

访问管理 实践教程





【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。



文档目录

实践教程 安全实践教程 授予标签下部分操作权限 使用 ADFS 进行用户 SSO 的示例 使用 OneLogin 进行角色 SSO 的示例 支持员工间资源隔离访问 概述 按照资源 ID 授权 按照标签授权 企业多账号权限管理 概述 集团账号 角色 协作者 查看员工腾讯云操作记录 使用 API 管理企业多账号权限 使用 ABAC 管理员工资源访问权限 ABAC 概述 应用场景 按标签鉴权时支持仅匹配标签键 创建资源时强制绑定固定标签键值 使用 MFA 保护 API 请求

实践教程 安全实践教程

最近更新时间:2025-04-1115:17:11

安全设置概述

在企业的实际应用场景中,随着业务的开展,账号下会有越来越多的资源,也会有不同部门、不同岗位的员工需要访问腾讯云,这让企业对资源的安全管理有了强 烈需求,需要建立安全、完善的资源控制体系。

- 不同岗位的员工分工不同,各司其职。
- 相同岗位的员工管理的资源可能不同。
- 员工对资源的访问方式多种多样,资源泄露风险高。
- 员工离开组织时,需要收回其对资源的访问权限。
- 员工账号使用情况需要进行回溯和审计。

通过访问管理 CAM,您可以统一分配账号权限、集中管控账号资源,遵循我们的安全设置建议,建立安全、完善的资源权限管理体系。

登录安全

1. 使用子账号访问腾讯云

请尽量不要使用主账号的身份凭证访问腾讯云,更不要将身份凭证共享给他人。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 <mark>用户类型</mark> 。

2. 使用组给子账号分配权限

按照工作职责定义好组,并给组分配相应的管理权限。然后把用户分配到对应的组里。这样,当您修改组的权限时,组里相关用户的权限随即发生变更。另外,当 组织架构发生调整时,只需要更新用户和组的关系即可。相关设置请参见 <mark>用户组</mark> 。

3. 使用不同的子账号管理用户、权限和资源

- 建议同一个子账号不同时管理用户、权限和资源。应该让部分子账号管理用户,部分子账号管理权限,部分子账号管理其他云资源。
- 不建议为一个 CAM 用户同时创建用于控制台操作的登录密码和用于 API 调用的访问密钥。具体如下:
 - 编程访问:只需要通过 API 访问资源,创建访问密钥即可。
 - 腾讯云控制台访问:只需要通过控制台操作资源,设置登录密码即可。

4. 使用子账号访问腾讯云

不要使用主账号的身份凭证访问腾讯云,更不要将身份凭证共享给他人。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 <mark>用户类型</mark> 。

5. 保护 CAM 用户凭证,以防止未经授权的使用

保护您的 CAM 用户凭证安全,防止未经授权的使用。请勿与任何人共享您的用户密码、MFA、访问密钥。

身份安全

1. 使用基于角色的访问控制

CAM 的角色是一种虚拟用户,与子账号、协作者或接收消息者这类实体用户不同。角色同样可被授予策略,使用基于角色的访问控制,根据实际场景进行合适的 角色分配。详情请参见 <mark>角色概述</mark> 。

腾讯云账号、产品服务、产品资源(例如工作负载、实例等)身份提供商等均可作为角色载体,角色并不是唯一地与某个账号绑定关联。角色没有关联的持久证书 (密码或访问密钥),主账号仅在申请角色时需要使用持久证书,在用户担任某个角色时,则会动态创建临时证书并为用户进行相应访问时提供该临时证书,即可 通过临时密钥签名调用腾讯云基础服务的开放 API 来访问用户的云资源。

2. 勿为根用户创建访问密钥

访问密钥允许您在命令行界面中运行命令或使用其中一个腾讯云 SDK 中的 API 操作。**强烈建议您不要为根用户创建访问密钥对**,因为根用户对账户中的所有腾 讯云服务和资源拥有完全访问权限,包括账单信息。

3. 降低特权账户的泄露风险



通过如下方式降低特权云账户的泄露风险:

- 具有减少访问权限的人数以降低恶意用户窃取的可能性,或合法用户误操作导致的泄露风险。
- 清除离职员工管理员账户。设置账户清除流程,在员工离开组织时禁用或删除管理员账户。
- 关键管理员账户,不允许执行生产任务(例如,浏览和电子邮件)的管理工作站。 保护管理员账户免受使用浏览和电子邮件的攻击途径的侵害。

4. 为用户开启 SSO 单点登录功能

开启 SSO 单点登录后,企业内部账号进行统一的身份认证,实现使用企业本地账号登录并访问腾讯云云资源。 相关信息请参见 用户 SSO 概述 。

5. 确保账户恢复机制可访问

请务必制定管理根用户凭证恢复机制的流程,以防在紧急情况(例如接管您的管理账户)下需要访问该机制。 确保您可以访问根用户电子邮件收件箱,以便可以重置丢失或忘记的 root 用户密码。相关设置请参见 重置登录密码 。

权限安全

1. 最小权限原则

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 CDN 服务的使用者,那么不需要将其他 服务的资源访问权限(如 COS 读写权限)授予给该用户。

2. 为 CAM 用户配置强密码策略

您可以通过 CAM 控制台设置密码策略,例如:密码长度、密码中必须包含元素等。如果允许 CAM 用户更改登录密码,则应该要求 CAM 用户创建强密码并且 定期轮换登录密码或访问密钥。

3. 不要为腾讯云主账号创建访问密钥

访问密钥用于 API 调用访问,登录密码用于控制台访问,两者具有同样的权限。由于主账号对名下资源有完全控制权限,为了避免因访问密钥泄露带来的安全风 险,不建议您为主账号创建访问密钥并使用该访问密钥进行日常工作。 您可以为 CAM 用户创建访问密钥,使用 CAM 用户进行日常工作。 相关操作请参见 子账号访问密钥管理。

4. 开启 MFA 保护

为增强账号安全性,建议您为所有账号绑定 MFA,为主账号及子账号都开启登录保护和敏感操作保护。对于支持邮箱登录或者微信登录的强烈推荐进行 MFA 二 次验证。开启 MFA 后,账号登录及敏感操作需进行二次校验。相关设置请参见 为协作者设置安全保护 、为子用户设置安全保护 。

5. 定期轮换身份凭证

建议您或 CAM 用户要定期轮换登录密码或云 API 密钥。这样可以让身份凭证泄露情况下的影响时间受限。

- 主账号密码设置请参见 账号密码。
- 子用户密码设置请参见 子用户重置密码。

密钥安全

1. 删除不需要的证书和权限

删除用户不需要的证书以及用户不再需要的权限。尽量减少访问凭证泄露后带来的安全风险。

2. 启用条件访问

云上用户可能会从任意位置访问云上资源。 因此需要确保这些访问符合安全性。 仅从用户身份认证角度关注是否可访问资源并不全面。还应考虑谁(身份)可以 且如何(条件)访问资源。

常见的方式是通过 CAM Policy 中自定义策略 condition 条件来限制子账号访问条件,例如限制访问 IP,设置成功后,子账号将通过所设置的 IP 管理主账号 下的资源,或者拒绝子账号通过设置的 IP 管理主账号下资源,详情请参见 限制 IP 访问 。

3. 使用策略条件来增强安全性

尽可能的为策略定义更精细化的条件,约束策略生效的场景,强化安全性。如约束用户必须在指定的时间,指定的服务器上执行某些操作等。 相关设置请参见 元素参考 condition 。

审计安全



1. 监控 CAM 账号的操作记录

您可以使用 腾讯云操作审计 的日志记录功能来确定 CAM 用户在您的账户中进行了哪些操作,以及使用了哪些资源。日志文件会显示操作的时间和日期、操作的 源 IP、哪些操作因权限不足而失败等。相关信息请参见 查看操作记录。

遵循最佳安全设置建议,在使用腾讯云时,综合利用这些保护机制,建立安全完善的资源控制体系,可以更有效地保护账号及资产的安全。

更多信息

您可以通过下载用户凭证报告获取腾讯云所有子账号及其用户凭证状态,包含控制台登录密码、访问密钥和账号安全设置。您可以使用该报告进行合规性审计。相 关信息请参见 下载安全分析报告 。

授予标签下部分操作权限

最近更新时间: 2024-10-11 17:33:22

操作场景

若您的公司购买了多种腾讯云资源,资源均通过标签分组管理,希望能够为不同团队员工按标签授予需要业务的部分接口操作权限。本文档以一个典型案例让您轻 松了解如何实现子账号拥有标签下资源的部分操作权限。

假设存在以下条件:

- 企业账号 CompanyExample 下有个子账号 Operator。
- 企业账号 CompanyExample 下有个为 Operator&activity 的标签键值对。
- 企业账号 CompanyExample 希望给子账号 Developer 授予标签 Operator&activity 下 CVM 资源的重启操作权限(cvm:RebootInstances)。

操作步骤

- 1. 使用企业账号 CompanyExample 登录 访问管理控制台。
- 2. 在策略页面,单击新建自定义策略 > 按策略语法创建。
- 3. 在选择模板类型下选择空白模板,单击下一步,进入编辑策略页面。

1 选择	 选择策略模板 > ② 编辑策略 						
模板类型:	全部模板 ▼	输入策略名关键词进行搜索	Q				
选择模板类	埋						
全部模版	反 (共566个)						
•	空白模版			0	AdministratorAccess 该策略允许您管理账户内所有用户及其权限、财务相关的信息、云服务资产。		
0	QCloudFinanceFullAccess 该策略允许您管理账户内财务相关的	内容,例如:付款、开票。		0	ReadOnlyAccess 该策略允许您只读访问账户内所有支持接口级鉴权或资源级鉴权的云服务资产。		
0	QcloudAAFullAccess 活动防刷(AA)全读写访问权限			0	QcloudABFullAccess 代理记账(AB)全读写访问权限		

4. 进入编辑策略页面,填写如下表单:

- 策略名称: 默认为 policygen-当前日期 ,推荐您自行定义一个不重复且有意义的策略名称,例如 cvm-RebootInstances。
- 描述: 可选,自行编写。
- 策略内容:复制以下内容并填写。其中, cvm:RebootInstances 为需要授权操作的接口名称,Operator&activity 为需要授权操作的标签键及标签 值。





"	
"	
}	
}	
]	
}	

- 5. 单击**完成**,完成策略的创建。新建的策略将显示在策略列表页。
- 6. 在 策略列表 中搜索找到刚才已创建的策略,单击右侧操作列下的关联用户/组/角色。

① 用户或者用户组与策略关联后,即可获得策略	都所描述的操作权限。		
新建自定义策略 副除			全部策略 预设策略 目定义策略 搜索策略名称描述备注(多关键词空格调开) Q 文 土
黄略名	服务类型 ▼	描述	上次修改时间 操作
cvm-RebootInstances			新於 <mark>·关联用产组织角色</mark>
	-	-	删除 关联用 户(组)角色

7. 在弹出的**关联用户/用户组/角色**窗口中,搜索勾选子账号 Operator,单击**确定**完成授权操作。 子账号 Operator 将拥有标签 Operator&activity 下 CVM 资源的重启操作权限。

支持多关键词(间隔为空格)搜	搜索用户名/ID/SecretId/手机/邮箱/备	Q		名称	类型	
用户	切换成用户组或角色 🍸			Operator	田白	0
Operator	用户				(נת	0
	用户					
	用户		\Leftrightarrow			
	用户					
	用户					
	用户					

关联文档

- 如果您想了解如何将资源和标签建立关联关系,请参见 管理标签。
- 如果您想了解如何授予标签下资源的所有操作权限,请参见 授权不同子账号拥有独立的云资源管理权限。



使用 ADFS 进行用户 SSO 的示例

最近更新时间: 2024-12-10 17:36:54

操作场景

本文提供一个以 ADFS 与腾讯云进行用户 SSO 的示例,帮助您理解企业 IdP 与腾讯云进行 SSO 的端到端配置流程。

前提条件

- 1. 拥有一台 Windows Server 服务器。如您需要购买服务器,请参见 云服务器-购买指南。
- 2. 在服务器内进行以下搭建工作。
 - 2.1 DNS 服务器: 将身份认证请求解析到正确的 Federation Service 上。
 - 2.2 Active Directory 域服务 (AD DS): 提供对域用户和域设备等对象的创建、查询和修改等功能。

2.3 Active Directory Federation Service (AD FS):提供配置 SSO 信赖方的功能,并对配置好的信赖方提供 SSO 认证。

() 说明:

本文中涉及到 Microsoft Active Directory 配置的部分属于建议,仅用于帮助理解腾讯云 SSO 登录的端到端配置流程,腾讯云不提供 Microsoft Active Directory 配置的咨询服务。

操作步骤

安装部署 Microsoft AD

```
🕛 说明:
```

如您已安装部署 Microsoft AD,可忽略步骤1-5,从 步骤6 开始操作。

1. 在云服务器内,进入 Server Manager > Dashboard,单击 Add roles and features,如下图所示:

è.		Sen	/er Manager			_ 0	x
Server Ma	anager • Dashbo	ard		• 🕲 I 🖡	Manage Tool	s View	Help
🔛 Dashboard	WELCOME TO SERVER M	IANAGER					^
Local Server		_					ו ר
All Servers		1 Confi	gure this local se	rver			
■File and Storage Services ▷	OUNCE CTART		5				
	QUICK START	2 Add	d roles and features				
		2 /100	a roles and reatares				
		3 Add	d other servers to ma	nage			
	WHAT'S NEW	4 Cre	ate a server group				=
		5 Cor	nnect this server to clo	oud services			
	LEARN MORE					Hide	
	ROLES AND SERVER GR Roles: 1 Server groups: 1	OUPS Servers total:	1				
	File and Storag	e 1	Local Server	1			
	 Manageability 		 Manageability 				
	Events		Events				
	Performance		Services				
	BPA results		Performance				
			BPA results				
E 占 🚞					• Q	12/ ³⁴	49 PM 13/2018

2. 一直单击 Next 直到单击 Install 完成安装,如下图所示:

<u> </u>	Add Roles and Features Wizard	
Before you begin		DESTINATION SERVER adserver
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	This wizard helps you install roles, role services, or features. You determine which ro features to install based on the computing needs of your organization, such as shar hosting a website. To remove roles, role services, or features: Start the Remove Roles and Features Wizard Before you continue, verify that the following tasks have been completed: • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The most current security updates from Windows Update are installed If you must verify that any of the preceding prerequisites have been completed, clos complete the steps, and then run the wizard again. To continue, click Next.	les, role services, or ing documents, or se the wizard,
	< Previous Next > Insta	Cancel
a	Add Roles and Features Wizard	_ D X
Select installation	type	DESTINATION SERVER adserver
Before You Begin Installation Type Server Selection	Select the installation type. You can install roles and features on a running physical machine, or on an offline virtual hard disk (VHD).	computer or virtual
Server Roles Features Confirmation Results	 Configure a single server by adding roles, role services, and features. Cemote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to create a vi or session-based desktop deployment. 	rtual machine-based
Server Roles Features Confirmation Results	 Note-based of feature-based installation Configure a single server by adding roles, role services, and features. Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to create a vi or session-based desktop deployment. 	rtual machine-based



b	Add Roles and Features Wizard
Select destination	DESTINATION SERVER adserver
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select a server or a virtual hard disk on which to install roles and features.
	Add servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
	Add Roles and Features Wizard
Select server role	S DESTINATION SERVER adserver
Before You Begin	Select one or more roles to install on the selected server.
Installation Type Server Selection Server Roles Features AD DS Confirmation Results	Roles Description Active Directory Certificate Services Active Directory Domain Services Active Directory Domain Services Active Directory Domain Services Active Directory Description Active Directory Domain Services Active Directory Description Active Directory Domain Services Active Directory Certificate Services Active Directory Description Active Directory Certificate Services Active Directory Certificate Services Active Directory Lightweight Directory Services and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process. DHCP Server DNS Server Fax Server File and Storage Services (1 of 12 installed) Hyper-V Network Policy and Access Services Print and Document Services Print and Document Services
	Remote Access Remote Desktop Services
	< Previous Next > Install Cancel



