访问管理

实践教程

腾讯云

文档目录

实践教程
安全实践教程

最近更新时间：2025-04-11 15:17:11

安全设置概述

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

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

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

登录安全

1. 使用子账号访问腾讯云

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

2. 使用组给子账号分配权限

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

3. 使用不同的子账号管理用户、权限和资源

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

4. 使用子账号访问腾讯云

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

5. 保护 CAM 用户凭证，以防止未经授权的使用

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

身份安全

1. 使用基于角色的访问控制

CAM 的角色是一种虚拟用户，与子账号、协作者或接收消息者这类实体用户不同。角色同样可被授予策略，使用基于角色的访问控制，根据实际场景进行合适的角色分配。详情请参见 角色概述 。
腾讯云账号、产品服务、产品资源（例如工作负载、实例等）身份提供商等均可作为角色载体，角色并不是唯一地与某个账号绑定关联。角色没有关联的持久证书（密码或访问密钥），主账号仅在申请角色时需要使用持久证书，在用户担任某个角色时，则会动态创建临时证书并为用户进行相应访问时提供该临时证书，即可通过临时密钥签名调用腾讯云基础服务的开放 API 来访问用户的云资源。

2. 勿为根用户创建访问密钥

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

3. 降低特权账户的泄露风险

通过如下方式降低特权云账户的泄露风险：

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

4. 为用户开启 SSO 单点登录功能

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

5. 确保账户恢复机制可访问

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

权限安全

1. 最小权限原则

最小权限原则是一项标准的安全原则。即仅授予执行任务所需的最小权限，不要授予更多无关权限。例如，一个用户仅是 CDN 服务的使用者，那么不需要将其他服务的资源访问权限（如 COS 读写权限）授予给该用户。

2. 为 CAM 用户配置强密码策略

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

3. 不要为腾讯云主账号创建访问密钥

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

4. 开启 MFA 保护

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

5. 定期轮换身份凭证

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

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

密钥安全

1. 删除不需要的证书和权限

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

2. 启用条件访问

云上用户可能会从任意位置访问云上资源。 因此需要确保这些访问符合安全性。 仅从用户身份认证角度关注是否可访问资源并不全面。还应考虑谁（身份）可以且如何（条件）访问资源。
常见的方式是通过 CAM Policy 中自定义策略 condition 条件来限制子账号访问条件，例如限制访问 IP，设置成功后，子账号将通过所设置的 IP 管理主账号下的资源，或者拒绝子账号通过设置的 IP 管理主账号下资源，详情请参见 限制 IP 访问 。

3. 使用策略条件来增强安全性

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

审计安全

1. 监控 CAM 账号的操作记录

您可以使用 腾讯云操作审计 的日志记录功能来确定 CAM 用户在您的账户中进行了哪些操作，以及使用了哪些资源。日志文件会显示操作的时间和日期、操作的源 IP、哪些操作因权限不足而失败等。相关信息请参见 查看操作记录 。
遵循最佳安全设置建议，在使用腾讯云时，综合利用这些保护机制，建立安全完善的资源控制体系，可以更有效地保护账号及资产的安全。

更多信息

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

授予标签下部分操作权限

最近更新时间：2024-10-11 17:33:22

操作场景

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

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

操作步骤

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

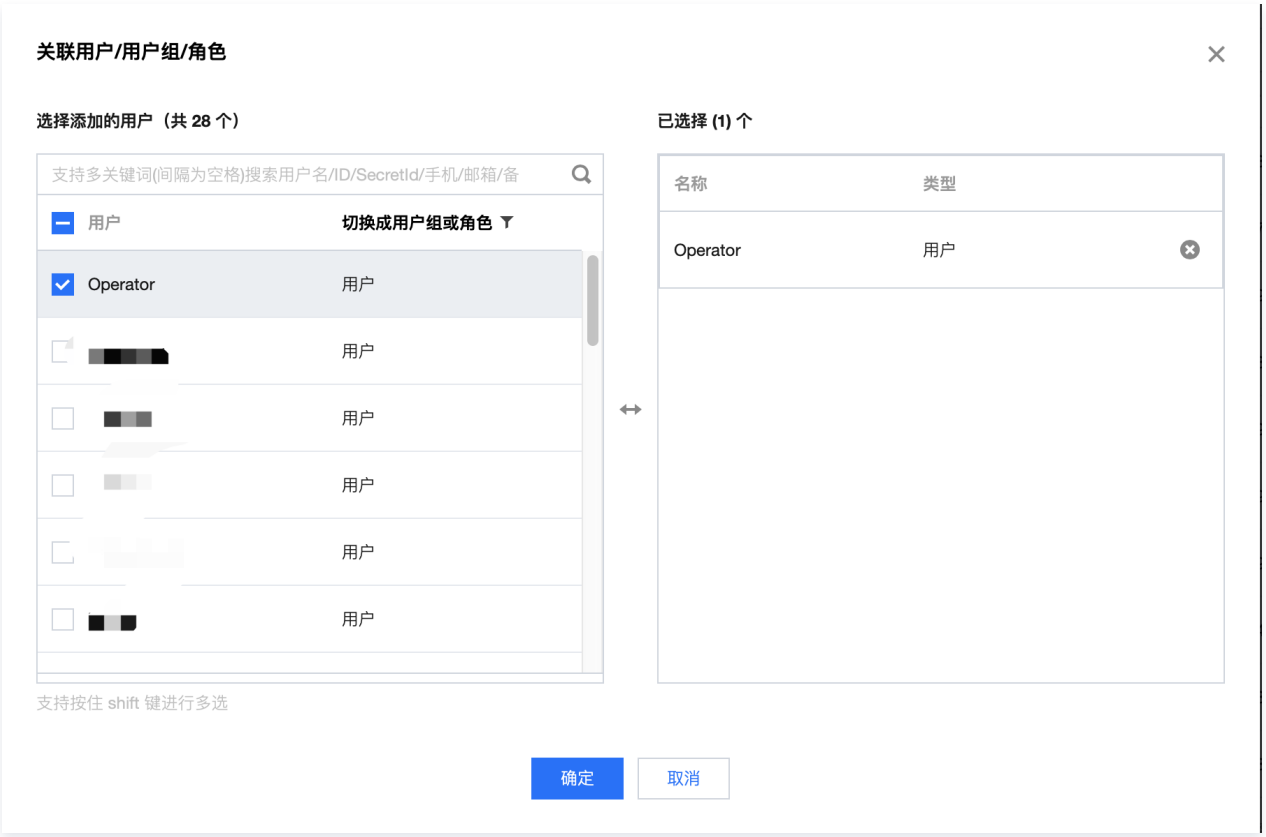
4. 进入编辑策略页面，填写如下表单：
   - 策略名称：默认为 `policygen-当前日期` ，推荐您自行定义一个不重复且有意义的策略名称，例如 cvm-RebootInstances。
   - 描述：可选，自行编写。
   - 策略内容：复制以下内容并填写。其中， `cvm:RebootInstances` 为需要授权操作的接口名称，Operator&activity 为需要授权操作的标签键及标签值。

```
{
"version": "2.0",
"statement": [
    {
        "effect": "allow",
        "action": [
            "cvm:RebootInstances"
        ],
```

```
        "resource": "*",
        "condition": {
            "for_any_value:string_equal": {
                "qcs:tag": [
                    "Operator&activity"
                ]
            }
        }
    }
]
}
```

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

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



关联文档

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

使用 ADFS 进行用户 SSO 的示例

最近更新时间：2024-12-10 17:36:54

操作场景

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

前提条件

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

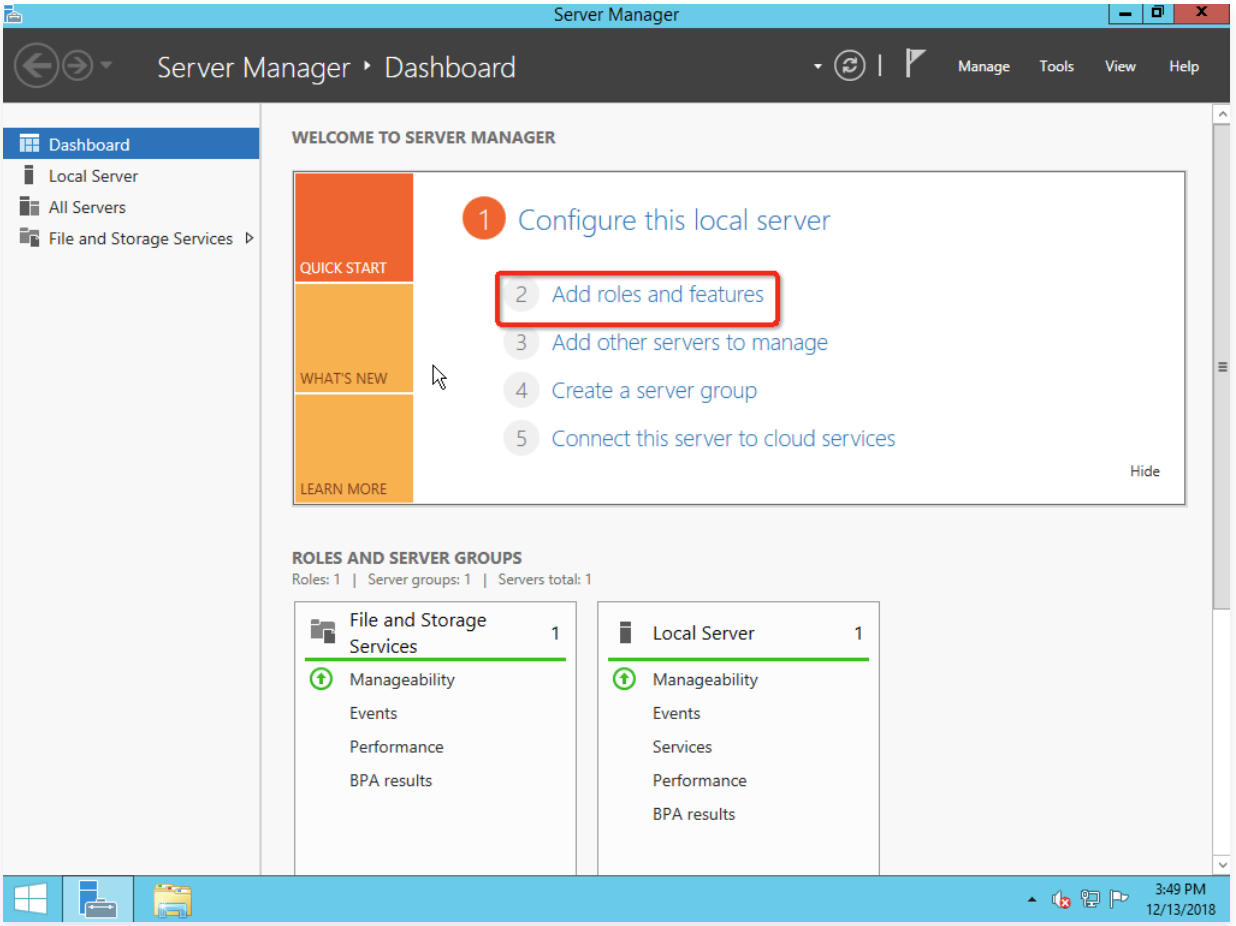
> **说明：**
> 本文中涉及到 Microsoft Active Directory 配置的部分属于建议，仅用于帮助理解腾讯云 SSO 登录的端到端配置流程，腾讯云不提供 Microsoft Active Directory 配置的咨询服务。

操作步骤

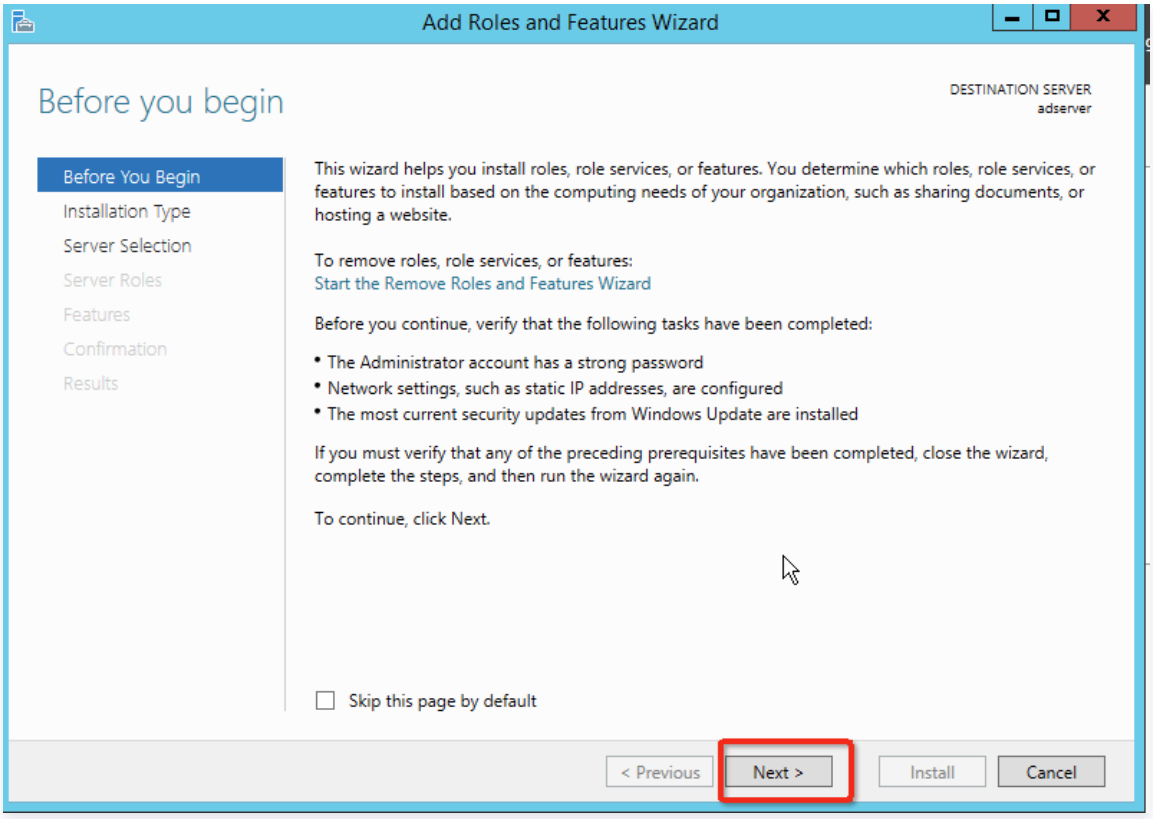
安装部署 Microsoft AD

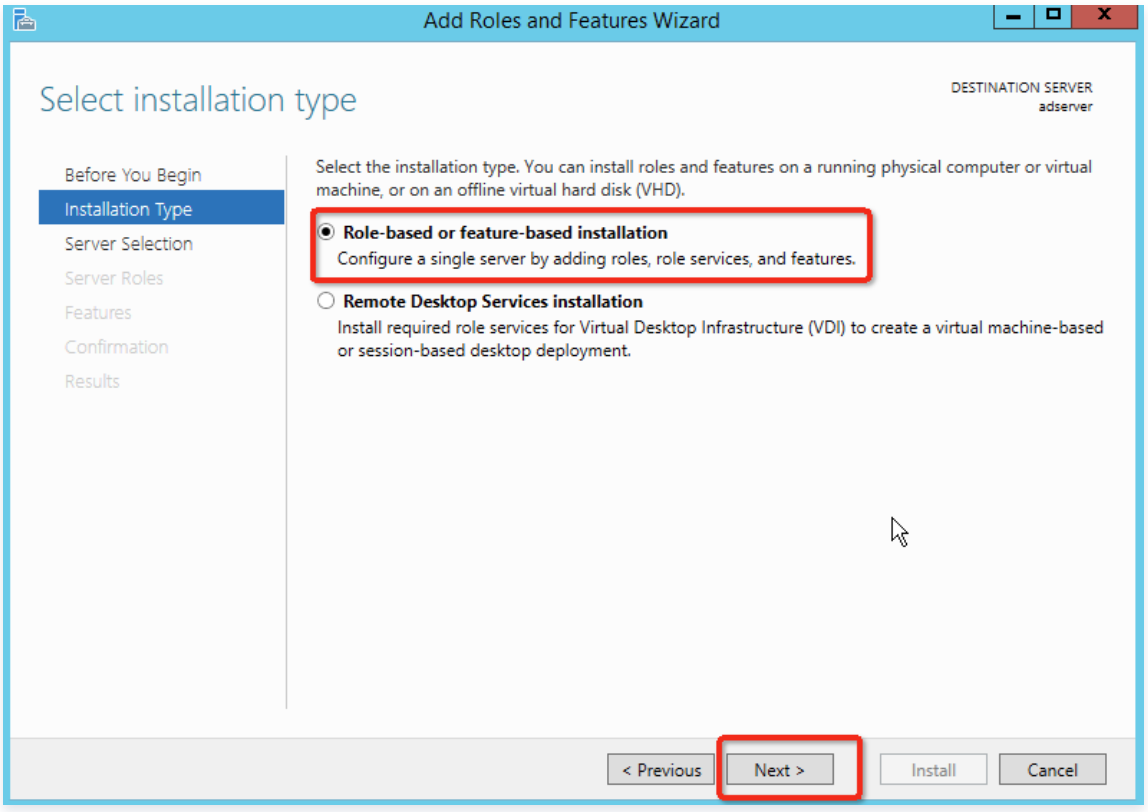
> **说明：**
> 如您已安装部署 Microsoft AD，可忽略步骤1-5，从 步骤6 开始操作。

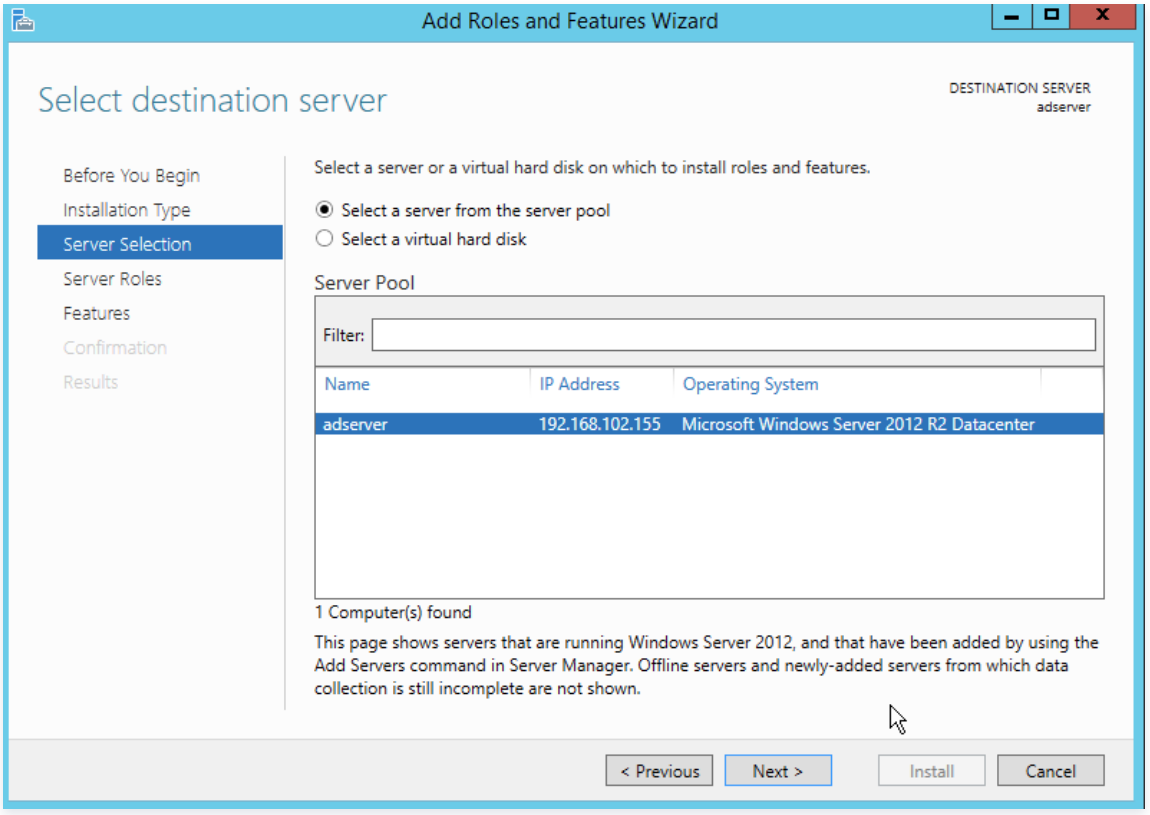
1. 在云服务器内，进入 **Server Manager** > **Dashboard**，单击 **Add roles and features**，如下图所示：

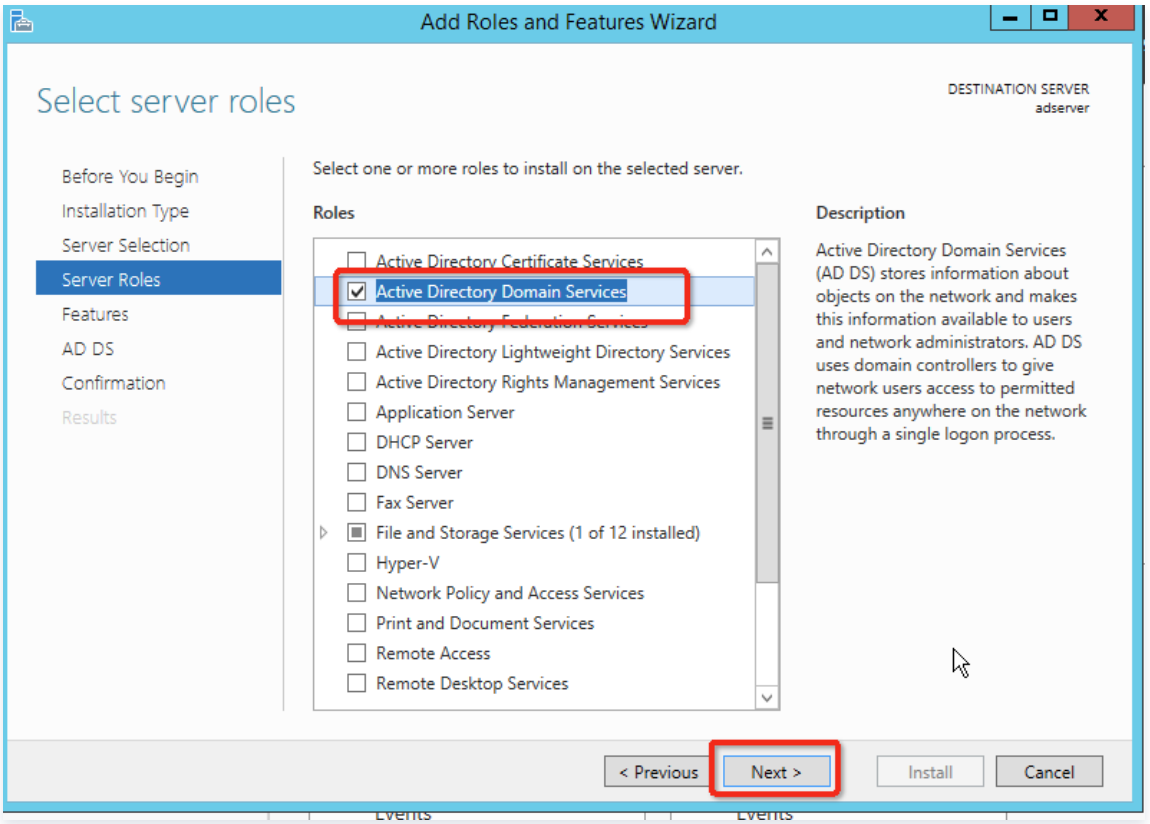


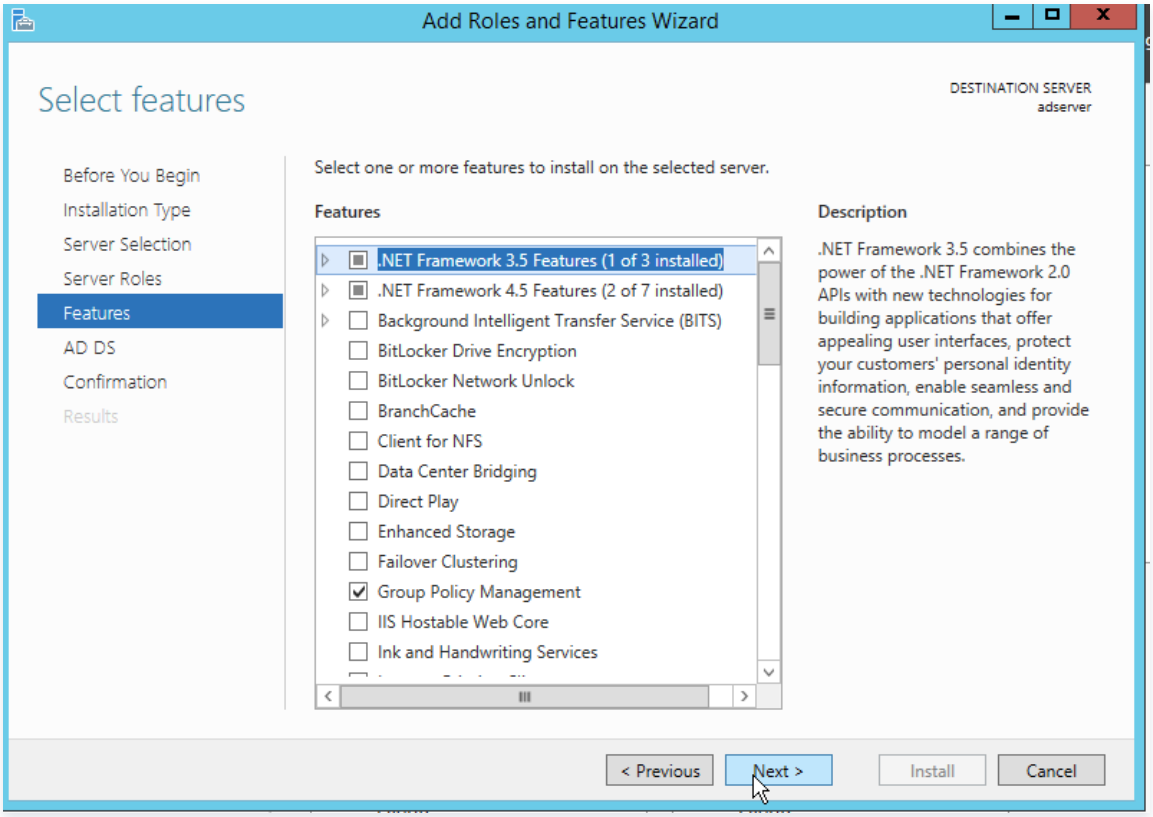
2. 一直单击 **Next** 直到单击 **Install** 完成安装，如下图所示：



