修改函
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				
日志来源	日志类型	账号来源	Topicld	1/名称 ()	投递状态
云防火墙	访问控制日志、零信任防护日志				正常
Web应用防火墙	攻击日志、访问日志				正常
主机安全	入侵检测日志、客户端相关日志				正常

Ckafka 支撑环境接入

1. 登录云安全中心控制台,在左侧导览中,单击日志分析。

2. 在日志分析页面,单击日志投递 > 投递至 kafka。

3. 在投递至 kafka 页面,云安全中心自动获取账号的腾讯云消息队列 Ckafka 实例、已接入云安全中心的日志来源,选择 Ckafka 支撑环境接入,配置相关参数。



投递至kafka	投递至CLS						前
 1.购买 2.根据 3.按照 	肖息队列Ckafka实例 肖息队列Ckafka文档 本页面中以下指引完	」,推荐按照需要投递的 错引,开通白名单实现 成日志投递配置,仅3	的日志量来选购X 见公网域名接入3 5持使用同一消息	寸应Ckafka实例规格 载支撑环境接入 即队列用户进行投递			
配置消息队列							
网络接入方式	Ckafk	a公网域名接入 🛛 🔾	Ckafka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		× C				
支撑环境接入 配置日志投递	请选择		~				
支撑环境接入 配置日志投递 日志来源	请选择	日志类型	~	账号来源		Topic ID/名称()	
支撑环境接入 配置日志投递 日志来源 云防火墙	请选择	日志类型 全部日志类型	~	账号来源 全部账号	~	Topic ID/名称 () 请选择Topic名称	~
 支撑环境接入 配置日志投递 日志来源 云防火墙 Web应用防火 	· 清选择 文 墙 、	日志类型 全部日志类型 全部日志类型	 <td>账号来源 全部账号 全部账号</td><td>~</td><td>Topic ID/名称 () 请选择Topic名称 请选择Topic名称</td><td>~</td>	账号来源 全部账号 全部账号	~	Topic ID/名称 () 请选择Topic名称 请选择Topic名称	~
 支撑环境接入 配置日志投递 日志来源 云防火墙 Web应用防火 主机安全 	请选择	日志类型 全部日志类型 全部日志类型 全部日志类型	 <	账号来源 全部账号 全部账号 全部账号	~	Topic ID/名称 () 请选择Topic名称 请选择Topic名称 请选择Topic名称	~ ~
 支撑环境接入 配置日志投递 日志来源 云防火墙 Web应用防火 主机安全 云安全中心 	请选择 ////////////////////////////////////	日志类型 全部日志类型 全部日志类型 全部日志类型 全部日志类型	 <	账号来源 全部账号 全部账号 全部账号 全部账号	× ×	Topic ID/名称 ① 请选择Topic名称 请选择Topic名称 请选择Topic名称 请选择Topic名称	× × ×
 支撑环境接入 配置日志投递 日志来源 云防火墙 Web应用防火 主机安全 云安全中心 云审计 	请选择 /* /* /* /* /* /* /* /* /* /* /* /* /* /* /* /* /*	日志类型 全部日志类型 全部日志类型 全部日志类型 全部日志类型	 <	账号来源 全部账号 全部账号 全部账号 全部账号 全部账号 全部账号	× × ×	Topic ID/名称 ① 请选择Topic名称 请选择Topic名称 请选择Topic名称 请选择Topic名称	· ·
 支撑环境接入 配置日志投递 日志来源 云防火墙 Web应用防火 主机安全 云安全中心 云审计 ④新増日志投递 		日志类型 全部日志类型 全部日志类型 全部日志类型 全部日志类型	 <	账号来源 全部账号 全部账号 全部账号 全部账号 全部账号 全部账号		Topic ID/名称 ① 请选择Topic名称 请选择Topic名称 请选择Topic名称 请选择Topic名称	 * * * * * * *