Select features		DESTINATION SERVE adserve
Before You Begin	Select one or more features to install on the selected server.	
Installation Type	Features	Description
Server Roles Features AD DS Confirmation Results	NET Framework 3.5 Features (1 of 3 installed) Image: NET Framework 4.5 Features (2 of 7 installed) Image: Background Intelligent Transfer Service (BITS) Image: BitLocker Drive Encryption Image: BitLocker Network Unlock Image: BranchCache Client for NFS Image: Data Center Bridging Image: Direct Play Enhanced Storage Failover Clustering Image: Group Policy Management IIIS Hostable Web Core Ink and Handwriting Services	APIs intermeter s.2 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

3. 安装完成后单击 Promote this server to a domain controller,如下图所示:

b	Add Roles and Features Wizard	_ D X
Installation progr	ess	DESTINATION SERVER adserver
Before You Begin	View installation progress	
Installation Type	i Feature installation	
Server Selection Server Roles	Configuration required. Installation succeeded on adserver.	
Features	Active Directory Domain Services	^
AD DS Confirmation	Additional steps are required to make this machine a comain controller. Promote this server to a domain controller	
Results	Remote Server Administration Tools Role Administration Tools AD DS and AD LDS Tools Active Directory module for Windows PowerShell AD DS Tools Active Directory Administrative Center AD DS Snap-Ins and Command-Line Tools You can close this wizard without interrupting running tasks. View task pr page again by clicking Notifications in the command bar, and then Task (Togress or open this Details.
	Export configuration settings	
	< Previous Next >	Cancei



4. 在 Deployment Configuration 页面选择 Add a new forest 补充 Root domain name 信息为 testdomain.com, 如下图所示:

Ē.	Active Directory Domain Services Configuration Wizard	_ _ ×
Deployment Configuration Deployment Configuration Domain Controller Options Additional Options Paths Review Options Prerequisites Check Installation Results	Active Directory Domain Services Configuration Wizard figuration Select the deployment operation Add a domain controller to an existing domain Add a new domain to an existing forest Add a new forest Specify the domain information for this operation Root domain name: testdomain.com	TARGET SERVER adserver
	More about deployment configurations Previous Next > Instant	all Cancel

5. 在 Domain Controller Options 中补充 Password 信息,如下图所示,完成后一直单击Next,单击 Install 完成安装

Active Directory Domain Services Configuration Wizard					
Domain Controller Options TARGET SERVER adserver					
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select functional level of the new forest Forest functional level: Domain functional level: Specify domain controller capabilities Domain Name System (DNS) server Global Catalog (GC) Read only domain controller (RODC) Type the Directory Services Restore Mod	ct functional level of the new forest and root domain st functional level: Windows Server 2012 R2 ain functional level: Windows Server 2012 R2 ify domain controller capabilities Domain Name System (DNS) server Slobal Catalog (GC) Read only domain controller (RODC) e the Directory Services Restore Mode (DSRM) password			
	Password:	•••••			
	Confirm password:	•••••			
Ls.					
	More about domain controller options				
	< Pr	evious Next > Install	Cancel		

6. 安装完成后,服务器将重启,重启完成后,进入 Start Menu > Active Directory Users and Computers,如下图所示:



Active Directory Users and Computers						
File Action View Help						
Active Directory Users and Com Name 1	Гуре	Description				
Saved Queries	ouiltinDomain					
Delegate Control	ntainer	Default container for up				
Find	ganizational	Default container for do				
▷ 🗊 🛛 Change Domain	ntainer	Default container for ma				
Change Domain Controller	ntainer	Default container for up				
Raise domain functional level	ganizational	· ·				
Operations Masters	ganizational					
i New b	Compute	er				
	Contact					
	Group					
View P	InetOraP	Person				
Refresh	mslmaqu	ing-PSPs				
Export List	MSMO 0	Dueue Alias				
Properties	Organiza	ational Unit				
Help	Printer	2				
	User					
	Shared Fo	older				
< III >						
Create a new object						

7. 在 Active Directory Users and Computers 页面,新建 Org 及 Users 信息,其中 Users-First name 名称需与后续腾讯云创建的子用户保持一致,如下图所示:

	Active	Dire	ectory Users	and Computers		_ D X
File Action	View Help					
🗢 🔿 🗖	1 🖬 🖬 🖬 🖬 🕷	2	🛅 🍸 🗾 🎕	5		
 Active Direct Saved Qu ■ testdama ■ testdama	ory Users and Com leries Delegate Control Find Change Domain Change Domain Controller Raise domain functional level Operations Masters New	Ty bu	pe ntainer ganizational ntainer ntainer ganizational ganizational	Description Default container fr Default container fr Default container fr Default container fr Default container fr	or up or do or sec or ma or up	
	All Tasks	•	Contact			
	View	•	Group			
	Refresh Export List		InetOrgPe msImagin MSMQ Q	erson ng-PSPs ueue Alias		
	Properties		Organizat	ional Unit		
	Help		Printer	NE		
			User			
			Shared Fo	lder]	
Create a new obje	act					
create a new obje	ittm					



	New Object - User
🧏 Create in:	testdomain.com/Group01
First name:	test Initials:
Last name:	user01
Full name:	test user01
User logon name:	
testuser01	@testdomain.com V
User logon name (pre	-Windows 2000):
TESTDOMAIN	testuser01]
	< Back Next > Cancel
	New Object - User
Create in:	New Object - User
Create in:	New Object - User
Create in: Password: Confirm password:	New Object - User testdomain.com/Group01
Password: Confirm password:	New Object - User testdomain.com/Group01
Create in: Password: Confirm password: User must change User cannot chan	New Object - User testdomain.com/Group01 ••••••• ••••••• ••••••• •password at next logon ge password
Create in: Password: Confirm password: User must change ✓ User cannot chan ✓ Password never e	New Object - User testdomain.com/Group01 ••••••• ••••••• ••••••• •password at next logon ge password xpires
Create in: Password: Confirm password: User must change User cannot chan Password never e Account is disable	New Object - User testdomain.com/Group01 ••••••• ••••••• ••••••• ••••••• ••••••• ••••••• •••••• •••••• •••••• •••••• •••••• •••••• •••••• •••••• •••••• •••••• •••••• •••••• ••••••• •••••• •••••• •••••• •••••• ••••••• ••••••• ••••••• •••••• ••••••• ••••••• ••••••• •••••• ••••••• •••••• •••••• •••••• •••••• •••••• •••••• •••••• •••••• ••••• ••••• ••••• •••• •••• ••• ••• ••• ••• ••• •• •• •• •• •• •• <
Create in: Password: Confirm password: User must change User cannot chan Password never e Account is disable	New Object - User testdomain.com/Group01 ••••••• ••••••• ••••••• •password at next logon ge password xpires ad
Create in: Password: Confirm password: User must change User cannot chan Password never e Account is disable	New Object - User testdomain.com/Group01 ••••••• ••••••• •password at next logon ge password xpires ad

安装 CA

1. 在云服务器内,进入 Server Manager > Dashboard,单击 Add roles and features,如下图所示:



à			Serve	er Manager				- 0 ×	
€⊛∙	Server Ma	anager • Dashboard	_		• ③ I	Manage	Tools Vi	ew Help	
Dashboard		WELCOME TO SERVER MANA	GER						^
All Servers		QUICK START	Confi <u>c</u> Add Add Crea	gure this local server roles and fattures other servers to mana ate a server group	ver age				
		LEARN MORE ROLES AND SERVER GROUPS Roles: 0 Server groups: 1 Serv	Con	nect this server to clou	ud services			Hide	=
		Local Server	1	All Servers	1				
		 Manageability 		 Manageability 					
		Events		Events					
		Services		Services					
		BPA results		BPA results					۲
				51711C5d1t5					
							• 👍 🔁	⊕ 4:43 PM 12/13/2018	8

2. 一直单击 Next 直到 Server Roles 页面,在 Server Roles 页面选择 Active Directory Certificate Services,如下图所示:

Ē.	Add Roles and Features Wizard	_ _ X
Select server role	5	DESTINATION SERVER adserver.testdomain.com
Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection		Active Directory Certificate Services
Server Roles	Active Directory Certificate Services	(AD CS) is used to create
Features	Active Directory Federation Services	role services that allow you to issue
AD CS	Active Directory Lightweight Directory Services	and manage certificates used in a variety of applications.
Role Services	Active Directory Rights Management Services	valiety of applications.
Confirmation	Application Server	
Results	DHCP Server	
	DNS Server (Installed) Eav Server	
	File and Storage Services (2 of 12 installed)	
	Hyper-V	\searrow
	Network Policy and Access Services	
	Print and Document Services	
	Remote Access	
	Remote Desktop Services	
	< Previous Next	> Install Cancel

3. 一直单击 Next 直到 AD CS > Role Services 页面,选择 Certification Authority、Certification Authority Web Enrollment,如下图所示:



2	Add Roles and Features Wizard	_ D X
Select role servic	res	DESTINATION SERVER adserver.testdomain.com
Before You Begin Installation Type Server Selection Server Roles	Select the role services to install for Active Directory Certifica Role services	te Services Description Certification Authority Web Enrollment provides a simple Web interface that allows users to
Features AD CS Role Services Web Server Role (IIS)	Certificate Enrollment Web Service Certification Authority Web Enrollment Network Device Enrollment Service Online Responder	perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.
Role Services Confirmation Results		1
	< Previous Ne	xt > Install Cancel

4. 一直单击 Next 直到 Results 页面,单击下图信息配置 AD CS Configuration,如下图所示:

b	Add Roles and Features Wizard	_ 🗆 X
Installation progre	ess	DESTINATION SERVER adserver.testdomain.com
Before You Begin	View installation progress	
Installation Type	Feature installation	
Server Selection	·	
Server Roles	Configuration required. Installation succeeded on adserver.testdomain.com	h.
Features	Active Directory Certificate Services	^
AD CS	Additional steps are required to configure Active Directory Certificate Services	s on the
Role Services	Configure Active Directory Contificate Services on the destination server	
Web Server Role (IIS)	Certification Authority	
Role Services	Certification Authority Web Enrollment	
Confirmation	Remote Server Administration Tools	
Results	Role Administration Tools Active Directory Certificate Services Tools Certification Authority Management Tools Web Server (IIS)	v
	You can close this wizard without interrupting running tasks. View task pro page again by clicking Notifications in the command bar, and then Task D Export configuration settings	gress or open this etails.
	< Previous Next > Clo	Cancel



<u>ا</u>	AD CS Configuration
Credentials	DESTINATION SERVER adserver.testdomain.com
Credentials Role Services	Specify credentials to configure role services
Confirmation Progress Results	To install the following role services you must belong to the local Administrators group: • Standalone certification authority • Certification Authority Web Enrollment • Online Responder To install the following role services you must belong to the Enterprise Admins group: • Enterprise certification authority • Certificate Enrollment Policy Web Service • Certificate Enrollment Web Service • Network Device Enrollment Service
	Credentials: TESTDOMAIN\Administrator Change
	More about AD CS Server Roles
	< Previous Next > Configure Cancel

5. 单击 Next,在 Role serveries 页面,勾选下图信息,单击 Next。

a	AD CS Configuration	_ D X
Role Services		DESTINATION SERVER adserver.testdomain.com
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation	Select Role Services to configure Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service	Ç,
Progress Results	More about AD CS Server Roles	Configure

6. 在 Setup Type 页面,选择 Enterprise CA,如下图所示:



2	AD CS Configuration
Setup Type	DESTINATION SERVER adserver.testdomain.com
Credentials Role Services	Specify the setup type of the CA
Setup Type CA Type	Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.
Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	 Enterprise CA Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies. Standalone CA Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require A DS and can be used without a network connection (offline).
	More about Setup Type
	< Previous Next > Configure Cancel

7. 在 CA Type 页面,选择 Root CA,如下图所示:

B	AD CS Configuration
СА Туре	DESTINATION SERVER adserver.testdomain.com
Credentials	Specify the type of the CA
Role Services	
Setup Type	When you install Active Directory Certificate Services (AD CS), you are creating or extending a
СА Туре	own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI
Private Key	hierarchy.
Cryptography	Root CA
CA Name	Root CAs are the first and may be the only CAs configured in a PKI hierarchy.
Validity Period	O Subordinate CA
Certificate Database	Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by
Confirmation	the CA above them in the hierarchy.
Progress	
Results	
	More about CA Type
	< Previous Next > Configure Cancel
	i inchous (i inchoise (i cun

8. 在 Private Key 页面,选择 Create a new private key,如下图所示:



	AD CS Configuration	
Private Key		DESTINATION SERVER adserver.testdomain.com
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	 Specify the type of the private key To generate and issue certificates to clients, a certification authority Create a new private key Use this option if you do no have a private key or want to create Use existing private key Use this option to ensure continuity with previously issued certificate and use its associated private key Select a certificate and use its associated private key. Select an existing private key on this computer Select an existing private key on this computer Select an existing private key on this computer Select this option if you have retained private keys from a preduce a private key from an alternate source. 	r (CA) must have a private key. e a new private key. ïcates when reinstalling a CA. imputer or if you want to evious installation or want to
	More about Private Key	
	< Previous Next >	Configure Cancel
	< Previous Next > AD CS Configuration	Configure Cancel
Cryptography fo	< Previous Next > AD CS Configuration Or CA	Configure Cancel
Cryptography fo Credentials Role Services	<pre></pre>	Configure Cancel
Cryptography fo Credentials Role Services Setup Type CA Type	<pre></pre>	Configure Cancel
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	AD CS Configuration AD CS Configuration AD CS Configuration Specify the cryptographic options Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider Select the hash algorithm for signing certificates issued by this CA: SHA256 SHA384 SHA512 SHA1 MD5 Allow administrator interaction when the private key is accessed	Configure Cancel
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	AD CS Configuration AD CS Configuration Or CA Specify the cryptographic options Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider Select the hash algorithm for signing certificates issued by this CA: SHA256 SHA384 SHA512 SHA1 MD5 Allow administrator interaction when the private key is accessed More about Cryptography	Configure Cancel



	AD CS Configuration
	DESTINATION SERVE
CA Name	adserver.testdomain.co
Credentials	Specify the name of the CA
Role Services	
Setup Type	Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but ca
СА Туре	be modified.
Private Key	Common name for this CA:
Cryptography	testdomain-adserver-CA
CA Name	
Validity Period	Distinguished name suffix:
Certificate Database	DC=testdomain,DC=com
Confirmation	Preview of distinguished name:
Results	CN=testdomain-adserver-CA,DC=testdomain,DC=com
	More shout CA Name
	< Previous Next > Configure Cancel
	< Previous Next > Configure Cancel
	< Previous Next > Configure Cancel
	AD CS Configuration
	AD CS Configuration
/alidity Period	AD CS Configuration
/alidity Period	AD CS Configuration
/alidity Period	AD CS Configuration
Validity Period Credentials Role Services	AD CS Configuration
Validity Period Credentials Role Services Setup Type	AD CS Configuration AD CS Configuration DESTINATION SERVE adserver.testdomain.com Specify the validity period Select the validity period for the certificate generated for this certification authority (CA):
/alidity Period Credentials Role Services Setup Type CA Type	AD CS Configuration AD CS Configuration DESTINATION SERVE adserver.testdomain.com Specify the validity period Select the validity period for the certificate generated for this certification authority (CA): Years
Validity Period Credentials Role Services Setup Type CA Type Private Key	Previous Next > Configure Cancel AD CS Configuration - <td< td=""></td<>
Validity Period Credentials Role Services Setup Type CA Type Private Key Cryptography	AD CS Configuration AD CS Configuration AD CS Configuration DESTINATION SERVE adserver.testdomain.com Specify the validity period Select the validity period for the certificate generated for this certification authority (CA): S Years CA expiration Date: 12/13/2023 4:52:00 PM The validity period configured for this CA certificate should exceed the validity period for the
Validity Period Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name	AD CS Configuration AD CS Configuration DESTINATION SERVE adserver.testdomain.com Specify the validity period Select the validity period for the certificate generated for this certification authority (CA): Select the validity period for the certificate generated for this certification authority (CA): CA expiration Date: 12/13/2023 4:52:00 PM The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.
Validity Period Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period	< Previous Next > Configure Cancel AD CS Configuration •
Validity Period Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database	< Previous
Validity Period Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation	< Previous
Validity Period Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress	AD CS Configuration DESTINATION SERVE adserver.testdomain.com Specify the validity period Select the validity period for the certificate generated for this certification authority (CA): Select the validity period for the certificate should exceed the validity period for the certificates it will issue. Cancel Cance
Validity Period Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	< Previous
Validity Period Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	< Previous
Validity Period Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	< Previous
Validity Period Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	AD CS Configuration Image: Configuration DESTINATION SERVE adserver.testdomain.com Specify the validity period Select the validity period for the certificate generated for this certification authority (CA): Societation Market addresses Configuration
Validity Period Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	< Previous
Validity Period Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	< Previous