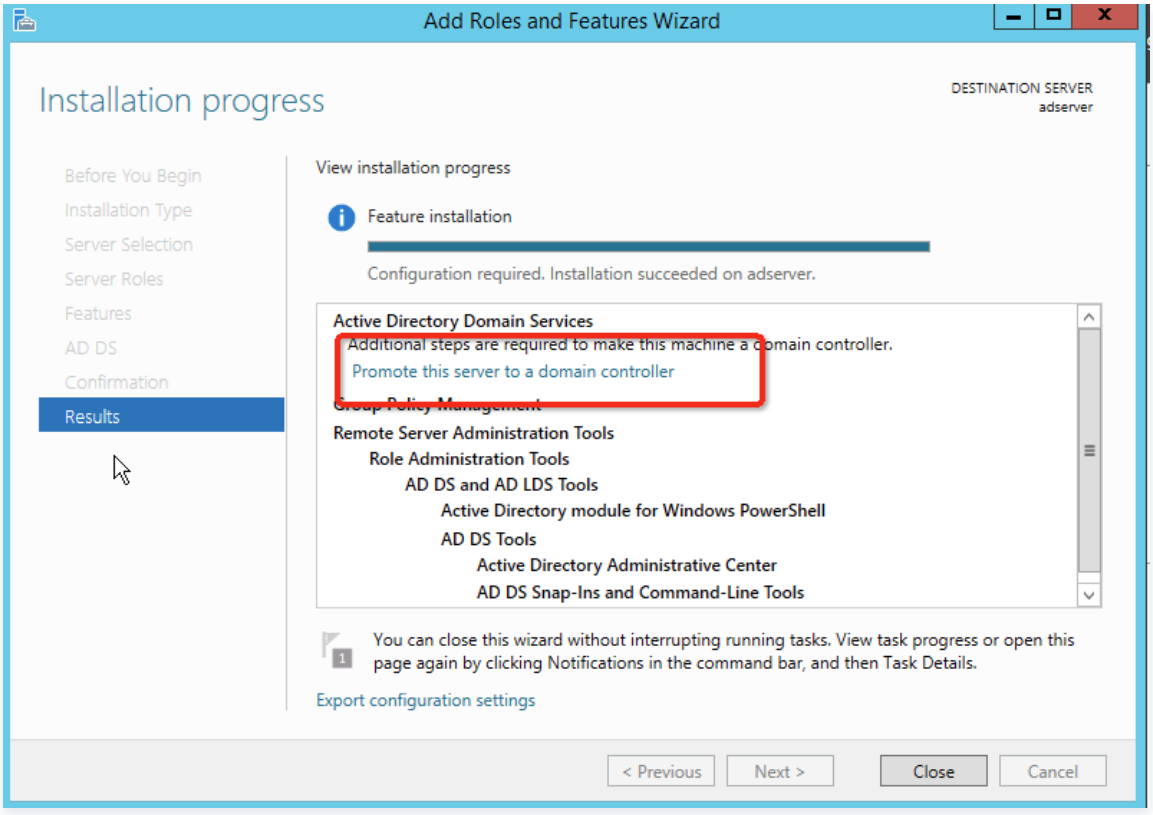



Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
adserver
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
adserver
192.168.102.155
Microsoft Windows Server 2012 R2 Datacenter
1 Computer(s) found
This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel

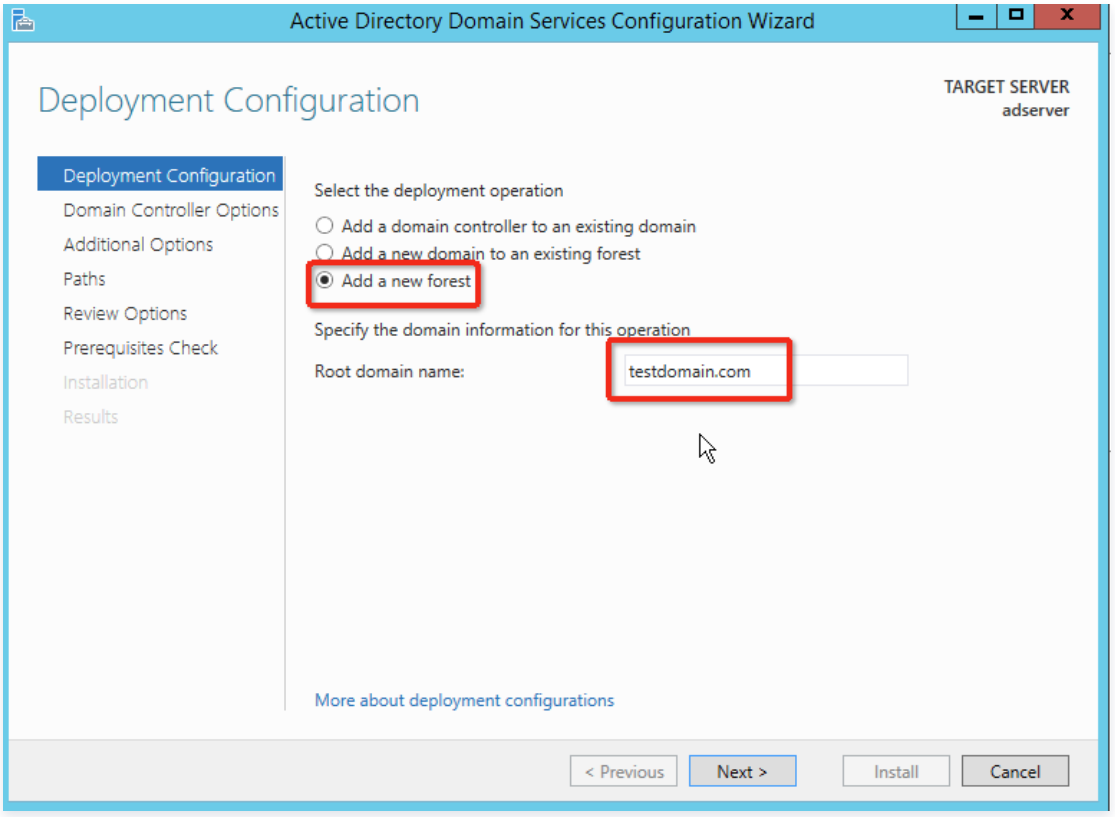

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
adserver
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Description
Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
< Previous
Next >
Install
Cancel



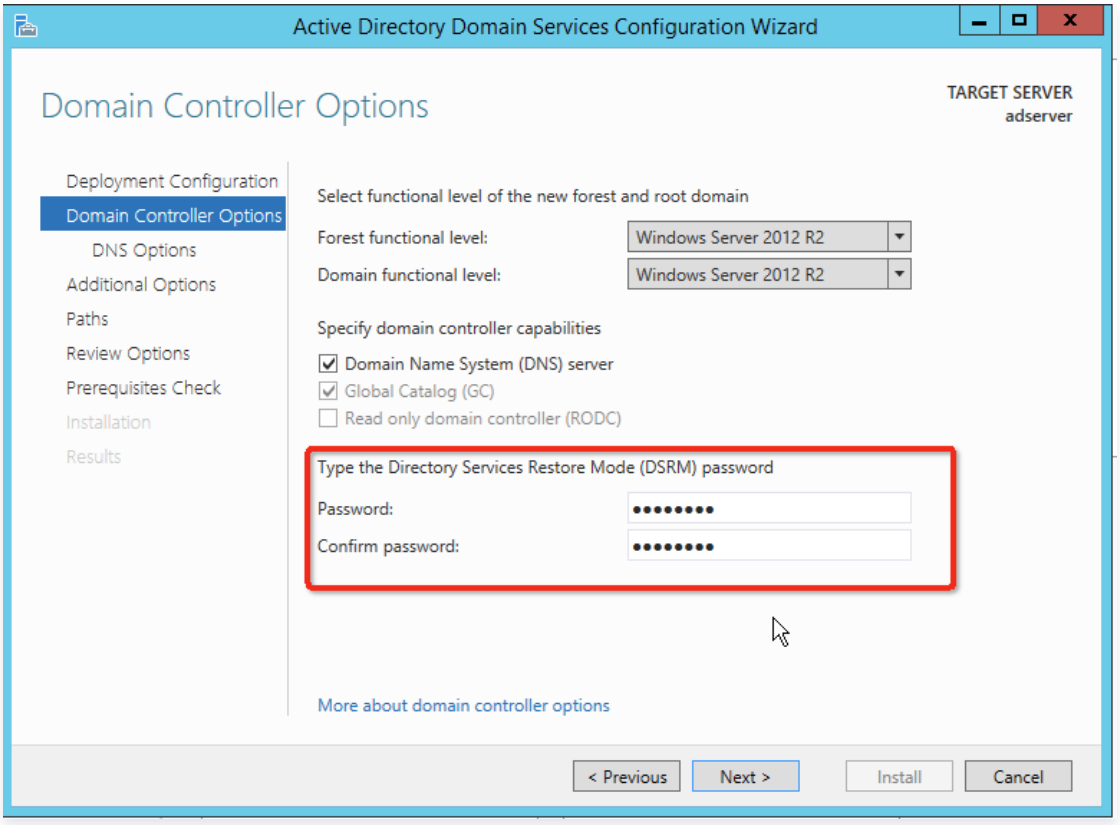
3. 安装完成后单击 **Promote this server to a domain controller**，如下图所示：



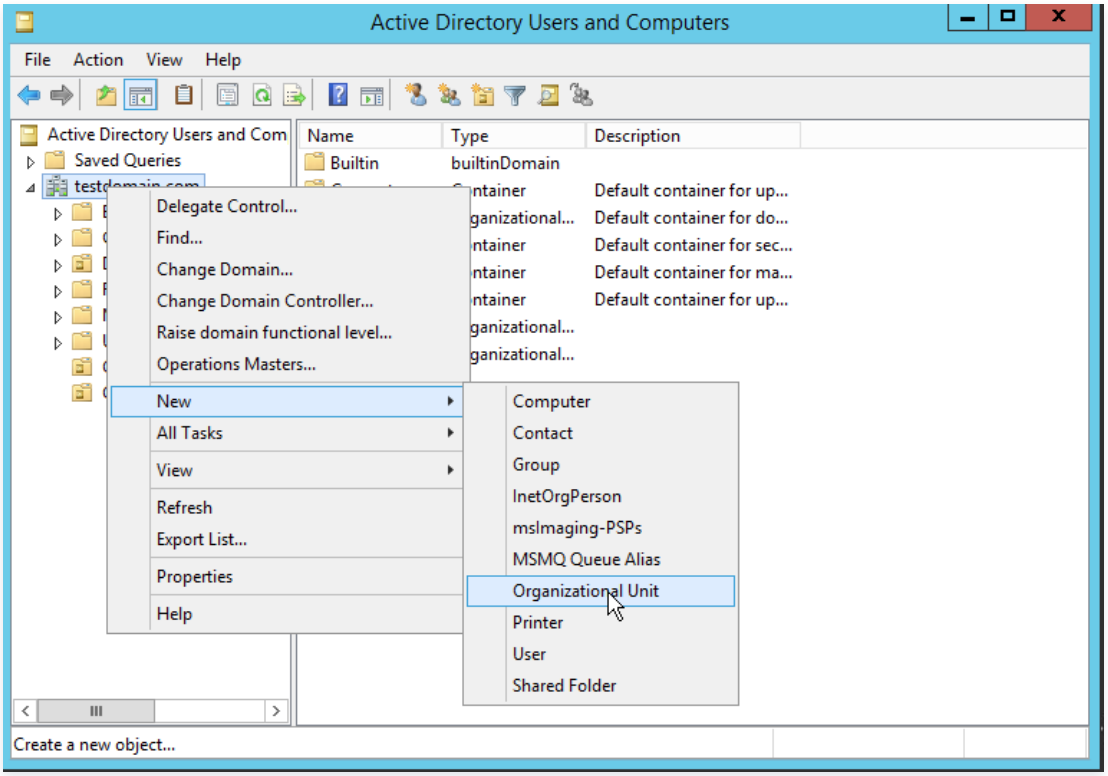
4. 在 Deployment Configuration 页面选择 **Add a new forest** 补充 Root domain name 信息为 testdomain.com，如下图所示：



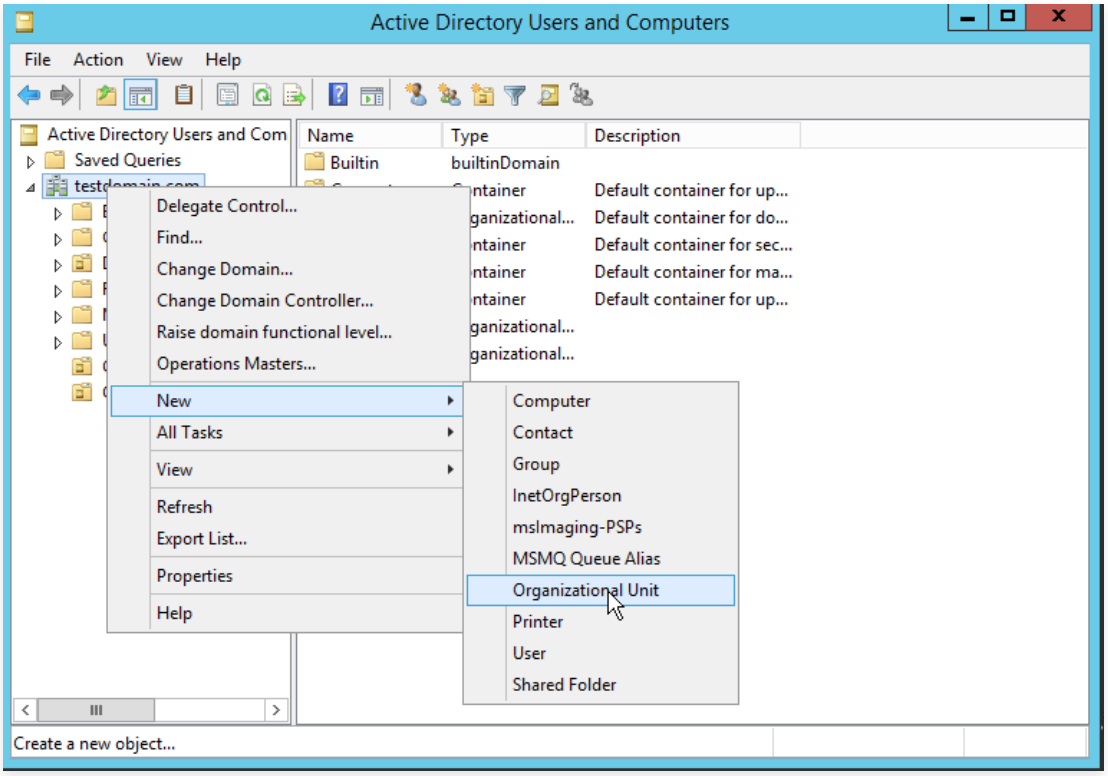
5. 在 Domain Controller Options 中补充 Password 信息，如下图所示，完成后一直单击**Next**，单击 **Install** 完成安装

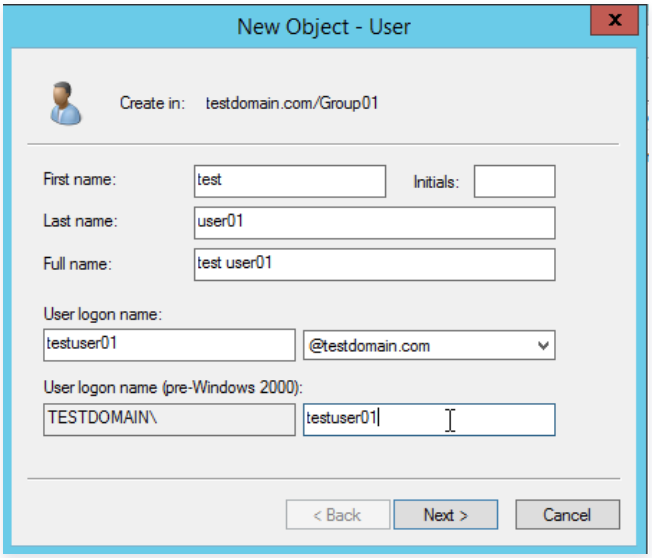


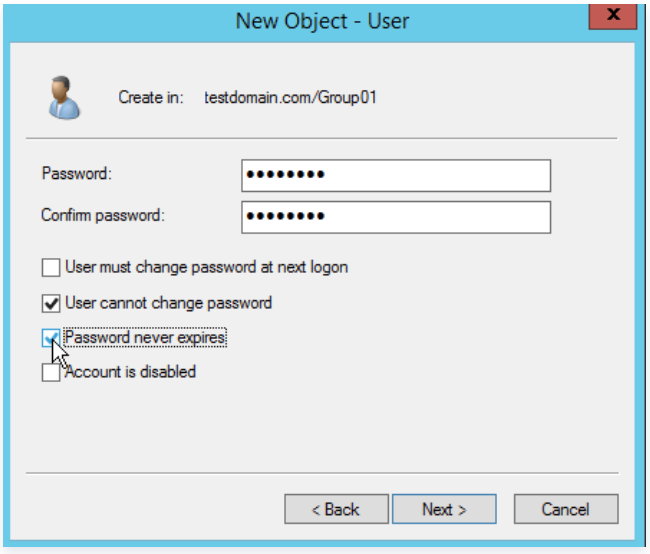
6. 安装完成后，服务器将重启，重启完成后，进入 **Start Menu > Active Directory Users and Computers**，如下图所示：



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

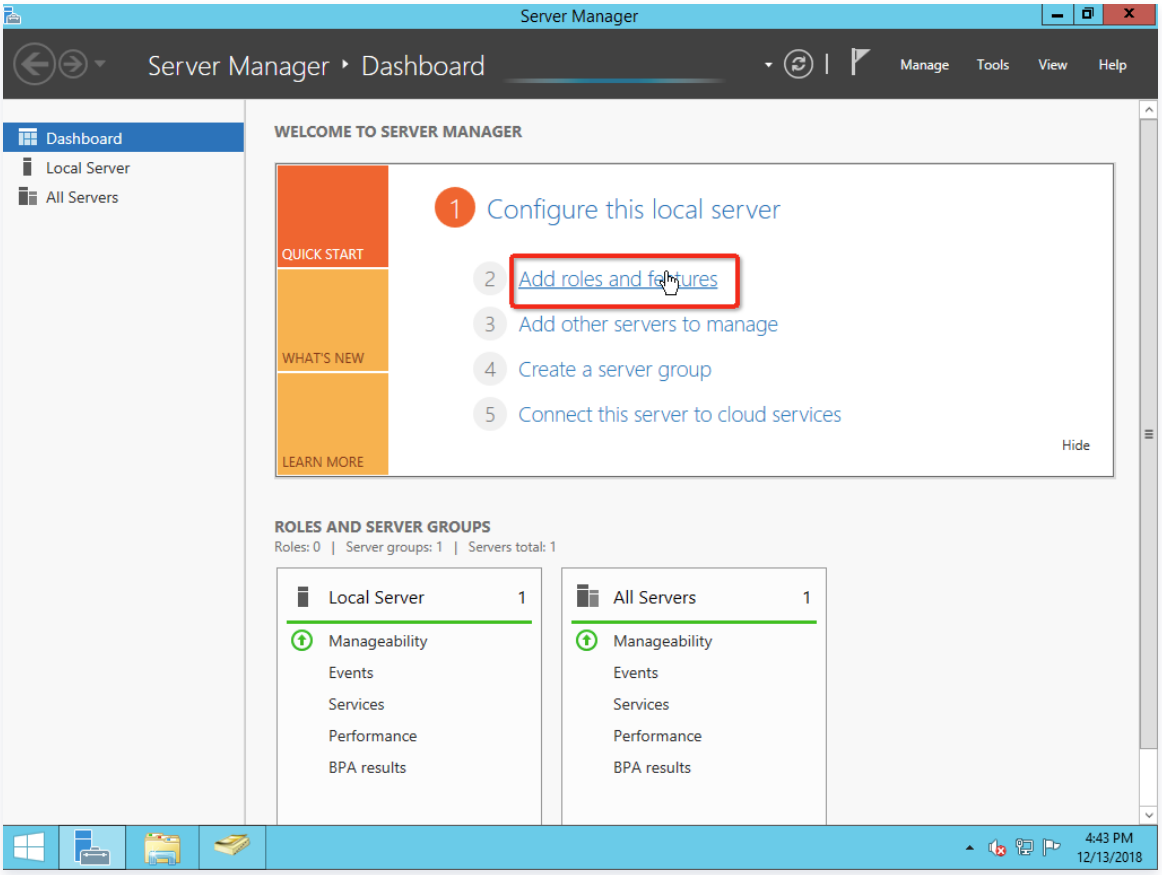




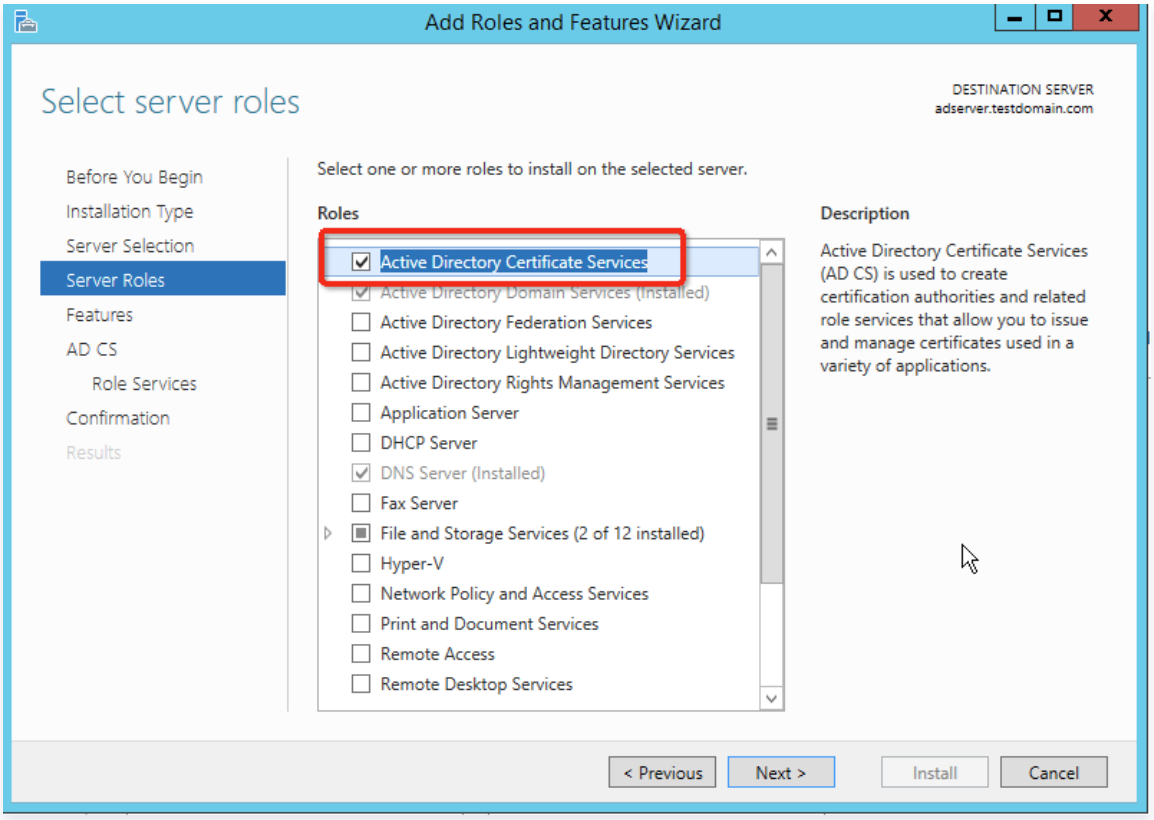


安装 CA

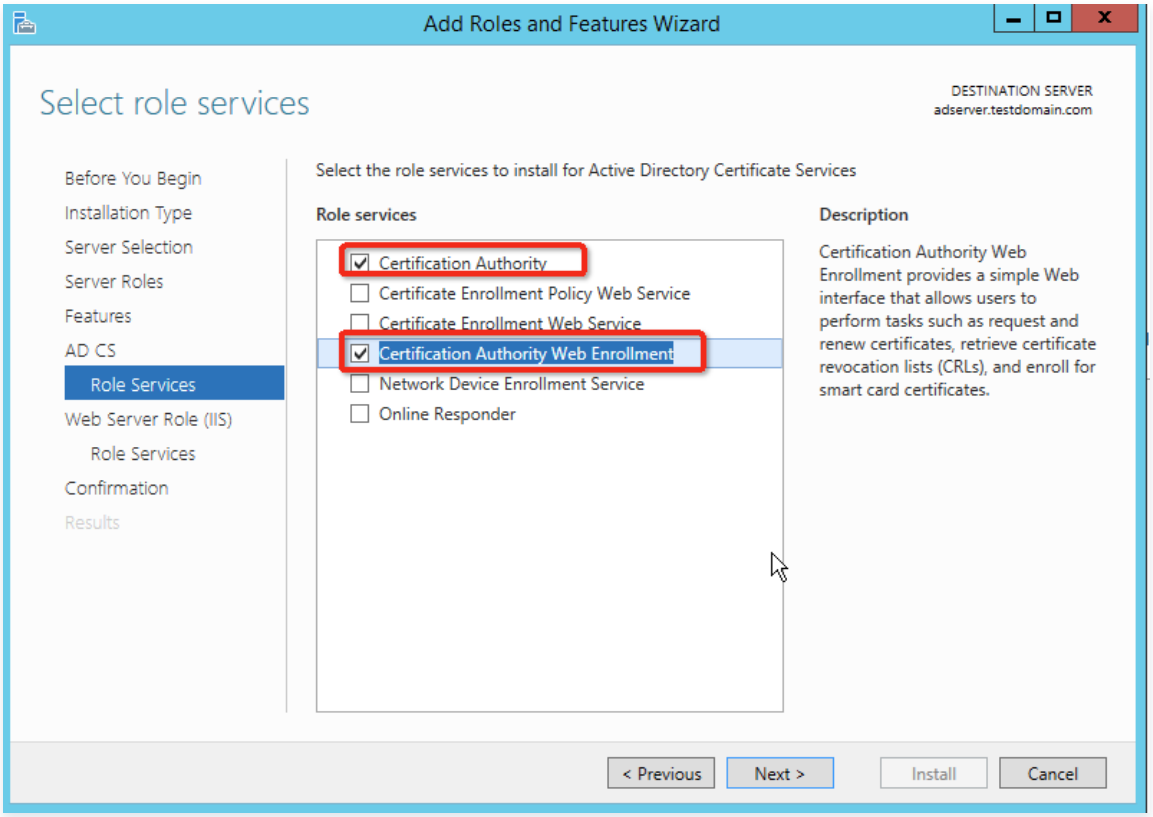
1. 在云服务器内，进入 **Server Manager** > **Dashboard**，单击 **Add roles and features**，如下图所示：