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



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

4. 确认无误后,单击确定,即可将采集到的日志投递至对应的消息队列。

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



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。

 2. 根据消息队 3. 按照本页面 	列Ckafka文档拍 i中以下指引完成	皆引,开通白名单实现公(成日志投递配置,仅支持(网域名接入或支撑环境 更用同一消息队列用户	中进行投递		
配置消息队列						
网络接入方式	Ckafka	公网域名接入 🔷 Cka	ika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 🛈	请输入用	户名				
周户名 () 请输入用户名						
密码	请输入密	码				
密码 配置日志投递 日志来源	请输入密	码	账号来	源		Topic名称(i)
密码 配置日志投递 日志来源 云防火墙	「「「「「」」」、「「」」、「」」、「」、「」、「」、「」、「」、「」、「」、「	日志类型 全部日志类型	账号来	源	~	Topic名称 (i) 请输入Topic名
密码 配置日志投递 日志来源 云防火墙 Web应用防火墙	请输入密	码 日志类型 全部日志类型 全部日志类型	账号来 金金 <p< td=""><td>源 账号</td><td>~</td><td>Topic名称 (i) 请输入Topic名 请输入Topic名</td></p<>	源 账号	~	Topic名称 (i) 请输入Topic名 请输入Topic名
密码 配置日志投递 日志来源 云防火墙 Web应用防火墙 主机安全	请输入密	码 日志类型 全部日志类型 全部日志类型 全部日志类型	 账号来 全部 全部 全部 全部 	源 账号 账号	~	Topic名称 () 请输入Topic名 请输入Topic名 请输入Topic名
密码 配置日志投递 日志来源 云防火墙 Web应用防火墙 主机安全 云安全中心	 请输入密 <l< td=""><td>日志类型 全部日志类型 全部日志类型 全部日志类型 全部日志类型</td><td> 株号来 全部 全部 全部 全部 全部 全部 </td><td>源 账号 账号 账号</td><td></td><td>Topic名称) 请输入Topic名) 请输入Topic名) 请输入Topic名) 请输入Topic名)</td></l<>	日志类型 全部日志类型 全部日志类型 全部日志类型 全部日志类型	 株号来 全部 全部 全部 全部 全部 全部 	源 账号 账号 账号		Topic名称) 请输入Topic名) 请输入Topic名) 请输入Topic名) 请输入Topic名)



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

4. 确认无误后,单击确定,即可将采集到的日志投递至对应的消息队列。

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

日志投递						修改
消息队列详情						
接入方式 其他Kafka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						
日志来源	日志类型	账号来源	т	opic名称()		投递状态
云防火墙	入侵防御日志、流量日志、操作					正常

日志投递至 CLS



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

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

投递至CLS
CLS (日志服务) • 已开通
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 务中创建后付费的存储空间,同时也会生成后付费账单。CL <mark>S计费详情 </mark>
F通日志服务 > 2 配置日志投递
<mark>没递</mark> 了。

说明:

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

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



投递账号 投递所属账号 投递内容 日志来源 日志来源账号 日志来源账号 日志未源账号 日本地域 日志集操作 日志集	请选择账号 请选择日志来源 请选择日志类型 请选择目标地域 请选择目标地域	● 创建日志集	▼ ▼ ▼		
投递所属账号 投递内容 日志来源 日志米源账号 日志未源账号 日志未源账号 日志未源账号 日本地域 日志集操作 日志集	请选择日志来源 请选择日志类型 请选择目标地域 请选择目标地域	● 创建日志集	▼ ▼ ▼		
投递内容 日志来源 日志、業型 日志、来源账号 投递目标 ③ 目标地域 日志集操作 日志集 	请选择日志来源 请选择日志类型 请选择目标地域 选择已有日志集	● 创建日志集	▼ ▼ ▼		
日志来源 日志类型 日志来源账号 投递目标 ① 目标地域 日志集操作 日志集	请选择日志来源 请选择日志类型 请选择目标地域 选择已有日志集	• 创建日志集	•		
日志类型 日志来源账号 投递目标 ① 目标地域 日志集操作 日志集	请选择日志类型 请选择 请选择目标地域 选择已有日志集	• 创建日志集	▼ ▼		
日志来源账号 投递目标 ① 目标地域 日志集操作 日志集	请选择 请选择目标地域 选择已有日志集	• 创建日志集	•		
投递目标 ① 目标地域 日志集操作 日志集	请选择目标地域 选择已有日志集	• 创建日志集	▼		
目标地域 日志集操作 日志集 日志生	请选择目标地域 选择已有日志集	• 创建日志集	~		
日志集操作 日志集	选择已有日志集	● 创建日志集			
日志集	連続)ロ士佳夕秒				
口去主師場作	<u> </u> 八口心未つ				
	选择已有日志主题	🔵 创建日志主题			
日志主题	请输入日志主题名称				
确定	取消				



