访问管理

用户指南

产品文档

腾讯云

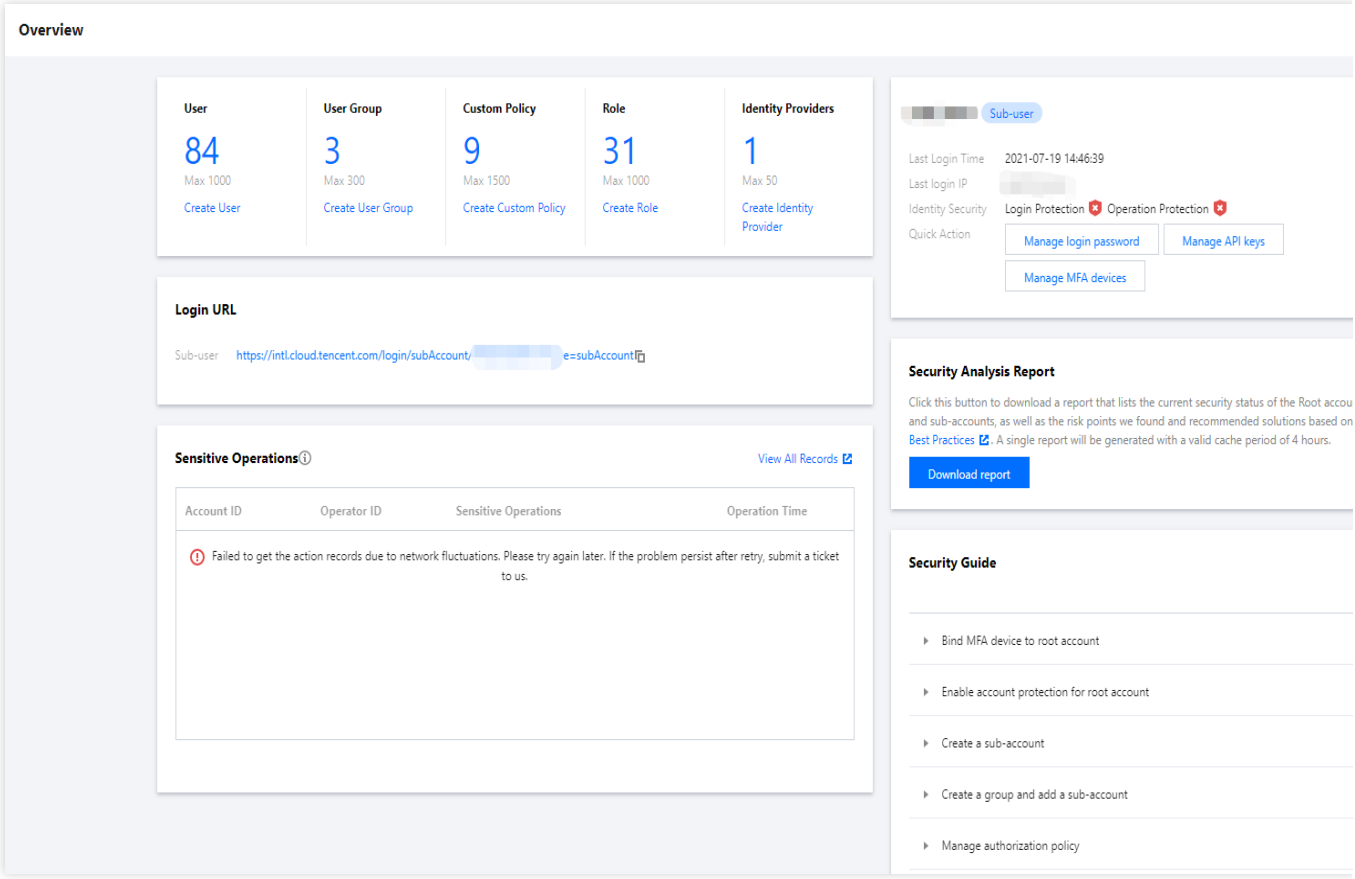
文档目录

用户指南

概览

最近更新时间：2024-12-16 17:25:30

访问管理控制台 的概览页包括六大模块：**访问管理资源**、**登录链接**、**敏感操作**、**上次登录信息**、**安全分析报告**、**安全指引**。



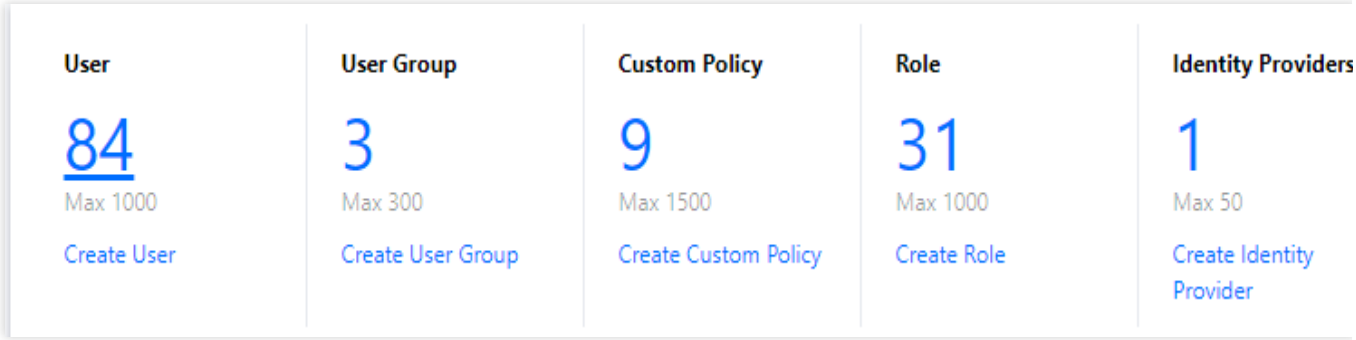
概览页权限

具有 QcloudCamSummaryAccess 策略权限的用户登录控制台，可查看所有模块的信息。
没有 QcloudCamSummaryAccess 策略权限的用户登录控制台，只能查看**登录链接**和**上次登录信息**。
主账号、管理员用户（AdministratorAccess）均已包含该策略权限。
子账号可以联系主账号（在 用户列表 > **用户详情**页面）查看其是否具有 QcloudCamSummaryAccess 策略权限。
主账号可以将 QcloudCamSummaryAccess 策略授权给需要的子账号，允许子账号查看控制台概览页的所有信息。
授权方法请参考 授权管理。

概览页模块

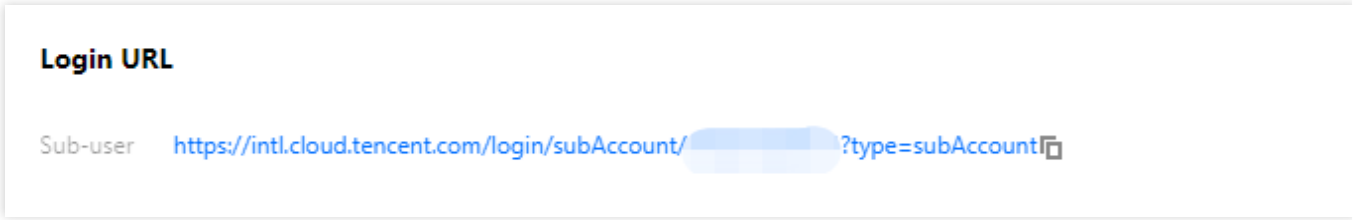
访问管理资源

访问管理资源模块展示当前主账号下所创建的用户、用户组、自定义策略、角色、身份提供商数量。您可以通过单击数量下方的按钮，进入对应的创建页面。



登录链接

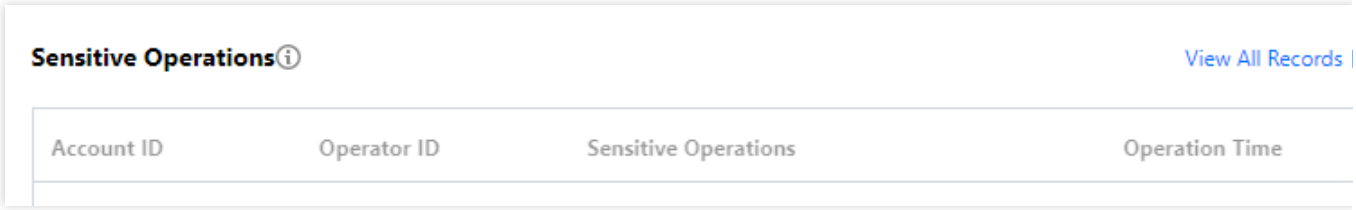
登录链接模块展示了子用户的登录链接。主账号和子账号均可通过链接右侧的复制按钮复制链接。



子用户登录链接：适用于子用户。

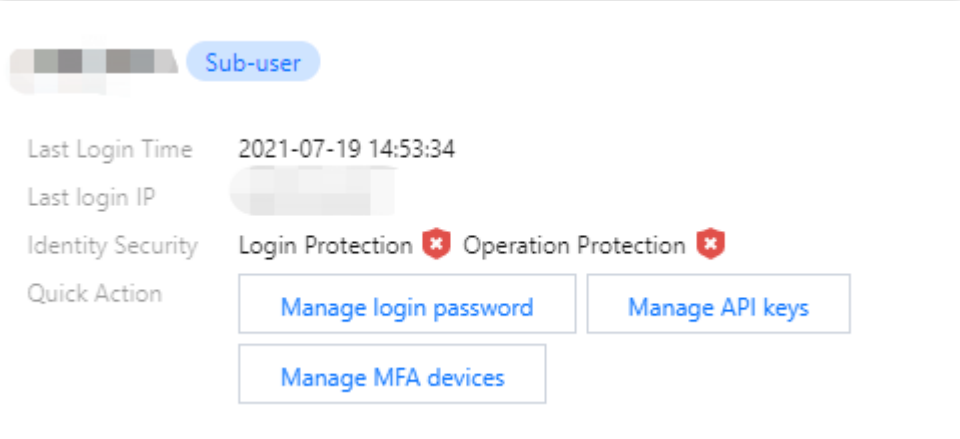
敏感操作

敏感操作模块展示最近3天（最高50条）当前主账号下所有敏感操作的概览信息，展示信息包括：账号 ID、操作者 ID、详细敏感操作和操作时间。用户还可以通过单击【查看所有记录】，进入云审计控制台，查看更详细的敏感操作记录。



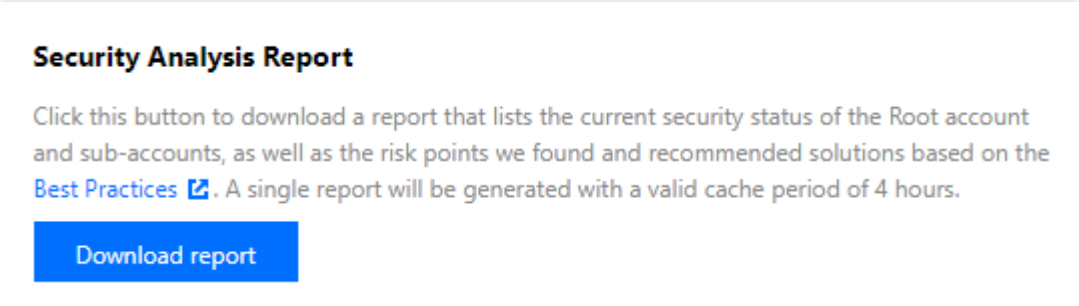
上次登录信息

上次登录信息模块展示当前账号的上次登录时间，上次登录 IP、身份安全状态、管理 API 密钥、管理 MFA 设置快捷操作入口。



安全分析报告

安全分析报告模块提供了【下载报告】按钮，您可以单击该按钮获取当前主子账号的安全状态，以及基于 安全实践教程 我们发现的风险点以及推荐方案。单次报告生成有效缓存期为4小时。



安全指引

注意：

为了保障您的账户以及云上资产的安全，我们强烈建议您完成安全指引下的所有设置。

安全指引模块为用户提供基础 CAM 功能学习和必要的安全操作指引，包括主账号绑定 MFA 设备、主账号开启账号保护、创建子账号和创建组并添加子账号等。

操作权限：**主账号绑定 MFA 设备** 和 **主账号开启账号保护** 两项设置只有主账号具有操作权限；其余五项设置，获得授权的所有用户都可以进行操作。

指引状态：各指引项分为 **未完成** 和 **已完成** 两种状态。主账号登录控制台可以看到各指引项的状态，具有权限的子账号无法查看状态。

设置入口：具有权限的子账号可通过单击各指引项左侧的三角符号查看对应的功能介绍和相应的设置入口。下图是主账号登录控制台后的安全指引模块示例。

Security Guide

- Bind MFA device to root account
- Enable account protection for root account
- Create a sub-account
- Create a group and add a sub-account
- Manage authorization policy
- Enable account protection for sub accounts
- Bind an MFA device to sub-account

用户
主账号
主账号相关

最近更新时间：2024-01-23 17:29:58

操作场景

本文档介绍主账号权限设置，消息接收，您可以通过以下步骤了解主账号权限以及如何修改消息接收方式。

前提条件

已注册腾讯云账号即主账号，主账号注册请参阅 注册腾讯云。

操作步骤

主账号无需授权

主账号默认拥有账号下腾讯云所有资源，无需授权，可以任意访问其任何资源。因此，不建议您使用主账号对资源进行操作，应创建子账号并按照最小权限原则赋予策略，使用权限范围有限的子账号操作您的云资源。更多账号权限的使用建议请参阅 最佳实践。

主账号消息接收

您注册腾讯云主账号时登记的安全手机、安全邮箱将同时作为初始消息接收方式。若您在 账号中心 - 控制台 内修改了安全手机或安全邮箱，您在 访问管理（CAM）- 控制台 用于腾讯云消息通知的联系手机或联系邮箱不会同步修改，如需修改请参阅 主账号消息订阅。

注意：

为避免您因消息遗漏造成的损失，请您及时前往 访问管理（CAM）- 控制台 确认用于消息订阅的联系手机或联系邮箱是否符合预期。

关联文档

如果您想了解如何修改主账号用于安全验证的安全手机或安全邮箱，请参阅 邮箱手机号常见问题。
如果您想了解如何创建子用户，请参阅 新建子用户。

如果您想了解如何为子账号设置权限，请参阅 授权管理。

主账号消息订阅

最近更新时间：2024-01-23 17:29:58

操作场景

本文档介绍如何为主账号修改、验证消息通知渠道以及设置订阅消息。如需主账号接收消息通知，需主账号验证通过消息渠道，为其订阅消息后主账号已验证通过的消息渠道即可接收相关的消息提醒。

前提条件

已登录访问管理控制台，进入 用户列表管理控制台 页面。

操作指南

验证消息通知渠道

1. 在用户列表管理控制台页面，找到用户类型为主账号的用户。
2. 单击**用户名称**进入用户详情页。
3. 在用户详情页，单击用户信息栏下的**发送验证**。如没有**发送验证**按钮，表示该消息通知渠道已完成验证，无需进行以下操作。

手机：系统将会向主账号已设置的手机号发送验证消息，用户收到验证消息后确认链接，即可完成验证手机消息渠道。

邮箱：系统将会向主账号已设置的邮箱发送验证消息，用户收到验证消息后确认链接，即可完成验证邮箱消息渠道。

修改消息通知渠道

1. 在用户列表管理控制台页面，找到用户类型为主账号的用户。
2. 单击**用户名称**进入用户详情页。
3. 在用户详情页单击右上角**修改**。
4. 在弹出的编辑信息页面，您可以变更您需要修改的手机，邮箱信息。
5. 修改消息通知渠道需要验证消息渠道才可正常接收消息，如何验证请参阅 验证消息通知渠道。

设置订阅消息

1. 在用户列表管理控制台页面，找到用户类型为主账号的用户。
2. 单击右侧操作列的**更多操作** > **订阅消息**。

3. 在弹出的 “订阅消息” 窗口，勾选需订阅的消息类型（可打开折叠按钮 “►”，选择具体需要的消息接收类型）。
4. 单击**确定**，完成设置订阅消息操作。

关联文档

如果您想了解如何为协作者订阅消息，请参阅 协作者消息订阅。
如果您想了解如何为子用户订阅消息，请参阅 子用户消息订阅。
如果您想了解如何为消息接收人订阅消息，请参阅 消息接收人消息订阅。

子用户
新建子用户

最近更新时间：2024-01-23 17:35:43

操作场景

如果您是拥有管理员权限（AdministratorAccess）或者拥有访问管理全读写权限（QcloudCamFullAccess）的子账号，在腾讯云购买了云服务器、私有网络、对象存储等多个云上资源，可以创建一个或多个子账号提供给您的团队成员，允许其访问您的云上资源。

该任务指导您使用管理员账号，在访问管理控制台创建一个子用户，并为其绑定权限策略。

说明：

子用户和协作者都属于子账号，相关定义和权限说明请参考 用户类型。

创建方式	适用场景	说明
快速创建	创建管理员用户	默认拥有 AdministratorAccess 权限，可修改
自定义创建	普通子用户、消息接收者	根据需要绑定策略权限

前提条件

已 创建拥有管理员权限的子账号 或拥有（QcloudCamFullAccess）的子账号。

操作指南

通过控制台创建

说明：

您可以点击以下页签，查看不同类型子账号创建及授权方式。

未实名认证主账号24小时内最多创建10个子账号。

快速创建

自定义创建

1. 登录腾讯云控制台，进入 用户列表， 单击**新建用户**，进入新建用户页面。
2. 在新建用户页面，单击**快速创建**，进入快速创建用户页面。
3. 在快速创建用户页面，在“设置用户信息”栏补充填写用户名，其它选项可根据需要调整。

说明：

单击**新建用户**可一次最多创建10个用户。

4. 在“需要设置重置密码”栏，根据您的实际需求勾选设置子用户下次登录时是否需要重置密码。

5. 单击**创建用户**进入提示成功创建用户页面。

6. 在提示成功创建用户页面，您可以通过以下两种方法获取子用户信息。

单击**发送至**补充您的邮箱信息，系统将把完整的子用户信息发送至邮箱。

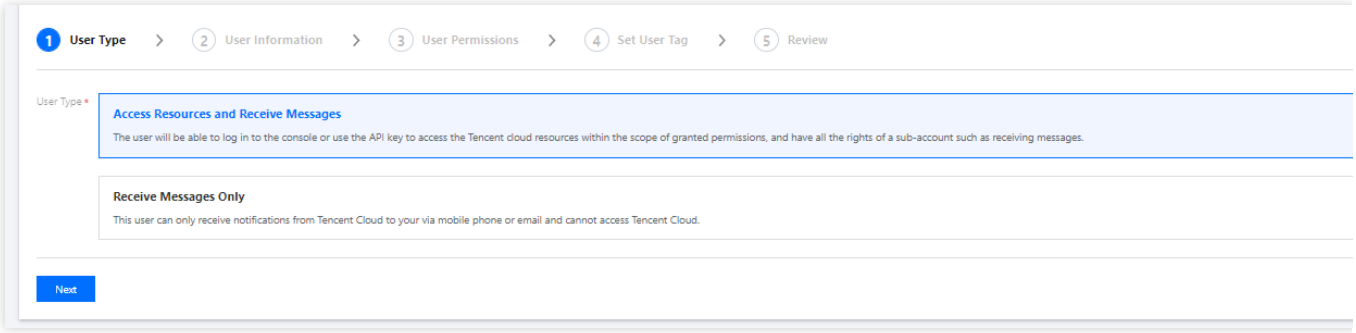
单击**复制**，粘贴保存至本地。

1. 登录访问管理控制台，并在左侧导航栏中，选择**用户** > **用户列表**，进入用户列表管理页面。

2. 在用户列表管理页面，单击**新建用户**，进入新建用户页面。

3. 在新建用户页面，单击**自定义创建**，进入选择用户类型页面。

4. 在选择用户类型页面，单击**可访问资源并接收消息**或**仅用于接收消息**后，单击**下一步**填写用户信息。



5. 根据页面提示填写并确认信息，单击**完成**，完成自定义创建子用户操作。

若为**可访问资源并接收消息**，进入提示新建子用户成功页面。

若为**仅用于接收消息**，进入用户列表页面。

通过 API 创建

您可以通过访问密钥调用 AddUser 接口添加子用户并设定权限，详细请参阅 添加子用户-API 文档。

关联文档

如果您想了解如何通过用户组管理子用户进行分组授权，请参阅 为用户组添加/移除用户、为用户组添加/解除策略。

如果您想了解如何为子用户添加、删除关联的策略，请参阅 子用户权限设置。

如果您想了解如何子用户如何登录，请参阅 子用户登录。

如果您想了解如何为子用户重置密钥，请参阅 为子用户重置登录密码。

如果您想了解如何为子用户订阅消息，请参阅 子用户消息订阅。

子用户权限设置

最近更新时间：2024-01-23 17:35:43

操作场景

本文档介绍如何授权和解除子用户关联的策略，子用户将在获得的权限范围内管理主账号下的资源。

操作步骤

为子用户授权关联策略

直接关联

您可以直接为用户关联策略以获取策略包含的权限。

1. 登录访问管理控制台，进入 用户列表 管理页面。
2. 在用户列表管理页面，选择需要设置权限的子用户。
3. 单击右侧操作列的**授权**。
4. 在弹出的关联策略窗口里勾选需要授权的策略（可多选）。
5. 单击**确定**完成直接为子用户授权关联策略操作。

随组关联

您可以将用户添加至用户组，用户将自动获取该用户组所关联策略的权限，通过此种方法获取的策略类型为随组关联。如需解除随组关联策略，需将用户移出相应用户组。

1. 登录访问管理控制台，进入 用户列表 管理页面。
2. 在用户列表管理页面，选择需要设置权限的子用户。
3. 单击右侧操作列的**更多操作 > 添加到组**。
4. 勾选需要添加到的用户组（可多选）。
5. 单击**确定**，完成通过添加到组进行随组关联策略操作。

为子用户解除关联策略

直接解除子用户关联策略

您可以直接解除用户关联的策略以解除用户关联的权限。

1. 登录访问管理控制台，进入 用户列表 管理页面。
2. 在用户列表管理页面，找到需要解除关联策略的子用户。
3. 单击子用户名称，进入用户详情页。
4. 进入用户详情页，单击**权限**，进入权限操作栏。

5. 在权限操作栏，找到需要解除的策略。
6. 单击右侧**解除** > **确定解除**，完成为子用户解除关联策略操作。

从组中移出用户

您可以从组中移出用户以解除用户关联的策略

1. 登录访问管理控制台，进入 用户列表 管理页面。
2. 在用户列表管理页面，找到需要解除关联策略的子用户。
3. 单击子用户名称，进入用户详情页。
4. 在用户详情页，单击**组**，进入用户组操作栏。
5. 在用户组操作栏，找到需要解除的策略。
6. 单击右侧操作列的**移出该组** > **确定移除**，完成通过从组中解除子用户关联策略的操作。

子用户安全凭证
子用户登录

最近更新时间：2024-01-23 17:37:00

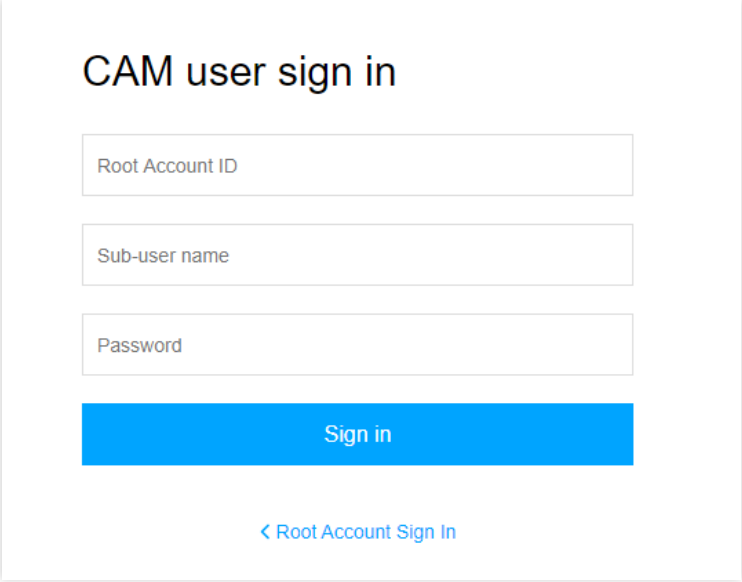
操作场景

本文档介绍如何登录子用户，登录成功后子用户将在权限范围内管理主账号下的资源。

操作步骤

子用户登录

1. 进入 腾讯云子用户登录 页面进行账号登录。
2. 在子用户登录页面，输入主账号 ID、子用户名、登录密码信息，如下图所示：



说明：

主账号 ID 即子用户所属主账号 ID。账号 ID（例如：100001234567）是账号在腾讯云的唯一标识，请联系主账号在 账号信息 处查看。

3. 单击**登录**，完成子用户登录操作。

为子用户重置登录密码

最近更新时间：2024-01-23 17:35:43

操作场景

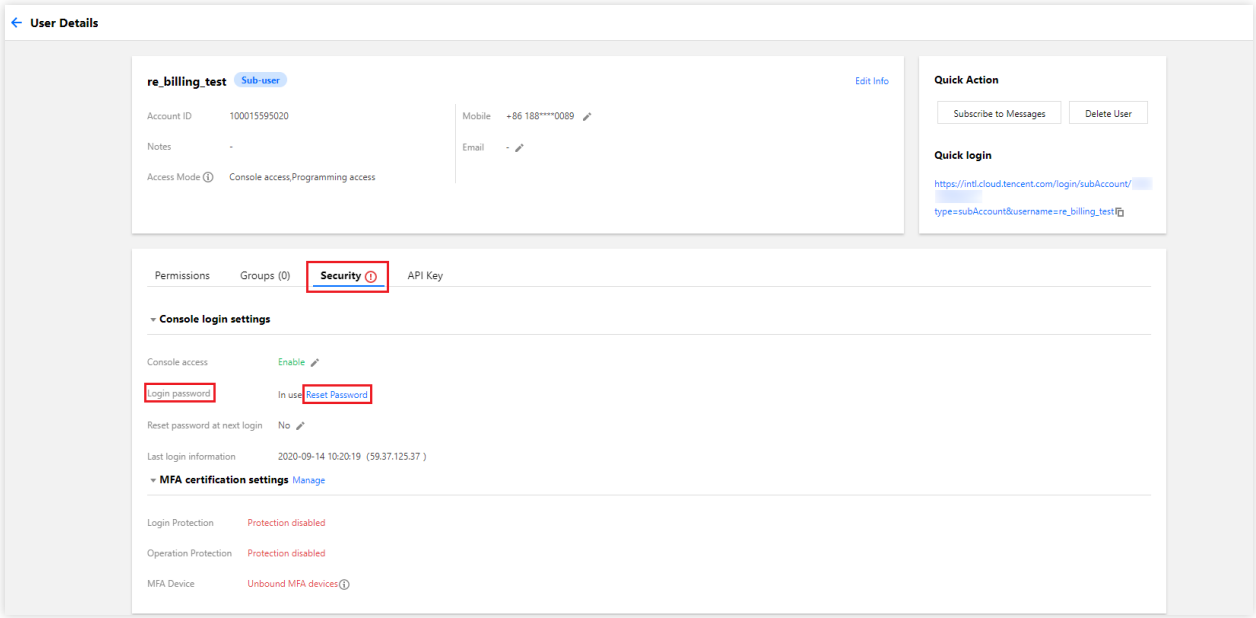
本文档介绍如何修改子用户密码，修改之后可以通过新的密码登录子用户管理主账号下资源。

操作步骤

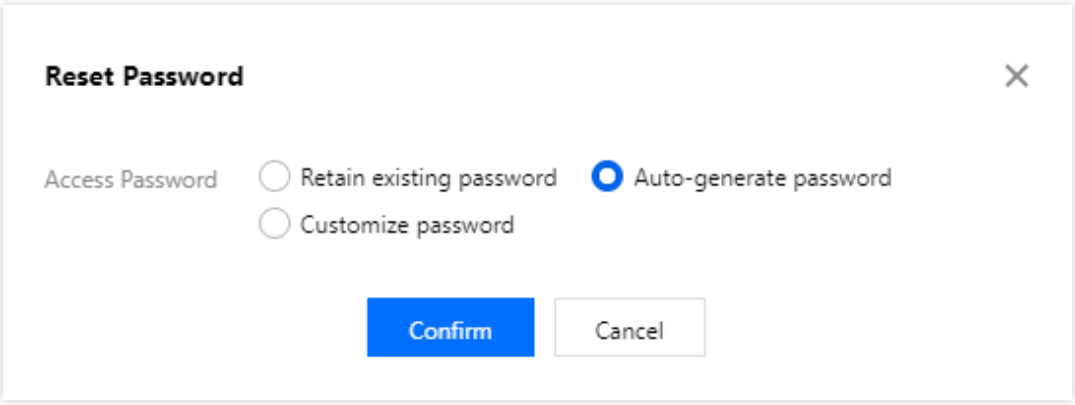
说明：

该步骤仅适用于通过自定义创建的子用户。

1. 在 用户列表 中选择需要修改密码的子用户，选择具体**用户名称**，进入用户详情页。
2. 在用户详情页中选择**安全** > **控制台登录设置** > **登录密码**，单击**重置密码**。如下图所示：



3. 在弹出的**重置密码**窗口中，设置当前用户密码。如下图所示：



若您需要为子用户设置新密码，您可以通过以下两种方式。

若您在**访问密码**中选择**自动生成的密码**，系统会自动生成控制台登录密码。您可以复制保存，如有需要可以单击**下载.csv** 保存密码。

若您在**访问密码**中选择**自定义密码**，输入您为该子用户设置的控制台登录密码。

若您需要当前用户自行重置密码，可勾选**需要重置密码**，子用户在下次登录成功后将被要求重新设置控制台登录密码。

关联文档

如果您想了解如何通过自定义方式创建子用户，请参阅 自定义创建子用户。

如果您想了解如何修改协作者登录密码，请参阅 修改账号密码。

为子用户设置安全保护

最近更新时间：2024-01-23 17:38:26

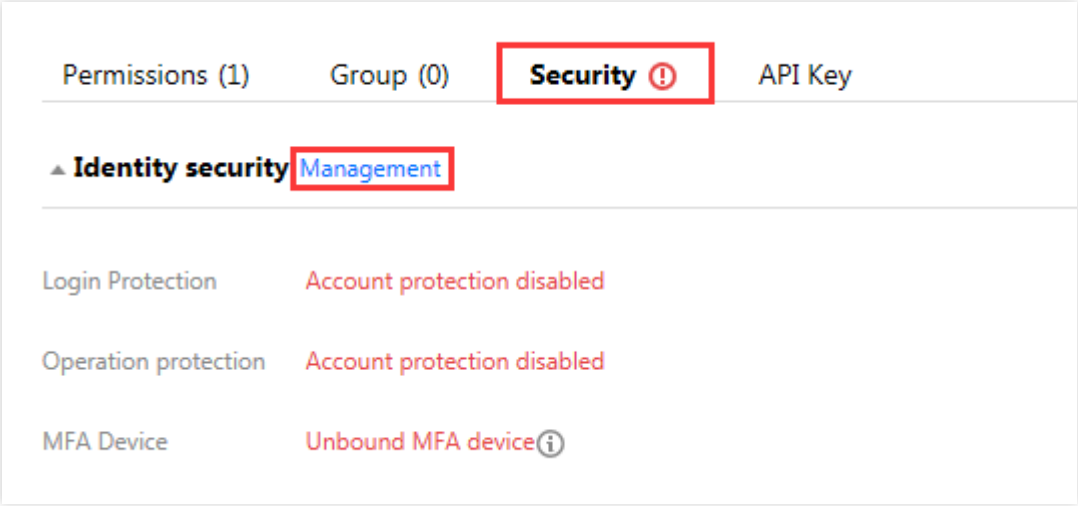
操作场景

本文档介绍如何开启和关闭子用户的安全保护，子用户将根据设置判断是否进行安全验证。

操作步骤

为子用户开启安全保护

1. 登录访问管理控制台，并在左侧导航栏中，选择**用户** > 用户列表，进入用户列表管理页面。
2. 在用户列表管理页面，选择需要设置安全保护的子用户。
3. 单击**用户名称**，进入用户详情页面。
4. 在用户详情页面，单击**安全**，进入安全管理页面。
5. 在安全管理页面，单击身份安全操作栏下的**管理**。如下图所示：



6. 在弹出的身份安全窗口中，勾选需要开启的保护类型，为当前子用户开启相应的安全保护。
7. 单击**确定**，完成为子用户开启安全保护操作。

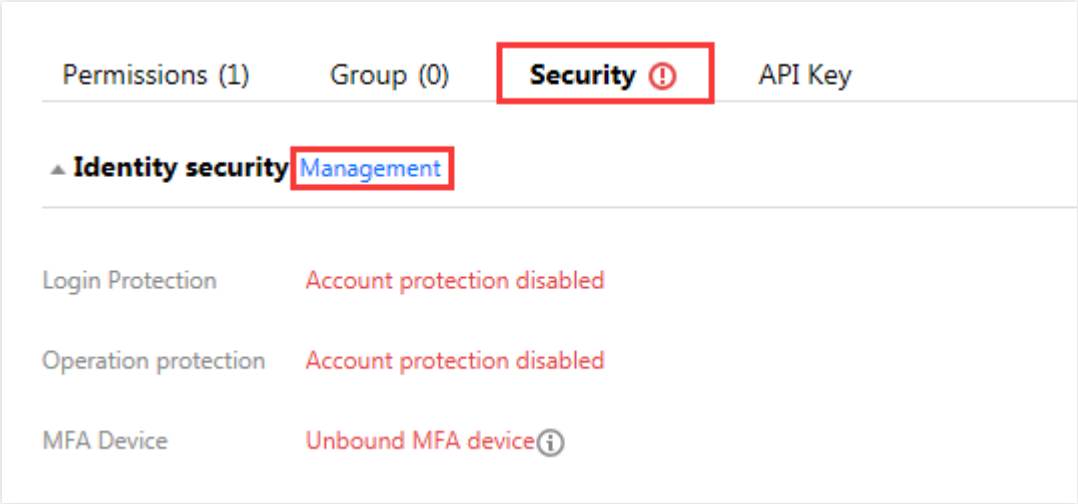
说明：

启用虚拟 MFA 设备校验之后，子用户需在下次登录时按照页面指引进行 MFA 设备绑定。

为子用户关闭安全保护

1. 登录访问管理控制台，并在左侧导航栏中，选择**用户** > 用户列表，进入用户列表管理页面。

2. 在用户列表管理页面，选择需要设置安全保护的子用户。
3. 单击**用户名称**，进入用户详情页面。
4. 在用户详情页面，单击**安全**，进入安全管理页面。
5. 在安全管理管理页面，单击身份安全操作栏下的**管理**。如下图所示：



6. 在弹出的身份安全窗口中，勾选需要关闭的保护类型，为当前子用户关闭相应的安全保护。
7. 单击**确定**，完成为子用户关闭安全保护操作。

子用户订阅消息

最近更新时间：2024-01-23 17:35:43

操作场景

本文档介绍如何为子用户验证消息渠道以及设置订阅消息。如需子用户接收消息，需子用户验证通过消息渠道，为其订阅消息后该用户已验证通过的消息渠道即可接收相关的消息提醒。

操作指南

验证消息渠道

1. 登录访问管理控制台，进入 用户列表 管理页面。
2. 在用户列表管理页面，找到需订阅消息的子用户。
3. 单击**用户昵称**进入用户详情页。
4. 在用户详情页，单击用户信息栏下的**发送验证链接**。

手机：系统将会向该子用户已设置的手机号发送验证消息，用户收到验证消息后确认链接，即可完成验证手机消息渠道。

邮箱：系统将会向该子用户已设置的邮箱发送验证消息，用户收到验证消息后确认链接，即可完成验证邮箱消息渠道。

设置订阅消息

1. 登录访问管理控制台，进入 用户列表 管理页面。
2. 在用户列表管理页面，找到需订阅消息的子用户。
3. 单击右侧操作列的**更多操作 > 订阅消息**。
4. 在弹出的**订阅消息**窗口，勾选需订阅的消息类型（可打开折叠按钮 “▼”，选择具体需要的消息接收类型）。
5. 单击**确定**，完成设置订阅消息操作。

子用户信息查询

最近更新时间：2024-01-23 17:35:43

操作场景

本文档介绍如何查看用户的消息订阅、备注、上次登录时间、上次登录方式、MFA 状态等信息，以及如何通过用户名、账号 ID、SecretId、手机、邮箱、备注等关键词搜索子用户。

前提条件

已登录访问管理控制台，进入 用户列表 管理页面。

操作步骤

使用抽屉查看子用户信息

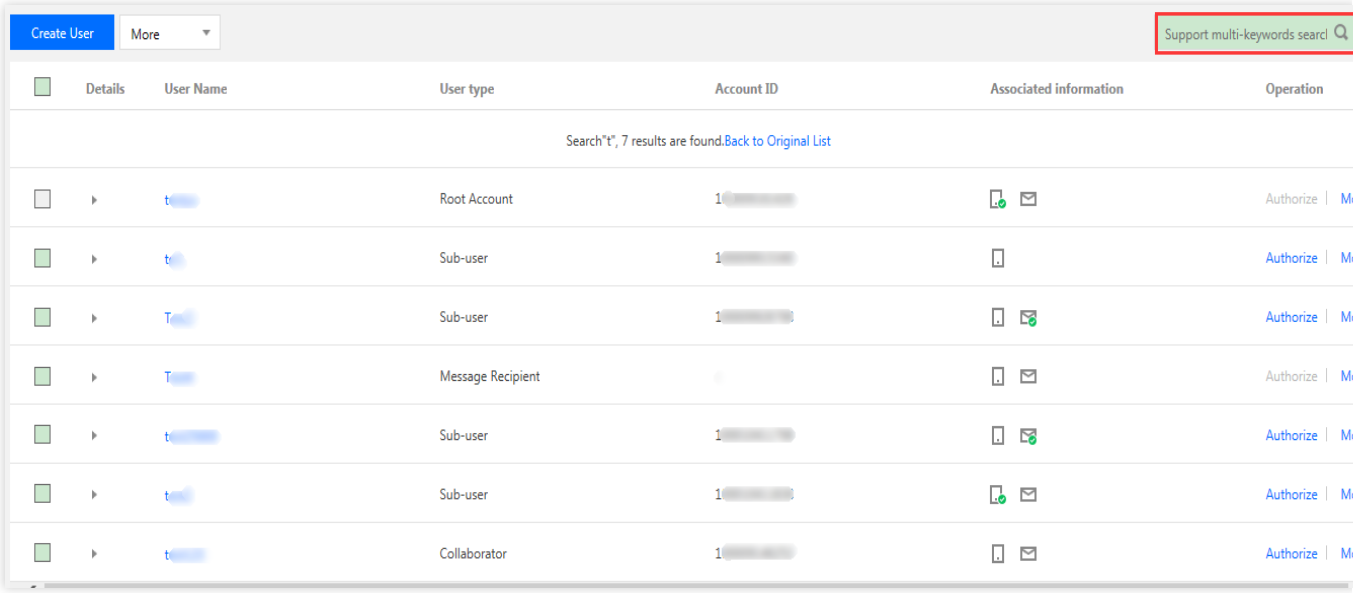
您可以在此查看子用户的用户组、消息订阅、登录保护、操作保护、MFA 设备状态、控制台访问状态等信息。

1. 在用户列表管理页面，找到需要查看的子用户。
2. 单击左侧的详情列图标 “▶”。
3. 在展开的抽屉信息里可以查看子用户的相关信息，完成使用抽屉查看子用户信息操作。

通过搜索框找到子用户

您可以通过用户名、账号 ID、SecretId、手机、邮箱、备注等关键词搜索子用户。

1. 在用户列表管理页面，找到右上角的搜索框。
2. 在搜索框中输入关键字，单击右侧搜索图标，可以搜索到相关子用户，完成通过搜索框找到子用户操作。如图所示：


Create User
More
Support multi-keywords searcl
Details
User Name
User type
Account ID
Associated information
Operation
Search"t", 7 results are found.Back to Original List
Root Account
Sub-user
Sub-user
Message Recipient
Sub-user
Sub-user
Collaborator
Authorize

删除子用户

最近更新时间：2024-01-23 17:35:43

操作场景

本文档介绍如何删除单个或者多个子用户，删除之后，子用户将不再拥有该主账号的管理权限。

前提条件

已登录访问管理控制台，进入 用户列表 管理页面。

操作步骤

删除单个子用户

1. 在用户列表管理页面，找到需要删除的子用户。
2. 单击右侧操作列的**更多** > **删除**。
3. 在弹出的删除用户窗口，确认当前子用户下的 API 密钥已禁用且删除，详细请参考 访问密钥。
4. 单击**确认删除**，完成删除单个子用户操作。

删除多个子用户

1. 在用户列表管理页面，左侧勾选需删除的子用户。
2. 单击左上方的**更多操作** > **删除**。
3. 在弹出的删除用户窗口，确认已勾选子用户下的 API 密钥已禁用且删除，详细请参考 访问密钥。
4. 单击**确认删除**，完成删除多个子用户操作。

禁用子用户

最近更新时间：2024-07-17 10:17:28

操作场景

本文档介绍如何禁用单个子用户。禁用之后，用户将无法通过已禁用的子用户登录控制台或编程访问本账号内的资源、且不再接收消息。此外，禁用子用户时会同时禁用以下三个权限：禁止子用户登录控制台、禁用子用户当前所有的 API 密钥，并禁止子用户接收订阅消息和系统消息。若用户想继续启用此子用户，请参见 启用已禁用的子用户 重新启用即可。

前提条件

已登录访问管理控制台，进入 用户列表 页面。

操作步骤

1. 在**用户列表**页面，找到需要禁用的子用户。
2. 单击右侧操作列的**更多操作 > 禁用**。
3. 在弹出的**禁用用户**窗口，单击**禁用**，即可完成禁用子用户的操作。

启用已禁用的子用户

最近更新时间：2024-07-17 10:17:44

操作场景

本文档介绍如何启用已禁用的子用户。三项禁用权限逐项启用之后，用户可重新通过子用户登录控制台或编程访问本账号内的资源、且重新接收消息。若想重新禁用此用户，请参见 禁用子用户 重新禁用即可。

前提条件

已登录访问管理控制台，进入 用户列表 页面。

操作步骤

启用子用户控制台访问权限

1. 在**用户列表**页面，找到需要启用的子用户。
2. 单击该子用户的**用户名称**进入**用户详情**页面。
3. 单击**用户详情**页面中的**安全 > 控制台登录设置 > 控制台访问**右侧的

。
4. 在弹出的**管理控制台访问**页面，选择**启用**，并按需选择相关信息，如下图所示：

5.单击**确定**即可。

启用子用户访问密钥权限

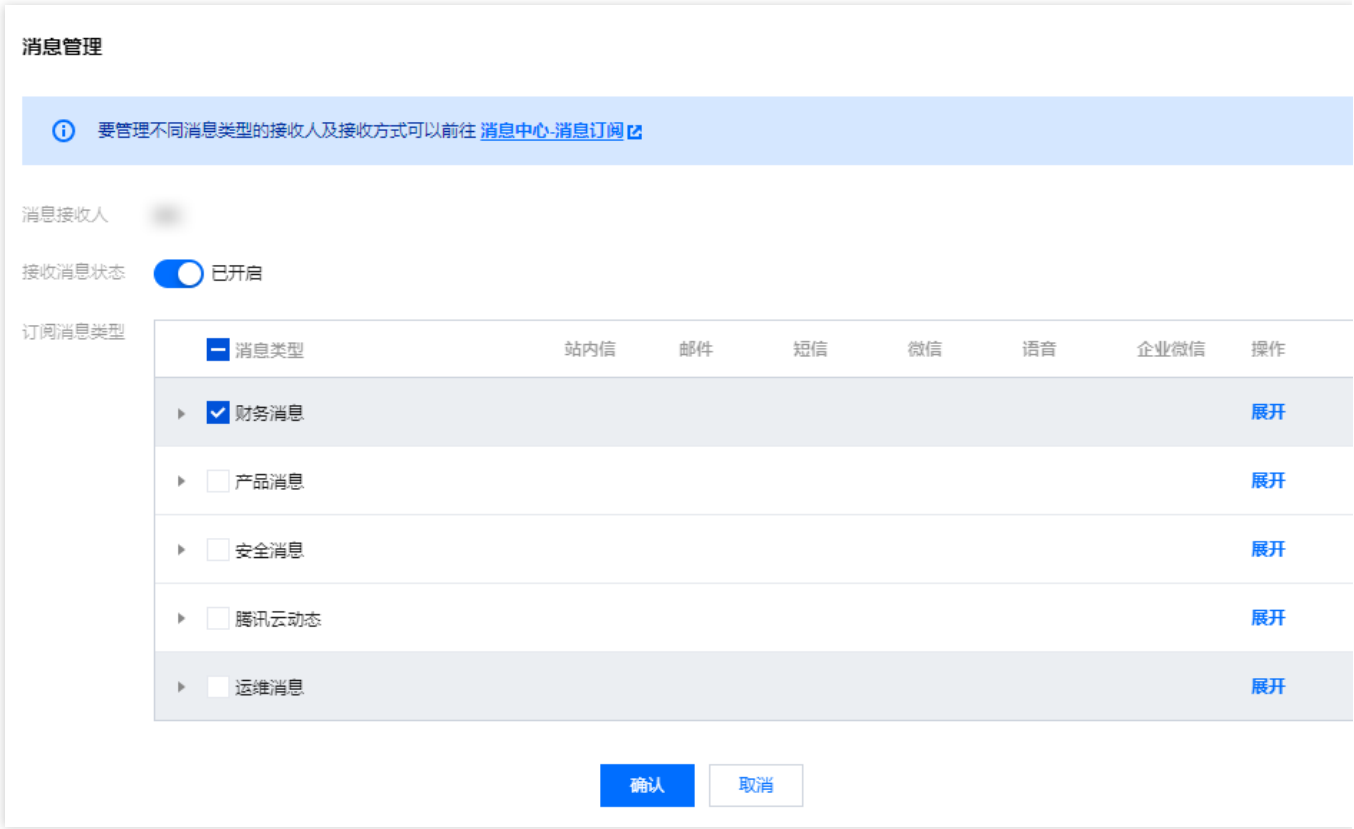
1. 在**用户列表**页面，找到需要启用的子用户。
2. 单击该子用户的**用户名称**进入**用户详情**页面。
3. 单击**用户详情**页面中的**API 密钥**，单击**启用**即可，如下图所示：

启用子用户接收消息权限

1. 在**用户列表**页面，找到需要启用的子用户。
2. 单击该子用户的**用户名称**进入**用户详情**页面。
3. 单击**用户详情**页面中的**快捷操作 > 消息管理。**

4. 在弹出的**消息管理**页面，单击**接收消息状态**右侧的

，设置为**已开启**后，按需选择订阅消息类型，单击**确认**即可。



协作者
新建协作者

最近更新时间：2024-01-23 17:31:58

操作场景

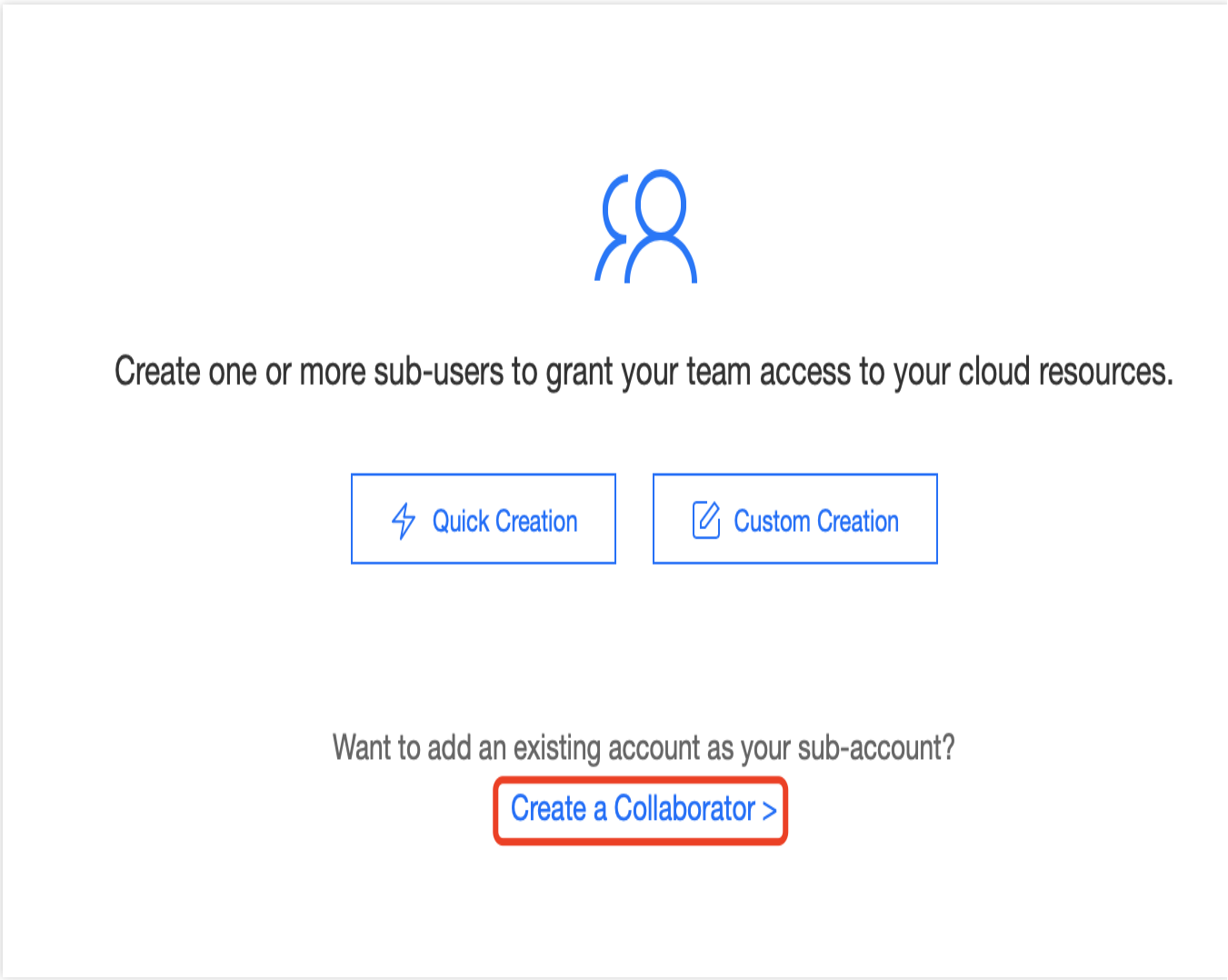
如果您是管理员用户，在腾讯云购买了云服务器、私有网络、对象存储等多个云上资源，可以将团队其他成员的腾讯云账号设置为协作者，允许其访问您的云上资源。
该任务指导您使用管理员账号，在访问管理控制台创建一个协作者，并为其绑定权限策略。
说明：
协作者和子用户都属于子账号，相关定义和权限说明请参考 用户类型。

前提条件

已 创建管理员用户。
已有可以作为协作者的腾讯云账号（若没有，请先 注册腾讯云账号）。

操作指南

1. 登录腾讯云控制台，进入 用户列表， 单击**新建用户**，进入新建用户页面。
2. 在新建用户页面，单击**前往创建协作者**。



3. 填写相关用户信息，单击**下一步**。

说明：

协作者默认允许登录腾讯云控制台，暂不支持取消。

为了保证您的账号安全，建议您开启登录保护和操作保护。

账号ID为腾讯云唯一标识符，需要您即将添加的协作者前往 账号中心-账号信息 进行查看。

4. 设定权限，您可以通过以下三种方法为当前新建的协作者设定权限。策略描述了权限，关联策略后协作者即获得策略描述的权限。

添加至组获得随组权限：使用组是按工作职能来管理用户权限的最佳做法，您可以通过随组关联获得权限。单击**添加至组获得随组权限**，勾选需要的用户组，将协作者添加到现有用户组或新建的用户组，协作者可以随组关联到该组附加的策略。

复制现有用户策略：通过复制现有用户的权限为协作者关联策略，单击**复制现有用户策略**，勾选需要复制的用户，协作者可以关联到被复制用户附加的策略。

通过从策略列表中授权：单击**从策略列表中选取策略关联**，勾选需要关联的策略。

5. 单击**完成**，完成新建协作者操作。

关联文档

如果您想了解新创建的协作者账号如何登录腾讯云，请参阅 子账号登录控制台-协作者登录。

协作者权限设置

最近更新时间：2024-01-23 17:31:58

操作场景

本文档介绍如何授权和解除协作者关联的策略，协作者将在获得的权限范围内管理主账号下的资源。

操作指南

为协作者授权关联策略

直接关联

您可以直接为用户关联策略以获取策略包含的权限。

1. 登录腾讯云控制台，进入 用户列表， 找到需授权策略的协作者，单击右侧操作列的**授权**。
2. 勾选需要授权的策略（可多选），单击**确定**，完成为协作者授权关联策略操作。

随组关联

您可以将用户添加至用户组，用户将自动获取该用户组所关联策略的权限，通过此种方法获取的策略类型为随组关联。如需移除随组关联策略，需将用户移出相应用户组。

1. 登录腾讯云控制台，进入 用户列表， 找到需授权策略的协作者，单击右侧操作列的**更多操作 > 添加到组**。
2. 勾选需要添加到的用户组（可多选），单击**确定**，完成通过添加到组进行随组关联策略操作。