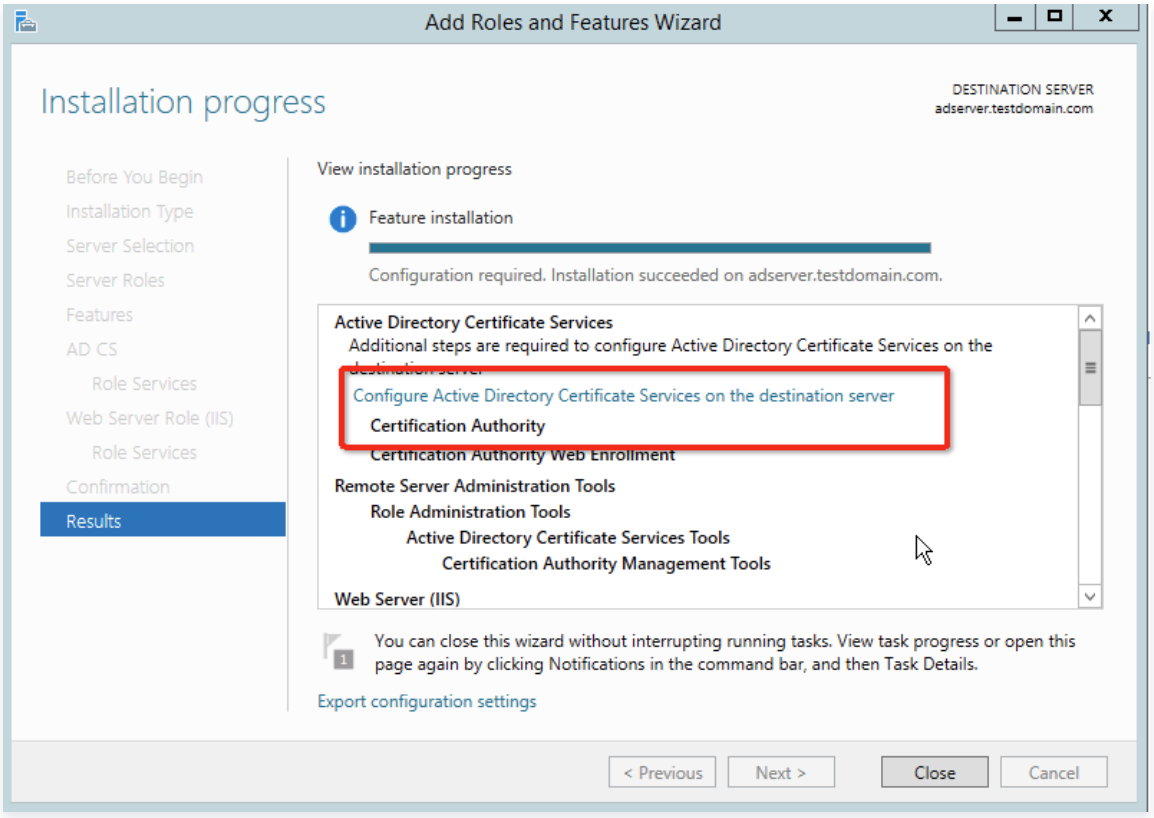
2. 一直单击 **Next** 直到 **Server Roles** 页面，在 **Server Roles** 页面选择 **Active Directory Certificate Services**，如下图所示：

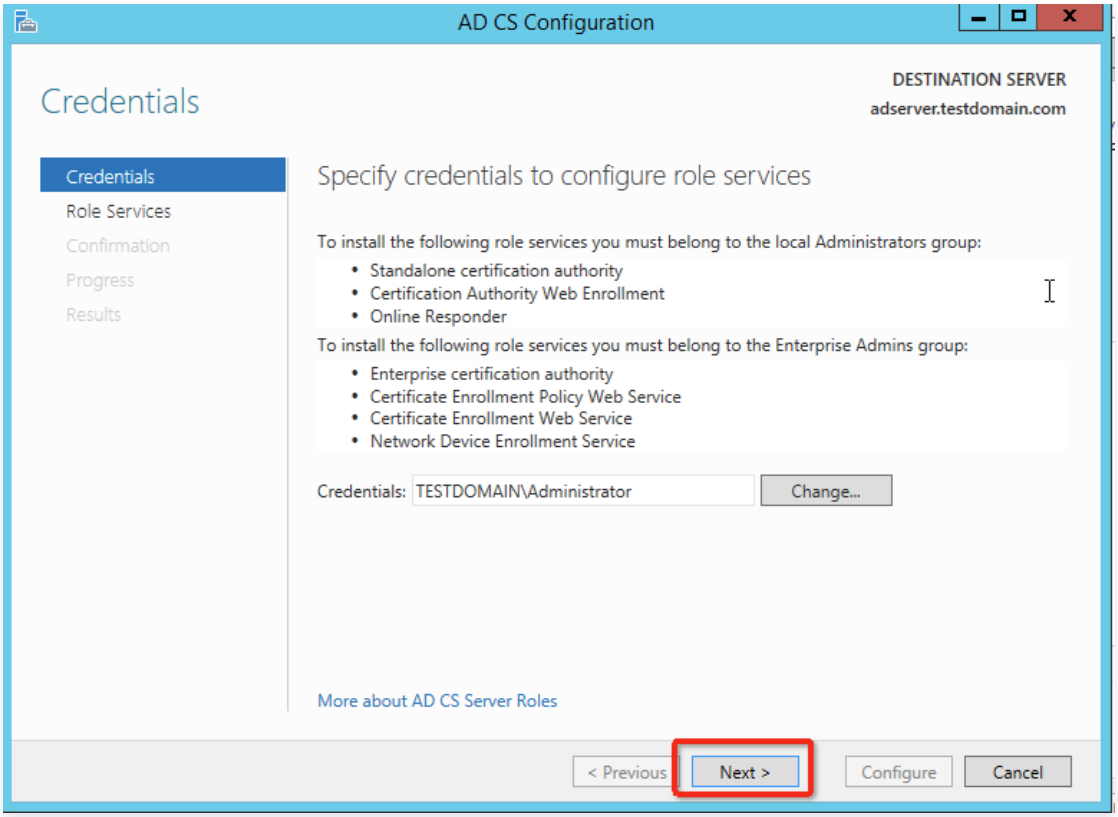


3. 一直单击 **Next** 直到 **AD CS > Role Services** 页面，选择 **Certification Authority**、**Certification Authority Web Enrollment**，如下图所示：

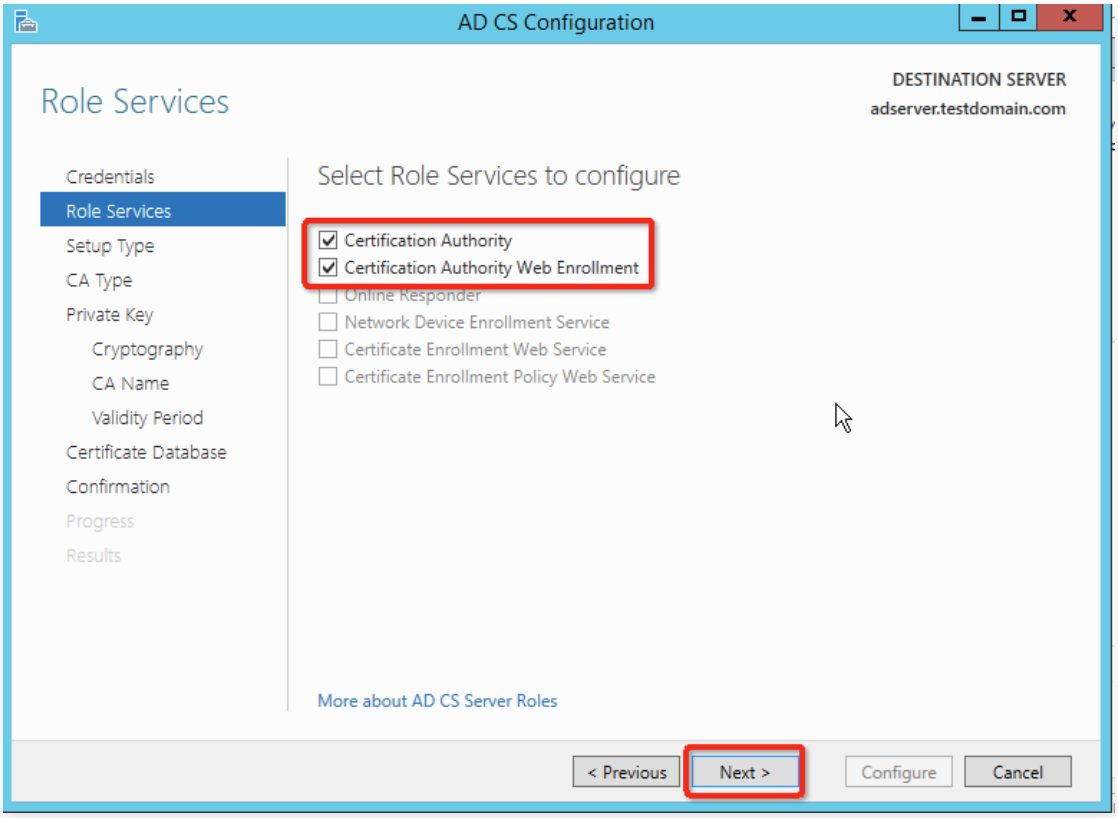


4. **一直单击 Next 直到 Results 页面，单击下图信息配置 AD CS Configuration，如下图所示：**

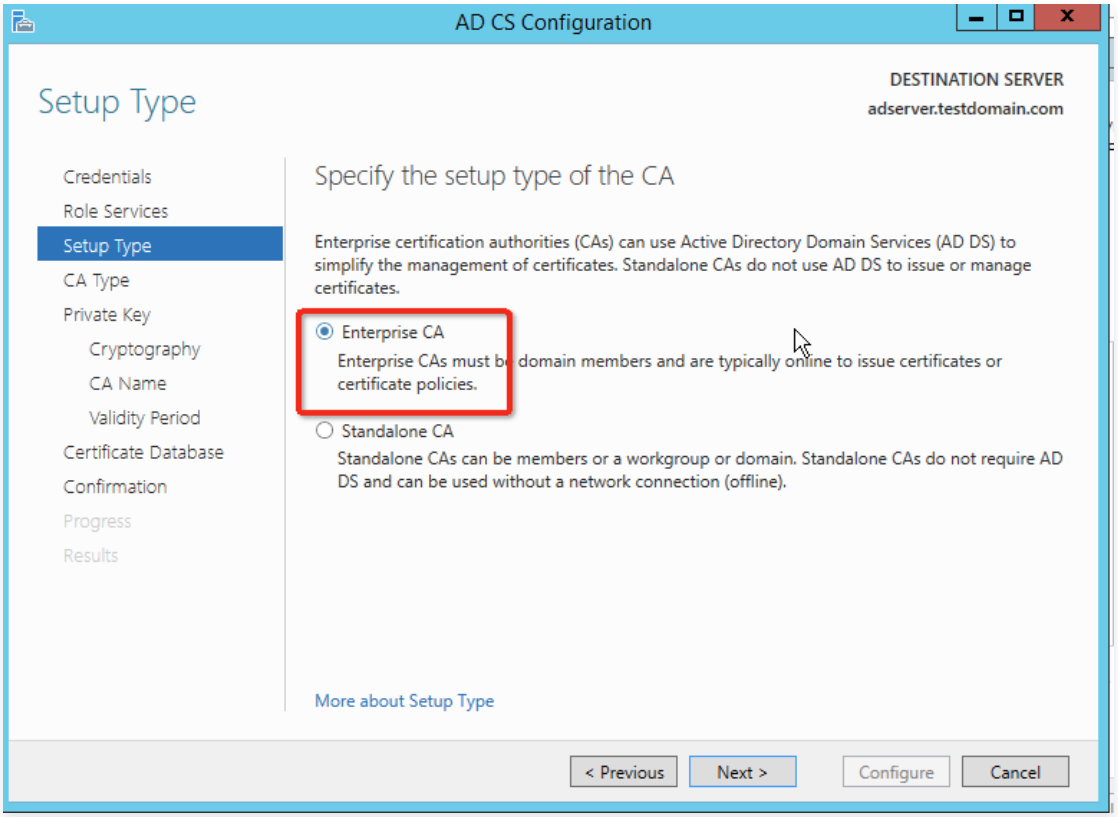




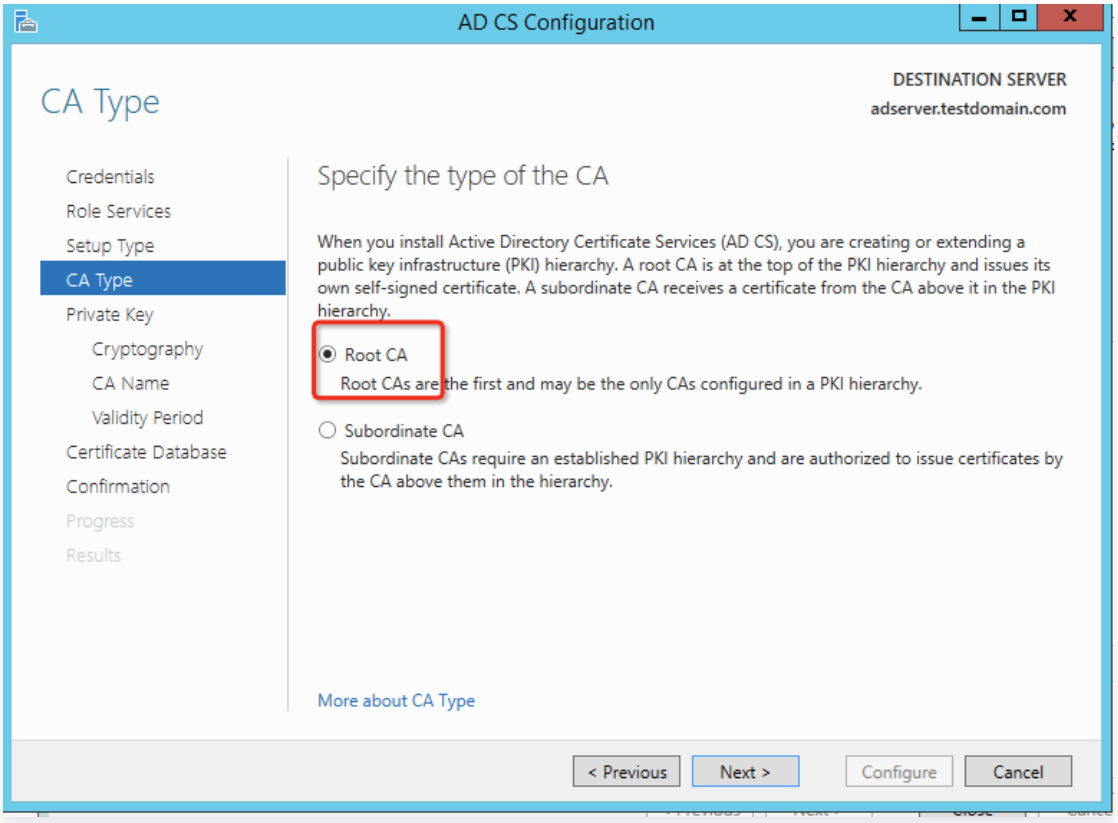
5. 单击 **Next**，在 **Role serveries** 页面，勾选下图信息，单击 **Next**。



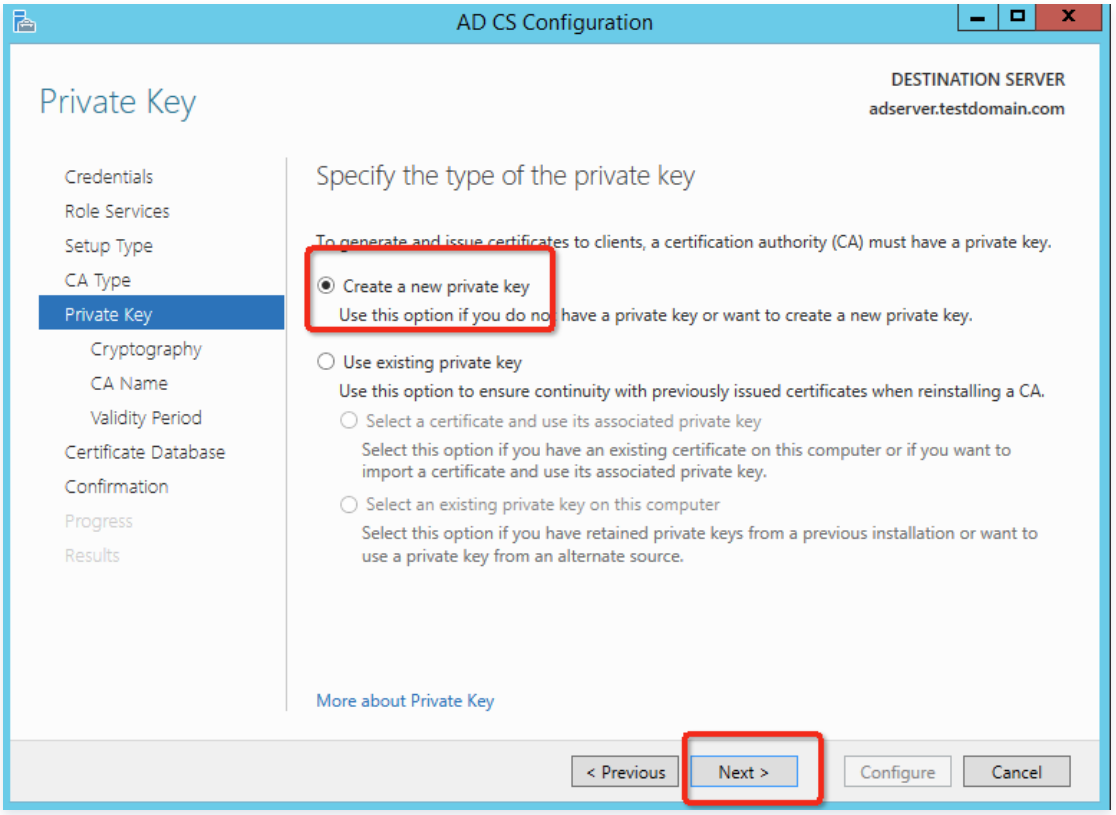
6. 在 **Setup Type** 页面，选择 **Enterprise CA**，如下图所示：

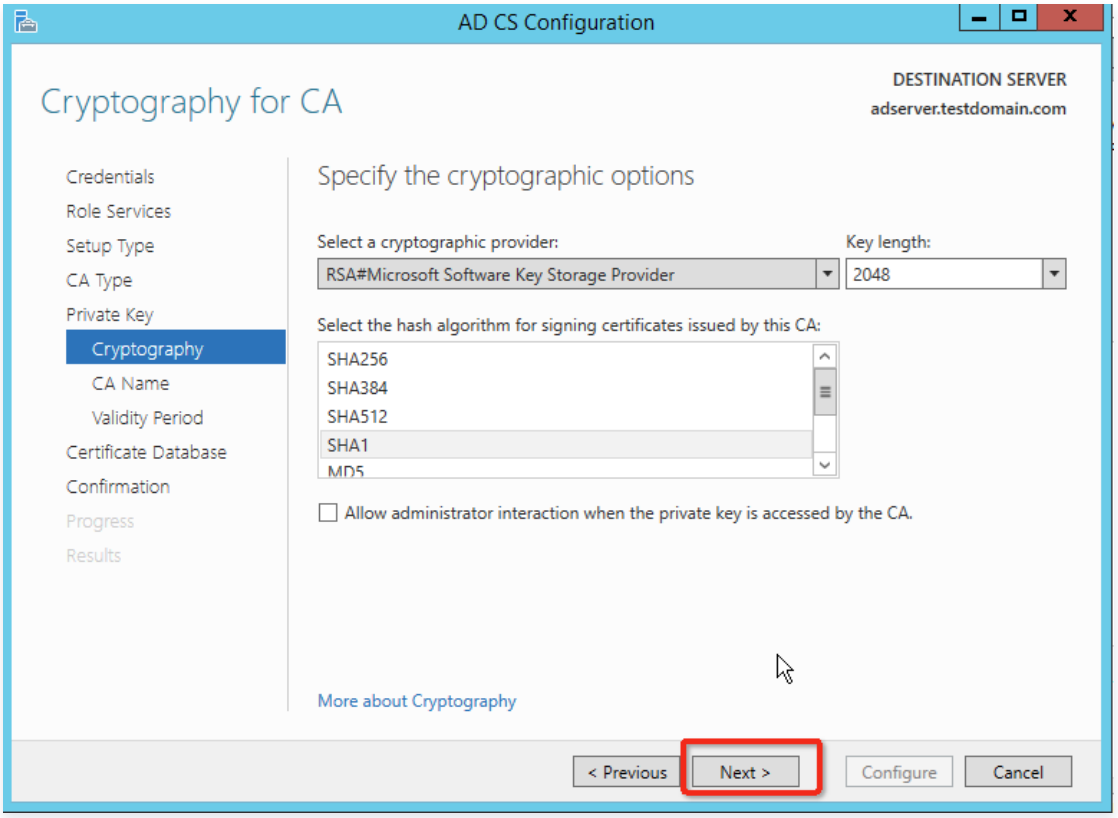


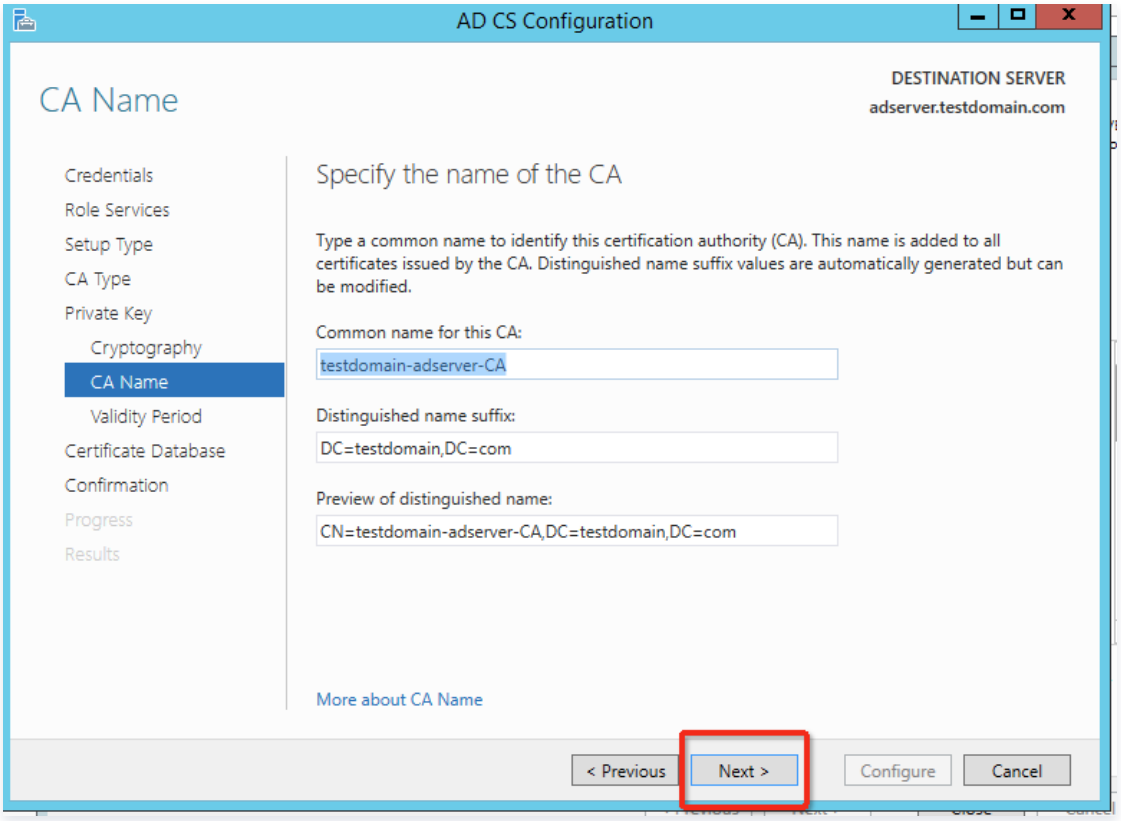
7. 在 **CA Type** 页面，选择 **Root CA**，如下图所示：

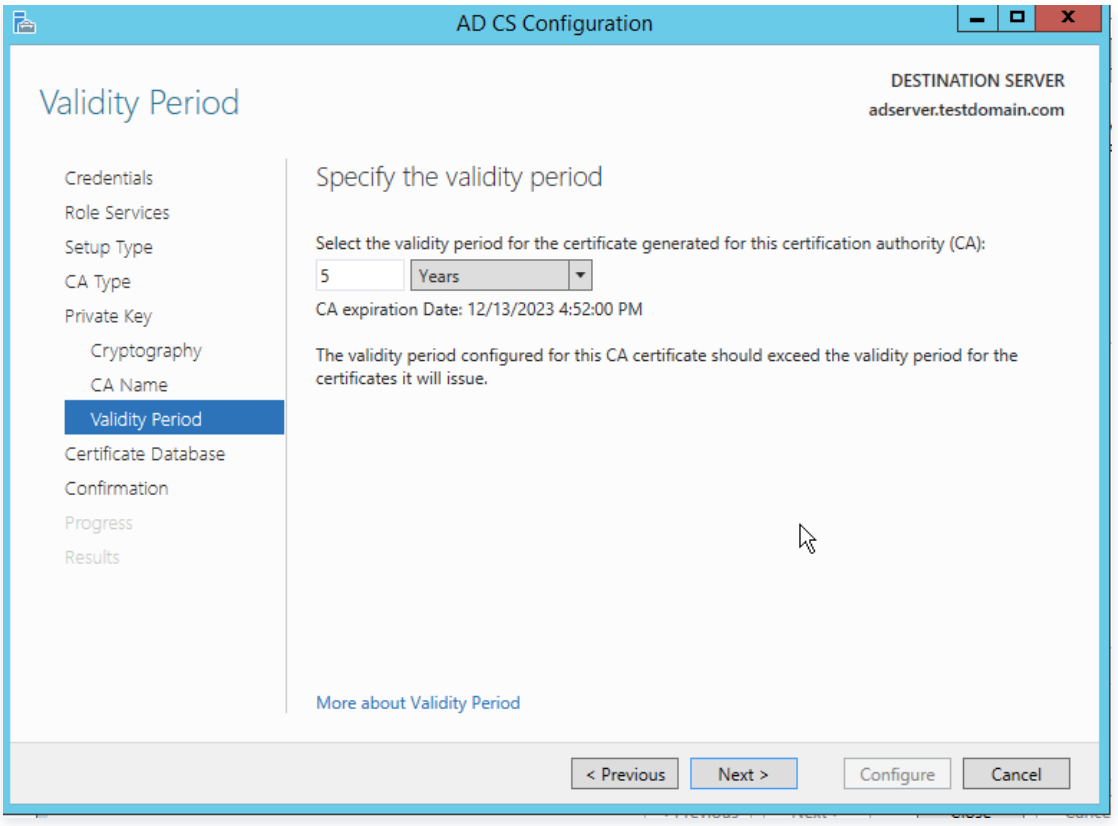


8. 在 **Private Key** 页面，选择 **Create a new private key**，如下图所示：

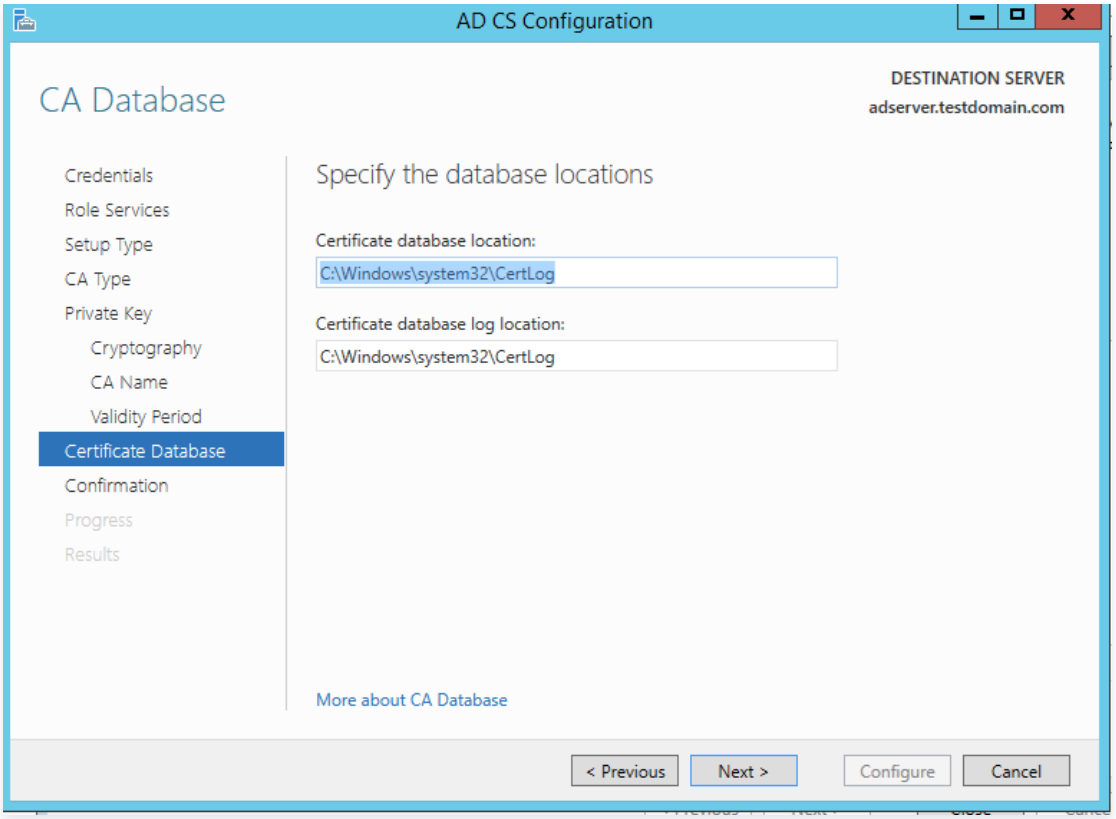

AD CS Configuration
Private Key
DESTINATION SERVER
adserver.testdomain.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the type of the private key
To generate and issue certificates to clients, a certification authority (CA) must have a private key.
Create a new private key
Use this option if you do not have a private key or want to create a new private key.
Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.
Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.
Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.
More about Private Key
< Previous
Next >
Configure
Cancel