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

3. 确认无误后,单击确定,即可将采集到的日志投递至对应的日志主题。

4. 在日志投递页面,支持查看账号名称/ID、所属部门,以及日志来源、日志类型、来源账号(多账号下)、日志主题、投递状态、投递开关等信息,并且允许编辑已投递任务、(批量)删除任务、(批量)开启/关闭任务、(批量)刷新、日志检索。



日志投递	弟					
投递至k	afka 投递至C	CLS				
投递账号	号信息					
账号名称	/ID					
所属部门						
日志投诉	递详情					
新增持	殳递 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 ()	投递状态	投
	Web应用防…	多个 (2)	多个 (15)		● 正常	(
共1项					10 ▼ 条 / 页	M .

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				多则
日志概况				
接入日志源	日志投递 0 个	已使用日志容量 GB / TB 前往扩容	日志趋势	近7天 >
配置日志接入	日志投递	■ 主机安全 ■ 云防火墙 ■ 云审计 ■ 云安全中心 ■ 其他	07-14	07-16

3. 在多账号管理页面,选择所需账号,单击确定。



请输入账号名称/账号ID进行搜索		Q
- 账号名称	账号ID/APPID	所属部门 ▼
✓ 🙆		Poot
✓ 🙆		
<mark>√</mark> ⊗		
any .		JSE
ans.		36:
	1	
	确定 取消	

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



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

单账号管理

仅支持对当前账号进行多产品日志投递。

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

注意:

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

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

常见问题

日志投递如何收费?

日志投递为云安全中心旗舰版专属,可前往购买日志投递。

公网日志投递出口 IP 白名单





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



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

日志投递支持哪些产品哪些日志类型?

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



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



资产中心

最近更新时间:2024-08-02 10:14:18

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

资产类型	资产详情
	云服务器 CVM
宁 扣次立	非腾讯云服务器
土机页)	轻量应用服务器 Lighthouse
	边缘计算器
	容器
	本地镜像
<u> </u>	仓库镜像
谷硷贝)	主机节点
	集群
	Pod
	IP
	高可用虚拟 IP
小网 ID 资产	弹性公网 IP
	非腾讯云 IP
	弹性 ipv6
	anycast IP
樹夕迩立	域名
	非腾讯云上域名
网络资产-网关	NAT 网关
	VPN 网关



	负载均衡 CLB
	NAT 防火墙
	探针
网络资产-网卡	弹性网卡
利右网纹	私有网络 VPC
127 H 10151	子网
	云数据库 MySQL
	云数据库 Redis
云数据库	云数据库 MariaDB
	云数据库 PostgreSQL
	云数据库 MongoDB
	云硬盘 CBS
	对象存储 COS
其他云资源	文件存储
	消息队列
	Elasticsearch Service

更新资产

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

说明:

资产更新可以自动同步腾讯云上的资产,非腾讯云上资产,请参见添加云外资产。





搜索资产

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

	三 按资产分组	〕 按服务类型	只看核心 只看未防法	À SA	关键字用竖线 "!" 分隔,	多个
	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(0) 其	其他云资源()	
	开启防护标记为核心资产	标记为非核心资产				
	资产实例ID/名称	IP地址 ▼	资源标签	资产类型	防护状态 🔻	所履
		公网: 1 内网: 1	核心资产	CVM	• 未安装	හ
		公网: 1 内网: 1	核心资产	CVM	•已防护	හි
在资产中	心页面 ,支持在网络结构的礼	视角,查询每个地域下,	分别有哪些 VPC,	每个 VPC 内分别不	有哪些资产。	