为协作者解除关联策略

直接解除协作者关联策略

您可以直接解除用户关联的策略以解除用户关联的权限。

1. 登录腾讯云控制台，进入 用户列表， 找到需要解除关联策略的协作者，单击协作者**用户名称**，进入协作者详情页。
2. 单击**权限**，在列表中找到需要解除的策略，单击右侧操作列的**解除**。
3. 单击**确认解除**，完成为协作者解除关联策略操作，解除后该用户将无法获得该策略所描述的相关权限。

从组中移出协作者

您可以将用户移出用户组，用户将自动解除随该用户组所关联的权限。

1. 登录腾讯云控制台，进入 用户列表， 找到需要解除关联策略的协作者，单击协作者名称，进入协作者详情。
2. 单击**权限**，在列表中找到需要解除的随组关联的策略，单击右侧操作列的**解除**。

3. 单击**确认解除**，将协作者移出用户组，随组关联的策略被解除，解除后该用户将无法获得该组关联的相关权限。

协作者安全凭证
协作者登录

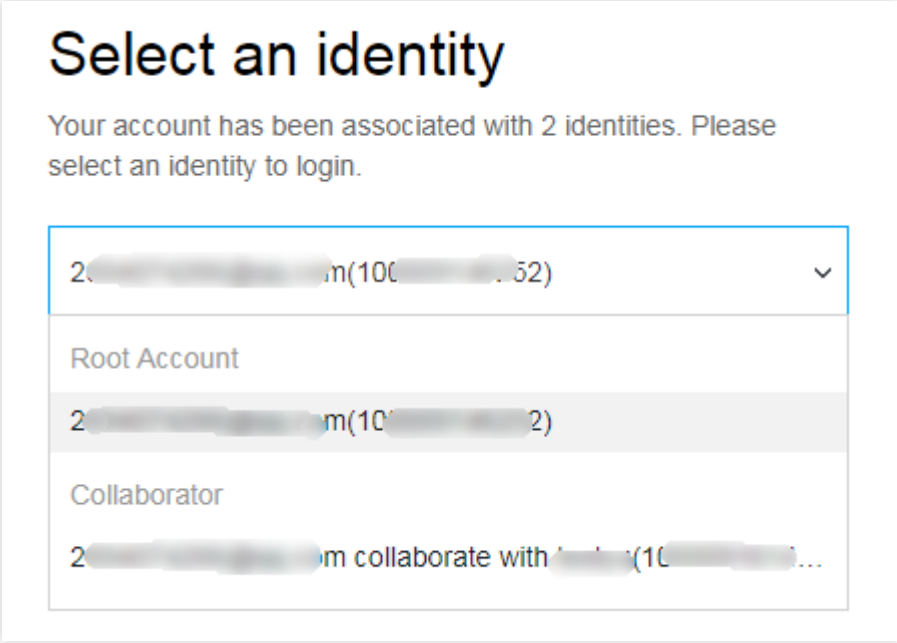
最近更新时间：2024-01-23 17:31:58

操作场景

本文档介绍如何登录协作者账号，登录成功后协作者将在权限范围内管理主账号下的资源。

操作步骤

1. 进入 腾讯云账号登录 页面，选择被添加协作者账号的登录方式。
2. 输入账号信息或者扫码成功之后，进入选择用户身份页面，如下图所示：



3. 在选择用户身份页面，单击账号信息右侧的

，选择需要管理的主账号身份。
4. 单击**登录**，完成协作者账号登录操作。

为协作者设置安全保护

最近更新时间：2024-01-23 17:31:59

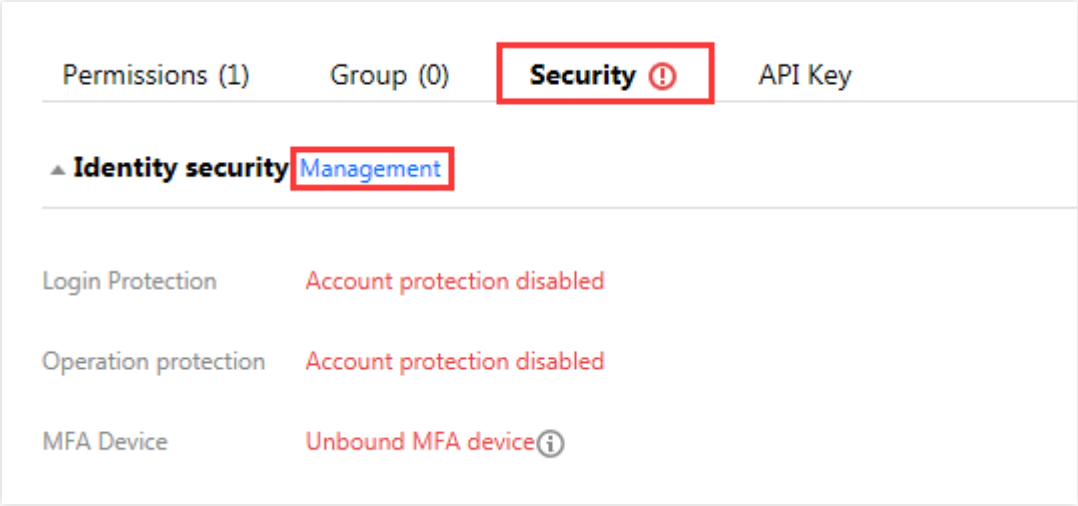
操作场景

本文档介绍如何开启和关闭协作者的安全保护，协作者将根据设置判断是否进行安全验证。

操作步骤

为协作者开启安全保护

1. 登录访问管理控制台，并在左侧导航栏中，选择**用户** > 用户列表，进入用户列表管理页面。
2. 在用户列表管理页面，选择需要设置安全保护的协作者。
3. 单击**用户名称**，进入用户详情页面。
4. 在用户详情页面，单击**安全**，进入安全管理页面。
5. 在安全管理管理页面，单击身份安全操作栏下的**管理**。如下图所示：



6. 在弹出的身份安全窗口中，勾选需要开启的保护类型，为当前协作者开启相应的安全保护。
7. 单击**确定**，完成协作者开启安全保护操作。

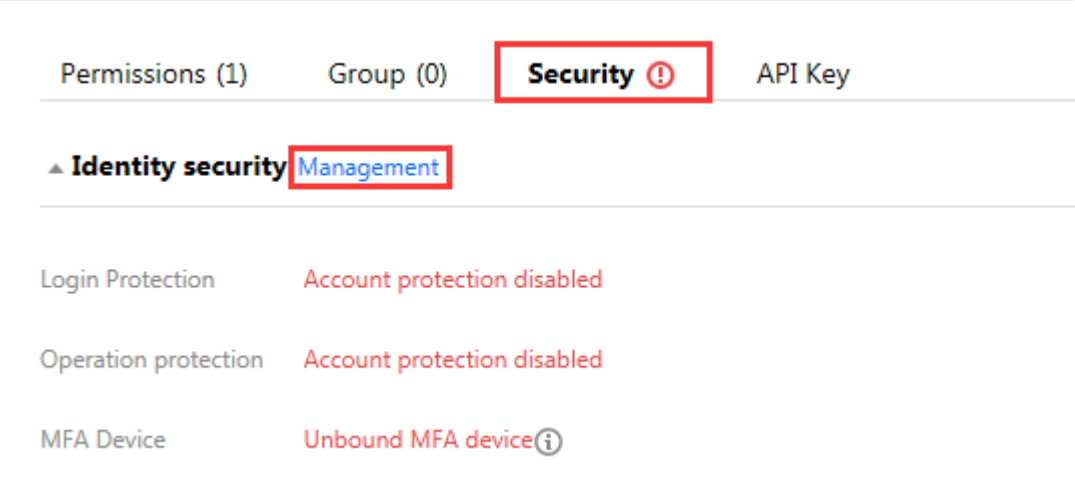
说明

启用虚拟 MFA 设备校验之后，协作者需在下次登录时按照页面指引进行 MFA 设备绑定。

为协作者关闭安全保护

1. 登录访问管理控制台，并在左侧导航栏中，选择**用户** > 用户列表，进入用户列表管理页面。
2. 在用户列表管理页面，选择需要设置安全保护的协作者。

3. 单击**用户名称**，进入用户详情页面。
4. 在用户详情页面，单击**安全**，进入安全管理页面。
5. 在安全管理管理页面，单击身份安全操作栏下的**管理**。如下图所示：



6. 在弹出的身份安全窗口中，勾选需要关闭的保护类型，为当前协作者关闭相应的安全保护。
7. 单击**确定**，完成为协作者关闭安全保护操作。

协作者订阅消息

最近更新时间：2024-01-23 17:31:58

操作场景

本文档介绍如何为协作者验证消息渠道以及设置订阅消息。如需协作者接收消息，需协作者验证通过消息渠道，为其订阅消息后该用户已验证通过的消息渠道即可接收相关的消息提醒。

操作指南

验证消息渠道

1. 登录访问管理控制台，并在左侧导航栏中，选择**用户** > 用户列表，进入用户列表管理页面。
2. 在用户列表管理页面，找到需订阅消息的协作者。
3. 单击**用户昵称**进入用户详情页。
4. 在用户详情页，单击用户信息栏下的**发送验证链接**。

手机：系统将会向该协作者已设置的手机号发送验证消息，用户收到验证消息后确认链接，即可完成验证手机消息渠道。

邮箱：系统将会向该协作者已设置的邮箱发送验证消息，用户收到验证消息后确认链接，即可完成验证邮箱消息渠道。

设置订阅消息

1. 登录访问管理控制台，并在左侧导航栏中，选择**用户** > 用户列表，进入用户列表管理页面。
2. 在用户列表管理页面，找到需订阅消息的协作者。
3. 单击右侧操作列的**更多操作 > 订阅消息**。
4. 在弹出的 “订阅消息” 窗口，勾选需订阅的消息类型（可打开折叠按钮 “▼”，选择具体需要的消息接收类型）。
5. 单击**确定**，完成设置订阅消息操作。

协作者信息查询

最近更新时间：2024-01-23 17:31:58

操作场景

本文档介绍如何查看协作者的用户组、消息订阅、登录保护、操作保护、MFA 设备状态、控制台访问状态等信息，以及如何通过用户名、账号 ID、SecretId、手机、邮箱、备注等关键词搜索协作者。

前提条件

已登录访问管理控制台，进入 用户列表 管理页面。

操作步骤

使用抽屉查看协作者信息

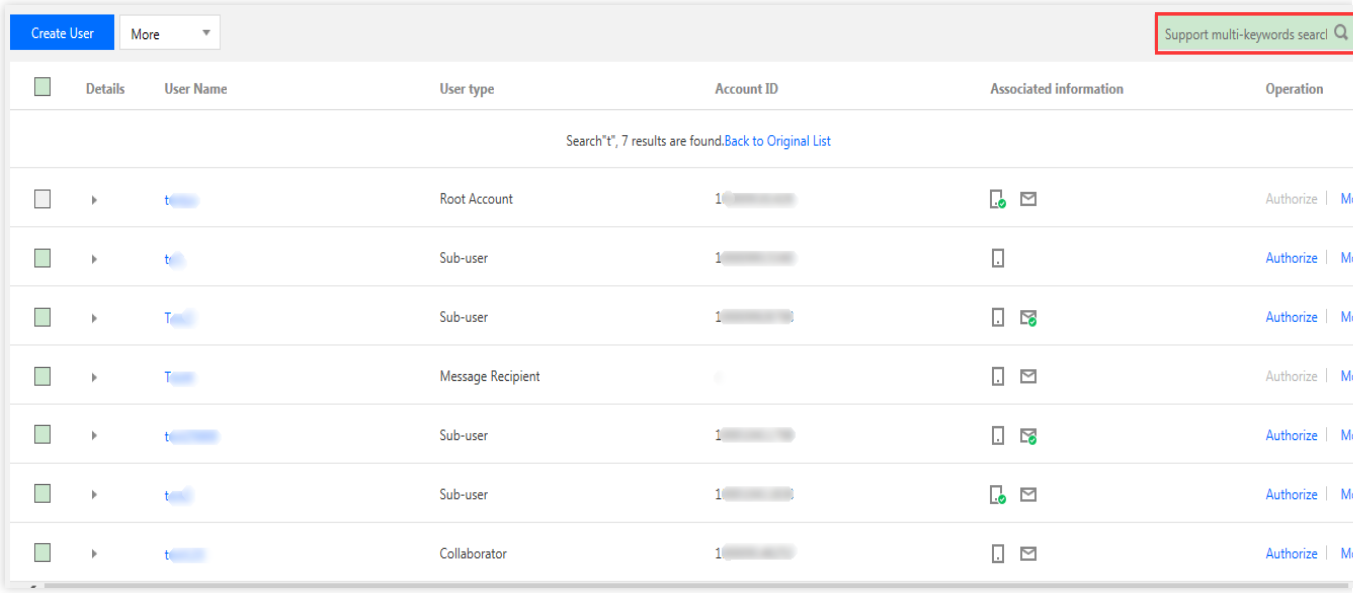
您可以在此查看协作者的用户组、消息订阅、登录保护、操作保护、MFA 设备状态、控制台访问状态等信息。

1. 在用户列表管理页面，找到需要查看的协作者。
2. 单击左侧的详情列图标 “▶”。
3. 在展开的抽屉信息里可以查看协作者的相关信息，完成使用抽屉查看协作者信息。

通过搜索框找到协作者

您可以通过用户名、账号 ID、SecretId、手机、邮箱、备注等关键词搜索协作者。

1. 在用户列表管理页面，找到右上角的搜索框。
2. 在搜索框中输入关键字，单击右侧搜索图标，可以搜索到相关协作者，完成通过搜索框找到协作者。如下图所示：


Create User
More
Support multi-keywords searcl
Details
User Name
User type
Account ID
Associated information
Operation
Search"t", 7 results are found.Back to Original List
Root Account
Sub-user
Sub-user
Message Recipient
Sub-user
Sub-user
Collaborator
Authorize

删除协作者

最近更新时间：2024-12-16 17:25:30

操作场景

本文档介绍如何删除单个或者多个协作者，删除之后，协作者将不再拥有该主账号的管理权限。

前提条件

已登录访问管理控制台，进入 用户列表 管理页面。

操作步骤

删除单个协作者

1. 在用户列表管理页面，找到需要删除的协作者。
2. 单击右侧操作列的**更多** > **删除**。
3. 在弹出的删除用户窗口，确认当前协作者下的 API 密钥已禁用且删除。
4. 单击**确认删除**，完成删除单个协作者操作。

删除多个协作者

1. 在用户列表管理页面，左侧勾选需删除的协作者。
2. 单击左上方的**更多操作** > **删除**。
3. 在弹出的删除用户窗口，确认已勾选协作者下的 API 密钥已禁用且删除。
4. 单击**确认删除**，完成删除多个协作者操作。

协作者身份切换

最近更新时间：2024-01-23 17:31:58

操作场景

本文档介绍如何切换协作者所属主账号身份，在权限范围内管理对应主账号下的资源。

前提条件

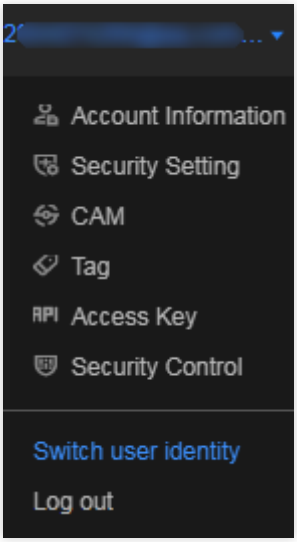
登录账号为其他主账号的协作者。

说明：

关于协作者的创建请参考 新建协作者。

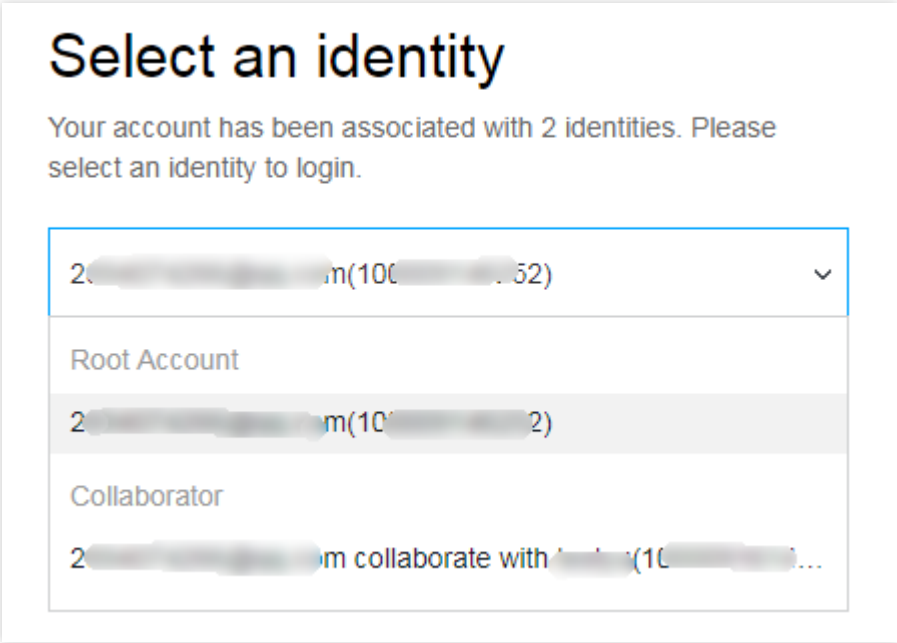
操作步骤

1. 进入 腾讯云管理控制台 页面，鼠标移动至页面右上角的账号图标。
2. 在弹出的下拉菜单中，单击**切换用户身份**，如下图：



3. 在选择用户身份页面，单击账号信息右侧的

，选择需要管理的主账号身份，如下图所示：



4. 单击**登录**，完成协作者身份切换操作。

消息接收人
新建消息接收人

最近更新时间：2024-01-23 17:29:58

操作场景

本文档介绍如何新建消息接收人，消息接收人是隶属于子账号的一种用户类型，无法编程访问或登录腾讯云控制台，仅可通过主账号设置的关联联系方式接收消息通知。

操作指南

1. 登录访问管理控制台，并在左侧导航栏中，选择**用户** > 用户列表，进入用户列表管理页面。
2. 在用户列表页面，单击**新建用户**，进入新建用户页面。
3. 在新建用户页面，单击**自定义创建**，进入选择类型页面。
4. 在选择类型页面，单击**仅用于接收消息**，进入填写用户信息页面。
5. 在填写用户信息页面，填写用户名、备注、手机、邮箱，其中备注为选填。
6. 单击**完成**，完成新建消息接收人操作。

消息接收人订阅消息

最近更新时间：2024-01-23 17:29:58

操作场景

本文档介绍如何为消息接收人验证消息渠道以及设置订阅消息，如需消息接收人接收消息，需消息接收人验证通过消息渠道，为其订阅消息后该用户已验证通过的消息渠道即可接收相关的消息提醒。

前提条件

已登录访问管理控制台，进入 用户列表 管理页面。

操作指南

验证消息渠道

1. 在用户列表管理页面，找到需订阅消息的消息接收人。
2. 单击**用户昵称**进入用户详情页。
3. 在用户详情页，单击用户信息栏下的**发送验证**。

手机：系统将会向该消息接收人已设置的手机号发送验证消息，用户收到验证消息后确认链接，即可完成验证手机消息渠道。

邮箱：系统将会向该消息接收人已设置的邮箱发送验证消息，用户收到验证消息后确认链接，即可完成验证邮箱消息渠道。

是否允许微信接收通知：在完成邮箱验证后，系统将向该消息接收人设置的邮箱发送一封包含二维码的邮件，微信扫码关注公众号，即可完成验证微信消息渠道。

设置订阅消息

1. 在用户列表管理页面，找到需订阅消息的消息接收人。
2. 单击右侧操作列的**更多 > 订阅消息**。
3. 在弹出的 “订阅消息” 窗口，勾选需订阅的消息类型（可打开折叠按钮 “▼”，选择具体需要的消息接收类型）。
4. 单击**确定**，完成设置订阅消息操作。

消息接收人用户组设置

最近更新时间：2024-01-23 17:29:58

操作场景

本文档介绍如何通过将消息接收人添加或移出用户组，获取和删除从用户组获取的消息通知。

前提条件

已登录访问管理控制台，进入 用户列表 管理页面。

操作指南

添加消息接收人到用户组

您可以通过将消息接收人添加至用户组， 获取用户组设置的消息通知。

1. 在用户列表管理页面，找到需添加到组的消息接收人。
2. 单击操作列的**更多操作 > 添加到组**。
3. 在弹出的添加到组窗口，勾选需要添加到的用户组。
4. 单击**确定**，完成添加到组操作。

从用户组移出消息接收人

您可以通过将消息接收人移出用户组， 删除从用户组获取的消息通知。

1. 在用户列表管理页面，找到需从组中移出的消息接收人。
2. 单击消息接收人名称，进入用户详情页。
3. 在用户详情页，单击**用户组**，找到需要移出的组。
4. 单击右侧操作列的**移出该组 > 确认移出**，完成从用户组移出消息接收人操作。

删除消息接收人

最近更新时间：2024-01-23 17:29:58

操作场景

本文档介绍如何删除单个或多个消息接收人，删除之后该用户将不再接收该主账号的消息提醒。

前提条件

已登录访问管理控制台，进入 用户列表 管理页面。

操作指南

删除单个消息接收人

1. 在用户列表管理页面，找到需删除的消息接收人。
2. 单击右侧操作列的**更多** > **删除**，完成删除单个消息接收人的操作。

删除多个消息接收人

1. 在用户列表管理页面，在左侧勾选需删除的消息接收人。
2. 单击左上方**删除** > **确认删除**，完成删除消息接收人操作。

用户信息

最近更新时间：2024-01-23 17:35:43

操作场景

本文档介绍如何查看和修改子账号用户名、备注、手机等信息。

查看用户信息

1. 登录访问管理控制台，进入用户列表 管理页面，找到需要查看用户信息的子账号。
2. 单击**用户名称**，进入用户详情页面。
3. 可在页面上方查看当前子账号的用户信息（含用户名、备注、手机、邮箱）。

修改用户信息

1. 登录访问管理控制台，进入用户列表 管理页面，找到需要修改用户信息的子账号。
2. 单击**用户名称**，进入用户详情页，单击右上角**修改**。
3. 在弹出的编辑信息窗口，修改相应的用户信息。

说明：

用户名：修改当前协作者用户的用户名，子用户因登录使用用户名，无法修改。

备注：修改当前子账号的备注信息。

手机：修改当前子账号绑定手机信息，该手机可以用于接收主账号消息通知及敏感操作前的身份验证。

邮箱：修改当前子账号绑定邮箱信息，该邮箱可以用于接收主账号消息通知。

4. 单击**确定**，完成修改用户信息操作。您可以通过修改之后的用户名、手机、备注、邮箱在 用户列表 管理页面，搜索到您的子账号。

关联文档

如果您想了解如何为子账号订阅消息，请参阅 子用户订阅消息、协作者订阅消息、消息接收人订阅消息。

用户设置
密码规则

最近更新时间：2024-01-23 17:31:58

背景信息

腾讯云不会保存您的密码明文，只会保存SHA256哈希（Hash）且加盐（Salt）后的值，以确保密码不会被泄露给任何人。

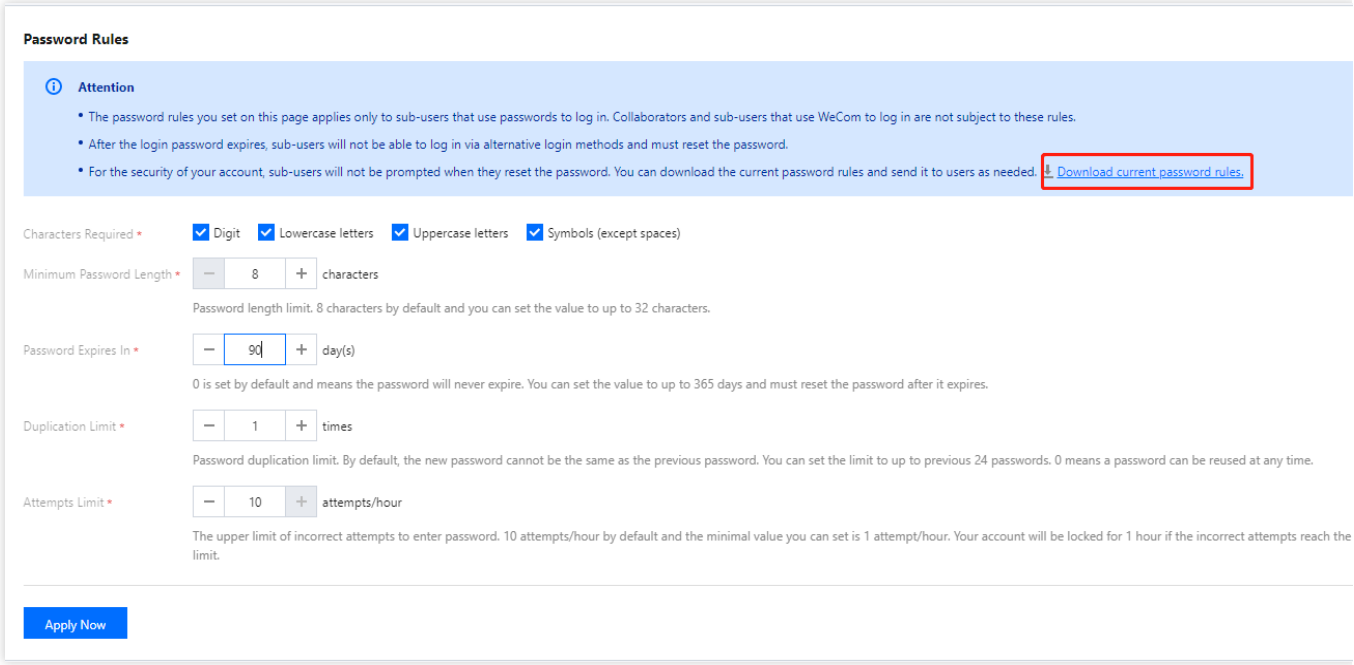
操作场景

该任务指导您通过访问管理控制台修改子用户的密码规则，包括密码的复杂度、长度、有效期等信息。如果不修改密码规则，则应用默认设置。
在以下设置密码的场景中，您需要遵守已设置的密码规则：
定义创建子用户时，勾选了**腾讯云控制台访问**和**自定义密码**。
重置子用户的登录密码时，勾选了**自定义密码**。

操作步骤

1. 登录访问管理控制台，并在左侧导航栏中，选择选择**用户** > **用户设置**，进入用户设置页面。
2. 在密码规则模块，修改密码的复杂度、长度、有效期等具体规则。
3. 单击击**应用修改**，该规则密码规则即可生效。您在下次重置密码时需要遵守本次设置的密码规则。

说明：
您在该模块所设定的密码规则仅适用于使用登录密码的子用户。
登录密码失效后子用户将无法通过其他登录方式（含微信扫码）进行登录，须重置登录密码。
为保障您的账户安全，子用户重置密码时不会提示密码规则细则，主账号、管理员或拥有 cam:GetPasswordRules 接口权限的子账号可以在密码规则页面下载当前密码规则传达给所需用户。如下图所示：


Password Rules
Attention
• The password rules you set on this page applies only to sub-users that use passwords to log in. Collaborators and sub-users that use WeCom to log in are not subject to these rules.
• After the login password expires, sub-users will not be able to log in via alternative login methods and must reset the password.
• For the security of your account, sub-users will not be prompted when they reset the password. You can download the current password rules and send it to users as needed. Download current password rules.
Characters Required *
Digit
Lowercase letters
Uppercase letters
Symbols (except spaces)
Minimum Password Length *
8
characters
Password length limit. 8 characters by default and you can set the value to up to 32 characters.
Password Expires In *
90
day(s)
0 is set by default and means the password will never expire. You can set the value to up to 365 days and must reset the password after it expires.
Duplication Limit *
1
times
Password duplication limit. By default, the new password cannot be the same as the previous password. You can set the limit to up to previous 24 passwords. 0 means a password can be reused at any time.
Attempts Limit *
10
attempts/hour
The upper limit of incorrect attempts to enter password. 10 attempts/hour by default and the minimal value you can set is 1 attempt/hour. Your account will be locked for 1 hour if the incorrect attempts reach the limit.
Apply Now

登录限制

最近更新时间：2024-01-23 17:31:58

操作场景

该任务指导您通过访问管理控制台设置子账号的登录限制，异常限制登录（异地登录、30天未登录）或 IP 限制登录（指定 IP 允许登录或者不允许登录），约束子账号在安全环境下登录腾讯云控制台。

操作步骤

IP 限制登录

设置 IP 限制登录

您可以通过设置 IP 限制来限制子账号登录腾讯云控制台，子账号将在限制条件下管理主账号下的资源。

1. 登录访问管理控制台，在**用户** > 用户设置 页面中，开启登录限制。
2. 选择**IP 限制登录**。
3. 设置 IP 类型。

白名单：设置白名单限制后，允许子账号在白名单限制 IP（段）内登录控制台。

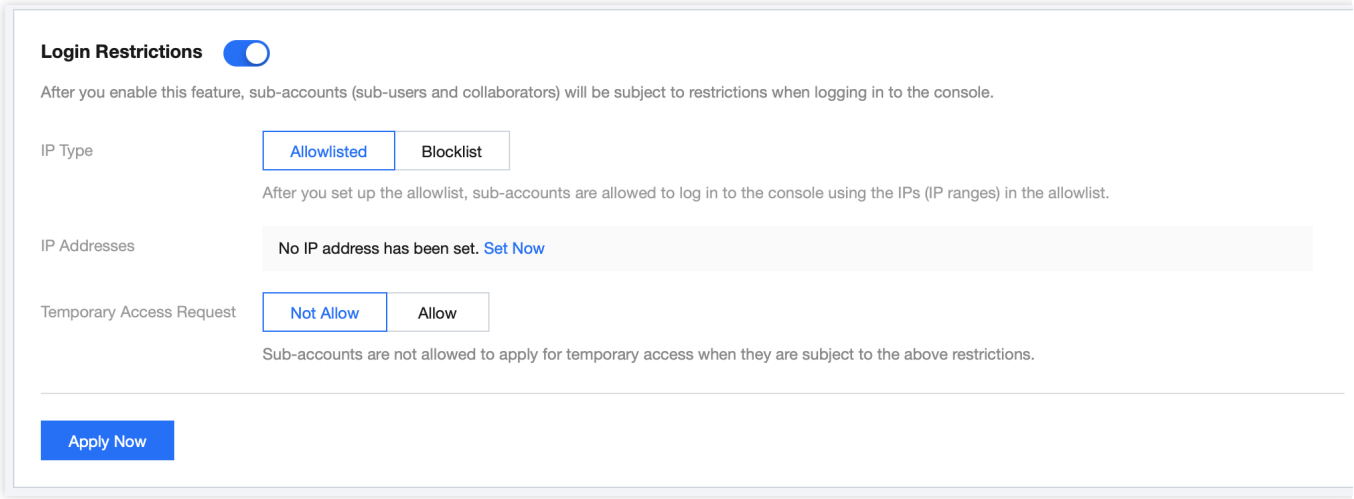
黑名单：设置黑名单限制后，不允许子账号在黑名单限制 IP（段）内登录控制台。

4. 配置 IP。单击**去添加**，可添加10条限制 IP。
5. 设置临时解封。子账号登录控制台时，是否允许申请临时解除限制。

不允许：子账号登录控制台受到上述限制时，不允许申请临时解除限制。

允许：子账号登录控制台受到上述限制时，允许申请临时解除限制，将通过有效消息渠道发送至审批人进行审批。若审批人通过其申请，将保持 2 小时内登录免审批。若设置为允许，需要您单击**去设置**，设置审批人。

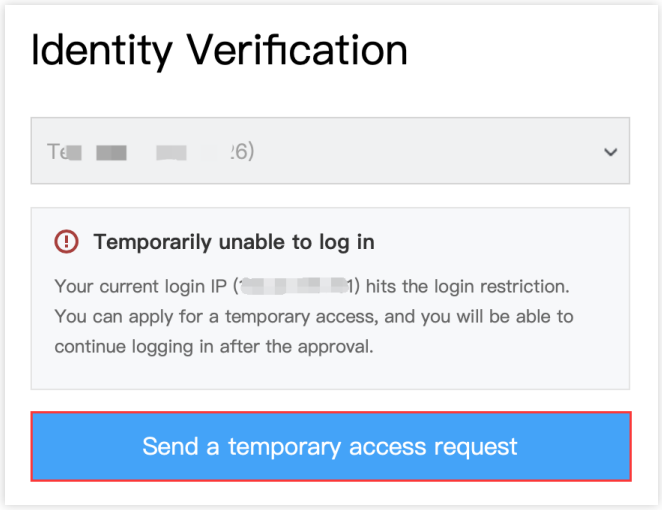
6. 单击**应用修改**，完成设置 IP 限制操作。



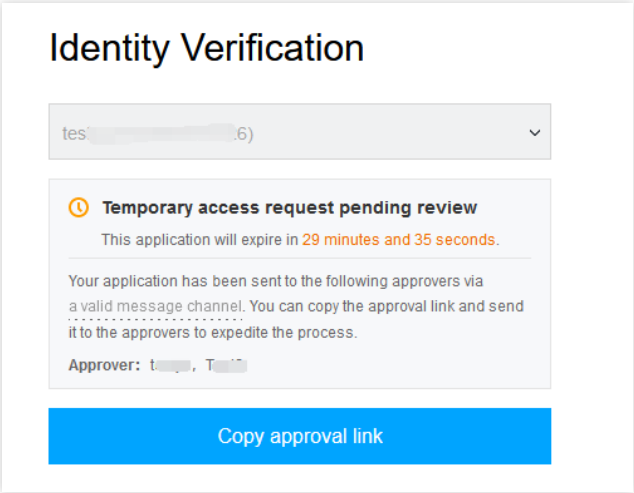
申请 IP 限制临时解封

当您的子账号登录命中登录 IP 限制条件时，若 设置登录限制 中允许您申请临时解除限制，则您可以申请临时访问权限，审核人审核通过您的子账号可以获得 2 小时的临时访问控制台权限。

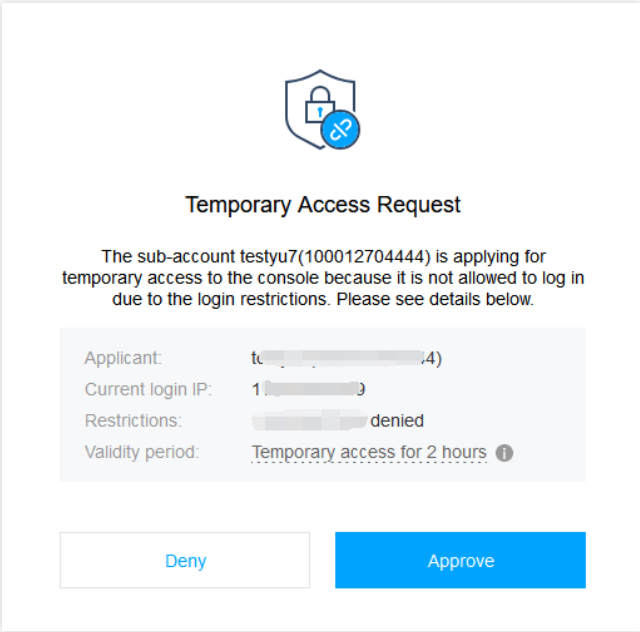
1. 当您的子账号登录命中登录限制条件，提示暂时无法登录时，单击**发送临时访问申请**，如下图所示：



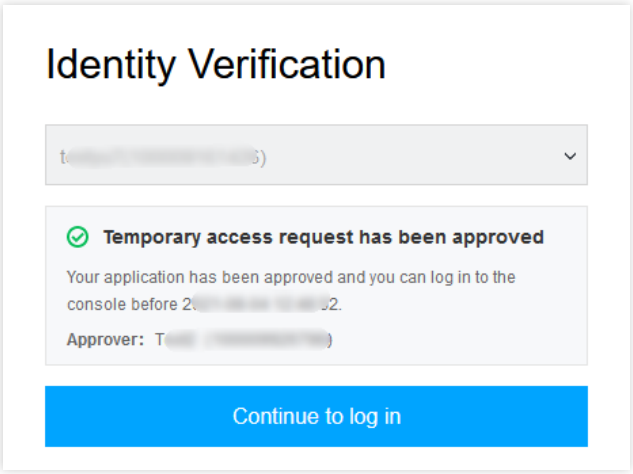
2. 页面弹出**临时访问申请等待审批中**提示，系统将您本次提交的申请已通过有效消息渠道发送至以下审核人，审核申请单次有效期为 30 分钟，您可以复制审批链接发送至审核人加快处理效率，如下图所示：



3. 在 设置登录限制 中设置的审批人将可以通过审核链接选择拒绝或者通过本次申请，完成审核临时解封申请，如下图所示：



4. 若审核人通过申请，子账号登录界面将提示临时访问申请已审核通过，单击**继续登录**，完成临时解封申请操作。子账号将获得 2 小时的临时访问控制台权限。如下图所示：



5. 若审核人拒绝申请，子账号登录界面将提示临时访问申请已被拒绝。建议您与审核人联系沟通后，重新发起申请。

高级设置

最近更新时间：2024-01-23 17:34:10

操作场景

该任务指导您通过访问管理控制台，设置子账号的单次登录会话过期时间。超过该会话时间后，需要重新登录控制台。

操作步骤

1. 登录访问管理控制台，在**用户** > 用户设置 页面，找到设置项**高级设置**。
2. 在单次登录会话过期时间中，设置时长。
3. 单击**保存**，完成设置。

访问密钥
主账号访问密钥管理

最近更新时间：2025-04-29 10:29:09

注意：

为降低密钥泄露的风险，自2023年11月30日起，对所有主账号、子账号的密钥，关闭查询 SecretKey 的功能，仅支持在创建时保存。请及时保存好 SecretKey。

操作场景

访问密钥即 API 密钥，是用户访问腾讯云 API 进行身份验证时需要用到的安全凭证，由 SecretId 和 SecretKey 一起组成。若用户还没有 API 密钥，则需要在 API 密钥管理中新建，否则就无法调用云 API 接口。

本文档介绍如何为主账号创建、禁用/启用、删除 API 密钥以及查看主账号的 API 密钥信息。

说明：

SecretId：用于标识 API 调用者身份，可以简单类比为用户名，拥有统一前缀“IKID”。

SecretKey：用于验证 API 调用者的身份，可以简单类比为密码。

注意：

访问密钥用于 API 调用访问，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。

前提条件

已使用 主账号登录 访问管理控制台，进入**访问管理 >访问密钥 >** API 密钥管理 页面。

操作步骤

创建主账号 API 密钥

您可以为主账号创建 API 密钥，创建后，主账号可以通过 API、SDK 或其他开发工具管理账号下的资源。

1. 在 API 密钥管理页面，单击左上角**新建密钥**，完成创建 API 密钥操作。如下图：

2. 在弹出的**创建 SecretKey** 窗口中会展示您创建的密钥，请妥善保存好您的密钥 SecretId 和 SecretKey，自2023年11月30日起，新建的密钥只在创建时提供SecretKey，后续不可再进行查询。

说明：
一个主账号最多可以创建两个 API 密钥。
主账号 API 密钥代表您的账号身份和所拥有的权限，等同于您的登录密码，切勿泄露他人。
API 密钥是构建腾讯云 API 请求的重要凭证，为了您的财产和服务安全，请妥善保存和定期更换密钥，当您更换密钥后，请及时删除旧密钥。

查看主账号 API 密钥

您可以查看和复制主账号 API 密钥的 SecretId，您可以通过 SecretId 和 SecretKey 使用 API、SDK 或其他开发工具管理账号下的资源。
1. 在 API 密钥管理页面，密钥操作列下的可直接获取复制 SecretId。

禁用/启用主账号 API 密钥

您可以设置禁用主账号 API 密钥，禁用后，腾讯云将拒绝当前密钥的所有请求，请您谨慎操作。
1. 在 API 密钥管理页面，单击操作列下的**禁用**。如下图：

2. 在弹出的提示窗口中，单击**禁用**，完成禁用访问密钥操作。
说明
单击操作列下的**启用**，可启用当前密钥，启用后，您将可以通过 API、SDK 或其他开发工具管理账号下的资源。

删除主账号 API 密钥

1. 在 API 密钥管理页面，单击操作列的**禁用**，如需删除的 API 密钥已禁用，可直接操作**步骤3**。
2. 在弹出的提示窗口中，单击**禁用**。
3. 在 API 密钥管理页面，单击操作列的**删除**。如下图所示：

4. 在弹出的提示窗口，单击**删除**，完成删除 API 密钥操作。
说明

API 密钥删除后无法恢复，请您谨慎操作。

API 密钥访问记录说明

1. 在 API 密钥管理 页面，单击操作列下的**更多访问记录**。如下图：

说明：

更多访问记录：展示最近三个月内最新的 20 条访问记录，包括成功和失败的调用。数据量较大，可能存在 1 小时左右的延迟。

访问记录仅记录调用服务器的请求，无论调用是否成功或是否拥有权限，都会被记录。

2 . 在右侧密钥访问记录页面，查看密钥访问记录信息。

最近访问时间：显示密钥最后一次使用的时间。

子账号访问密钥管理

最近更新时间：2025-04-29 10:29:09

注意：

为降低密钥泄露的风险，自2023年11月30日起，对所有主账号、子账号的密钥，关闭查询 SecretKey 的功能，仅支持在创建时保存。请及时保存好 SecretKey。

操作场景

访问密钥即 API 密钥，是用户访问腾讯云 API 进行身份验证时需要用到的安全凭证，由 SecretId 和 SecretKey 一起组成。若用户还没有 API 密钥，则需要在 API 密钥管理中新建，否则就无法调用云 API 接口。

本文档介绍如何为子用户/协作者创建、禁用/启用、删除 API 密钥以及查看 API 密钥信息。

说明：

SecretId：用于标识 API 调用者身份，可以简单类比为用户名，拥有统一前缀“IKID”。

SecretKey：用于验证 API 调用者的身份，可以简单类比为密码。

前提条件

已登录访问管理控制台，进入 用户列表控制台 页面找到需要设置的子用户/协作者，单击**用户名称**，进入用户详情页面。

操作步骤

创建子账号 API 密钥

您可以为子用户/协作者创建 API 密钥，创建后，子用户/协作者可以在权限范围内通过 API、SDK 或其他开发工具管理主账号下的资源。

1. 在用户详情页面，单击 **API 密钥**，进入 API 密钥管理页面。
2. 在 API 密钥管理页面，单击**新建 API 密钥**，完成创建 API 密钥操作。

3. 在弹出的**创建 SecretKey** 窗口中会展示您创建的密钥，请妥善保存好您的密钥 SecretId 和 SecretKey，自2023年11月30日起，新建的密钥只在创建时提供SecretKey，后续不可再进行查询。

说明：
一个子用户/协作者最多可以创建两个 API 密钥。
API 密钥是构建腾讯云 API 请求的重要凭证，为了您的财产和服务安全，请妥善保存和定期更换密钥，当您更换密钥后，请及时删除旧密钥。

查看子账号 API 密钥

您可以查看和复制子用户/协作者 API 密钥的 SecretId，子用户/协作者可通过 SecretId 和 SecretKey 在权限范围内使用 API、SDK 或其他开发工具管理主账号下的资源。
1. 在用户详情页面，单击 **API 密钥**，进入 API 密钥管理页面。
2. 在 API 密钥管理页面，进行以下操作可以查看和复制 API 密钥的 SecretId，API 密钥是构建腾讯云 API 请求的重要凭证，为了您的财产和服务安全，请妥善保存和定期更换密钥，当您更换密钥后，请及时删除旧密钥。
说明：
SecretId：在密钥列可直接查看，单击

可复制保存相关信息。
SecretKey：在密钥列单击**显示**，完成身份验证后，可直接查看，单击

可复制保存相关信息。（为降低密钥泄漏的风险，自2023年11月30日起，对所有主账号、子账号的密钥，关闭查询 SecretKey 的功能，仅支持在创建时保存。请及时保存好 SecretKey。）

禁用/启用子账号 API 密钥

您可以设置禁用子用户/协作者 API 密钥，禁用后，腾讯云将拒绝当前密钥的所有请求，请您谨慎操作。
1. 在用户详情页面，单击 **API 密钥**，进入 API 密钥管理页面。
2. 在 API 密钥管理页面，单击操作列的**禁用**。
3. 在弹出的确认窗口中，单击**确认**，完成禁用访问密钥操作。
说明：
单击操作列下的**启用**，可启用当前密钥，启用后，子账号/协作者将在权限范围内通过 API、SDK 或其他开发工具管理主账号下的资源。

删除子账号 API 密钥

1. 在用户详情页面，**API 密钥**，进入 API 密钥管理页面。
2. 在 API 密钥管理页面，单击操作列的**禁用**，如需删除的 API 密钥已禁用，可直接操作第 4 步。
3. 在弹出的确认窗口中，单击**确认**。
4. 在 API 密钥管理页面，单击操作列的**删除**，完成删除 API 密钥操作。
说明：
API 密钥删除后无法恢复，请您谨慎操作。

API 密钥访问记录说明

1 . 在 API 密钥管理 页面，单击操作列下的**更多访问记录**。如下图：

说明：

更多访问记录：展示最近三个月内最新的 20 条访问记录，包括成功和失败的调用。数据量较大，可能存在 1 小时左右的延迟。

访问记录仅记录调用服务器的请求，无论调用是否成功或是否拥有权限，都会被记录。

2 . 在右侧密钥访问记录页面，查看密钥访问记录信息。

最近访问时间：显示密钥最后一次使用的时间。

关联文档

如果您想了解如何通过访问密钥的 SecretId 查询子账号信息，请参阅 通过搜索框找到子用户、通过搜索框找到协作者。

用户组
新建用户组

最近更新时间：2024-01-23 17:49:51

操作场景

用户组是多个相同职能的用户（子账号）的集合。主账号和有管理员权限的子账号可以根据业务需求创建不同的用户组，通过用户组进行批量的授权、设置订阅消息等，从而更好地管理用户及其权限。
本文档介绍如何新建用户组并为用户组关联策略，您可以将您的用户分配至不同的用户组进行分组管理。用户组下的用户将在获得的权限范围内管理主账号下的资源。

操作指南

1. 登录访问管理控制台，进入 用户组 页面。
2. 单击**新建用户组**，进入填写用户组信息页面。
3. 在填写用户组信息页面，填写用户组名和备注，其中用户组名为必填项。

说明：
在用户组列表中您可以搜索用户组名或备注，在众多用户组中快速准确定位到对应的用户组。

4. 单击**下一步**，进入设置用户组权限页面。
5. 在设置用户组权限页面，勾选需要授权的策略（可多选）。
6. 单击**下一步**，进入审阅页面。
7. 在审阅页面，您可以查看用户组的相关设置，如有误可修改。
8. 确认无误后，单击**完成**，完成新建用户组操作。

关联文档

如果您想了解如何通过用户组管理子用户进行分组授权，请参阅 用户管理、用户组权限设置。
如果您想了解如何创建子用户，请参阅 自定义创建子用户。

为用户组添加/移除用户

最近更新时间：2024-01-23 17:50:49

操作场景

创建用户组并完成授权后，您可以为用户组添加或移除子账号，快速实现用户的权限变更。
当添加某个用户到用户组时，该用户将拥有用户组的所有权限。
当从用户组移除某个用户时，该用户将不再拥有用户组的权限。

前提条件

已有用户组（若没有，请 新建用户组）。
已有子账号（若没有，请 新建子账号）。

操作步骤

为用户组添加用户

1. 登录访问管理控制台，进入 用户组页面。
2. 找到目标用户组，单击操作列的**添加用户**。
3. 在弹出的添加用户窗口，勾选要添加的用户。
4. 单击**确定**，完成为用户组添加用户操作。

说明：
您也可以单击用户组名称，在详情页的**用户**页签中添加用户。

为用户组删除用户

1. 登录访问管理控制台，进入 用户组 页面。
2. 单击用户组名称，进入用户组详情页。
3. 在用户组详情页，单击**用户**，进入用户列表页面。
4. 找到要删除的用户，单击右侧操作列的**移出该组**。
5. 单击**移出用户**，完成为用户组删除单个用户操作。

说明：
您也可以勾选用户，单击用户列表上方的**移出用户**，批量删除多个用户。

为用户组添加/解除策略

最近更新时间：2024-01-23 17:49:51

操作场景

创建用户组并完成授权后，您可以为用户组添加/解除策略，快速实现用户组的权限变更。用户组下的子账号将在获得的权限范围内管理主账号下的资源。
当用户组添加某个策略时，该用户组中的所有用户将拥有该策略对应的权限。
当用户组解除某个策略时，该用户组中的所有所有将不再拥有该策略对应的权限。

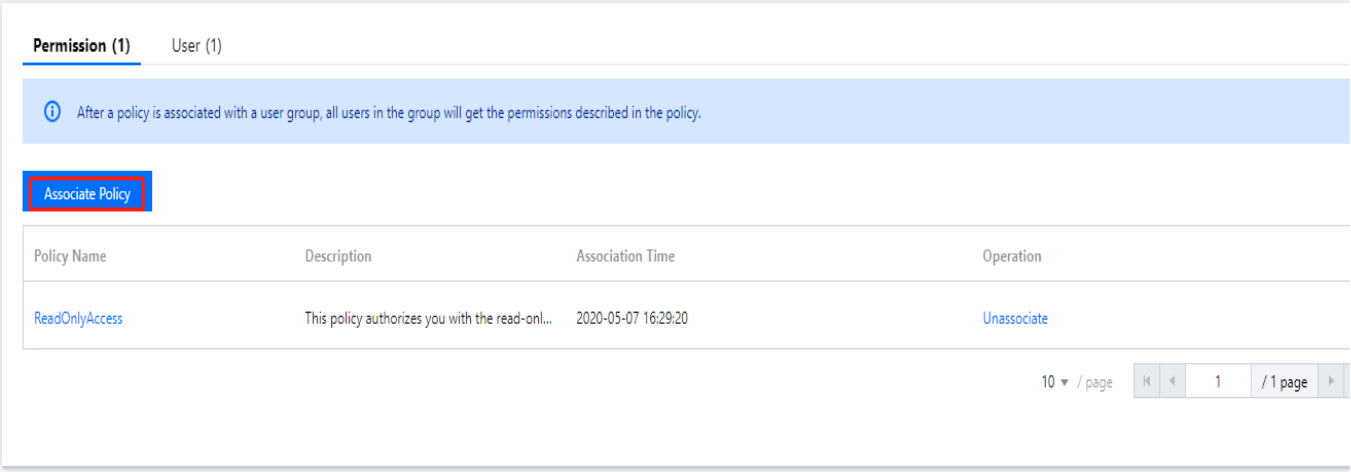
前提条件

已有用户组（若没有，请 新建用户组）。

操作步骤

为用户组添加策略

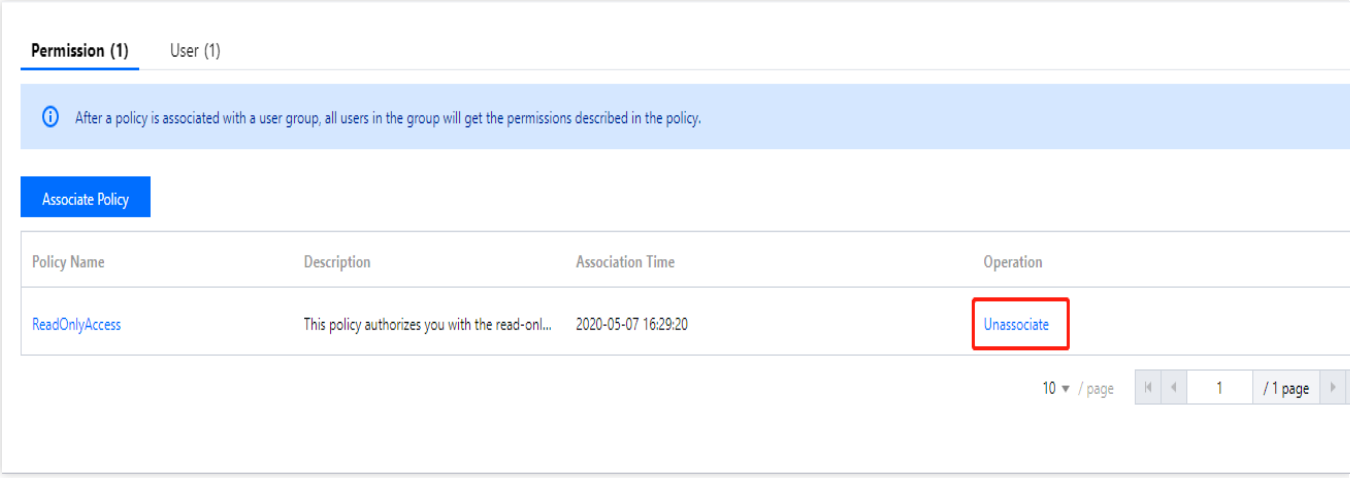
1. 登录访问管理控制台，进入 用户组 页面。
2. 找到目标用户组，单击用户组名称，进入用户组详情页。
3. 在用户组详情页的**权限**模块，单击**关联策略**。