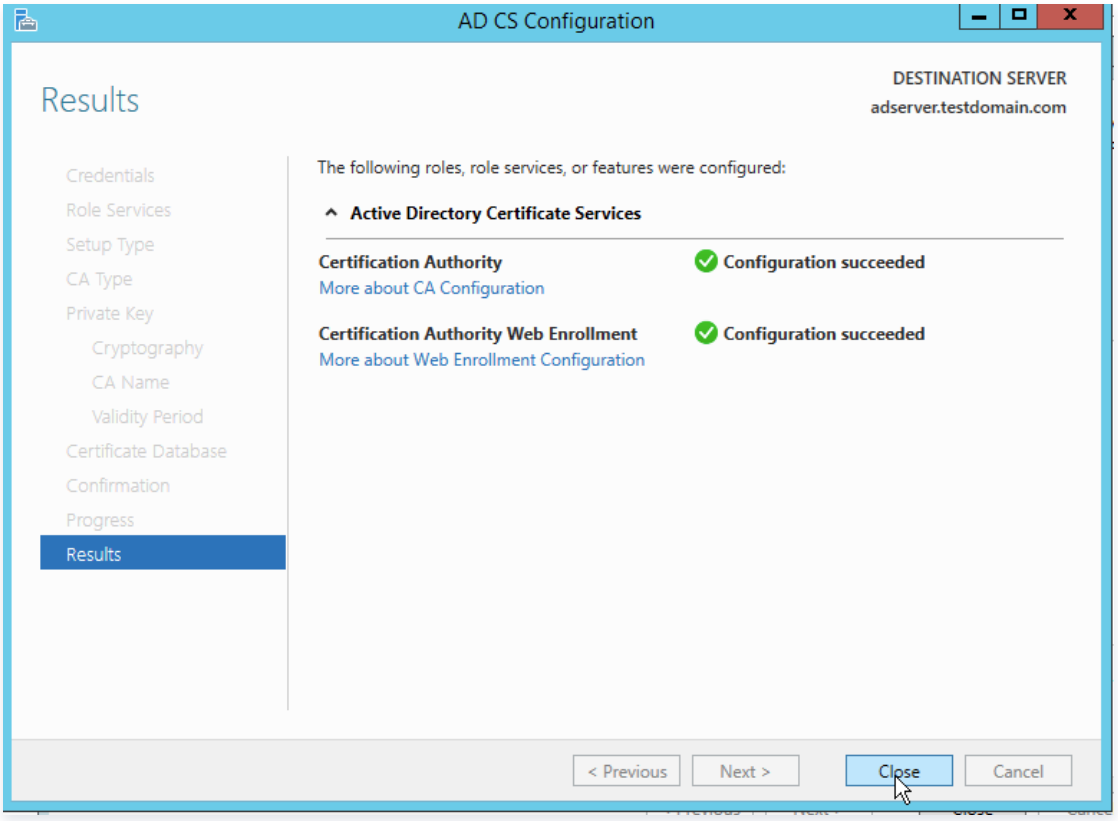

AD CS Configuration
Cryptography for CA
DESTINATION SERVER
adserver.testdomain.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the cryptographic options
Select a cryptographic provider:
RSA#Microsoft Software Key Storage Provider
Key length:
2048
Select the hash algorithm for signing certificates issued by this CA:
SHA256
SHA384
SHA512
SHA1
MD5
Allow administrator interaction when the private key is accessed by the CA.
More about Cryptography
< Previous
Next >
Configure
Cancel



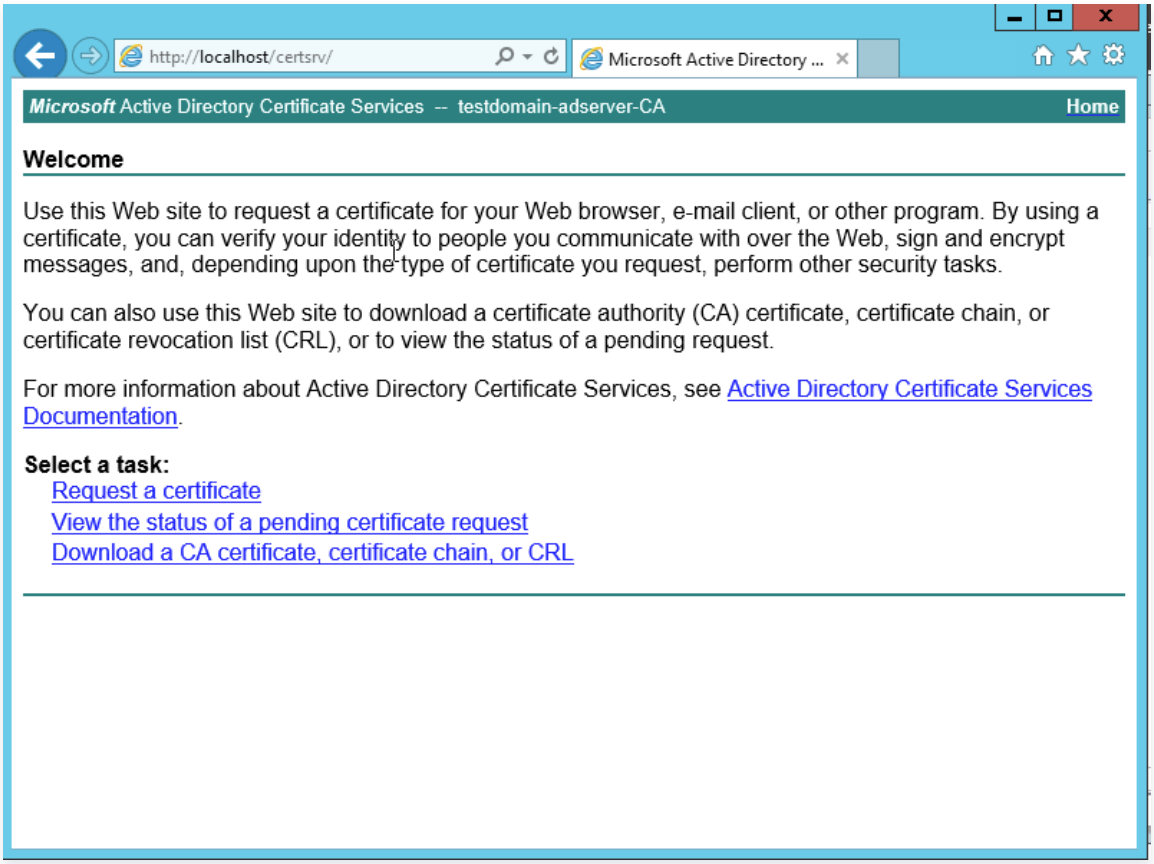


9. 在 **Certificate Database** 页面，补充信息，单击 **Next**，如下图所示：





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

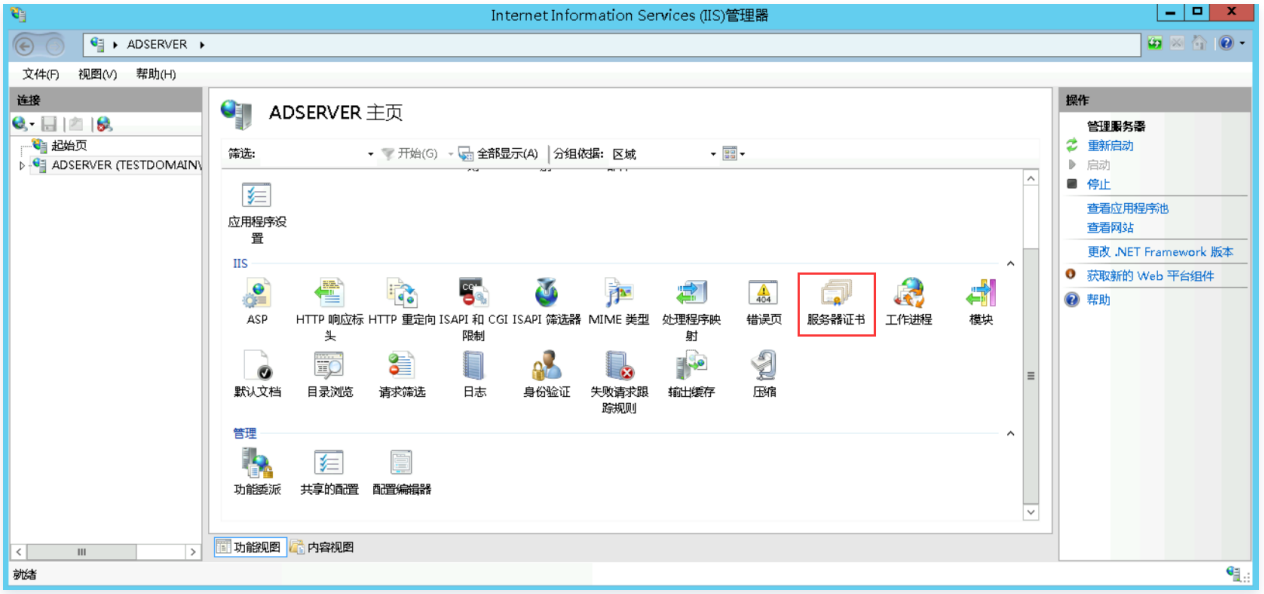


安装 ADFS 服务

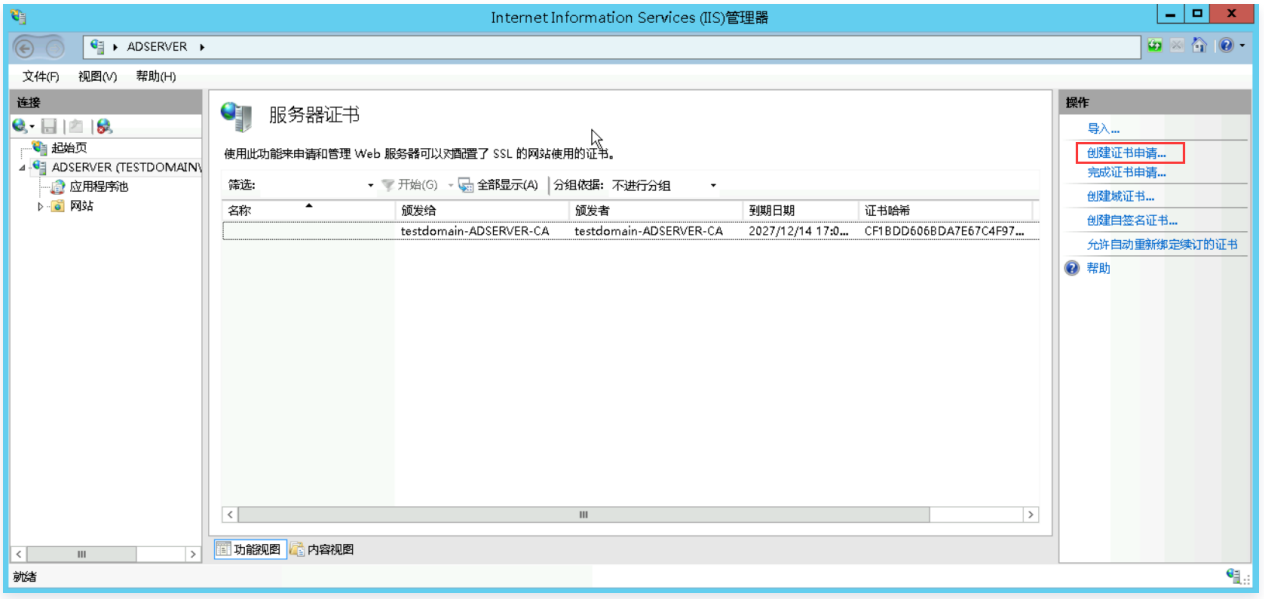
在配置前您需要给计算机或者指定的用户或者计算机授权证书颁发。安装 ADFS 前，需要创建和配置证书，本文中通过 IIS 进行证书申请。

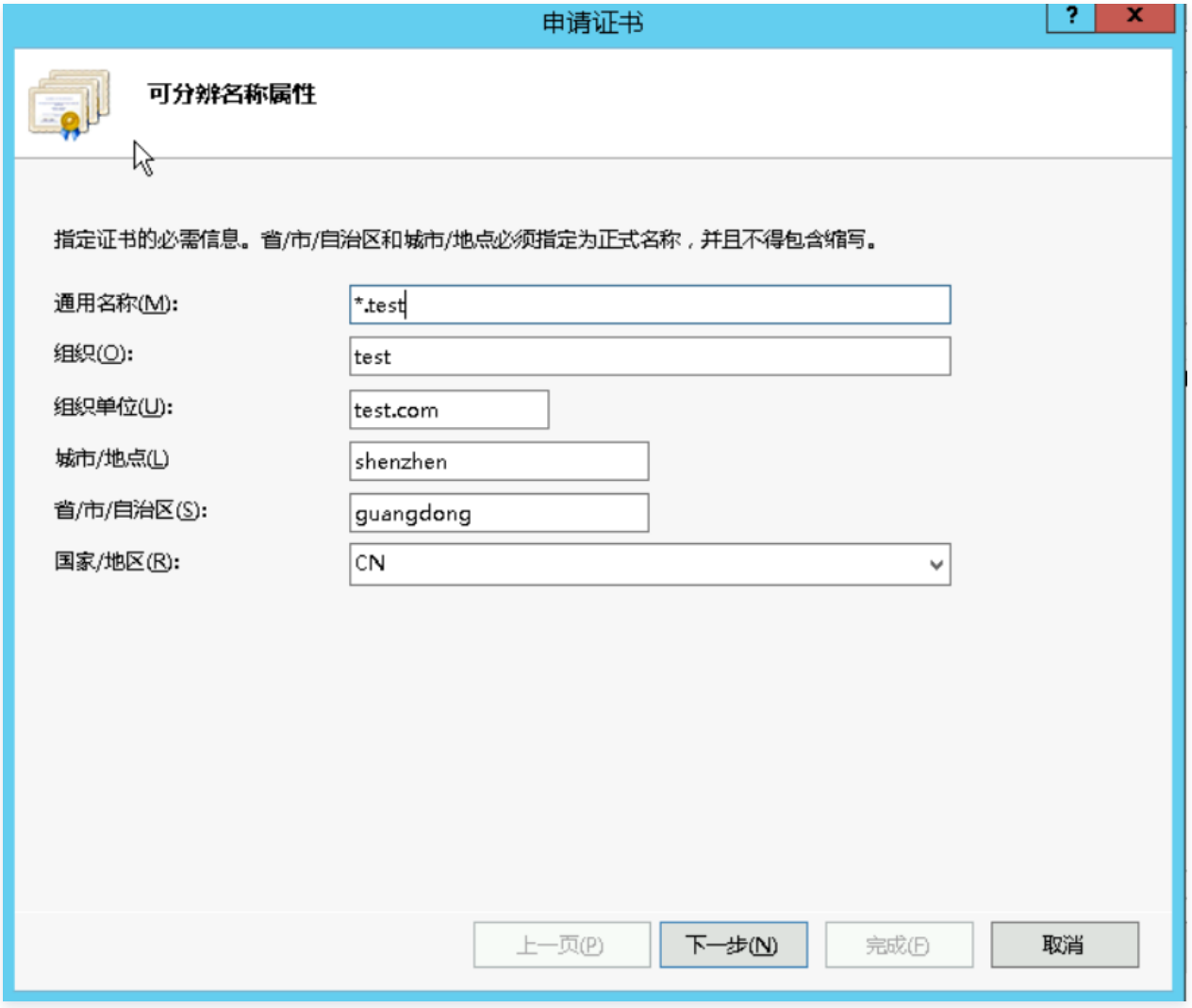
1. 在云服务器内，单击 ，在弹出的窗口单击**工具**，选择 **IIS 管理器**。

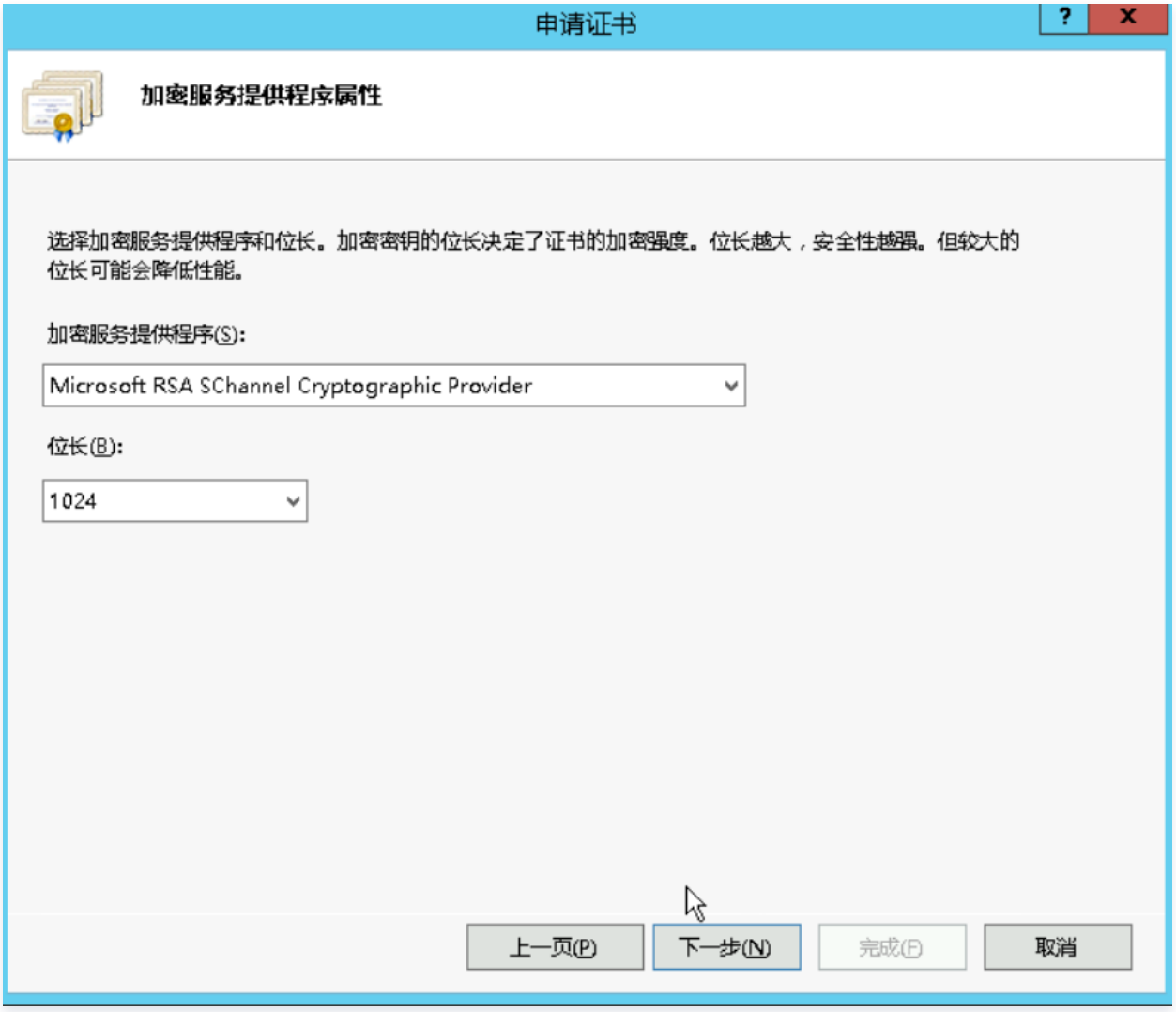
2. 在 IIS 管理器中，单击**服务器证书**，如下图所示：

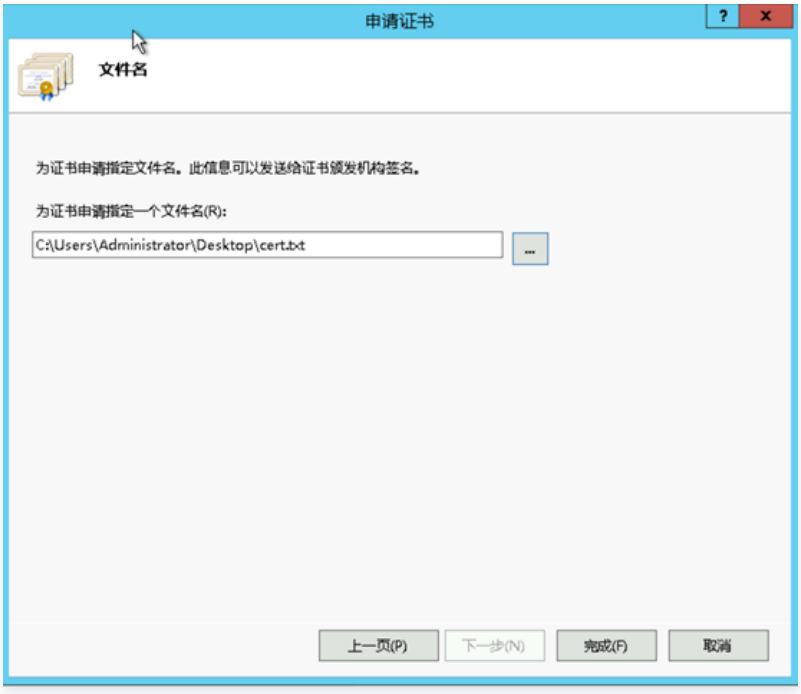


3. 进入服务器证书页面，单击**创建证书申请**，如下图所示：



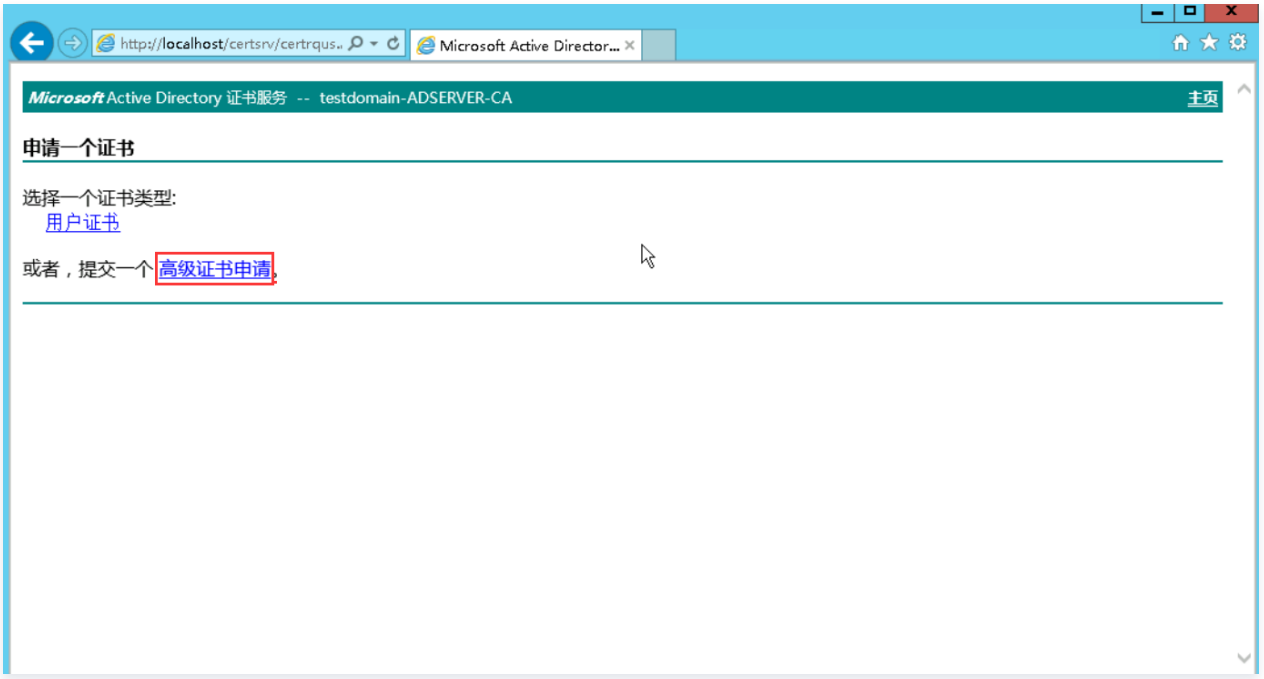

申请证书
可分辨名称属性
指定证书的必需信息。省/市/自治区和城市/地点必须指定为正式名称，并且不得包含缩写。
通用名称(M):
*.test
组织(O):
test
组织单位(U):
test.com
城市/地点(L)
shenzhen
省/市/自治区(S):
guangdong
国家/地区(R):
CN
上一页(P)
下一步(N)
完成(F)
取消