■ 按资产分组 目 按资产类组	型 ① 按服务类型					
网络结构 资源标签						
网络结构					多个关键字用竖线" "分隔,	多个过
▼ 全部资产	资产实例ID/名称	IP地址	资产类型	地域 🔻	所属私有网络	端口
▶ 中国香港		公网: 内网:	- 公网资产	广州		1
▶ 北京 ▶ 新加坡		公网:) 内网:	- 公网资产	广州		1

标记核心资产

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

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

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
主机资产	容器资产()	公网IP资产()	城名资产(网络资产()	数据库资产 其他云资源()
开启防护	記为核心资产	标记为非核心资产		
资产实例ID/名	称	Ⅳ地址 ▼	资源标签	资产类型 防护状态 🕇
	ГС Э	公网: 内网:	5 Ta - 🖍	CVM • 未安装
		公网: 内网:	核心资产	CVM •未安装

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。



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	₹ <u>≁</u>	其他云资源(1	
开启防护	标记为核心资产	标记为非核心资产							
资产实例	ID/名称	IP地址 ▼		资源标签			资产类型	防护状态 ▼	所
	< T <u>n</u>	公网: 内网:	Ē	核心资产	- /		CVM	• 未安装	ø
		公网: 内网: -		核心资产	æ		CVM	• 已防护	Ø

在资产中心页面,可以筛选关注核心/非核心资产。云安全中心会自动同步展示资产的防护情况,对应关系为: 主机资产,使用腾讯云主机安全防护。

IP 资产,使用腾讯云防火墙防护。

域名资产,使用腾讯云 Web 应用防火墙防护。

说明:

我们建议您关注自己的核心资产,确保核心资产都得到防护。

添加自定义资产标签

1. 在 资产中心页面, 选择目标资产, 单击资源标签列下的



2. 在编辑标签弹窗中,选择标签键和标签值,单击确定。



(i) 编 •	辑须知						
	际金用于从不同: 前往 <mark>标签管理</mark> [進度对资源 1	分类管理。如	现有标签不符	合您的	要求,请	
已选择 1 个	资源						
标签键		▼	蒁値		•	×	
+ 添加 (>> 键值粘贴板						

3. 添加标签后,单击资源标签,可以按照自定义标签分类查看资产。

添加云外资产

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





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

如需添加云外资产,请提交工单联系我们。

请勿添加非本账号所有的资产,如使用他人资产将由本账号归属企业承担法律责任。



手动添加资产	2 × X
● 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.	
请輸入公网IP地址、Web网站域名、API均 最多支持输入1000行,外部复制粘贴多个 地址,若输入重复IP,后台将自动合并	洺,手动输入使用回车换行,每行一个; 地址,请用英文逗号","分隔;不支持CIDR
承诺添加资产归本账号所属企业所有,如使用他/ 查看详情	\资产将由本账号归属企业承担法律责任
确定	反消

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。



请输入账号名称/账号D进行搜索 所居部门 ▼ ● ●		多账号	管理 t	.等4个账号 ▼
账号名称 账号ID/APPID 所展部门▼ ○ 1 1 1 1	请输入账号名称/账号ID进行搜索			Q,
	— 账号名称	账号ID/APPID	所属部门 🔻	
	🔽 🙆 t	2 1	I	
	✓ Ø (2 1	3	
	✓ Ø:	2 1	(
		е 3	h (
	<u>805</u>	ε 7	3	
			(



安全体检 功能简介

最近更新时间:2023-09-21 17:32:10

功能背景

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

应用场景

日常安全体检

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

功能详情

体检项目

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



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

说明:

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

体检资产

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

注意:

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

体检消耗

体检资产	体检项目	消耗体检配额
公网 IP、域名资产	漏洞、弱口令、网站内容风险	
 云服务器、负载均衡、 MySQL、Redis、 MariaDB、PostgreSQL、 MongoDB、Elasticsearch Service、对象存储 COS 	云资源配置风险	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	V	V
应急漏洞	V	V	V	V
漏洞风险	-	V	Ń	V
弱口令风险	-	V	\checkmark	V
云资源配置风险	-	V	V	V
风险服务暴露	-	-	\checkmark	V
网站内容风险	-	-	Ń	V
体检配额	20次	400次/月,可扩 展	1200次/月,可扩 展	4800次/月,可扩展
任务配额	1个	10个	20个	50个,可扩展至不 限制