4. 在关联策略的探矿中，勾选要添加的策略（可多选），单击**确定**，完成为用户组添加策略操作。

为用户组解除策略

1. 登录访问管理控制台，进入 用户组 页面。
2. 找到目标用户组，单击用户组名称，进入用户组详情页。
3. 在用户组详情页的**权限**模块，找到需要解除的策略，单击右侧的**解除**。



4. 确认无误后单击**确定**，完成为用户组解除策略操作。

删除用户组

最近更新时间：2024-01-23 17:49:51

操作场景

本文档介绍如何删除用户组，删除之后，用户组下的子账号将不再拥有通过用户组获得的权限。

操作步骤

删除单个用户组

1. 进入 用户组管理控制台 页面。
2. 在用户组管理控制台页面，找到需删除的用户组。
3. 单击右侧**操作**列的**删除**，完成删除用户组的操作。

角色
角色概述

最近更新时间：2024-01-23 17:52:00

什么是角色

CAM 的角色是一种虚拟用户，与子账号、协作者或消息接受者这类实体用户不同。角色同样可被授予策略。
角色可以是任一腾讯云账号代入，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。

角色使用场景

能够申请担任角色的对象我们称它为角色载体。目前，腾讯云角色载体分为三类：腾讯云账号、已支持角色功能的产品服务、身份提供商。对应的场景如下：
您要向您账号中的用户授予临时的资源访问权限，或者是向另一个腾讯云主账号内的用户授予您账户中的资源访问权限。
您可能需要允许腾讯云产品服务对您的资源拥有访问权限，但不希望将长期密钥嵌入在产品服务中，因为这样存在难以轮换密钥以及被截取后泄露导致的安全问题。
如果您的企业或组织已有自己的账号体系，同时希望管理组织内成员使用腾讯云资源，腾讯云支持您使用身份提供商（Identity Provider，IdP）功能而不必在您的腾讯云账户中为每一位组织成员创建 CAM 子用户。

基本概念

最近更新时间：2024-01-23 17:52:00

在您开始使用角色前需要了解一些基本术语，包括角色、服务角色、自定义角色、角色载体、权限策略等。更多术语介绍请参考 词汇表。

角色

拥有一组权限的虚拟身份。用于对角色载体授予腾讯云中服务、操作和资源的访问权限。这些权限附加到角色，而不附加到具体的用户或者用户组。
CAM 支持以下 2 种类型的角色：
服务（预设）角色：由腾讯云服务进行预定义的角色，服务角色需经过用户授权，服务即可通过扮演服务角色对用户资源进行访问操作。
自定义角色：由用户自行定义的角色，用户可以自由灵活地决定角色载体和角色权限。
角色可由以下用户使用：
可作为角色的腾讯云主账号。
可作为角色的腾讯云子用户以及协作者。
以及，角色还可由支持角色的腾讯云产品服务使用。查询腾讯云产品服务是否支持使用服务角色请参阅 支持 CAM 的产品。

服务角色

服务角色是腾讯云各个产品服务直接提供的独特类型的 CAM 预设角色。服务角色的关联权限由相关产品服务预定义，一旦相关产品服务被您赋予服务角色，即该产品服务能够全权代表您调用服务角色权限范围内的其他腾讯云产品服务。服务角色可以让您更轻松地使用服务，因为在赋予角色的流程中您不必手动添加权限，只需要选择是否给该服务授予服务角色的相关权限。
给相关产品服务赋予服务角色的流程中，服务角色的相关权限和角色载体已经被定义，除非另外定义，否则仅该服务可以代入角色。服务角色的预定义包括角色名称、角色载体、权限策略。

自定义角色

自定义角色是用户自己对 CAM 角色进行定义。自定义角色的角色名称、角色载体以及角色权限均由用户决定。自定义角色可以让您更自由灵活地对您云上资源的访问使用权限进行分配。
被您授予角色的对象仅在使用角色的过程中能够获得相关权限，避免给予持久密钥可能带来的安全问题。

角色载体

角色载体是被允许承载角色权限的对象。您可以对角色进行角色载体编辑，添加或删除相应对象来允许或者拒绝其扮演角色来访问您的腾讯云资源。目前腾讯云支持的角色载体类型为：腾讯云账号和支持角色的腾讯云服务。查询腾讯云产品服务是否支持使用服务角色，请参阅 支持 CAM 的产品。

权限策略

JSON 格式的权限文档。您可以在权限策略中定义角色可使用的操作和资源。该文档规则依赖于 CAM 策略语言规则。

信任策略

JSON 格式的权限文档。您可以在信任策略中定义可扮演角色的对象以及扮演角色时需满足的条件。该文档规则依赖于 CAM 策略语言规则。

创建角色

最近更新时间：2024-12-16 17:25:30

操作场景

本文档介绍如何通过使用访问管理控制台或 CAM API 两种方式创建角色。创建成功后，角色可以在获得的权限范围内管理主账号下的资源。

前提条件

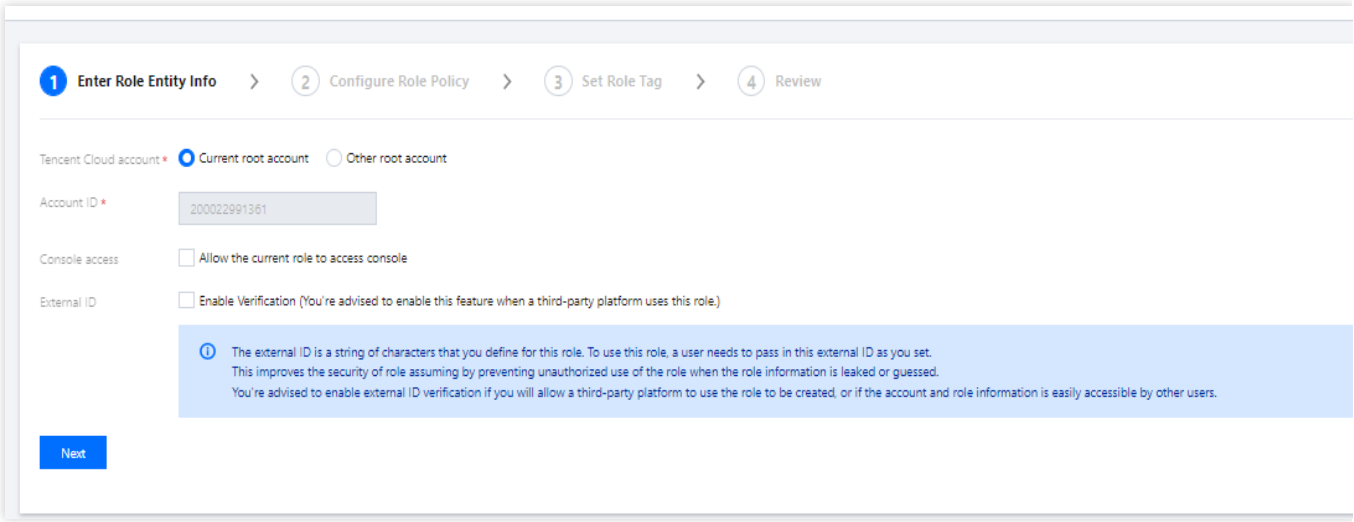
已登录访问管理控制台，进入 角色 列表页面。

操作步骤

通过控制台创建

为腾讯云主账号创建角色

1. 在角色列表页面，单击**新建角色**。
2. 在弹出的选择角色载体窗口，选择**腾讯云账户**作为角色载体，进入角色信息填写页面。



3. 在输入角色载体信息页面，填写以下信息，单击**下一步**。

云账号类型：选择“当前主账号”或“其他主账号”。

账号 ID：填写您允许其扮演角色来访问您腾讯云资源的主账户 ID，默认键入为您的主账户 ID。

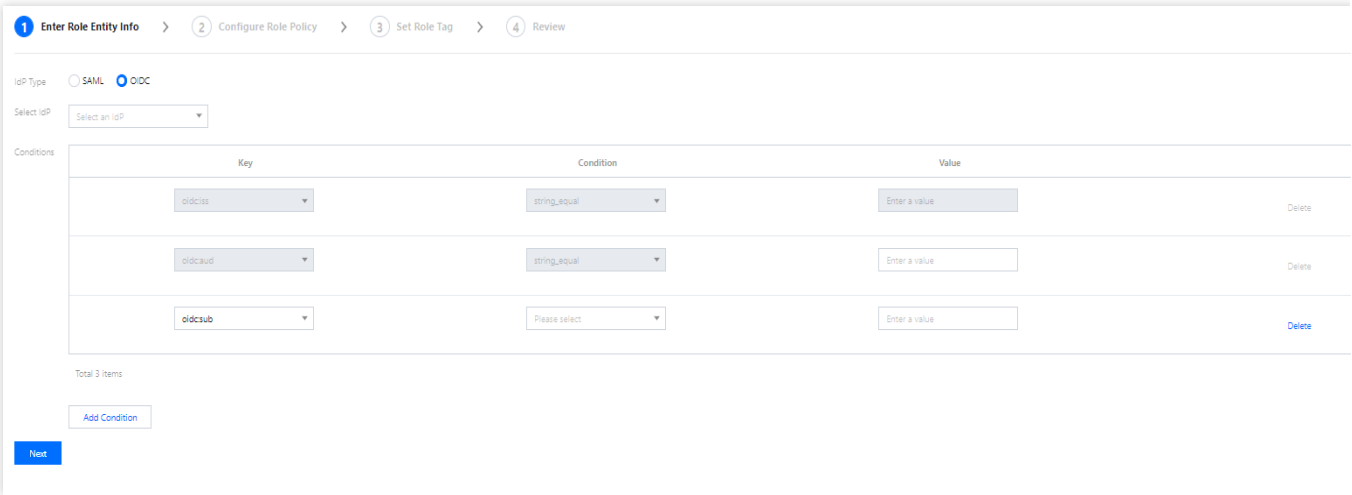
控制台访问：勾选后则允许当前角色访问控制台。
外部 ID：若您要创建的角色要分配给第三方外部平台使用，或账号及角色信息较容易被其他用户获取到，建议您开启外部 ID 校验。开启后需输入外部 ID。
4. 在策略列表内，勾选您想要给当前创建角色赋予的策略，单击**下一步**。
5. 标记角色的标签键和标签值，单击**下一步**。
6. 输入您的角色名称，审阅角色载体及策略信息无误后，单击**完成**后即完成自定义角色创建。
说明：
如果您想为其他腾讯云子账号授予角色，请参阅 为子账号赋予扮演角色策略。

为腾讯云产品服务创建角色

1. 在角色列表页面，单击**新建角色**。
2. 在弹出的选择角色载体窗口，选择**腾讯云产品服务**作为角色载体，进入角色信息填写页面。
查询腾讯云产品服务是否支持使用服务角色请参阅 支持 CAM 的产品。
3. 在已支持角色功能的服务产品列表中，勾选您需要的服务作为角色载体，单击**下一步**。
4. 在策略列表内，勾选您想要给当前角色添加的策略为角色配置策略，单击**下一步**。
5. 标记角色的标签键和标签值，单击**下一步**。
6. 输入您的角色名称，审阅您即将创建角色的相关信息无误后，单击**完成**后即完成自定义角色创建。

为身份提供商创建角色

1. 在角色列表页面，单击**新建角色**。
2. 在弹出的选择角色载体窗口，选择**身份提供商**作为角色载体，进入角色信息填写页面。
身份提供商即表示您已成功创建的身份提供商，从中选择本次为哪个身份提供商创建角色。



3. 选择身份提供商类型和具体的身份提供商，并根据需要配置使用条件，单击**下一步**。
身份提供商类型：支持 SAML 和 OIDC。
选择身份提供商：选择本次为哪个身份提供商创建角色。
控制台访问（可选）：管理是否允许角色登录腾讯云管理控制台，角色均默认可通过编程访问腾讯云。

使用条件（可选）：管理身份提供商使用该角色的条件。具体可参考 使用条件。

4. 在策略列表内，勾选您想要给当前角色添加的策略，为角色完成权限配置，单击**下一步**。

5. 标记角色的标签键和标签值，单击**下一步**。

6. 输入您自定义的角色名称，审阅您即将创建角色的相关信息无误后，单击**完成**后即完成自定义角色创建。

通过 API 创建

为腾讯云账号创建角色

腾讯云支持您使用 CAM API 进行新建角色，我们以一个典型案例让您轻松了解如何使用 API 来创建角色。

假设如下场景，公司 A 有一个运维工程师的职位，并且希望将该职位外包给公司 B，该职位需要操作公司 A 广州地域所有云服务器资源。

公司 A 企业账号 CompanyExampleA（ownerUin 为 12345），创建一个角色并将角色载体设置为公司B的企业账号 CompanyExampleB（ownerUin 为 67890）。

1. 公司 A 企业账号 CompanyExampleA（ownerUin 为 12345） 调用 CreateRole 接口创建一个 roleName 为 DevOpsRole 的角色，policyDocument（角色信任策略）参数设为：

```
{
 "version": "2.0",
 "statement": [
 {
     "action": "name/sts:AssumeRole",
     "effect": "allow",
     "principal": {
         "qcs": ["qcs::cam::uin/67890:root"]
     }
 }
]
}
```

2. 公司 A 企业账号 CompanyExampleA（ownerUin 为 12345） 需要为刚才创建的角色附加权限。

3. 公司 A 企业账号 CompanyExampleA（ownerUin 为 12345） 创建策略 DevOpsPolicy，策略语法如下：

```
{
 "version": "2.0",
 "statement": [
 {
     "effect": "allow",
     "action": "cvm:*",
     "resource": "qcs::cvm:ap-guangzhou::*"
 }
]
}
```

4. 公司 A 企业账号 CompanyExampleA（ownerUin 为 12345）调用 AttachRolePolicy 将 step1 中创建的策略绑定到角色 DevOpsRole，入参 policyName=DevOpsPolicy，roleName=DevOpsRole。
经过上面的步骤，公司 A 企业账号 CompanyExampleA（ownerUin 为 12345）完成了角色的创建和授权。

为身份提供商创建角色

在为身份提供商创建角色前，您需要在 CAM 中创建 SAML 身份提供商。关于创建 SAML 身份提供商，请参阅 创建 SAML 身份提供商。
1. 为即将创建的角色准备信任策略。
说明：
信任策略各字段规定如下：
action 字段：定义允许 SAML 联合身份使用当前角色的接口。使用 `sts:AssumeRoleWithSAML` 。
principal 字段：定义允许使用当前角色的身份提供商。使用 `{"federated": [ IdPArn ]}` 字符串，例如 qcs::cam::uin/10001:saml-provider/idp_name。
condition 字段：定义允许使用当前角色的条件。默认使用 `{"StringEquals": {"SAML:aud": "https://cloud.tencent.com/login/saml"}}` 。此条件限制为仅 SAML 联合终端节点为腾讯云的身份提供商才被允许使用此角色。
角色信任策略示例如下：

```
{
  "version": "2.0",
  "statement": [
    {
      "action": "name/sts:AssumeRoleWithSAML",
      "effect": "allow",
      "principal": {
        "federated": [
          "qcs::cam::uin/10001:saml-provider/idp_name"
        ]
      },
      "condition": {
        "string_equal": {
          "saml:aud": "https://cloud.tencent.com/login/saml"
        }
      }
    }
  ]
}
```

2. 为即将创建的角色准备权限策略。关于权限策略请参阅 策略。
3. 调用 cam:CreateRole 接口创建身份提供商角色。

使用条件

SAML 目前支持的条件如下：

条件键	含义	是否必填	说明
saml:aud	接收方	选填	SAML 断言提交到的终端节点 URL，此键的值来自断言中的 SAML Recipient 字段，而不是 Audience 字段。
saml:iss	发送方	选填	以 URN 表示，此键的值来自断言中的 SAML Issuer 字段。
saml:sub	外部账号 ID	选填	这是该陈述的主题，其中包含唯一标识组织中某个用户的值。此键来自断言中 SAML NameID 字段。
saml:sub_type	外部用户类型	选填	此键来自断言中 SMAL NameID 的 Format 属性。

OIDC 目前支持的条件如下：

条件键	含义	是否必填	说明
oidc:iss	OIDC 颁发者（Issuer）	必填	该限定条件必须使用 string_equal，条件值只能是您在 OIDC 身份提供商中填写的身份提供商 URL。用来扮演角色的 OIDC 令牌中的iss字段值必须满足该限制条件要求，角色才允许被扮演。
oidc:aud	OIDC 受众（Audience）	必填	该限定条件必须使用 string_equal，条件值只能使用在 OIDC 身份提供商中配置的一个或多个客户端 ID。用来扮演角色的 OIDC 令牌中的 aud 字段值必须满足该限制条件要求，角色才允许被扮演。
oidc:sub	OIDC 主体（Subject）	选填	该限定条件可以使用任何 string 类的条件操作类型，且条件值最多可以设置10个 OIDC 主体。用来扮演角色的 OIDC 令牌中的 sub 字段值必须满足该限制条件要求时，角色才允许被扮演。

修改角色

最近更新时间：2024-01-23 17:52:00

操作场景

本文档介绍如何编辑修改角色关联策略及角色载体。修改成功后，角色将根据当前设置在获得的权限范围内管理主账号下的资源。

前提条件

已登录访问管理控制台，进入 角色 列表页面。

操作步骤

编辑角色关联策略

1. 在角色列表页面，单击您要修改的角色名称，进入角色详情页。
2. 在角色详情页，单击**已授权策略**，进入权限操作栏。
3. 在权限操作栏，单击**关联策略**。
4. 在弹出的策略列表窗口，勾选您想要给当前角色添加的策略。
5. 单击**确定**，完成编辑角色关联操作操作。

编辑角色载体

1. 在角色列表页面，单击您要修改的角色名称，进入角色详情页。
2. 在角色详情页，单击**角色载体**，进入角色载体操作栏。
3. 单击**管理载体**，进入角色载体设置页面，您可以根据需求修改已下信息：
针对账号的修改：单击**添加账号**，添加账号（仅可输入主账号）作为当前角色的角色载体，或者删除相应的账号标签将其从角色载体内移除。
针对服务的修改：勾选产品服务作为当前角色的角色载体，或者取消勾选相应的产品服务将其从角色载体内移除。
4. 单击**确定**，完成编辑角色载体操作。

使用角色

最近更新时间：2024-01-23 17:52:00

操作场景

腾讯云支持您通过控制台和 API 两种方式使用角色，本文档以一个典型案例让您轻松了解如何使用角色。

前提条件

假设存在以下条件：
公司 A 有一个运维工程师的职位，外包给公司 B，并且希望该职位可操作公司 A 广州地域所有云服务器资源。
已知公司 A 的企业账号 CompanyExampleA 的 ownerUin 为 12345。
已知公司 B 的企业账号 CompanyExampleB 的 ownerUin 为 67890。
公司 B 有一个子账号 DevB，希望由 DevB 完成这项工作。

操作步骤

您可以点击以下页签，查看对应的操作说明。
通过控制台使用角色
通过 API 使用角色
1. 公司 A 为公司 B 创建角色（参考 创建角色）。
选择**腾讯云账户**作为角色载体创建一个角色，如 DevOpsRole，将角色载体设置为公司 B 的企业账号 “67890”，并为 DevOpsRole 角色附加上可操作公司 A 广州地域所有云服务器资源的权限。
2. 公司 B 为公司 B 子账号授权（参考 为子账号赋予扮演角色策略）。
为公司 B 的子账号 DevB 授予可扮演公司 A（ownerUin 为 12345）的 DevOpsRole 角色的策略，需包含“sts:AssumeRole”接口权限。
3. 公司 B 子账号使用角色登录控制台。
公司 B 的子账号 DevB 登录控制台，在控制台头像下拉菜单中，选择“切换角色”，进入切换角色页面；
输入公司 A 的主账号“12345”，以及角色名称“DevOpsRole”，确定后即可切换为公司 A（ownerUin 为 12345）的 DevOpsRole 角色身份。
相同地，若有切换其他角色的需求，可在控制台头像下拉菜单中，选择“切换角色”，进入切换角色页面切换其他角色。
控制台切换角色登录后，若要返回原子用户，控制台头像下拉菜单中，选择“返回子用户”即可退出角色返回原子用户。

注意：

子账号仅能切换已授权的，且角色载体为云账户的角色，其他未授权的角色不可切换。

公司 A 参考 通过 API 创建 文档，执行以下操作：

1. 创建一个角色，并将角色载体设置为公司 B 的企业账号 CompanyExampleB。
2. 调用 CreateRole 接口创建角色名称（roleName）为 DevOpsRole，并为该角色附加上可操作公司 A 广州地域所有云服务器资源的权限。

公司 B 参考 为子账号赋予扮演角色策略 文档，执行以下操作：

1. 授权子账号 DevB 扮演 CompanyExampleA 的 DevOpsRole 角色。
2. 调用 AssumeRole 接口，申请角色 DevOpsRole 的临时凭证。输入参数如下:

说明：

若公司 B（CompanyExampleB）希望直接操作公司 A（CompanyExampleA）的资源，也可以通过申请角色的临时凭证进行操作。

```
roleArn=qcs::cam::uin/12345:roleName/DevOpsRole,
roleSessionName=DevBAssumeTheRole,
durationSeconds=7200
```

若该接口执行成功，则返回结果将如下所示：

```
{
    "credentials": {
        "sessionToken": "5e776c4216ff4d31a7c74fe194a978a3ff2a42864",
        "tmpSecretId": "AKI***PCl",
        "tmpSecretKey": "Vpx***MqD"
    },
    "expiredTime": 1506433269,
    "expiration": "2018-09-26T13:41:09Z"
}
```

3. 在凭证有效期内，根据实际需求，DevB 对公司 A 执行权限范围内的操作。

例如，通过 API 查看云服务器列表，在调用 DescribeInstances 接口时，将 API 密钥 SecretId 和 SecretKey 的值替换为 tmpSecretId 和 tmpSecretKey 的值，同时将 公共参数 中的 Token 设置为 sessionToken 的值。

注意：

当公司 A 想终止对公司 B 的授权时，删除角色 DevOpsRole 即可。

删除角色

最近更新时间：2024-01-23 17:52:00

操作场景

本文档介绍如何删除角色，删除后，角色将无法获取相关权限管理主账号下的资源。

操作步骤

1. 登录访问管理（CAM）控制台，进入 角色 列表页面。
2. 在角色列表页面，选择您要删除的角色。
3. 单击操作列的**删除** > **确定**，完成删除角色操作。

说明：

删除角色会一并删除与角色绑定的授权信息，单击**确定**即可删除角色，作为该角色的角色载体的产品服务或者账号均无法再使用该角色。

为子账号赋予扮演角色策略

最近更新时间：2024-01-23 17:52:00

作为角色载体的主账号可以允许其子账号对角色进行扮演，这里我们通过一个案例让您轻松了解如何为子账号创建并赋予扮演角色的策略。

假设如下场景，公司 A 有一个运维工程师的职位，并且希望将该职位外包给公司 B，该职位需要操作公司 A 广州地域所有云服务器资源。

公司 A 企业账号 CompanyExampleA（ownerUin 为 12345），创建一个角色并将角色载体设置为公司 B 的企业账号 CompanyExampleB（ownerUin 为 67890）。公司 A（CompanyExampleA）调用 CreateRole 接口创建一个角色名称（roleName）为 DevOpsRole 的角色，公司 A 企业账号 CompanyExampleA 为创建的角色 DevOpsRole 附加了权限。上述步骤请参阅 通过 API 创建。

公司 B 企业账号（CompanyExampleB）被授权这个角色后，希望由子账号 DevB 来完成这项工作。公司 B（CompanyExampleB）需要授权子账号 DevB 可以申请扮演公司 A（CompanyExampleA）的角色 DevOpsRole：

1. 创建策略 AssumeRole，示例如下：

```
{
 "version": "2.0",
 "statement": [
 {
     "effect": "allow",
     "action": ["name/sts:AssumeRole"],
     "resource": ["qcs::cam::uin/12345:roleName/DevOpsRole"]
 }
 ]
}
```

2. 将该策略授权给子账号 DevB。子账号即被赋予了扮演角色 DevOpsRole 的权限。
3. 子账号拥有扮演角色的权限后如何使用，请参阅 使用角色。

基于资源的服务角色

最近更新时间：2024-01-23 17:52:00

操作场景

角色是拥有一组权限的虚拟身份。用于对角色载体授予腾讯云中的服务、操作和资源访问权限。您可以将角色关联到云资源中，在云资源内部基于腾讯云安全凭证服务 STS 临时密钥访问其他云产品的 API（临时密钥可周期性更新）。相比于直接用持久密钥进行权限控制，通过此方式可以进一步保证账号下的持久密钥安全，也可以基于角色关联策略实现更加精细化的控制和权限管理。

功能优势

为云资源绑定 CAM 角色后，将具备以下功能及优势：
可通过 STS 临时密钥访问腾讯云其他云服务，详情请参见 STS 相关 API 接口文档。
可为不同的资源赋予包含不同授权策略的角色，使云资源对不同的云服务具有不同的访问权限，实现更精细粒度的权限控制。
无需自行在实例中保存持久密钥，通过修改角色的授权即可变更权限，快捷地维护云资源所拥有的访问权限。

操作步骤

示例：为容器实例绑定服务角色

示例场景：允许容器实例上传日志到日志服务。

1. 新建策略 role-tke-cls

（1）进入腾讯云控制台，**访问管理** > 策略 页面。
（2）单击**新增自定义策略**，创建自定义策略 role-tke-cls。
（3）创建允许上传日志的自定义策略（注：可根据场景不同，赋予角色不同的策略）。

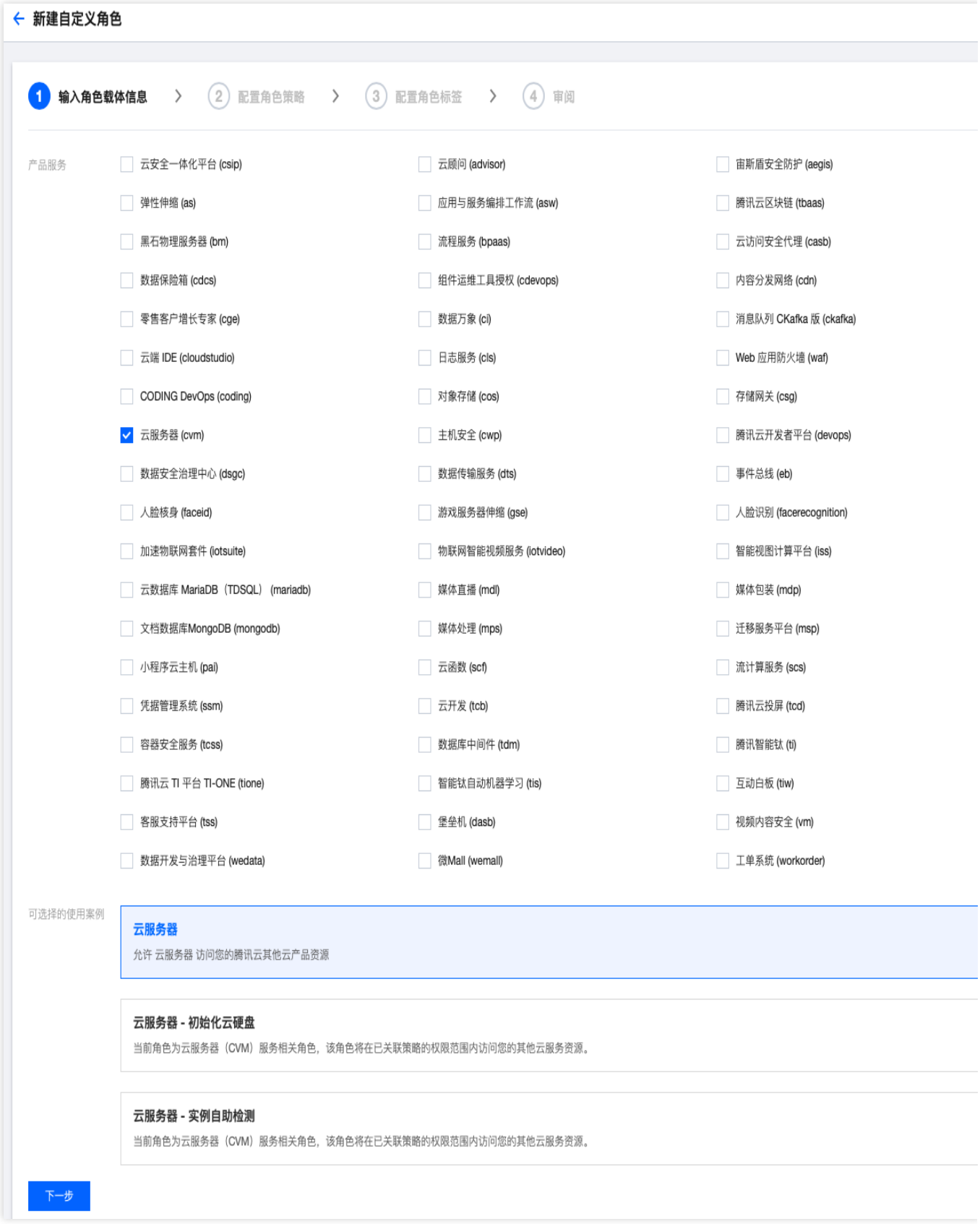
（4）完成策略创建。

2. 新建角色 instance-role

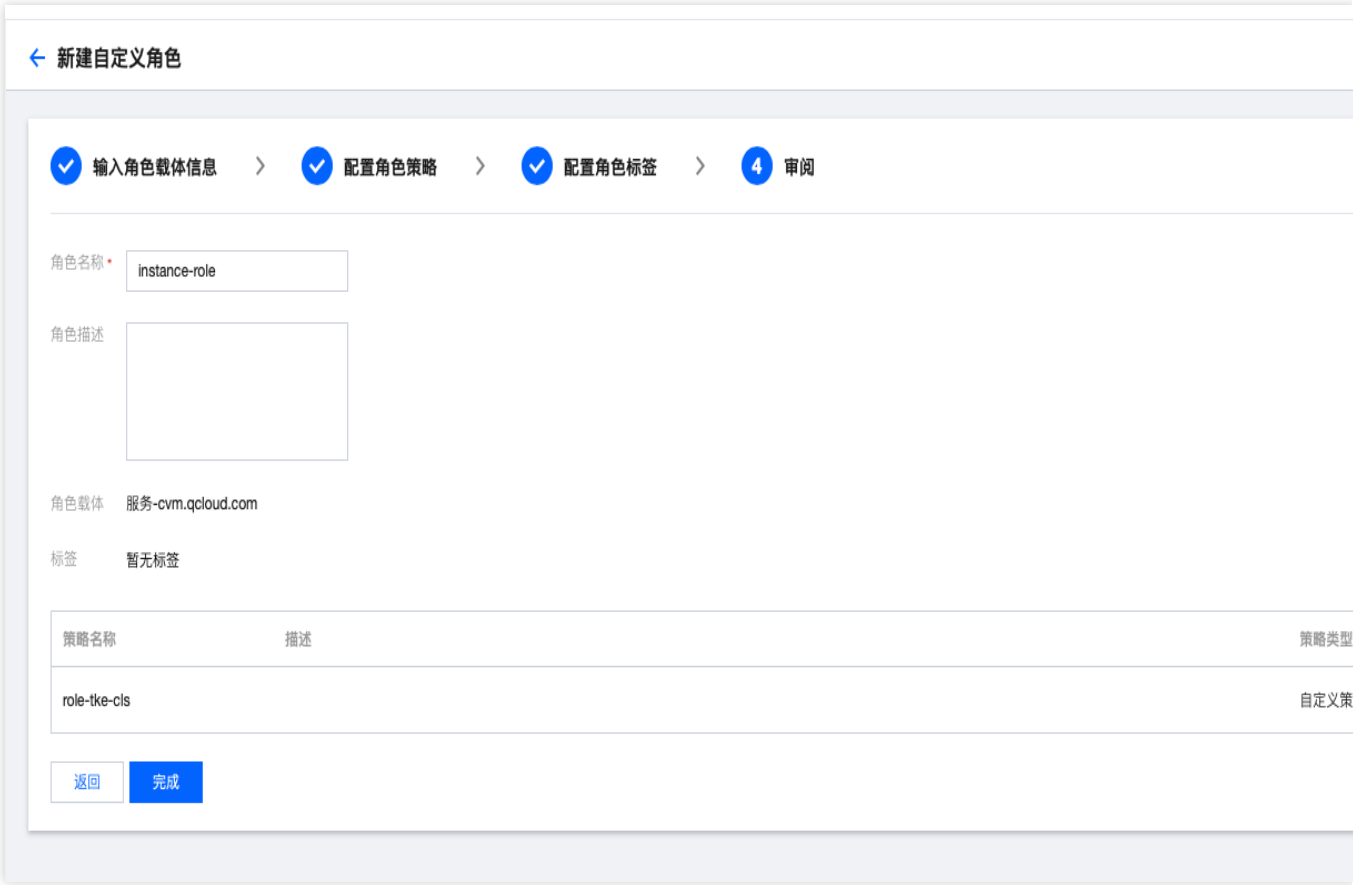
（1）进入腾讯云控制台，**访问管理** > 角色 页面。

（2）单击**新增角色**，创建自定义角色 instance-role。

（3）选择角色载体为**云服务器（CVM）**。


新建自定义角色
1 输入角色载体信息
2 配置角色策略
3 配置角色标签
4 审阅
产品服务
云安全一体化平台 (csip)
云顾问 (advisor)
宙斯盾安全防护 (aegis)
弹性伸缩 (as)
应用与服务编排工作流 (asw)
腾讯云区块链 (tbaas)
黑石物理服务器 (bm)
流程服务 (bpaas)
云访问安全代理 (casb)
数据保险箱 (cdcs)
组件运维工具授权 (cdevops)
内容分发网络 (cdn)
零售客户增长专家 (cge)
数据万象 (ci)
消息队列 CKafka 版 (ckafka)
云端 IDE (cloudstudio)
日志服务 (cls)
Web 应用防火墙 (waf)
CODING DevOps (coding)
对象存储 (cos)
存储网关 (csg)
云服务器 (cvm)
主机安全 (cwp)
腾讯云开发者平台 (devops)
数据安全治理中心 (dsgc)
数据传输服务 (dts)
事件总线 (eb)
人脸核身 (faceid)
游戏服务器伸缩 (gse)
人脸识别 (facerecognition)
加速物联网套件 (iotsuite)
物联网智能视频服务 (iotvideo)
智能视图计算平台 (iss)
云数据库 MariaDB（TDSQL） (mariadb)
媒体直播 (mdl)
媒体包装 (mdp)
文档数据库MongoDB (mongodb)
媒体处理 (mps)
迁移服务平台 (msp)
小程序云主机 (pai)
云函数 (scf)
流计算服务 (scs)
凭据管理系统 (ssm)
云开发 (tcb)
腾讯云投屏 (tcd)
容器安全服务 (tcss)
数据库中间件 (tdm)
腾讯智能钛 (ti)
腾讯云 TI 平台 TI-ONE (tione)
智能钛自动机器学习 (tis)
互动白板 (tiw)
客服支持平台 (tss)
堡垒机 (dasb)
视频内容安全 (vm)
数据开发与治理平台 (wedata)
微Mall (wemall)
工单系统 (workorder)
可选择的使用案例
云服务器
允许 云服务器 访问您的腾讯云其他云产品资源
云服务器 - 初始化云硬盘
当前角色为云服务器（CVM）服务相关角色，该角色将在已关联策略的权限范围内访问您的其他云服务资源。
云服务器 - 实例自助检测
当前角色为云服务器（CVM）服务相关角色，该角色将在已关联策略的权限范围内访问您的其他云服务资源。
下一步

（4）完成角色创建。



3. 为容器实例绑定角色

（1）进入腾讯云控制台，容器实例列表页面。

（2）单击**新建实例**。根据实际需求，设置容器实例参数。

（3）在CAM角色参数项，选择提前创建的角色 instance-role，并完成绑定。

其他基于资源的服务角色

如您需要为您的容器服务-容器实例绑定角色，请参见 为容器实例绑定角色。

如您需要为您的云函数-函数服务绑定角色，请参见 角色与策略-配置角色。

如您需要为您的云服务器-云主机绑定角色，请参见 管理实例角色。

身份提供商
SSO 概览

最近更新时间：2024-01-23 17:39:39

腾讯云支持基于 SAML 2.0和 OIDC 的 SSO（Single Sign On，单点登录），通过 IdP 身份验证的外部用户可直接访问您的腾讯云资源。腾讯云目前支持两种 SSO 登录方式：用户 SSO、角色 SSO。

SSO基本概念

概念	说明
身份提供商（IdP）	一个包含有关外部身份提供商元数据的实体，身份提供商可以提供身份管理服务。 企业本地 IdP：Microsoft Active Directory Federation Service （ADFS）、Shibboleth 等。 Cloud IdP：Azure AD、Google Workspace、Okta、OneLogin 等。
服务提供商（SP）	利用 IdP 的身份管理功能，为用户提供具体服务的应用，SP 会使用 IdP 提供的用户信息。一些非 SAML 协议的身份系统（例如：OpenID Connect），也把服务提供商称作 IdP 的信赖方。
安全断言标记语言（SAML 2.0）	实现企业级用户身份认证的标准协议，它是 SP 和 IdP 之间实现沟通的技术实现方式之一。SAML 2.0已经是目前实现企业级 SSO 的一种事实标准。
SAML 断言（SAML assertion）	SAML 协议中用来描述认证请求和认证响应的核心元素。例如：用户的具体属性就包含在认证响应的断言里。
信赖（Trust）	建立在 SP 和 IdP 之间的互信机制，通常由公钥和私钥来实现。SP 通过可信的方式获取 IdP 的 SAML元数据，元数据中包含 IdP 签发 SAML 断言的签名验证公钥，SP 则使用公钥来验证断言的完整性。
OIDC	OIDC（OpenID Connect）是建立在 OAuth 2.0基础上的一个认证协议。OAuth 是授权协议，而 OIDC 在 OAuth 协议上构建了一层身份层，除了 OAuth 提供的授权能力，它还允许客户端能够验证终端用户的身份，以及通过 OIDC 协议的 API（HTTP RESTful 形式）获取用户的基本信息。
OIDC 令牌	OIDC 可以给应用签发代表登录用户的身份令牌，即 OIDC 令牌（OIDC Token）。OIDC 令牌用于获取登录用户的基本信息。
客户端 ID	您的应用在外部 IdP 注册的时候，会生成一个客户端 ID（Client ID）。当您从外部 IdP 申请签发 OIDC 令牌时必须使用该客户端 ID，签发出来的

	OIDC 令牌也会通过 aud 字段携带该客户端 ID。在创建 OIDC 身份提供商时配置该客户端 ID，然后在使用 OIDC 令牌换取 STS Token 时，腾讯云会校验OIDC 令牌中 aud 字段所携带的客户端 ID 与 OIDC 身份提供商中配置的客户端 ID 是否一致。只有一致时，才允许扮演角色。
验证指纹	为了防止颁发者 URL 被恶意劫持或篡改，您需要配置外部 IdP 的 HTTPS CA 证书生成的验证指纹。腾讯云会辅助您自动计算该验证指纹，但是建议您在本地自己计算一次（例如：使用 OpenSSL 计算指纹），与腾讯云计算的指纹进行对比。如果对比发现不同，则说明该颁发者 URL 可能已经受到攻击，请您务必再次确认，并填写正确的指纹。
身份提供商 URL	OpenID Connect 身份提供商标识。 对应身份提供商提供的 OpenID Connect 元数据文档中的 "issuer" 字段值。
映射字段	OpenID Connect 身份提供商中与腾讯云 CAM 子用户名映射的字段。 可选身份提供商提供的 OpenID Connect 元数据文档中 "claims_supported" 的值，此示例中使用 name 字段映射 CAM 的 username。
签名公钥	验证 OpenID Connect 身份提供商 ID Token 签名的公钥。 对应身份提供商提供的 OpenID Connect 元数据文档中 "jwks_uri" 字段中链接的内容（在浏览器中打开链接获取内容）。 为了您的账号安全，建议您定期轮换签名公钥。

SSO 方式

腾讯云提供以下两种 SSO 方式：

用户 SSO

腾讯云通过 IdP 颁发的 SAML 断言确定企业用户与腾讯云 CAM 用户的对应关系 。企业可以在本地 IdP 中管理员工信息，企业员工可通过指定的链接登录腾讯云，企业用户登录后，使用该 CAM 用户访问腾讯云资源。更多信息，请参见 用户 SSO 概述。

角色 SSO

腾讯云通过 IdP 颁发的 SAML 断言或 OIDC 令牌确定企业用户与腾讯云 CAM 用户的对应关系，企业用户登录后，使用该 CAM 用户访问腾讯云，支持基于SAML 2.0和 OIDC 的两种角色 SSO：
SAML 角色 SSO：腾讯云通过 IdP 颁发的 SAML 断言确定企业用户在腾讯云上可以使用的 CAM 角色。企业用户登录后，使用 SAML 断言中指定的 CAM 角色访问腾讯云资源。更多信息，请参见 SAML 角色 SSO 概览。
OIDC 角色 SSO：企业用户通过 IdP 签发的 OIDC 令牌（OIDC Token），调用腾讯云 API 扮演指定角色并换取角色临时身份凭证（STS Token），然后使用 STS Token 安全地访问腾讯云资源。更多信息，请参见 OIDC 角色 SSO 概览。

SSO 方式对比

SSO 方式	SP 发起的 SSO	IdP 发起的 SSO	使用子用户账号密码登录	一次性配置 IdP 关联 多个腾讯云账号	多个 IdP
用户 SSO	支持	支持	不支持	不支持	不支持
角色 SSO	不支持	支持	支持	支持	支持

SSO 的适用场景

最近更新时间：2024-01-23 17:39:39

腾讯云目前支持两种 SSO 方式：角色 SSO 和用户 SSO。本文为您介绍这两种方式的适用场景和选择依据，帮助您根据整体业务需求选择合适的 SSO 方式。

角色SSO

角色 SSO 适用于以下场景：
出于管理成本考虑，您不希望在云端创建和管理用户，从而避免用户同步带来的工作量。
您希望在使用 SSO 的同时，仍然保留一部分云上本地用户，可以在腾讯云直接登录。云上本地用户的用途可以是新功能测试、网络或企业 IdP 出现问题时的备用登录方式等。
您希望根据用户在本地 IdP 中加入的组或者用户的某个特殊属性，来区分云上拥有的权限。当进行权限调整时，只需要在本地进行分组或属性的更改。
您拥有多个腾讯云账号但使用统一的企业 IdP，希望在企业 IdP 配置一次，就可以实现到多个腾讯云账号的 SSO。
您的各个分支机构存在多个 IdP，都需要访问同一个腾讯云账号，您需要在一个腾讯云账号内配置多个 IdP 进行 SSO。
除了控制台，您也希望使用程序访问的方式来进行 SSO。

用户SSO

用户 SSO 适用于以下场景：
您希望从腾讯云的登录页面发起登录，而非直接访问您 IdP 的登录页面。
您需要使用的云产品中有部分暂时不支持角色访问。支持角色访问（即通过 STS 访问）的云产品请参见 支持角色的业务。
您的 IdP 不支持复杂的自定义属性配置。
您没有上述需要使用角色 SSO 的业务需求，而又希望尽量简化 IdP 配置。

用户SSO
用户 SSO 概述

最近更新时间：2024-01-23 17:39:39

操作场景

腾讯云与企业进行用户 SSO 时，腾讯云是服务提供商（SP），而企业自有的身份管理系统则是身份提供商（IdP）。通过用户SSO，企业员工在登录后，将以 CAM 子用户访问腾讯云。

操作步骤

配置流程

为了建立腾讯云与企业 IdP 之间的互信关系，需要对腾讯云 SP 进行 SAML 配置，同时也要对企业 IdP 进行 SAML 配置，两边配置完成后才能进行用户 SSO。

1. 将企业 IdP 配置到腾讯云。

操作目的：为了建立腾讯云对企业 IdP 的信任。

具体配置操作：请参见 腾讯云 SP 进行 SAML 配置。

2. 在企业 IdP 中配置腾讯云为可信 SP 并进行 SAML 断言属性的配置。

操作目的：为了建立企业 IdP 对腾讯云的信任。

具体配置操作：请参见 企业 IdP 进行 SAML 配置。

3. 企业登录到 CAM 控制台 或通过 API 调用创建与企业 IdP 中名称完全匹配的 CAM 子用户。

操作目的：为了使用子用户进行后续登录操作。

具体配置操作：请参见 新建子用户。

登录验证流程

完成上述用户 SSO 的相关配置后，企业 IdP 中的用户便可通过 SSO 的方式登录腾讯云并访问有权限的资源。以用户 user1 为例，其具体的登录验证流程如下：

1. user1 在腾讯云子用户登录界面发起用户 SSO 登录。
2. 腾讯云将 SAML 认证请求返回给浏览器。
3. 浏览器将接收到的 SAML 认证请求转发给企业 IdP。
4. 企业 IdP 认证用户 user1，并在认证通过后生成 SAML 响应返回给浏览器。
5. 浏览器将接收到的 SAML 响应转发给腾讯云。
6. 腾讯云通过 SAML 互信配置，验证 SAML 断言的真伪和完整性，并通过 SAML 断言中的 NameID 元素值，匹配到腾讯云账号中的 CAM 子用户。

7. 验证且匹配成功后，腾讯云向浏览器返回控制台的 URL 并成功登录。

腾讯云 SP 进行 SAML 配置

最近更新时间：2024-01-23 17:39:39

操作场景

腾讯云作为服务提供商（SP），需进行企业身份提供商（IdP）的 SAML 配置，以建立腾讯云对企业 IdP 的信任，实现企业 IdP 用户通过用户 SSO 的方式登录腾讯云。

操作步骤

1. 腾讯云账号登录 CAM 控制台。
2. 在左侧导航栏中，单击**身份提供商** > **用户 SSO**。
3. 在用户 SSO 管理页面可查看当前用户 SSO 状态和配置信息。

4. 单击用户 SSO 后的开关按钮，可开启或关闭用户 SSO。
开启状态：此时 CAM 子用户不能通过账号密码的方式登录腾讯云，所有 CAM 子用户统一跳转到企业 IdP 登录页面进行身份认证。
关闭状态：此时 CAM 子用户可以通过账号密码的方式登录腾讯云，用户 SSO 设置不会生效。
5. 单击**选择文件**按钮，上传企业 IdP 提供的元数据文档，上传后如需更换文件可点击**重新上传**按钮。
说明：
元数据文档由企业 IdP 提供，一般为 XML 格式，包含IdP的登录服务地址以及 X.509 公钥证书（用于验证 IdP 所颁发的SAML 断言的有效性）
若企业 IdP 只提供元数据访问地址，可复制地址到浏览器打开，并保存为 XML 格式的文件后再上传。

腾讯云 SP 进行 OIDC 配置

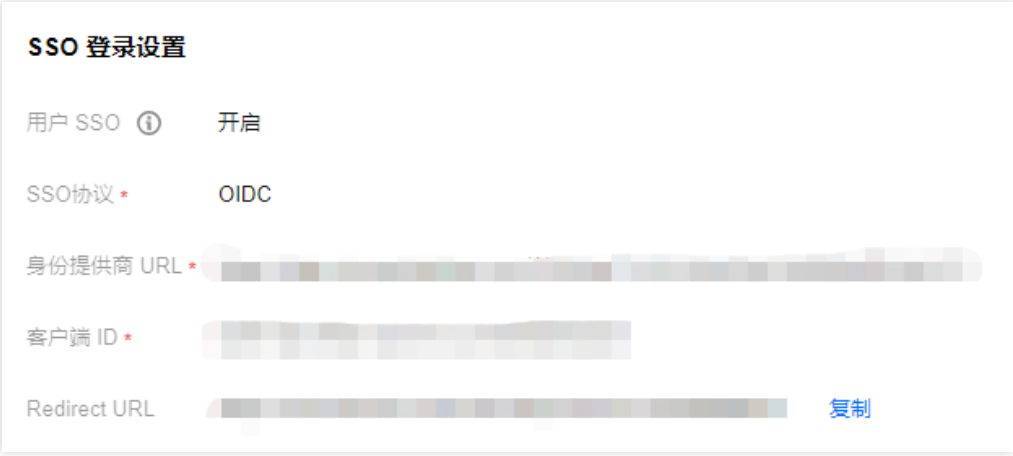
最近更新时间：2024-01-23 17:39:39

操作场景

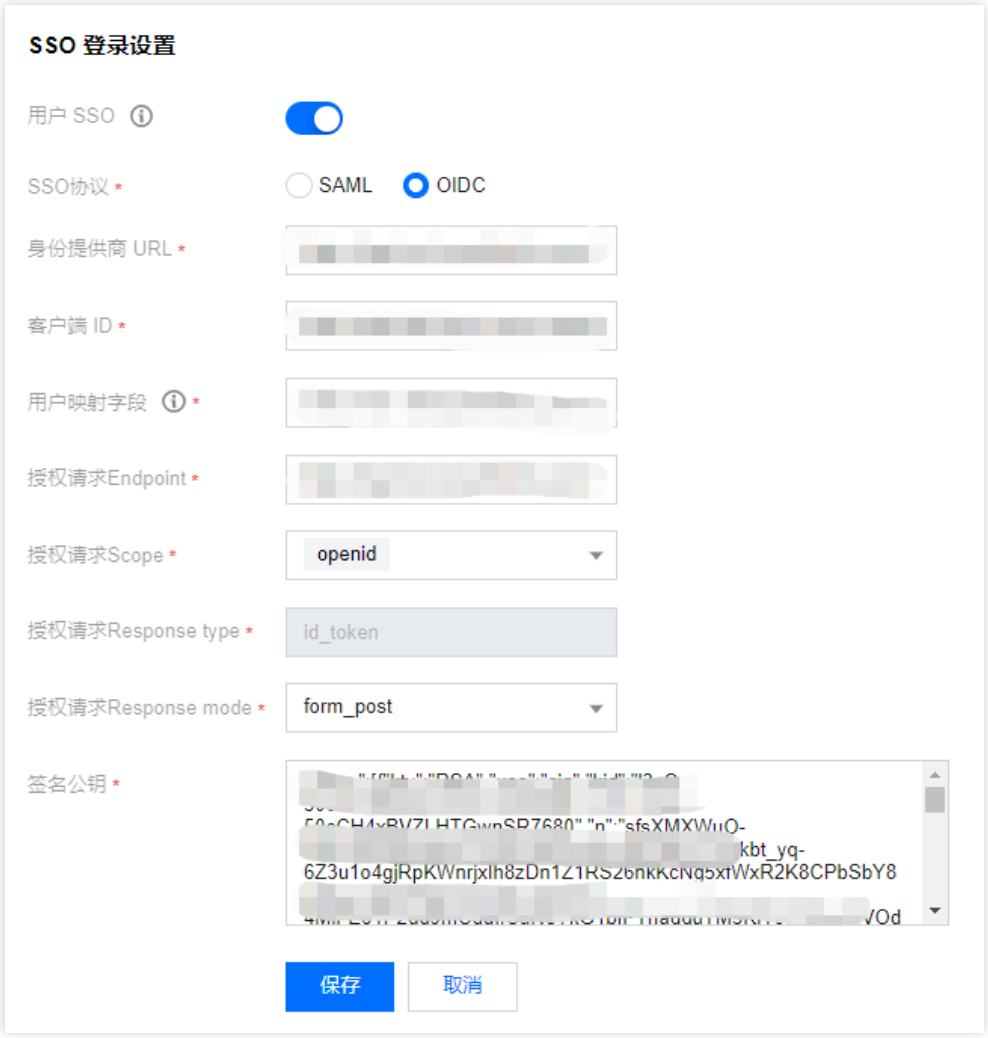
腾讯云作为服务提供商（SP），需进行企业身份提供商（IdP）的OIDC 配置，以建立腾讯云对企业 IdP 的信任，实现企业 IdP 用户通过用户 SSO 的方式登录腾讯云。
本文以身份提供商 Azure Active Directory 为例。
说明
查看 OIDC 协议配置信息。（复制 Azure Active Directory > 应用注册 > 终结点 > OpenID Connect 元数据文档处的链接，并在浏览器中打开以获得具体配置信息）

操作步骤

1. 腾讯云账号登录 访问管理控制台。
2. 在左侧导航栏中，单击**身份提供商** > **用户SSO**。
3. 在用户 SSO 管理页面可查看当前用户 SSO 状态和配置信息。



4. 单击用户 SSO 后的开关按钮，可开启或关闭用户 SSO。



开启状态：此时 CAM 子用户不能通过账号密码的方式登录腾讯云，所有 CAM 子用户统一跳转到企业 IdP 登录页面进行身份认证。

关闭状态：此时 CAM 子用户可以通过账号密码的方式登录腾讯云，用户 SSO 设置不会生效。

SSO 协议：选择OIDC类型。

身份提供商 URL：OpenID Connect 身份提供商标识。对应身份提供商提供的 OpenID Connect 元数据文档中的 "issuer" 字段值。

客户端ID：在 OpenID Connect 身份提供商注册的客户端 ID。在 **Azure Active Directory > 企业应用程序 > OIDCSSO 应用概述页**获取。