9. 在 Certificate Database 页面,补充信息,单击 Next,如下图所示:



	AD CS Configuration	
CA Database		DESTINATION SERVER adserver.testdomain.com
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Specify the database locations Certificate database location: C:\Windows\system32\CertLog Certificate database log location: C:\Windows\system32\CertLog	
	More about CA Database	
	< Previous Next >	Configure Cancel
	< Previous Next > AD CS Configuration	Configure Cancel
Results	< Previous Next > AD CS Configuration	Configure Cancel
Results Credentials	< Previous Next > AD CS Configuration The following roles, role services, or features were configured:	Configure Cancel
Results Credentials Role Services	< Previous Next > AD CS Configuration The following roles, role services, or features were configured: Active Directory Certificate Services	Configure Cancel
Results Credentials Role Services Setup Type CA Type	< Previous Next > AD CS Configuration The following roles, role services, or features were configured: • Active Directory Certificate Services Certification Authority Orniguration Configuration	Configure Cancel
Results Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	< Previous	Configure Cancel

10. 访问 http://localhost/certsrv 确保 CA 安装成功,如下图所示:





安装 ADFS 服务

在配置前您需要给计算机或者指定的用户或者计算机授权证书颁发。安装 ADFS 前,需要创建和配置证书,本文中通过 IIS 进行证书申请。

1. 在云服务器内,单击 📥 ,在弹出的窗口单击工具,选择 IIS 管理器。



2. 在 IIS 管理器中,单击**服务器证书**,如下图所示:



8 3	Internet Information Services (IIS)管理器	_ _ X
ADSERVER >		😰 🛛 🟠 🔞 •
文件(F) 视图(V) 帮助(H)		
¥ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲		設作 管理新名書 重新启动 声言の 使止 重着内34 更改、NET Framework 版本 研究時的 Web 平台组件 常期)
就诸		S

3. 进入服务器证书页面,单击**创建证书申请**,如下图所示:

V		Internet In	formation Services (IIS)管	理器		
ADSERVER >						😰 🛛 🟠 🔞 -
文件(F) 视图(V) 帮助(H)						
	 服务器证书 使用此功能来申请印管理 Web 』 簿选: 	服务器可以次面置了 SSL 的网站使 『开始(G) - 📢 全部显示(A) 名	用的证书。 细依据:不进行分组 ·			续作 导入 也建证书申请 完成证书申请 也是就成证书由请
D - [0] 20]2£	名称	颁发给	颁发者	到期日期	证书哈希	创建自签名证书
		testdomain-ADSERVER-CA	testdomain-ADSERVER-CA	2027/12/14 17:0	CF1BDD606BDA7E67C4F97	
< <u>m</u> >	< 功能規图		в		δ	 帮助
就绪						¢1.:
						H.::



	申请证书	? X
可分辨名称属性		
以 指定证书的必需信息。省/市/自	治区和城市/地点必须指定为正式名称,并且不得包含缩写。	
通用名称(<u>M</u>):	*.test	
组织(0):	test	
组织单位(U):	test.com	
城市/地点(L)	shenzhen	
省/市/自治区(S):	guangdong	
国家/地区(R):	CN ~	
	上一页(P) 下一步(N) 完成(D)	取消



	中哨业书
」 加密服务	提供程序属性
选择加密服务提供程 位长可能会降低性能	序和位长。加密密钥的位长决定了证书的加密强度。位长越大,安全性越强。但较大的 。
加密服务提供程序(S)):
MICrosoft KSA SCh	
1211 (b):	✓
	した 上一页(2) 下一步(1) 完成(5) 取消
↓ 文#名	レー页の 下一步(N) 完成(B) 取消 申请证书 ? ×
文#名	した 上一页(2) 下一步(1) 完成(2) 取消 申请证书 ? ×
文件名 为证书申请指定文件名。此信息可以 为证书申请指定一个文件名(R):	上一页の 下一步 (N) 完成 (D) 取消 申请证书 2 又发送给证书级发机构签名。
文件名 为证书申请指定文件名。此信息可 为证书申请指定一个文件名(R): C:(Users\Administrator\Desktop	上一页の 下一步の 市靖征书 2 × 以发送给证书级发机构签名。
文件名 为证书申请指定文件名。此信息可 为证书申请指定一个文件名(R): C?(Users\Administrator\Desktop	上一页(2) 下一步(N) 完成(5) 取消 申请证书 2 × 以发送给证书级发机构签名。
文 件名 为证书申请指定文件名。此信息可 为证书申请指定一个文件名(R): C?(Users\Administrator\Desktop	レー页の 下ー歩い 完成の 取消 申请证书 ? × 以发送给证书缀发机构签名。
文 代名 为证书申调描定文件名。此信息可以 为证书申调描定一个文件名(R): C:\Users\Administrator\Desktop	上一页(P) 下一步(N) 完成(P) 取消 申请证书 2 × 以发送给证书颁发机构签系。
文件名 为证书申请指定文件名。此信息可 为证书申请指定一个文件名(R): C:{Users\Administrator\Desktop	上一页四 下一步
文 件名 为证书申请指定文件名。此信息可 为证书申请指定一个文件名(R): CAUSers\Administrator\Desktop	上一页の 下一步の 完成の 取消



🙀 🔿 🧭 http://localhost/certsrv/ 🔎 = C 🦉 Microsoft Active Director ×
Microsoft Active Directory 证书服务 testdomain-ADSERVER-CA 主页
欢迎使用
使用此网站为你的 Web 浏览器、电子邮件客户端 或其他程序申请证书。通过使用证书,你可以 向通过 Web 进行通信的用户确认你的身份、签名并 加密 邮件,并根据你申请的证书类型执行其他 安全任务。
你也可以使用此网站下载证书颁发机构(CA)证书、证书链,或证书吊销列表(CRL),或者查看挂起申请的状态。
有关 Active Directory 证书服务的详细信息,请参阅 Active Directory 证书服务文档.
选择一个任务: 申请证书 查看挂起的证书申请的状态 下载 CA 证书、证书链或 CRL
C C C Mitp://localhost/certsrv/certrqus. ア・ C // Microsoft Active Director ×
Microsoft Active Directory 近书服务 testdomain-ADSERVER-CA キロ ヘ
选择一个证书类型:
或者,提交一个 <mark>高级证书申请</mark> ,





5. 在弹出的提交证书申请页面,将申请证书保存的证书文件内容复制之后补充至以下输入框,证书模板选择 Web 服务器,单击提交。如下图所示:

	x
🗇 🕘 🖉 http://localhost/certsrv/certrqxt.e 🔎 < 🖒 Microsoft Active Directory 🦉 Microsoft Active Director ×	7 🌣
提交一个证书申请或续订申请	~
	-
要提交一个保存的申请到 CA,在"保存的申请"框中粘贴一个由外部源(如 Web 服务器)生成的 base-64 编码的 CMC 或 PKCS #10 证书申请或	
PKCS #/	
保存的申请:	
MAOGCSqGSIb3DQEBBQUAA4GBAA7Hfls87b5maoyf Base-64 编码的 www.maf.Db.TuMa2=p42CfabaB8CV5aTa1Wb1dWDb1/	
征书申请 5duFimLuORYGWoSkPuVDLNi3dfEBJZp6kDE1D0cZl	
(CMC 政 HDZD PKCS #10 或END NEW CERTIFICATE REQUEST ✓	
PKCS #7):	
<u>证书模板:</u>	
Web 服务器	
附加属性:	
提交 >	
	- ~

6. 提交之后,单击**下载证书**,如下图所示:

て <i>Microsoft</i> Active Directory 证书服务 testdomain-ADSERVER-CA	듌	^
证书已颜发		
你申请的证书已颁发给你。		
● DER 编码 或 ○ Base 64 编码		

7. 在服务器证书页面,单击完成证书申请,在弹出的页面选择步骤6 下载的证书,如下图所示:



9		Internet Ir	nformation Services (IIS)智	理器		_ D X
ADSERVER >						😐 🖂 🔞 •
文件(F) 视图(V) 帮助(H)						
连接 ९ू.• 🔒 🖄 🔗	🖣 服务器证书					操作 导入
	使用此功能来申请和管理 Web I	最多器可以对面置了 SSL 的网站使	间的证书。			创建证书申请
ADSERVER (TESTDOMAIN)	筛选: • 1	『 开始(G) - 🜄 全部显示(A) 🛛	3组依据:不进行分组 🔹			
▶ 🔞 网站	名称	颁发给	颁发者	到期日期	证书哈希	创建现址书
	٢	testdomain-ADSERVER-CA	testdomain-ADSERVER-CA	2027/12/14 17:0	CF1BDD606BDA7E67C4F97	创建目至名业书品。 元许自动重新称定续订的证书 ? 帮助
	11 11 11 11 11 11 11 11 11 11 11 11 11					
< III >						€∃ .
910 1 8						10,::
		3	完成证书申请			? X
月 指定	言证书颁发机构响	应				
通过检索包含) 包含证书颁发标	1、岁颜发机构响应的 几构响应的文件名(E)文件来完成先前创)):	则建的证书申请。			

¥

...

确定

取消

好记名称():

test.cert

为新证书选择证书存储(<u>S</u>):

个人

8. 在 网站	> Default Web	Site 主页,	右键单击 编辑绑定 ,	如下图所示:
----------------	---------------	----------	--------------------	--------



🛐 Internet Information Services (IIS)管理器	_ _ X
● → ADSERVER → 网站 → Default Web Site →	🕶 🛛 🟠 🕡 -
文(木(F) 视 関(M) 帮助(H)	
送援 Default Wale Site 主西	操作
Q- 品 2 18. UPFault Web Site 王贝	🔉 浏览
3. 起始页 (資法: ・ ▼ 开始(G) ・ ↓ 金録显示(A) 分组 祝道: 区域 ・ ■・	编辑权限
A DSERVER (TESTDOMAIN) ASP.NET	偏韻网站
	□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	查看应用程序
· · · · · · · · · · · · · · · · · · ·	
	■ ▶ 启动
編節定	■ 停止
	浏览网站
	● 浏览 *:80 (http)
新聞会 日田戸 順広塔 HTTP 重定向 ISAPI 常活器 MIME 英型 SSL 役置 处理程序映 借規页 模块 武人文档 目表浏览 エ	高级设置
	风制
新水源法 口ぶ 身份延近 大火県水県 輸出規行 154項 路規則	🕢 帮助
	. 🗹
	¶.:

9. 在弹出的网站绑定页面,单击添加,选择类型为 https,IP 地址为全部未分配,端口为 80,SSL 证书为 test.cert,如下图所示:

🛐 Internet Information Services (IIS)管理器				
€ S ADSERVER →	网站 → Default Web	ite 🕨		😰 🖂 🔞 -
文件(E) 視图(⊻) 帮助(土)				
连接	🔕 Defa	网站绑定 ? ×		操作
◎ □ 2 8		^{差型} 添加网站绑定 ? ×		打开功能
	》第125: ASP.NET	₩ ₩型(D): IP thath(D):		》 浏览 编辑权限
	۵	https v 全部未分配 v 80		编辑网站
👂 😔 Default Web Site	.NET 编译 .NE	主机名(1):	计算机密钥	郑正… 圖 基本设置…
				查看应用程序 查看虑10日录
	(ab) 连接字符串 扎	□ 需要服务器名称指示(N)		管理网站
		hz	=	🗢 重新启动
	IIS	SSL 证书@:	^	 ▶ 启动 ■ 停止
		test.cert		浏览网站
	ASP HI	16 中	HRAD	 浏览 *:80 (http) 高级沿客
	a	WEAL *1X/FB		R音
	请求筛选			失败请求跟踪
	管理		~ ~	₩ ● 帮助
< III >	🔝 功能视图 👫 内容视	§		
就诸				€ <u>1</u> .:

10. 在管理工具页面,单击**证书颁发机构**,如下图所示:



文件 主页 共享 查看 ✓ (?)					
🍥 🛞 = 🕇 👼 🗄	湖面板 ▶ 系统和安全 ▶ 管理工具		~ ¢	搜索"管理工具"	Q
 ○ ○ ○ ↑ ○ ○ ○ ○ ○ ○ ○ ○ 	 潮面板 → 系統和安全 → 管理工具 Ferminal Services Active Directory 管理中心 Active Directory 唐理中心 Active Directory 成和信任关系 Active Directory 成和信任关系 Active Directory 成和信任关系 Active Directory 成和信任关系 Active Directory 就和信任关系 Construction Services (IIS)管理器 SISCSI 发起程序 Microsoft Azure 服务 ODBC 数据原(32 位) ODBC 数据原(64 位) Windows PowerShell ISE (x86) Windows PowerShell ISE Windows PowerShell ISE Windows Server Backup Windows Server Backup Windows 内存诊断 索全費置向导 本地安全策略 派券 	 斎級安全 Windows 防火備 於計算机管理 於 任 公告计划程序 計 季件查看器 读件查看器 读件查看器 读 碎片整理和优化运动器 泛 系統電置 系統信息 会 任能监视器 彼 用于 Windows PowerShell 的 Active Directory 模块 读证书颁发机构 没预原监视器 或组集器 通 组集略管理 余.组件服务 	× ٿ	搜索"管理工具"	٩
	🔁 服务器管理器				

11. 在**证书颁发机构**页面,选择**证件模板**,右键单击管理,如下图所示:



12. 请参考下图配置:



P		证书模板控制台	
文件(F) 操作(A) 查看(V) 帮助	1(H)		
🗢 🌒 🖬 🗎 🖬			
书模板(adserver.testdomain.com)	模板显示名称	架构版本	^
	回 Kerberos 身份验证	2	
	🗵 OCSP 响应签名	3	
	🗟 RAS 和 IAS 服务器	2	
	🗟 Web 服务器	1	
	🗟 从属证书颁发机构	1	
	🖳 代码签名	1	
	🗟 根证书颁发机构	1	
	🗟 工作站身份验证	2	
	🗟 管理员	1	
	· 星基本 EFS	1	
	图 计算机	1	
	图 交叉证书颁发机构	2	
	🖳 仅 Exchange 签名	1	
	图 仅用户签名	1	
	图路由器(脱机申请)	1	
	图 密钥恢复代理	2	≡
	图 目录电子邮件复制	2	
	图 通过身份验证的会话	1	
	图 信任列表签名	1	
		1	
	國 域控制器	1	
	☑ 域控制器身份验证 ──	2	
	图 证书颁发机构交换	2	
	图 智能卡查; 复制模板(U)	1	
	图 智能卡用/ 所有任务(10)	1	
		1	
	□ 注册代理(雨TE(R)	1	~
< III >	< 帮助(H)		>



対象类型	X
选择你想查找的对象类型。	
对最美型(0):	
 ✓ 總内置安全主体 ○ ◎ 服务帐户 ✓ ● 计算机 ✓ 總 組 	
☑ & 用户	
	确定取消

选择用户、计算机、服务帐户或组	X
选择此对象类型(S): 平 用户、计算机、组或内置安全主体	对象类型(O)
查找位置(F): testdomain.com	位置(L)
输入对象名称来选择(示例)(E): adserver	检查名称(C)
高级(A) 确定	取消

- 13. 进入**服务器管理器 > 仪表板**页面,单击**添加角色和功能**,按照默认选择一直单击**下一步**直到服务器角色选择页面,勾选 Active Directory Federation Services,一直单击**下一步**,**直至安装完成**。
- 14. 在安装完成页面,单击**在此服务器上配置联合身份验证服务**,如下图所示:



B	添加角色和功能向导	_ D X
安装进度	adserve	目标服务器 er.testdomain.com
开始之前 安装类型 服务器选择 服务器角色 功能 AD FS 确认 结果	 査査安装进度 ⑦ 功能安装 需要配置。已在 adserver.testdomain.com 上安装成功。 Active Directory Federation Services 需要执行其他步骤才能在此计算机上配置 Active Directory 联合身份验证服务。 企此服务器上配置联合身份验证服务。 	
	你可以关闭此向导而不中断正在运行的任务。请依次单击命令栏中的"通知"和"你 查看任务进度或再次打开此页面。 导出配置设置 < 上一步(P) 下一步(N) > 关闭	£务详细信息",以 取消

15. 在弹出的向导页面,单击**下一步。**

a	Active Directory 联合身份验证服务配置	前导 <mark> ×</mark>
连接到 Active D	rectory 域服务	目标服务器 adserver.testdomain.com
欢迎 连接到 AD DS 指定服务属性 指定 服务帐户 指定数据库 查看选项 先决条件检查 安装 结果	☆ 指定一个具有 Active Directory 域管理员权限的帐户 TESTDOMAIN\Administrator (当前用户)	, 以执行联合身份验证服务配置。 更改(<u>C</u>)
	< 上一步(P) 下·	一步(N) > 配置(C) 取消



16. 设置指定服务属性,选择并填写好所需数据,单击**下一步**。

B	Active Directory 联合	身份验证服务配置向导	
指定服务属性		目标服务器 adserver.testdomain.com	
欢迎 连接到 AD DS 指定服务属性	SSL 证书:	adserver.testdomain.com ▼ 导入①… 查看	
指定服务帐户 指定数据库 查奏选证	联合身份验证服务名称:	adserver.testdomain.com * 示例: fs.contoso.com	
三有 些	联合身份验证服务显示名称:	crm_adfs 用户将在登录时看到显示名称。 <i>示例: Contoso Corporation</i>	
		< 上一步(P) 下一步(N) > 配置(C) 取消	

17. 设置指定服务账户,选择使用现有的域用户账户或组托管服务账户,单击选择。

B	Active Directo	ory 联合身份验证服务配置向导	_ D X
除 指定服务帐户			目标服务器 adserver.testdomain.com
欢迎 连接到 AD DS 指定服务属性 指定数据库 查看选项 先决条件检查 安装 结果	指定一个域用户帐户画) 创建组托管服务帧 帐户名称: ④ 使用现有的域用户 帐户名称:	或组托管服务帐户。 《户 不能户或组托管服务帐户 *<未提供>	选择(5)
		<上─步(₽) 下─歩(№) >	配置(C) 取消

18. 选择指定账户后,单击确认,确认后直至安装完成。

腾讯云

选择用户或服务帐户	×
选择此对象类型(S):	
用户或服务帐户	对象类型(0)
查找位置(F):	
testdomain.com	位置(L)
输入要选择的对象名称(例如)(E):	
adfs svc (adfs svc@testdomain.com)	检查名称(C)
高级(A) 确定	取消

用户SSO配置

- 1. 在服务器内浏览器访问 https://adserver.testdomain.com/FederationMetadata/2007-06/FederationMetadata.xml ,将源数据 XML 下载 至本地。
- 2. 进入访问管理-用户 SSO 控制台,单击右侧编辑,设置 SSO 协议为 SAML,上传 步骤1 保存的 XML 文件。
- 在服务器内进入 ADFS 管理页面,选择信任关系 > 信赖方信任,右键选择添加信赖方信任,单击启动,补充联合元数据地址,元数据地址从第 2 步中获取, 一直单击下一步,如下图所示:


\$		AD FS			_ D X
🧌 文件(F) 操作(A) 查看(V) 窗口(W) 帮	助(H)				- F ×
	信袖士信江	_	_		19.0-
→ AD FS	显示名称	已启用	类型	标识符	探™ 信赖方信仟 ▲
▲ 🛗 信任关系	Device Registration Service	是	WS	urn:ms=drs:adserver.testdoma https://cloud_tencent_com/10	添加信赖方信任
		Æ		http:///oroda.com/rolling	添加非声明感知信赖方信任
○ 特性存 添加信赖方信任(A) ○ 特性存 添加信赖方信任(A) ○ 時性存 添加非声明感知信赖方信	任(N)				
2 Strib 2010年1月 音看(V)	•				
从这里创建窗口(W)					2 帮助
刷新(F)					Device Registration Service
(H)					从联合元数据更新
					编辑声明规则 禁用
					属性
					🗙 删除
					? 帮助
6	添加	信赖方信	責任□ਿ	雪母	X
12	1040H			1.1	
欢迎使用					
先骤					
- 动间体用	次迎使用添加信赖万信1	刊日台			
◎ 从应使用	此向导将帮助你向 AD PS	配数据	驝渤	·新的信赖方信任。信赖	防使用此联合身份验证服务颁发
◎ 选择数据源	ロリダ王マ族中の中の欧山	31/J324E14	-1212		
◎ 是否立即配置多重身份验 征?	此向导创建的信赖方信任? 向导后,你可以完义用于	2.义此联合 司信畅方发)身份 ()::::::::::::::::::::::::::::::::::::	绘证服务如何识别信赖) 狙的颁发转换规则。	方以及如何向其发出声明。完成
·또· · · · · · · · · · · · · · · · · · ·	1-14314 - 16-19(AE)(0.011	-314-10/2 500			
◎ 选择测发授权规则					
◎ 准备好添加信任					
◎ 完成					
				<上一步(P)) 启动(S) 取消

步骤 选择此向导将用 > 欢迎使用 选择数据源 ● 选择数据源 ● 导入有关在线使用此选项从 ● 遗择数据源 ● 导入有关在线使用此选项从 ● 遗择颁发授权规则 ● https://dl ● 准备好添加信任 ○ 从文件导入有 ● 完成 ○ 从文件导入有	目于获取有关此信赖方的数据的选项: 线或在本地网络上发布的信赖方的数据(M) 从在线或在本地网络上发布其联合元数据的信赖方组织导入必要的数据和证书。 据地址(主机名或 URL)(F): cloud.tencent.com/saml/SpMetadata.xml?tenantID=、Jet
 步骤 选择处面导将用 选择数据源 是否立即配置多重身份验 选择颁发授权规则 准备好添加信任 完成 关本输入有关 	用于获取有关此信赖方的数据的选项: 线或在本地网络上发布的信赖方的数据(M) 从在线或在本地网络上发布其联合元数据的信赖方组织导入必要的数据和证书。 据地址(主机名或 URL)(F): cloud.tencent.com/saml/SpMetadata.xml?tenantID=.Jec.Jec.Jec.Jec.Jec.Jec.Jec.Jec.Jec.Jec
使用此选项手	漏文(H)应(U). 浏览(B) 关信赖方的数据(T) 手动输入有关此信赖方组织的必要数据。

4. 配置完后,效果如下图所示:

🔗 腾讯云

操作
操作 iserver.testdoma. 信赖方信任 添加非声明感知信赖方信任 添加非声明感知信赖方信任 查看) 从此处新建窗口 ② 帮助 Cloud.tencent.com 从联合元数据更新 編編声明规则 募用 属性 》 翻除

为腾讯云 SP 配置 SAML 断言属性



为保证腾讯云 SAML 响应定位到正确的子用户,SAML 断言中的 NameID 字段需要是腾讯云子用户名。SAML 断言中的 NameID 默认传入为 (TESTDOMAIN\子用户名)格式,需正则表达式去除原有配置 TESTDOMAIN,仅保留子用户名(TESTDOMAIN 是前面的默认 NETBIOS 名)。自定 义规则为:安装 ADFS 服务中步骤3 申请证书所在文件内的 txt 内容。

%	添加转换声明规则向导	x
选择规则模板		
 步骤 选择规则类型 配置声明规则 	法择要从以下列表创建的声明规则的模板。说明提供有关每个声明规则模板的详细信息。 声明规则模板(c): 使用自定义规则按送声明 ✓ 声明规则模板说明: 使用自定义规则时,可以创建用规则模板无法创建的规则。自定义规则以 AD FS 声明规则语言 编写而成。需要目定义规则的功能包括: ·发送来自 SQL 特性存储的声明 ·发送来自 SQL 特性存储的声明 ·发达和自定义 LDAP 饰法器发送来自 LDAP 特性存储的声明 ·发达和自定义 PHP 行動声明 ·发达者自定之为性存储的声明 ·发达者自定之为性存储的声明 ·发达者自定之为性存成的声明 ·发达者自定之为性存成的声明 ·发达者们的是全部成分声明 ·发达者们的是全部成分声明	
	< 上一步(P) 下一步(N) > 取消	



() 说明:

```
若出现请求终止,无法创建 SSL/TLS 安全通道时,可通过 powershell 执行方式重启服务器解决。
```

• 32位机器:

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Wow6432Node\Microsoft.NetFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -Value '1' -Type DWord
```

• 64位机器:

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft.NetFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -Value '1' -Type DWord
```

用户 SSO 登录:

```
1. 在浏览器输入 https://adserver.testdomain.com/adfs/ls/idpinitiatedsignon 。
```

2. 输入用户名、密码信息,即可完成登录,如下图所示:



(→) Ø https://adserver.testdomain 𝒫 ▼ (■ × O 正在等待 adserver.testdo ×	_ □ × ⋒ ☆ \$
	Windows 安全 X	
	iexplore 正在连接到 adserver.testdomain.com, testuser1 ••••••••• • TESTDOMAIN · 记住我的凭握 连接智能卡	~
	确定取消	
	© 2013 Microsoft	



使用 OneLogin 进行角色 SSO 的示例

最近更新时间: 2025-04-17 17:33:02

操作场景

OneLogin 是一家云身份访问管理解决方案提供商,可以通过其身份认证系统一键登录企业内部所有需要的系统平台。腾讯云支持基于 SAML 2.0(安全断言标 记语言 2.0)的联合身份验证,SAML 2.0 是 OneLogin 等许多身份验证提供商(Identity Provider,IdP)使用的一种开放标准。

本示例中,企业拥有一个腾讯云账号、一个 OneLogin 管理员用户和多个 OneLogin 普通用户。企业希望经过配置,使 OneLogin 普通用户直接使用 OneLogin 账号通过角色 SSO 的方式访问腾讯云,不需要在腾讯云重新创建账号。

OneLogin 的详细信息,请参见 OneLogin 帮助文档。

操作步骤

创建 OneLogin 企业应用程序

() 说明:

- 您可以通过本步骤创建 OneLogin 企业应用程序。如您已经有正在使用的应用程序,请忽略本操作,进行 配置 CAM 。
- 本文中应用程序名称以"test"为示例。

1. 登录并访问 OneLogin 网站,单击 Applications,进入应用管理页。

- 2. 在应用管理页,单击右上角 ADD APP。
- 3. 在搜索框中输入 "SAML",按 "Enter" 键,并在结果列表中单击 Pilot Catastrophe SAML(IdP)。如下图所示:

Find A	Applications	
	JIRA/Confluence (with Resolution SAML SingleSignOn) re:solution	SAML2.0
2	Pilot Catastrophe SAML (IdP) OneLogin, Inc.	SAML2.0
d'	SAML 1.1 Test Connector (Advanced) OneLogin, Inc.	SAML1.1

4. 在 Display Name 中输入应用名 ,并单击右上角 Save,即可完成应用程序的创建。如下图所示:

App Listing / Add Pilot Catastrophe Sa	AML (IdP)		Cancel	Save
Configuration	Portal Display Name test Visible in portal			
	Rectangular Icon Image: Constraint of 2.64.1 as either a transparent. PNG or. SVG	Square Icon		

配置 CAM



() 说明:

- 您可以通过本步骤配置 OneLogin 和腾讯云之间的信任关系使之相互信任。
- 本示例中 SAML 身份提供商以及角色名称均为 "test"。
- 1. 在 OneLogin 应用管理页,选择您已创建的应用 test。
- 2. 单击右上角 More Actions,选择 SAML Metadata,下载 IdP 云数据文档。如下图所示:

More Actions 👻 Save
Vendor Homepage
Reapply entitlement mappings
SAML Metadata
Delete

3. 创建腾讯云 CAM 身份提供商以及角色,详细操作请参见 创建身份提供商 、创建角色 为身份提供商创建角色。

配置 OneLogin 单点登录

① 说明: 您可以通过本步骤将 OneLogin 应用程序属性映射到腾讯云的属性,建立 OneLogin 应用程序和腾讯云的互信关系。

- 1. 在 OneLogin 应用管理页,单击已创建的 "test" 应用,跳转至应用编辑页。
- 2. 选择 Configuration 页签,输入以下内容,单击 Save。如下图所示:

Applications / Pilot Catastrophe SAML	(IdP)	More Actions 👻 Save
Info	Application details	
Configuration	SAML Consumer URL	
Parameters	https://cloud.tencent.com/login/saml	
Rules	SAML Audience	
SSO	https://cloud.tencent.com	
Access	SAML Recipient	
Users	https://cloud.tencent.com/login/saml	
Privileges	SAML Single Logout URL	
	ACS URL Validator	
	() Regular expression - Validates the ACS URL when initiated by an AuthnRequest	

您可以根据您的腾讯云账号所在站点进行配置:

所在站点	SAML Consumer URL	SAML Audience	SAML Recipient
中国站	https://cloud.tencent.com/logi n/saml	https://cloud.tencent.com	https://cloud.tencent.com/login/sa ml
国际站	https://tencentcloud.com/logi n/saml	https://tencentcloud.com/login/saml	https://tencentcloud.com/login/sam l

() 说明:

 SAML Recipient 为跳转的腾讯云页面,如您需要指定其他页面,可使用 https://cloud.tencent.com/login/saml?s_url=xxxx
 形式指

 定,其中 xxxx 为需要指定的地址,需要做 urlencode。

3. 单击 Parameters,单击 + ,添加以下两条配置信息。

Field name	Flags	Value	源属性
https://cloud.tencent.com/ SAML/Attributes/Role	Include in SAML assertion	Macr o	qcs::cam::uin/{AccountID}:roleName/{RoleName1};qcs::cam::uin/{A ccountID}:roleName/{RoleName2},qcs::cam::uin/{AccountID}:saml- provider/{ProviderName}
https://cloud.tencent.com/ SAML/Attributes/RoleSes sionName	Include in SAML assertion	Macr o	Test

! 说明:

- 在 Role 源属性中 {AccountID}, {RoleName}, {ProviderName} 分别替换内容下:
- {AccountID} 替换为您的腾讯云账户 ID,可前往 账号信息 控制台 查看。
- {RoleName} 替换您在腾讯云创建的角色名称,可前往角色 控制台 查看。
- {ProviderName} 替换您在腾讯云创建的 SAML 身份提供商名称,可前往 身份提供商 控制台 查看。

4. 单击右上角 Save 保存配置。

配置 OneLogin 用户

- 1. 登录并访问 OneLogin 网站,单击 Users,进入用户管理页面。
- 2. 单击右上角 New User,跳转至新建用户页。
- 3. 输入 "First name" 、 "Last name" 、 "Email" 、 "Username" ,单击 Save User 保存。如下图所示:

Last name *	Email		
Required			
Phone number	Manager		
	Choose a manager 🗸		
Department	Title		
	Last name * Required Phone number Department	Last name * Email Required	Last name * Email Required

🕛 说明:

此账户密码可查看 Email,或单击 More Actions 选择 change password 修改密码。

4. 单击用户编辑页 Applications,选择右侧的 + 。如下图所示:

Users / test test				More Actions 👻	Save User
User Info	Roles	Applications			•
Authentication Applications	Default				
Activity					



5. 在弹出对话框选择您已创建的 SAML 应用 "test",单击 Continue。如下图所示:

Assign new login to test test		
This login will override any apps assigned via roles. Select application		
test		•
	Cancel	Continue

6. 在 Edit test login for test test 页面,单击 Save。如下图所示:

Edit test login for test test		
Show this app in Portal		
SAML ID		
Reset login (What's this?)		
	Cancel	Delete Save