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



云安全中心

操作指引

最近更新时间:2023-09-21 17:32:59

安全体检入口

安全体检

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

Health check tasks		Health check history	
Task quota (Used/Total) (Health check quota (Used/Total)	Start time	Task na
- 196	Upgrade	A REPORT OF	- 19 M
Scheduled checks In progress	View report	1.00	- 10 K

总览体检

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

立体防护-应急漏洞

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

单个应急漏洞限免2次扫描。

创建任务

1. 登录 云安全中心控制台,在左侧导览中,单击**体检任务**。

- 2. 在体检任务页面,单击创建任务。
- 3. 在创建资产体检任务弹窗中, 配置相关参数, 单击确定。



Create task (i)		≗ ×
Task name 🛈	104103-001	(Called
Mode	Basic O Standard Adv	anced 🖾
Plan 🛈	Immediate Specified time Daily	O Scheduled checks
Included assets	 All assets (1) Select from Import Exclude assets (0) 	existing O Manual input
Check items 🛈	 Port risks (i) Weak passwords (i) Configuration risks (i) 	 Vulnerabilities (i) Content risks (i) Exposed risk services (i)
Estimated duration	minutes	
Quota usage 🛈		
Agree to Health	Check Authorization Agreement. View ledge that the assets to check are on shall bear the legal responsibility for the OK Can	v details wned by current enterprise account. The unauthorized usage of the assets. cel

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



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

编辑报告

1. 登录 云安全中心控制台, 在左侧导览中, 单击体检任务。

2. 在体检任务页面,选择目标任务,单击**编辑**。

注意:

不支持编辑立即执行的任务、待开始的非周期任务、正在进行中的周期和定时任务。

	Task ID/name	Plan T	Included \$	Check items ▼	Start time \$	Estimated dura	Task status	Reports	Mode T
	100			1997 - S. 1997 -	1990 - A.	19 A.	Continues of		12
	10	10.00		1948	in a second	1.1	10.0		10

3. 在编辑资产体检任务弹窗中,修改相关参数,单击确定。



Edit task 🛈		≥ ×
Task name 🛈		
Mode	Basic O Standard A	dvanced 🔼
Plan 🛈	Immediate Specified tin	ne O Scheduled checks
	Daily 🔻	D
Included assets	All assets O Select fro	om existing O Manual input
	Select assets All assets	
Check items 🛈	✓ Port risks (i)	Vulnerabilities (j
	Veak passwords (j)	Content risks (i)
	Configuration risks	✓ Exposed risk services (j)
Estimated duration	minutes	
Quota usage 🛈	All the second sec	

删除任务

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


Task ID/name	Plan T	Included \$	Check items ▼	Start time \$	Estimated dura	Task status	Reports	Mode ▼
	14 A		100	1.1	1.1	Citizen et al.		ч.
			1.21	100	1.00	100 m -		6.

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。

Download report				
Report name	Included assets \$	Risks ‡	Task ID/name	Generation time \$
 Alter Participation 				1.00
 Parts 1996 			Sec. 1.	1000

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**。

Dow	nload report				
	Report name	Included assets \$	Risks \$	Task ID/name	Generation time \$
	1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.			Station	C.C
	all shares and shares and			10 C	1.0

批量:选择一个或多个报告,单击左上角的下载报告。



Dov	wnload report				
	Report name	Included assets \$	Risks \$	Task ID/name	Generation time \$
	1.00			Witness .	
	This sector a		1. Alt	548	Sec. 2
				Sec. 19	1.1.1.1.
	Sector Sector				