用户映射字段：OpenID Connect 身份提供商中与腾讯云 CAM 子用户名映射的字段。可选身份提供商提供的 OpenID Connect 元数据文档中 "claims_supported" 的值，此示例中使用 name 字段映射 CAM 的 username。

授权请求Endpoint：OpenID Connect 身份提供商授权请求地址。对应身份提供商提供的 OpenID Connect 元数据文档中的 "authorization_endpoint" 字段值。

授权请求Scope：OpenID Connect 身份提供商授权请求信息范围。默认必选 openid。

授权请求Response type：OpenID Connect 身份提供商授权请求返回参数类型，默认必选 id_token。

授权请求Response mode：OpenID Connect 身份提供商授权请求返回模式，可选 form_post 和 fragment 两种模式，推荐选择 form_post 模式。

签名公钥：验证 OpenID Connect 身份提供商 ID Token 签名的公钥。对应身份提供商提供的 OpenID Connect 元数据文档中 "jwks_uri" 字段中链接的内容（在浏览器中打开链接获取内容）。为了您的账号安全，建议您定期轮换签名公钥。

5.单击**保存**即可。

企业 IdP 进行 SAML 配置

最近更新时间：2024-01-23 17:39:39

企业原有的身份系统作为身份提供商（IdP），需进行腾讯云SP的SAML 配置，以建立企业 IdP对腾讯云的信任，实现企业IdP用户通过用户SSO的方式登录腾讯云。

配置步骤

1. 从腾讯云获取 SAML 服务提供商元数据 URL。

1.1 腾讯云账号登录 CAM 控制台

1.2 在左侧导航栏中，单击身份提供商-用户 SSO

1.3 在用户 SSO 管理页面可查看或复制当前用户的 SAML 服务提供商元数据 URL

2. 在企业IdP中创建一个SAML SP并将腾讯云配置为可信赖的服务提供商，具体配置方式可根据企业 IdP 的实际情况选择以下几种：

2.1 **企业 IdP 支持 URL 配置：**将步骤1中的腾讯云服务提供商元数据 URL 直接复制到企业 IdP 中进行配置

2.2 **企业 IdP 支持上传文件配置：**将步骤1中的腾讯云服务提供商元数据 URL 复制到浏览器打开并保存为 XML 格式的文件，然后再将文件上传到企业 IdP 中进行配置。

2.3 **上述两种方式企业 IdP 均不支持：**这种情况，需要在企业 IdP 上手动配置以下参数：

2.3.1 Entity ID：下载的元数据XML中，EntityDescriptor 元素的 entityID 属性值。

2.3.2 ACS URL：下载的元数据XML中，AssertionConsumerService 元素 Location属性值。

企业 IdP 进行 OIDC 配置

最近更新时间：2024-01-23 17:39:39

操作场景

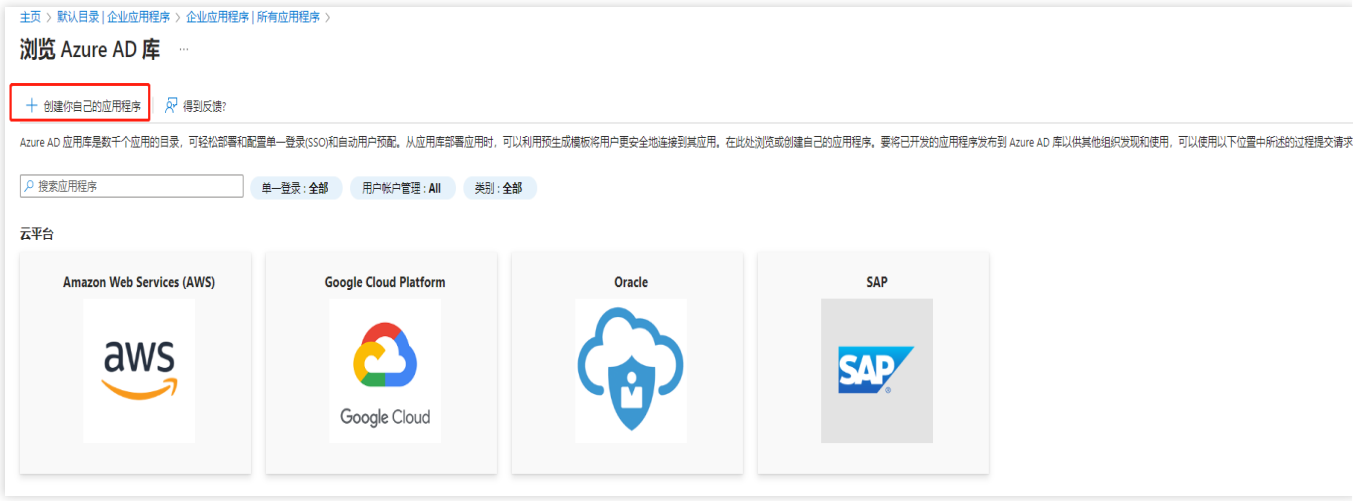
企业原有的身份系统作为身份提供商（IdP），需进行腾讯云 SP 的OIDC配置，以建立企业 IdP 对腾讯云的信任，实现企业 IdP 用户通过用户 SSO 的方式登录腾讯云。
说明：本文以身份提供商 Azure Active Directory 为例。

操作步骤

在企业 IdP 中创建应用

1. 管理员用户登录 Azure Active Directory 门户。
2. 进入 Azure Active Directory > **企业应用程序 > 所有应用程序**。
3. 单击**新建应用程序**。

4. 单击**创建你自己的应用程序**。



5. 在右侧弹出的窗口中，填写应用的名称，并选择集成未在库中找到的任何其他应用程序(非库)。

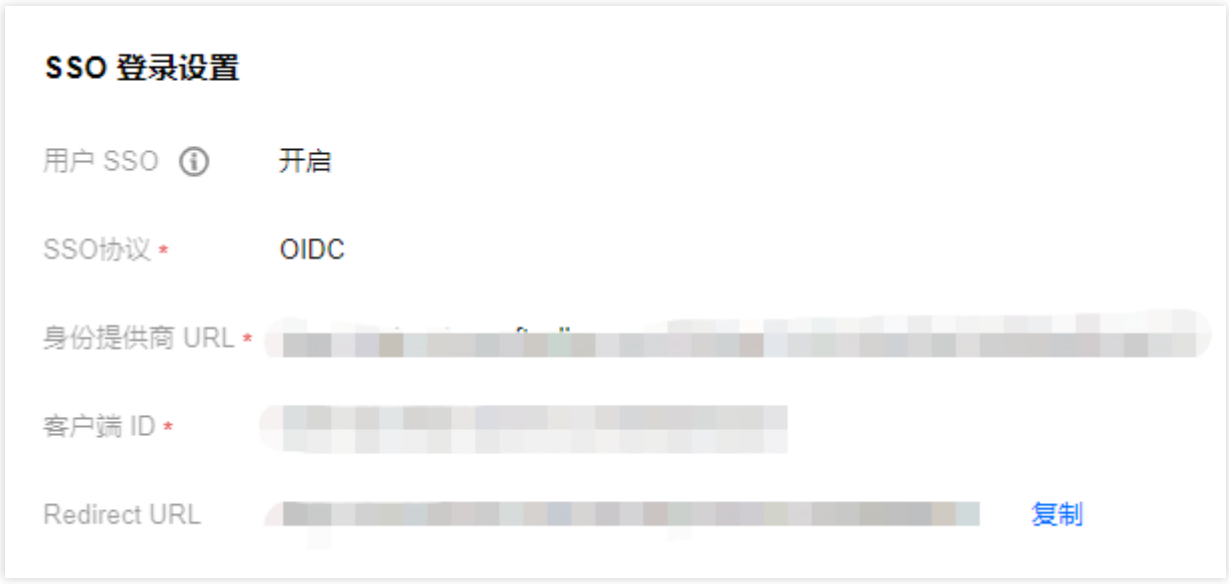
从腾讯云获取 OIDC 服务提供商元数据 URL

1. 腾讯云账号登录 访问管理控制台。

注意：

腾讯云配置 OIDC 请参见 腾讯云 SP 进行 OIDC 配置。

2. 在左侧导航栏选择**身份提供商 > 用户SSO**，信息如下：



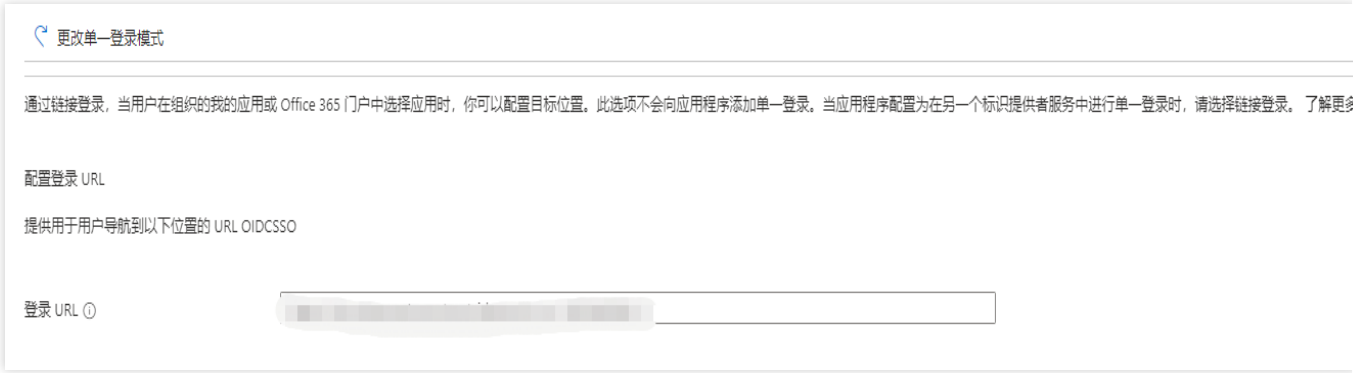
3. 单击**复制**，获取 Redirect URL 信息。

将从腾讯云获取的 Redirect URL 填写至企业 IdP

1. 进入Azure Active Directory**> 应用注册 > 所有应用程序**。
2. 在应用程序名称处，单击已创建好的应用。

3. 在左侧导航栏，单击**单一登录**。
4. 选择单一登录方式为链接形式，如下图所示：

5. 填写从腾讯云获取的 Redirect URL。



6. 单击**保存**即可。

角色SSO
角色 SSO 概述

最近更新时间：2024-09-25 16:37:27

如果您的企业或组织已有自己的账号体系，同时希望管理组织内成员使用腾讯云资源，腾讯云支持您使用身份提供商（Identity Provider, IdP）功能而不必在您的腾讯云账户中为每一位组织成员创建 CAM 子用户。使用身份提供商（IdP），您可以管理腾讯云外部用户身份，可以向这些外部用户身份授予权限使用您的腾讯云资源。
您不必自定义登录代码或进行登录验证，身份提供商（IdP）提供了身份验证，外部身份用户通过已知的身份提供商（IdP）身份验证后，将使用角色进行腾讯云登录。您可以向身份提供商角色授予使用您的腾讯云资源权限，外部身份用户将在角色的有限权限范围内进行资源访问。因外部身份用户登录腾讯云所用的是角色，而角色使用的是临时密钥，您可避免因长期使用密钥（例如云 API 密钥），导致难以轮换密钥以及被截取后泄露导致的安全问题。

使用场景

如果您的企业或组织已建立自己的账号体系及用户，并且这些用户需要访问腾讯云资源，您可以使用腾讯云访问管理（CAM）的身份提供商（IdP）功能，不必在腾讯云账户中为这些用户创建 CAM 子用户。使用身份提供商（IdP）功能，您可以管理腾讯云外部用户，并使用角色功能为身份提供商（IdP）进行联合认证的用户指定腾讯云的访问权限。

功能特性

无需创建腾讯云账号
企业客户无需为组织内每个成员创建腾讯云账号，避免因用户所分配的长期访问证书（例如云 API 密钥）泄露而导致的安全问题。
提供联合单点登录（SSO）
企业客户已有身份验证体系的场景下，通过身份提供商可实现联合单点登录（SSO）。
简化身份验证登录流程
因身份提供商提供登录代码，企业客户能够低成本完成与腾讯云的联合身份验证，便捷上云。

SAML 角色 SSO 概览

最近更新时间：2024-01-23 17:46:25

腾讯云与企业进行角色 SSO 时，腾讯云是服务提供商（SP），而企业自有的身份管理系统则是身份提供商（IdP）。通过角色 SSO，企业可以在本地 IdP 中管理员工信息，无需进行腾讯云和企业 IdP 间的用户同步，企业员工将使用指定的 CAM 角色登录腾讯云。

基本流程

企业员工可以通过控制台或程序访问腾讯云。

通过控制台访问腾讯云

当管理员在完成角色 SSO 的相关配置后，企业员工可以通过以下方法登录到腾讯云。基本流程如下：
1. 使用浏览器在 IdP 的登录页面中选择腾讯云作为目标服务。
2. IdP 生成一个 SAML 响应并返回给浏览器。
3. 浏览器重定向到 SSO 服务页面，并转发 SAML 响应给 SSO 服务。
4. SSO 服务使用 SAML 响应向腾讯云 STS 服务请求临时安全凭证，并生成一个可以使用临时安全凭证登录腾讯云控制台的 URL。
5. SSO 服务将 URL 返回给浏览器。
6. 浏览器重定向到该 URL，以指定 CAM 角色登录到腾讯云控制台。

通过程序访问腾讯云

企业员工通过编写程序来访问腾讯云，基本流程如下：
1. 使用程序向企业 IdP 发起登录请求。
2. IdP 生成一个 SAML 响应，其中包含关于登录用户的 SAML 断言，并将此响应返回给程序。
3. 程序调用腾讯云 STS 服务提供的 APIAssumeRoleWithSAML，并传递以下信息：腾讯云中身份提供商的 PrincipalArn（扮演者访问描述名）、要扮演的角色的 RoleArn（角色访问描述名） 以及来自企业 IdP 的 SAML 断言信息。
4. STS 服务将校验 SAML 断言并返回临时安全凭证给程序。
5. 程序使用临时安全凭证调用腾讯云 API。

配置步骤

为了建立腾讯云与企业 IdP 之间的互信关系，需要进行腾讯云作为 SP 的 SAML 配置和企业 IdP 的 SAML 配置，配置完成后才能进行角色 SSO。

1. 为了建立腾讯云对企业 IdP 的信任，需要将企业 IdP 配置到腾讯云。更多信息，请参见 创建 SAML 身份提供商。
2. 企业需要在 CAM 控制台或程序创建用于 SSO 的 CAM 角色，并授予相关权限。更多信息，请参见创建 角色载体为身份提供商的 CAM 角色。
3. 为了建立企业 IdP 对腾讯云的信任，需要在企业 IdP 中配置腾讯云为可信 SAML SP 并进行 SAML 断言属性的配置。

配置示例

Azure Active Directory 单点登录腾讯云指南

OIDC 角色 SSO 概览

最近更新时间：2024-01-23 17:46:25

OIDC（OpenID Connect）是建立在 OAuth 2.0基础上的一个认证协议，腾讯云 CAM 支持基于 OIDC 的角色 SSO。

基本概念

概念	说明
OIDC	OIDC（OpenID Connect）是建立在 OAuth 2.0 基础上的一个认证协议。OAuth 是授权协议，而 OIDC 在 OAuth 协议上构建了一层身份层，除了 OAuth 提供的授权能力，它还允许客户端能够验证终端用户的身份，以及通过 OIDC 协议的 API（HTTP RESTful 形式）获取用户的基本信息。
OIDC 令牌（OIDC Token）	OIDC 可以给应用签发代表登录用户的身份令牌，即 OIDC 令牌（OIDC Token）。 OIDC令牌用于获取登录用户的基本信息。
临时身份凭证	STS（Security Token Service）是腾讯云提供的一种临时访问权限管理服务，通过 STS 获取可以自定义时效和访问权限的临时身份凭证（STS Token）。
颁发者 URL	颁发者 URL由外部 IdP 提供，对应 OIDC Token 的 iss 字段值。颁发者 URL 必须以 https 开头，符合标准 URL 格式，但不允许带有 query 参数（以 ? 标识）、fragment 片段（以 # 标识）和登录信息（以 @ 标识）。
验证指纹	为了防止颁发者URL被恶意劫持或篡改，您需要配置外部IdP的HTTPS CA证书生成的验证指纹。 腾讯云会辅助您自动计算该验证指纹，但是建议您在本地自己计算一次（例如：使用OpenSSL计算指纹），与腾讯云计算的指纹进行对比。如果对比发现不同，则说明该颁发者URL可能已经受到攻击，请您务必再次确认，并填写正确的指纹。
客户端 ID（Client ID）	您的应用在外部 IdP 注册的时候，会生成一个客户端 ID（Client ID）。 当您从外部 IdP 申请签发 OIDC 令牌时必须使用该客户端 ID，签发出来的 OIDC 令牌也会通过 aud 字段携带该客户端 ID。 在创建 OIDC 身份提供商时配置该客户端 ID，然后在使用 OIDC 令牌换取 STS Token 时，腾讯云会校验 OIDC 令牌中 aud 字段所携带的客户端 ID 与 OIDC 身份提供商中配置的客户端 ID 是否一致。只有一致时，才允许扮演角色。

应用场景

当企业应用需要频繁访问腾讯云时，如果使用固定的访问密钥（AccessKey），且安全防护措施不足时，可能会因 AccessKey 泄露而带来安全隐患。为了解决这个问题，有些企业会将应用注册在企业自建或者第三方的具有 OIDC 能力的身份提供商中（例如：Google G Suite 或 Okta 等），以借助 OIDC 身份提供商的能力来为应用生成 OIDC 令牌（OIDC Token）。在这种情况下，借助腾讯云 CAM 提供的角色 SSO 能力，企业应用可以通过持有的 OIDC 令牌换取腾讯云临时身份凭证（STS Token），从而安全地访问腾讯云资源。
此外，有些个人开发者或中小企业允许员工使用其在一些网站（例如：社交网站）上注册的身份来登录腾讯云，如果这些网站支持生成 OIDC 令牌，则可以使用腾讯云 CAM 来完成基于 OIDC 的单点登录。

基本流程

1. 在外部 IdP 中注册应用，获取应用的客户端 ID（Client ID）。
2. 在腾讯云 CAM 中创建 OIDC 身份提供商，配置腾讯云与外部 IdP 的信任关系。具体操作，请参见 创建 OIDC 身份提供商。
3. 在腾讯云 CAM 中创建 OIDC 身份提供商的 CAM 角色，并为 CAM 角色授权。具体操作，请参见 创建 OIDC 身份提供商的 CAM 角色。
4. 在外部 IdP 中签发 OIDC 令牌（OIDC Token）。
5. 使用 OIDC Token 换取 STS Token。具体操作，请参见 AssumeRoleWithWebIdentity。
6. 使用 STS Token 访问腾讯云资源。

配置示例

Azure Active Directory 单点登录腾讯云指南

基于 SAML 2.0 联合身份验证

最近更新时间：2024-01-23 17:46:25

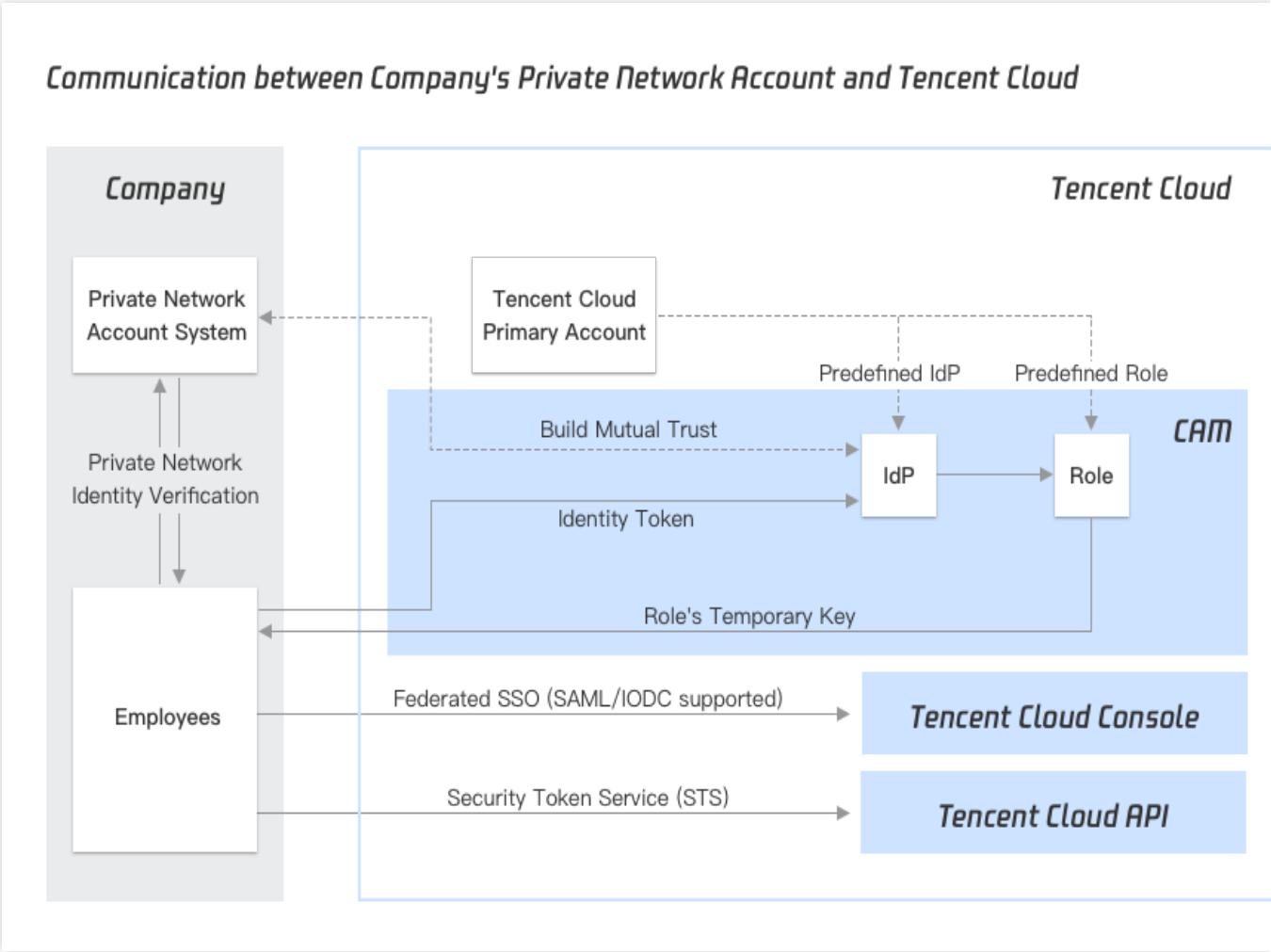
腾讯云支持基于 SAML 2.0（安全断言标记语言 2.0）的联合身份验证，SAML 2.0 是许多身份验证提供商（Identity Provider, IdP）使用的一种开放标准。使用身份提供商可实现联合单点登录（Federated Single Sign-on, SSO），用户可以授权经过联合身份验证通过的用户登录腾讯云管理控制台或调用腾讯云 API 操作，而不必为企业或组织中的每一个成员都创建一个 CAM 子用户。同时 SAML 2.0 为通用开放协议，您不必编写自定义身份代理代码，可以直接通过使用 SAML 来简化在腾讯云的联合身份验证的过程。

SAML 身份提供商

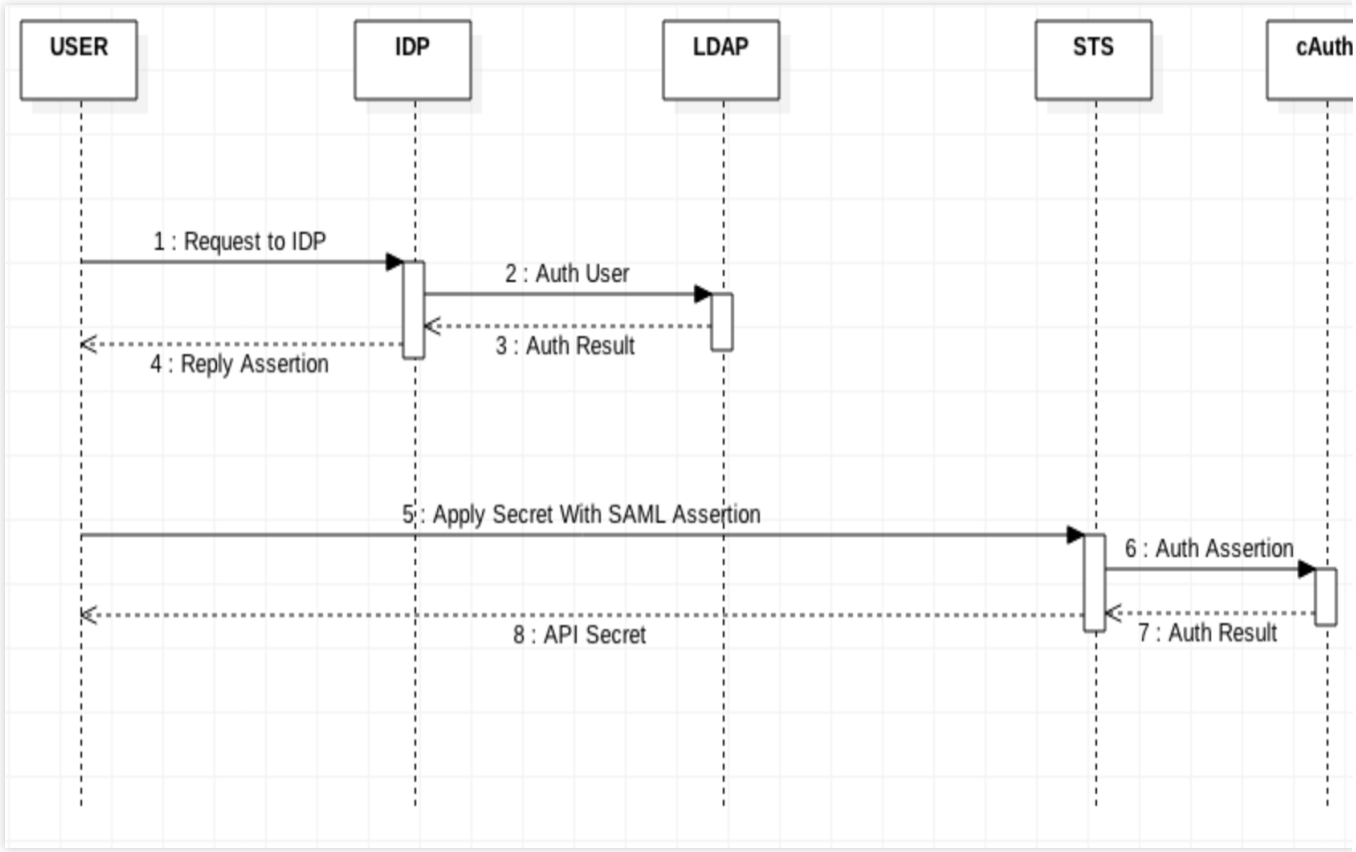
身份提供商是访问管理（CAM）中的一个实体，可以认为是外部授信账号集合。基于 SAML 2.0 联合身份验证的身份提供商（IdP）描述了支持 SAML 2.0（安全断言标记语言 2.0）标准的身份提供商（IdP）服务。如果您希望建立 SAML 2.0 协议兼容的身份提供商（例如 Microsoft Active Directory 联合身份验证服务）与腾讯云之间的信任，以便企业或组织内成员能够访问腾讯云资源，则需要创建 SAML 身份提供商。关于创建 SAML 身份提供商，请参阅 创建身份提供商。

身份提供商角色

创建 SAML 提供商后，您必须创建一个或多个以 SAML 身份提供商作为角色载体的身份提供商角色。角色是拥有一组权限的虚拟身份，进行资源访问时使用的是临时安全证书。在 SAML 2.0 断言上下文中，角色可分配给经身份提供商 (IdP) 验证身份的联合身份用户使用。此角色允许身份提供商请求临时安全证书进行腾讯云资源访问。此角色关联的策略决定了联合身份用户可在腾讯云资源的访问范围。关于创建基于 SAML 2.0 联合身份验证的身份提供商的角色，请参阅 创建角色。

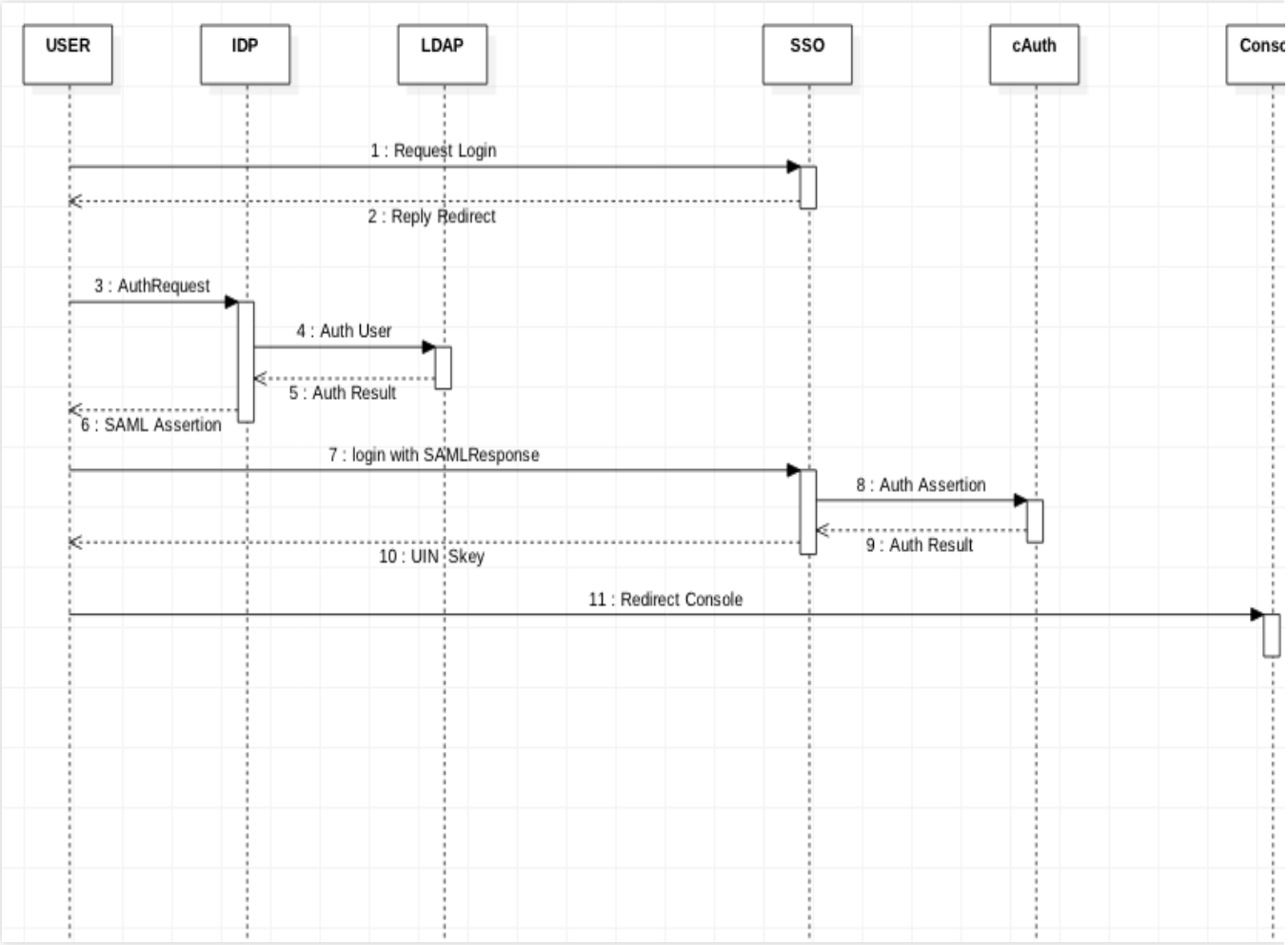


使用基于 SAML 2.0 联合身份验证访问腾讯云 API



1. 企业或组织用户使用客户端请求企业的身份提供商进行身份验证。
2. 身份提供商根据企业的身份认证系统进行验证。
3. 返回用户验证的结果。
4. 身份提供商根据验证结果，生成一个标准的 SAML 2.0 断言文档，并返回到客户端。
5. 客户端根据 SAML 2.0 断言、身份提供商的资源描述和使用的身份提供商角色的资源描述向 sts:AssumeRoleWithSAML 请求申请临时安全密钥。
6. STS 校验 SAML 2.0 断言信息。
7. 返回校验结果。
8. 根据返回结果申请临时证书，并返回到客户端。

使用基于 SAML 2.0 联合身份验证实现联合单点登录（SSO）



1. 企业或组织用户使用浏览器访问腾讯云服务。
2. 腾讯云服务返回认证请求到浏览器。
3. 浏览器重定向到企业组织的身份提供商（IdP）。
4. 企业验证用户身份。
5. 企业用户身份验证成功，返回用户信息到身份提供商（IdP）。
6. 身份提供商（IdP）生成标准的 SAML2.0 断言，返回到浏览器。
7. 浏览器将 SAML 2.0 断言重定向到腾讯云。
8. 开始进行腾讯云 SSO 登录服务，请求 cAuth 并验证用户身份。
9. 返回腾讯云验证结果。
10. 验证成功，返回登录态。
11. 重定向到腾讯云控制台服务。

使用 SAML 2.0 联合身份用户访问腾讯云管理控制台

最近更新时间：2024-01-23 17:46:25

操作场景

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 是许多身份验证提供商（Identity Provider， IdP）使用的一种开放标准。您可以通过基于 SAML 2.0 联合身份验证将身份提供商与腾讯云进行集成，从而实现身份提供商用户自动登录（单一登录）腾讯云控制台管理腾讯云的资源，不必为企业或组织中的每一个成员都创建一个 CAM 子用户。

操作步骤

您可以通过本步骤创建一个或多个角色作为身份提供商的载体登录腾讯云管理控制台，授予权限后可以在权限范围内通过腾讯云控制台管理主账号下的资源。

1. 通过浏览器访问身份提供商的门户网站，并选择跳转到腾讯云管理控制台。
2. 该门户网站可以验证当前用户的身份。
3. 验证成功后，该门户网站会生成一个 SAML 2.0 身份验证响应，其中包括识别用户身份的断言以及用户的相关属性。该门户网站将此响应发送到客户端浏览器。
4. 该客户端浏览器将被重定向到腾讯云单一登录终端节点并发布 SAML 断言。
5. 终端节点将代表用户请求临时安全凭证，并创建一个使用这些凭证的控制台登录 URL。
6. 腾讯云将登录 URL 作为重定向发回客户端。
7. 该客户端浏览器将重定向到腾讯云管理控制台。如果 SAML 2.0 身份验证响应包含映射到多个 CAM 角色的属性，则系统将首先提示用户选择要用于访问控制台的角色。

从用户的角度来看，整个流程以透明的方式进行：用户在您企业组织的内部门户网站开始操作，在腾讯云管理控制台结束操作，无需提供任何腾讯云凭证。有关如何配置此行为的概述以及指向详细步骤的链接，请参阅以下章节。

在企业组织中配置基于 SAML 2.0 的身份提供商

在您的企业组织中，配置身份存储（例如 Azure Active Directory）以使用基于 SAML 2.0 的身份提供商，例如 Azure Active Directory、OneLogin、Okta 等。通过使用身份提供商，可以生成一个元数据文档。该文档将您的企业组织描述为包含身份验证密钥的身份提供商，会把您企业组织的门户网站配置为将访问腾讯云管理控制台的用户请求路由至腾讯云终端节点，以便使用 SAML 2.0 断言进行身份验证。如何配置您的身份提供商来生成 metadata.xml 文件取决于您的身份提供商。请参阅您的 IdP 文档以获得指示，或参阅以下文档。

Azure Active Directory 单点登录腾讯云指南

OneLogin 单点登录腾讯云指南
Okta 单点登录腾讯云指南

在 CAM 中创建 SAML 身份提供商

您可以在访问管理（CAM）控制台创建一个 SAML 2.0 身份提供商，该身份提供商是访问管理（CAM）中的一个实体，可以认为是外部授信账号集合。基于 SAML 2.0 联合身份验证的身份提供商描述了支持 SAML 2.0（安全断言标记语言 2.0）标准的身份提供商服务。在创建过程中，您可以上传在 在企业组织中配置基于 SAML 2.0 的身份提供商 中的身份提供商的元数据文档。详细请参阅 创建身份提供商。

在腾讯云中为 SAML 提供商用户配置权限

您可以创建一个角色，用于建立您企业组织中的身份提供商和腾讯云的互信关系。在 SAML 2.0 断言上下文中，角色可分配给身份提供商验证身份的联合身份用户使用。此角色允许身份提供商请求临时安全证书进行腾讯云资源访问。在此过程中，您可以为该角色关联策略和设置角色的使用条件，从而决定联合身份用户在腾讯云资源的访问范围及使用条件。详细请参阅 为身份提供商创建角色。

配置身份提供商的单一登录

下载并保存腾讯云联合元数据 XML文档：http://cloud.tencent.com/saml.xml， 将您企业组织中的身份提供商属性映射到腾讯云的属性，建立您企业组织中的身份提供商和腾讯云的互信关系。安装该文件的方式取决于您的身份提供商。一些提供商为您提供了键入该 URL 的选项，此时，身份提供商将为您获取并安装该文件。另一些提供商则要求您从该 URL 处下载该文件，然后将其作为本地文件提供。请参阅您的 IdP 文档以获得指示，或参阅以下文档。

Azure Active Directory 单点登录腾讯云指南
OneLogin 单点登录腾讯云指南
Okta 单点登录腾讯云指南

SAML 响应示例

SAML 示例如下：

```
<samlp:Response>
    <saml:Issuer>...</saml:Issuer>
    <ds:Signature>
            ...
    </ds:Signature>
    <samlp:Status>
        ...
    </samlp:Status>
    <saml:Assertion>
        <saml:Issuer>...</saml:Issuer>
        <saml:Subject>
            <saml:NameID>${NameID}</saml:NameID>
            <saml:SubjectConfirmation>
                ...
```

```
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions>
            <saml:AudienceRestriction>
                <saml:Audience>${Audience}</saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement>
            ...
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute
Name="https://cloud.tencent.com/SAML/Attributes/RoleSessionName">
                ...
            </saml:Attribute>
            <saml:Attribute
Name="https://cloud.tencent.com/SAML/Attributes/Role">
                ...
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

在 SAML 断言的 AttributeStatement 元素中，必须包含以下腾讯云要求的 Attribute 元素：

1. Name 属性值为 https://cloud.tencent.com/SAML/Attributes/Role 的 Attribute 元素，该元素为必选，可以有多个。其包含的 AttributeValue 元素取值代表允许当前用户扮演的角色，取值的格式是由角色描述与身份提供商描述组合而成的，中间用英文逗号（,）隔开。

说明：

如果是多个，当使用控制台登录时，将会在界面上列出所有角色供用户选择。

以下是一个 Role Attribute 元素示例：

```
<Attribute Name="https://cloud.tencent.com/SAML/Attributes/Role">

<AttributeValue>qcs::cam::uin/{AccountID}:roleName/{RoleName1},qcs::cam::uin/{A
ccountID}:saml-provider/{ProviderName1}</AttributeValue>

<AttributeValue>qcs::cam::uin/{AccountID}:roleName/{RoleName2},qcs::cam::uin/{A
ccountID}:saml-provider/{ProviderName2}</AttributeValue>
</Attribute>
```

如果是同一个身份提供商，也可以合并为一条，不同角色 ARN 之间使用英文分号（;） 隔开。

```
<Attribute Name="https://cloud.tencent.com/SAML/Attributes/Role">
<AttributeValue>qcs::cam::uin/{AccountID}:roleName/{RoleName1};qcs::cam::uin/{A
ccountID}:roleName/{RoleName2},qcs::cam::uin/{AccountID}:saml-
provider/{ProviderName}</AttributeValue>
```

```
</Attribute>
```

说明：

在 Role 源属性中 {AccountID}，{RoleName}，{ProviderName} 分别替换内容下：

{AccountID} 替换为您的腾讯云主帐户 ID，可前往 账号信息 - 控制台 查看。

{RoleName}替换您在腾讯云为身份提供商所创建的角色名称（单击查看如何在腾讯云 为身份提供商创建的角色），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。

2. Name 属性值为 https://cloud.tencent.com/SAML/Attributes/RoleSessionName 的 Attribute 元素，该元素为必选且只能有一个。该字段由用户自定义，长度不超过32个字符。以下是一个 RoleSessionName Attribute 元素示例。该示例中，“userName”可替换成您的自定义信息。