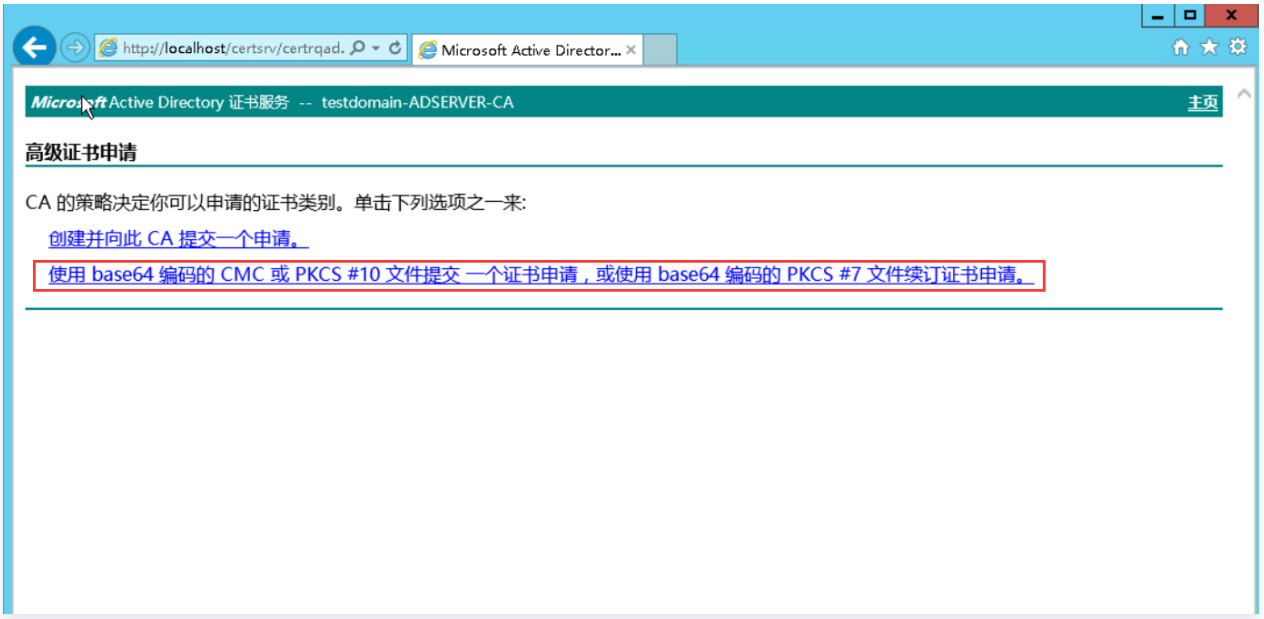




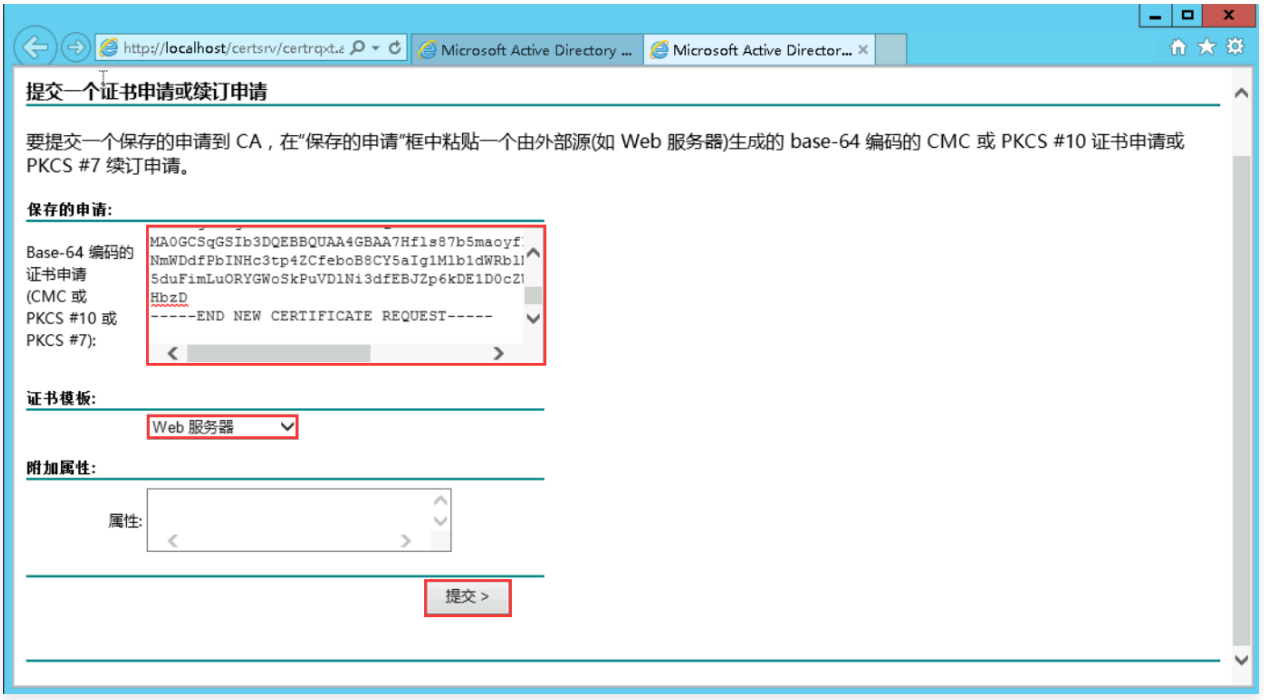
4. 访问 `http://localhost/certsrv`，单击**申请证书 > 高级证书申请 > 使用 base64 编码**，如下图所示：


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

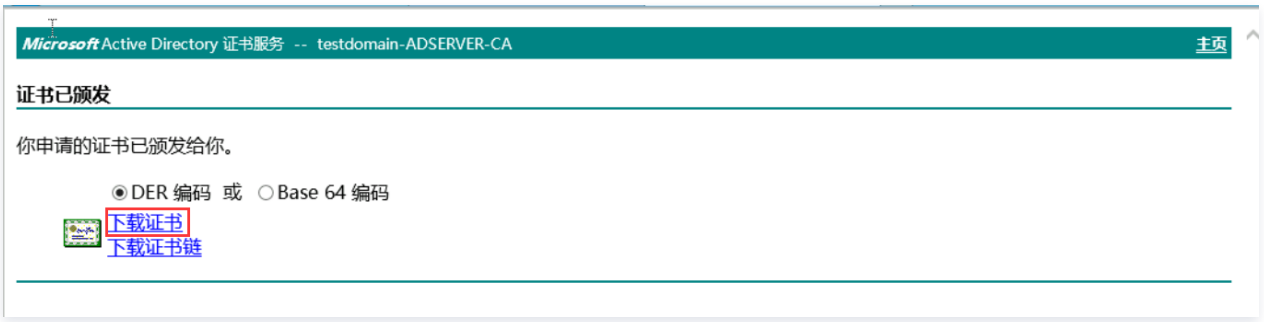

http://localhost/certsrv/certrqus...
Microsoft Active Director...
Microsoft Active Directory 证书服务 -- testdomain-ADSERVER-CA
主页
申请一个证书
选择一个证书类型:
用户证书
或者，提交一个 高级证书申请。



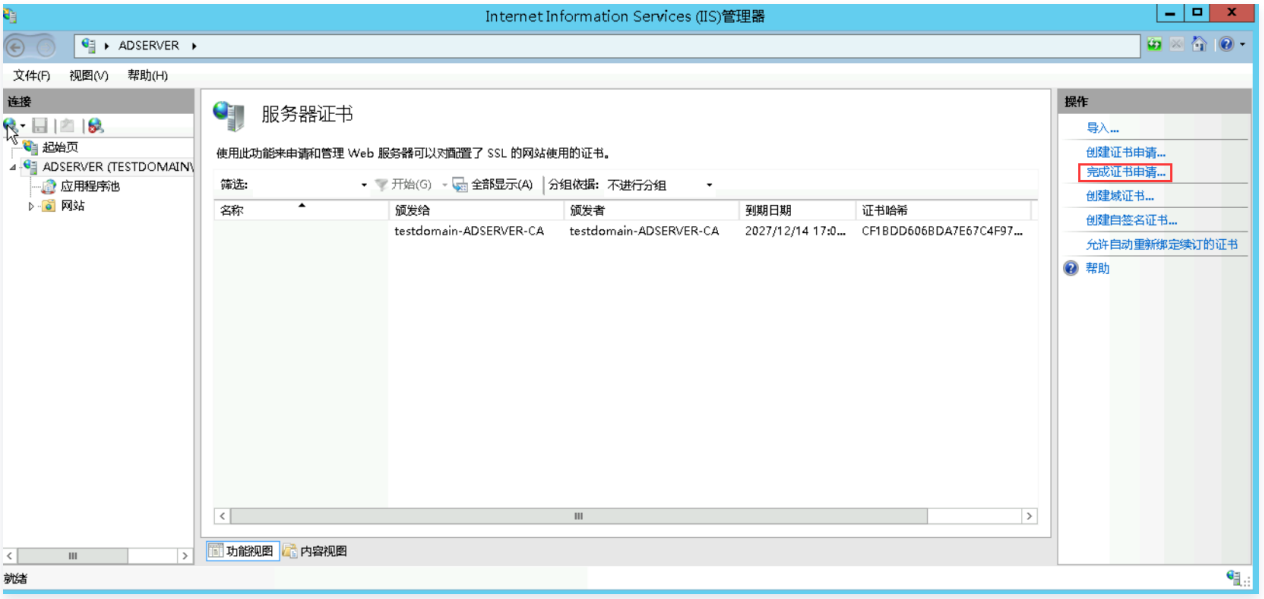
5. 在弹出的提交证书申请页面，将申请证书保存的证书文件内容复制之后补充至以下输入框，证书模板选择 **Web 服务器**，单击**提交**。如下图所示：

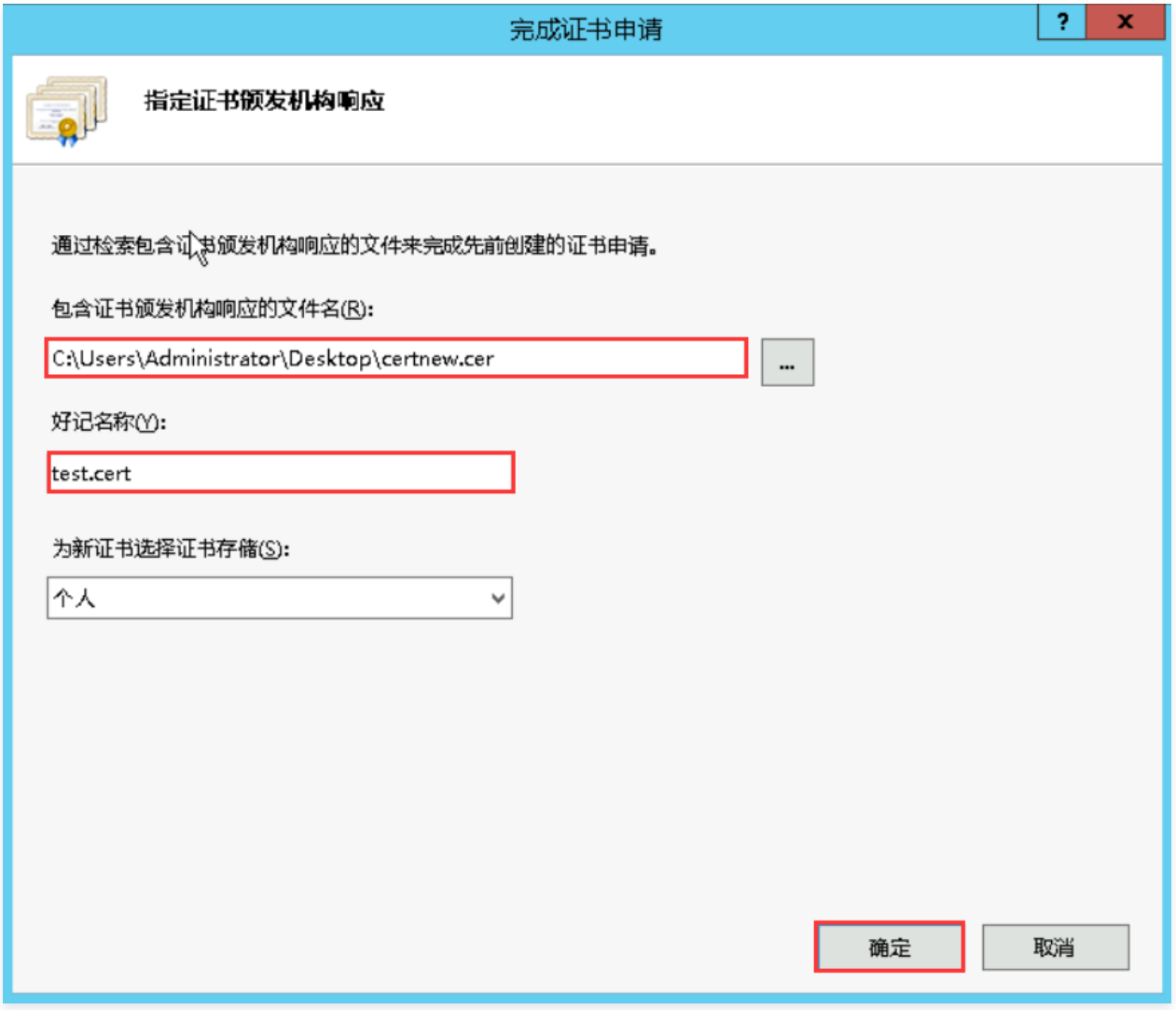


6. 提交之后，单击**下载证书**，如下图所示：

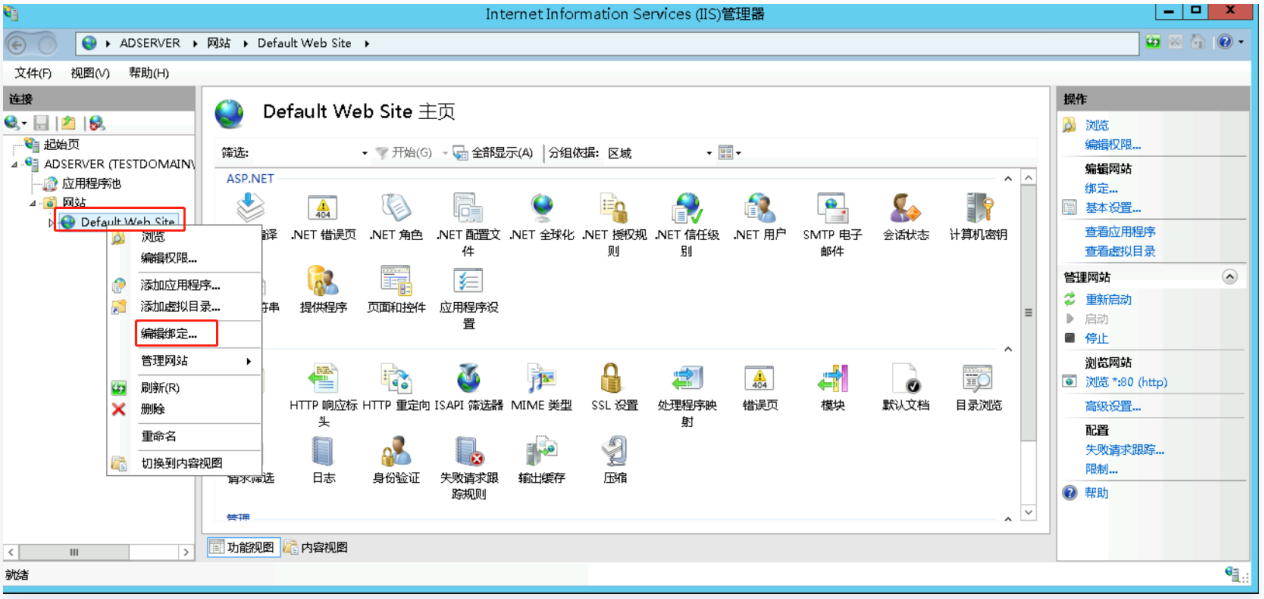


7. 在**服务器证书**页面，单击**完成证书申请**，在弹出的页面选择 步骤6 下载的证书，如下图所示：

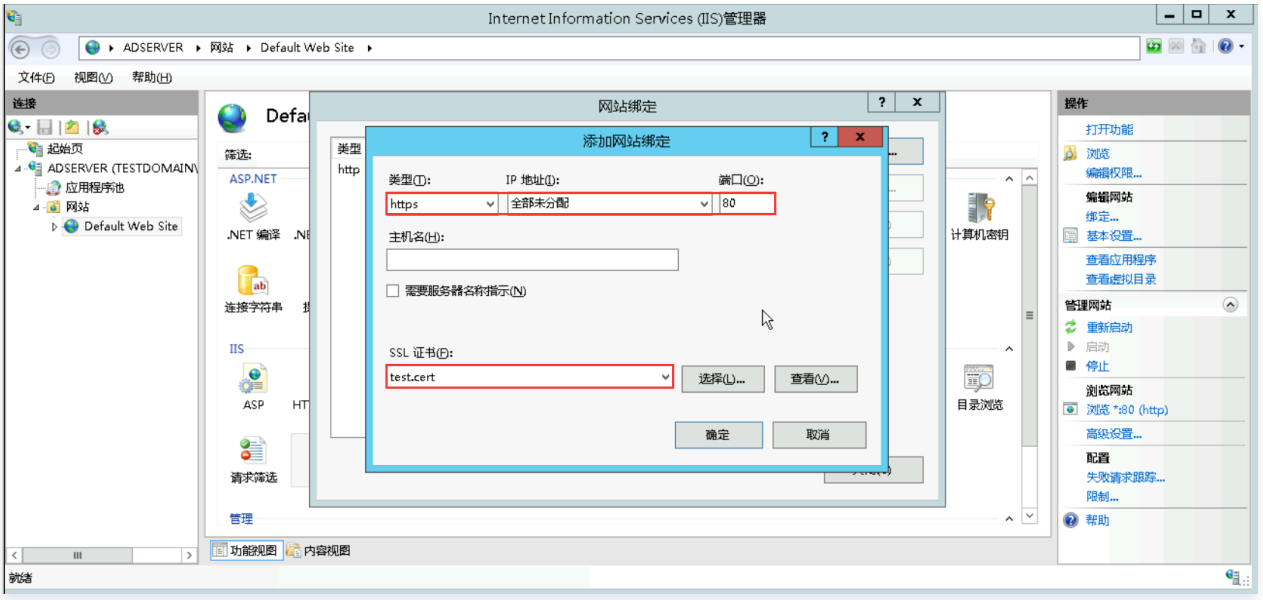




8. 在**网站** > **Default Web Site** 主页，右键单击**编辑绑定**，如下图所示：

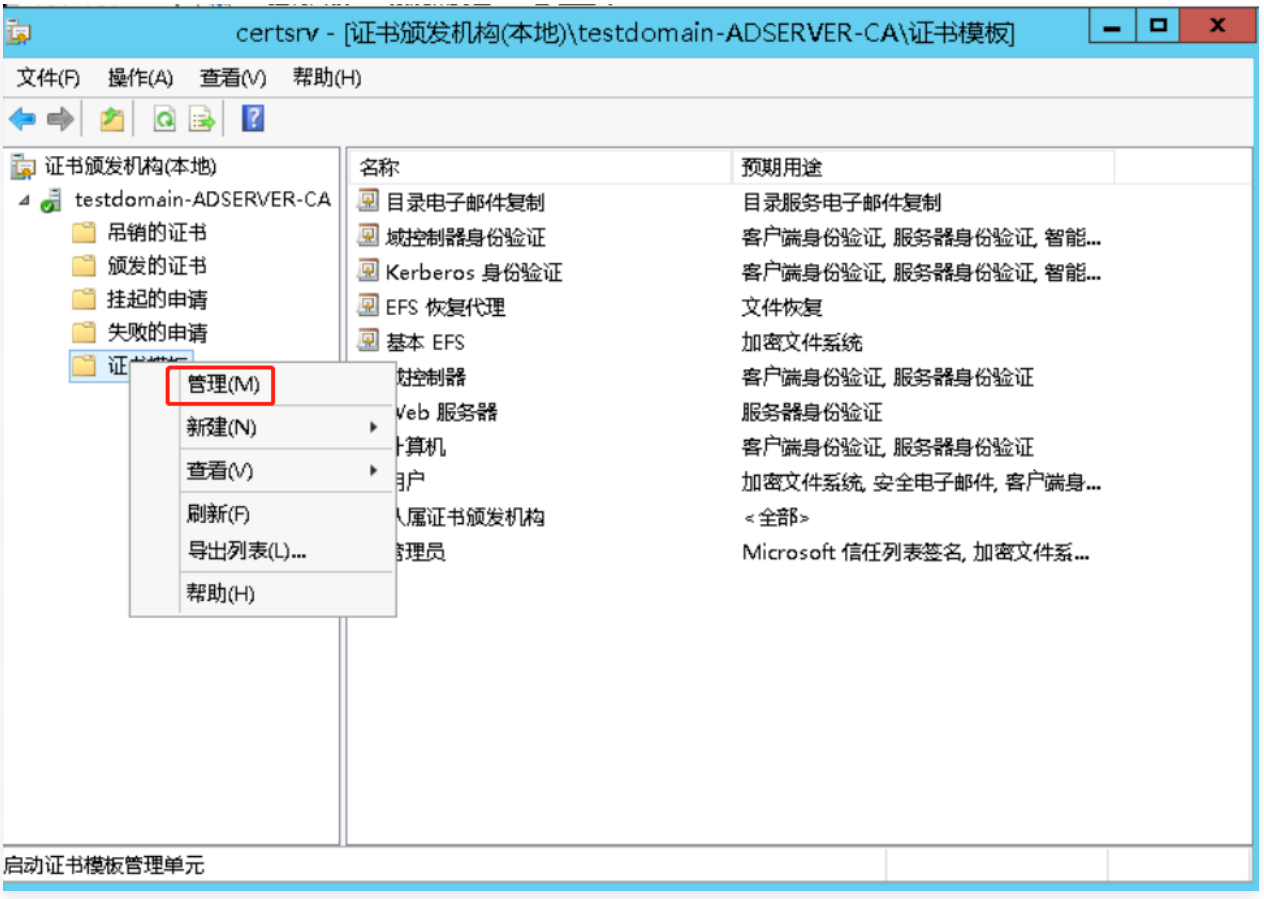


9. 在弹出的**网站绑定**页面，单击**添加**，选择类型为 **https**，IP 地址为**全部未分配**，端口为 **80**，SSL 证书为 **test.cert**，如下图所示：

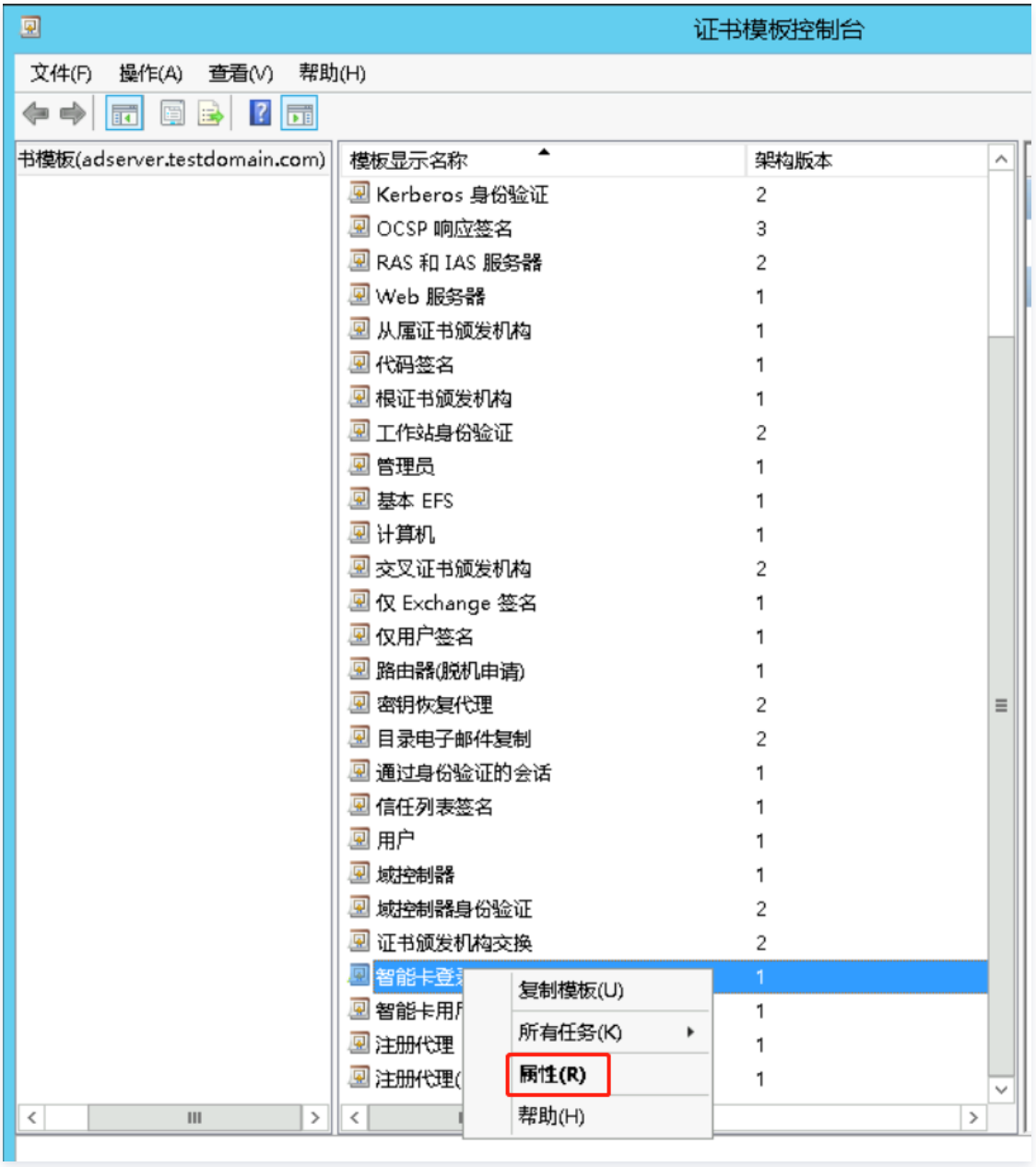


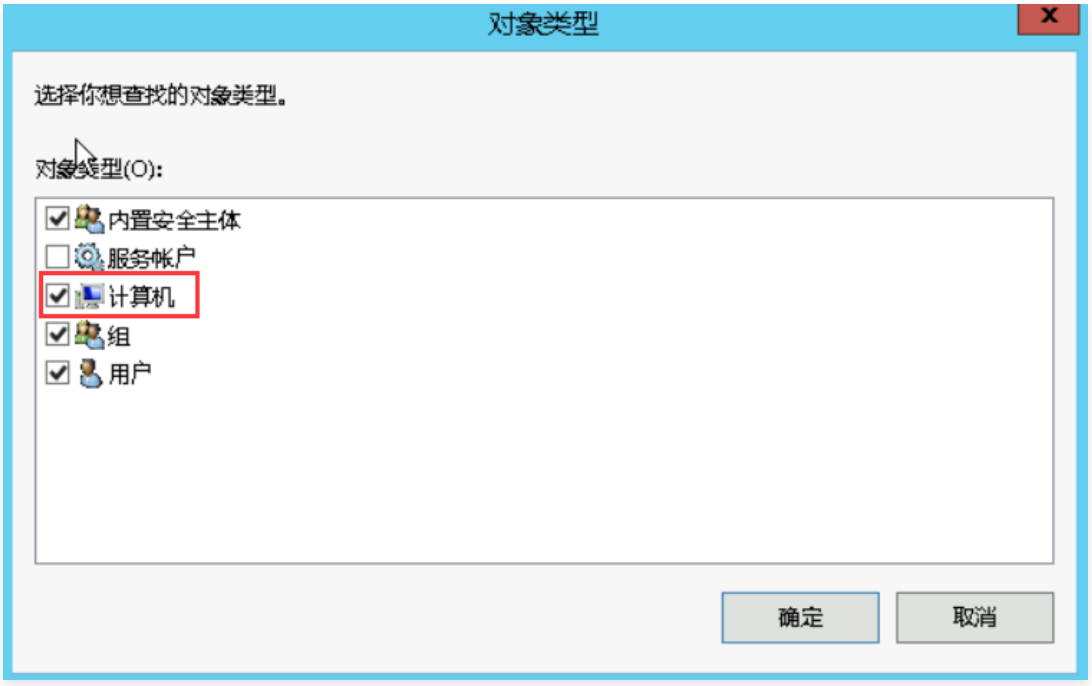
10. 在管理工具页面，单击**证书颁发机构**，如下图所示：

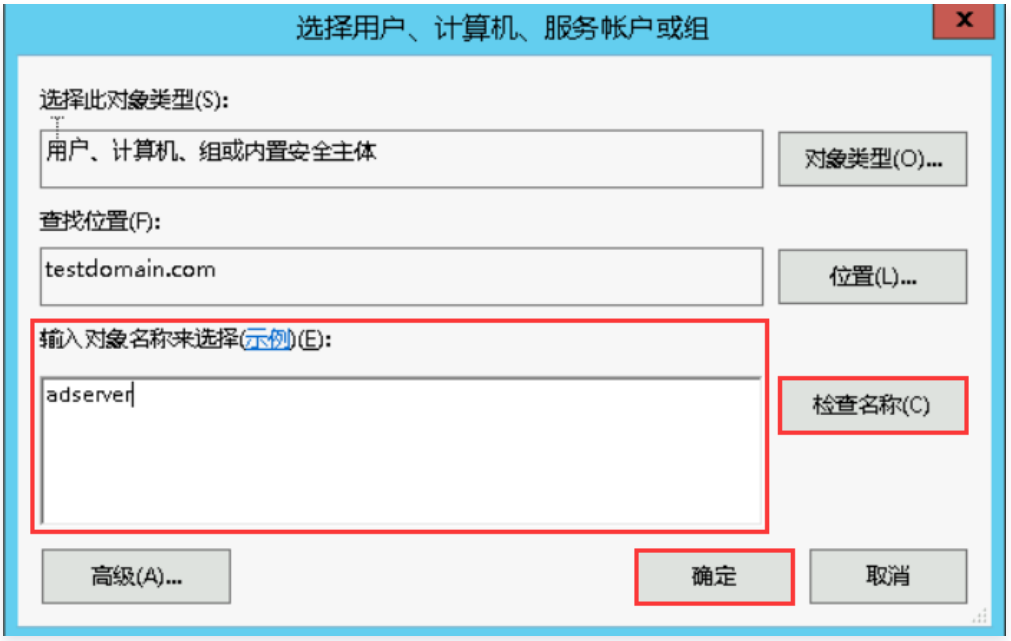
11. 在**证书颁发机构**页面，选择**证件模板**，右键单击**管理**，如下图所示：