多账号模式

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

编辑任务

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

删除任务

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



添加白名单 IP

最近更新时间:2024-08-02 10:14:18

本文档将为您详细介绍如何将腾讯云安全中心的监测 IP 加入到白名单。

操作场景

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

129.211.162.110

129.211.162.87

129.211.163.253

129.211.164.19

129.211.166.123

129.211.167.182

129.211.167.200

129.211.167.70

129.211.162.158

129.211.162.23

129.211.166.134

129.211.167.108

129.211.167.181

129.211.166.142

129.211.166.163

129.211.167.128

129.211.167.166

43.139.244.231

43.139.243.246

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

操作步骤

说明



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

已购买 Web 应用防火墙。

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

方式1:通过 IP 查询添加白名单

1. 登录 Web 应用防火墙控制台,在左侧导航栏中,单击 IP 查询。

2. 在 IP 查询页面, 左上角选择需要防护的域名, 输入需要查询的 IP, 单击**查询**。

IP查询 ▼
IP查询 IP封堵状态
⑥ 在这里,你可以查询某个IP的封堵状态,是否在IP黑白名单中,是否触发了CC,自定义人机识别等
· 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	s	拦截
域名	lb	
生效时间	2024-	
结束时间	2024-	;
类别	1	
触发策略名称		
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。



翻 ○ 黑名单 ○ 白名单 ² 地址	翻 黑名单 ○ 白名单 ² 地址 ¹ ¹ ¹ ¹ ¹ ¹ ¹ ¹	翻 黑名单 ○ 白名单 ^{四地址} 家文生效 ▼	添加黑白IP			
P地址	P地址 說至时间• 永久生效 ▼	P地址 謀至时间• 永久生效 ▼ 备注	类别 〇	黑名单	白名单	
	截至时间 • 永久生效 ▼	截至时间• 永久生效 ▼ 备注	IP地址			
	截至时间• 永久生效 ▼	截至时间• 永久生效 ▼ 备注				
	截至时间• 永久生效 ▼	截至时间• 永久生效 ▼ 备注		2. <i>b. il. etc</i>		

5. 参数说明:

类别:选择**白名单**。

IP 地址:填写需要添加到白名单的地址。

截止时间:填写白名单有效期的截止时间。

备注:自定义描述。

方式2:直接添加 IP 白名单

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

手动添加白名单

1. 在 IP 白名单页面, 单击添加地址, 进入添加白名单页面。



黑白名单	!		Ę) 💌				
IP黑名单	IP白名单	精准白名单 规则白谷	3单				
沃加	1Hbtil-		导入粉探	日中全部签法结果		获取鼠标焦点即可选择过	浅屋性
				TUITHMARA			
	规则ID	IP地址	来源 ▼	截止时间	更新时间 \$	生效状态 ▼	备注
						1 已过期	无
共1项						50	▼ 条/页

^{2.} 在添加白名单页面, 配置相关参数, 单击确定。

添加白名单						
IP地址 *	支持任意IP地址,例如10.0.0.10或FF05::B5;支持CIDR格式地址,例如 10.0.0.0/16或FF05:B5::/60,使用换行符进行分隔,一次最多添加20个					
截止时间 *	○ 永久生效 ○ 限定日期	0				
限定日期 *	2024-07-30 09:47:40					
备注	请输入备注, 50个字符以内					

字段说明

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

说明

选择域名为 ALL 时, 添加的 IP 地址或 IP 段为全局的白名单。

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

截止时间:永久生效或限定日期。

备注:自定义,50个字符以内。

批量导入白名单



1. 在 IP 白名单页面,单击导入数据,将弹出"导入 IP 名单"窗口。

2. 在"导入 IP 名单"窗口中,单击导入,选择导入白名单文件,上传完成后,单击确认导入即可。

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

方式3:将已封堵 IP 添加白名单

1. 登录 Web 应用防火墙控制台,在左侧导航中,选择 IP 查询 > 封禁查询。

2. 在封禁查询页面,输入相关信息,单击**查询**,可以查询云安全中心的相关 IP 信息,即可对已封堵 IP 进行加白操 作。

IP查询 [№]			坂) 🔻			
IP查询 封禁查讨	甸					
*类型:	ALL		▼ 触发策略:	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	2024-07-23 09:37:00 ~ 2024-07-23 2:	3:59:59 💼	
查询	有效截止	时间: 2024-07	7-23 09:42:00 ~ 202	4-07-31 09:42:00		



热点问题

最近更新时间:2023-08-29 15:59:14

如何选购体检配额?

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

计算消耗体检配额公式

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

体检时间过长是否有异常?

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

体检任务被中止后是否还有报告生成?