```
<Attribute Name="https://cloud.tencent.com/SAML/Attributes/RoleSessionName">
<AttributeValue>userName</AttributeValue>
</Attribute>
```

创建 SAML 身份提供商

最近更新时间：2024-01-23 17:46:25

创建 SAML 身份提供商

您创建身份提供商有两种方式：使用访问管理控制台或 CAM API。

通过控制台创建

1. 您需要从身份提供商（IdP）处获取联合元数据文档，才能创建 SAML 身份提供商。该元数据文档包括发布者名称、验证从身份提供商收到 SAML 断言的密钥。

说明

元数据文档采用不含字节顺序标记 (BOM) 的 UTF-8 格式编码的 XML 格式。文档大小限制为40KB，若超出此大小，可手动修改元数据文档，只保留以上提到的元素即可。

2. 登录访问管理（CAM）控制台，进入 身份提供商 > 角色SSO 页面，单击**新建提供商**。

3. 在新建身份提供商页面，选择提供商类型为 SAML 并配置提供商信息，单击**下一步**。

身份提供商名称：输入身份提供商名称。

备注信息：输入您对当前身份提供商的备忘信息。

元数据文档：您需要在**元数据文档**上传步骤1中下载的 SAML 元数据文档，元数据文档内容检验合法即可上传成功。

4. 审阅您输入的身份提供商相关信息，确认无误后，单击**完成**，创建身份提供商。

通过 API 创建

创建身份提供商并上传元数据文档，请调用 创建SAML身份提供商（CreateSAMLProvider） 接口。

创建 OIDC 身份提供商

最近更新时间：2024-01-23 17:46:25

您创建身份提供商有两种方式：使用访问管理控制台或 CAM API。

通过控制台创建

1. 您需要从身份提供商（IdP）处获取联合元数据文档，才能创建 OIDC 身份提供商。该元数据文档包括发布者名称、客户端 ID、身份提供商 URL、验证从身份提供商收到的签名公钥。

说明

本文以身份提供商Azure Active Directory 为例。

2. 登录访问管理（CAM）控制台，进入 身份提供商 > 角色SSO 页面，单击**新建提供商**。

3. 在新建身份提供商页面，选择提供商类型为 SAML 并配置提供商信息，单击**下一步**。

身份提供商名称：输入身份提供商名称。

身份提供商URL：OpenID Connect 身份提供商标识。对应身份提供商提供的 OpenID Connect 元数据文档中的 "issuer" 字段值。

客户端ID：在 OpenID Connect 身份提供商注册的客户端 ID。在 **Azure Active Directory > 企业应用程序 > OIDCSSO 应用概述页**获取。

签名公钥：验证身份提供商 ID Token 签名的公钥。对应身份提供商提供的 OpenID Connect 元数据文档中 "jwks_uri" 字段中链接的内容（在浏览器中打开链接获取内容）。为了您的账号安全，建议您定期轮换签名公钥。

4. 单击下一步，审阅您输入的身份提供商相关信息，确认无误后，单击**完成**，创建身份提供商。

通过 API 创建

创建身份提供商并上传元数据文档，请调用 创建OIDC身份提供商（CreateOIDCConfig） 接口。

管理身份提供商

最近更新时间：2024-01-23 17:46:25

删除 SAML 身份提供商

您管理身份提供商有两种方式：使用访问管理控制台或 CAM API。

通过控制台删除

1. 登录访问管理（CAM）控制台，进入 身份提供商 > 角色SSO 页面。
2. 在您账户的身份提供商列表中，选择您要删除的身份提供商，在**操作**列单击**删除**。
3. 删除身份提供商时，需要您再次确认是否删除相关身份提供商，单击**确定**，即可删除身份提供商。

通过 API 删除

（可选）要分页列出所有 IdP 的信息，请调用 ListSAMLProviders。
（可选）要获取有关特定提供商的详细信息，请调用 GetSAMLProvider。
要删除 SAML 身份提供商，请调用 DeleteSAMLProvider。

修改 SAML 身份提供商

您修改身份提供商有两种方式：使用访问管理控制台或 CAM API。

通过控制台修改

1. 登录访问管理（CAM）控制台，进入 身份提供商 > 角色SSO 页面。
2. 在您账户的身份提供商列表中，选择您要修改的身份提供商，单击提供商名称进入详情页。
3. 您可以上传元数据文档重新定义当前身份提供商，或下载当前的元数据文档。

通过 API 修改

更新 SAML 身份提供商描述或者元数据文档。
调用此操作：UpdateSAMLProvider

Azure Active Directory 单点登录腾讯云指南

最近更新时间：2024-01-23 17:46:25

操作场景

Azure Active Directory （Azure AD） 是 Microsoft 推出的基于云的标识和访问管理服务，可帮助员工管理内外部资源。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 是许多身份验证提供商（Identity Provider， IdP）使用的一种开放标准。您可以通过基于 SAML 2.0 联合身份验证将 Azure Active Directory 与腾讯云进行集成，从而实现 Azure AD 帐户自动登录（单一登录）腾讯云控制台管理腾讯云的资源，不必为企业或组织中的每一个成员都创建一个 CAM 子用户。

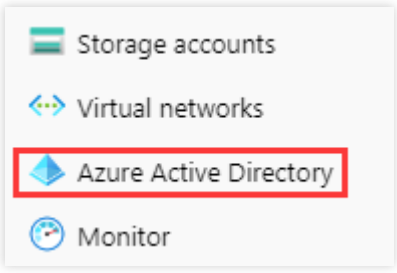
操作步骤

创建 Azure AD 企业应用程序

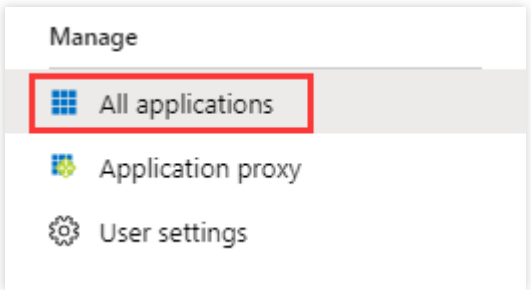
说明：

您可以通过本步骤创建 Azure AD 企业应用程序，如您已经有正在使用的应用程序，可忽略本操作，进行 配置 CAM。

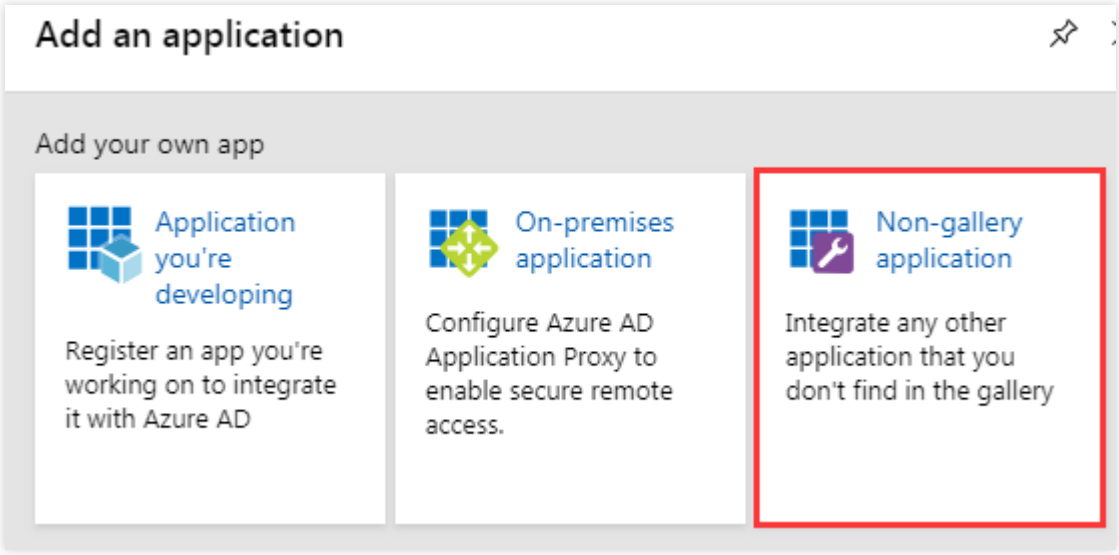
1. 进入 Azure AD 门户页，单击左侧导航栏中 **Azure Active Directory**。如下图所示：



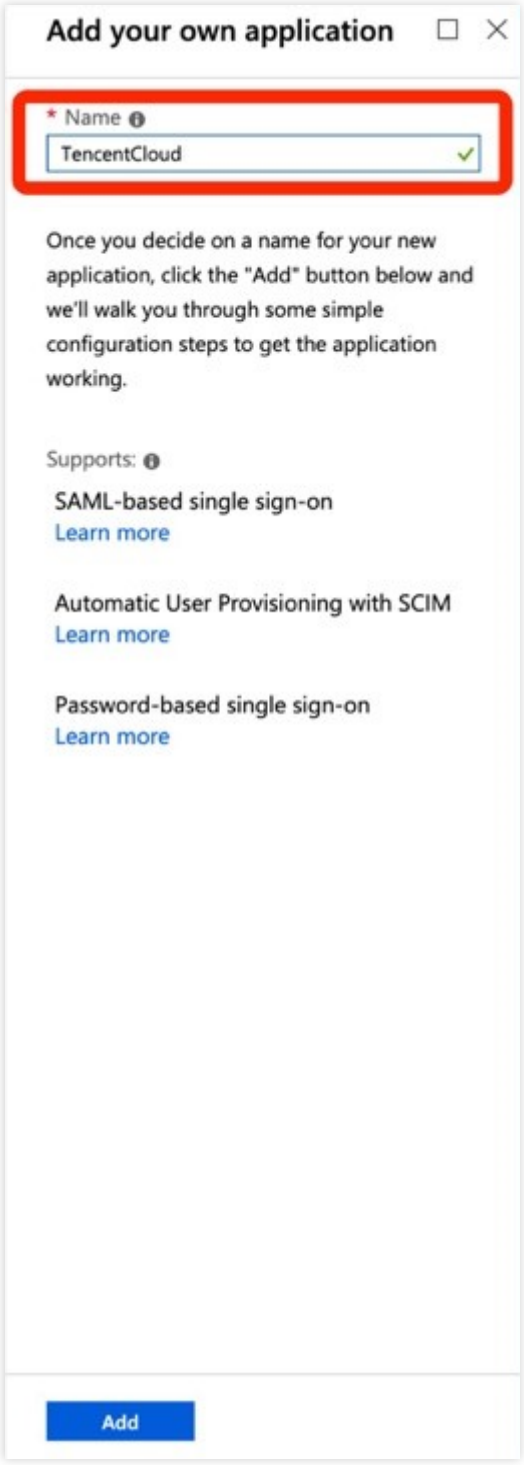
2. 单击**企业应用程序**，选择**所有应用程序**。如下图所示：



3. 单击**新建应用程序**打开“添加应用程序”窗口，选择**非库应用程序**。如下图所示：



4. 填写**名称**，单击**添加**，即可完成 Azure AD 应用程序的创建。如下图所示：

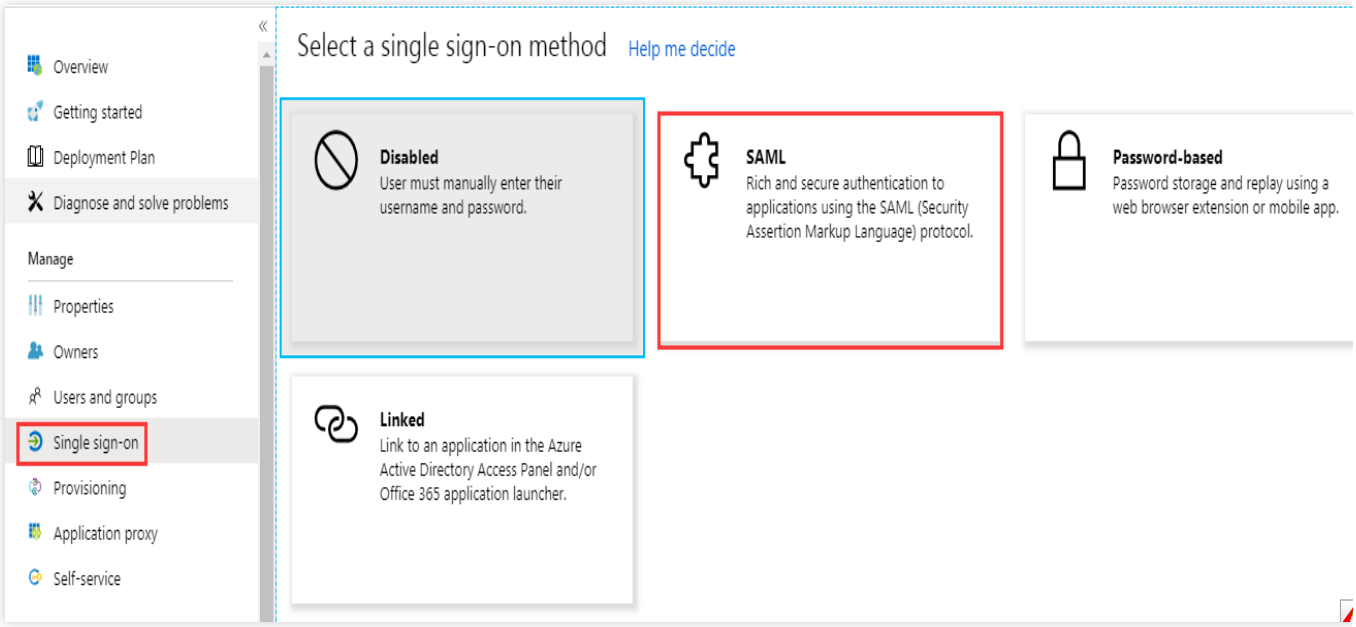


配置 CAM

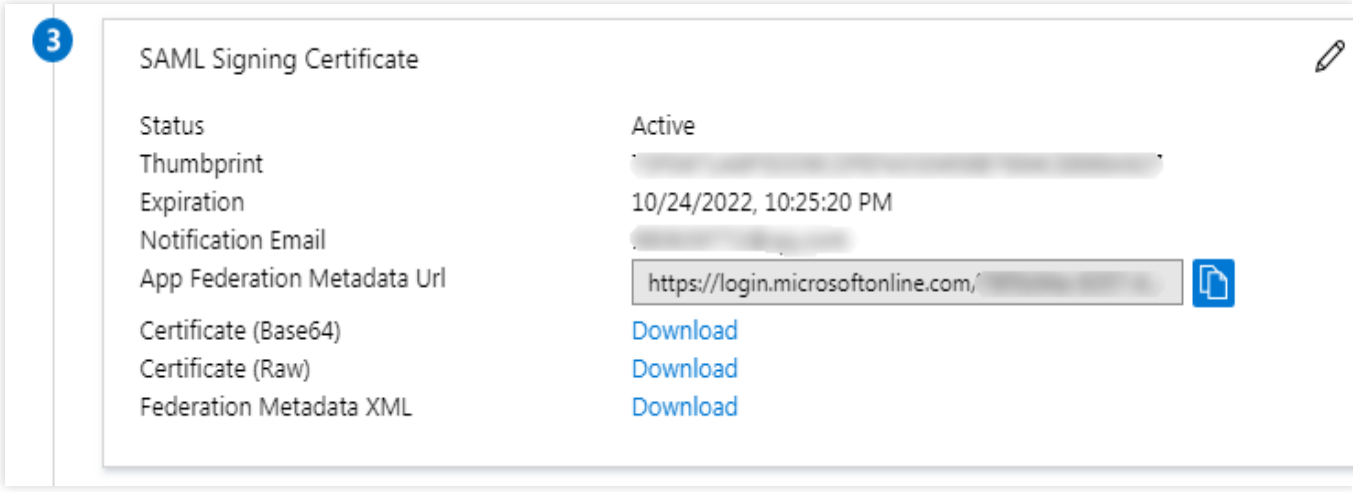
说明：

您可以通过本步骤配置 Azure AD 和腾讯云之间的信任关系使之相互信任。

1. 在左侧导航栏中，选择 **Azure Active Directory>企业应用程序>** 您创建的应用程序，进入应用程序概览页面。
2. 单击**单一登录**，打开“选择单一登录方法”页面。
3. 在打开的“选择单一登录方法”页面，选择 **SAML**。如下图所示：



4. 在 “SAML 单一登录”的预览页面，下载**SAML签名证书**中的**联合元数据 XML**文件。如下图所示：



5. 在腾讯云创建 SAML 身份提供商及角色，详细操作请参考 创建身份提供商、创建角色-为身份提供商创建角色。

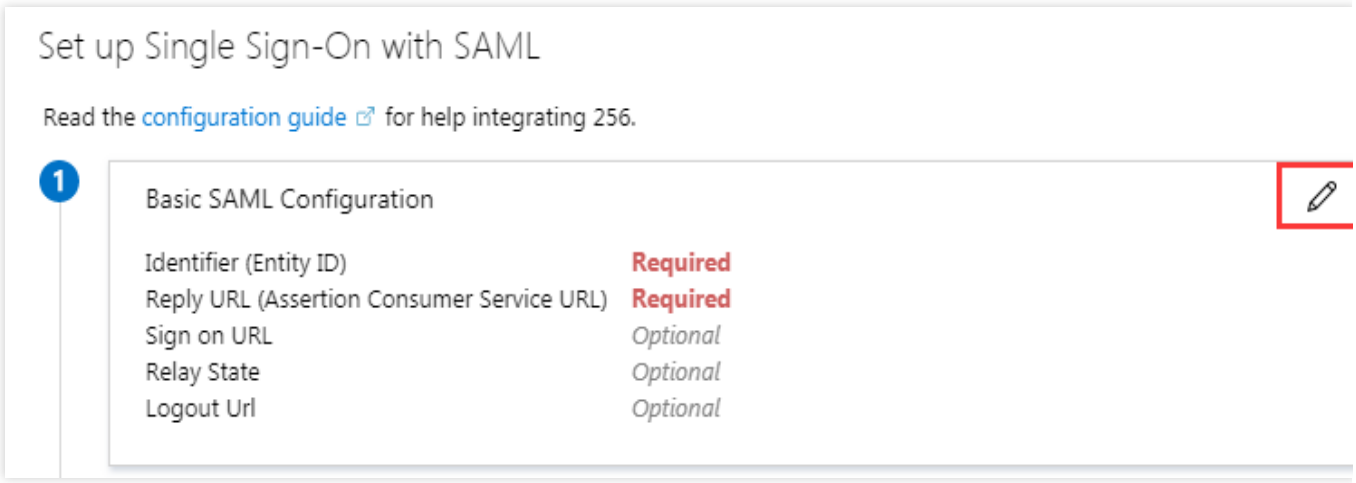
配置 Azure AD 的单一登录

说明：

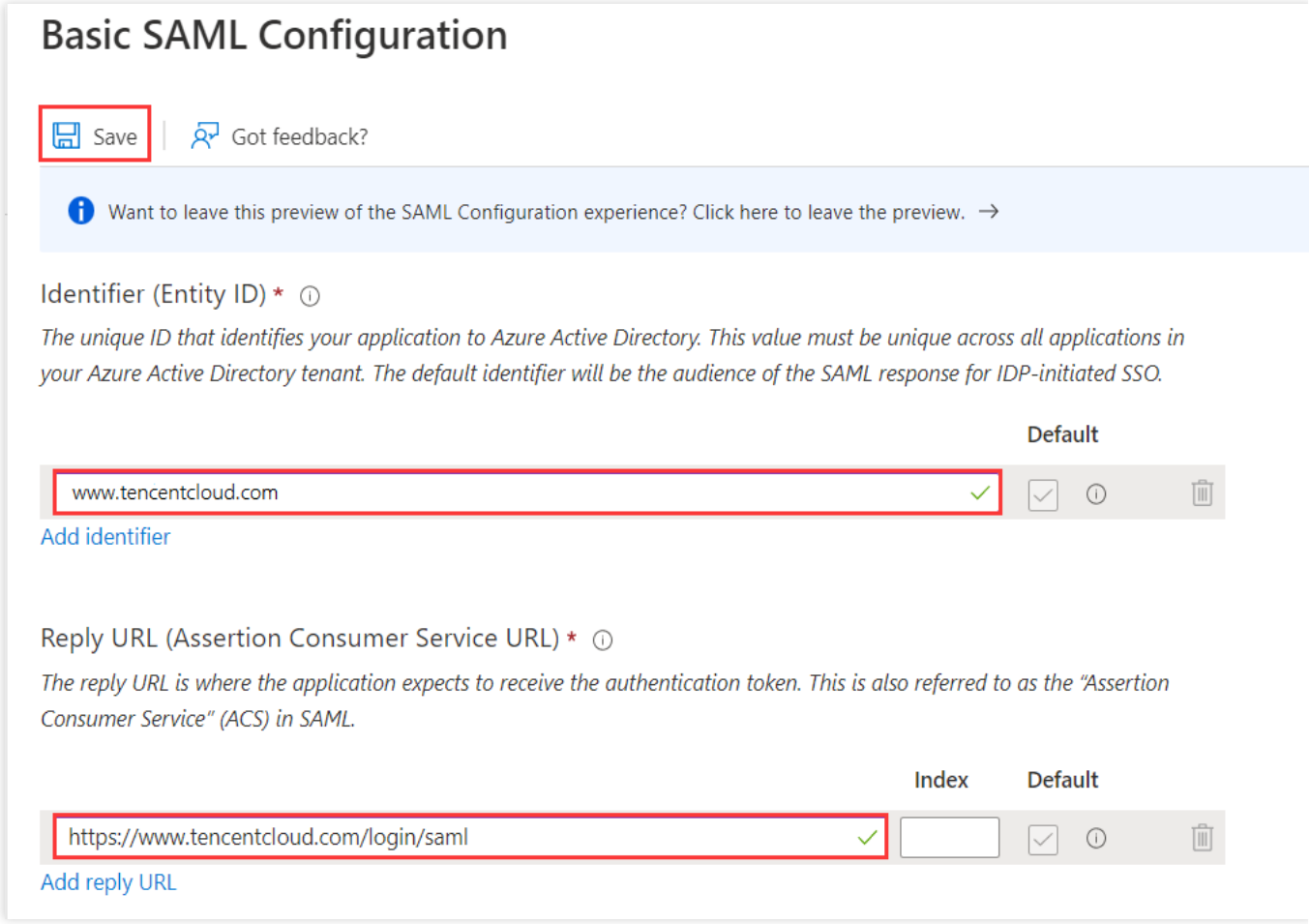
您可以通过本步骤将 Azure AD 应用程序属性映射到腾讯云的属性，建立 Azure AD 应用程序和腾讯云的互信关系。

1. 在 “SAML 单一登录”概览界面，单击“基本 SAML 配置”右上角的

。如下图所示：



2. 在“基本 SAML 配置”编辑页面填写以下信息，并单击**保存**。如下图所示：



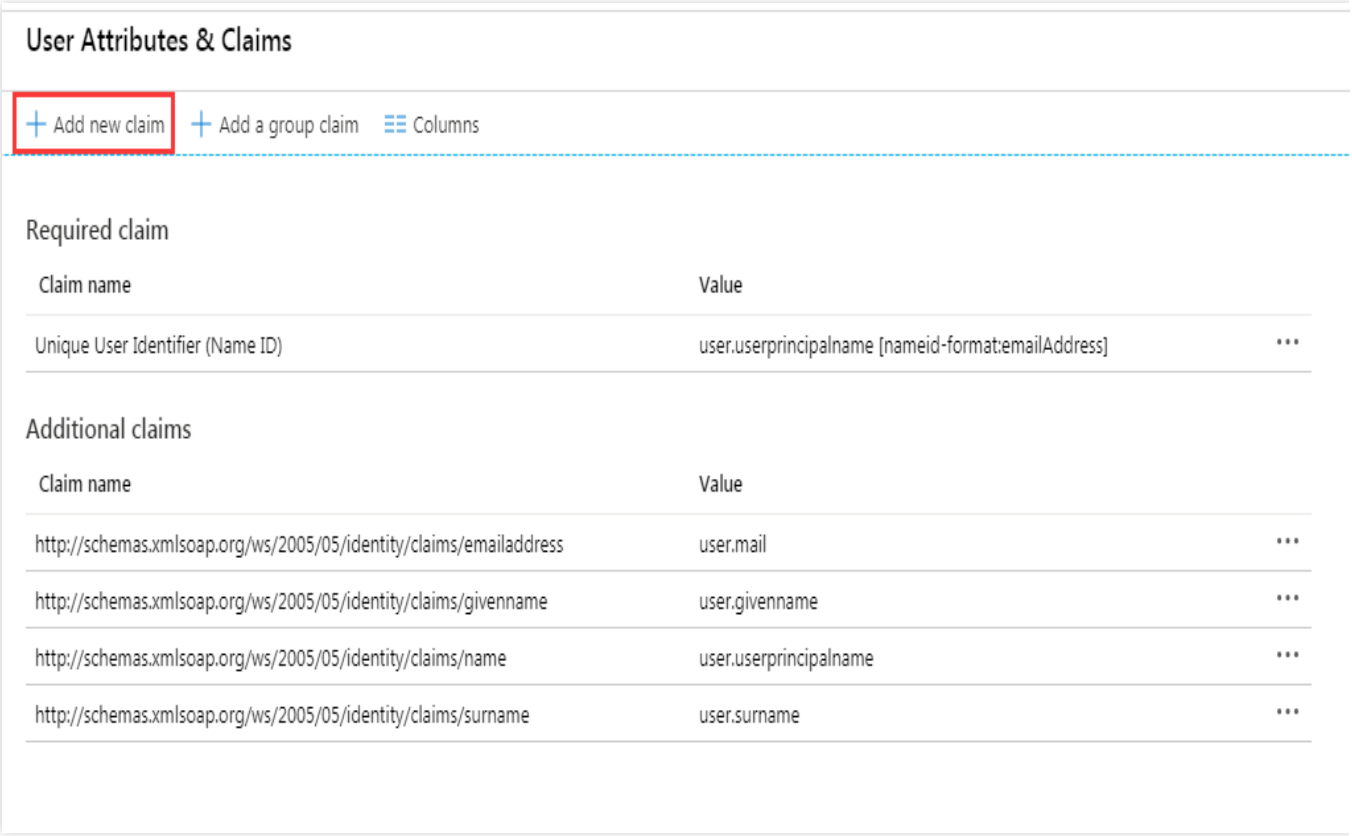
您可以根据您的腾讯云账号所在站点进行配置。

所在站点	标识符（实体 ID）	回复 URL（断言使用者服务 URL）
中国站	cloud.tencent.com	https://cloud.tencent.com/login/saml
国际站	www.tencentcloud.com	https://www.tencentcloud.com/login/saml

3. 在 “SAML 单一登录”概览界面，单击“用户属性和声明”右上角的

，打开“用户属性声明”编辑页面。如下图所示：

4. 在“用户属性和声明”编辑页面，单击**添加新的声明**，进入“管理用户声明”页面。如下图所示：



5. 在“管理用户声明”页面，增加以下两条声明，并单击**保存**。如下图所示：

名称	命名空间	源	源属性
Role	https://cloud.tencent.com/SAML/Attributes	属	qcs::cam::uin/{AccountID}:roleName/{F

		性	provider/{ProviderName}
RoleSessionName	https://cloud.tencent.com/SAML/Attributes	属性	Azure

说明：

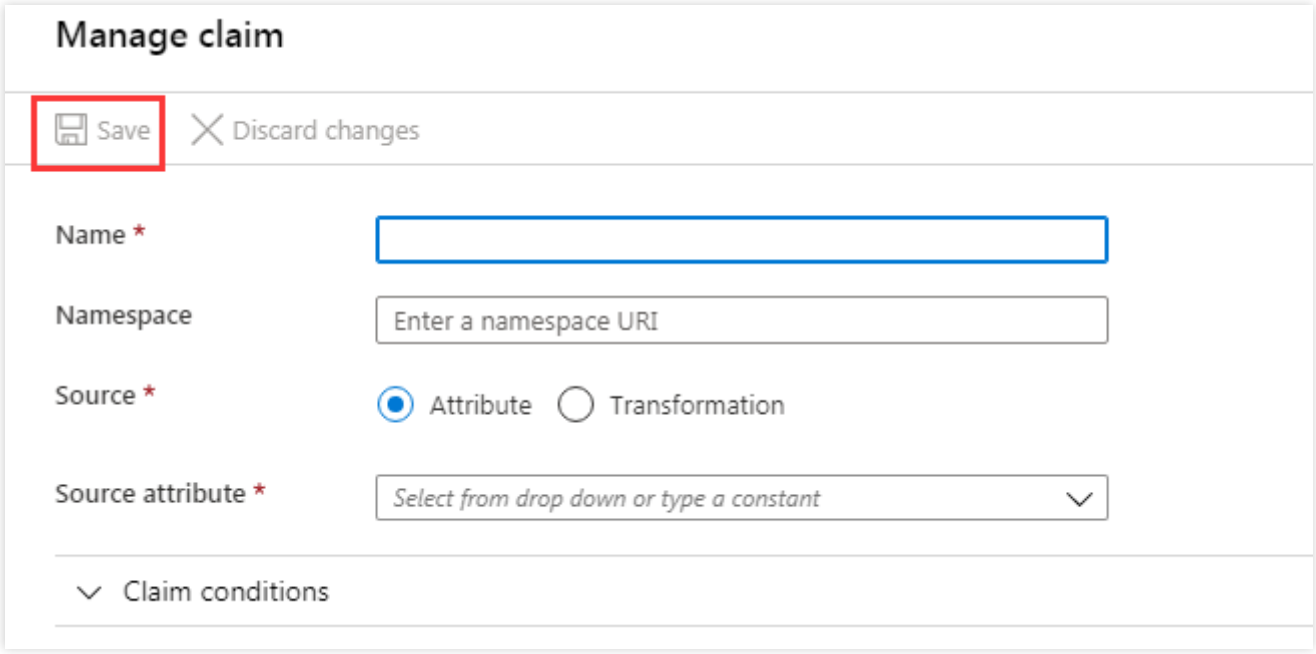
在 Role 源属性中 {AccountID}，{RoleName}，{ProviderName} 分别替换内容下：

{AccountID} 替换为您的腾讯云帐户 ID，可前往 账号信息 - 控制台 查看。

{RoleName} 替换您在腾讯云为身份提供商所创建的角色名称（单击查看如何在腾讯云 为身份提供商创建的角色），角色名称可前往 角色 - 控制台 查看，如需要添加更多可按照该格式添加：

qcs::cam::uin/{AccountID}:roleName/{RoleName}，以 ; 隔开。

{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。

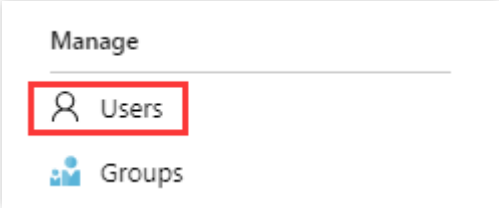


配置 Azure AD 用户

说明：

您可以通过本步骤分配用户访问权限，向 Azure AD 用户分配腾讯云的 SSO 访问权限。

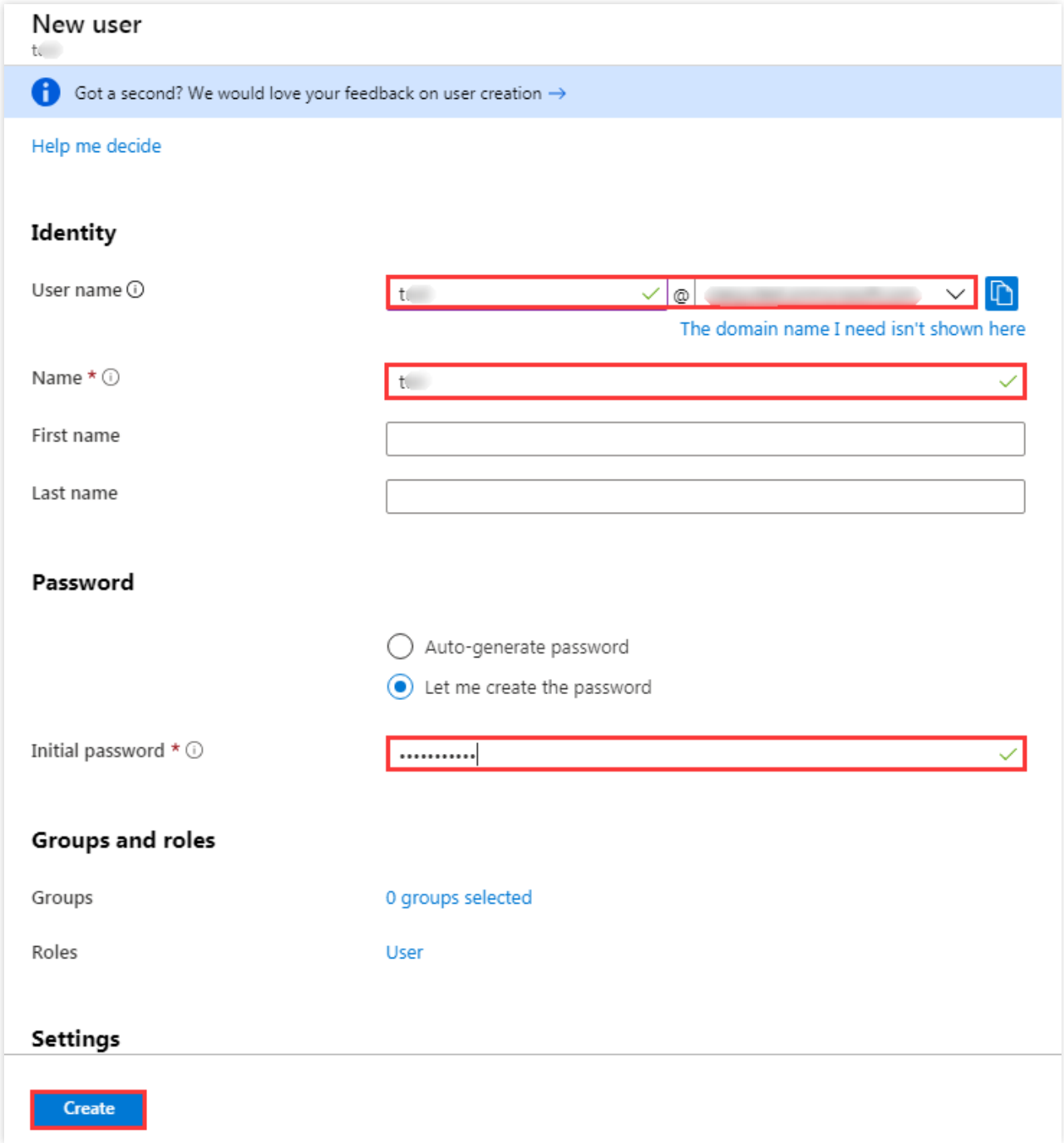
1. 单击左侧导航栏 **Azure Active Directory**，单击**用户 > 所有用户**。



2.

单击左

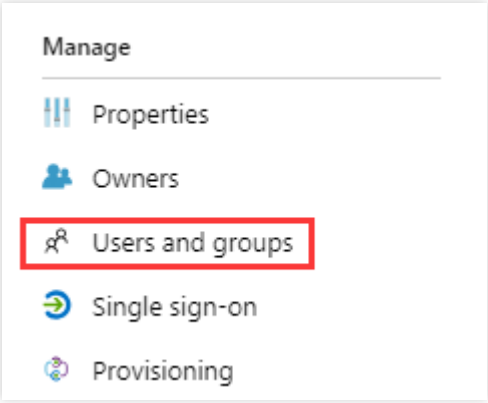
上角**新建用户**，在“用户”页面填写**姓名**、**用户名**，勾选**显示密码**，信息无误后单击下方**创建**完成创建。如下图所示：



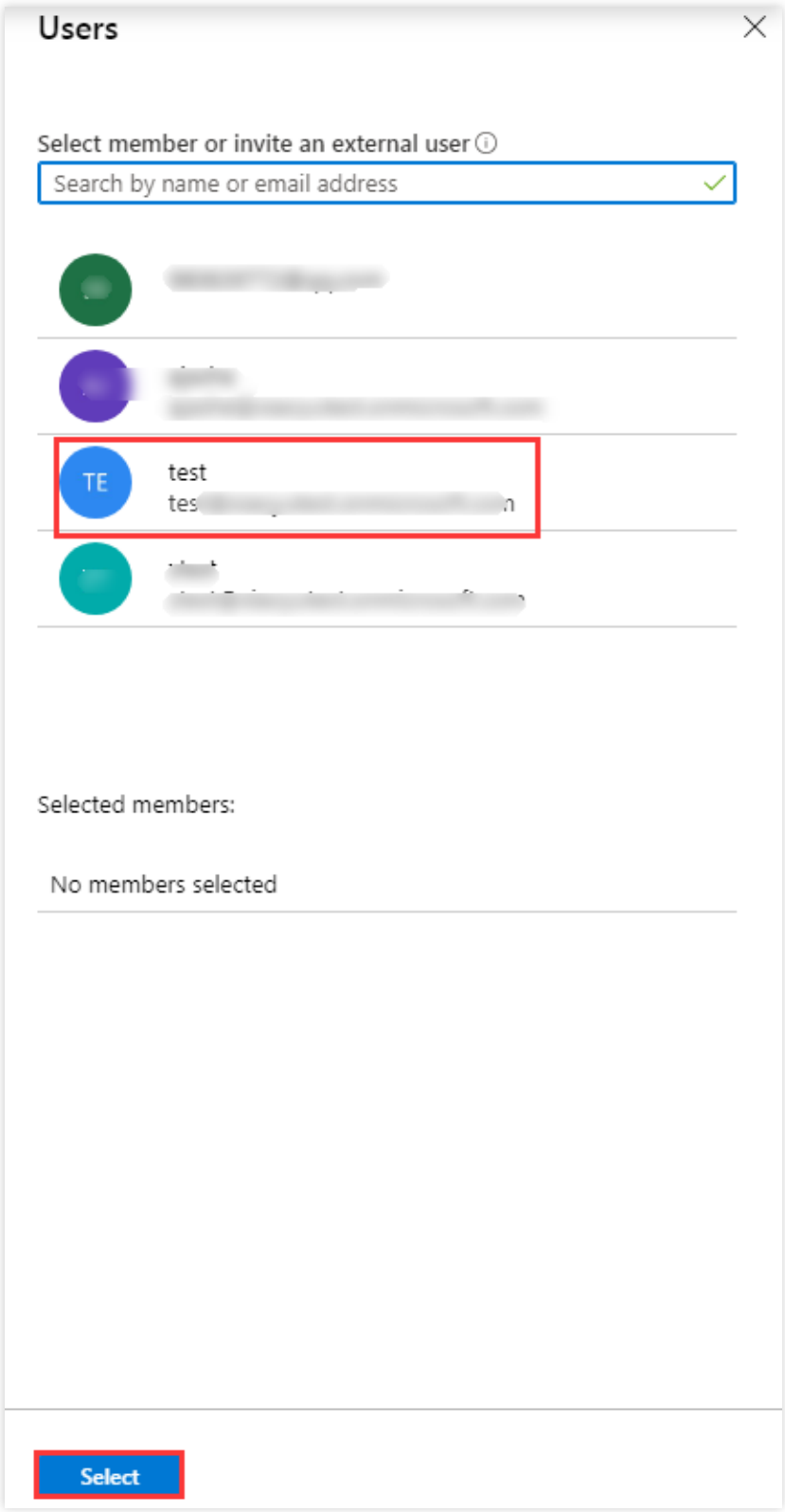
说明：

用户名格式为：用户名@域名。您可以自定义用户名，域名可以单击左侧导航栏 **Azure Active Directory**，打开概述页，查看您之前设置的**初始域名**。您可以复制保存用户名、密码留用。

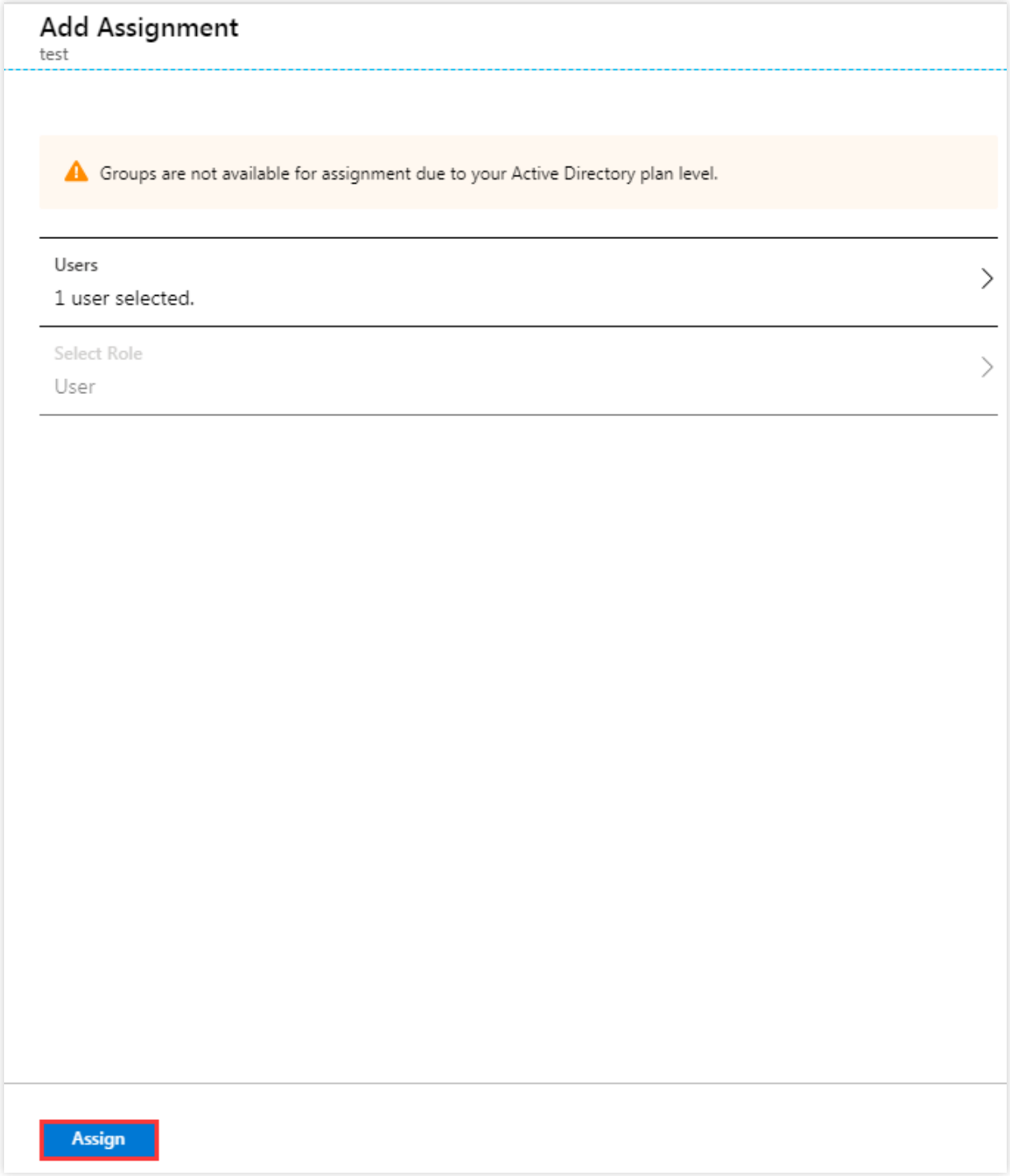
3. 在左侧导航栏中，选择 **Azure Active Directory** > **企业应用程序** > 您创建的应用程序，进入应用程序概览页面，并单击**用户和组**。如下图所示：



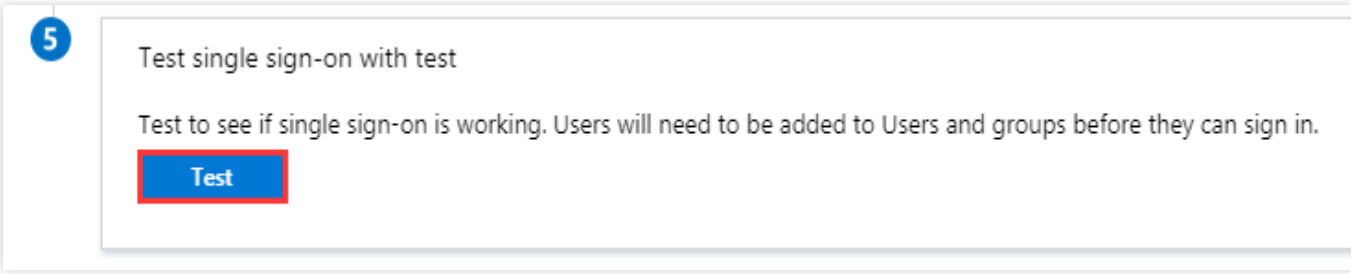
4. 单击**添加用户**，打开**用户和组**，选择 步骤2 您创建的用户，单击**选择**。如下图所示：



5. 跳转到“添加分配”页面，确认后单击**分配**。如下图所示：



6. 在左侧导航栏中，选择 **Azure Active Directory>企业应用程序>** 您创建的应用程序，进入应用程序概览页面。
7. 单击**单一登录**，打开 “SAML 单一登录”概览界面，单击**测试**。如下图所示：



8. 在“测试单一登录”界面，选择**以其他用户的身份登录**。
9. 输入 步骤2 保存的用户名、密码，登录腾讯云控制台。

OneLogin 单点登录腾讯云指南

最近更新时间：2024-12-16 17:19:58

操作场景

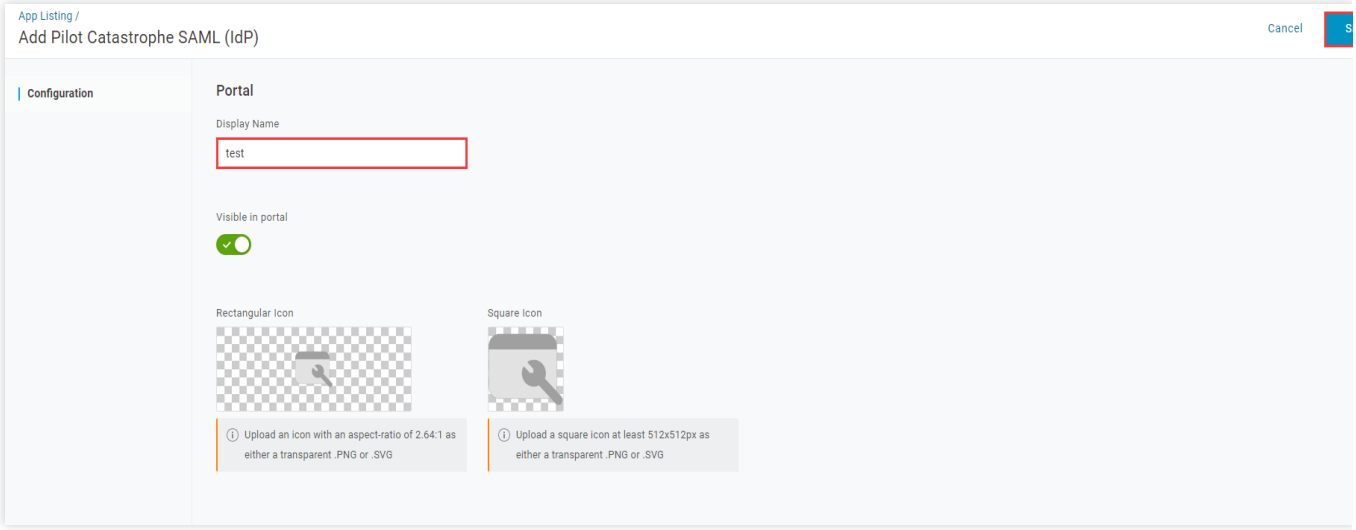
OneLogin 是一家云身份访问管理解决方案提供商，可以通过其身份认证系统一键登录企业内部所有需要的系统平台。腾讯云支持基于 SAML 2.0（安全断言标记语言 2.0）的联合身份验证，SAML 2.0 是 OneLogin 等许多身份验证提供商（Identity Provider，IdP）使用的一种开放标准。
使用身份提供商可实现联合单点登录（Federated Single Sign-on，SSO），管理者可以授权通过联合身份验证的用户登录腾讯云管理控制台或调用腾讯云 API 操作，而不必为企业或组织中的每一个成员都创建一个 CAM 子用户。
本教程为 OneLogin 单点登录至腾讯云的配置指南。

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”，并在结果列表中单击 **Pilot Catastrophe SAML(IdP)**。如下图所示：

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：



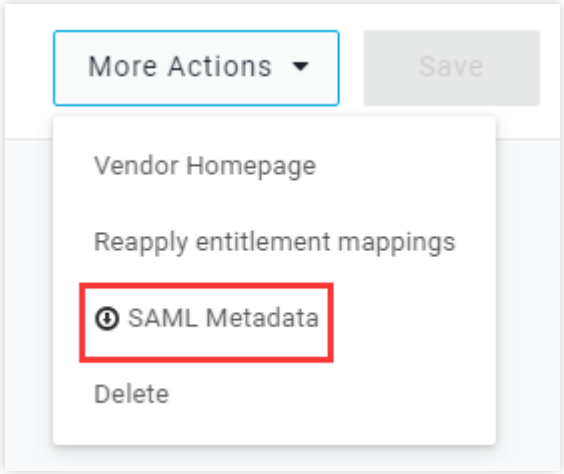
配置 CAM

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 ACTION**，选择**SAML Metadata**，下载 IDP 云数据文档。如下图所示：



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

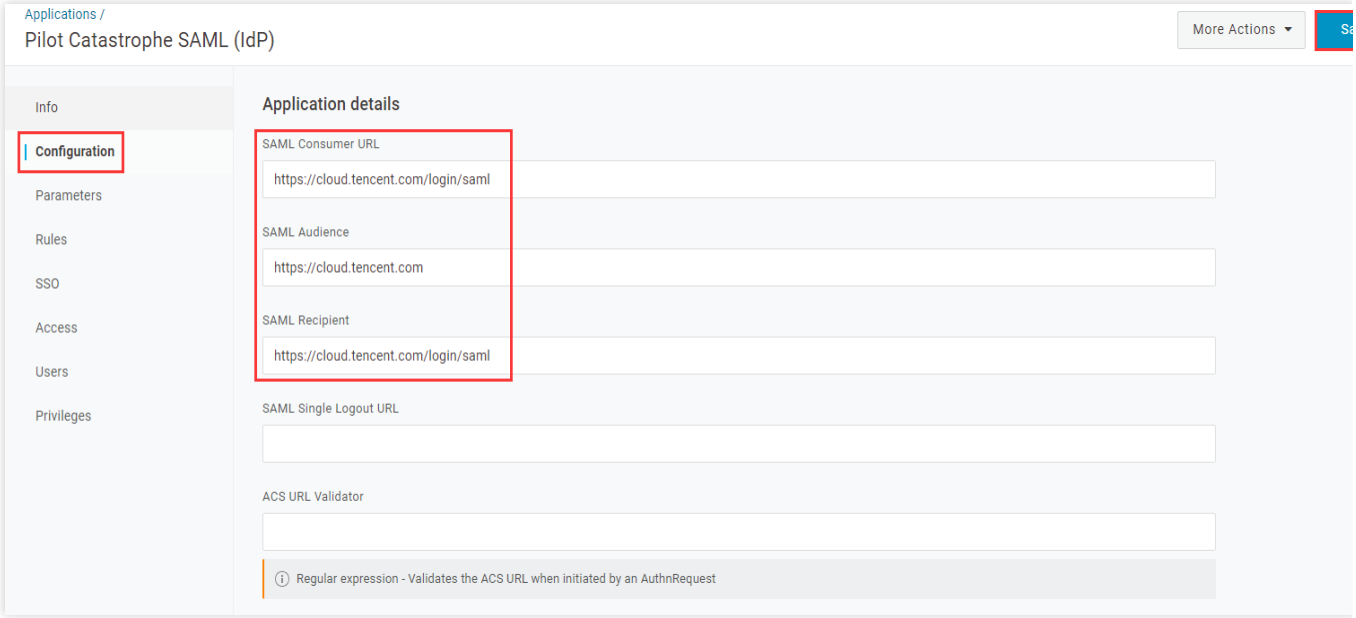
配置 OneLogin 单点登录

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：



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
国际站	https://www.tencentcloud.com/login/saml	https://www.tencentcloud.com/login/saml	https://www.tence

3. 单击 **Parameters**，选择 **Add parameter**，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	Macro	qcs::cam::uin/{AccountID provider/{ProviderName}
https://cloud.tencent.com/SAML/Attributes/RoleSessionName	Include in SAML assertion	Macro	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

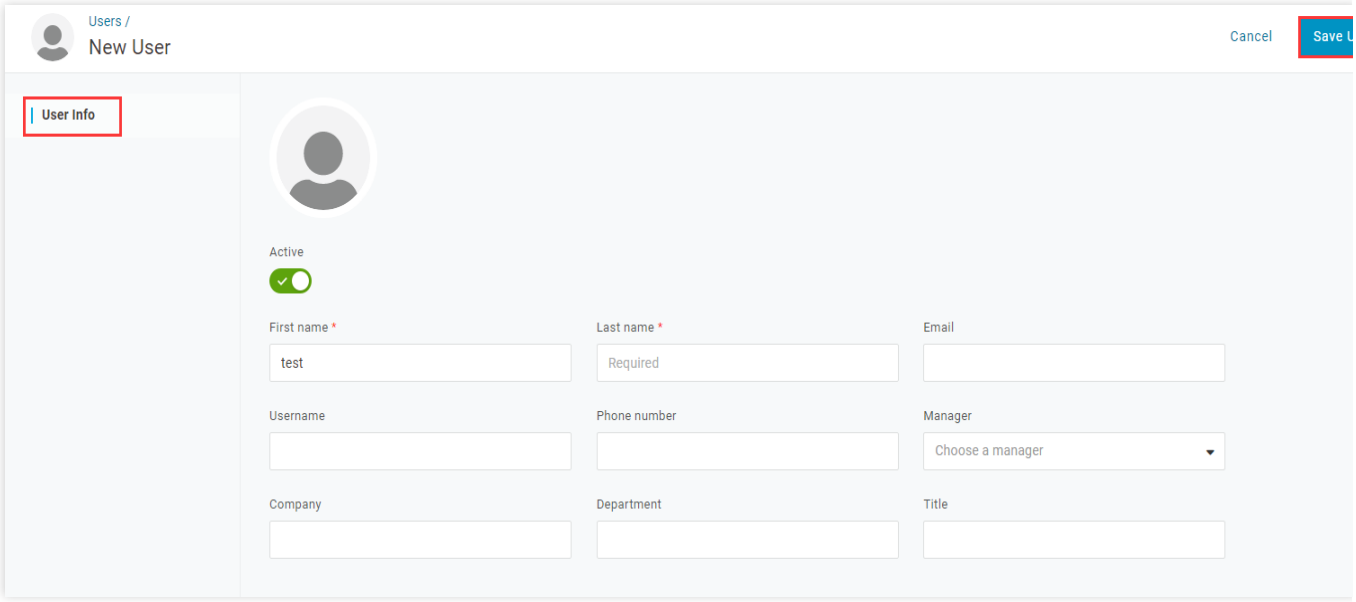
1. 登录并访问 OneLogin 网站，单击 **Users**，进入用户管理页面。

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：

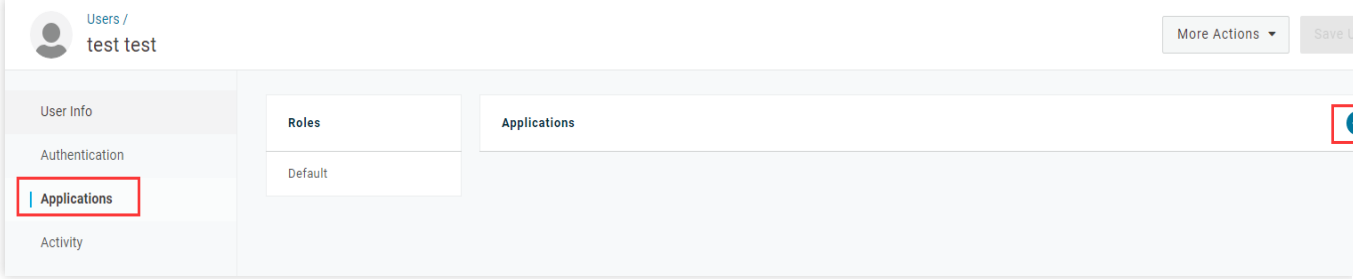


说明：

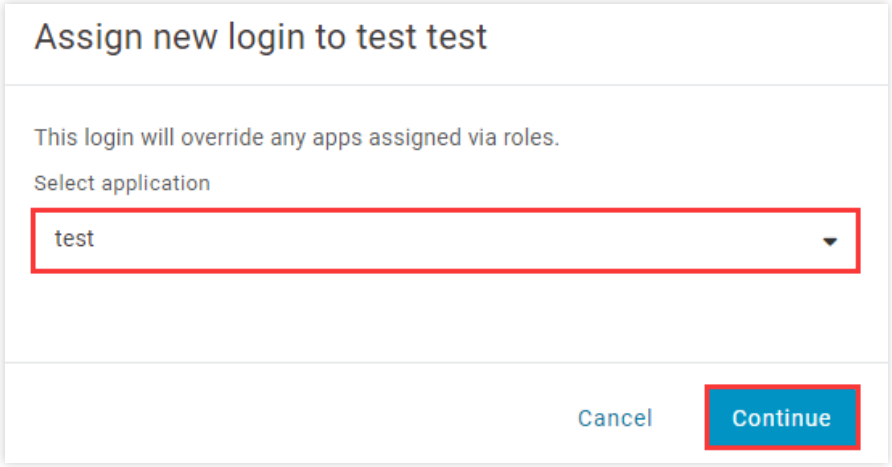
此帐户密码可查看 Email，或单击 **MORE ACTIONS** 选择 **change password** 修改密码。

4. 单击用户编辑页 **Applications**，选择右侧的

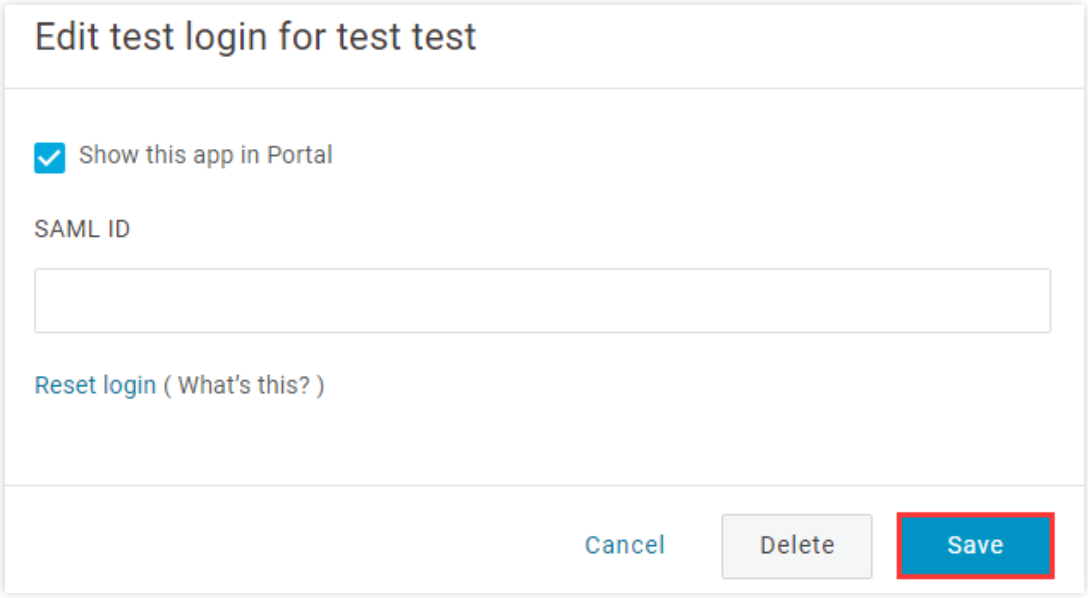
。如下图所示：



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



6. 在编辑页面，单击 **SAVE**。如下图所示：



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

Okta 单点登录腾讯云指南

最近更新时间：2024-01-23 17:46:25

操作场景

Okta 是身份识别与访问管理解决方案提供商。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 是许多身份验证提供商（Identity Provider， IdP）使用的一种开放标准。您可以通过基于 SAML 2.0 联合身份验证将 Okta 与腾讯云进行集成，从而实现 Okta 帐户自动登录（单一登录）腾讯云控制台管理腾讯云的资源，不必为企业或组织中的每一个成员都创建一个 CAM 子用户。

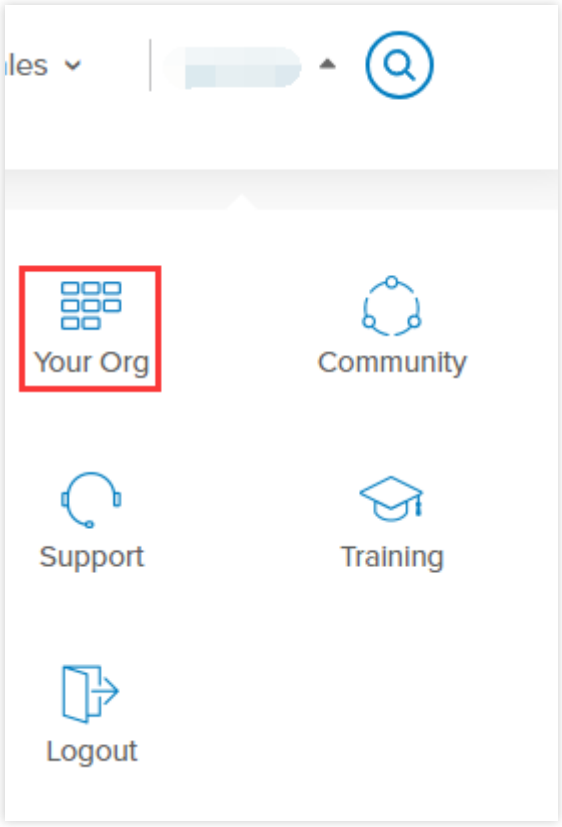
操作步骤

创建 Okta 应用程序

说明：

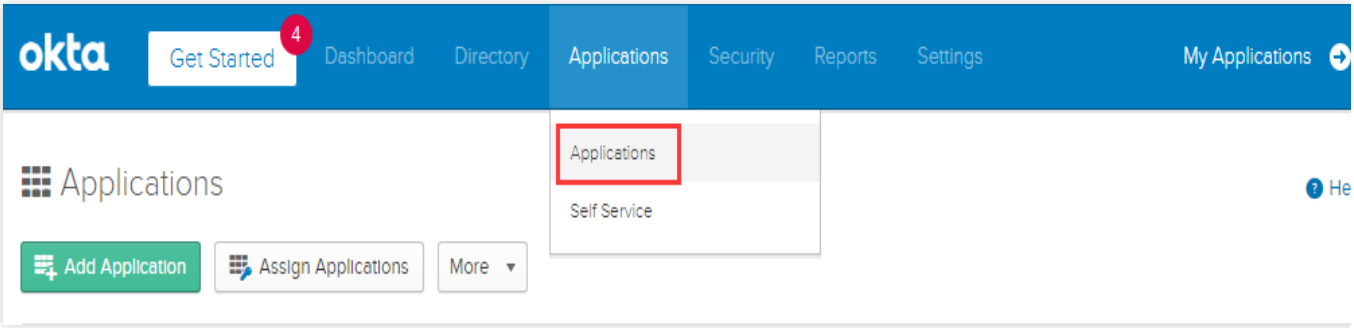
您可以通过本步骤创建 Okta 应用程序，如您已经有正在使用的应用程序，可忽略本操作，进行 配置 CAM。

1. 登录进入 Okta 网站，单击右上角**用户名称>Your Org**，如下图所示：

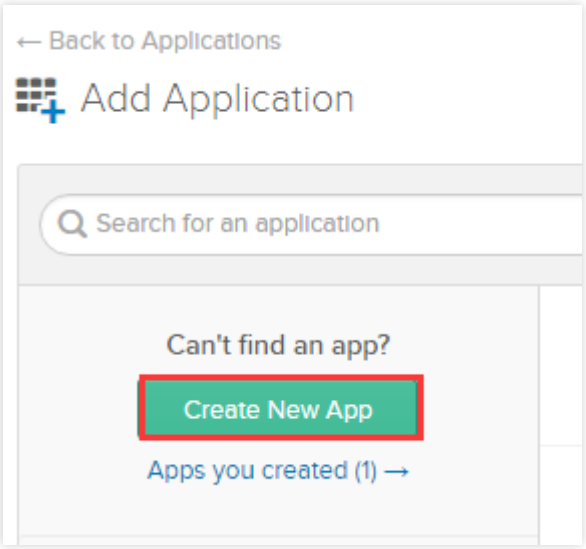


2. 在 Okta 主页，单击右上角**管理员**，进入

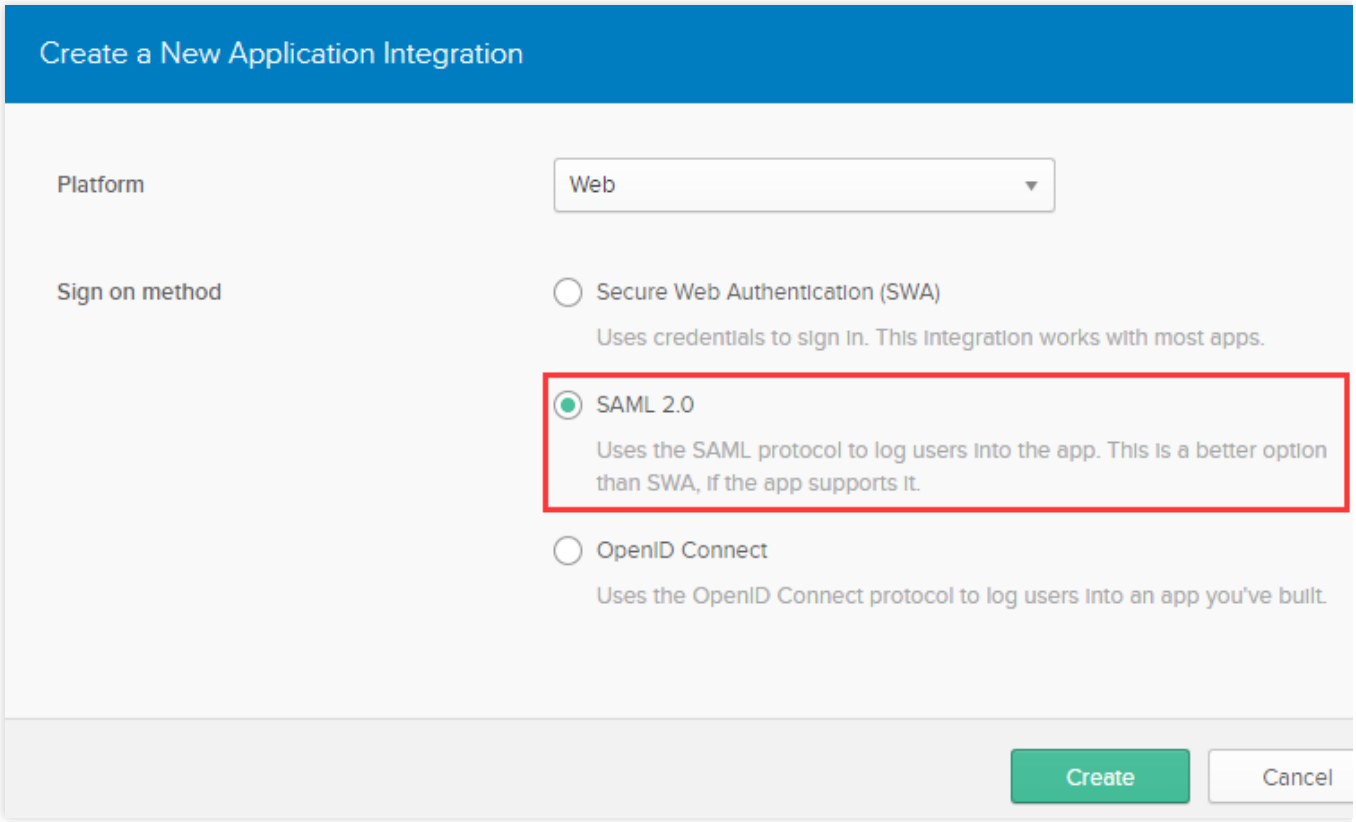
管理员界
面。
3. 在管理员页面，选择 Applications，进入应
用管理页面。
如下图所示：



4. 在应用管理页面，单击 **Add Application**。进入添加应用页面。
5. 在添加应用页面，单击 **Create New APP**。如下图所示：



6. 在弹出的创建应用程序/Create a New Application Integration 窗口，选择 Platform 及 Sign on method，其中 Sign on method 设置为 SAML 2.0，单击 **Create**，如下图所示：



7. 在通用设置/General Settings 页面，补充 App name、App logo（可选）、App visibility（可选）信息，单击 **Next**，此应用程序可以用于和腾讯云进行集成，实现 Okta 帐户自动登录（单一登录）腾讯云控制台管理腾讯云的资源。

为 Okta 应用程序配置 SAML

说明：

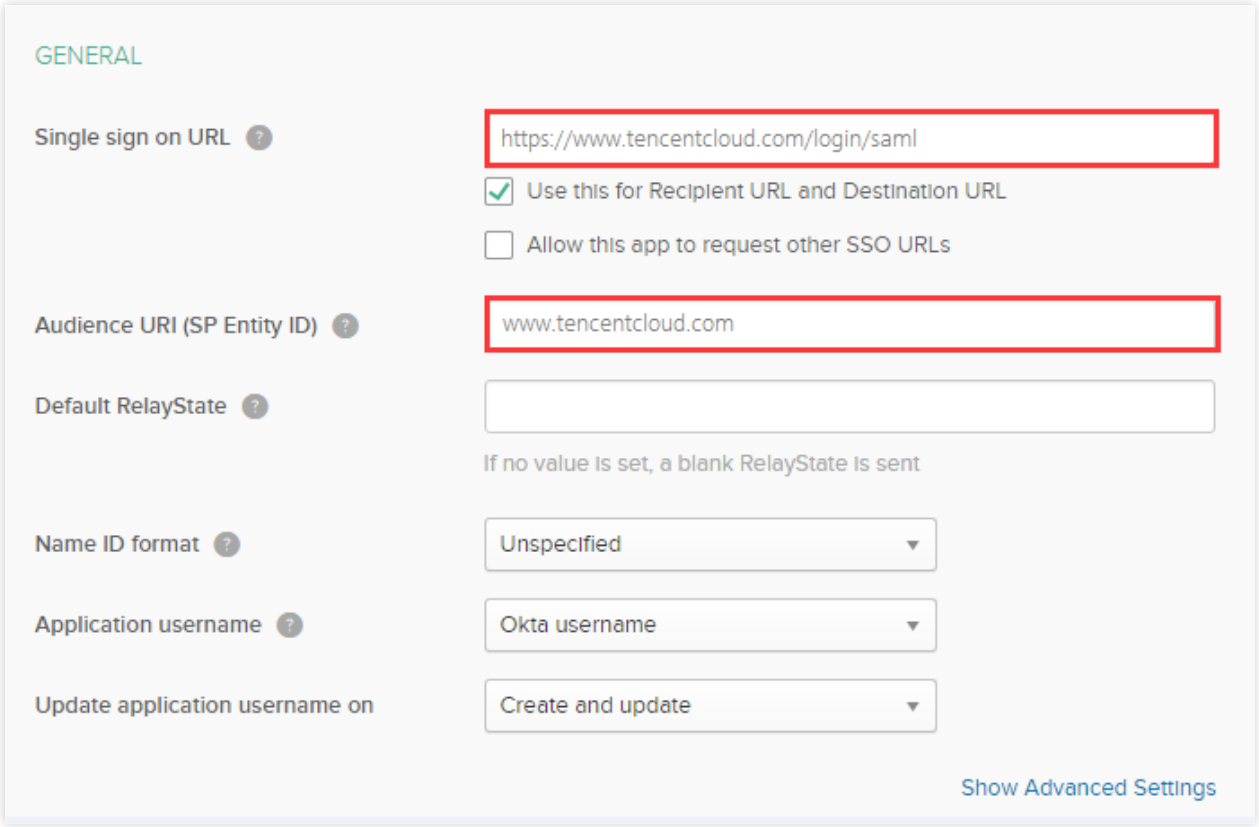
您可以通过本步骤将 Okta 应用程序属性映射到腾讯云的属性，建立 Okta 和腾讯云之间的信任关系使之相互信任。

如您是参考 创建 Okta 应用程序 创建的应用程序，可直接进行操作 步骤3 。

1. 前往 应用管理页面 ，单击您创建的应用程序名称。

2. 在通用/GENERAL 页面，单击 SAML Settings 栏下的 **Edit**，确认当前 App name、App logo（可选）、App visibility（可选）信息，单击 **Next**，进入配置 SAML/Configure SAML 页面。

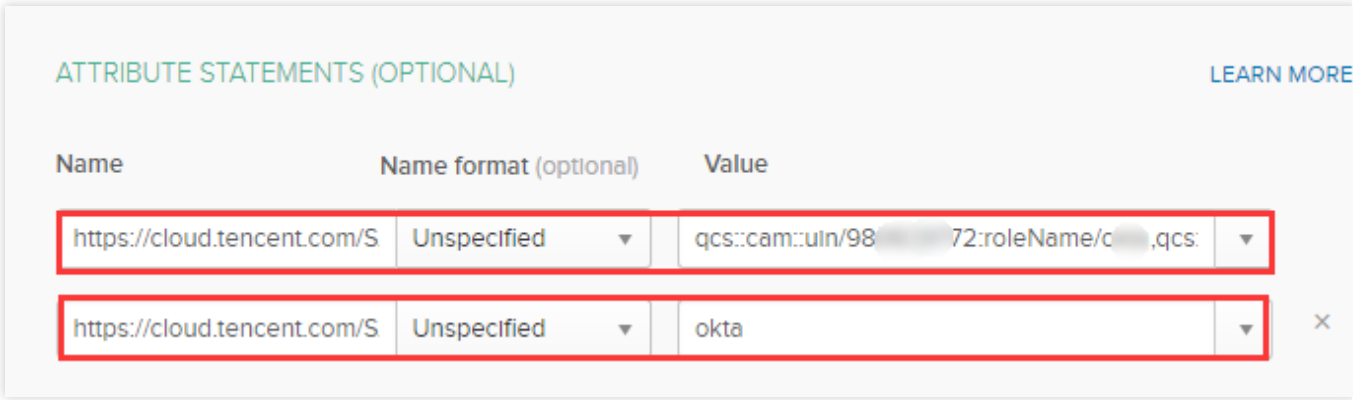
3. 在
配置 SAML/C
onfigure SAML 页面将 GENERAL 下 Single sign on URL 和 Audience URL(SP Entity ID)补充为以下信息，如下图所示：



您可以根据您的腾讯云账号所在站点进行配置：

所在站点	Single sign on URL	Audience URL(SP Entity ID)
国际站	https://www.tencentcloud.com/login/saml	www.tencentcloud.com

4. 在配置 SAML/Configure SAML 页面将 GENERAL 下 ATTRIBUTE STATEMENTS 补充为以下信息。如下图所示：

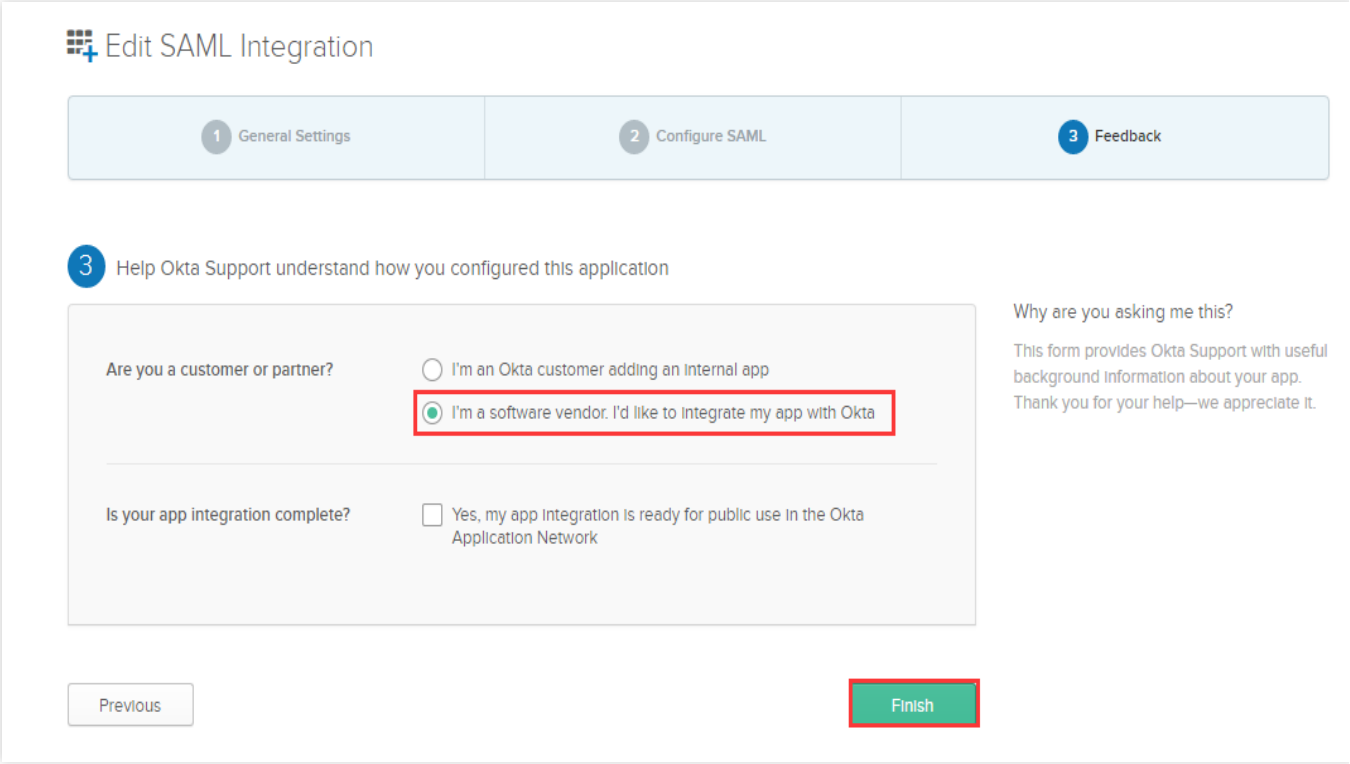


Name	Name format	Value
https://cloud.tencent.com/SAML/Attributes/Role	Unspecified	qcs::cam::uin/{AccountID}:roleNa

		provider/{ProviderName}
https://cloud.tencent.com/SAML/Attributes/RoleSessionName	Unspecified	okta

说明：

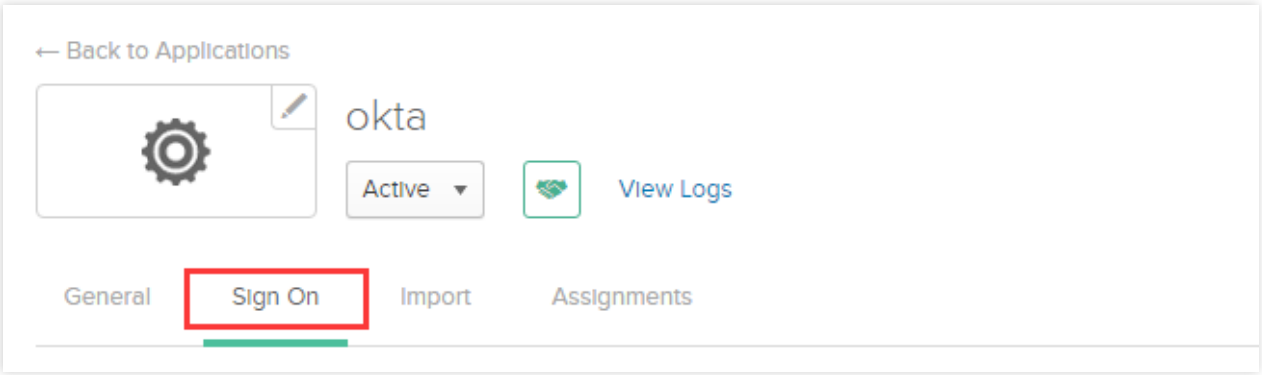
在 Value 中 {AccountID}，{RoleName}，{ProviderName} 分别替换内容下：
{AccountID} 替换为您的腾讯云帐户 ID，可前往 账号信息 - 控制台 查看。
{RoleName}替换您在腾讯云为身份提供商所创建的角色名称（单击查看如何在腾讯云 为身份提供商创建的角色），角色名称可前往 角色 - 控制台 查看，如需要添加更多可按照该格式添加：
qcs::cam::uin/{AccountID}:roleName/{RoleName}，以 ; 隔开。
{ProviderName} 替换您在腾讯云创建的 SAML 身份提供商名称，可前往 身份提供商 - 控制台 查看。
5. 单击 **Next**，进入反馈/Feedback 页面，选择以下信息之后单击 **Finish**，完成配置 CAM 操作。如下图所示：



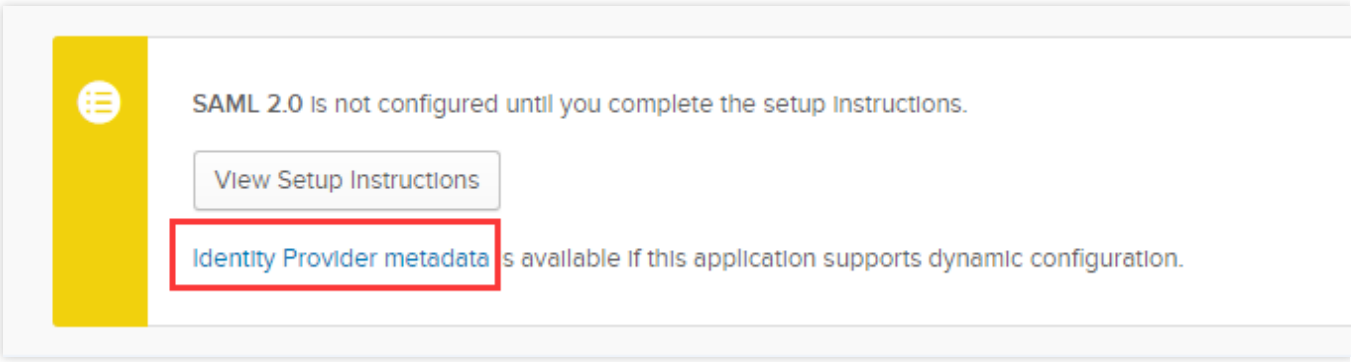
为 Okta 应用程序配置 SAML 集成

说明：

您可以通过本步骤配置 Okta 和腾讯云之间的信任关系使之相互信任。
1. 登录进入 管理员界面，选择 Applications，进入应用管理页面。
2. 在应用管理页面，单击您创建的应用程序名称，进入应用详情页，单击 **Sign On**。如下图所示：



3. 在 Sign On 页面，单击 **Identity Provider metadata**查看身份提供商元数据。如下图所示：



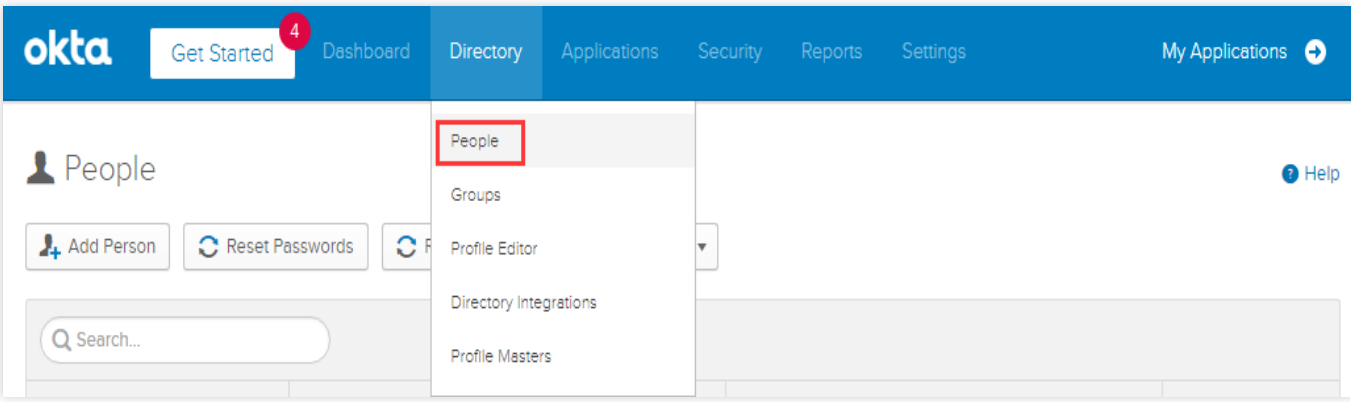
4. 获取身份提供商元数据之后可在查看页面右键保存至本地。
5. 在腾讯云创建 SAML 身份提供商及角色，详细操作请参考 创建身份提供商。

配置 Okta 用户

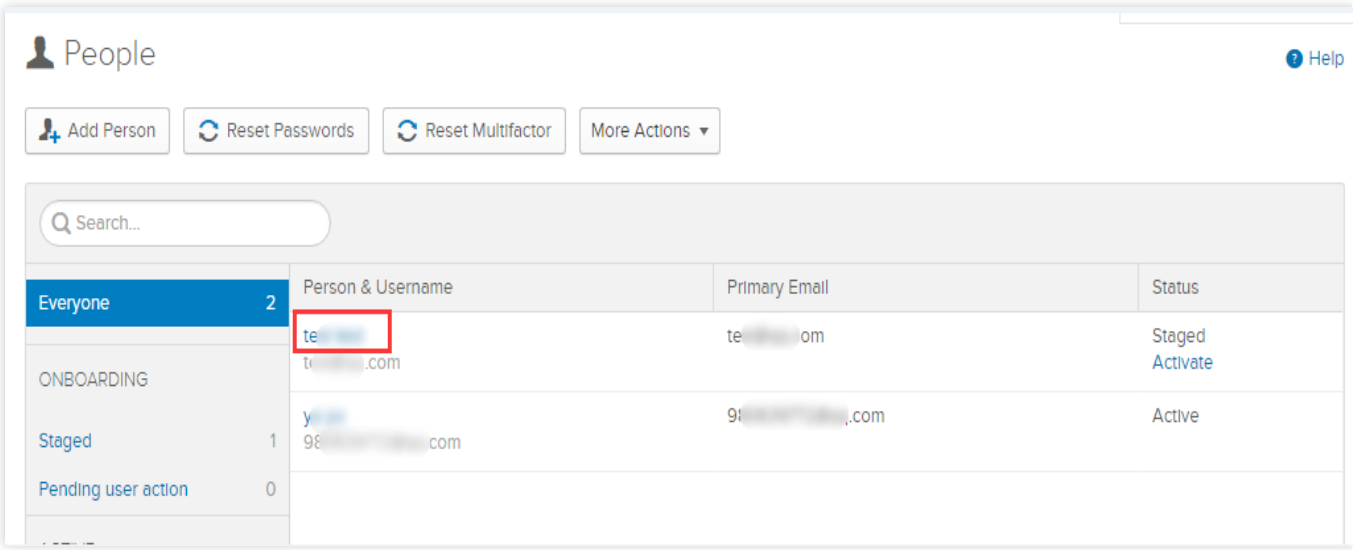
说明：

您可以通过本步骤分配用户访问权限，向 Okta 用户分配腾讯云的 SSO 访问权限。

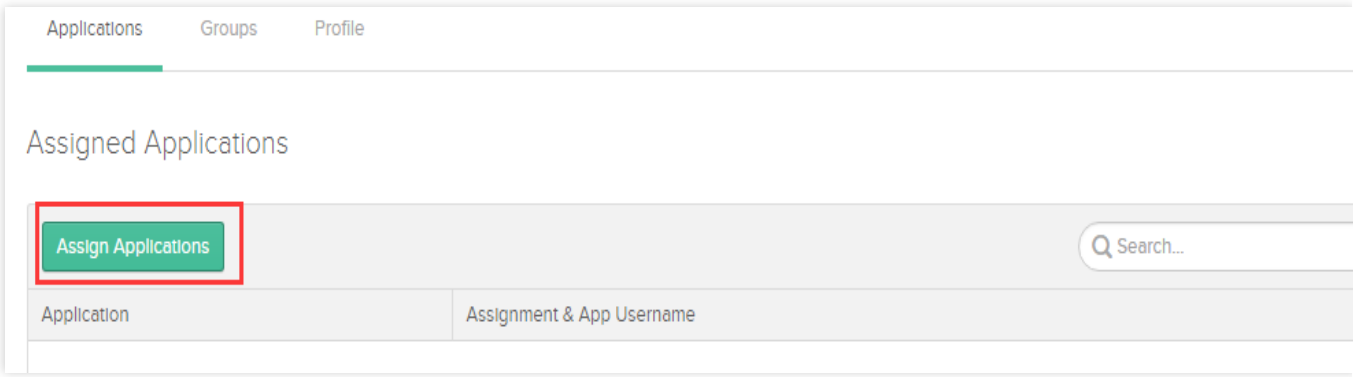
1. 登录进入 管理员界面，单击 Directory 下的 **people**，进入用户管理页面。如下图所示：



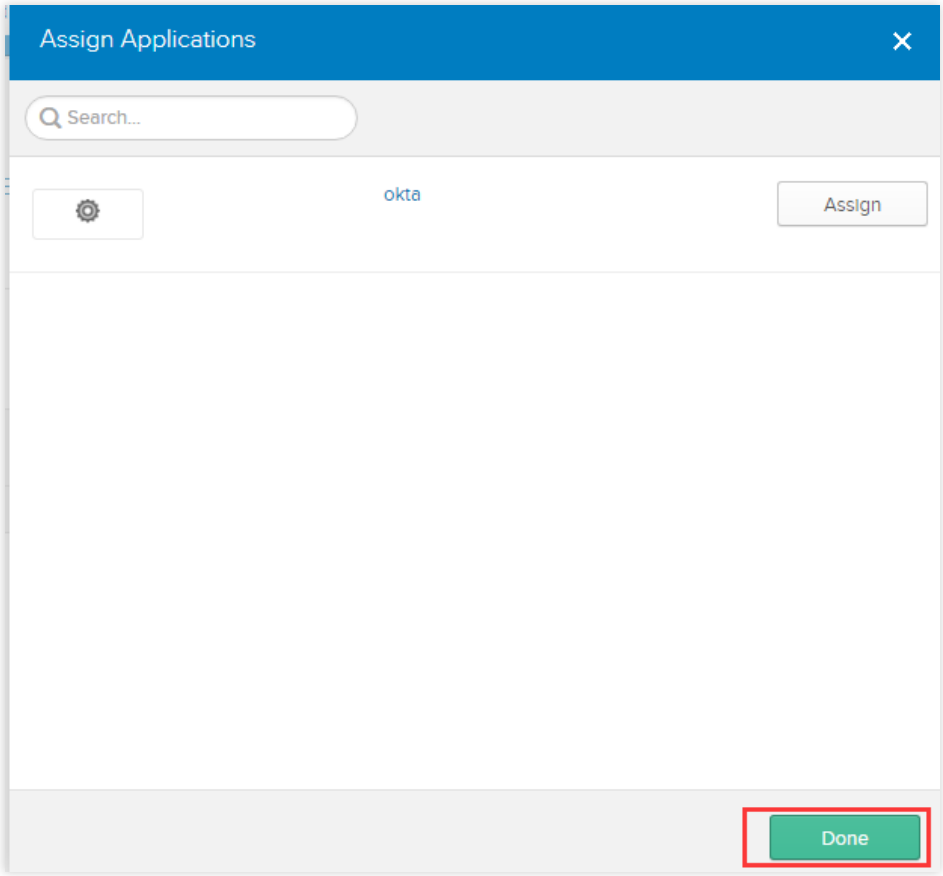
2. 在用户管理页面，单击左上角的 **Everyone**，找到您需要授权的用户。如下图所示：



3. 单击用户名称，进入用户详情页，单击左上角 **Assigned Applications**。如下图所示：



4. 在弹出的设置窗口中，单击 **Done**，完成配置 Okta 用户操作。如下图所示：



5. 前往 应用管理页面，单击您创建的应用程序名称，进入应用详情页。
6. 在应用详情页，选择 GENERAL，复制 App Embed Link 栏下的 EMBED LINK，登录腾讯云控制台。

ADFS 单点登录腾讯云指南

最近更新时间：2024-01-23 17:46:25

操作场景

Active Directory Federation Services（ADFS）是 Microsoft's 推出的 Windows Server 活动目录联合服务 (ADFS). ADFS是一种能够用于一次会话过程中多个Web应用用户认证的新技术。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 是许多身份验证提供商（Identity Provider， IdP）使用的一种开放标准。您可以通过基于 SAML 2.0 联合身份验证将 ADFS 与腾讯云进行集成，从而实现 ADFS 帐户自动登录（单一登录）腾讯云控制台管理腾讯云的资源，不必为企业或组织中的每一个成员都创建一个 CAM 子用户。

前提条件

拥有一台 Windows Server 云服务器。如您需要购买服务器，请参阅 云服务器-购买指南。
已进入服务器管理-仪表板页面，找到电脑中的添加角色和功能向导（ 参考 安装或卸载角色、角色服务或功能）。
拥有一个已完成实名认证的域名。

操作步骤

安装 AD 域服务和 DNS 服务

1. 在仪表板管理页面，单击**添加角色和功能**，保持页面默认信息，一直单击**下一步**，进入添加角色和功能向导页面。
2. 在添加角色和功能向导页面， 保持页面默认信息，一直单
击**下一**
步，在服务器角色信息栏勾选 Active Directory 域服务、DNS 服务器。
3. 保持页面默认信息，一直单击**下一步**，单击**安装**。在完成安装成功界面，单击右上角

或在安装完成界面。
4. 单击**提升为域控制器**，进入部署配置页面，填写域名，本文中示例为：example.com。
5. 单击**下一步**，完成安装后，输入密码。保持页面默认信息，一直单击**下一步**。
6. 单击**安装**，安装完成后重启服务器。
7. 完成 AD 域服务、DNS 服务安装，并将服务器提升为域控制器完毕。

安装 Web 服务器

1. 参考安装 AD 域服务和 DNS 服务中 步骤2，进入服务器角色页面，在服务器角色信息栏勾选 Web 服务器。
2. 保持页面默认信息，一直单击**下一步>安装**，完成 Web 服务器安装。

申请证书

如您已拥有 SSL 证书，可直接进行 安装 ADFS 操作。

1. 单击左下角**Windows图标**，在搜索框输入“mmc”命令，回车执行，进入控制台1-[控制台根节点]页面。
2. 在控制台1-[控制台根节点]页面，单击**文件 > 添加/删除管理单元**，在弹出的窗口中选择证书，单击**添加 > 完成**。
3. 单击
证书
，在展开的目录中，右键单击**个人**，单击**所有任务 > 高级操作 > 创建自定义请求**。
4. 保持页面默认信息，一直单击**下一步**，进入证书注册页面，单击**不使用注册策略继续**。
5. 在自定义请求页面，选择以下信息：
模板：（无模板）旧密钥
请求格式：PKCS#10
6. 单击**详细信息 > 证书属性**，在常规栏补充友好名称、描述信息。
7. 在使用者栏，填写值信息，本次示例为（*.example.com），单击**添加**。
8. 在私钥栏下勾选 Microsoft RSA SChanel Cytographic Provider（加密）、使私钥可以导出。
9. 单击**确认 > 下一步**，选择需要保存的目录，保存证书，单击完成。

安装 ADC(AD证书服务器)

1. 参考安装 AD 域服务和 DNS 服务中 步骤2，在服务器角色信息栏勾选 Active Directory 证书服务器。
2. 保持默认信息，一直单击**下一步**，在角色服务栏勾选证书颁发机构、证书颁发机构 Web 注册。
3. 单击**安装**，在完成安装成功界面，单击右上角

，单击**配置目标服务器的 Active Directory 证书服务**。
4. 保持页面默认信息，一直单击**下一步**，在角色服务栏勾选证书颁发机构、证书颁发机构 Web 注册。
5. 保持页面默认信息，一直单击**下一步**，单击**配置**，完成安装 ADC。

生成 SSL 证书

1. 访问 https://localhost/certsrv， 单击**申请证书**。
2. 在申请一个证书页面，单击**高级证书申请**。
3. 在高级证书申请页面，单击**使用 base64 编码的 CMC 或 PKCS#10 文件提交一个证书申请，或使用 base64 编码的 KCS#7 文件 续订证书申请**。
4. 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**。
5. 申请成功，
单击**下载**
（两种格式均需下载）。

6. 参考申请证书的 步骤3，右键单击**个人**，单击**所有任务>导入**。
7. 选择 步骤5 保存的证书文件，保持页面默认信息，一直单击**下一步>完成**。
8. 参考申请证书的 步骤3，右键单击**个人**，单击**所有任务>导出**。
9. 在证书导出向导页面，选择“是，导出私钥”，勾选“组或用户名（建议）”，单击下一步，完成导出保存文件

。

安装 ADFS

1. 参考
安装 AD 域服务
和 DNS 服务中 步骤2，进入服务器角色页面，勾选 Active Directory 联合身份验证服务。
2. 保持页面默认信息，一直单击**下一步>完成**，在结果页面，单击**在此服务器上配置联合身份验证服务**。
3. 保持页面默认信息，一直单击**下一步**，进入指定服务属性页面，填写导入以下信息
SSL 证书：导入在生成 SSL 证书中 步骤9 保存的证书文件。
联合身份服务名称：目标服务器名称（与右上角信息保持一致）或 sts.域名或 adfs.域名。
联合身份验证服务显示名称：用户在登录时看到显示名称。
4. 在指定服务账户页面，输
入账户名称
、密码，保持页面默认信息，一直单击**下一步**直到安装 ADFS 完成。
5. 访问以下链接下载 XML 文件。