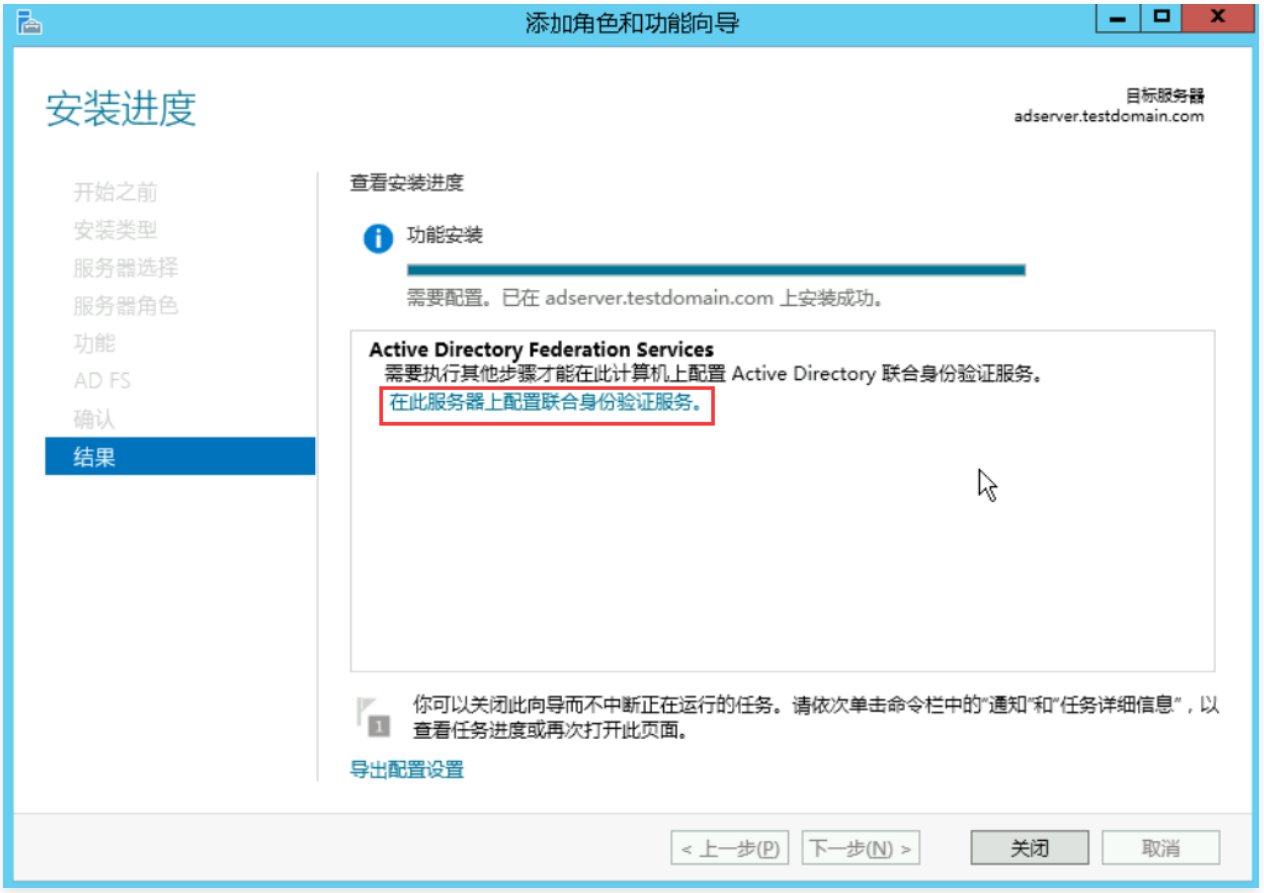
12. 请参考下图配置：


证书模板控制台
文件(F)
操作(A)
查看(V)
帮助(H)
书模板(adserver.testdomain.com)
模板显示名称
架构版本
Kerberos 身份验证 2
OCSP 响应签名 3
RAS 和 IAS 服务器 2
Web 服务器 1
从属证书颁发机构 1
代码签名 1
根证书颁发机构 1
工作站身份验证 2
管理员 1
基本 EFS 1
计算机 1
交叉证书颁发机构 2
仅 Exchange 签名 1
仅用户签名 1
路由器(脱机申请) 1
密钥恢复代理 2
目录电子邮件复制 2
通过身份验证的会话 1
信任列表签名 1
用户 1
域控制器 1
域控制器身份验证 2
证书颁发机构交换 2
智能卡登录 1
智能卡用户 1
注册代理 1
注册代理(1
复制模板(U)
所有任务(K)
属性(R)
帮助(H)

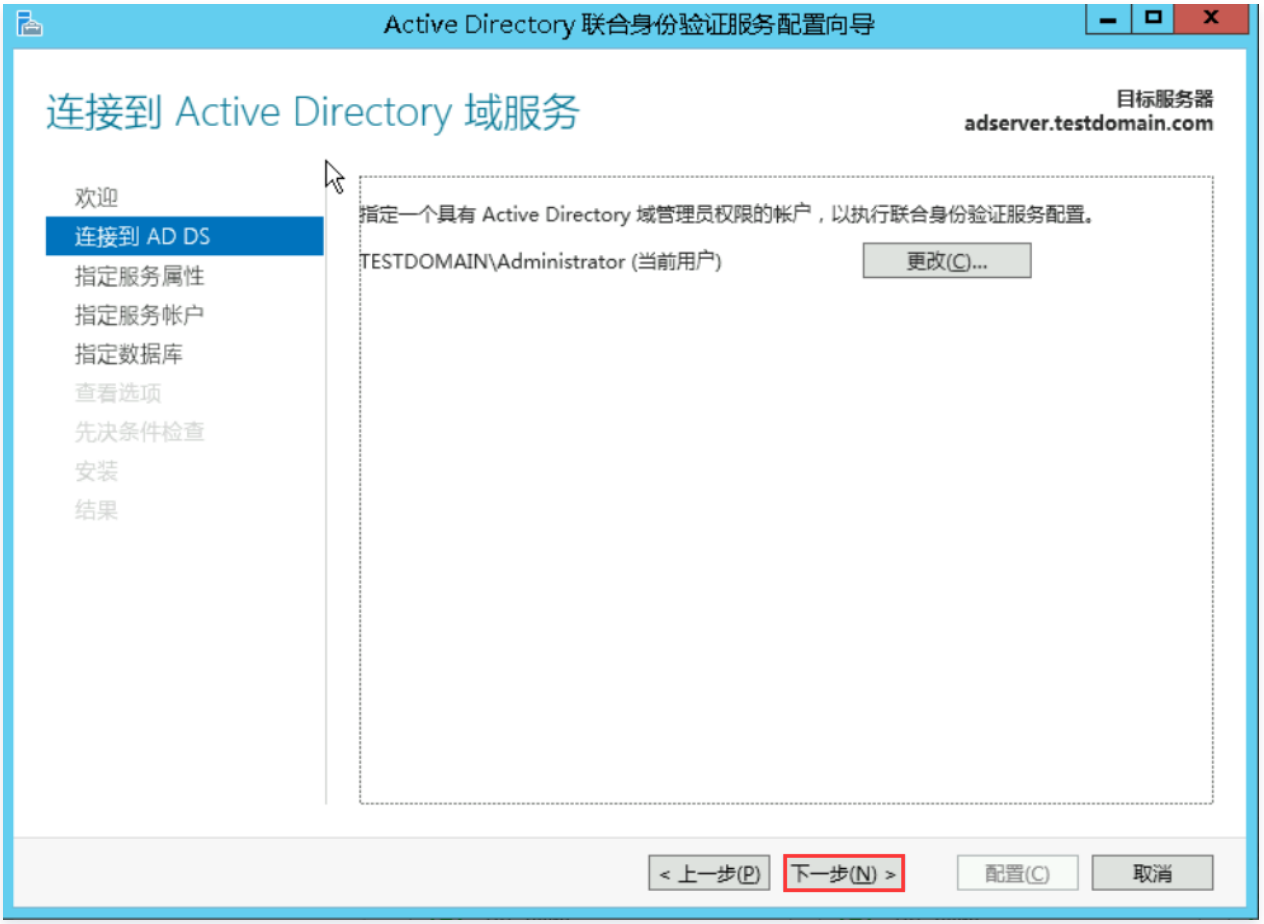




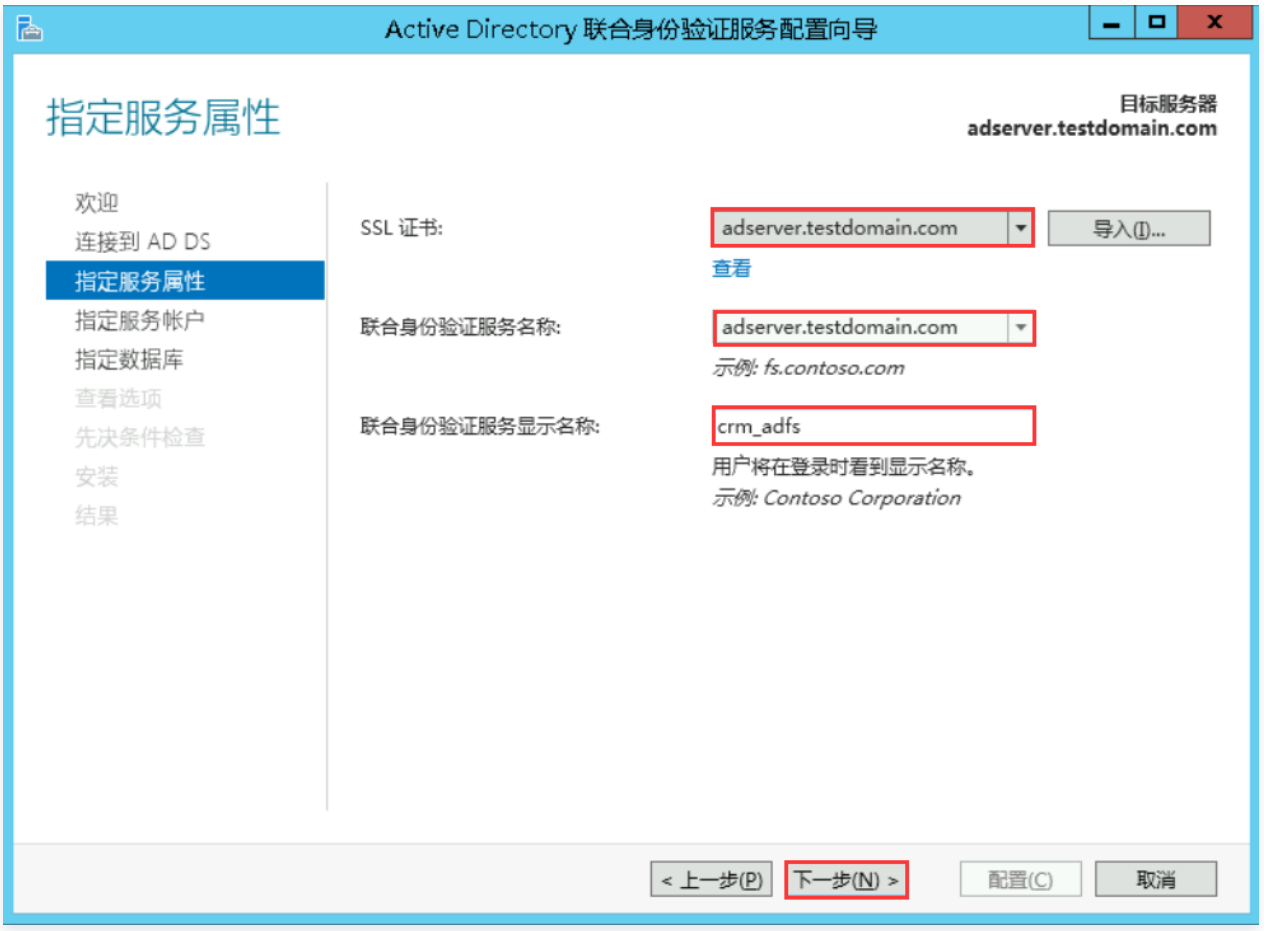
13. 进入**服务器管理器 > 仪表板**页面，单击**添加角色和功能**，按照默认选择一直单击**下一步**直到服务器角色选择页面，勾选 **Active Directory Federation Services**，一直单击**下一步**，**直至安装完成**。
14. 在安装完成页面，单击**在此服务器上配置联合身份验证服务**，如下图所示：



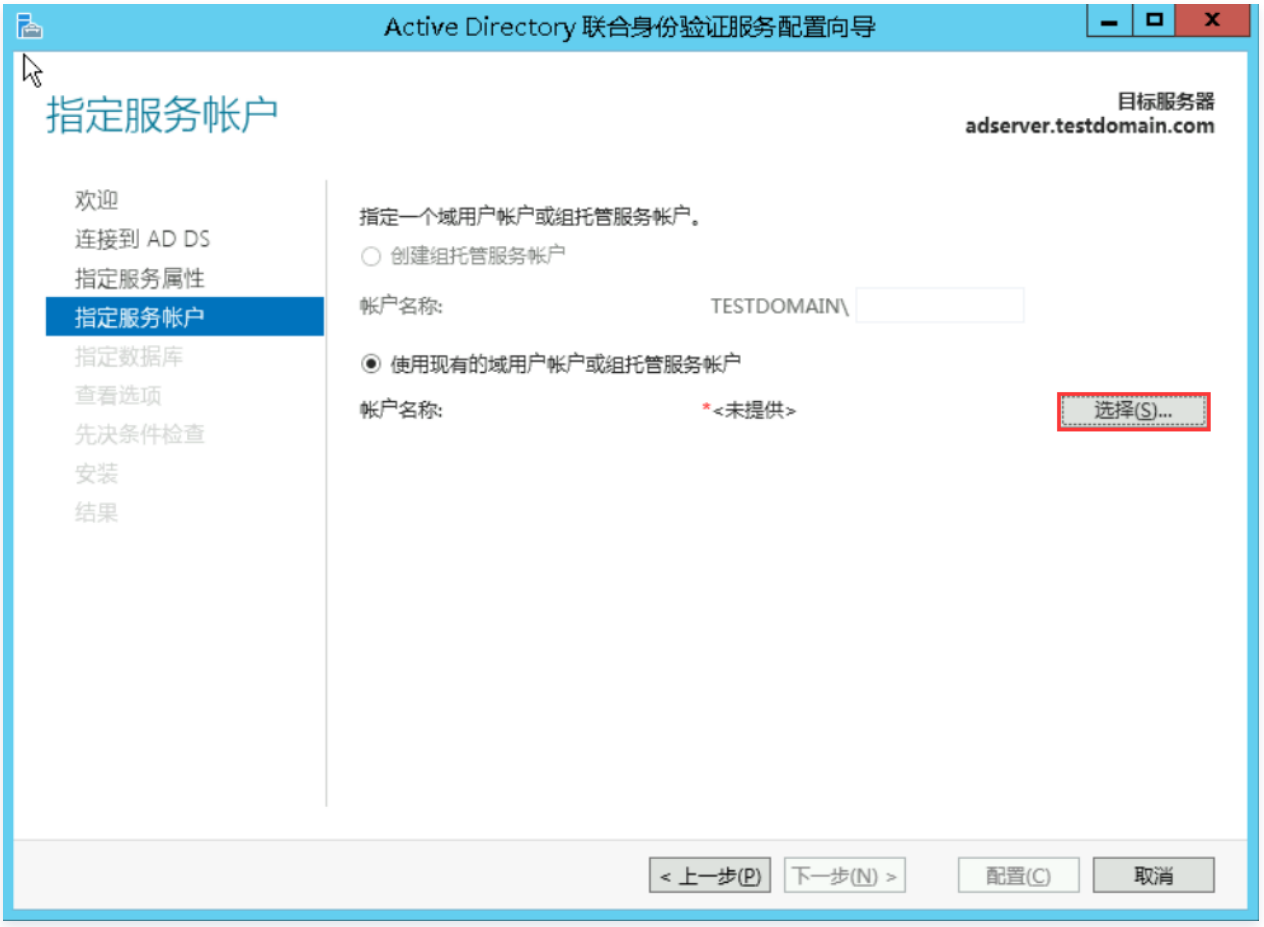
15. 在弹出的向导页面，单击**下一步**。



16. 设置指定服务属性，选择并填写好所需数据，单击**下一步**。



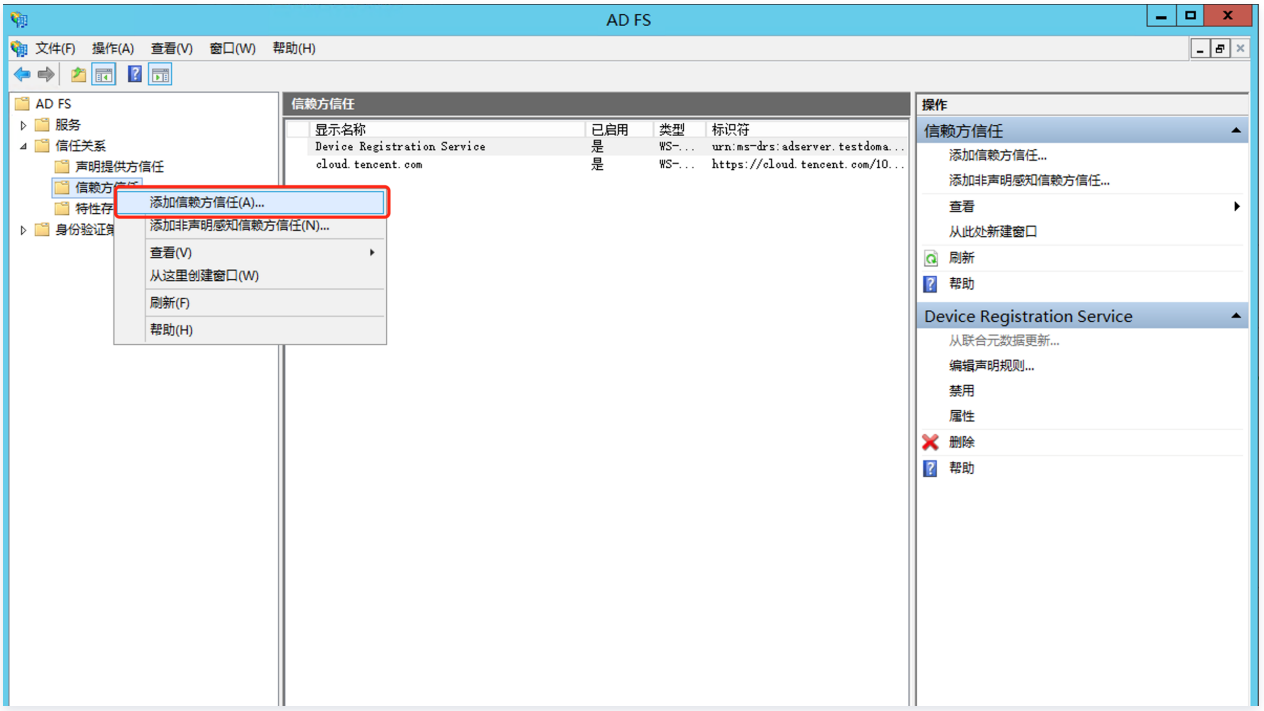
17. 设置指定服务账户，选择使用现有的域用户账户或组托管服务账户，单击**选择**。