7. 使用 步骤3 创建的账户登录 OneLogin ,访问上述创建的 SAML 应用 "test",即可跳转至腾讯云控制台。

支持员工间资源隔离访问

概述

最近更新时间: 2025-01-22 17:56:12

当一个主账号下有多个业务时,每个业务都有自己的资源,企业管理者会希望员工在使用 CAM 子账号登录时,不同业务的员工可以看到和操作的资源不同。 针对该场景,您可以通过访问管理(CAM)的两种权限设置方式(按照资源 ID 授权、按照标签授权)来实现资源的隔离访问。

场景说明

以云服务器(CVM)产品为例,假设在云上有两台云服务器,对应的信息如下:

资源 ID	镜像 ID	所属标签	所属项目
ins-dugxxxxx	img-ebxxxxx	game:webpage	webpage
ins-ijxxxxx	img-ebxxxxx	game:app	арр

为员工创建 CAM 子用户 CvmDev_zhangsan,通过上述两种权限设置方式实现 Cvm_Resource_ins_dugxxxxx 只能管理 ins-duglsqg0 的 资源级 接口 权限。

预期结果

• 使用管理员账号查看 CVM 广州区域列表效果:

实例 🕓 广州 3	3 其它地	域(2) ▼					有类	2问卷,产品体验您说了算	必 场景教学	🖆 [🏭 限时领福	利 实例使用指南 ▼
 用户之声: : 	欢迎您提交	CVM产品的功能	》/体验/文档等方	面的需求和建议,其	月待您的声音! <u>点击提交</u> ☑					0	••• ×
新建开机		关机 重	[c] 续	费重置密码	马 销毁/退还	更多操作 ▼				切换至页签礼	us ¢¢±
多个关键字用竖线 "	" 分隔,多	个过滤标签用回	车键分隔			Q	查看待回收实例				
ID/名称	监控	状态 ▼	可用区 🍸	实例类型 ▼	实例配置	主IPv4地址(i)	实例计费模式 ▼	网络计费模式 👅	所属项目 ▼	标签 (key:value)	操作
ins-dlastand 未命名	di	🛞 运行中	广州六区	标准型S6 🔁	2核 2GB 0Mbps 系统盘:高性能云硬盘 网络:Default-VPC	- (内)	按量计费 2022-05-19 10:17:51创建	-	webpage	r 1	登录 更多 ▼
ins-ij, 未命名	ılı	🐼 运行中	广州三区	标准型SA2 🚹	1核 1GB 0Mbps 系统盘:高性能云硬盘 网络:share-3-10	- (内)	按量计费 2022-05-19 10:13:45创建	-	арр	ि 1	登录 更多 ▼

• 使用 CvmDev_zhangsan 查看 CVM 广州区域列表效果:

实例 🔇 广州 1 🗦	其它地域 ▼	r					E	有奖问卷,产品体弱	逾您说了算	场景教学 🚦	冒 限时领福利	实例使用]指南 ▼
 有奖调研:填写z 	云服务器C\	/M满意度调查问衤	巻,赢取代金券。	立即前往也							0 •	0 0	×
新建开机	关机	重启	续费	重置密码	销毁/退还 更多操作	·					切换至页签视图	φx	¢±
多个关键字用竖线" "分隔	扇,多个过	滤标签用回车键分	分隔				Q	查看待回收实例					
ID/名称	监控	状态 ▼	可用区 🔻	实例类型 ▼	实例配置	主IPv4地址()		实例计费模式 ▼	网络计费模式 🔻	所属项目、	▼ 操作		
未命名	di.	阙 运行中	广州六区	标准型S6 <u>1</u>	2核 2GB 0Mbps 系统盘:高性能云硬盘 网络:Default-VPC	- (内)		按量计费 2022-05-19 10:17:51创建	-	webpage	登录 更	3 ▼	
共 1 条									20 ▼ 条 /	页 🛛 🖌 🖣	1 /1	□页 ▶	H

实现方式

- 方式一: 按照资源 ID 授权
- 方式二: 按照标签授权



按照资源 ID 授权

最近更新时间: 2025-01-22 17:56:12

操作场景

该任务指导您按照资源 ID 授权,实现子用户 CvmDev_zhangsan 只能管理 ins-duglsqg0 的 资源级接口 权限。

点此 查看详细操作场景。

策略内容

按照资源 ID 授权,最终实现上述预期结果时,对应的策略内容如下:

	"qcs::cvm::uin/12345678:instance/ins-duglsqg0", //12345678 为主账号 UIN

操作步骤

步骤1: 使用管理员账号创建策略并授权



1. 使用管理员账号登录访问管理控制台,在 策略 页面,按照策略生成器创建自定义策略(请参见 通过策略生成器创建自定义策略)。

「云服穷畚(王部保作)						
				资源六段式 🛙	用于唯一描述腾讯云的资源对象	₿.
效果(Effect) *	○ 允许 ○ 拒绝	٤ 		qes::evm::u	in/1 :image/img-el	p30mz8
服务(Service) ·	云服务器 (cvm)			服务・	cvm	
操作(Action) ·	全部操作 (*)			地域・	所有地域	Ŧ
资源(Resource) *	🔾 全部资源 🚺	特定资源		账户•	uin/1300-1509-1466	
收起		🗹 不拆分资源级和操作级接口 ①		资源前缀*	image	
	volume	为 AttachDisks 外加 2 个操作指定 volume 资源六段式① 此类 添加资源六段式 来限制访问	型任意资源	资源•	img-eb30mz89	
	ps	为 DescribeDisasterRecoverGroupQuota 外加 9 个操作指定 ps 资源六 添加资源六段式 来限制访问	段式① 」此类型任意资源			
	prepinstancepack	为 DescribeDedicatedPrepInstanceStatistics 外加 1 个操作指定 prepin 添加资源六段式 来限制访问	stancepack 资源六段式① U类型任意资源			
	lt	为 CreateLaunchTemplateVersion 外加 4 个操作指定 It 资源六段式 ③ 添加资源六段式 来限制访问	此类型任意资源			
	instance	为 DescribeDiagnosticReports 外加 5 个操作指定 instance 资源六段式 添加资源六段式 来限制访问	escribeDlagnosticReports 外加 5 个操作指定 instance 资源介段式① 此类型任意资源 资源介段式 未限制访问			
	image	为 DeleteImages 外加 4 个操作指定 image 资源六段式 ① 此类 添加资源六段式 来限制访问	型任意资源			
	dr	为 DescribeDiagnosticReports 外加 1 个操作指定 dr 资源六段式① 添加资源六段式 来限制访问	此类型任意资源			
		qcs::cvm::uin/* :instance/ins-dugIsqg0	编辑 删除 此类型任意资源			
		qcs::cvm::uin/* :image/img-eb30mz89	编辑 删除 此类型任意资源			
		添加自定义资源六段式 来限制访问		76.92		

- 如何确定资源的前缀:在云服务器支持 CAM 的接口中有云服务器对应的资源六段式,具体请参见 云服务器支持 CAM 的接口 。
- 云服务器产品页面除了调用 CVM 相关接口外,还会使用 VPC 等接口,这时我们可以先跳过,继续生成策略,在实际操作的时候按照 CAM 的提示添加相关接口。

2. 单击下一步,指定策略的名称为 Cvm_Resource_ins_duglsqg0,并将策略授予子账号 CvmDev_zhangsan。

3. 单击完成,完成授权。



🗸 编辑策略	> 2 关联用户/用户组/角色	
基本信息		
策略名称 •	Cvm_Resource_ins_duglsqg0	
	策略创建后,策略名称不支持修改	
描述	请输入策略描述	
关联用户/用户组/角	<u> </u>	
将此权限授权给用户	CvmDev_zhangsan 重新选择用户	
将此权限授权给用户组	选择用户组	
将此权限授权给角色	选择角色	

步骤2:使用子账号登录验证权限

- 1. 使用子用户登录 云服务器控制台,进入实例列表页面。此时 CVM 页面会提示缺少 VPC 产品 DescribeVpcEx 以及对应资源的权限。
- 2. 根据页面提示内容,联系管理员账号在策略中添加对应授权。

477 175		左西以下 (六)
14 X 1	对后息'许慎·	复制以下1言/
1	User (uin:) is not authorized to perform operation	
	(vpc:DescribeVpcEx)	
2	resource (gcs::vpc:gz:uin/ :vpc/*) has no permission	

步骤3:使用管理员账号调整策略内容

1. 使用主账号在 VPC 支持 CAM 的接口 清单中,找到 DescribeVpcEx 确定接口为操作级的接口。

存储	\sim		10/1-/7	
网络与CDN	~	DescribeUserGw	操作级	×
网络	^	DescribeUserGwVendor	操作级	*
负载均衡		DescribeVpcClassicLink	操作级	*
私有网络			2001-20	
专线接入		DescribeVpcEx	操作级	*
全局接入		DescribeVpcInstances	操作级	*
CDN与加速	\sim			

- 2. 在访问管理控制台的 策略 页面,找到策略 Cvm_Resource_ins_duglsqg0,单击策略名进入策略详情。
- 3. 在策略语法中单击编辑,按照操作级接口的授权书写形式在策略详情中添加接口授权。



Cvm_Resource_ins_duglsqg0							
Cvm_Resource_ins_duglsqg0 自定义策略 描述 - 創建时間 2023-09-25 17:39:58 上次修改时間 2023-09-25 17:43:19							
策略语法 策略版本 (3) 策略用法							
策略摘要 {} JSON 搜索服务 Q							
服劳 允许 (1 个服务)	资源	请求责件					
云服务器 (cvm)	\$^	au					

○ 添加之前:



○ 添加之后:



4. 添加之后重复 步骤2,使用子账号 CvmDev_zhangsan 再次验证,发现仍有异常,缺少 VPC 下 DescribeNetworkInterfaces 以及对应资源的访问 权限,请查看 私有网络支持 CAM 的接口 确定 DescribeNetworkInterfaces 为操作级的接口。



无权降	 長信息详情:	复制以下信息
1	User (uin:) is not authorized to perform operation	
2	(vpc:DescribeNetworkInterfaces)	
	resource (qcsvpc.gz.unv	

 按照 步骤3 继续调整策略内容,直至系统没有报错。 最终策略的内容如下:



() 说明:

在书写 CAM 策略时,在需要操作具体资源时,资源级的接口授权需要和操作级分开书写,多个操作级接口可以书写在一起。

步骤4:验证结果

使用子用户 CvmDev_zhangsan 再次验证,达到预期效果。

至此,子用户 CvmDev_zhangsan 可以对实例进行开关机、重启、更名、重置密码等操作。

实例 🕲 广州 1 其 1	已地域 ▼						Ē	有奖问卷,产品体验	您说了算 🖉	▶ 场景教学	[<u>]</u> 限时领福利	实例(使用指南 ▼
 有奖调研:填写云朋 	服务器CV	M满意度调查问卷	》,赢取代金券。立	.即前往 🖸							0	• • •	×
新建开机	关机	重启	续费	重置密码	销毁/退还 更多操作,	•					切换至页签视	8 ¢	☆ ∓
多个关键字用竖线" "分隔,	多个过	滤标签用回车键分	隔			(2	查看待回收实例					
ID/名称	监控	状态 ▼	可用区 🔻	实例类型 ▼	实例配置	主IPv4地址 (j)		实例计费模式 ▼	网络计费模式 🔻	所属项目	目▼ 操作		
	ılı	函 运行中	广州六区	标准型S6 📘	2核 2GB 0Mbps 系统盘:高性能云硬盘 网络:Default-VPC	- (内)		按量计费 2022-05-19 10:17:51创建	-	webpag	e 登录	更多 ▼	
共 1 条									20 * 条/	/页 🔟 🧃	(1)	/1页	



按照标签授权

最近更新时间: 2025-01-22 16:14:43

操作场景

该任务指导您按照标签授权,实现子用户 CvmDev_zhangsan 只能管理 ins-duglsqg0 的 资源级接口 权限。 点此 查看详细操作场景。

策略内容

按照标签授权,最终实现上述预期结果时,对应的策略内容如下:



操作步骤

步骤1: 创建策略并授权



1. 使用管理员账号登录访问管理控制台,在 策略 页面,按照标签创建自定义策略(请参见 通过标签授权创建自定义策略)。

UIL東略生成器 JSC	N .	
服务与操作 添加		
▼ 云服务器(全部操作)		101 P3
服务(Service) *	云服务器 (cvm)	
操作(Action) *	全部操作 (*)	
▼ 私有网络(2 个操作)		删時
服务(Service) *	私有网络 (vpc)	
操作(Action) *	读操作 编辑	
	DescribeVpcEx 查询私有网络列表 列表操作 编辑	
	支持标签搜口	
	DescribeNetworkInterfaces 查询弹性网卡信息	
示签(resource_tag) (j)		
10 v	webpage v X	

- 授予用户: CvmDev_zhangsan
- 绑定标签: game: webpage
- 操作权限: 云服务器的全部操作权限和 VPC 的 DescribeVpcEx 和 DescribeNetworkInterfaces (说明: 无法确定涉及的其他接口时,请参见 按照资源 ID 授权-步骤3进行验证添加)。
- 2. 单击下一步,填写策略名称。
- 3. 单击**保存**,完成授权。

🖌 编辑策略	〉 2 关联用户/用户组/角色	
基本信息		
策略名称★	Cvm_Resource_ins_duglsqg0	
	策略创建后,策略名称不支持修改	
描述	请输入策略描述	
关联用户/用户组/角包	<u>a</u>	
将此权限授权给用户	选择用户	
将此权限授权给用户组	选择用户组	
将此权限授权给角色	选择角色	
上一步 完成		



步骤2:验证结果

使用子用户 CvmDev_zhangsan 登录 云服务器控制台,访问实例列表页面,达到预期效果。

至此,子用户 CvmDev_zhangsan 可以对实例进行开关机、重启、更名、重置密码等操作。

实例 🔇 广州 1 英	它地域 ▼						E	有奖问卷,产品体验	您说了算 🛛 💋 场	景教学 🚦] 限时领福利	实例使用	朋指南 ▼
 有奖调研:填写云册 	服务器CV	M满意度调查问卷	6,赢取代金券。立	即前往 2							0 •	0 0	×
新建开机	关机	重启	续费	重置密码	销毁/退还 更多操作 •					ţ	刀换至页签视图	¢	¢⊥
多个关键字用竖线" "分隔,	多个过法	想标签用回车键分					۹ 🗆	查看待回收实例					
ID/名称	监控	状态 ▼	可用区 🕇	实例类型 ▼	实例配置	主IPv4地址 (j)		实例计费模式 ▼	网络计费模式 ▼	所属项目 🍸	7 操作		
	di	🐼 运行中	广州六区	标准型S6 📘	2核 2GB 0Mbps 系统盘:高性能云硬盘 网络:Default-VPC	- (内)		按量计费 2022-05-19 10:17:51创建	-	webpage	登录 更	3 ▼	
共 1 条									20 ▼ 条/页	H	1 /1	页 →	×

企业多账号权限管理

概述

最近更新时间: 2024-10-11 09:44:41

很多企业在腾讯云上会有多个主账号,账号越多,账号和权限的管理就会越复杂。这时企业管理者希望能够跨账号管理资源权限,减少管理的复杂度。员工如果需 要访问多个主账号,希望能够减少 CAM 子账号的数量和登录次数。

针对上述场景,腾讯云提供集团账号、角色和协作者三种方式进行跨账号的访问和管理。三种方式的对比如下,您可以根据实际场景选择适合自己企业的方式:

管理方式	特性说明
集团账号	图形化界面操作简易,只支持同一个集团内的企业实名账号使用。
角色	需要在每个被管理主账号下创建角色,操作流程相对较长。
协作者	只支持主账号作为协作对象。



集团账号

最近更新时间: 2024-11-28 15:34:01

集团账号简介

集团账号管理是腾讯云上面向集团客户的多账号管理产品,支持集团管理员统一管理集团及旗下子公司的腾讯云主账号,提供账号、财务、安全等的管理能力,更 多说明请参见 集团账号管理文档 。

在集团账号管理中,管理账号可以为 CAM 子账号同时授予多个创建的成员账号的管理权限,授权后,该 CAM 子账号支持只登录一次,就可以选择成员,访问 管理多个成员账号。