```
https://联合身份验证服务器名称/federationmetadata/2007-06/federationmetadata.xml
```

6. 在 powerShell 中执行 Set-AdfsProperties –EnableIdpInitiatedSignonPage $True，
访问以下入口进行登录。

```
https://联合身份验证服务器名称/adfs/ls/idpinitiatedSignOn.htm
```

7. 输入 步骤4 中的账号名称、密码登录。

说明：

如浏览器登录提示出现400 Bad Request，在 powerShell 中进行以下操作：
首先获取启动 ADFS 服务的用户。然后打开 PowerShell，执行脚本 setspn -s http/ADFS 所在服务器的访问地址 域控\\用户。例如，ADFS 所在服务器的全称为 172_21_0_13.weezer.club ，域控机器为WEEZER，用户为 Administrator，那么所执行的脚本就是 setspn -s http/172_21_0_13.weezer.club WEEZER\\Administrator。

在腾讯云创建身份提供商

说明：

您可以通过本步骤配置 ADFS 和腾讯云之间的信任关系使之相互信任。
在腾讯云创建 SAML 身份提供商，命名格式为纯英文，保存您的身份提供商名称。详
细操作

请参阅 创建身份提供商。

为身份提供商创建角色

说明：

您可以通过本步骤分配用户访问权限，向 ADFS 用户分配腾讯云的 SSO 访问权限。

为您的身份提供商创建角色，命名格式为纯英文，保存您的角

色名称

。详细操作请参阅 为身份提供商创建角色 。

其中身份提供商选择在 腾讯云创建身份提供商 步骤中创建的身份提供商。

配置用户和用户组

1. 在服务器管理器仪表板页面，单击右上角工具，选择 Active Directory 用户和计算机。
2. 在 Active Directory 用户和计算机页面，单击**操作** > **新建** > **组**。
3. 在新建对象-组页面， 填写组名信息。

说明：

<您的主账号 ID>替换为您的腾讯云帐户 ID，可前往 账号信息 - 控制台 查看。

<腾讯云角色名>替换为您在腾讯云为身份提供商所创建的 角色名称。

4. 在 Active Directory 用户和计算机页面，单击**操作** > **新建** > **用户**。
5. 新建员工，填写员工基本信息，以英文命名用户名称，保存用户名称。
6. 在 Active Directory 用户和计算机页面，在 Users 文件夹中找到新添加的用户，将用户添加至用户组。

配置映射规则

1. 单击服务器管理器-ADFS 页面右上角**工具**。
2. 选择 ADFS 管理，单击**添加信赖方**。
3. 在添加信赖方信任向导页面，选择“声明感知”，单击**启动**。
4. 访问以下链接下载腾讯云身份提供商的 XML 文件。

```
https://cloud.tencent.com/saml.xml
```

5. 导入腾讯云身份提供商的文件。
6. 保持页面默认信息，一直单击**下一步** > **完成**。
7. 单击**信赖方信任** > **添加规则** > **编辑声明颁发策略**。
8. 在添加转换声明规则向导页面，单击**选择规则类型** > **转换传入声明** > **下一步**。
9. 在编辑规则页面，补充规则信息，单击**确定**。

说明：

声明规则名称：补充为 NameID。

传入声明类型： 选择 Windows 账户名。

传出声明类型：选择名称 ID。

传出名称 ID 格式：选择永久标识符。

勾选传递所有声明值。

10. 在添加转换声明规则向导页面，单击**选择规则类型 > 使用自定义规则发送声明 > 下一步**。

11. 在编辑规则页面，补充规则信息，单击确定。

说明：

声明规则名称：补充为 Get AD Groups。

自定义规则： 补充以下信息

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "AD AUTHORITY"]
=> add(store = "Active Directory", types = ("http://temp/variable"), query =
";tokenGroups;{0}", param = c.Value);
```

12. 在添加转换声明规则向导页面，单击**选择规则类型 > 使用自定义规则发送声明 > 下一步**。

13. 在编辑规则页面，补充规则信息，单击确定。

说明：

声明规则名称：补充为 Role。

自定义规则： 补充以下信息：

```
c:[Type == "http://temp/variable", Value =~ "(?i)^Tencent-([\\d]+)"]
 => issue(Type = "https://cloud.tencent.com/SAML/Attributes/Role", Value =
RegExReplace(c.Value, "Tencent-([\\d]+)-(.+)",
"qcs::cam::uin/$1:roleName/$2,qcs::cam::uin/$1:saml-provider/身份提供商名称"));
```

其中“身份提供商名称”替换为您在 腾讯云创建身份提供商 步骤创建的身份提供商名称。

14. 在添加转换声明规则向导页面，单击**选择规则类型>使用自定义规则发送声明>下一步**。

15. 在编辑规则页面，补充规则信息，单击**确定**。如下图所示：

说明：

声明规则名称：RoleSessionName。

自定义规则： 补充以下信息

```
 c:[Type == "http://temp/variable", Value =~ "(?i)^Tencent-([\\d]+)"]
 => issue(Type = "https://cloud.tencent.com/SAML/Attributes/RoleSessionName",
Value = RegExReplace(c.Value, "Tencent-([\\d]+)-(.+)", "test"));
```

说明：

如您需要在 ADFS 服务器之外的浏览器单点登录腾讯云，可以在域名服务商配置子域名（您的联合身份验证服务器名称），然后在进行访问登录。

使用 OIDC 进行角色 SSO

最近更新时间：2024-01-23 17:46:25

使用基于 OIDC 协议的角色 SSO 时，需要在腾讯云控制台创建身份提供商并为其创建角色，然后再使用身份提供商签发的 OIDC Token 换取腾讯云的 STS Token（角色的临时秘钥）。

一、创建 OIDC 身份提供商

1. 在 CAM 控制台的左侧导航栏，选择身份提供商 > 角色SSO。
2. 在角色 SSO 页面，单击**新建提供商**。
3. 在新建身份提供商页面，选择提供商类型“OIDC”，并填写身份提供商信息：

身份提供商名称：自定义身份提供商的名称，同一个腾讯云账号下必须唯一。
身份提供商 URL：OIDC 身份提供商标识，由外部 IdP 提供，必须以 http 开头，符合标准 URL 格式。
客户端 ID：在 OIDC 身份提供商注册的客户端 ID，如果有多个应用需要访问腾讯云，可以配置多个客户端ID。
签名公钥：验证 OIDC 身份提供商 ID Token 签名的公钥。对应身份提供商提供的 OIDC 元数据文档中 "jwks_uri" 字段中链接的内容（在浏览器中打开链接获取内容）。为了您的账号安全，建议您定期轮换签名公钥。
备注信息：为身份提供商添加的备注信息。

4. 单击**下一步**进入信息审阅页面。
5. 确认信息无误后，单击**完成**保存。

二、为身份提供商创建角色

1. 在 CAM 控制台的左侧导航栏，单击**角色**。
2. 在角色管理页面，单击**新建角色**。
3. 选择角色载体为身份提供商。
4. 在新建自定义角色页面，选择身份提供商类型为 OIDC。
5. 选择已经创建好的身份提供商。
6. 设置角色的使用条件：

oidc:iss：OIDC 颁发者（Issuer），必填。该限定条件必须使用 string_equal，条件值只能是您在 OIDC 身份提供商中填写的身份提供商 URL。用来扮演角色的 OIDC 令牌中的 iss 字段值必须满足该限制条件要求，角色才允许被扮演。
oidc:aud：OIDC 受众（Audience），必填。该限定条件必须使用 string_equal，条件值只能使用在 OIDC 身份提供商中配置的一个或多个客户端 ID。用来扮演角色的 OIDC 令牌中的 aud 字段值必须满足该限制条件要求，角色才允许被扮演。

oidc:sub：OIDC 主体（Subject），选填。该限定条件可以使用任何 string 类的条件操作类型，且条件值最多可以设置10个 OIDC 主体。用来扮演角色的 OIDC 令牌中的 sub 字段值必须满足该限制条件要求时，角色才允许被扮演。

7. 单击**下一步**。
8. 在配置角色策略页面，为角色关联权限策略，并单击**下一步**。
9. 在审阅页面，输入角色名称和角色描述（选填），并单击**完成**保存。

三、在身份提供商签发 OIDC Token

腾讯云不支持使用 OIDC 登录控制台，需要使用程序访问的方式完成 OIDC SSO 流程（即通过调用 API 获取临时秘钥，再使用临时秘钥访问腾讯云）。由于生成 OIDC Token 本质上是个 OAuth 流程，所以需要通过标准的 OAuth 2.0流程从 OIDC 身份提供商（例如：Okta）获取OIDC Token，具体方式参见提供商的相关文档。

四、使用 OIDC Token 换取 STS Token

从身份提供商处获取到 OIDC Token 后，可以直接调用 AssumeRoleWithWebIdentity API 以换取可以访问腾讯云的 STS Token。

请求示例：

```
POST / HTTP/1.1
Host: sts.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: AssumeRoleWithWebIdentity
<公共请求参数>

{
    "DurationSeconds": "5000",
    "RoleSessionName": "test_OIDC",
    "WebIdentityToken": "eyJraWQiOiJkT**********CNOQ",
    "RoleArn": "qcs::cam::uin/798950673:roleName/OneLogin-Role",
    "ProviderId": "OIDC"
}
```

返回示例：

```
{
  "Response": {
    "ExpiredTime": 1543914376,
    "Expiration": "2018-12-04T09:06:16Z",
    "Credentials": {
      "Token": "1siMD5r0tPAq9xpR******6a1ad76f09a0069002923def8aFw7tUMd2nH",
```

```
        "TmpSecretId": "AKID65zyIP0mp****qt2SlWIQVMn1umNH58",
        "TmpSecretKey": "q95K84wrzuE****y39zg52boxvp71yoh"
      },
      "RequestId": "f6e7cbcb-add1-47bd-9097-d08cf8f3a919"
    }
}
```

五、使用 STS Token 访问腾讯云资源

使用从上述步骤中换取的临时秘钥（STS Token）访问有权限的腾讯云资源。

策略

相关概念

最近更新时间：2024-01-23 17:54:33

权限是描述在某些条件下允许或拒绝执行某些操作访问某些资源。

默认情况下，主账号是资源的拥有者，拥有其名下所有资源的访问权限；子账号没有任何资源的访问权限；资源创建者不自动拥有所创建资源的访问权限，需要资源拥有者进行授权。

策略是定义和描述一条或多条权限的语法规范。CAM 支持两种类型的策略，预设策略和自定义策略。预设策略是由腾讯云创建和管理的一些常见的权限集合，如超级管理员、云资源管理员等，这类策略只读不可写。自定义策略是由用户创建的更精细化的描述对资源管理的权限集合。预设策略不能具体描述某个资源，粒度较粗，而自定义策略可以灵活的满足用户的差异化权限管理需求。

通过给用户或者用户组绑定一个或多个策略完成授权。被授权的策略既可以是预设策略也可以是自定义策略。

相关定义

策略

最近更新时间：2024-01-23 17:54:33

策略是用于定义和描述一条或多条权限的语法规范。腾讯云的策略类型分为预设策略和自定义策略。CAM 从不同角度切入，为您提供了多种方法来创建和管理策略。若您需要向 CAM 用户或组添加权限，您可以直接关联预设策略，或创建自定义策略后将自定义策略关联到 CAM 用户或组。每个策略允许包含多个权限，同时您可以将多个策略附加到一个 CAM 用户或组。

预设策略

预设策略由腾讯云创建和管理，是被用户高频使用的一些常见权限集合，如超级管理员、资源全读写权限等。操作对象范围广，操作粒度粗。预设策略为系统预设，不可被用户编辑。

自定义策略

由用户创建的更精细化的描述对资源管理的权限集合，允许作细粒度的权限划分，可以灵活的满足用户的差异化权限管理需求。例如，为某数据库管理员关联一条策略，使其有权管理云数据库实例，而无权管理云服务器实例。

授权指南
通过策略生成器创建自定义策略

最近更新时间：2024-09-29 16:19:33

操作场景

本文档介绍如何通过不同的创建方式创建自定义策略，自定义策略允许作细粒度的权限划分，可以灵活满足用户的差异化权限管理需求。

操作步骤

按策略生成器创建

按策略生成器创建的策略，通过从策略向导中选择服务和操作，并定义资源，自动生成策略语法，简单灵活，优先推荐使用。

1. 在访问管理控制台的 策略 页面，单击左上角的**新建自定义策略**。
2. 在弹出的选择创建方式窗口中，单击**按策略生成器创建**，进入编辑策略页面。
3. 在“可视化策略生成器”中选择服务的页面，补充以下信息，编辑一个授权声明。（您也可以选择 JSON，使用策略语法方式编辑策略，授权效果同“可视化策略生成器”）

效果（必选）：选择允许或拒绝。
服务（必选）：选择要授权的产品。
操作（必选）：选择您要授权的操作。
资源（必填）：选择全部资源或您要授权的特定资源。
授权粒度为操作级、服务级的云产品不支持填写具体资源六段式，选择全部资源即可。
授权粒度为资源级的云产品，可选择特定资源，资源描述方式请参阅 支持 CAM 的产品 中对应产品的「访问管理指南」文档。云产品支持的授权粒度请参阅 支持 CAM 的产品 中的「授权粒度」。
条件（选填）：设置上述授权的生效条件。详细可参阅 生效条件。

说明：

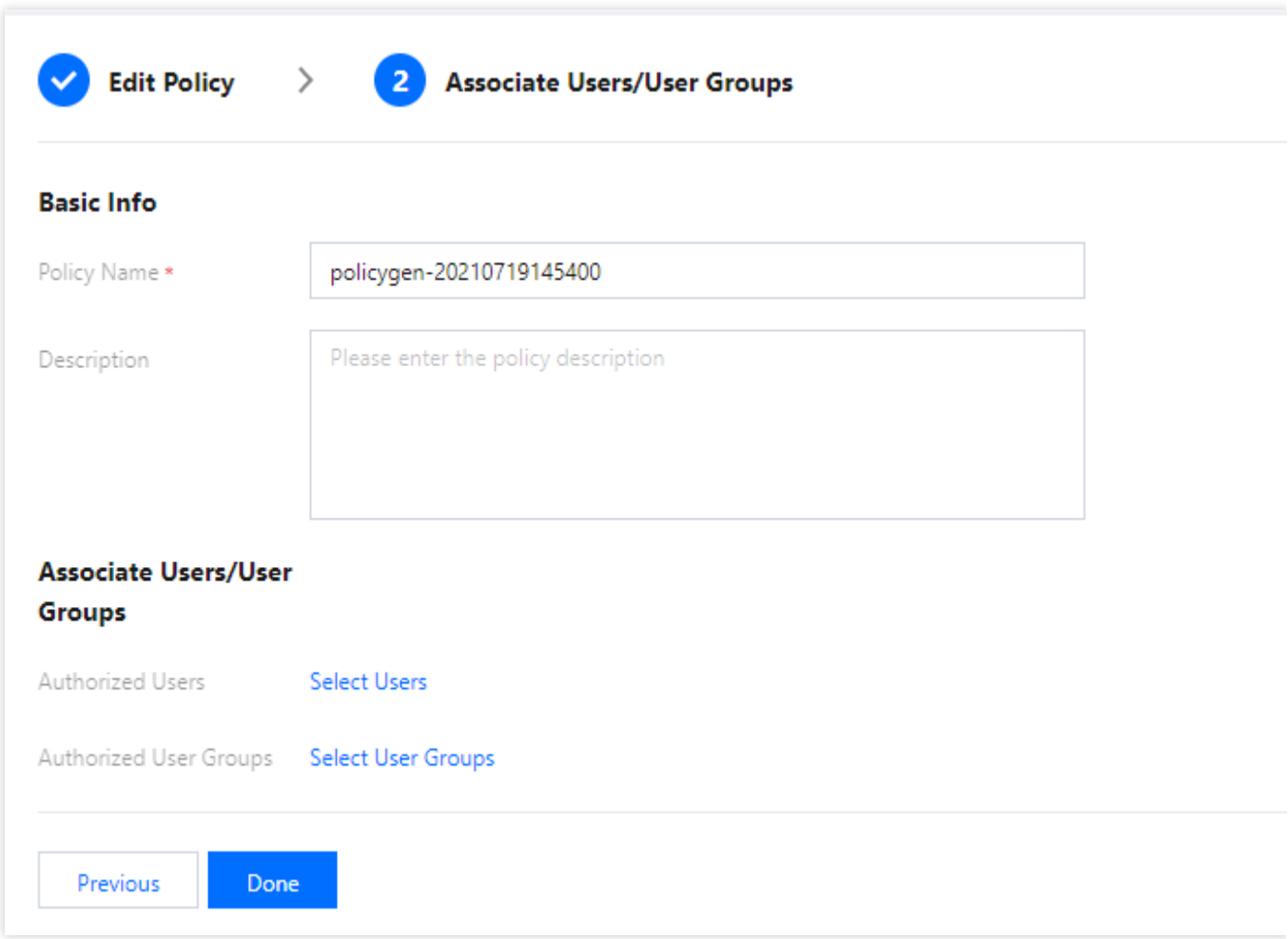
若要支持多个服务的手段，可单击**添加权限**，继续添加多个授权声明，对另外的服务进行授权策略配置。
一条策略中可以添加多条声明。

4. 完成策略授权声明编辑后，单击**下一步**，进入基本信息和关联用户/用户组页面。
5. 在关联用户/用户组页面，补充策略名称和描述信息，可同时关联用户或用户组快速授权。

说明：

策略名称由控制台自动生成，默认为 "policygen" ，后缀数字根据创建日期生成。您可进行自定义。

6. 单击**完成**，完成按策略生成器创建自定义策略的操作。


Edit Policy
2
Associate Users/User Groups
Basic Info
Policy Name *
policygen-20210719145400
Description
Please enter the policy description
Associate Users/User Groups
Authorized Users
Select Users
Authorized User Groups
Select User Groups
Previous
Done

通过标签授权创建自定义策略

最近更新时间：2024-01-23 17:54:33

操作场景

本文档介绍如何通过标签授权创建自定义策略，策略生成后该策略将具有一类标签属性资源的权限。策略的相关定义，请参见 相关概念。

操作步骤

1. 在访问管理控制台的 策略 页面，单击左上角的**新建自定义策略**。
2. 在弹出的选择创建方式窗口中，单击**按标签授权**，进入按标签授权页面。
3. 在“可视化策略生成器”中添加服务与操作栏，补充以下信息，编辑一个授权声明。

服务（必选）：选择要授权的产品。

操作（必选）：选择您要授权的操作。

说明

操作中包含该服务所有接口，您可以通过“**是否支持按标签授权**”筛选查看接口是否支持按标签授权。

是：支持按标签授权接口，将包含关联对应标签资源的操作权限。

否：不支持按标签授权接口，将包含所有资源的操作权限。

若要支持多个服务的授权，可单击左上角“添加”，继续添加多个授权声明，对另外的服务进行授权策略配置。

一条策略中可以添加多条声明。

4. 在选择标签栏，选择需要授权的标签信息，可添加多个标签，单击**下一步**，进入关联用户/用户组/角色页面。

5. 关联用户/用户组/角色页面补充策略名称和描述信息，可同时关联用户/用户组/角色快速授权。

说明

策略名称由控制台自动生成，默认为 "policygen" ，后缀数字根据创建日期生成。您可进行自定义。

6. 单击**完成**，完成按策略生成器创建自定义策略的操作。


编辑策略
2
关联用户/用户组/角色
基本信息
策略名称 *
policygen-20221227154847
描述
请输入策略描述
关联用户/用户组/角色
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

后续操作

授权管理

通过策略语法创建自定义策略

最近更新时间：2024-01-23 17:54:33

操作场景

本文档介绍如何通过策略语法创建自定义策略，该方式由用户编写策略语法，生成对应的策略，权限粒度灵活，可以解决对权限精细划分有较高要求的用户诉求。策略的相关定义，请参见 相关概念。

操作步骤

1. 在访问管理控制台的 策略 页面，单击左上角的**新建自定义策略**。
2. 在弹出的选择创建方式窗口中，单击**按策略语法创建**，进入选择策略模板页面。
3. 选择策略模板页面，可输入关键字进行搜索。例如：模板类型为全部模板，关键字为 a，选择 AdministratorAccess 模板。
4. 单击**下一步**，进入**编辑策略**页面。
5. 在编辑策略页面，确认策略名称、策略内容后单击**完成**，完成按策略语法创建自定义策略操作。其中默认的策略名称和策略内容由控制台自动生成，策略名称默认为 **policygen**，后缀数字根据创建日期生成。


选择策略模板
2
编辑策略
策略名称 *
policygen-20210602112042
描述
策略内容 使用旧版
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": "*",
"resource": "*"
}
]
}