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

体检任务异常是否会消耗体检、占用任务配额?

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

除了主机和容器之外,配置风险检测还包括哪些云资源的配置检测项?

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



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



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



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



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



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



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



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



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



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



时使用编程访问 与用户界面访问	防护			规范	同时开启,则可能导致一个账号的 暴露面增加,且可能导致机器账号 与人工账号混用,增加账号被恶意 使用的可能性。本检查项涉及的账 号信息同步可能存在延时,建议检 查间隔4小时以上。
具备高风险权限 的协作者应开启 登录保护	基础安全 防护	cam	高危	默认安全 规范	协作者账号不归属于您的账号管控 体系中,账号安全风险不可控,且 高权限协作者具有超级管理员权 限,如协作者账号泄露,您的云上 资产会面临非常高的安全风险,开 后登录保护后,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 后操作保护后,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	基础安全	cam	低危	默认安全	高权限子账号具有超级管理员的权



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



云安全中心

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



用户行为分析(UEBA)

最近更新时间:2024-08-02 10:14:18

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

功能特性

审计日志接入:通过多云多账户功能模块,可以获取云账户对应的用户列表和云外用户信息。通过操作审计日志,可以获取所有云用户的行为记录,并识别用户行为字段。此外,还能对云用户的操作行为和云 API 调用日志进行可 视化监控和实时审计。

风险检测:对AKSK 异常调用、高危接口调用、用户高危操作、未授权服务使用、权限提升等风险行为进行检测和 告警。同时,支持用户自定义启用或禁用检测规则,并自定义添加检测策略。

安全可视化:从异常行为和异常账号等方面展示近7天内检测到的风险数据,客户可以通过对比数据快速了解风险趋势,并及时进行风险管理。

用户概况

1. 登录 云安全中心控制台, 在左侧导览中, 单击用户行为分析(UEBA)。

2. 在用户行为分析(UEBA)页面,支持对您所有用户的行为分析,用户包括您的主账号、子账号、协作者。

用户行为管理				
用户概况			行为概况	
全部用户	云账号/用户	自定义用户 ①		暂无行为数据,请先接入云审计日志
92 ↑	92 ↑	O		① 云安全中心还没有接入云审计日志,无法提供用户行为概范数据,请前往日志分析页面完成云审计日志接入,
异常行为用户 0	子账号 91	配置自定义用户		

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。



自定义用户			×
日志类型	选择一个日志类型	•	
	还没有接入日志,前往 接入日志		
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)	•	
操作对象 🛈	请选择		
操作方式 🛈	请选择		
	确定取消		

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**。

暂无行为数据,请先接入云审计日志	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 立即接入		U	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 立即接入

3. 在接入日志源对话框中, 日志来源可选择操作和自定义日志来源。

说明:

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





日志样例

איבוקישערא, רדים גריין נה, איבויייטטנירגאיב

请输入目标解析文件的其他字段信息

样例解;

我们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

请先输入日志样例 ▼ 请选择

请选择时间戳格式



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



时间戳	选择日志样例及其对应的时间戳格式。	

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

行为概况							- Я	常行为(次)
发现异常行为								
0 ↑								
查看所有行为	05–06	05–07	05-08	05-09	05-09	05–10	05–11	05–12

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。

	添加的	黄略 删除策略					多个关键字用竖线 " " :	分隔,多个过濾标	签用回车键分隔
		策略ID/名称		策略类型 ▼	告警等级 🔻	策略内容		开关 🍸	命中次数 🤅 🛊
		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	了高危接口		0次
		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
		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	∄jaksk		0次
		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 敏感/存在安全隐患的接口列表	用户,高危操作指调用		0次
		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 内调用较少	高, 但是其在过去七天		0次
参数名	3称		说明						
策略I	D		系统默认	生成。					
策略名	名称		系统策略	由产品后台	定义;用户	自定义策略由用户定	定义。		
策略封	策略类型 包括系		包括系统	包括系统策略和自定义策略。					
上 藝 な			包括严重、	、高危、中	心 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	● 每10分钟 每小时 每天 每周 每月							
发生事件 〇 语句检索 〇 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							
课作力式 🛈								
数名称 说E	月							



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