操作场景

假设某集团在腾讯云有账号 A 和账号B,选择账号 A 作为管理账号开通按账号管理产品,集团内有子公司1和子公司2,分别有账号 C 和账号 D。集团内有安全管 理员工 m,希望能够同时运维管理集团及其子公司的账号。

这时集团管理账号可以为员工 m 创建 CAM 子用户1,并授予账号 B、C、D 的安全运维权限,则员工通过 CAM 子用户1登录腾讯云控制台后,可以选择不同的 成员账号进行切换执行安全运维的相关操作,无需在每个账号下分别为员工创建 CAM 子用户。

操作步骤

添加授权

- 1. 管理员账号登录集团账号控制台,进入 成员登录权限设置 页面。
- 2. 设置管理所有成员的权限模型,如网络运维、安全运维、云服务器运维、财务管理员等。
 详细操作请参见创建成员登录权限。
- 3. 在 成员账号管理 中,单击**添加成员**,选择**新建成员**,并选择需要管理的权限。 详细操作请参见 添加组织成员 。
- 成员创建成功后,选择左侧导航栏中的成员登录,在成员登录页面中,单击添加成员授权页签,单击添加授权。
 详细操作请参见 授权登录成员账号。

使用子用户登录

使用 CAM 子用户登录**集团账号管理控制台 >** 选择左侧导航栏中的 成员登录。在**成员登录**页面中,选择需要登录的成员账号,并单击操作列的**登录账号**,在弹出 的**登录账号**窗口中选择登录权限进行登录。



角色

最近更新时间: 2024-10-11 09:44:41

角色简介

角色是 CAM 的一种虚拟用户,可以被授予权限策略,拥有所属主账号的相应权限,详细信息请参见 角色概述 。

在创建角色时,可以选择以腾讯云主账号作为角色载体、创建角色,并为角色绑定授权策略。 作为载体的主账号可以通过创建权限策略,将扮演角色的权限授予其 CAM 子账号,之后 CAM 子账号可以在腾讯云控制台通过切换角色登录到对应的主账号控制台执行授权范围内的操作,也可以通过云 API 发起跨账号请求。



操作场景

假设企业内有账号 A 和账号 B 两个主账号,企业安全管理员工 m 在账号 A 下有 CAM 子用户 a,员工 m 希望使用该子账号能够同时运维管理账号 B 下的安全 信息。这时我们可以按照以下步骤执行操作:

操作步骤

- 1. 在账号 B 下创建安全运维角色 role,并将角色载体指定为主账号 A。 详细操作请参见 创建角色。
- 2. 在账号 A 下创建权限策略,策略支持通过 AssumeRole 扮演安全运维角色 role。
- 将策略授权给 CAM 子用户 a。
 详细操作请参见 为子账号赋予扮演角色策略。
- 4. 员工 m 登录 CAM 子用户 a。
- 5. 员工 m 在腾讯云控制台选择切换角色,使用安全角色 role 登录腾讯云控制台。 详细操作请参见 使用角色登录腾讯云控制台。
- 6. 执行安全运维相关操作。
- 7. 如果员工 m 需要同时对多个主账号执行安全运维的相关操作,则可以参照上述步骤为员工 m 授予对应主账号的安全运维权限。



协作者

最近更新时间:2024-10-1017:42:11

协作者简介

本身拥有主账号身份,被添加作为当前主账号的协作者,则为当前主账号的子账号之一,可以协助管理主账号下的云资源。

操作场景

假设企业在云上有多个账号,如账号 A、账号 B、账号 C 等,希望账号 B 和账号 C 能够具有账号 A 下的资源访问权限。

操作步骤

- 1. 账号 A 登录 CAM 控制台,将账号 B、账号 C 添加为协作者,并授予权限。
 详细操作请参见 新建协作者、协作者权限设置。
- 1. 账号 B 或者账号 C 以协作者身份登录腾讯云控制台。
 详细操作请参见 子账号登录控制台 协作者登录。
- 如果您想切换访问其他账号,则需要退出重新登录。
 详细操作请参见协作者身份切换。



查看员工腾讯云操作记录

最近更新时间: 2024-10-11 14:36:51

操作场景

当您为员工创建 CAM 子用户并授权后,员工可以使用 CAM 子用户登录腾讯云控制台,或者使用 CAM 子用户密钥通过云 API 来访问和操作您账号下资源。当 有较多员工需要同时登录腾讯云并访问资源时,您可能需要了解以下信息:

- 员工访问了哪些资源
- 员工操作是否遇到问题
- 某个资源是哪个员工购买的
- 如何查看资源配置的修改记录
- 如何跟踪敏感操作
- 员工是否在您限定的环境内访问腾讯云

这时您可以通过操作审计查看和跟踪员工操作记录,操作审计支持在线查看90天以内的腾讯云控制台和云 API 操作记录。

前提条件

- 1. 已 创建子用户。
- 2. 已登录 操作审计控制台,进入操作记录页面。

操作步骤

查看操作记录事件详情

• 您可以通过筛选条件"操作者"按照CAM子用户/角色搜索,查看指定员工的操作记录。

近 30 分钟 近1小时	近1天 近7天	自选时间		
操作类型	只写	▼	事件名称 🛈	请选择资源类型/事件名称 ▼
操作者	请输入操作者/ID	Q	敏感操作筛选	全部 ▼
资源标签	用户角色			
	ā ar se			
查询 重置				

● 您可以通过单击事件名称在右侧查看事件详情,在具体的日志摘要中,通过操作者字段来识别实际操作的账号 ID 和名称,通过源 IP 地址查看操作来源。

								事件详情				
 以下列表包括了近三 	一个月 API活动的支持服务,	如果需要查看更长	时间的操作记录,请使用	跟踪集功能,日志数据将持久化存f	者到指定存储 模	禹成CLS中。		基本信息	事件说明 ☑			
								密钥 ID		事件区域	ap-guangzhou	
 根据等保合规2.0及序 	网安法备例要求,企业云上、	业务日志必须保存1	80天以上,建议您可以创	建設院街,投递到存储桶,方便长	明保存您的操作	作日志。		事件名称	ConsoleLogin	事件源	acco	
•								事件时间	2023-11-15 15:19:32	请求 ID	17	
(F30分曲) (F1/LR)	近1王 近7王	白海村市						源 IP 地址	 ? (中国 广东省 深圳市 中国电信) 	攝作會	100)	
200010 21040		H-A243143						资源地域	gz			
								CAM 错误码	-			
操作类型	只写	*	事件名称 ()	请选择资源类型/事件名称	*	操作者	10 1	相关资源				
敏感摄作筛选	全部	Ŧ	资源标签	请选择标签	Ŧ			资源类型	资源ID/名称		操作	
										无		
查询 里普	展开更多搜索							共0魚			10 * 垒/页 🖂 4 1	/1页 → →
爭件时间		操作者		事件名称		资源类型		事件记录	查看事件字段说明 🗹			
2023-11-15 15:19:32		-		ConsoleLogin(登录)		account(账号中心)		1 2 3	"userIdentity": { "principalId": "1			
2023-11-15 11:22:05		-		ConsoleLogin(登录)		account(账号中心)		4 5 6	"accountid": "1 33", "secretId": "", "secsionContext": (

• 在具体的日志详情中,您可以通过 principalld 来识别实际操作的账号 ID。



"userIdentity": {
"principalId": "1 ",//操作者ID
"accountId": "1
"secretId": "",
"sessionContext": { //请求信息
"MFAUsed": "No",
"aid": "",
<pre>"clientType": "pcweb",</pre>
"clientUA": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/110.0.0.0 Safari/537.36",
<pre>"loginTo": "https://console.cloud.tencent.com/cloudaudit",</pre>
"loginType": "qq",
"platform": "gcloud",

详细操作请参见: 查看操作记录事件详情。

使用跟踪集投递日志

如果您需要查看更长时间的员工操作记录,您可以使用操作审计的跟踪集功能,将日志投递到 COS 存储桶或者 CLS。 在投递到 CLS 时,您可以选择指定产品的具体操作(如敏感操作),并在 CLS 中配置告警策略。 详细操作请参见:使用跟踪集投递日志。

设置集团账号跨账号日志投递

如果您在腾讯云上有多个主账号,通过操作审计跟踪集您可以同时集中跟踪和查看操作审计的操作记录,详细操作请参见: 设置集团账号跨账号日志投递 。

使用 API 管理企业多账号权限

最近更新时间: 2024-11-28 15:34:01

操作场景

很多企业客户会在企业内部构建 IT 系统来管理员工子账号申请的流程,当企业内有多个账号时,将集团账号和 CAM 结合使用能够大幅提升管理的效率和安全 性。

假设存在以下条件:

- 公司已有账号 A,作为管理账号开通了集团账号管理产品。
- 在账号 A 下有 CAM 子用户 Administrator,具有全部管理权限。详情请参见新建子用户。
- 在公司内有游戏业务负责人小王,想要申请一个新的主账号来运行新发布的游戏,并为开发员工小李在该主账号申请一个具有开发权限的子用户,用于日常登 录访问腾讯云。

流程说明

通过 CAM 子用户 Administrator 的密钥来完成整个主账号创建以及子账号申请和授权的流程。

• 流程1: 为新游戏申请主账号



• 流程2:为开发员工小李创建 CAM 子账号并授权



操作步骤

使用管理子用户 Administrator 为新业务创建账号

1. 子用户 Administrator 调用集团账号管理产品的 CreateOrganizationMember API, 创建新的主账号。

🕛 说明

- 创建的主账号为使用集团管理账号的实名信息,自动完成企业实名认证。
- 创建的主账号,管理账号会自动具有管理权限。
- 同时也可以为新创建的账号分配财务管理权限,当前支持五类权限:查看成员账号的账单、查看成员账号的消费、为成员账号划拨资金、为成员账
 号申请开具发票、合并出账。
- 也可以为成员账号设置付费方式: 自付费 + 优惠继承、代付费。
- 成员财务管理说明请参见 查看成员财务权限。



2. 新的主账号调用访问管理产品的 CreatePolicy API,在创建的账号下,创建所需的自定义授权策略(按需执行)。

🕛 说明

如使用预设策略可以满足授权需要,则可忽略该步骤。

至此,为新游戏创建账号流程已完成,如果需要同时开通多个账号,则可重复上述流程。

使用管理子用户 Administrator 为员工创建 CAM 子账号

1. 调用访问管理产品的 AddUser API,在创建的腾讯云账号下,创建子用户。

🕛 说明

子用户的创建需要使用管理员身份,并扮演创建的成员的角色 OrganizationAccessControlRole,API 使用角色的调用请参见 使用角色 文档。

2. 获取需要绑定策略的策略 ID。

2.1 在访问管理控制台的 策略 页面,通过搜索找到需要绑定的策略(以 TI-ONE 的全读写策略为例)。

Š.							CAM策略使用说明
1) 用戶或者用戶組与策略大款后,即可获得策略	所抽还的操作权限。						
新建自定义策略			全部策略	预设策略	自定义策略	tione	8 Q 1
策略名	服务类型 🕈	描述				上次修改时间	操作
QcloudTIONEFullAccess	腾讯云 TI 平台 TI-ONE	腾讯云 TI 平台 TI-ONE	(TIONE) 全读写访	可权限		2022-01-04 10:37:14	关联用户/组/角色
QcloudTIONEFullAccessContainMultiserv	腾讯云 TI 平台 TI-ONE	腾讯云TI平台TI-ONE全设	卖写访问权限,包括	CAM, COS, V	PC、监控、标…	2022-03-29 10:41:33	关联用户/组/角色
QcloudTIONEReadOnlyAccess	腾讯云 TI 平台 TI-ONE	腾讯云 TI 平台 TI-ONE	(TIONE) 只读访问	权限		2022-01-04 10:36:17	关联用户/组/角色
QcloudTIONEReadOnlyAccessContainMu	腾讯云 TI 平台 TI-ONE	腾讯云TI平台TI-ONE只该	奏访问权限, 包括关	联的其他云产品	(CAM/TAG/mo	2022-03-29 10:30:39	关联用户/组/角色
QcloudTIONEResouceGroupFullAccessC	腾讯云 TI 平台 TI-ONE	腾讯云TI平台TI-ONE资源	原组管理模块全读写	访问权限和其他	模块读权限,包	2022-03-29 10:31:15	关联用户/组/角色
QcloudAccessForTIONERole		腾讯云 TI 平台 TI-ONE(「IONE)攝作权限含列	则举对象存储(CC	OS)文件,增删改…	2022-03-29 15:13:28	关联用户/组/角色
QcloudAccessForTIONERoleInCodeRepo	-	腾讯云 TI 平台 TI-ONE(FI-ONE)操作权限含	密钥管理系统(I	KMS) 创建密钥	2022-01-04 10:38:21	关联用户/组/角色

2.2 单击策略名称,进入策略详情页,浏览器地址栏的如下位置即为策略 ID。

$\leftarrow \rightarrow C$ \triangleq console.cl	oud.tencent.com/cam/policy/detail/353478688QcloudTIONEFullAccess&2		
	品 - 二二二二二二二二二二二二二二二二二二二二二二二二二二二二二二二二二二二	搜索产品、文档	Q ⑧小程序 2 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
访问管理	← QcloudTIONEFullAccess		
名用户 ·	QcloudTIONEFullAccess 预设策略		
瓷 用户组	描述 腾讯云 TI 平台 TI-ONE (TIONE) 全读写访问权限		
◎ 策略	备注 -		
🔄 角色	创建时间 2020-05-13 15:08:31		
「自身份提供商 、			
际联合账号 ~	硫酸语注 策略新大 (1) 策略田注		
(12)访问密钥 ~			
	策略擔要 {} JSON		
	搜索服务 Q		
	服务 资源		请求条件
	允许 (1 个服务)		
	腾讯云 TI 平台 TI-ONE (lione) 所有资	题	无



3. 调用访问管理产品的 AttachUserPolicy API,为创建的子用户授权。

使用 ABAC 管理员工资源访问权限 ABAC 概述

最近更新时间:2024-10-1017:54:54



ABAC 简介

什么是 ABAC

ABAC(Attribute−Based Access Control)是基于属性的访问控制授权策略,该策略使用属性来定义权限。在腾讯云中,使用标签来代表该属性。 在腾讯云中创建资源时,您可以将标签附加到资源中,来标记资源(查看 支持标签的产品)。在为角色授权时,您可以创建单个 ABAC 策略,将策略设计为角 色请求的标签与资源标签匹配时允许操作。ABAC 在资源变化频繁的环境中非常有用,在策略管理变得繁琐的情况下帮助您提升管理效率。

假设有三个项目 GroupA、GroupB 和 GroupC,分别有开发员工 a、b、c,您可以通过以下步骤管理员工资源访问权限:

- 1. 为三个员工分别创建标签键为 GroupA、GroupB、GroupC 的三个CAM子用户,标签值为 dev,并为三个子用户授予 assumeRole 的权限。
- 2. 创建开发角色,角色对应的标签的值为 dev。
- 3. 使用单个策略,允许访问三个项目下的资源,将策略附加给创建好的角色。
- 4. 员工通过 CAM 子用户代入角色来访问,当员工的标签键和资源的标签值相同时,允许访问。



ABAC 与传统授权方式对比

在 CAM 中,您通过为不同工作岗位的员工创建不同策略来管控权限,然后,您可将策略附加到 CAM 角色。按照 最佳实践, 您在为员工授予所需的最小权限 时,通常通过在策略中指定可以访问的具体资源来实现。这种方式的缺点在于,当员工需要添加访问新的资源时,就必须更新策略来允许访问这些资源。 假设有三个项目 GroupA、GroupB 和 GroupC,每个项目的资源不同,两种授权方式的对比如下:

授权方式	ABAC 授权	传统授权
三个项目相同岗位 的授权	 三个子用户 一个角色 两个策略(三个子用户共用一个角色切换策略,一个角色一 个权限管理策略) 	 三个子用户 三个角色 六个策略(每个子用户一个角色切换策略,每个角色一个 权限管理策略)
单个项目添加/减少 资源	无需调整授权策略	调整角色对应的权限管理策略
增加新的项目	只需要创建新的子用户	需要创建新的子用户、角色以及关联的两个策略