后续操作

授权管理

授权管理

最近更新时间：2024-01-23 17:54:33

操作场景

创建用户/用户组时，默认没有任何权限，您可以通过为其关联策略，使用户/用户组获得对应的操作权限。

前提条件

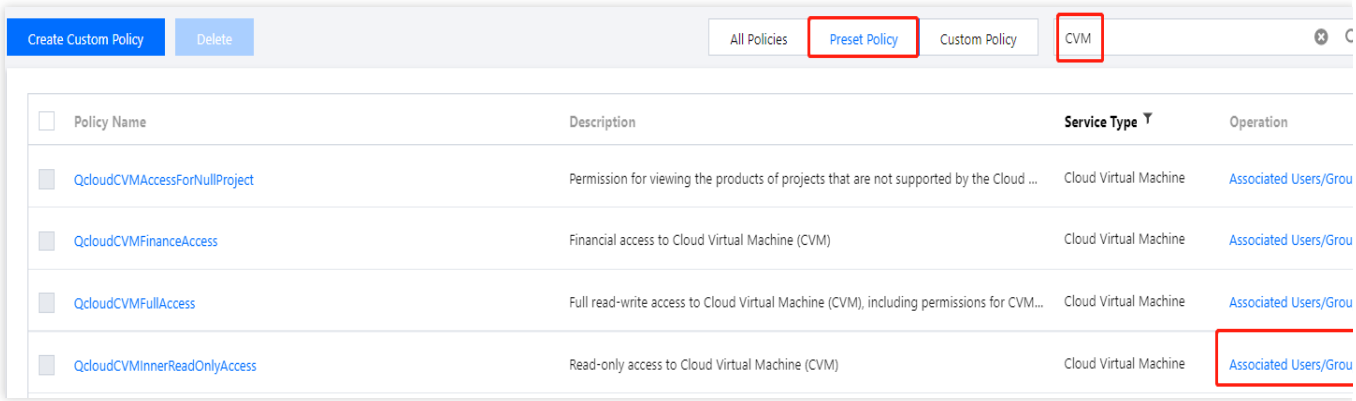
已 创建子用户 / 用户组。
如果需要关联自定义策略，请先 创建自定义策略。

操作步骤

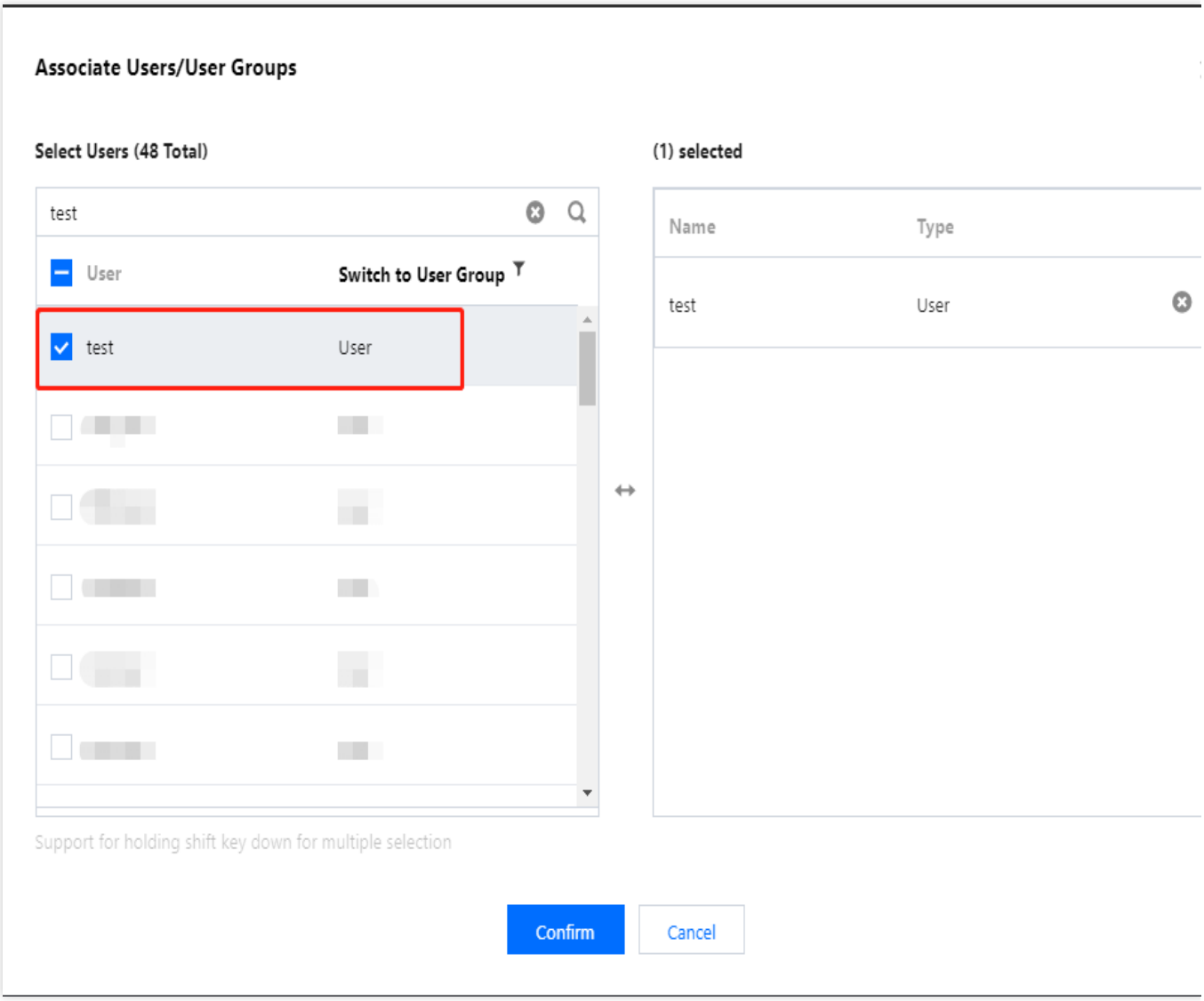
您可以通过策略关联用户/用户组，或者通过用户/用户组关联策略，两种方式操作入口有区别，实现的功能无区别。

通过策略关联用户/用户组

通过策略关联用户
通过策略关联用户组
1. 在访问管理控制台的 策略 页面，选择策略类型。
说明：
本示例以**预设策略**为例，您也可以选择**自定义策略**。
2. 通过搜索筛选需要授权的预设策略，单击操作列的**关联用户/组**。



3. 在弹出的关联用户/用户组窗口，勾选要关联的用户，单击**确定**，完成通过策略关联用户操作。

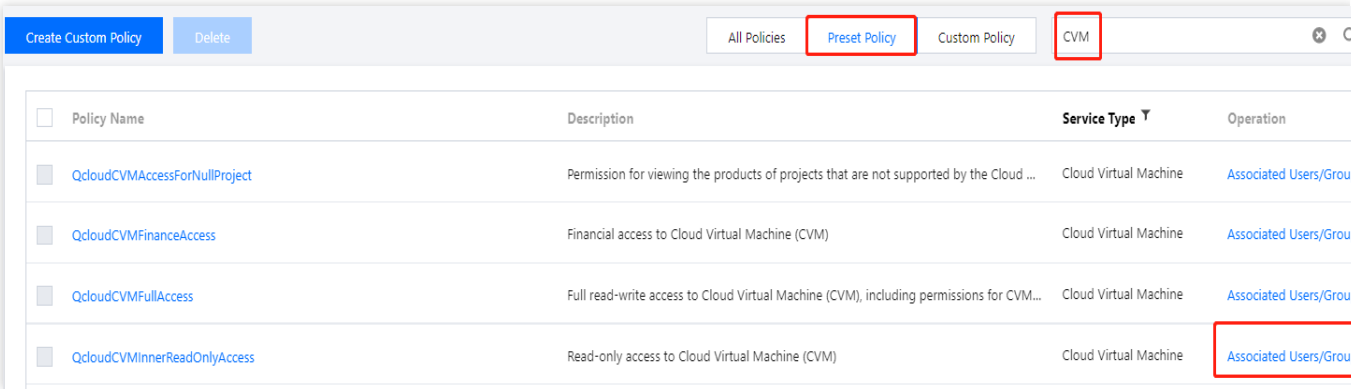


1. 在访问管理控制台的 策略 页面，选择策略类型。

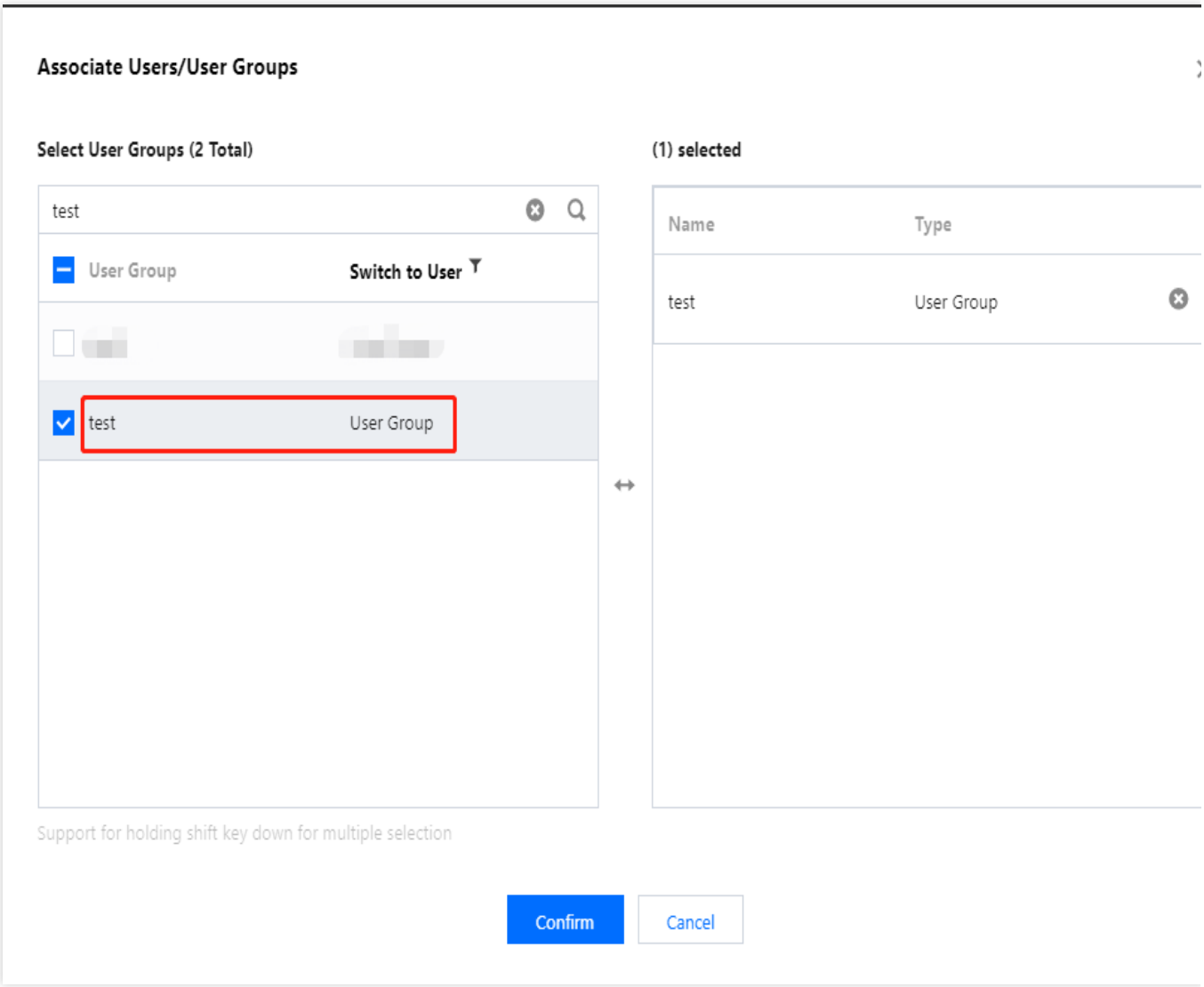
说明

本示例以**预设策略**为例，您也可以选择**自定义策略**。

2. 通过搜索筛选需要授权的预设策略，单击操作列的**关联用户/组**。



3. 在弹出的关联用户/用户组窗口，单击**切换用户组**。
4. 勾选要关联的用户组，单击**确定**，完成通过策略关联用户组操作。

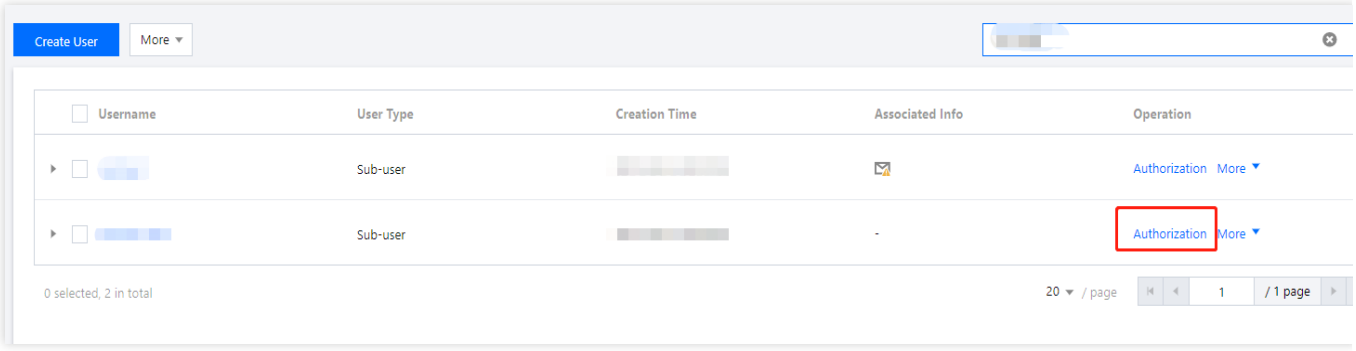


通过用户/用户组关联策略

通过用户关联策略

通过用户组关联策略

1. 在访问管理控制台的【用户】>【用户列表】页面，找到需要授权的用户，单击操作列的【授权】，进入关联策略页面。

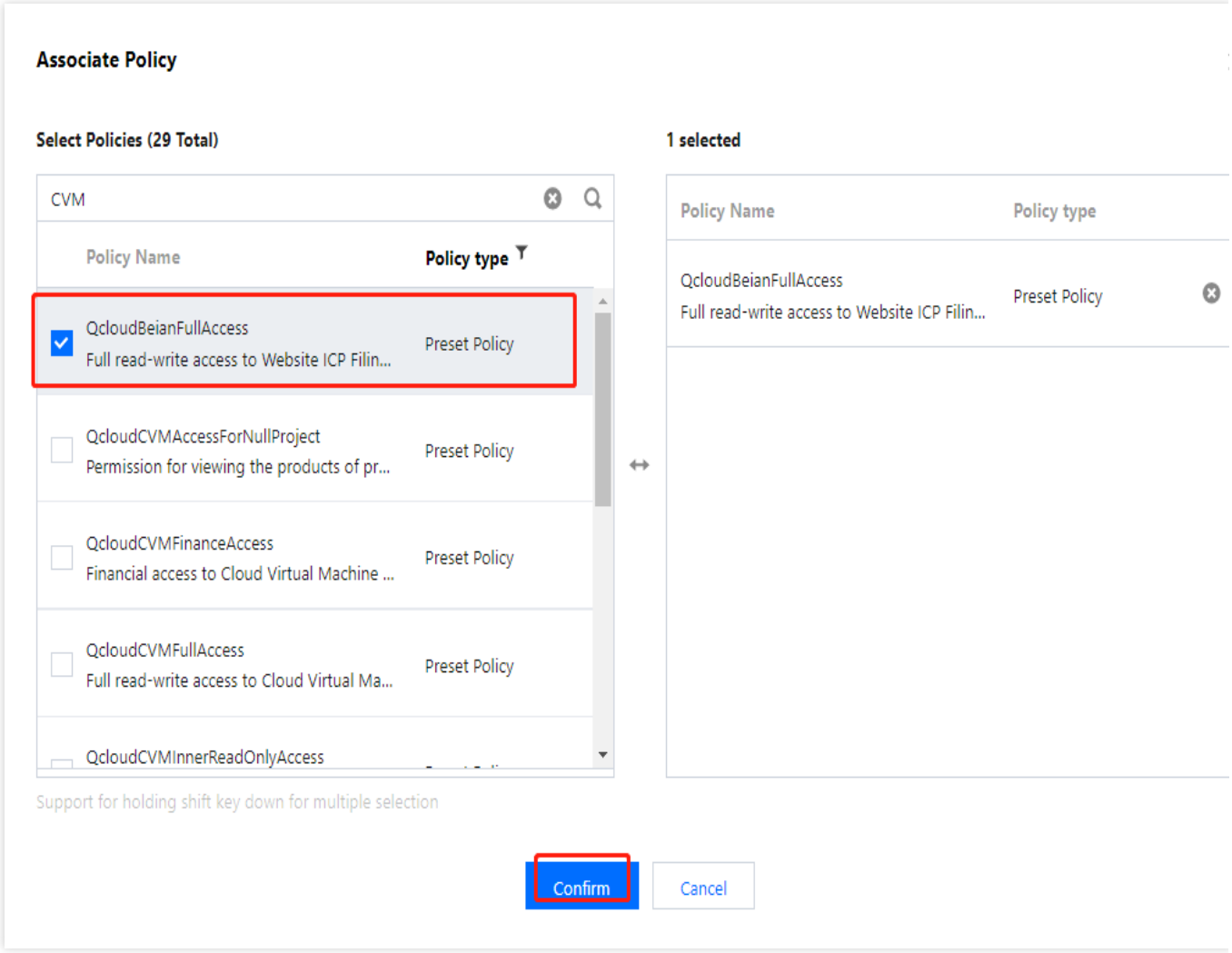


2. 在关联策略页面，选择策略类型。

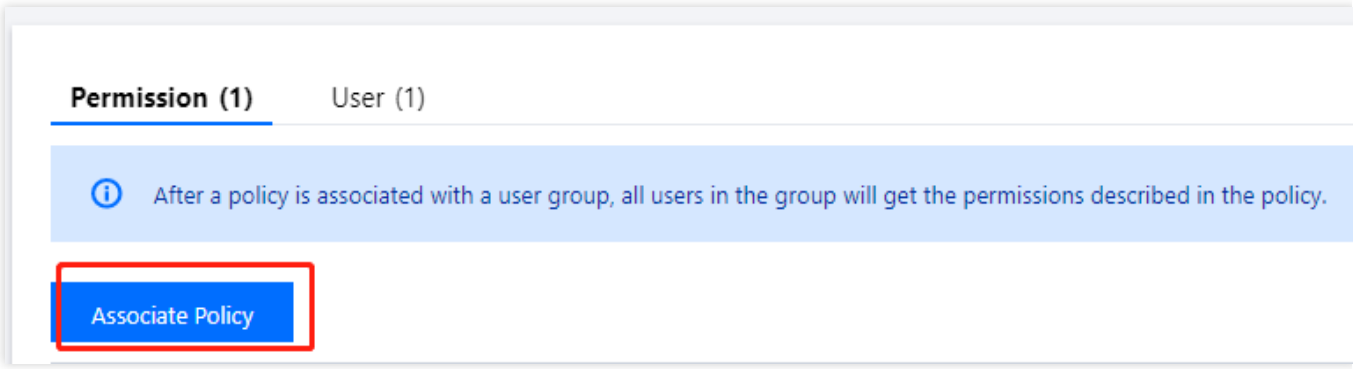
说明

默认展示全部策略，您可以筛选自定义策略或预设策略，方便查找具体的策略信息。

3. 勾选需要授权的策略，单击**确定**，完成通过用户关联预设策略操作。



1. 在访问管理控制台的 用户组 页面，单击目标用户组名称，进入用户组详情页。
2. 在用户组详情页，单击**关联策略**，进入关联策略页面。

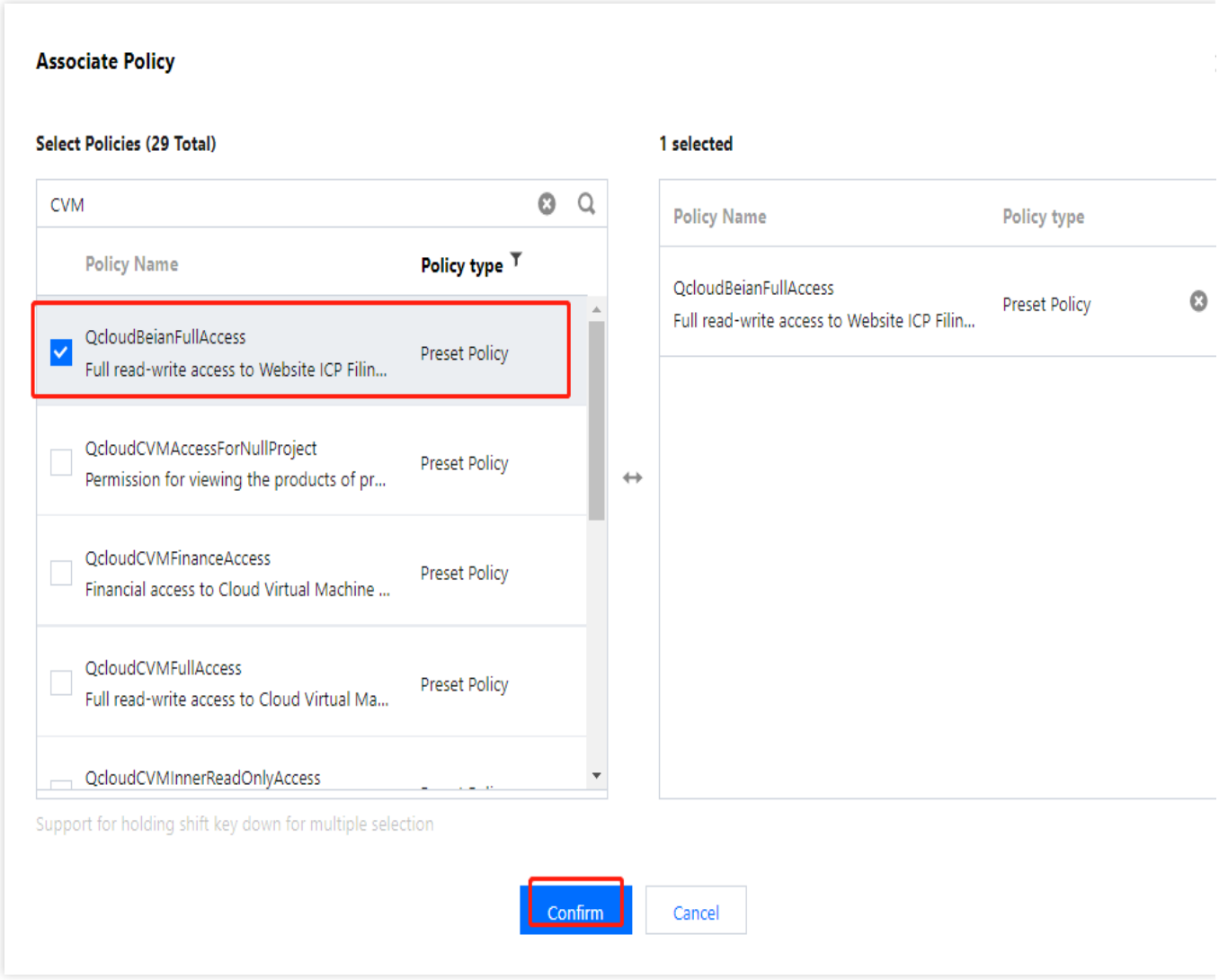


3. 在关联策略页面，选择策略类型。

说明

默认展示全部策略，您可以筛选自定义策略或预设策略，方便查找具体的策略信息。

4. 勾选需要授权的策略，单击**确定**，完成通过用户关联预设策略操作。



关联文档

如果您想了解策略概念，请参阅 策略相关定义。

限制 IP 访问

最近更新时间：2024-01-23 17:54:33

操作场景

本文档介绍如何通过自定义策略限制子账号访问 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。

前提条件

需要设置的产品支持按 IP 限制业务访问，详细可参考 常见问题。

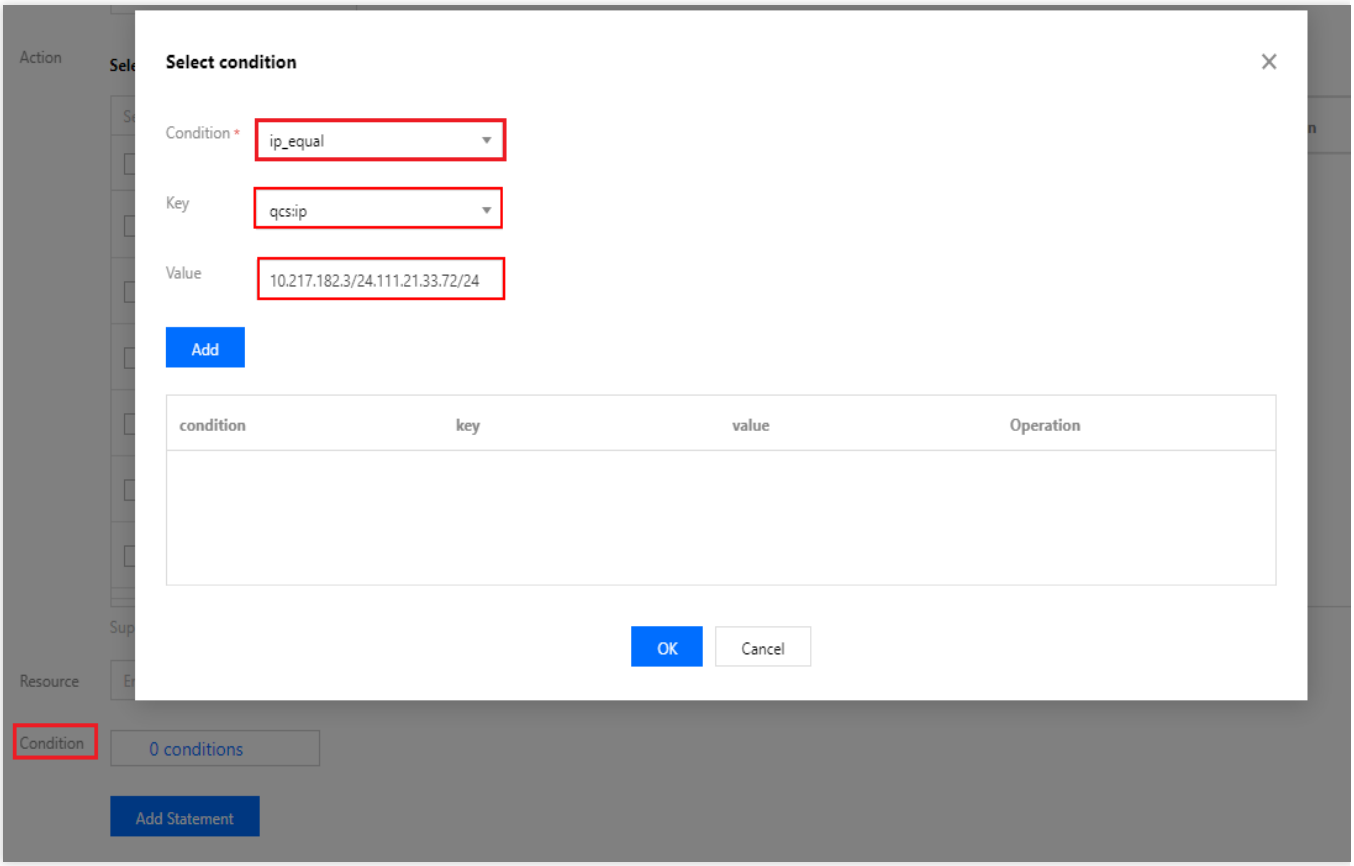
操作步骤

1. 进入 策略 管理页面，单击左上角的**新建自定义策略**。
2. 在弹出的选择创建方式窗口中，单击**按策略生成器创建**，进入选择服务和操作页面。
3. 在选择服务和操作页面，补充以下信息。

效果：必填项，选择 "允许"。如选择 "拒绝"，用户或用户组不能获取授权。
服务：必填项，选择需要添加的产品。
操作：必填项，根据您的需求勾选产品权限。
资源：必填项，您可以参考 资源描述方式 填写。
条件：根据您的需求选择条件，输入 IP 地址。可以添加多条限制。例如，效果选择"允许"，仅限使用该 IP 地址的用户或组获取授权。

使用示例

以下示例表示用户必须在 10.217.182.3/24 或者 111.21.33.72/24 网段才能调用云 API 访问 cos:PutObject，如下图：



策略语法如下：

```
{
 "version": "2.0",
 "statement": [
 {
     "effect": "allow",
     "action": "cos:PutObject",
     "resource": "*",
     "condition": {
         "ip_equal": {
             "qcs:ip": [
                 "10.217.182.3/24",
                 "111.21.33.72/24"
             ]
         }
     }
 }
 ]
}
```

语法逻辑
元素参考
元素参考概述

最近更新时间：2024-06-27 16:15:11

策略（policy）由若干元素构成，用来描述授权的具体信息。核心元素包括委托人（principal）、操作（action）、资源（resource）、生效条件（condition）以及效力（effect）。元素保留字仅支持小写。它们在描述上没有顺序要求。对于策略没有特定条件约束的情况，condition 元素是可选项。在控制台中不允许写入 principal 元素，仅支持在策略管理 API 中和策略语法相关的参数中使用 principal。

1. 版本（version）

描述策略语法版本。该元素是必填项。目前仅允许值为“2.0”。

2. 委托人（principal）

描述策略授权的实体。包括用户（主账号、子账号），未来会包括角色、联合身份用户等更多实体。仅支持在角色的信任策略和cos的存储桶策略中使用该元素。

3. 语句（statement）

描述一条或多条权限的详细信息。该元素包括 action、resource、condition、effect 等多个其他元素的权限或权限集合。一条策略有且仅有一个 statement 元素。

4. 操作（action）

描述允许或拒绝的操作。操作可以是 API（以 name 前缀描述）或者功能集（一组特定的 API，以 actionName 前缀描述）。该元素是必填项。

5. 资源（resource）

描述授权的具体数据。资源是用六段式描述。每款产品的资源定义详情会有所区别。有关如何指定资源的信息，请参阅您编写的资源声明所对应的产品文档。该元素是必填项。

6. 生效条件（condition）

描述策略生效的约束条件。条件包括操作符、操作键和操作值组成。条件值可包括时间、IP 地址等信息。有些服务允许您在条件中指定其他值。该元素是非必填项。

7. 效力（effect）

描述声明产生的结果是“允许”还是“显式拒绝”。包括 allow（允许）和 deny （显式拒绝）两种情况。该元素是必填项。

8. 策略样例

该样例描述为：允许属于主账号 APPID 1238423下的子账号 ID 3232523， 对北京地域的 cos 存储桶 bucketA 和广州地域的 cos 存储桶 bucketB 下的对象 object2，在访问 IP 为10.121.2.*网段时，拥有所有 cos 读 API 的权限以及写对象的权限，以及可以发送消息队列的权限。

```
{
  "version": "2.0",
  "statement": [
    {
      "principal": {
        "qcs": [
          "qcs::cam::uin/1238423:uin/3232523"
        ]
      },
      "effect": "allow",
      "action": [
        "cos:PutObject",
        "cos:GetObject",
        "cos:HeadObject",
        "cos:OptionsObject",
        "cos:ListParts",
        "cos:GetObjectTagging"
      ],
      "resource": [
        "qcs::cos:ap-beijing:uid/1238423:bucketA-1238423/*",
        "qcs::cos:ap-guangzhou:uid/1238423:bucketB-1238423/object2"
      ],
      "condition": {
        "ip_equal": {
          "qcs:ip": "10.121.2.10/24"
        }
      }
    },
    {
      "principal": {
        "qcs": [
          "qcs::cam::uin/1238423:uin/3232523"
        ]
      },
      "effect": "allow",
      "action": "cmqqueue:SendMessage",
      "resource": "*"
    }
  ]
}
```

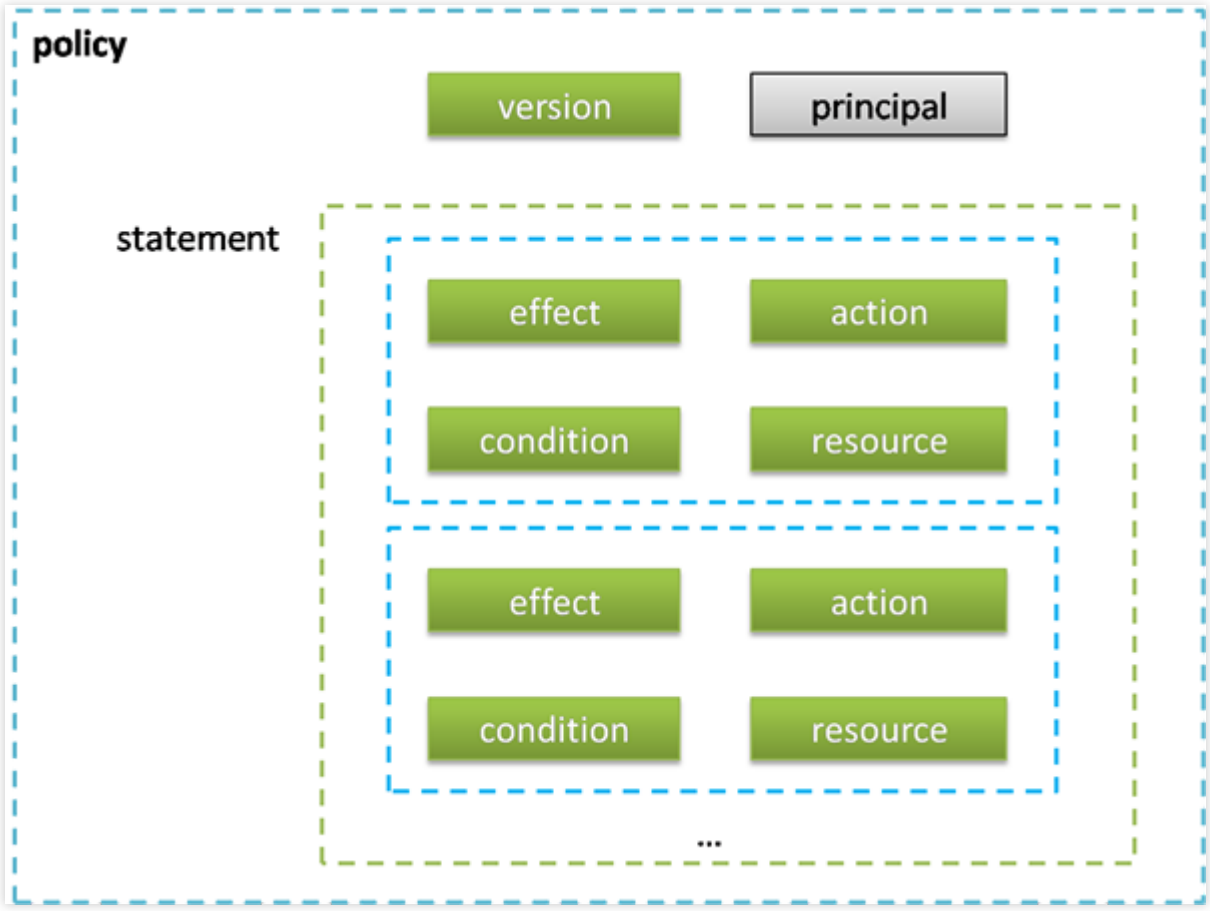
关联文档

如果您想了解 CAM 资源（resource）描述信息请参阅 资源描述方式。

语法结构

最近更新时间：2024-01-23 17:54:33

整个策略的语法结构如下图所示。策略 policy 由版本 version 和语句 statement 构成，还可以包含委托人信息 principal，委托人仅限于策略管理 API 中策略语法相关的参数中使用。
语句 statement 是由若干个子语句构成。每条子语句包括操作 action、资源 resource、生效条件 condition 以及效力 effect 四个元素，其中 condition 是非必填项。



JSON 格式

策略语法以 JSON 格式为基础。创建或更新的策略不满足 JSON 格式时，将无法提交成功，所以用户必须要确保 JSON 格式正确。 JSON 格式标准在 RFC7159 中定义，您也可以使用在线 JSON 验证程序检查策略格式。

语法约定

语法描述中有如下约定：
以下字符是包含在策略语法中的 JSON 字符：

```
{ } [ ] " , :
```

以下字符是用于描述策略语法中的特殊字符，不包含在策略中：

```
= < > ( ) |
```

当一个元素允许多个值时，使用逗号分隔符和省略号进行表示。例如：

```
[<resource_string>, < resource_string>, ...]
<principal_map> = { <principal_map_entry>, <principal_map_entry>, ... }
```

允许多个值时，也可以只包含一个值。当元素只有一个值时，尾部的逗号必须去掉，且中括号"[]"标记可选。例如：

```
"resource": [<resource_string>]
"resource": <resource_string>
```

元素后的问号 (?) 表示该元素是非必填项。例如：

```
<condition_block?>
```

元素是枚举值的情况下，枚举值之间用竖线 "|" 表示，并用 "()" 括号定义枚举值的范围。例如：

```
("allow" | "deny")
```

字符串元素用双引号包括起来。例如：

```
<version_block> = "version" : "2.0"
```

语法描述

```
policy  = {
     <version_block>
     <principal_block?>,
     <statement_block>
}

<version_block> = "version" : "2.0"

<statement_block> = "statement" : [ <statement>, <statement>, ... ]

<statement> = {
    <effect_block>,
    <action_block>,
    <resource_block>,
    <condition_block?>
}

<effect_block> = "effect" : ("allow" | "deny")
```

```
<principal_block> = "principal": ("*" | <principal_map>)

<principal_map> = { <principal_map_entry>, <principal_map_entry>, ... }

<principal_map_entry> = "qcs":
    [<principal_id_string>, <principal_id_string>, ...]

<action_block> = "action":
    ("*" | [<action_string>, <action_string>, ...])

<resource_block> = "resource":
    ("*" | [<resource_string>, <resource_string>, ...])

<condition_block> = "condition" : { <condition_map> }
<condition_map> {
  <condition_type_string> : { <condition_key_string> : <condition_value_list>
},
  <condition_type_string> : { <condition_key_string> : <condition_value_list>
}, ...
}
<condition_value_list> = [<condition_value>, <condition_value>, ...]
<condition_value> = ("string" | "number")
```

语法说明：

一个策略 policy 可以包含多条语句 statement。

策略的最大长度是 6144 个字符（不包含空格），具体信息请参阅 限制。

各个块 block 的显示顺序无限制。例如，在策略中， version_block 可以跟在 effect_block 后面等。

当前支持的语法版本为 2.0。

principal_block 元素在控制台中不允许写入，仅支持在策略管理 API 中和策略语法相关的参数中使用 principal 。

操作 action 和资源 resource 都支持列表。

生效条件可以是单个条件，或者包括多个子条件块的逻辑组合。每个生效条件包括条件操作符 condition_type、条件键 condition_key，条件值 condition_value。

每条语句 statement 的效力 effect 为 deny 或 allow 。当策略中包含的语句中既包含有 allow 又包含有 deny 时，遵循 deny 优先原则。

字符串说明

语法描述的元素字符串说明如下：

action_string

由描述作用域、服务类型和操作名称组成。

```
//所有产品所有操作
"action":"*"
"action":"*:*"
```

```
// COS 产品所有操作
"action":"cos:*"
// COS 产品的名为 GetBucketPolicy 的操作
"action":"cos:GetBucketPolicy"
// COS 产品部分匹配 Bucket 的操作
"action":"cos:*Bucket*"
// cos 产品，名为 GetBucketPolicy\\PutBucketPolicy\\DeleteBucketPolicy 的操作列表
"action":["cos:GetBucketPolicy","cos:PutBucketPolicy","cos:
DeleteBucketPolicy"]
```

resource_string

资源通过六段式描述。

```
qcs: project :serviceType:region:account:resource
```

示例如下所示：

```
// COS 产品的 object 资源，上海地域，资源拥有者的 uid 是10001234，资源名是
bucket1/object2
qcs::cos:sh:uid/10001234:prefix//10001234/bucket1/object2
// CMQ 产品的队列，上海地域，资源拥有者的 uin 是12345678，资源名是12345678/queueName1，
资源前缀是 queueName
qcs::cmqqueue:sh:uin/12345678:queueName/12345678/queueName1
// CVM 产品的云服务器，上海地域，资源拥有者的 uin 是12345678，资源名是 ins-abcdefg,资源
前缀是 instance
qcs::cvm:sh:uin/12345678:instance/ins-abcdefg
```

如果您想了解各个产品对应的资源定义详情，请参阅 支持CAM 的产品 中对应产品的参考文档。

condition_type_string

条件操作符，描述测试条件的类型。例如 string_equal、string_not_equal、date_equal、date_not_equal、ip_equal、ip_not_equal、numeric_equal、numeric_not_equal 等。示例如下所示:

```
"condition":{
         "string_equal":{"cvm:region":["sh","gz"]},
         "ip_equal":{"qcs:ip":"10.131.12.12/24"}
}
```

condition_key_string

条件键，表示将对其值采用条件操作符进行操作，以便确定条件是否满足。CAM 定义了一组在所有产品中都可以使用的条件键，包括 qcs:current_time、qcs:ip 、qcs:uin 和 qcs:owner_uin 等。具体信息请参阅 生效条件。

principal_id_string

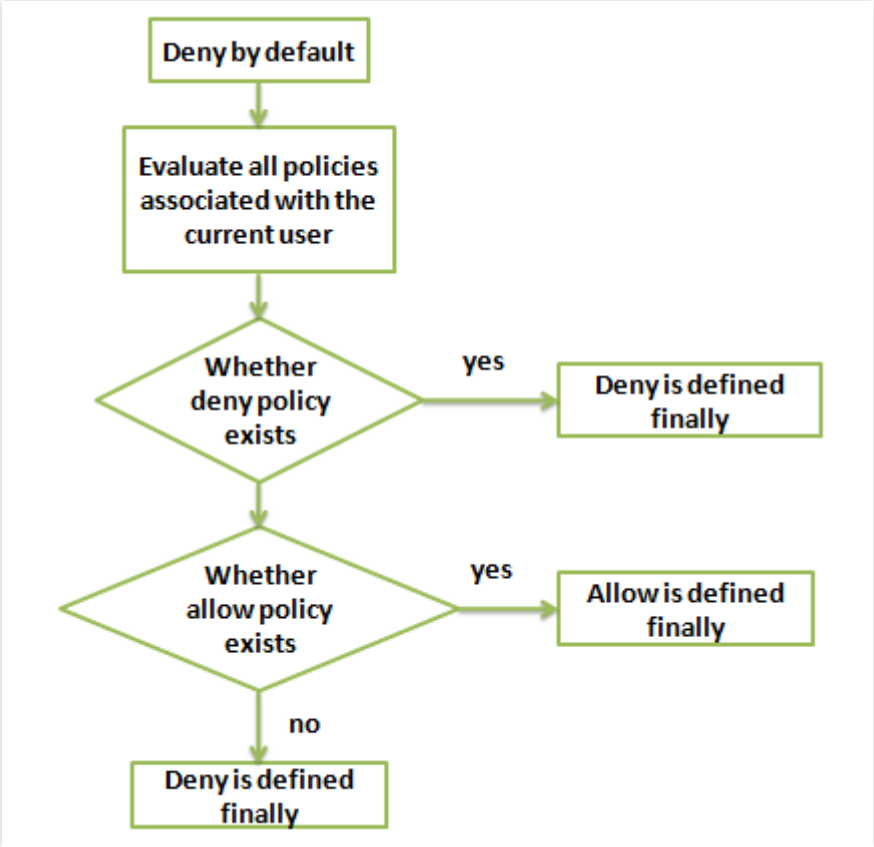
对于 CAM 而言，用户也是它的资源。因此委托人 principal 也采用六段式描述。示例如下，具体信息请参阅 资源描述方式。

```
"principal":   {"qcs":["qcs::cam::uin/1238423:uin/3232",
             "qcs::cam::uin/1238423:groupid/13"]}
```

评估逻辑

最近更新时间：2024-12-16 17:25:30

腾讯云用户访问云资源时， CAM 通过以下评估逻辑决定允许或拒绝。



1. 默认情况下，所有请求都将被拒绝。
2. CAM 会检查当前用户关联的所有策略。
2.1 判断是否匹配策略，是则进行下一步判断；否则最终判断为 deny ，不允许访问云资源。
2.2 判断是否有匹配 deny 策略，是则最终判定为 deny ，不允许访问云资源；否则进行下一步判断。
2.3 判断是否有匹配 allow 策略，是则最终判断为 allow ，允许访问云资源；否则最终判定为 deny，不允许访问云资源。

注意：

对于主账号，默认拥有其名下所有资源的访问权限；且目前仅 COS/CAS 产品支持跨账号的资源访问。
有些通用策略，会默认关联所有 CAM 用户。具体请见下文的 通用策略表。
其他策略都必须显式指定，包括 allow 和 deny 策略。
对于支持跨账号资源访问的业务，存在权限传递的场景，即主账号 A 授权主账号 B 下的某个子账号对其资源的访问权限。这个时候 CAM 会同时校验 A 是否授权给 B 该权限以及 B 是否授权给子帐号该权限，两者同时满足的前提下， B 的子账号才有权访问 A 的资源。

目前支持的
通用策略表如下：

策略说明	策略定义

查询密钥需要 MFA 验证	{
	"principal":"*",
	"*action":"account:QueryKeyBySecretId",*
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

设置敏感操作需要 MFA 验证	{
	"principal":"*",
	"action":"account:SetSafeAuthFlag",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

绑定 token 需要 MFA 验证	{
	"principal":"*",
	"action":"account:BindToken",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

解绑 token 需要 MFA 验证	{
	"principal":"*",
	"action":"account:UnbindToken",
	"resource":"",
	condition":{"string_equal":{"mfa":"0"}}
	}

修改邮箱需要 MFA 验证	{
	"principal":"*",
	"action":"account:ModifyMail",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

修改手机号需要 MFA 验证	{
	"principal":"*",
	"action":"account:ModifyPhoneNum",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

资源描述方式

最近更新时间：2024-12-16 17:25:30

资源（resource）元素描述一个或多个操作对象，如 CVM 资源、COS 存储桶等。本文档主要介绍 CAM 的资源描述信息。

所有资源定义

资源（resource）为 `*` 时代表所有资源，即可授予操作 action 的所有资源的操作权限。
若所授权云服务授权粒度为服务级或所授权服务的操作 action 支持粒度为 接口级时，资源（resource）需填 *，即授予该云服务或该服务操作 action 的所有资源权限。

单个或多个资源定义

授予单个或多个资源权限时可采用下述的六段式描述方式，每种产品都拥有其各自的资源和对应的资源定义详情。
六段式定义方式如下所示：

```
qcs:project_id:service_type:region:account:resource
```

资源六段式包含以下六个字段，详细含义及示例如下：

字段名称	含义及取值	是否必填	示例
qcs	qcloud service 的简称，表示是腾讯云的云资源。	是	qcs
project_id	描述项目信息，仅兼容 CAM 早期逻辑，当前策略语法禁止填写该信息，置空即可。	否	置空
service_type	描述产品简称，详细可查看 支持 CAM 的产品 中的“CAM 中简称”。 值为空时表示所有产品。	否	云服务器为 cvm 内容分发网络为 cdn
region	描述地域信息，地域命名方式请参考 地域列表； 值为空的时候表示所有地域。	否	华北地区(北京)为 ap-beijing 华南地区(广州)为 ap-guangzhou
account	描述资源拥有者的主账号信息，目前支持两种方式描述资源拥有者，uin 和 uid 方式。uin 方式，即主账号的账户ID，表示为 `uin/${uin}` 。	否	uin 如：uin/12345678 uid 如：uid/10001234

	uid 方式，即主账号的 APPID，表示为 `uid/${appid}`，仅 COS 和 CAS 业务的资源拥有者使用该方式描述。 值为空的时候表示创建策略的 CAM 用户所属的主账号。		
resource	描述各产品的具体资源详情，目前支持两种方式描述资源信息，`resource_type/${resourceid}` 和 `<resource_type>/<resource_path>`。 `resource_type/${resourceid}`：`resourcetype` 为资源前缀，描述资源类型；${resourceid} 为具体的资源 ID，可前往各个产品控制台查看，值为 `*` 时代表该类型资源的所有资源。 `<resource_type>/<resource_path>`：`resourcetype` 为资源前缀，描述资源类型。`<resource_path>` 为资源路径，该方式下，支持目录级的前缀匹配。	是	云服务器：instance/ins-1 云数据库 MySQL：instanceId/cdb-1 对象存储 COS：prefix//10001234/bucket1/* 表示 bucket1 下的所有文件。COS 资源（resource）支持多种类型，详情请参见 COS 授权策略使用指引。

CAM 的资源定义

CAM 包含了用户、组、策略等资源，CAM 资源的描述方式如下所示：

主账号：

```
qcs::cam::uin/164256472:uin/164256472
```

或

```
qcs::cam::uin/164256472:root
```

子账号：

```
qcs::cam::uin/164256472:uin/73829520
```

组：

```
qcs::cam::uin/164256472:groupid/2340
```

所有资源：

```
*
```

策略：

```
qcs::cam::uin/12345678:policyid/*
```

或

```
qcs::cam::uin/12345678:policyid/12423
```

资源的重要说明

资源的拥有者一定是主账号。如果资源是子账号创建的，在没有授权的情况下，不会自动拥有资源的访问权限，需要由资源拥有者授权。
COS、CAS 等业务支持跨账号授权资源的访问权限。被授权账号可以通过权限传递方式将资源授权给其子账号。

关联文档

如果您想了解各个产品对应的资源定义详情，请参阅 支持 CAM 的产品 中对应产品的参考文档。

策略变量

最近更新时间：2024-01-23 17:54:33

使用场景

场景假设：您希望给每个 CAM 用户授予其创建资源的访问权限。例如，您想要设置 COS 资源的创建者默认拥有该资源的访问权限。
如果由资源拥有者（主账号）将资源逐个授权给资源创建者，授权成本很高，需要为每种资源都编写策略并授权给创建者。在这种情况下，您可以通过使用策略变量来实现您的需求。在策略的资源定义中增加占位符描述创建人的子账号 uin，该占位符即是策略变量。当鉴权时，策略变量将被替换为来自请求本身的上下文信息。
授予创建者资源访问权限的策略描述方式如下：

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": "cmqqueue:*",
            "resource": "qcs::cmqqueue::uin/1000001:queueName/uin/${uin}/*"
        }
    ]
}
```

策略变量在每个资源的路径中带上创建人的子账号 uin。如子账号uin 为 125000000 的子账号（对应主账号 uin 是 1000001）创建了名为 queueName/uin/125000000 的成都地域 cmq 消息队列，则其对应的资源描述方式为

```
qcs::cmqqueue:ap-chengdu:uin/1000001:queueName/uin/125000000
```

子账号 uin 为 125000000 的子账号访问该资源时，鉴权过程中会把对应的策略信息的占位符替换为访问者，即

```
qcs::cmqqueue::uin/1000001:queueName/uin/125000000
```

策略中的资源 `qcs::cmqqueue::uin/1000001:queueName/uin/125000000` 可以通过前缀匹配访问资源 `qcs::cmqqueue:ap-chengdu:uin/1000001:queueName/uin/125000000` 。

策略变量的位置

资源元素位置 ：策略变量可以用在 资源六段式 的最后一段。
条件元素位置 ：策略变量可以用在条件值中。
以下策略表示 VPC 创建者拥有访问权限。

```
{
        "version":"2.0",
        "statement": [
         {
            "effect":"allow",
            "action":"name/vpc:*",
            "resource":"qcs::vpc::uin/12357:vpc/*",
            "condition":{"string_equal":{"qcs:create_uin":"${uin}"}}
         }
      ]
}
```

说明：

对象存储 COS 的资源六段式为 `qcs::cos:$region:uid/$appid:$bucketname-$appid/$ResourcesPath`，其中 $ResourcesPath 为具体的资源路径，且 $ResourcesPath 中不能使用上述策略变量，完整的 COS 存储桶 Bucket 的资源六段式如下：`qcs::cos:ap-guangzhou:uid/1250000000:examplebucket-1250000000/path_1/path_2/pic.jpeg`。

策略变量列表

目前支持的策略变量列表如下：

变量名	变量含义
${uin}	当前访问者的子账号 uin。对于访问者是主账号的情况，它和主账号 uin 一致。
${owner_uin}	当前访问者所属的主账号 uin。
${app_id}	当前访问者所属的主账号的 APPID。

生效条件

生效条件概述

最近更新时间：2024-01-23 17:54:33

在设置访问管理策略时，您可以指定策略生效的条件（Condition）。生效条件是可选的，设置后，当用户向腾讯云发出请求时，系统会使用请求上下文中的条件键和条件值与您在策略中指定的生效条件的条件键和条件值进行匹配，只有条件匹配成功，对应的权限策略才会生效。

生效条件构成

生效条件由一个或多个条件子句构成。一个条件子句由条件键、运算符和条件值组成，一个条件键可以指定一个或多个条件值。

`"condition" : { "{condition-operator}" : { "{condition-key}" : "{condition-value}" }}`

条件子句示例

请求 IP 为 `192.168.1.1` ，且请求日期小于2022-05-31 00:00:00，Condition 如下：

```
"condition":{
                "ip_equal": {
                    "qcs:ip": "192.168.1.1"
                },