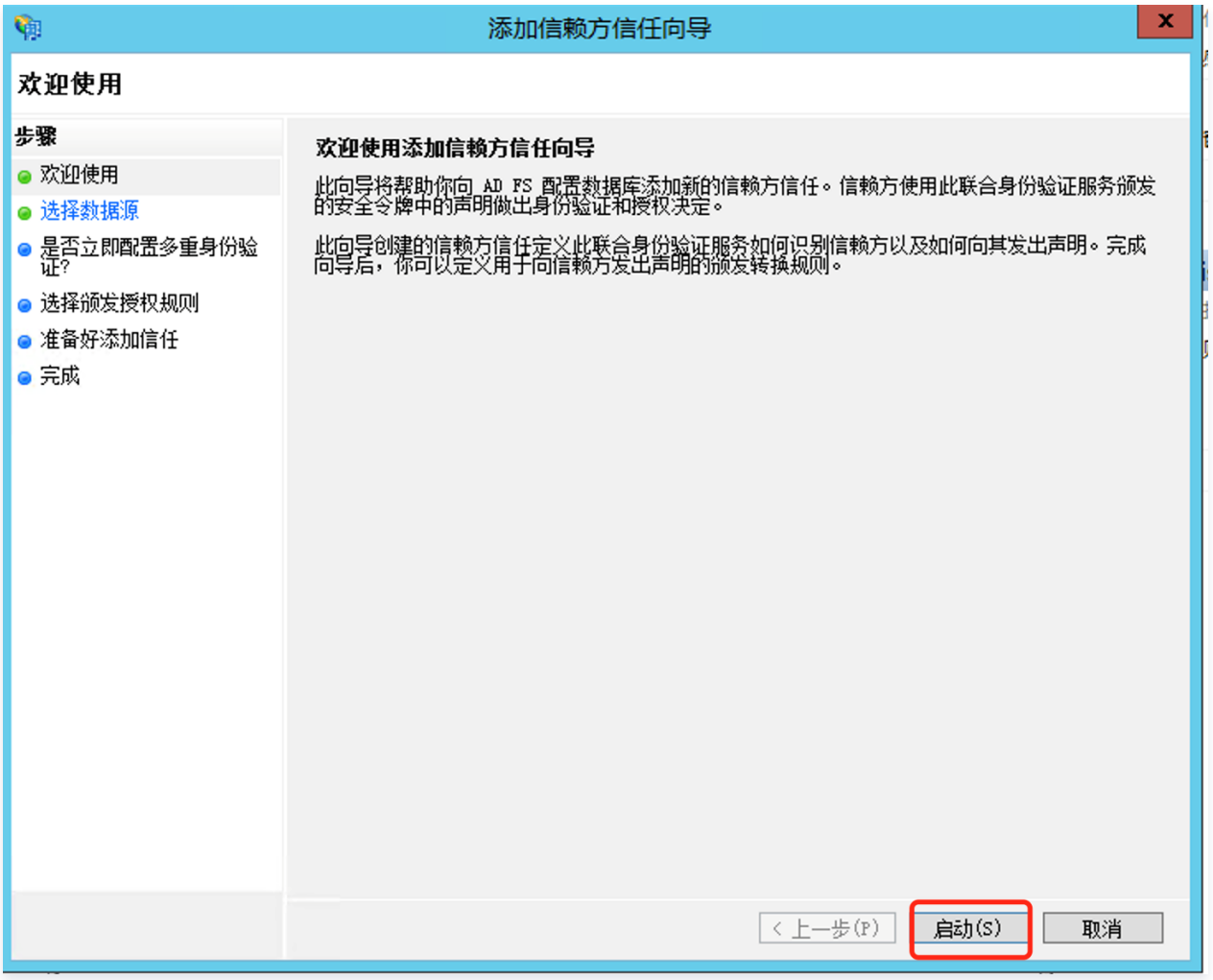


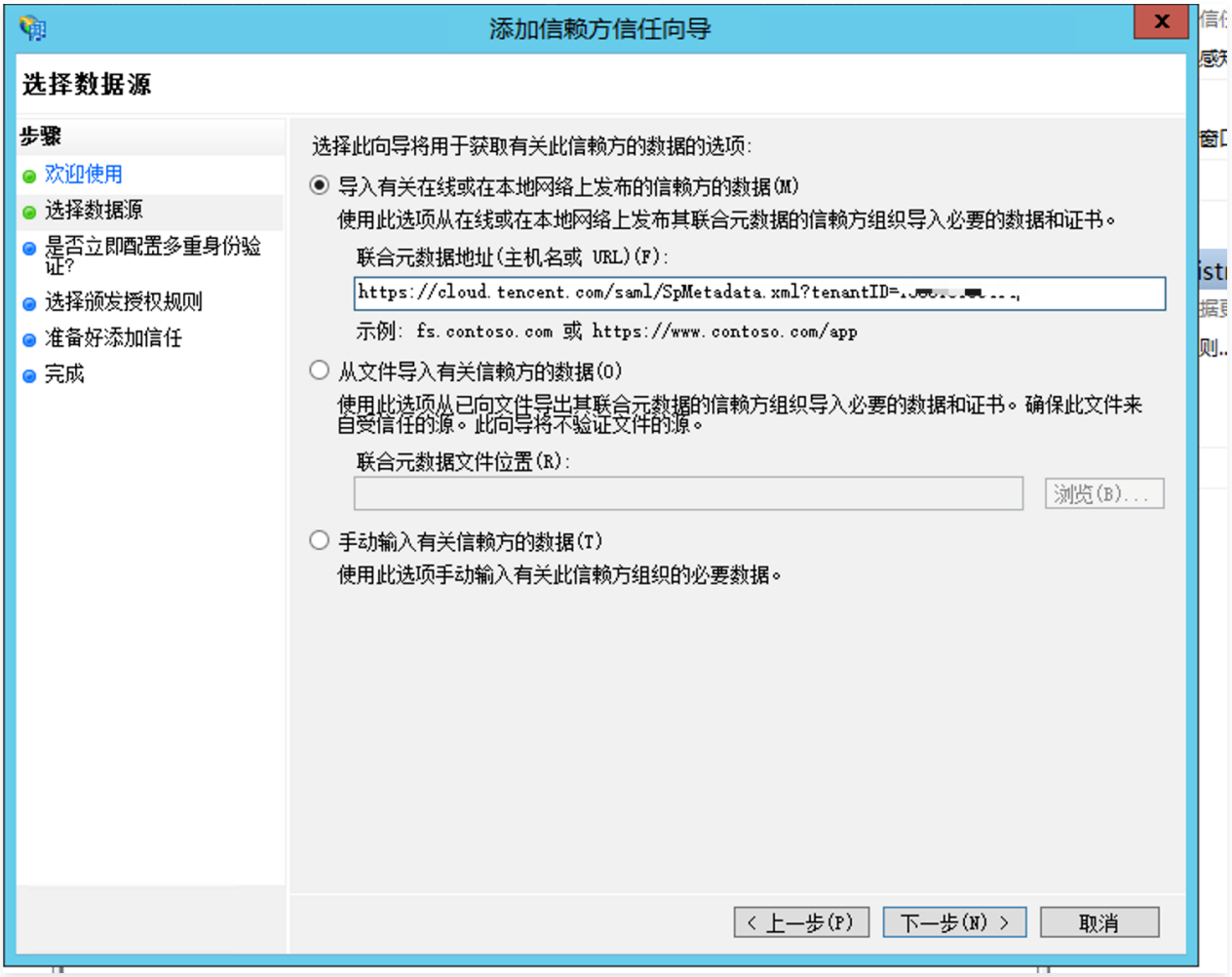
18. 选择指定账户后，单击**确认**，确认后直至安装完成。

用户SSO配置

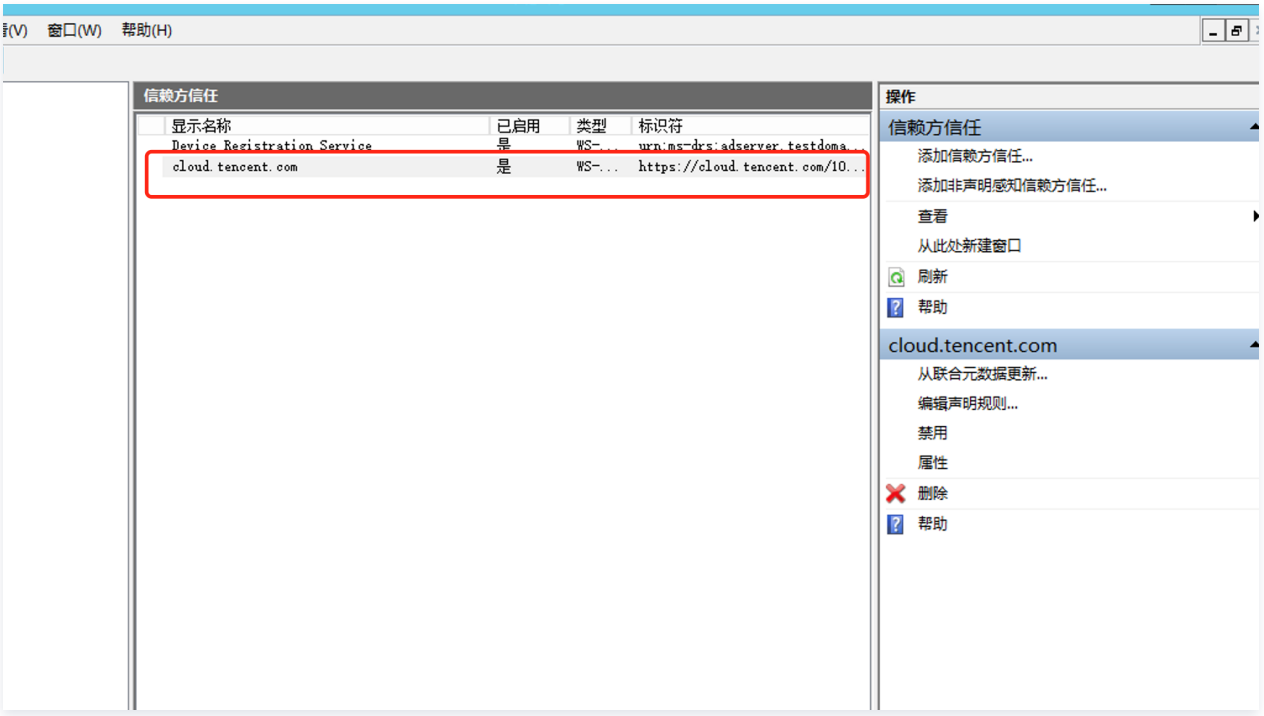
1. 在服务器内浏览器访问 `https://adserver.testdomain.com/FederationMetadata/2007-06/FederationMetadata.xml` ，将源数据 XML 下载至本地。
2. 进入访问管理-用户 SSO 控制台，单击右侧**编辑**，设置 SSO 协议为 SAML，上传 步骤1 保存的 XML 文件。
3. 在服务器内进入 ADFS 管理页面，选择**信任关系** > **信赖方信任**，右键选择**添加信赖方信任**，单击**启动**，补充联合元数据地址，元数据地址从第 2 步中获取，一直单击**下一步**，如下图所示：


AD FS
文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H)
AD FS
服务
信任关系
声明提供方信任
信赖方信任
特性存
身份验证
信赖方信任
显示名称 已启用 类型 标识符
Device Registration Service 是 WS-... urn:ms-drs:adserver.testdoma...
cloud.tencent.com 是 WS-... https://cloud.tencent.com/10...
添加信赖方信任(A)...
添加非声明感知信赖方信任(N)...
查看(V)
从这里创建窗口(W)
刷新(F)
帮助(H)
操作
信赖方信任
添加信赖方信任...
添加非声明感知信赖方信任...
查看
从此处新建窗口
刷新
帮助
Device Registration Service
从联合元数据更新...
编辑声明规则...
禁用
属性
删除
帮助


添加信赖方信任向导
欢迎使用
步骤
欢迎使用
选择数据源
是否立即配置多重身份验证?
选择颁发授权规则
准备好添加信任
完成
欢迎使用添加信赖方信任向导
此向导将帮助你向 AD FS 配置数据库添加新的信赖方信任。信赖方使用此联合身份验证服务颁发的安全令牌中的声明做出身份验证和授权决定。
此向导创建的信赖方信任定义此联合身份验证服务如何识别信赖方以及如何向其发出声明。完成向导后，你可以定义用于向信赖方发出声明的颁发转换规则。
< 上一步(P)
启动(S)
取消

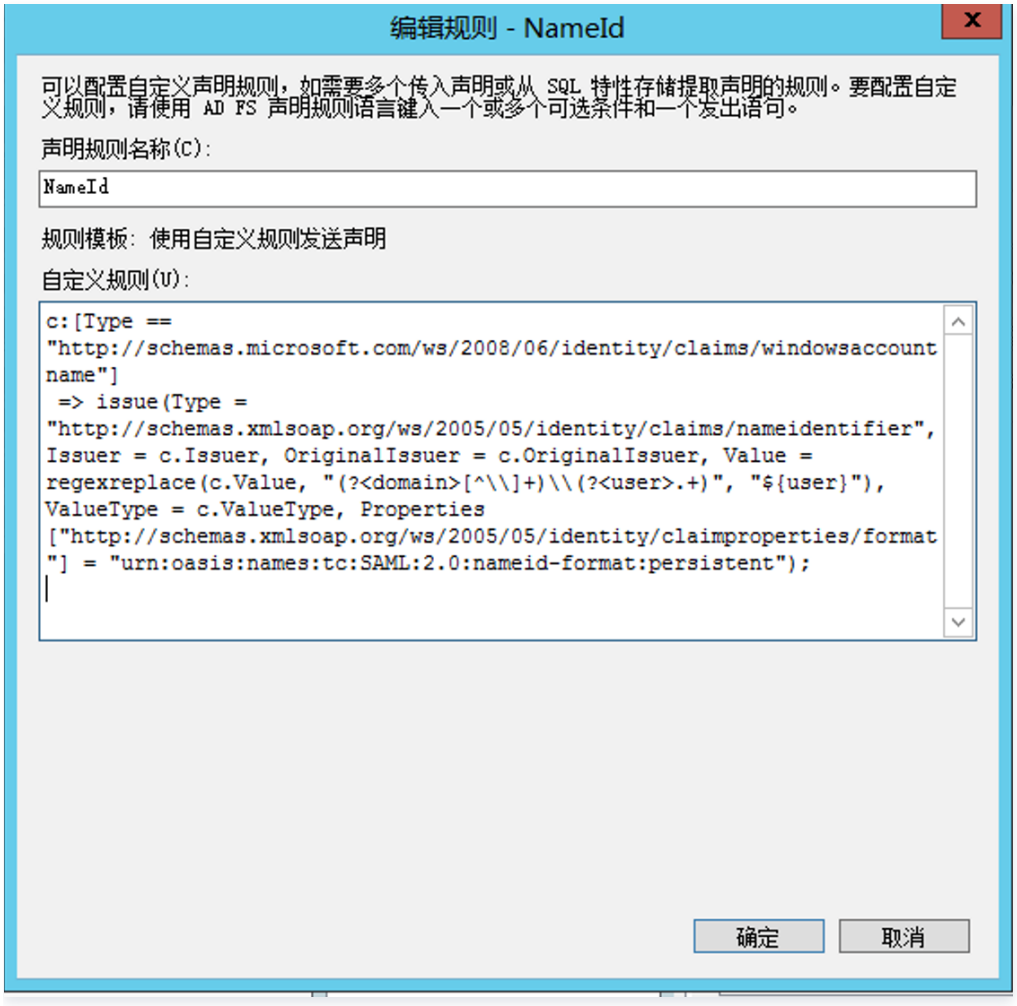


4. 配置完后，效果如下图所示：



为腾讯云 SP 配置 SAML 断言属性

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



说明：

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

- **32位机器：**

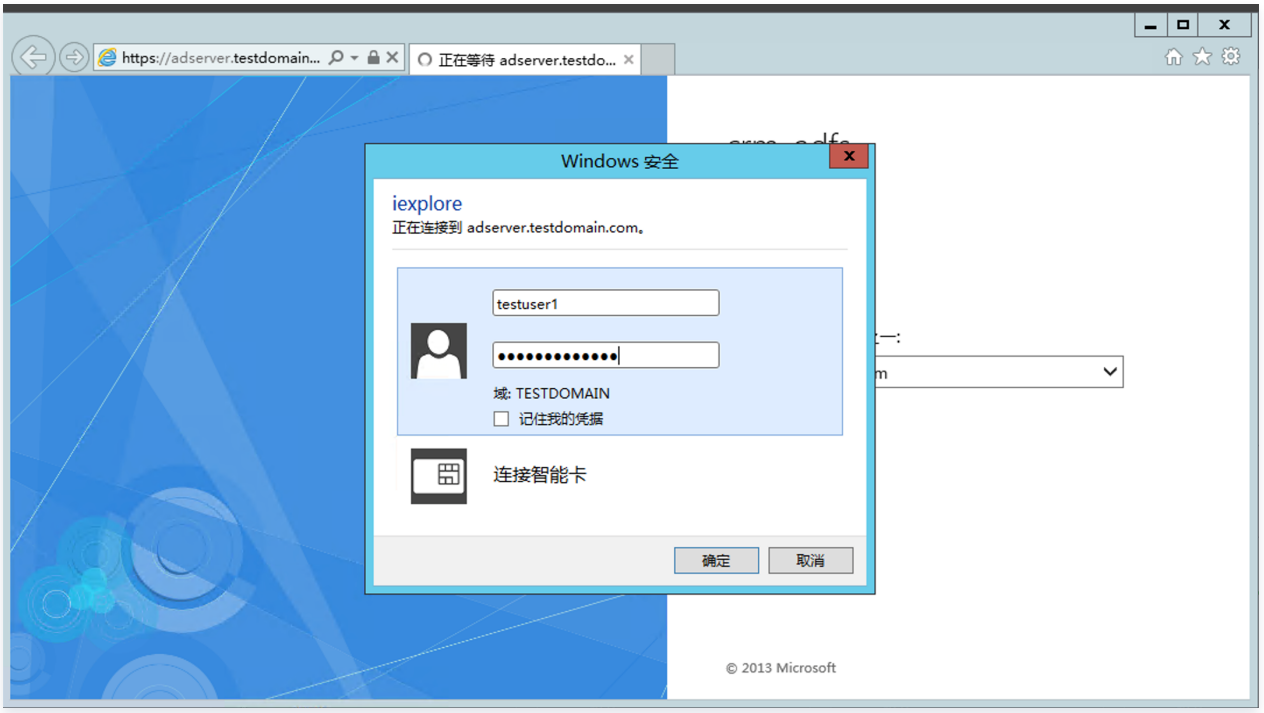
```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Wow6432Node\Microsoft.NetFramework\v4.0.30319' -Name
'SchUseStrongCrypto' -Value '1' -Type DWord
```

- **64位机器：**

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

用户 SSO 登录：

1. **在浏览器输入** `https://adserver.testdomain.com/adfs/ls/idpinitiatedsignon` **。**
2. **输入用户名、密码信息，即可完成登录，如下图所示：**


https://adserver.testdomain...
正在等待 adserver.testdo...
Windows 安全
iexplore
正在连接到 adserver.testdomain.com。
testuser1
域: TESTDOMAIN
记住我的凭据
连接智能卡
确定
取消
© 2013 Microsoft

使用 OneLogin 进行角色 SSO 的示例

最近更新时间：2025-04-17 17:33:02

操作场景

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

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

OneLogin 的详细信息，请参见 OneLogin 帮助文档。

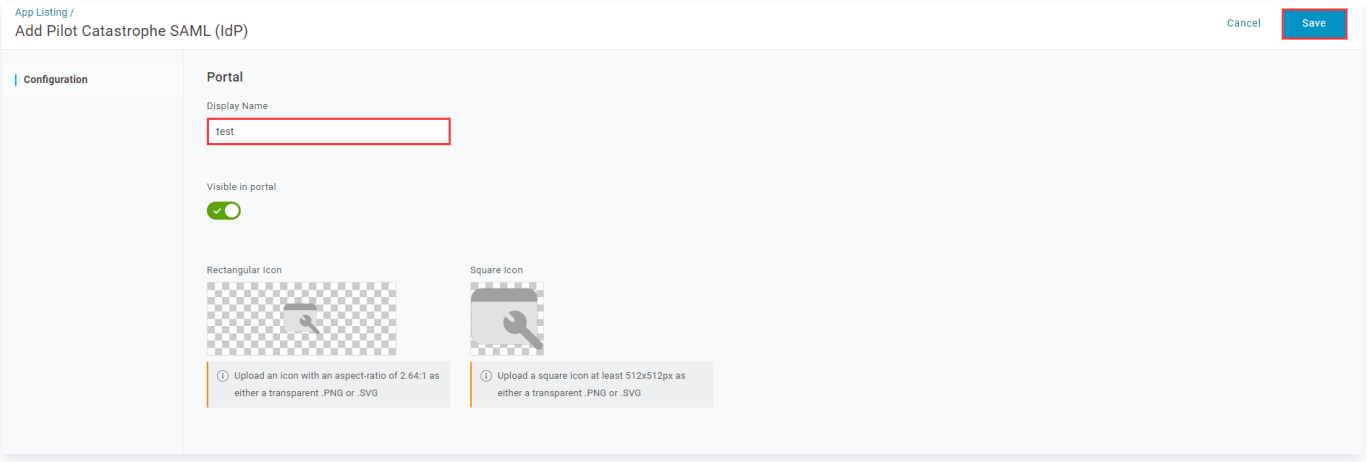
操作步骤

创建 OneLogin 企业应用程序

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

1. 登录并访问 OneLogin 网站，单击 **Applications**，进入应用管理页。
2. 在应用管理页，单击右上角 **ADD APP**。
3. 在搜索框中输入 “SAML”，按 “Enter” 键，并在结果列表中单击 **Pilot Catastrophe SAML(IdP)**。如下图所示：

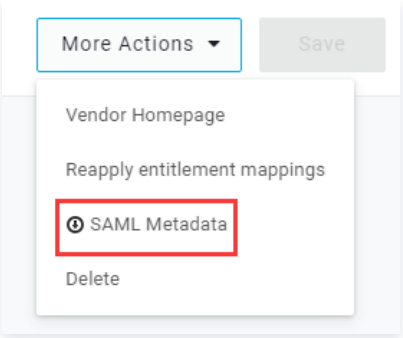
4. 在 **Display Name** 中输入应用名，并单击右上角 **Save**，即可完成应用程序的创建。如下图所示：



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

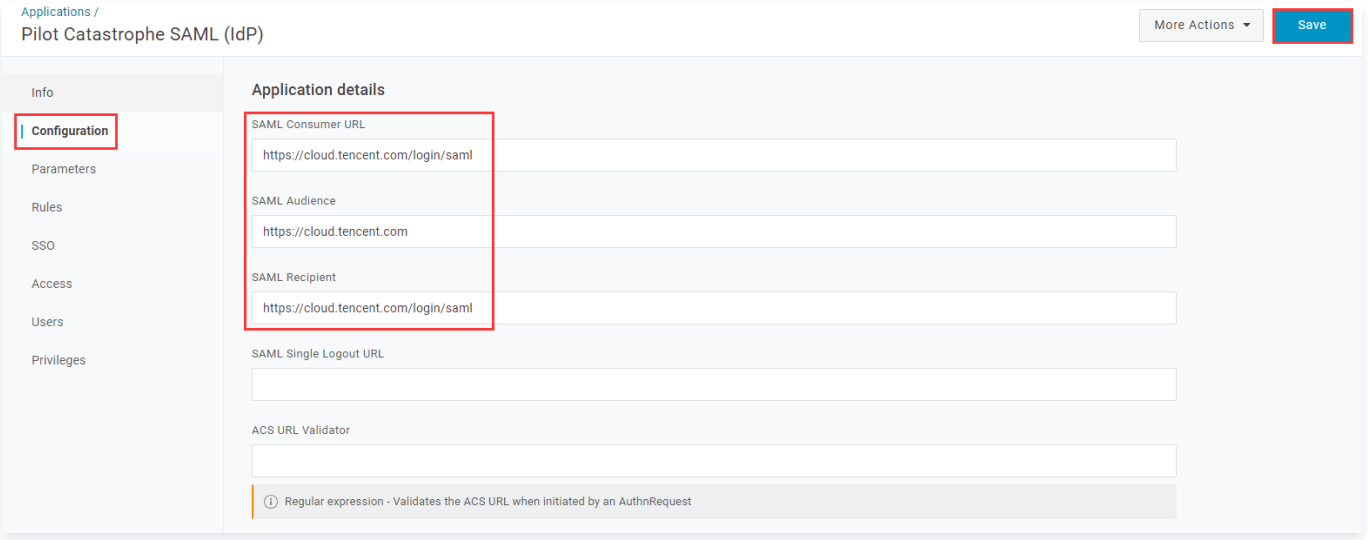


3. 创建腾讯云 CAM 身份提供商以及角色，详细操作请参见 创建身份提供商 、创建角色 为身份提供商创建角色。

配置 OneLogin 单点登录

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
中国站	https://cloud.tencent.com/login/saml	https://cloud.tencent.com	https://cloud.tencent.com/login/saml
国际站	https://tencentcloud.com/login/saml	https://tencentcloud.com/login/saml	https://tencentcloud.com/login/saml

说明：
SAML Recipient 为跳转的腾讯云页面，如您需要指定其他页面，可使用 `https://cloud.tencent.com/login/saml?s_url=xxxx` 形式指定，其中 xxxx 为需要指定的地址，需要做 urlencode。

3. 单击 **Parameters**，单击 **+**，添加以下两条配置信息。

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

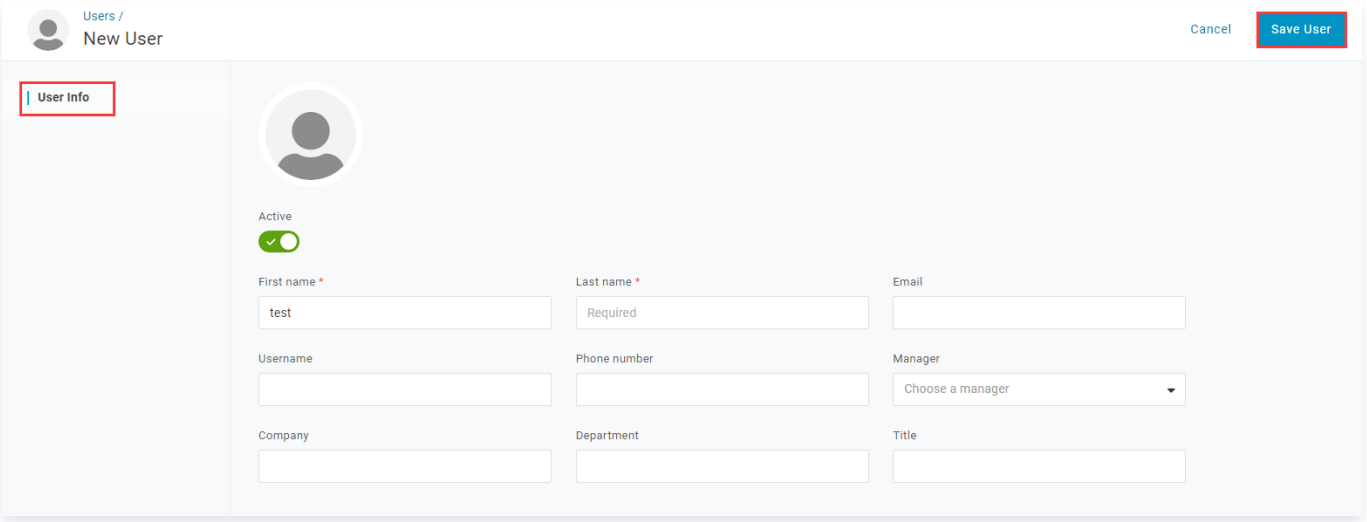
说明：

- 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

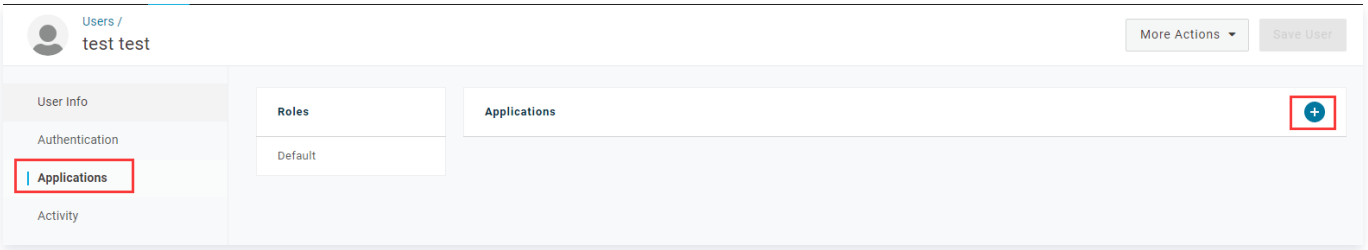
1. 登录并访问 OneLogin 网站，单击 **Users**，进入用户管理页面。
2. 单击右上角 **New User**，跳转至新建用户页。
3. 输入 “First name” 、“Last name”、“Email”、“Username”，单击 **Save User** 保存。如下图所示：



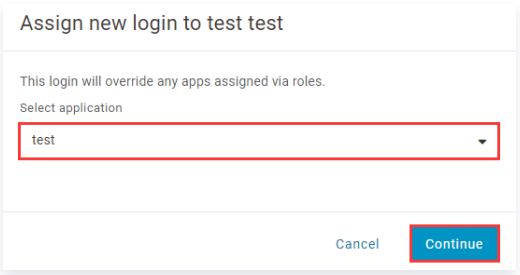
说明：

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

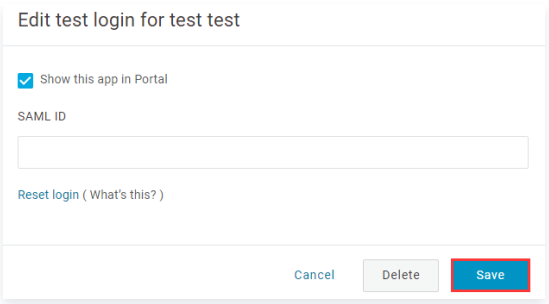
4. 单击用户编辑页 **Applications**，选择右侧的 **+**。如下图所示：