ABAC 授权的优势

使用 ABAC 管理资源访问权限具备以下优势:

自动扩展资源权限

支持权限随着资源的变更自动扩展,不再需要管理员更新现有策略来允许访问新的资源。

例如:假设您使用 access-project 标签附加到 ABAC 策略。开发人员使用access-project = GroupA 的标签来访问资源。当GroupA项目中的员工需要 额外的 CVM 云服务器资源时,开发人员可以使用 access-project = GroupA 标签创建新 CVM 实例。创建后,GroupA 项目中的任何授权员工可以启动和 停止这些实例,因为 GroupA 项目的员工对应角色的标签与资源的标签匹配。

减少策略数量

可以减少策略的数量,不再需要为不同项目的相同岗位员工创建不同策略,因此创建的策略数量减少,更易于管理。



方便后续扩展策略

如果有新的项目,可以快速基于已有策略进行扩展。

例如:您已经使用管理资源访问权限的支持项目 GroupA 和 GroupB,这时可以快速支持新增项目 GroupD。CAM 管理员可以创建 GroupD 对应的新的子 用户,并赋予 GroupD 对应的标签,然后为子用户授予切换角色的策略,这时有权限代入该角色的员工都可以访问具有 access-project = GroupD 标签资 源。

实现精细权限控制

在您创建策略时,最佳实践是授予最小权限。使用传统授权方式,您必须编写一个策略,仅允许访问特定资源。但是,如果使用 ABAC,您可以允许在所有资源 上的操作,但仅在资源标签与委托人标签匹配时可以访问该权限。



应用场景

最近更新时间: 2024-02-29 15:34:01

操作场景

在腾讯云的实际使用中,通过 ABAC 的授权策略,我们可以使用标签来定义权限。将标签绑定到 CAM 子用户、角色以及具体的云资源,之后可以定义权限策 略,这些策略使用标签条件键来根据请求身份的标签向其授予权限。当您使用标签控制对腾讯云资源的访问时,可通过对授权策略进行较少更改来实现团队和资源 的变更,操作更加灵活。

本章节将详细说明如何为员工在 CAM 中创建一个带有标签的 CAM 角色 ,以及支持通过带入角色的属性拥有访问与其标签匹配的资源的权限策略。当员工通过 该角色向腾讯云发出请求时,将根据带入的角色标签和资源标签是否匹配来授予权限,实现仅允许员工查看或操作其工作需要的资源。

使用示例

假设在游戏公司 A 中,有两个项目 webpage 和 app,其中员工 m 为 webpage 的开发员工,员工 n 为 app 的开发员工,在创建授权策略时,需要保证不同 团队内的员工能够访问其工作所需的资源,同时随着公司发展要考虑后续的扩展性。

可以通过使用资源标签和 CAM 角色标签来为支持 ABAC 策略的产品创建授权策略。当您的员工希望通过联合身份访问到腾讯云中时,其属性将应用到腾讯云中 的角色标签中。然后,您可以使用 ABAC 来允许或拒绝基于这些属性的访问。

() 说明

- 通过 支持标签的产品,了解哪些产品支持基于标签的授权。
- 通过 生效条件概述,了解授权策略中支持哪些标记条件键。

我们根据上述项目和团队,做以下标签定义:

- game-project = web(对应web项目)
- game-project = app(对应 app 项目)
- web = dev (对应 web 项目开发人员)
- app = dev (对应 app 的开发人员)
- game=dev (对应 web/app 项目开发人员)

实现原理

- 1. 员工使用CAM 用户凭证进行登录,然后扮演其团队和项目的 CAM 角色。
- 2. 将向相同岗位的角色附加同一策略,根据标签来实现允许或拒绝操作。

验证场景

假设有两台云服务器 ins-78qewdr8(标签 game-project:app)和 ins-7txjj4a6(标签 game-project:web),分别属于 app 和 webpage 项目。

- 验证点1:不同项目的员工使用不同的 CAM 子用户登录后,如何实现不同员工只能访问到其所属项目下的云服务器。
- 验证点2:假设员工岗位变更,员工 n 也需要项目 webpage 的权限,如何快速调整权限。
- 验证点3:假设公司新增加一个 H5 类的项目,如何快速为员工授予新项目的权限。

操作步骤

步骤1: 创建测试 CAM 子用户

1. 创建名为 access-assume-role 的自定义策略,策略内容为"当带入身份的标签与角色标签匹配时,允许带入 ABAC 角色"。







2. 创建 CAM 子用户 m-developer 和 n-developer,并为子用户绑定 access-assume-role 的授权策略,并为子用户绑定下述标签。

 说明 创建 CAM 子用户的详细操作,请参见 新建子用户。 	
子用户名称	关联标签
m-developer	web=dev
n-developer	app=dev

步骤2: 创建 ABAC 策略

1. 创建名为 access-resource-project (以 cvm 产品为例子)的自定义策略,策略内容如下:





	"gcs:resource tag": [
},	
{	
}	
]	
}	

 \odot game-project 与 \${qcs:principal_tag_key} 标签绑定的 key 和 value 值关联并确定项目与特定标签键相关联的数值。

2. 创建角色 access-developer-role,关联上述策略,并绑定如下标签。

 说明 创建 CAM 角色的详细操作,请参见 创建角色。 	
CAM 角色名称	关联标签
access-developer-role	game=dev

步骤3:场景验证

验证点1:使用不同的子用户登录后,只能访问到对应项目下的云服务器



1. 使用子用户 m-developer 登录 腾讯云控制台,在控制台右上角,单击账号下的切换角色。



2. 在切换角色页面,应用选择 web (子用户 m-developer 的标签 value) ,角色选择 access-developer-role,单击切换角色。

	切换角色	
 可使 角色 管理 换角 集团 	用子账号切换角色,切换角色后将获得角色的登录身份和相关权限,可管理 所在主账号的相关资源。 员授予您切换角色的权限,并为您提供主账号和角色详细信息后,您便可切 色。查看帮助文档 账号管理的用户,可以点击此链接就转到集团账号管理控制台快速切换角色	
请输入角色所	所属的主账号 ID	-
_ 应用 * web	~	-
请选择要访问 角色 *	developer rele	
access- 请选择要切扣	<u>Revenupei - i ote</u> 象的角色	_
显示名称	(
可设置此角的	色登录后在控制台显示的别名	
	切换角色	
	取消	

3. 以角色身份登录腾讯云控制台,进入 CVM 实例 页面。

在 CVM 产品控制台,若仅可以查看到 ins-7txjj4a6 (标签 game-project:web),则符合预期。



实例 🔇 南京 1 其著	宮地域 ▼						•	有奖问卷,产品体验您	说了算	Ø 场景教学 💈	ng 限时领福利 👳	例使用指南 ▼
 有奖调研:填写云朋 	服务器CVM	满意度调查问卷,	赢取代金券。立	<u>即前往</u> 2							0 • 0 0	• ×
新建开机	关机	重启	续费	重置密码 销货	//退还 更多操作 ▼						切换至页签视图	¢ ¢ ₹
多个关键字用竖线" "分隔,	多个过滤	标签用回车键分隔				Q, 宣看	待回收实例					
ID/名称	监控	状态 ▼	可用区 🍸	实例类型 ▼	实例配置	主IPv4地址 ④	实例计费模式 ▼	网络计费模式 👅	所属项目	起答 game-project:web	操作	
ins-7txjj4a6 ि <mark>终</mark> 未命名✔	di	🖂 运行中	南京一区	标准型S5 🏶	2核 2GB 5Mbps 系统盘:高性能云硬盘 网络:Default-VPC	(公) 后 【】 (内) 后	包年包月 2022-08-01 16:56:18到期	按流量计费	默认项目	© 1	登录 续费	更多 ▼
共 1 条									20 -	条/页 🛛 🖣	1 /13	Į – H

4. 切换身份,使用子用户 n-developer 登录 腾讯云控制台,登录后切换角色,应用选择 app,角色选择 access-developer-role,显示名称为 ndeveloper-app,单击**切换角色**。

切换角色	
りけた用 E	
· 亚尔石林 n-developer-app 可设置此角色登录后在控制台显示的别名	
切换角色	
取消	

5. 以角色身份进入腾讯云控制台,进入 CVM 实例 页面。 在 CVM 产品控制台,若仅能查看云服务器 ins-78qewdr8(标签 game-project:app),则符合预期。

实例 🔇 南京 1 其	它地域 ▼							有奖问卷,产品体验您	说了算 🧭 场景	牧学 🔄 限时领福利	削 实例使用指南 ▼
() 依相关法规及监管到	要求,腾讯:	云禁止客户利用云	服务从事虚拟货币	,相关业务, <u>查看声明</u> 🖸	3 。 如您有虚拟货币行为或感	染挖矿木马,请参考 <u>自助清理</u> 目	<u>戶册</u> 🖸 进行处理。			0 0	••• ×
	关机 多个过速		续费	重置密码 销货	/追还 更多操作 ▼	0	冬回近空间			切换至页签礼	ue o o i
●「大班子用亚线 〒 万桶, ■ ID/名称	「シーロンスス	标並用回半確方解 状态 ▼	可用区 🕇	实例类型 ▼	实例配置	望着 主IPv4地址 ④	(特回收买例) 实例计费模式 ▼	网络计费模式 🍸	所属项目 , 标	第 操作	
ins-78qewdr8 līt test e*	di	🗟 运行中	南京三区	标准型S6 📘	2核 2GB 5Mbps 系统盘:高性能云硬盘 网络:Default-VPC	(公) 后 [] (内) 后	按量计费 2022-06-24 16:32:57创建	按流量计费	game-pr	oject:app 1 登录	更多 ▼
共 1 条									20 🔻 条 / 页		/1页 🕨 🕅

验证点2:假设岗位变更,员工 n 也需要项目 webpage 的权限,该如何设置



当前场景下,我们仅需要在 访问管理控制台 的用户详情中,为员工 n 对应的 CAM 子用户 n-developer 增加标签 app:web 即可。

← 用户详情		
n-developer 子用户		编辑信息
账号ID	手机 - 🖍	
备注 -	郎箱 - 🖍	
访问方式 ① 控制台访问	微信 - 🖍	
标签 web:dev app:dev 🎤		
权限 服务 组 (0) 安全 () API 密钥	小程序 集团组织成员管理	
- 权限策略		

- 1. 使用子用户 n-developer 登录 腾讯云控制台,在控制台右上角,单击账号下的切换角色。
- 2. 在切换角色页面,应用选择 web,角色选择access-developer-role,别名为 n-developer-web,单击切换角色。

切换角色	
① 可使用子账号切换角色,切换角色后将获得角色的登录身份和相关权限,可管理 角色所在主账号的相关资源。 管理员授予您切换角色的权限,并为您提供主账号和角色详细信息后,您便可切 协会会。查考想你达得。	
集团账号管理的用户,可以点击此链接跳转到集团账号管理控制台快速切换角色 主账号 * 请输入角色所属的主账号 ID	
□	
角色★ access-developer-role ✓ 请选择要切换的角色	
显示名称 n-developer-web 可设置此角色登录后在控制台显示的别名	
切换角色	
取消	

3. 以角色身份登录腾讯云控制台,进入 CVM 实例 页面。

在 CVM 产品控制台,若仅能查看云服务器 ins-7txjj4a6(标签 game-project:web),则符合预期。

实例 🕲 南京 1 其它	地域 🔻							有奖问卷,产品体验您	说了算	Ø 场景教学 🛄	限时领福利 实例	刘使用指南 ▼
有奖调研:填写云服	务器CVM满意	度调查问卷,测	【取代金券。 <u>立即前</u>	前往2							0 • 0 0 0	• ×
新建 开机 多个关键字用竖线 "!" 分隔,	关机 多个过滤标签	重启 用回车键分隔	续费	建置密码 销毁	/退还 更多操作 ▼	Q. 查看	待回收实例			t01	央至页签视图 (¢¢±
D/名称	監控 り	《态 ▼	可用区 ▼	实例类型 ▼	实例配置	主IPv4地址 ④	实例计费模式 ▼	网络计费模式 🍸	所属项目:	編⋘ game-project:web	操作	
ins-7txjj4a6 <mark>行</mark> 续 未命名 ✔	ılı 🤅	у 运行中	南京一区	标准型S5 🛟	2核 2GB 5Mbps 系统盘:高性能云硬盘 网络:Default-VPC	(公) 后 「」 (内) 后	包年包月 2022-08-01 16:56:18到期	按流量计费	默认项目	© 1	登录 续费	更多 ▼
共 1 条									20 👻		1 /1页	► H



验证点3:假设公司新增加一个 H5 类的项目,该如何调整权限策略适配

公司新增 H5 项目后,如果我们需要增加 H5 项目的开发权限,则无需对策略本身进行变更,仅需要:

- 1. 为 H5 项目的开发同事创建新的子用户。
- 2. 为子用户绑定 H5 项目对应的标签,关联 access-assume-role 策略即可。
按标签鉴权时支持仅匹配标签键

最近更新时间: 2024-10-11 11:55:22

本文档介绍如何为您的子账号授予某个标签下所有资源的权限以及如何授予子账号只能绑定某个标签键的权限。

() 说明:

resource_tag 授予某个标签下所有资源的权限,request_tag 授予子账号只能绑定某个标签键的权限,对于控制台列表及相关 API 不生效。

授予关联某个标签键下所有资源的权限(resource_tag)

操作场景

若您的公司购买了多种腾讯云资源,资源均通过标签分组管理,希望能够授予关联某个标签键下所有资源的权限(resource_tag)。 假设存在以下条件:

- 企业账号 CompanyExample 下有个子账号 Operator。
- 企业账号 CompanyExample 下有个为运营的标签键。
- 企业账号 CompanyExample 希望给子账号 Operator 授予标签键运营下的所有资源。

操作步骤

- 1. 使用企业账号 CompanyExample 登录 访问管理控制台。
- 2. 在策略页面,单击新建自定义策略 > 按策略语法创建。
- 3. 在选择模板类型下选择空白模板,单击下一步,进入编辑策略页面。

1 选择策略模板 > 2 编辑策略	
模板类型: 全部模板 ▼ 输入策略名关键词进行搜索 Q	
选择模板类型	
全部機版 (共566个)	
○ 空白模版	AdministratorAccess 该策略允许您管理账户内所有用户及其权限、财务相关的信息、云服务资产。
QCloudFinanceFullAccess 该策略允许您管理账户内财务相关的内容,例如:付款、开票。	ReadOnlyAccess 该策略允许您只读访问账户内所有支持接口级鉴权或资源级鉴权的云服务资产。
 QcloudAAFullAccess 活动防劑(AA)全读写访问权限 	 QcloudABFullAccess 代理记账 (AB) 全读写访问权限
下一步	

- 4. 进入编辑策略页面,填写如下表单:
 - 策略名称: 默认为 policygen-当前日期 ,推荐您自行定义一个不重复且有意义的策略名称,例如 Operator-resource_tag 。
 - 描述:可选,自行编写。
 - 策略内容:复制以下内容并填写。其中,运营为标签键名称,可为中文和英文,false 为固定的标签值。

```
{
    "version": "2.0",
        "statement": [
        {
            "effect": "allow",
            "action": "*",
```



_	
	"qcs:resource_tag/ 运营": "false"

- 5. 单击完成,完成策略的创建。新建的策略将显示在策略列表页。
- 6. 在 策略列表 中搜索找到刚才已创建的策略,单击右侧操作列下的关联用户/组/角色。

① 用户或者用户组与策略关联后,即可获得策日	略所描述的操作权限。							
新建自定义策略 删除			全部策略	预设策略	自定义策略	搜索策略名称/描述/备注(多关键词空格隔开)	Q ¢ <u>+</u>
策略名	服务类型 ▼	描述				上次修改时间	操作	
Operator-resource_tag	-	-				2023-09-26 17:19:06	删除关联用	户/组/角色

7. 在弹出的**关联用户/用户组/角色**窗口中,搜索勾选子账号 Operator,单击确定完成授权操作。 子账号 Operator 将拥有标签运营下所有资源的权限。