                "date_less_than": {
                    "qcs:current_time": "2022-05-31 00:00:00"
                }
            }
```

生效条件匹配逻辑

生效条件的评估逻辑如下：

评估逻辑	说明
条件满足	一个条件键可以指定一个或多个条件值，在条件检查时，如果条件键的值与指定值中的某一个相同，即可判定条件满足。
条件子句满足	同一条件操作类型的条件子句下，若有多个条件键，则所有条件键必须同

	时满足，才能判定该条件子句满足。
条件块满足	条件块下的所有条件子句同时满足的情况下，才能判定该条件块满足。
条件运算符（null_equal 除外）加上后缀 if_exist	表示上下文信息中即便不包含对应的键值依然生效。
for_all_value	限定词搭配条件运算符使用，表示上下文信息中条件键的每个条件值都满足要求时才生效。
for_any_value	限定词搭配条件运算符使用，表示上下文信息中条件键的任意一个条件值满足要求时就可以生效。

说明

按标签授权仅支持 for_any_value。

生效条件示例

```
"condition":{
                "ip_equal": {
                    "qcs:ip": "192.168.1.1"
                }
            }
```

请求中的条件值由条件键表示，在此示例中为 qcs:ip。将上下文键值与您指定为文本值的值进行比较，例如 `192.168.1.1` 。要进行的比较类型由条件运算符指定（此处为 ip_equal）。

在某些情况下，需要匹配多种访问情况来满足实际需求，这时您可以在设置 Condition 时，指定多个条件值来匹配，例如：用户必须在 `10.217.182.3/24` 或者 `111.21.33.72/24` 网段才能上传对象（cos:PutObject），权限策略内容如下：

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "cos:PutObject"
            ],
            "resource": [
                "*"
            ],
            "condition":{
                "ip_equal": {
                    "qcs:ip": [
                        "10.217.182.3/24",
```

```
                        "111.21.33.72/24"
                    ]
                }
            }
        }
    ]
}
```

条件键和条件运算符

最近更新时间：2024-01-23 17:54:33

在通过 CAM 控制台的 策略生成器创建策略 时，您可以根据需要设置策略生效条件。

条件键

腾讯云通用条件键命名格式： `qcs:<condition-key>` ，当前只支持5种条件键，条件键的内容及描述如下：

通用条件键	类型	描述
qcs:current_time	Date and time	Web Server 接收到请求的时间。以 ISO8601 标准表示，并需要使用 UTC 时间。
qcs:ip	IP address	发起请求的 IP 地址。要符合 CIDR 规范。
qcs:resource_tag	String	基于资源上的标签控制对这些资源的访问。可将策略中指定的标签键/值对与绑定在资源上的键/值对进行比较，仅当匹配时才能访问资源。
qcs:request_tag	String	控制可以在请求中传递哪些标签。可将策略中指定的标签键/值对与请求中传递的键/值对进行比较，仅当匹配时才能绑定或解绑标签。

注意

当前条件键即可以应用于全局服务，也可以应用于特定服务。

条件键区分大小写。

运算符

在生效条件(Condition) 中使用条件运算符来将策略中的条件键和条件值与请求上下文中的值进行匹配。

按照类型将条件运算符分为7类：字符串类型（String）、数字类型（Number）、日期类型（Date and time）、布尔类型（Boolean）和 IP 地址类型（IP address）、二进制条件运算符（Binary）、空条件键运算符（Null）。

条件运算符类型	条件运算符	描述
字符串条件运算符	string_equal	字符串等于（区分大小写）
	string_not_equal	字符串不等于（区分大小写）
	string_equal_ignore_case	字符串等于（不区分大小写）
	string_not_equal_ignore_case	字符串不等于（不区分大小写）

数字条件运算符	numeric_equal	数值等于
	numeric_not_equal	数值不等于
	numeric_less_than	数值小于
	numeric_less_than_equal	数值小于等于
	numeric_greater_than	数值大于
	numeric_greater_than_equal	数值大于等于
日期条件运算符	date_equal	日期时间等于
	date_not_equal	日期时间不等于
	date_less_than	日期时间小于
	date_less_than_equal	日期时间小于等于
	date_greater_than	日期时间大于
	date_greater_than_equal	日期时间大于等于
布尔值条件运算符	bool_equal	布尔值匹配
二进制条件运算符	binary_equal	数值等于
IP 地址条件运算符	ip_equal	IP 地址等于
	ip_not_equal	IP 地址不等于
空条件键运算符	null_equal	条件键为空匹配

映射关系

在生效语句中，可以使用的条件（Condition）取决于选择的条件键，条件键与运算符的映射关系如下：

说明

运算符 string_like 和 string_not_like 对应的条件值只支持 `大小写字母` 、 `数字` 、 `-` 、 `_` ，不支持列表类接口。列表类接口可以通过 支持 CAM 的业务接口 查询。

条件键	运算符
qcs:resource_tag/qcs:request_tag	string_equal
	string_not_equal

	string_equal_ignore_case
	string_not_equal_ignore_case
	string_like
	string_not_like
qcs:current_time	date_equal
	date_not_equal
	date_less_than
	date_less_than_equal
	date_greater_than
	date_greater_than_equal
qcs:ip	ip_equal
	ip_not_equal

应用场景

最近更新时间：2024-01-23 17:54:33

场景类型	场景说明	示例
条件运算符包含一个条件键的一个条件值	允许 VPC 绑定指定的对等连接，VPC 的地域需要指定	示例
	只能对绑定标签的云服务器实例进行重启	示例
条件运算符包含一个条件键的多个条件值	允许指定两个 IP 的用户访问	示例
具有多个条件运算符的场景	允许指定 IP 和指定日期的用户访问	示例
单个条件运算符包含多个条件键	将多个条件键附加到单个条件运算符则	示例
布尔值条件运算符的应用	子用户需绑定 token 后才可删除 API 密钥	示例

条件运算符包含一个条件键的一个条件值

场景说明1

当 CAM 用户在调用 VPC 对等连接 API 时，除了需要判断 CAM 用户是否拥有对等连接 API 和对等连接资源的访问权限外，还需要确认 CAM 用户是否拥有对等连接关联的 VPC 的访问权限。

使用示例1

以下示例描述允许 VPC 绑定指定的对等连接， VPC 的地域必须是上海。

```
{
    "version": "2.0",
    "statement": [
    {
        "effect": "allow",
        "action": "name/vpc:AcceptVpcPeeringConnection",
        "resource": "qcs::vpc:sh::pcx/2341",
        "condition": {
            "string_equal_if_exist": {
                "vpc:region": "sh"
            }
        }
    }
   ]
}
```

场景说明2

当 CAM 用户访问腾讯云资源时，需要限制用户仅可访问绑定指定标签的资源。

使用示例2

以下示例描述用户只能对绑定标签“部门&研发部”的云服务器实例进行重启（cvm:RebootInstances）。

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "cvm:RebootInstances"
            ],
            "resource": "*",
            "condition": {
                "for_any_value:string_equal": {
                    "qcs:resource_tag": [
                        "Department&Research and Development"
                    ]
                }
            }
        }
    ]
}
```

条件运算符包含一个条件键的多个条件值

场景说明

单个条件运算符包含一个条件键的多个条件值，则采用逻辑 OR 评估该条件运算符，多个条件值时需要使用集合运算符号表示。
CAM 用户调用云 API 时，需要限制用户访问来源，则要求在现有的策略基础上加上 IP 条件。

使用示例

以下示例描述用户必须在 `10.217.182.3/24` 或者 `111.21.33.72/24` 网段才能上传对象（cos:PutObject）。

```
{
    "version": "2.0",
    "statement":[
    {
```

```
            "effect": "allow",
            "action": "cos:PutObject",
            "resource": "*",
            "condition": {
                "ip_equal": {
                    "qcs:ip": [
                        "10.217.182.3/24",
                        "111.21.33.72/24"
                    ]
                }
            }
        }
    ]
}
```

具有多个条件运算符的场景

场景说明

如果您的策略具有多个条件运算符，则使用逻辑 AND 评估条件。

使用示例

以下示例描述用户必须请求 IP 为 `192.168.1.1` ，请求日期小于2022-05-31 00:00:00才可以匹配。

```
"condition":{
                "ip_equal": {
                    "qcs:ip": "192.168.1.1"
                },
                "date_less_than": {
                    "qcs:current_time": "2022-05-31 00:00:00"
                }
            }
```

单个条件运算符包含多个条件键

场景说明

如果您的策略具有多个条件运算符或将多个条件键附加到单个条件运算符则使用逻辑 AND 评估条件。

使用示例

以下示例描述资源标签为"部门&研发部"，且请求标签为"部门&研发部"才可以匹配。

```
"condition": {
                "string_equal": {
                    "qcs:resource_tag": [
                        "Department&Research and Development"
                    ],
                    "qcs:request_tag": [
                        "Department&Research and Development"
                    ]
                }
            }
```

布尔值条件运算符的应用

场景说明

子用户需绑定 token 后才可删除 API 密钥。

使用示例

以下示例描述，授权此条策略的子用户，需要绑定 token 后，才可删除 API 密钥。

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "cam:DeleteApiKey"
            ],
            "resource": [
                "*"
            ],
            "condition": {
                "bool_equal": {
                    "qcs:BindToken": "true"
                }
            }
        }
    ]
}
```

策略版本控制

最近更新时间：2024-01-23 17:54:33

概述

当您设置的自定义策略操作变更时，系统不会覆盖原有策略而是自动新建一条新的版本。保存后，您可以通过将不同的版本设置为默认版本，快速回滚到不同版本的策略。

设置默认策略版本的权限

主账号或者具有 cam:ListPolicies、cam:GetPolicy、cam:UpdatePolicy 接口权限的子账号可以操作设置默认策略版本。
主账号可以通过以下策略语法授权给子账号设置默认策略版本的权限：

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "name/cam:ListPolicies",
                "name/cam:GetPolicy",
                "name/cam:UpdatePolicy"
            ],
            "resource": [
                "*"
            ]
        }
    ]
}
```

设置自定义策略默认版本

您可以将自定义策略的其中一个版本设置为默认版本，即有效版本。设置成功之后，所有关联该自定义策略的子账号将获取当前默认版本设置的权限。
1. 登录访问管理控制台，进入 策略 管理页面。
2. 在策略管理页面，单击需要设置的自定义策略名称，进入策略详情页。

3. 在策略详情页，选择**策略版本**。
4. 找到需要设置的版本，勾选左侧选择框，单击**设置为默认**，完成设置自定义策略默认版本操作。

使用不同版本回滚更改

您可以通过设置自定义策略的默认版本以回滚您的更改。例如，参考以下场景：
创建一个允许子账号拥有云服务器 ins-1 读权限的自定义策略。创建时，当前自定义策略只有一个版本（标记为版本 1），该版本自动设置为默认版本。该策略可正常工作。
当您更新该自定义策略，在原有策略基础上新增云服务器 ins-2 的读权限，保存之后，系统会创建新的策略版本（标记为版本 2）。将版本2 设置为默认版本之后，子账号反馈缺少云服务器管理权限。在此情况下，您可以将当前策略回滚到可正常工作的策略版本 版本 1。您可以将版本 1 设置为默认版本，子账号将可恢复管理原始云服务器。
在确定策略版本版本 2 中的错误并更新之后，系统会创建该策略的另一个新版本，标记为版本 3。您可以将版本 3 设置为默认版本以满足子账号拥有两台云服务器 ins-1 和 ins-2 的读权限。此时，您可以删除错误的策略版本版本 2。

版本限制

一个自定义策略最多保存 5 个策略版本。当自定义策略的策略版本数量达到 5 个时，您编辑且保存策略时必须先删除一个或多个现有版本才可保存成功。您可以在弹出的提示框中选择以下两种方式删除已有策略版本：

删除最旧的非默认策略版本。
勾选需要删除的策略版本（可多选）。您可以单击左侧【▼】查看每个版本的策略语法，以方便做出决定。
说明：
删除某个版本时，其余版本的版本标记符不会更改。因此，版本标记符可能是不连续的。例如，如果您删除策略版本版本 2 和 版本 4，然后添加两个新版本，则其余版本标记符可能是版本 1、版本 3、版本 5、版本 6 和版本 7。

权限策略 deny 不生效场景

最近更新时间：2024-01-23 17:54:33

当权限策略中同时包含允许（allow）和拒绝（deny）的授权语句时，需要根据具体的场景判断 deny 是否生效。本文通过查询资源列表类的操作、COS 权限 deny 所有用户（匿名用户 anonymous）、计费相关操作三类典型场景，帮助您理解 deny 不生效的逻辑。

查询资源列表类的操作

腾讯云各个服务的操作（action）可以简单划分为增、删、改、查 4 类，其中查询类又可以分为查询单个资源详情和查询某类资源列表，查询某类资源列表的操作。在以下场景中可能存在 deny 不生效，**建议对这类操作避免使用 deny，避免使用 string_not_equal、string_like 等条件键**。

不生效场景列举：

场景1：授权允许（allow）子用户访问 CVM 实例 a、b、c，拒绝（deny）访问实例 d，同时又授予子用户访问绑定标签 T 的资源，其中实例 d 绑定了标签T，此时“拒绝（deny）访问实例 d”的策略不会生效。
例如：授权以下策略，用户在查看 CVM 实例列表的时候仍然能够查看到实例 d。

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "*"
            ],
            "resource": "*",
            "condition": {
                "for_any_value:string_equal": {
                    "qcs:resource_tag": [
                        "key&T"  //标签 T
                    ]
                }
            }
        },
        {
            "effect": "allow",
            "action": [
                "*"
            ],
            "resource": [
```

```
                "qcs::cvm:ap-guangzhou::instanceid/a",  //实例 a
                "qcs::cvm:ap-guangzhou::instanceid/b",  //实例 b
                "qcs::cvm:ap-guangzhou::instanceid/c"   //实例 c
            ]
        },
        {
            "effect": "deny",
            "action": [
                "*"
            ],
            "resource": [
                "qcs::cvm:ap-guangzhou::instanceid/d"   //实例 d
            ]
        }
    ]
}
```

场景2：授权允许子用户访问绑定标签 T1 的资源，拒绝访问绑定标签 T2 的资源，其中资源 a 既绑定了标签 T1，又绑定了标签 T2，则拒绝访问 a 资源的策略不会生效。

例如：授权以下策略，仍然可以在查看资源列表的时候查看到资源 a。

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "*"
            ],
            "resource": "*",
            "condition": {
                "for_any_value:string_equal": {
                    "qcs:resource_tag": [
                        "key&T1"  //标签 T1
                    ]
                }
            }
        },
        {
            "effect": "deny",
            "action": [
                "*"
            ],
            "resource": "*",
            "condition": {
                "for_any_value:string_equal": {
                    "qcs:resource_tag": [
```

```
                        "key&T2"  //标签 T2
                    ]
                }
            }
        }
    ]
}
```

场景3：权限策略包含 condition 时，支持精确匹配的策略条件键使用 string_equal、ip_equal、ip_not_equal 等才会生效，其他类型条件键（例如 string_not_equal 等）不会生效。
例如：授权以下策略，用户仍然可能看到关联了标签 T 的资源。

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "*"
            ],
            "resource": "*",
            "condition": {
                "for_any_value:string_not_equal": {
                    "qcs:resource_tag": [
                        "key&T"  //标签 T
                    ]
                }
            }
        }
    ]
}
```

场景4：同时授权允许访问所有 resource，以及拒绝访问绑定指定标签的资源时，拒绝访问可能无法生效，即仍然能查看到关联了该标签的资源。
例如：授权以下策略，用户在查看资源列表的时候仍然可能查看到主账号下所有的资源。

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

```
        {
            "effect": "deny",
            "action": [
                "*"
            ],
            "resource": "*",
            "condition": {
                "for_any_value:string_equal": {
                    "qcs:resource_tag": [
                        "key&T"  //标签 T
                    ]
                }
            }
        }
    ]
}
```

COS 权限 deny 所有用户（匿名用户 anonymous）

在 COS 的 Bucket ACL 或 Bucket Policy 中配置 deny 所有用户（匿名用户 anonymous）访问，但如果同时还有另外指定 allow 某个用户，被 allow 的用户仍然可以访问 COS 存储桶。

计费相关操作

如果一个子用户关联了 AdministratorAccess 或 QCloudFinanceFullAccess 策略，同时还关联了一个 deny action finance:xx 的策略，这个子用户在 action finance:xx 仍然可以鉴权通过，不会被拒绝访问。

策略分析器

最近更新时间：2024-08-26 16:48:01

策略分析器，用于分析您创建策略的 JSON 语句，对策略进行验证检查，其中包括策略的错误、警告和建议，可以帮助您编写更符合安全实践教程的策略。

version

1. 错误——缺少 version

在腾讯云控制台中，策略分析器的错误提示为：错误——缺少 version，version 是描述策略语法（version）版本，该元素是必填项。

解决错误：Version 是描述策略语法版本。该元素是必填项。目前仅允许值为“2.0”或“3.0”（Version 3.0使用指引）。要使用所有可用策略功能，需将以下 Version 元素包含在所有策略中的 Statement 元素之前。每一个策略仅允许一个 version 元素。

相关文档参考：元素参考概述。

2. 错误——无效的 version

在腾讯云控制台中，策略分析器的错误提示为：错误——无效的 version，version 是描述策略语法（version）版本，该元素是必填项，目前仅允许值为“2.0”或“3.0”。

解决错误：Version 是描述策略语法版本。该元素是必填项。目前仅允许值为“2.0”或“3.0”（Version 3.0使用指引）。要使用所有可用策略功能，需将以下 Version 元素包含在所有策略中的 Statement 元素之前。每一个策略仅允许一个 version 元素。

相关文档参考：元素参考概述。

3. 错误——冗余 version

在腾讯云控制台中，策略分析器的错误提示为：错误——冗余 version，version 是描述策略语法（version）版本，该元素是必填项，每一个策略仅允许一个 version 值。

解决错误：Version 是描述策略语法版本。该元素是必填项。目前仅允许值为“2.0”或“3.0”（Version 3.0使用指引）。要使用所有可用策略功能，需将以下 Version 元素包含在所有策略中的 Statement 元素之前。每一个策略仅允许一个 version 元素。

相关文档参考：元素参考概述。

statement

4. 错误——缺少 statement

在腾讯云控制台中，策略分析器的错误提示为：错误——缺少 statement，statement 是描述一条或多条权限的详细信息。

解决错误：statement 是描述一条或多条权限的详细信息。该元素包括 principal、action、resource、condition、effect 等多个其他元素的权限或权限集合。一条策略有且仅有一个 statement 元素。

相关文档参考：元素参考概述。

5. 错误——无效的 statement

在腾讯云控制台中，策略分析器的错误提示为：错误——无效的 statement，statement 是包括 principal、action、resource、condition、effect 等多个其他元素的权限或权限集合。

解决错误：statement 是描述一条或多条权限的详细信息。该元素包括 principal、action、resource、condition、effect 等多个其他元素的权限或权限集合。一条策略有且仅有一个 statement 元素。

相关文档参考：元素参考概述。

6. 错误——冗余 statement

在腾讯云控制台中，策略分析器的错误提示为：错误——冗余 statement，statement 是描述一条或多条权限的详细信息，一条策略有且仅有一个 statement 元素。

解决错误：statement 是描述一条或多条权限的详细信息。该元素包括 principal、action、resource、condition、effect 等多个其他元素的权限或权限集合。一条策略有且仅有一个 statement 元素。

相关文档参考：元素参考概述。

effect

7. 错误——缺少 effect

在腾讯云控制台中，策略分析器的错误提示为：错误——缺少 effect，effect 是描述声明产生的结果是“允许”还是“显式拒绝”。

解决错误：effect 是描述声明产生的结果是“允许”还是“显式拒绝”。包括 allow（允许）和 deny （显式拒绝）两种情况。该元素是必填项。

相关文档参考：元素参考概述。

8. 错误——无效的 effect

在腾讯云控制台中，策略分析器的错误提示为：错误——无效的 effect，该元素是必填项，effect 仅包括 allow（允许）和 deny （显式拒绝）两种情况。

解决错误：effect 是描述声明产生的结果是“允许”还是“显式拒绝”。包括 allow（允许）和 deny （显式拒绝）两种情况。该元素是必填项。

相关文档参考：元素参考概述。

principal

9. 错误——缺少 principal

在腾讯云控制台中，策略分析器的错误提示为：错误——缺少 principal，principal 是描述策略授权的实体，基于资源的策略必须包含 principal 元素。

解决错误：principal 是描述策略授权的实体。包括用户（主账号、子账号、角色、联合身份用户等实体）。基于资源的策略必须包含 principal 元素。

相关文档参考：元素参考概述。

10. 错误——无效的 principal

在腾讯云控制台中，策略分析器的错误提示为：错误——无效的 principal，principal 是描述策略授权的实体。

解决错误：principal 是描述策略授权的实体。包括用户（主账号、子账号、角色、联合身份用户等实体）。仅支持在基于资源的策略中使用该元素。

示例：

```
"principal": {
"qcs": [
"qcs::cam::uin/100000000001:uin/100000000002"
]
}
```

相关文档参考：元素参考概述。

11. 错误——SCP 不支持 principal

在腾讯云控制台中，策略分析器的错误提示为：错误——Organizations 服务控制策略 (SCP) 不支持 Principal。

解决错误：Organizations 服务控制策略 (SCP) 不支持 Principal 元素。请删除 Principal 元素。

相关文档参考：元素参考概述、服务管控策略。

12. 建议——principal 为空

在腾讯云控制台中，策略分析器的错误提示为：建议——未指定 principal。

解决错误：需要在角色的信任策略和基于资源的策略中使用 Principal 元素。基于资源的策略是直接嵌入资源中的策略。语句的 Principal 元素为空时，语句对策略虽然没有影响，但腾讯建议您指定主体。

相关文档参考：元素参考概述。

resource

13. 错误——缺少 resource

在腾讯云控制台中，策略分析器的错误提示为：错误——缺少 resource，resource 是描述授权的具体数据。

解决错误：resource 是描述授权的具体数据。资源是用六段式描述。该元素是必填项。每款产品的资源定义详情会有所区别。
相关文档参考：元素参考概述、资源描述方式。

14. 错误——resource 为空

在腾讯云控制台中，策略分析器的错误提示为：错误——resource 为空，resource 是描述授权的具体数据，该元素是必填项。
解决错误：resource 是描述授权的具体数据。资源是用六段式描述。该元素是必填项。每款产品的资源定义详情会有所区别。
相关文档参考：元素参考概述、资源描述方式。

15. 错误——资源六段式第一段错误

在腾讯云控制台中，策略分析器的错误提示为：错误——资源六段式第一段错误，资源六段式前缀固定为 qcs。
解决错误：资源六段式前缀固定为 qcs，qcloud service 的简称，表示是腾讯云的云资源。资源六段式：qcs:project_id:service_type:region:account:resource。
相关文档参考：元素参考概述、资源描述方式。

16. 错误——资源六段式第二段错误

在腾讯云控制台中，策略分析器的错误提示为：错误——资源六段式第二段错误。
解决错误：资源六段式第二段错误，资源六段式第二段为描述项目信息，仅兼容 CAM 早期逻辑，当前策略语法禁止填写该信息，置空即可。
相关文档参考：元素参考概述、资源描述方式。

17. 错误——资源六段式第三段无效的服务

在腾讯云控制台中，策略分析器的错误提示为：错误——资源六段式第三段服务无效的服务。
解决错误：资源六段式第三段为描述产品简称，详细可查看 支持 CAM 的产品 中的 “CAM 中简称”。
相关文档参考：元素参考概述、资源描述方式、支持 CAM 的产品。

18. 错误——资源六段式第四段无效的地域

在腾讯云控制台中，策略分析器的错误提示为：错误——资源六段式第四段无效的地域。
解决错误：资源六段式第四段描述地域信息，值为空的时候表示所有地域。
相关文档参考：元素参考概述、资源描述方式。

19. 错误——资源六段式第五段无效的 uin

在腾讯云控制台中，策略分析器的错误提示为：错误——资源六段式第五段无效的 uin。
解决错误：资源六段式第五段为描述资源拥有者的主账号信息，目前支持两种方式描述资源拥有者，uin 和 uid 方式。uin 方式，即主账号的账户 ID，表示为uin/${uin}。uid 方式，即主账号的 APPID，表示为 uid/${appid}，仅 COS 和 CAS 服务的资源拥有者使用该方式描述。值为空的时候表示创建策略的 CAM 用户所属的主账号。

相关文档参考：元素参考概述、资源描述方式。

20. 错误——资源六段式第五段无效的 uid

在腾讯云控制台中，策略分析器的错误提示为：错误——资源六段式第五段无效的 uid。
解决错误：资源六段式第五段为描述资源拥有者的主账号信息，目前支持两种方式描述资源拥有者，uin 和 uid 方式。uin 方式，即主账号的账户 ID，表示为 uin/${uin}。uid 方式，即主账号的 APPID，表示为 uid/${appid}，仅 COS 和 CAS 服务的资源拥有者使用该方式描述。值为空的时候表示创建策略的 CAM 用户所属的主账号。
相关文档参考：元素参考概述、资源描述方式。

21. 错误——资源六段式第五段无效的账户格式

在腾讯云控制台中，策略分析器的错误提示为：错误——资源六段式第五段无效的账户格式。
解决错误：资源六段式第五段为描述资源拥有者的主账号信息，目前支持两种方式描述资源拥有者，uin 和 uid 方式。uin 方式，即主账号的账户 ID，表示为 uin/${uin}。uid 方式，即主账号的 APPID，表示为 uid/${appid}，仅 COS 和 CAS 服务的资源拥有者使用该方式描述。值为空的时候表示创建策略的 CAM 用户所属的主账号。
相关文档参考：元素参考概述、资源描述方式。

22. 错误——资源六段式第六段无效的资源格式

在腾讯云控制台中，策略分析器的错误提示为：错误——资源六段式第六段无效的资源格式。
解决错误：资源六段式第六段为描述各产品的具体资源详情，目前支持两种方式描述资源信息，resource_type/${resourceid} 和 <resource_type>/<resource_path>。
resource_type/${resourceid}：resourcetype 为资源前缀，描述资源类型，详细可查看 支持 CAM 的业务接口中产品的资源六段式；${resourceid} 为具体的资源 ID，可前往各个产品控制台查看，值为 * 时代表该类型资源的所有资源。
<resource_type>/<resource_path>：resourcetype 为资源前缀，描述资源类型；<resource_path> 为资源路径，该方式下，支持目录级的前缀匹配。详细可查看 支持 CAM 的业务接口 中产品的资源六段式。
相关文档参考：元素参考概述、资源描述方式、支持 CAM 的业务接口。

23. 错误——资源六段式第六段通配符错误

在腾讯云控制台中，策略分析器的错误提示为：错误——资源六段式第六段通配符错误。
解决错误：资源六段式第六段为描述各产品的具体资源详情，不支持 qcs::ckafka:bj:check:*/ckafka-37zqnevtest* 或 *qcs::ckafka:bj:check:/** 格式。
相关文档参考：元素参考概述、资源描述方式。

24. 错误——资源六段式第六段有前缀时，第三段服务不能为空

在腾讯云控制台中，策略分析器的错误提示为：错误——资源六段式第六段有前缀时，第三段服务不能为空。
解决错误：资源六段式第六段为描述各产品的具体资源详情，资源六段式第六段有前缀时，第三段必须填写相应服务简称。
相关文档参考：元素参考概述、资源描述方式。

25. 错误——资源六段式格式错误

在腾讯云控制台中，策略分析器的错误提示为：错误——资源六段式格式错误。
解决错误：资源六段式必须包含 6 个字段并包含以下结构: qcs:project_id:service_type:region:account:resource。
相关文档参考：元素参考概述、资源描述方式。

26. 错误——资源六段式长度超限

在腾讯云控制台中，策略分析器的错误提示为：错误——资源六段式长度超限。
解决错误：资源六段式长度上限为500字符。
相关文档参考：元素参考概述、资源描述方式。

27. 建议——资源冗余

在腾讯云控制台中，策略分析器的错误提示为：建议——资源冗余。
解决错误：描述的指定资源与资源通配符“*”冗余。
示例：

```
"Resource": [
              "qcs::cam::uin/111122223333:rolename/admin",
              "qcs::cam::uin/1111122223333:rolename/readonly",
              "qcs::cam::uin/1111122223333:rolename/*"
            ]
```

在示例中，第三个资源六段式已描述所有 rolename 资源，其他角色 admin、readonly 已包含在通配符“*”。
相关文档参考：元素参考概述、资源描述方式。

action

28. 错误——缺少 action

在腾讯云控制台中，策略分析器的错误提示为：错误——缺少 action，action 是描述允许或拒绝的操作。
解决错误：action 是描述允许或拒绝的操作。操作可以是 API（以 name 前缀描述）或者功能集（一组特定的 API，以 actionName 前缀描述）。该元素是必填项。
示例：

```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": [
        "ES:CreateServerlessSpace",
        "ES:CreateServerlessInstance",
```

```
          "ES:DescribeServerlessInstances",
          "ES:CreateServerlessInstanceUser",
          "ES:DescribeServerlessInstanceUsers",
          "ES:CreateServerlessDi",
          "ES:DescribeServerlessDi",
          "ES:DeleteServerlessInstanceUser",
          "ES:DeleteServerlessDi",
          "ES:DeleteServerlessInstance",
          "ES:DescribeServerlessSpaces",
          "ES:SearchServerlessData"
        ],
        "resource": [
          "*"
        ]
      }
    ]
}
```

相关文档参考：元素参考概述。

29. 错误——无效的 action

在腾讯云控制台中，策略分析器的错误提示为：错误——无效的 action。

解决错误：action 是描述允许或拒绝的操作。输入的 action 无效，请检查您输入的 action 前缀和 action 名称。

相关文档参考：支持 CAM 的业务接口。

30. 错误——action 中无效的服务前缀

在腾讯云控制台中，策略分析器的错误提示为：错误——action 中无效的服务前缀。

解决错误：action 是描述允许或拒绝的操作。action 中服务前缀无效，请检查您输入的 action 前缀。

相关文档参考：支持 CAM 的业务接口。

31. 建议——action 冗余

在腾讯云控制台中，策略分析器的错误提示为：建议——action 冗余。

解决错误：action 有冗余，指定的 action 与通配符“*”冗余。

示例：

```
"Action": [
        "cam:Get*",
        "cam:List*",
        "cam:Getrole"
        ],
```

在示例中，通配符"cam:Get*"已经包含了 Getrole 权限。

相关文档参考：元素参考概述、资源描述方式。

condition

32. 错误——数据类型不匹配

在腾讯云控制台中，策略分析器的错误提示为：错误——数据类型不匹配。
解决错误：输入的条件值和条件运算符、条件键要求的数据类型不匹配。
相关文档参考：条件键和条件运算符。

33. 错误——无效的全局条件键

在腾讯云控制台中，策略分析器的错误提示为：错误——无效的条件键。
解决错误：全局条件键是带有 qcs: 前缀的条件键，目前支持 qcs:current_time、qcs:ip、qcs:resource_tag、qcs:request_tag 四种全局条件键。
相关文档参考：条件键和条件运算符。

34. 错误——无效的服务条件键

在腾讯云控制台中，策略分析器的错误提示为：错误——无效的服务条件键。
解决错误：服务条件键是带有服务简称的前缀，例如 vpc: 前缀的条件键。
相关文档参考：条件键和条件运算符。

35. 错误——不支持多个布尔值

在腾讯云控制台中，策略分析器的错误提示为：错误——不支持多个布尔值。
解决错误：布尔条件运算符仅支持一个布尔值。
相关文档参考：条件键和条件运算符。

36. 错误——condition 长度超限

在腾讯云控制台中，策略分析器的错误提示为：错误——condition 长度超限。
解决错误：condition 长度最大支持4095字符。
相关文档参考：条件键和条件运算符。

37. 错误——无效的条件运算符

在腾讯云控制台中，策略分析器的错误提示为：错误——无效的条件运算符。
解决错误：条件运算符输入无效，请参见 条件键和条件运算符。
相关文档参考：条件键和条件运算符。

38. 建议——条件键和条件运算符不匹配

在腾讯云控制台中，策略分析器的错误提示为：错误——条件键和条件运算符不匹配。
解决错误：条件键和条件运算符不匹配，请参见 条件键和条件运算符。
相关文档参考：条件键和条件运算符。

其他

39. 错误——无效的策略元素

在腾讯云控制台中，策略分析器的错误提示为：错误——无效的策略元素。
解决错误：策略语句仅支持版本（version）、语句（statement）、委托人（principal）、操作（action）、资源（resource）、生效条件（condition）以及效力（effect）元素。
相关文档参考：元素参考概述。

40. 错误——JSON 语法错误

在腾讯云控制台中，策略分析器的错误提示为：错误——JSON 语法错误。
解决错误：您的策略包含语法错误。请检查您的 JSON 语法。
相关文档参考：JSON验证程序、元素参考概述。

41. 错误——策略长度超过限制

在腾讯云控制台中，策略分析器的错误提示为：错误——策略长度超过限制。
解决错误：策略长度超过限制，策略长度最大支持6144。
相关文档参考：元素参考概述。

42. 错误——ACL 策略长度超过限制

在腾讯云控制台中，策略分析器的错误提示为：错误——ACL 策略长度超过限制。
解决错误：ACL 策略长度超过限制，策略长度最大支持20480。
相关文档参考：元素参考概述。

43. 错误——自定义策略数量超过上限

在腾讯云控制台中，策略分析器的错误提示为：错误——自定义策略数量超过上限。
解决错误：腾讯云账号自定义策略数量上限为1500条。
相关文档参考：元素参考概述。

44. 警告——无效的日期值

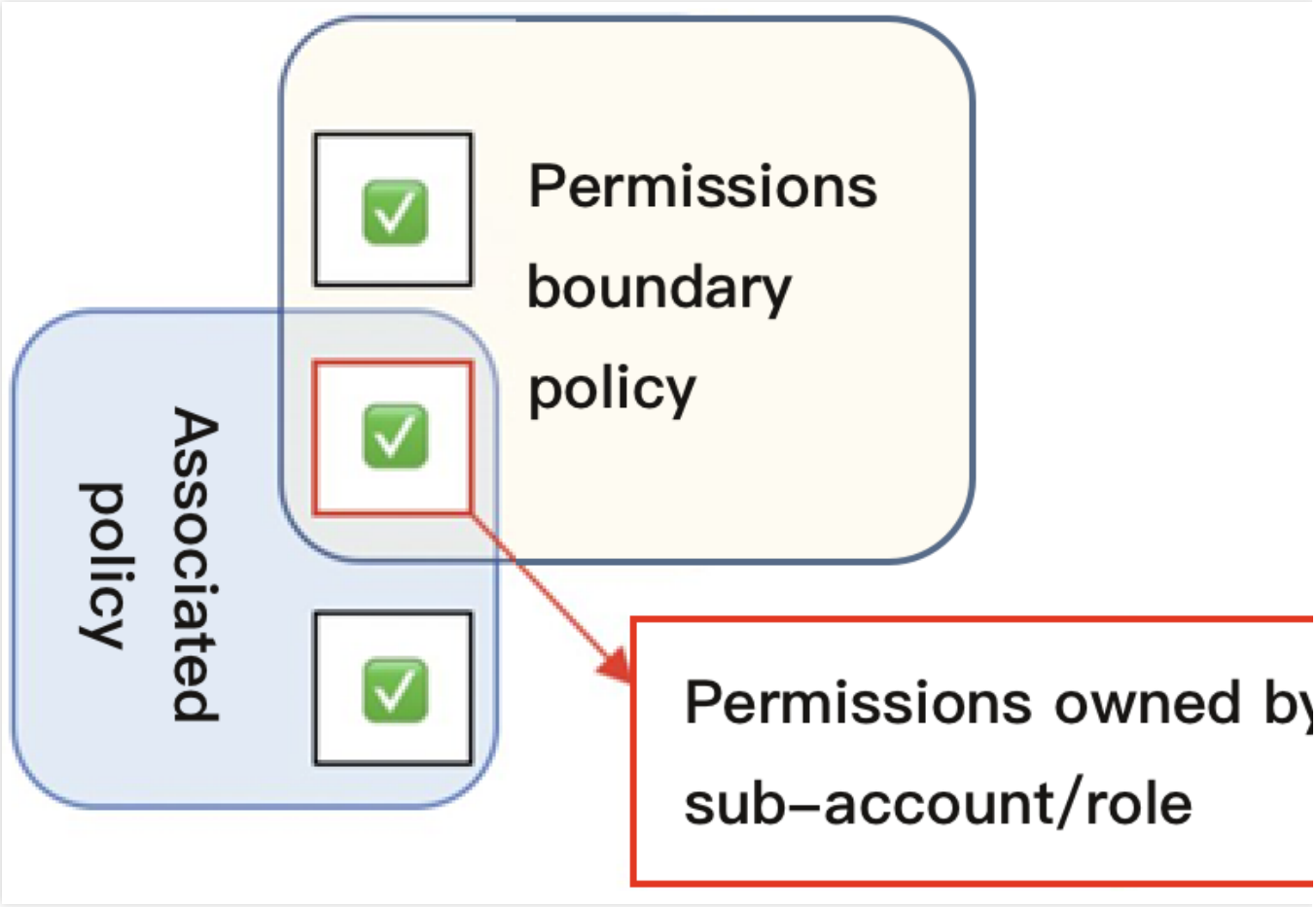
在腾讯云控制台中，策略分析器的错误提示为：警告——无效的日期值。
解决警告：Unix Epoch 时间描述自 1970 年 1 月 1 日以来已经过去的时间点，减去闰秒。Epoch 时间可能无法解析到您期望的精确时间。腾讯云建议您对日期和时间格式使用 W3C 标准。例如，您可以指定一个完整的日期，如 YYYY-MMM-DD (1997-07-16)，也可以将时间附加到秒，例如 YYYY-MM-DDThh:mm:ssTZD (1997-07-16T19:20:30+01:00)。
相关文档参考：W3C 日期和时间格式。

权限边界

最近更新时间：2024-01-23 17:57:37

概念

权限边界是腾讯云用于对子账号/角色设置权限边界的一种高级功能。当您设置子账号/角色的权限边界时，该子账号/角色只能执行子账号/角色关联策略和其权限边界同时允许的操作。权限边界仅限制子账号/角色拥有的最大权限范围，不能用于设置子账号/角色关联的权限，详细评估逻辑可参考下图：



使用场景

您可以使用预设策略或自定义策略为子账号/角色设置权限，该策略为子账号/角色的最大权限。本文档以一个典型案例让您轻松了解如何使用权限边界设置子账号的最大权限。
假设公司腾讯云资源管理员需要为运维员工设置权限，需满足以下需求：

公司有两个运维员工，分别拥有昵称为 test1、test2 的两个子账号。
拥有子账号 test1 的员工仅需要管理主账号下云数据库 MySQL 的所有权限。
拥有子账号 test2 的员工仅需要管理主账号下实例 ID 为 ins-1 的服务器操作权限。
公司规定所有子账号对于主账号下云服务器、 云数据库 MySQL 的相关的操作都必须在公司所在网段（10.217.182.3/24 或者 111.21.33.72/24 ）操作。

操作步骤

子账号 test1 权限设置

1. 登录公司管理员账号，进入 用户列表页面。
2. 在用户列表页面，找到昵称为 test1 的子账号，单击用户昵称进入用户详情页面。
3. 在**权限-权限策略**操作栏，单击**关联策略**勾选 QcloudCDBFullAccess 策略 ，为子账号 test1 设置云数据库 MySQL 的所有权限。
4. 在**权限-权限边界**操作栏，单击**设置边界**，进入设置权限边界页面。
5. 在设置权限边界页面，单击**新建自定义策略**，进入新建自定义策略页面。
6. 在新建自定策略页面，策略名称设置为「policygen-1」。
7. 在可视化策略生成器栏，勾选补充以下信息：
效果（Effect）：选择「允许」。
服务（Service）：选择「云数据库 MySQL」。
操作（Action）：选择「全部操作」，单击**确定**。
资源（Resource）：默认为全部资源（*）。
条件（Condition）：勾选来源 IP，补充IP值为「10.217.182.3/24，111.21.33.72/24」。
8. 单击**创建**，进入设置权限边界页面。
9. 在设置权限边界页面，策略列表操作栏下勾选创建的自定义策略。
10. 单击**设置边界**，完成为子账号 test1 权限设置。

子账号 test 2 权限设置

1. 登录公司管理员账号，参考以下策略语法创建策略名称为 policygen-2 的自定义策略语法，操作步骤可参阅按策略语法创建。

```
{
 "version": "2.0",
 "statement": [
     {
         "effect": "allow",
         "resource": [
             "qcs::cvm:gz::instance/ins-1"
         ],
         "action": [
```

```
                "name/cvm:*"
            ]
        }
    ]
}
```

2. 在 用户列表页面，找到昵称为 test2 的子账号，单击用户昵称进入用户详情页面。
3. 在**权限-权限策略**操作栏，单击**关联策略**勾选 policygen-2 策略，为子账号 test2 设置云服务器 ins-1 的操作权限。
4. 在**权限-权限边界**操作栏，单击**设置边界**，进入设置权限边界页面。
5. 在设置权限边界页面，单击**新建自定义策略**，进入新建自定义策略页面。
6. 在新建自定策略页面，策略名称设置为「policygen-3」。
7. 在可视化策略生成器栏，勾选补充以下信息：

效果（Effect）：选择「允许」。

服务（Service）：选择「云服务器」。

操作（Action）：选择「全部操作」，单击**确定**。

资源（Resource）：默认为全部资源（*）。

条件（Condition）：勾选来源 IP，补充IP值为「10.217.182.3/24，111.21.33.72/24」。

8. 单击**创建**，进入设置权限边界页面。
9. 在设置权限边界页面，策略列表操作栏下勾选 policygen-3 策略。
10. 单击**设置边界**，完成为子账号 test2 权限设置。

排除故障
如何根据故障反馈创建策略

最近更新时间：2024-01-23 17:57:37

操作场景

本文档介绍如何通过故障反馈创建策略解除故障，解除之后子账号将在新设置的权限范围内管理主账号下的资源。

示例

当拥有 QcloudCVMReadOnlyAccess 策略的子账号尝试进行重装云服务器时将进行如下报错：

```
you are not authorized to perform operation (cvm:ResetInstance)
resource (qcs:id/1158313:cvm:ap-guangzhou:uin/2159973417:instance/ins-esuithv2) has n
 (9956aa75)
```

如您愿意授权子账号继续进行操作，您可以根据当前报错信息为其创建并关联一个自定义策略。

操作步骤

1. 进入 CAM 的 策略-控制台，单击新建自定义策略。
2. 在弹出的选择创建方式窗口中，单击【按策略生成器创建】，进入编辑策略页面。
3. 在编辑策略页面，补充以下信息：

效果（必选）：根据授权效果，选择允许还是拒绝。在本次示例中，选择「允许」。

服务（必选）：根据产品英文简称选择您要授权的产品。在本次示例中，对应报错信息的 operation 中的 「cvm」，您将从产品列表里选择「云服务器」。

操作（必选）：选择您要授权的操作。在本次示例中，对应报错信息 operation 中的「ResetInstance」。

资源（必填）：授权粒度为非资源级产品只能选择全部资源。授权粒度为资源级产品，可选择特定资源，点击添加资源六段式，填写资源前缀和资源。在本次示例中，对应报错信息的「resource」，需要对特定资源授权，选择特定资源，点击添加资源六段式，您可直接复制「qcs:id/1158313:cvm:ap-guangzhou:uin/2159973417:instance/instance/ins-esuithv2」中的前缀和资源填入。

条件（选填）：设置子账号上述授权的生效条件，例如指定 IP 才可访问。在本次示例中，不需要填入。

4. 单击**下一步**，进入关联用户/用户组页面。
5. 在关联用户/用户组页面，补充策略名称、描述，其中策略名称由控制台自动生成。

说明：

策略名称默认为 "policygen" ，后缀数字根据创建日期生成。您可进行自定义。

描述与 步骤 3 的服务和操作对应，您可根据实际需求进行修改。

6. 单击**完成**，完成按策略生成器创建自定义策略的操作。

7. 参考 通过策略关联用户 为子账号授权，授权成功后，子账号将获得相应的权限，解除故障。

如何根据无权限信息创建权限策略

最近更新时间：2024-01-23 17:57:37

操作场景

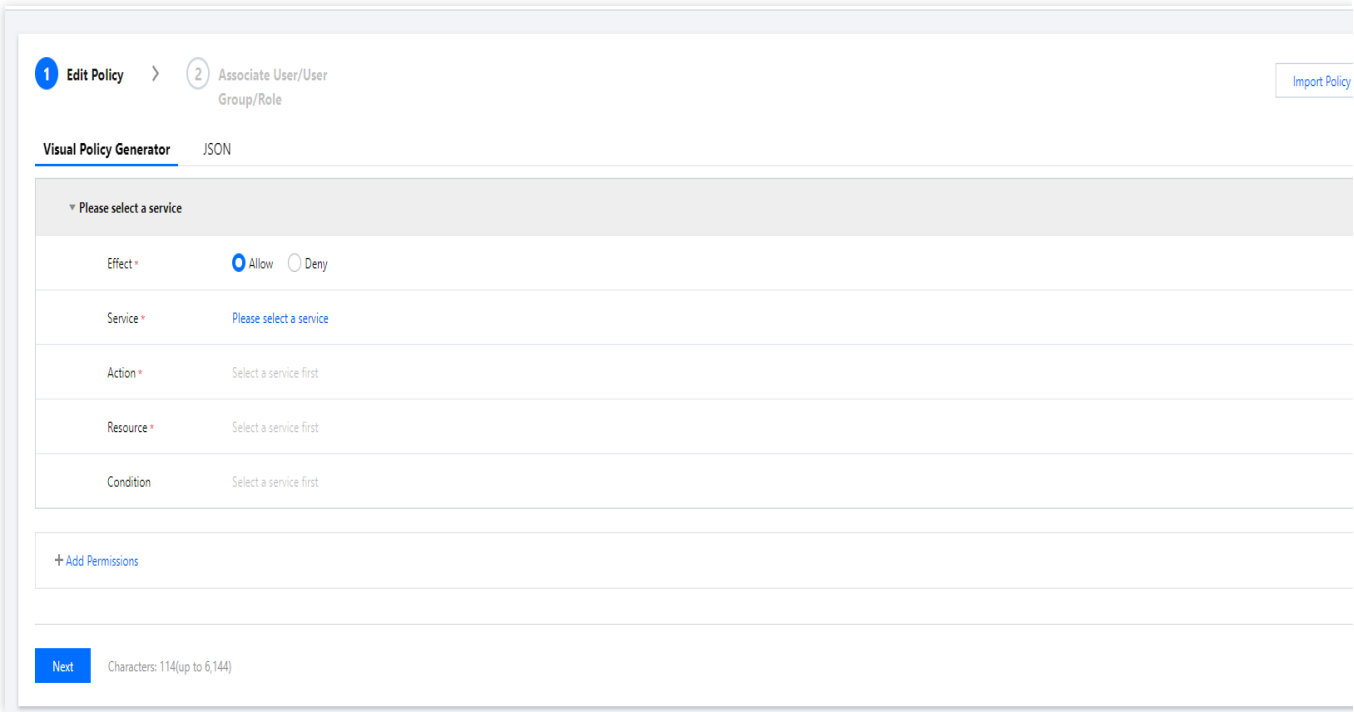
本文档介绍如何根据无权限信息创建权限策略，创建之后子账号将在新设置的权限范围内管理主账号下的资源。

前提条件

使用主账号或拥有访问管理全读写权限（QcloudCamFullAccess）的子账号操作。

操作步骤

1. 进入 CAM 的 策略-控制台，单击新建自定义策略。
2. 在弹出的选择创建方式窗口中，单击**按策略生成器创建**，进入编辑策略页面。
3. 在编辑策略页面，补充以下信息：



效果（必选）：根据授权效果，选择允许还是拒绝。在本次示例中，选择「允许」。

服务（必选）：根据产品英文简称选择您要授权的产品。在本次示例中，对应报错信息的 operation 中的「cvm」，您将从产品列表里选择「云服务器」。

操作（必选）：选择您要授权的操作。在本次示例中，对应报错信息 operation 中的「RebootInstances」。

资源（必填）：授权粒度为非资源级产品只能选择全部资源。授权粒度为资源级产品，可选择特定资源，点击添加资源六段式，填写资源前缀和资源。在本次示例中，对应报错信息的「resource」，需要对特定资源授权，选择特定资源，点击添加资源六段式，您可直接复制「qcs:id/0:cvm:ap-guangzhou:uin/10***6:instance/ins-arh4gyp2」中的前缀和资源填入。

条件（选填）：设置子账号上述授权的生效条件，其中「key」为条件键，「ope」为运算符，「value」为条件值。本次示例中，条件键（key）为「qcs:request_tag」，运算符(ope)为「for_all_value:string_equal」，条件值（value）为「"server&1024","a&b"」。

4. 单击**下一步**，进入关联用户/用户组页面。
5. 在关联用户/用户组页面，补充策略名称、描述，其中策略名称由控制台自动生成。

说明：

策略名称默认为 "policygen"，后缀数字根据创建日期生成。您可进行自定义。

描述与 步骤3 的服务和操作对应，您可根据实际需求进行修改。

6. 单击**完成**，完成按策略生成器创建自定义策略的操作。
7. 参考 通过策略关联用户 为子账号授权，授权成功后，子账号将获得相应的权限，解除故障。

下载安全分析报告

最近更新时间：2024-01-23 17:57:37

操作场景

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。

操作步骤

1. 登录 访问管理控制台，进入**概览**页面。
2. 在安全分析报告模块，单击**下载用户凭证报告**，根据提示进行身份验证，系统会自动生成相关报告。
3. 报告完成下载之后，您可请前往本地查看。

说明：

每4小时您可以在控制台生成一份新的 CSV 格式的用户凭证报告，如果距离上一份报告生成时间不足4小时，则直接返回已经生成的报告，不会再生成新报告。

报告格式

用户凭证报告采用 CSV 文件格式。您可以使用常用电子表格软件打开 CSV 文件以执行分析，也可以构建应用程序以编程方式使用 CSV 文件并执行自定义分析。

CSV 文件包含以下信息：

字段	含义	取值说明
AccountID	账号 ID	子账号 ID
Username	用户名称	子账号用户名称
UserType	用户类型	Sub-user：子用户 Collaborator：协作者 WeWork-Sub-user：企业微信子用户 Message-receiver：消息接收人
CreationTime	创建时间	示例：2019/8/16 9:25:56
PasswordEnabled	控制台密码是否启用	TRUE：已启用 FALSE：未启用，已禁用控制台访问，未设置登录密码

		not_supported：不涉及，WeWork-Sub-user（企业微信子用户）使用企业微信扫码登录，无登录密码；Message-receiver（消息接收人）仅用于接受消息，无登录密码；Collaborator（协作者）使用主账号身份登录密码，不涉及该项
PasswordLastRotation	密码最后修改时间	FALSE：已禁用控制台访问，未设置登录密码 not_supported：不涉及，WeWork-Sub-user（企业微信子用户）使用企业微信扫码登录，无登录密码；Message-receiver（消息接收人）仅用于接受消息，无登录密码；Collaborator（协作者）使用主账号身份登录密码，不涉及该项
LoginConsoleActive	是否支持登录控制台	TRUE：支持 FALSE：不支持 not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码；Collaborator（协作者）使用主账号身份登录，不涉及该项
LoginProtectionActive	登录保护是否启用	TRUE：已启用 FALSE：未启用 not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码
OperationProtectionActive	操作保护是否启用	TRUE：已启用 FALSE：未启用 not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码
MFADeviceActive	MFA 是否启用	TRUE：已启用 FALSE：未启用 not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码；Sub-user（子用户）未绑定联系方式（手机、微信）
Abnormal LoginsNumWithin30Days	30天内异登录	TRUE：存在异常登录 FALSE：未存在异常登录
AccessKey1SecretId	密钥1 SecretId	N/A：无密钥
AccessKey1MayBeAtRisk	密钥1是否有存在泄漏风险	TRUE：存在泄漏风险 FALSE：无风险 N/A：无密钥1 not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码

AccessKey1CreationTime	密钥1创建时间	N/A：无密钥1 not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码
AccessKey1Status	密钥1状态	Active：已启用 Disable：已禁用 N/A：无密钥1 not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码
AccessKey1lastUsedDate	密钥1最后一次使用时间	N/A：无密钥1 not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码
AccessKey1CreatedOver90Days	密钥1创建是否超过90天	N/A：无密钥1 not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码
AccessKey1CreatedOver30Days	密钥1创建是否超过30天	N/A：无密钥1 not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码
AccessKey2SecretId	密钥2 SecretId	N/A：无密钥2
AccessKey2MayBeAtRisk	密钥2是否有存在泄漏风险	TRUE：存在泄漏风险 FALSE：无风险 N/A：无密钥 2 not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码
AccessKey2CreationTime	密钥2创建时间	N/A：无密钥 2 not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码
AccessKey2Status	密钥2状态	Active：已启用 Disable：已禁用 N/A：无密钥 2 not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码
AccessKey2lastUsedDate	密钥2最后一次使用时间	N/A：无密钥 2 not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码
AccessKey2CreatedOver90Days	密钥2创建是否超过90天	N/A：无密钥2

		not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码
AccessKey2CreatedOver30Days	密钥2创建是否超过30天	N/A：无密钥2 not_supported：不涉及，Message-receiver（消息接收人）仅用于接受消息，无登录密码