支持多关键词(间隔为空格)	搜索用户名/ID/SecretId/手机/邮箱/备	Q		之称	米刑	
一 用户	切换成用户组或角色 🔻					•
✓ Operator	用户			Operator	用户	U
in ar	用户					
	用户		\Leftrightarrow			
,	用户					
	用户					
	用户					

授予子账号只能绑定某个标签键的权限(request_tag)

操作场景

若您的公司购买了多种腾讯云资源,资源均通过标签分组管理,希望能够授予子账号只能绑定某个标签键的权限(request_tag)。 假设存在以下条件:

- 企业账号 CompanyExample 下有个子账号 Developer。
- 企业账号 CompanyExample 下有个为开发的标签键。



● 企业账号 CompanyExample 希望给子账号 Developer 授予只能绑定**开发**标签键的权限(request_tag)。

操作步骤

腾讯云

- 1. 使用企业账号 CompanyExample 登录 访问管理控制台。
- 2. 在策略页面,单击新建自定义策略 > 按策略语法创建。
- 3. 在选择模板类型下选择空白模板,单击下一步,进入编辑策略页面。

板类型:	全部模板 🔻	输入策略名关键词进行搜索	Q	
择模板类	型			
全部模版	(共566个)			
0	空白模版		(AdministratorAccess 该策略允许您管理账户内所有用户及其权限、财务相关的信息、云服务资产。
0	QCloudFinanceFullAccess 该策略允许您管理账户内财务相关的	内容,例如:付款、开票。	(ReadOnlyAccess 该策略允许您只读访问账户内所有支持接口级鉴权或资源级鉴权的云服务资产。
0	QcloudAAFullAccess 活动防刷 (AA) 全读写访问权限		(QcloudABFullAccess 代理记账 (AB) 全读写访问权限

- 4. 进入编辑策略页面,填写如下表单:
 - 策略名称:默认为 policygen-当前日期 ,推荐您自行定义一个不重复且有意义的策略名称,例如 Developer-request_tag。
 - 描述:可选,自行编写。
 - 策略内容:复制以下内容并填写。其中,开发为标签键名称,可为中文和英文,false 为固定的标签值。



5. 单击完成,完成策略的创建。新建的策略将显示在策略列表页。



6. 在 策略列表 中搜索找到刚才已创建的策略,单击右侧操作列下的关联用户/组/角色。

新建自定义策略 删除			全部策略	预设策略	自定义策略	搜索策略名称/描述/备注(多关键	詢空格隔开) Q 文 보
策略名	服务类型 ▼	描述				上次修改时间	操作
Developer-request_tag	-	-				2023-09-25 17:09:16	删除 关联用户/组/角色

7. 在弹出的**关联用户/用户组/角色**窗口中,搜索勾选子账号 Developer,单击**确定**完成授权操作。 子账号 Developer 将拥有只能绑定**开发**标签键的权限。

译称加时用广(共 27 节)				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/备	Q		名称	类型	
— 用户	切换成用户组或角色 🔻			Developer	用户	ß
✓ Developer	用户					
-	用户					
	用户		+			
	用户					
	用户					
	用户					

关联文档

如果您想了解如何将资源和标签建立关联关系,请参见 管理标签 。

创建资源时强制绑定固定标签键值

最近更新时间: 2024-11-28 11:21:41

本文档介绍如何为您的子账号授予在子账号创建资源时,强制给资源绑定固定标签键值的权限策略。

() 说明:

强制绑定标签:是指用户可以通过 CAM 权限策略配置,指定子用户或角色在创建资源的时候,必须绑定权限策略里面指定的标签键值对才能创建,不绑 定标签或者绑定其他标签都会创建失败。

操作场景:

若您希望您的子账号(Operator)在购买云服务器(CVM)资源时,只能绑定某个标签键值的权限。 假设存在以下条件:

企业账号 CompanyExample 下有个子账号 Operator。

企业账号 CompanyExample 下有个为(App&Dev)的标签键值。

企业账号 CompanyExample 希望给子账号 Operator 授予只能绑定(App&Dev)标签键值的权限。

操作步骤

- 1. 使用企业账号 CompanyExample 登录 访问管理控制台。
- 2. 在策略页面,单击新建自定义策略 > 按策略语法创建。
- 3. 在选择模板类型界面选择空白模板,单击下一步,进入编辑策略页面。

1	选择的	策略模板 > 2 编辑	衰略		
模板类	裡:	全部模板 ▼	输入策略名关键词进行搜索 C		
选择模	誕飯类	型			
全部	部模版	(共566个)			
	•	空白模版		0	AdministratorAccess 该策略允许您管理账户内所有用户及其权限、财务相关的信息、云服务资产。
		QCloudFinanceFullAccess 该策略允许您管理账户内财务相关的	内容,例如:付款、开票。		ReadOnlyAccess 该策略允许您只读访问账户内所有支持接口级鉴权或资源级鉴权的云服务资产。
		QcloudAAFullAccess 活动防刷 (AA) 全读写访问权限			QcloudABFullAccess 代理记账 (AB) 全读写访问权限
- م	步	•			

4. 在编辑策略页面,填写下列内容:

- 策略名称:默认为 policygen-当前日期,推荐您自行定义一个不重复且有意义的策略名称,例如 Operator-request_tag。
- 描述: 可选, 自行编写。
- 策略内容:复制以下内容并填写。





	"App&Dev"
},	
{	
},	
{	N - 66 + N - N - 11 N
}	
]	
}	
① 说明:	
· 通过 acs	stresource tag 控制:可以访问所有绑定标签(Ann&Dev)的资源。
, 通过 ~~~	
● 通迟 qcs	
 其他不支 · · ·	持资源级授权的接口需要在最后一个 effect 里面附加授予,本策略增加了 cvm:CreateSecurityGroup 和 tag、vpc 权限,
可按需添加	ЛИо

- 5. 单击**完成**,完成策略的创建。新建的策略将显示在策略列表页。
- 6. 在策略列表中搜索找到刚才已创建的策略,单击右侧操作列的关联用户/组/角色。

新建自定义策略 删除			全部策略	预设策略	自定义策略	搜索策略名称/描述/备注(多乡	会議 (1997) (19977) (19977) (19977) (1997) (1997) (1997) (1997) (1997) (1997) (1997	Ŧ
策略名	服务类型 ▼	描述				上次修改时间	操作	
Developer-request_tag	-	-				2023-09-25 17:09:16	删除 关联用户/组/角色	

7. 在弹出的**关联用户/用户组/角色**窗口中,搜索勾选子账号 Operator,单击**确定**完成授权操作。子账号 Operator 将拥有只能绑定(项目名称&Dev)标签键 值的权限。



支持多关键词(间隔为空格)		Q		夕弥	米刑	
一 用户	切换成用户组或角色 🍸			-1100	~±	
 Operator 	用户			Operator	用尸	0
	用户					
	用户		↔			
•	用户					
	用户					
	用户					

- 8. 登录子账号 Operator ,在不设置标签和不设置对应标签(App&Dev)的情况下,尝试购买服务器。
 - 不设置标签情况下,购买失败。

标签 ()	杨登雄 > 杨登值 >	删除	
	+ 添加		
	② 键值和贴版		
实例名称 ⑦	选填,不填默认未命名,支持自动批量命名		
	支持批量连续命名或指定模式串命名,最多128个字符,你还可以输入128个字符		
登录方式 ⑦	设置密码 立即关联密钥 自动生成密码		
	(注意)创建后,自动生成的密码将通过站内信和邮箱发送给您,也可登录CVM控制台重置密码。		
实例销毁保护 ⑦	防止实例通过控制台或者API误销毁		
安全加固	✔ 免费开通		
	安装组件免费开通DDoS防护和主机安全基础版 ⑦		
云监控	✔ 免费开通		
	免费开递云产品监控、分析和实时告誓,安装组件获取主机监控指标 ⊘		
自动化助手	✔ 免费开通		
	—— 安装组件免费开通自动化助手,免密码、免SSH登录即可批量管理实例、执行命令,完成日常管理任务 ⑦		
高级设置 (主机名、C	M 角色、置放群组、自定义数据) 🎽		
已选 SA5.MEDIUM	(标准型SA5,2核2GB) 时长 1个月 / 子子3天3名 数量 - 1 +		费用宣询中 上一步 下一步:确认配置信息





○ 不设置对应标签(App&Dev)情况下,购买失败。

其他设置								
标签 ()	AGD V dev V	删除						
	+ 75/10							
	② 罐值粘贴板							
实例名称 🕜	选填,不填默认未命名,支持自动批量命名							
	支持批量连续命名或批定模式串命名,最多128个字符,你还可以输入128个字符							
登录方式 ⑦	设置密码 立即关联密钥 自动生成密码							
	注意的提后,自动生成的密码将通过站内信和邮箱发送给您。也可登录CVM控制台重要密码。							
实例销毁保护 ⑦	防止实例通过控制台或者API误销毁							
安全加固	✓ 免费开通							
	安装组件免费开递DDoS防护和主机安全基础版 🕥							
云监控	✔ 免费开通							
	免费开通云产品监控、分析和实时告望,安装组件获取主机监控指标 ②							
自动化助手	✓ 免费开通							
	安装结件免费并通自动化如手,免密码、免SSH整杂即可批量管理实例、执行命令,完成日常管理任务 🕐							
高级设置 (主机名、CAM 角色、置放群组、自定义数据) >>								
已洗 SA5 MEDIUM	2/标准图\$A5_2#2GB) 时长 1个月 ~ \$5555 数量 - 1 +							





○ 在设置对应标签(App&Dev)情况下,购买成功。

标签 ()	App V Dev V Bill	
	+ 75.0	
实例名称 ⑦	透現,不填默认未命名,支持自动批量命名	
	支持批量连续命名或指定模式丰命名,最多128个字符,仍还可以输入128个字符	
登录方式 ②	设置密码 立即关联密钥 自动生成器码	
	[2] 台段云,自动生成的密码将通过站内结和攀稿发送给您。也可是来CVM控制台重重密码。	
实例销毁保护 ⑦	5. 防止实例通过控制台域者API误销限	
安全加固	柔.费开通 家庭相传免费开递D0065的产程主机安全基础级 ①	
云监控	文表开通 文表用通訊/単品目表、分析和取り合葉、支展目中存取主系品目示相称 ③	
自动化助手	☑ 免费开通 实家组件免费开通自动化加手、免密码、免疫研查点部可监监管理实例、执行命令、完成日常管理任务 ⑦	
高级设置 (主机名、CA	M 角色、重数群组、自定义数据) ≫	
已选 SA5.MEDIUM2	(標准型SA5,2模2GB) 时长 1个月 ~ 5 年5年 数量 - 1 ÷	费用查询中 上一步 下一步:确认配置信息



产品清单											
~ 3	页付费产品 (1)							应付合计			
ŕ	*品名称	配置		类型	单价	数量	时长		订单金额		
9	前新云服务器	地域: 可用区: 机型: 镜像: 存储: 带宽: 不面网络: 所在子网: 收起	南京 南京一区 SA5.MEDUM2 (2楼CPU, 2G内穿) OpenClouIdOS Server 9 系统盘 (50GB 道用型SSD乙硬盘) 按带宽计费 (带宽OMbps) 未命名	新狗		xl	1个月				
摺	記购买 船低优惠只用此页面										
不	一年,下一代CDN—EdgeOne 止加速,更享边缘安全智能服务,个人版每月]赠50GB安全	全流量+300万次安全请求			浙			+		
M	ySQL8.0版1核-1G-50G 限时限购1个					0.9折起			+		
企 提	12 安倉—6058存候、5人可用 代文件存储、在线协作等服务,提升数据管理双率								+		
高限	性能数据缓存服务Redis 时专享特惠 1G/1个月					5.1折起			+		
							实付金额		去支付		

腾讯云

使用 MFA 保护 API 请求

最近更新时间: 2025-04-11 15:17:12

本文档介绍如何为您的子账号在请求 API 时,要求先进行 MFA 多因素认证后再允许调用 API。

操作场景

本文档介绍如何通过腾讯云访问管理(CAM)的自定义策略,限制未经过 MFA 多因素认证的身份请求敏感 API 操作。通过为策略添加 MFA 条件键 "qcs:mfaPresent",可要求用户在调用 API 前完成 MFA 设备认证,提升账号安全性。

典型场景示例:

- 要求跨账号扮演角色时必须通过 MFA 认证。
- 限制未绑定 MFA 的用户终止云服务器(CVM)实例。
- 保护敏感操作(例如删除 COS 存储桶、修改数据库密码等)。

前提条件

- 服务支持:目标 API 操作需支持 qcs:mfaPresent 条件键,详情请参见 支持 CAM 的业务接口(支持 qcs:mfaPresent 的接口范围与"支持 IP 限制"的接口范围相同)
- MFA 设备:用户需提前绑定 MFA 设备,在控制台使用的用户需要开启登录保护。(如未绑定,请参见 步骤 1:绑定虚拟 MFA 并开启登录保护)

注意事项

MFA 设备限制

- 使用 API 调用时,仅支持虚拟 MFA 设备(例如 Google Authenticator、Microsoft Authenticator、腾讯云助手小程序),暂不支持手机号验证码、 微信扫码验证。
- 使用控制台登录时,需开启登录保护,登录保护的验证方式不限于虚拟 MFA、手机号验证码、微信扫码验证。

操作步骤

步骤 1: 绑定虚拟 MFA 并开启登录保护

- 1. 管理员操作
 - 进入**访问管理控制台** > 用户列表,选择目标子用户,在用户详情页面中,为其开启用户登录保护,并选择虚拟 MFA 验证方式。详情请参见 为子账号设 置安全保护 。
 - 检查用户 MFA 绑定状态,确保为绑定状态。
 - 确保有访问控制台权限的子用户开启了登录保护,要求登录时验证 MFA 动态口令。
- 2. 子用户操作
 - 未绑定虚拟 MFA 设备的子用户,登录腾讯云控制台,根据指引绑定虚拟 MFA 设备。
 - 已绑定虚拟 MFA 设备的子用户,登录腾讯云控制台,根据指引输入 MFA 动态口令进行身份验证。

步骤 2: 创建 MFA 保护策略

1. 策略语法

在 CAM 策略中,通过 condition 字段添加 qcs:mfaPresent 条件键,限制 API 调用必须附带 MFA 认证。 **示例策略**(限制终止 CVM 实例):





2. 策略关联

将策略关联至目标用户/用户组,确保权限生效。

步骤 3:调用支持 MFA 的 API

用户需通过以下方式获取临时凭证并调用 API:

方式 1: GetSessionToken (获取 MFA 临时凭证)

- 适用场景:当前账号内受策略保护的 API 操作(例如 COS 桶删除)。
- API 调用示例:

```
curl -X POST <https://sts.tencentcloudapi.com> \

-H "Authorization: TC3-HMAC-SHA256 ..." \

-d '{

    "Action": "GetSessionToken",

    "Name": "temp_token",

    "Policy": "{\"version\":\"2.0\", ...}",

    "SerialNumber":"qcs::cam:uin/12345678::mfa/softToken", # 输入虚拟MFA序列号

    "MfaCode": "123456" # 输入虚拟 MFA 动态口令

}'
```

使用示例

场景:强制删除 COS 存储桶前验证 MFA

1. 策略配置

2. 用户操作

- 调用 GetSessionToken 接口获取临时凭证(需附带 MFA 动态口令)。
- 使用临时凭证调用 cos:DeleteBucket 接口删除存储桶。

♀ 警告:

使用示例仅作演示作用,请根据使用场景替换策略中的"effect"、"action"、"resource"等信息。避免误删 COS 桶,造成业务损失。

方式 2: AssumeRole (角色代入)

- 适用场景: 跨账号访问或角色委托。
- API 调用示例:



```
curl -X POST <https://sts.tencentcloudapi.com> \
-H "Authorization: TC3-HMAC-SHA256 ..." \
-d '{
    "Action": "AssumeRole",
    "RoleArn": "qcs::cam::uin/12345678:role/TestRole",
    "RoleSessionName": "test",
    "DurationSeconds": 7200,
    "SerialNumber":"qcs::cam:uin/12345678::mfa/softToken", # 输入虚拟 MFA 序列号
    "MfaCode": "123456" # 输入虚拟 MFA 动态口令
}'
```