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



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



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

支持员工间资源隔离访问

概述

最近更新时间：2025-01-22 17:56:12

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

场景说明

以云服务器（CVM）产品为例，假设在云上有两台云服务器，对应的信息如下：

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

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

预期结果

- 使用管理员账号查看 CVM 广州区域列表效果：

- 使用 CvmDev_zhangsan 查看 CVM 广州区域列表效果：

实现方式

- 方式一：按照资源 ID 授权
- 方式二：按照标签授权

按照资源 ID 授权

最近更新时间：2025-01-22 17:56:12

操作场景

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

策略内容

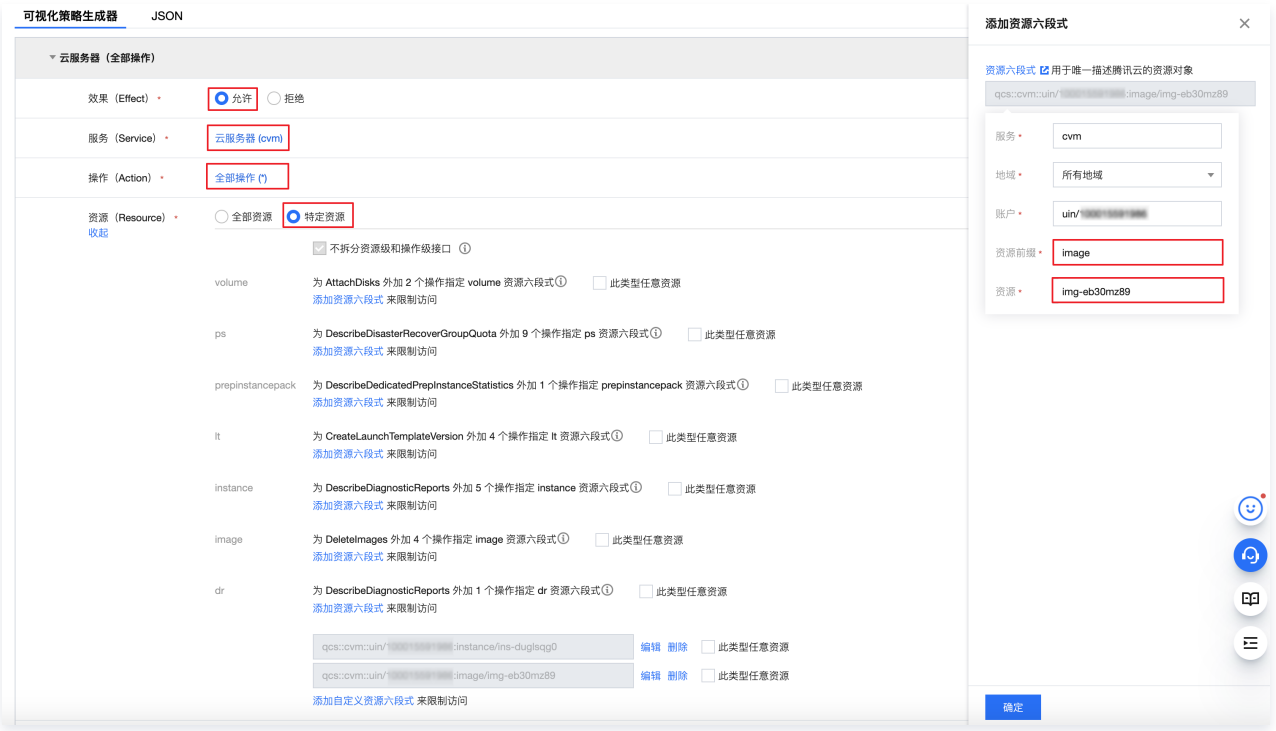
按照资源 ID 授权，最终实现上述预期结果时，对应的策略内容如下：

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "cvm:*"
            ],
            "resource": [
                "qcs::cvm::uin/12345678:instance/ins-duglsqg0",//12345678为主账号UIN
                "qcs::cvm::uin/12345678:image/img-eb30mz89"
            ]
        },
        {
            "effect": "allow",
            "action": [
                "vpc:DescribeVpcEx",
                "vpc:DescribeNetworkInterfaces",
                "cvm:DescribeCbsStorages"
            ],
            "resource": [
                "*"
            ]
        }
    ]
}
```

操作步骤

步骤1：使用管理员账号创建策略并授权

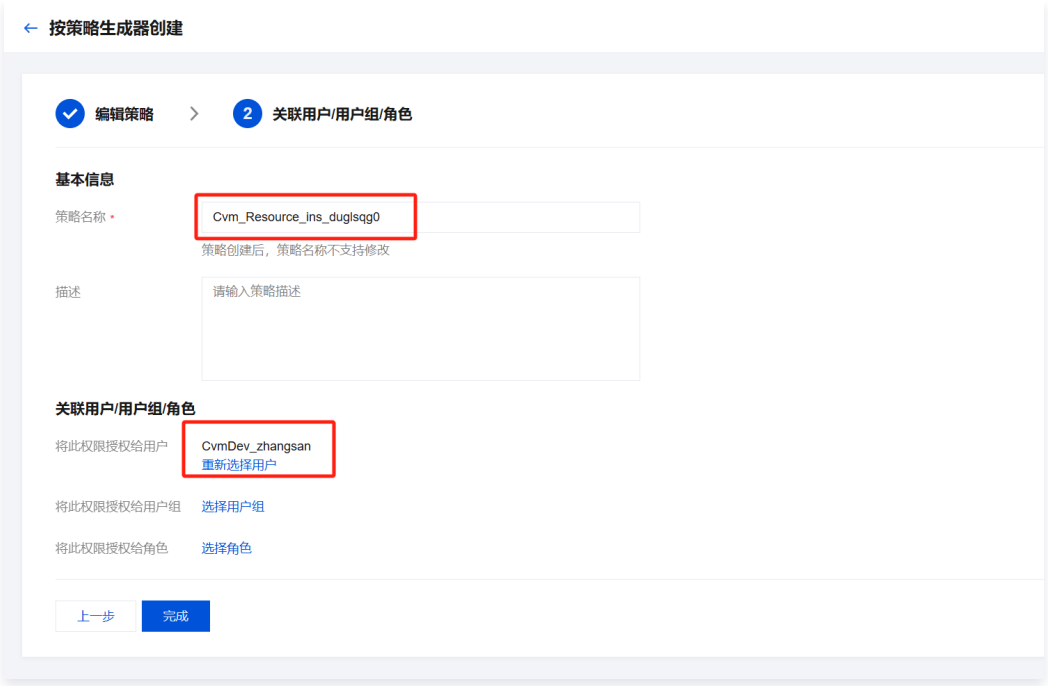
1. 使用管理员账号登录访问管理控制台，在 策略 页面，按照策略生成器创建自定义策略（请参见 通过策略生成器创建自定义策略 ）。



- 效果：允许
- 服务：云服务器 cvm
- 操作：全部操作
- 资源：特定资源 – 添加自定义资源六段式
  - 分别填写：资源前缀：instance 和资源 ID：ins-duglsqg0，以及资源前缀：image 和资源 ID：img-eb30mz89。

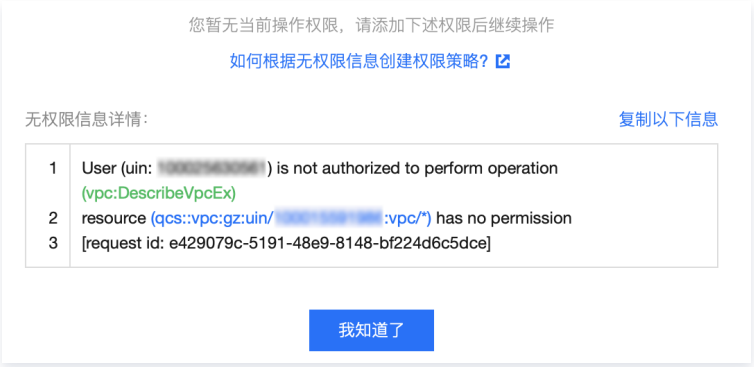
> **说明：**
> - 如何确定资源的前缀：在云服务器支持 CAM 的接口中有云服务器对应的资源六段式，具体请参见 云服务器支持 CAM 的接口 。
> - 云服务器产品页面除了调用 CVM 相关接口外，还会使用 VPC 等接口，这时我们可以先跳过，继续生成策略，在实际操作的时候按照 CAM 的提示添加相关接口。

2. 单击**下一步**，指定策略的名称为 Cvm_Resource_ins_duglsqg0，并将策略授予子账号 CvmDev_zhangsan。
3. 单击**完成**，完成授权。



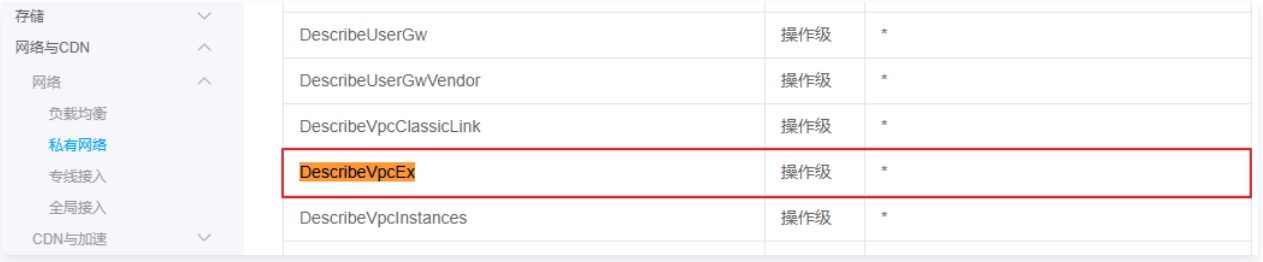
步骤2：使用子账号登录验证权限

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

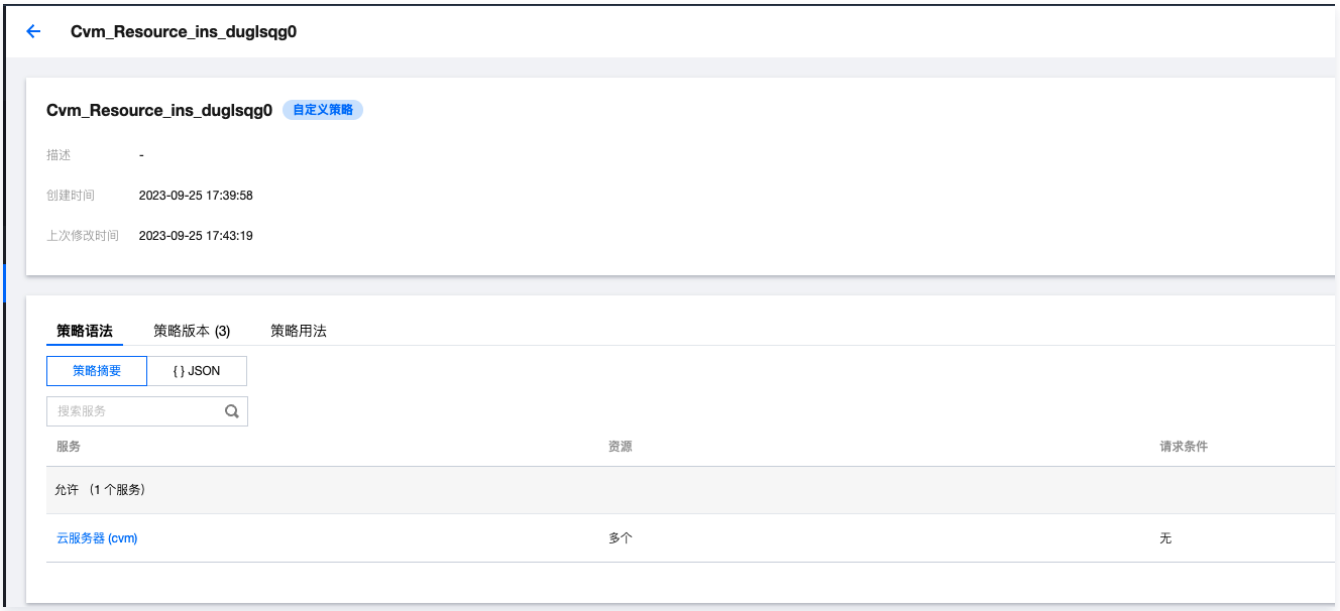


步骤3：使用管理员账号调整策略内容

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



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



- 添加之前：

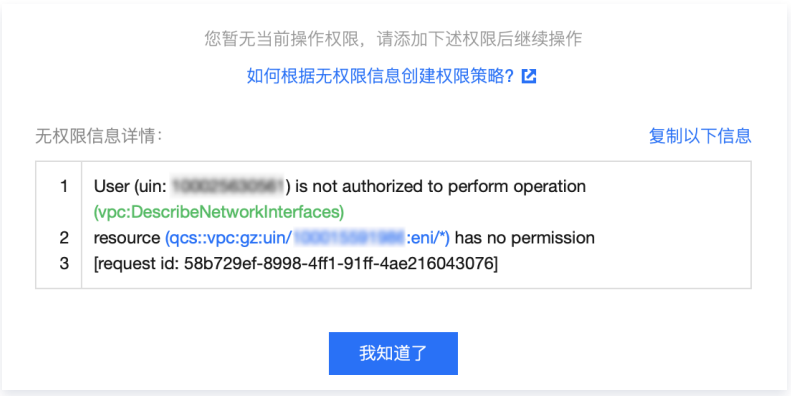
```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "cvm:*"
            ],
            "resource": [
                "qcs::cvm::uin/[redacted]:instance/ins-duglsqg0",
                "qcs::cvm::uin/[redacted]:image/img-eb30mz89"
            ]
        }
    ]
}
```

- 添加之后：

```
        {
            "effect": "allow",
            "action": [
                "cvm:*"
            ],
            "resource": [
                "qcs::cvm::uin/[redacted]:instance/ins-duglsqg0",
                "qcs::cvm::uin/[redacted]:image/img-eb30mz89"
            ]
        },
        {
            "effect": "allow",
            "action": [
                "vpc:DescribeVpcEx"
            ],
            "resource": [
                "*"
            ]
        }

    ]
}
```

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



5. 按照 步骤3 继续调整策略内容，直至系统没有报错。
   最终策略的内容如下：

```
        "effect": "allow",
        "action": [
            "cvm:*"
        ],
        "resource": [
            "qcs::cvm::uin/[redacted]:instance/ins-duglsqg0",
            "qcs::cvm::uin/[redacted]:image/img-eb30mz89"
        ]
    },
    {
        "effect": "allow",
        "action": [
            "vpc:DescribeVpcEx",
            "vpc:DescribeNetworkInterfaces",
            "cvm:DescribeCbsStorages"
        ],
        "resource": [
            "*"
        ]
    }
  ]
}
```

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

步骤4：验证结果

使用子用户 CvmDev_zhangsan 再次验证，达到预期效果。
至此，子用户 CvmDev_zhangsan 可以对实例进行开关机、重启、更名、重置密码等操作。

按照标签授权

最近更新时间：2025-01-22 16:14:43

操作场景

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

策略内容

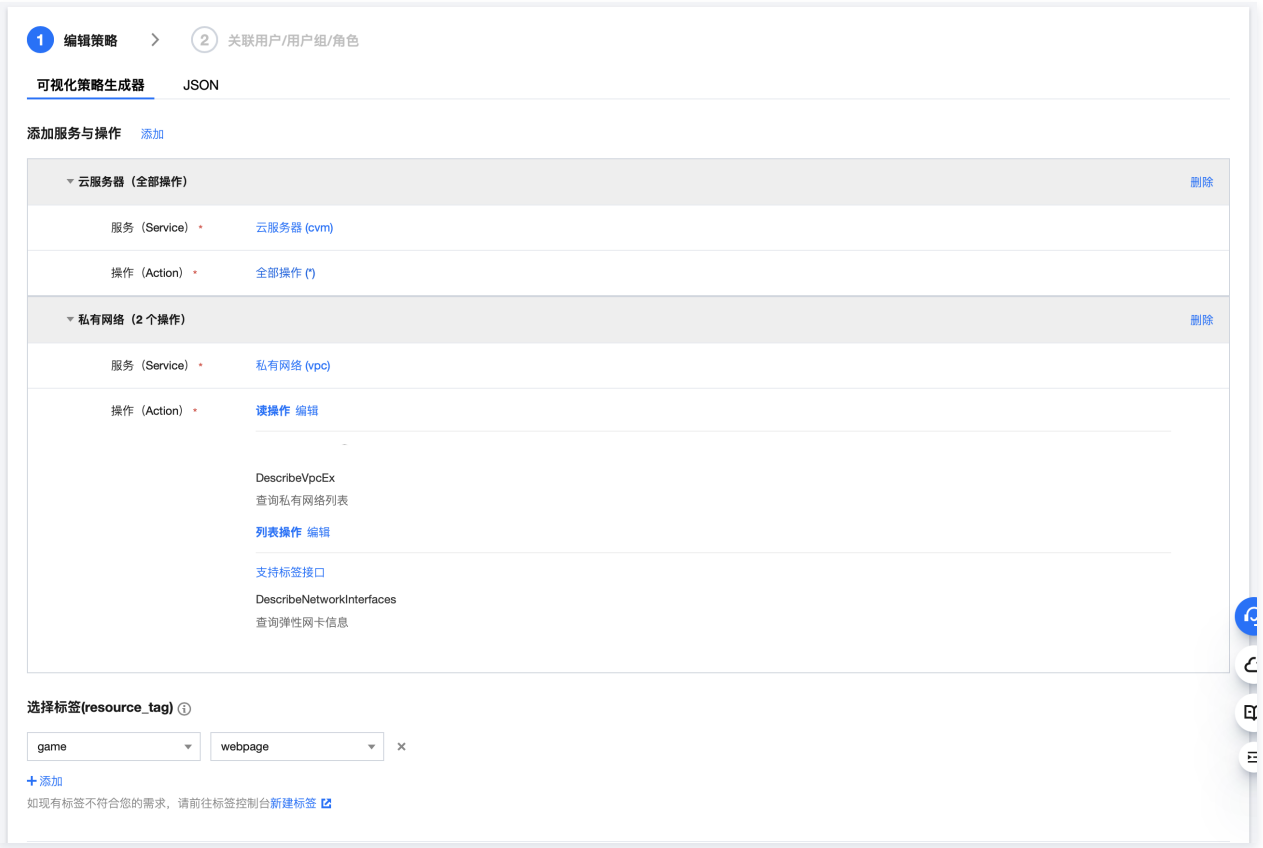
按照标签授权，最终实现上述预期结果时，对应的策略内容如下：

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "cvm:*",
                "vpc:DescribeVpcEx",
                "vpc:DescribeNetworkInterfaces"
            ],
            "resource": "*",
            "condition": {
                "for_any_value:string_equal": {
                    "qcs:resource_tag": [
                        "game&webpage"
                    ]
                }
            }
        }
    ]
}
```

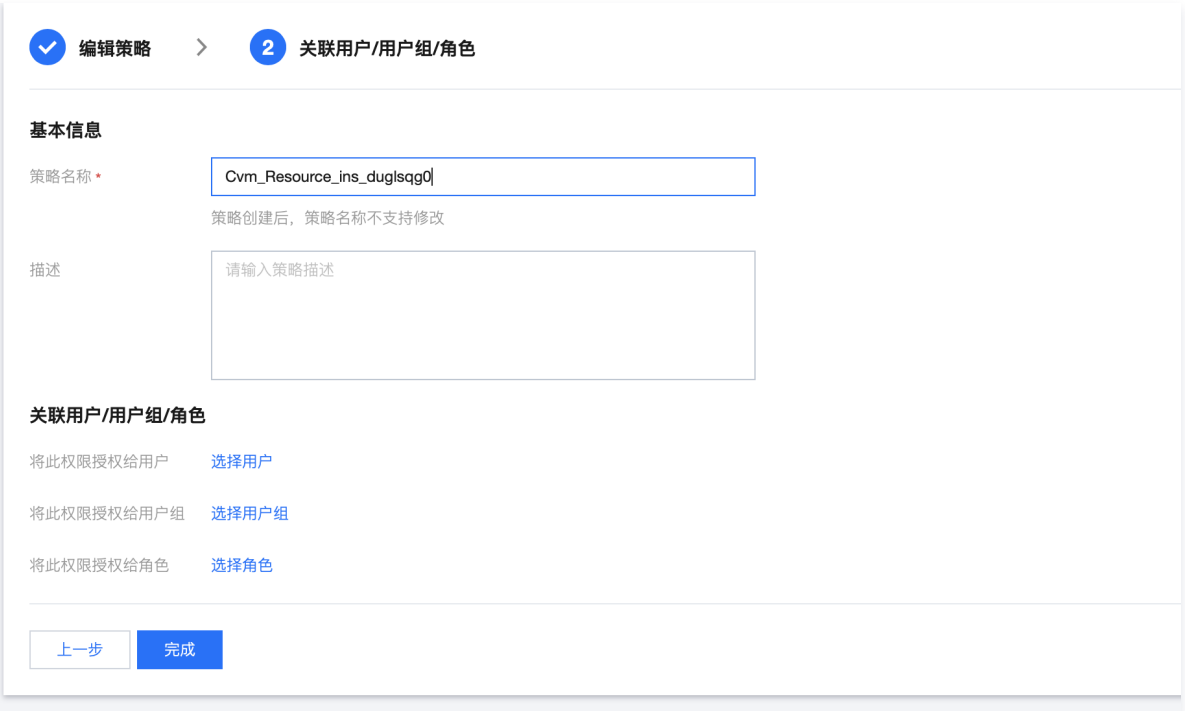
操作步骤

步骤1：创建策略并授权

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



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



步骤2：验证结果

使用子用户 CvmDev_zhangsan 登录 云服务器控制台，访问实例列表页面，达到预期效果。
至此，子用户 CvmDev_zhangsan 可以对实例进行开关机、重启、更名、重置密码等操作。

企业多账号权限管理

概述

最近更新时间：2024-10-11 09:44:41

很多企业在腾讯云上会有多个主账号，账号越多，账号和权限的管理就会越复杂。这时企业管理者希望能够跨账号管理资源权限，减少管理的复杂度。员工如果需要访问多个主账号，希望能够减少 CAM 子账号的数量和登录次数。
针对上述场景，腾讯云提供集团账号、角色和协作者三种方式进行跨账号的访问和管理。三种方式的对比如下，您可以根据实际场景选择适合自己企业的方式：

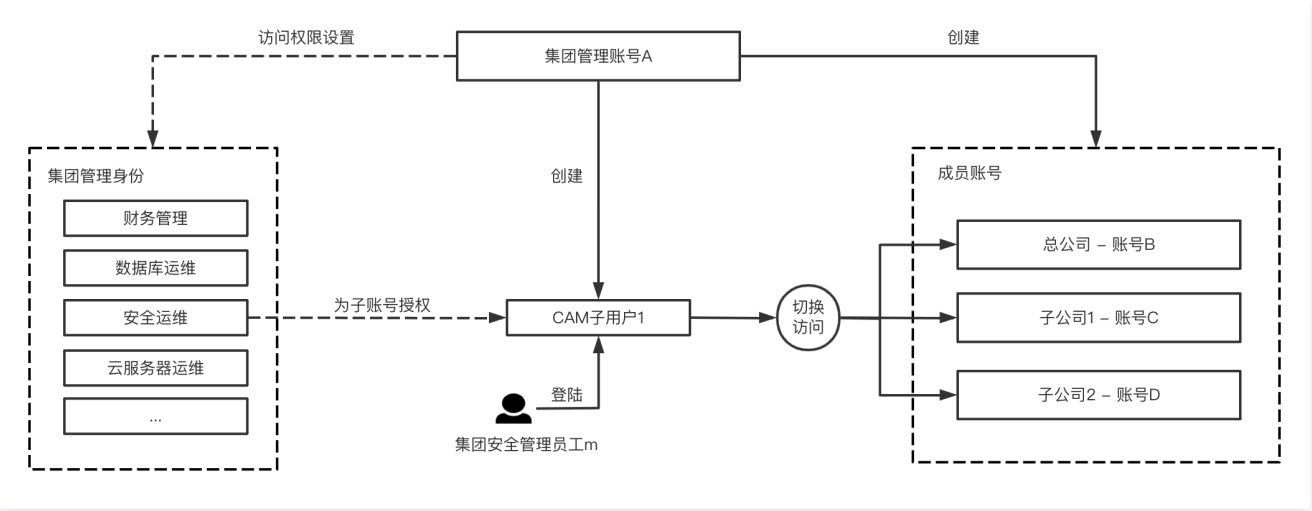
管理方式	特性说明
集团账号	图形化界面操作简易，只支持同一个集团内的企业实名账号使用。
角色	需要在每个被管理主账号下创建角色，操作流程相对较长。
协作者	只支持主账号作为协作对象。

集团账号

最近更新时间：2024-11-28 15:34:01

集团账号简介

集团账号管理是腾讯云上面向集团客户的多账号管理产品，支持集团管理员统一管理集团及旗下子公司的腾讯云主账号，提供账号、财务、安全等的管理能力，更多说明请参见 集团账号管理文档 。
在集团账号管理中，管理账号可以为 CAM 子账号同时授予多个创建的成员账号的管理权限，授权后，该 CAM 子账号支持只登录一次，就可以选择成员，访问管理多个成员账号。



操作场景

假设某集团在腾讯云有账号 A 和账号B，选择账号 A 作为管理账号开通按账号管理产品，集团内有子公司1和子公司2，分别有账号 C 和账号 D。集团内有安全管理员工 m，希望能够同时运维管理集团及其子公司的账号。
这时集团管理账号可以为员工 m 创建 CAM 子用户1，并授予账号 B、C、D 的安全运维权限，则员工通过 CAM 子用户1登录腾讯云控制台后，可以选择不同的成员账号进行切换执行安全运维的相关操作，无需在每个账号下分别为员工创建 CAM 子用户。

操作步骤

添加授权

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

使用子用户登录

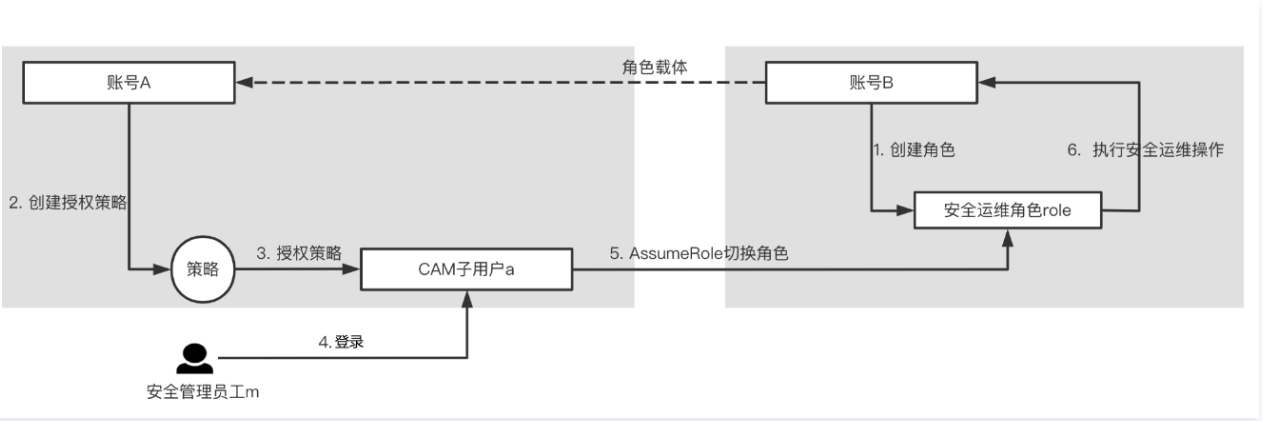
使用 CAM 子用户登录**集团账号管理控制台** > 选择左侧导航栏中的 成员登录 。在**成员登录**页面中，选择需要登录的成员账号，并单击操作列的**登录账号**，在弹出的**登录账号**窗口中选择登录权限进行登录。

角色

最近更新时间：2024-10-11 09:44:41

角色简介

角色是 CAM 的一种虚拟用户，可以被授予权限策略，拥有所属主账号的相应权限，详细信息请参见 角色概述 。
在创建角色时，可以选择以腾讯云主账号作为角色载体、创建角色，并为角色绑定授权策略。作为载体的主账号可以通过创建权限策略，将扮演角色的权限授予其 CAM 子账号，之后 CAM 子账号可以在腾讯云控制台通过切换角色登录到对应的主账号控制台执行授权范围内的操作，也可以通过云 API 发起跨账号请求。



操作场景

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

操作步骤

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

协作者

最近更新时间：2024-10-10 17:42:11

协作者简介

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

操作场景

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

操作步骤

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

查看员工腾讯云操作记录

最近更新时间：2024-10-11 14:36:51

操作场景

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

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

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

前提条件

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

操作步骤

查看操作记录事件详情

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

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

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

详细操作请参见：查看操作记录事件详情 。

使用跟踪集投递日志

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

设置集团账号跨账号日志投递

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

使用 API 管理企业多账号权限

最近更新时间：2024-11-28 15:34:01

操作场景

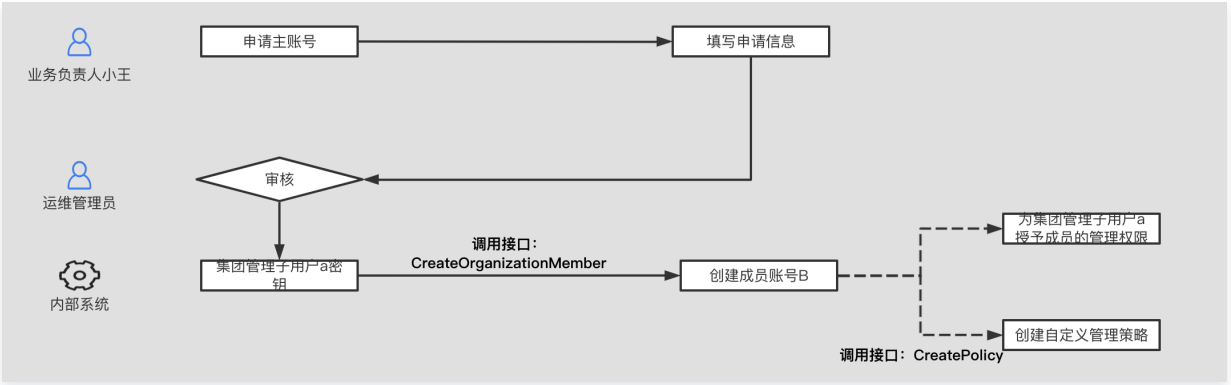
很多企业客户会在企业内部构建 IT 系统来管理员工子账号申请的流程，当企业内有多个账号时，将集团账号和 CAM 结合使用能够大幅提升管理的效率和安全性。
假设存在以下条件：

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

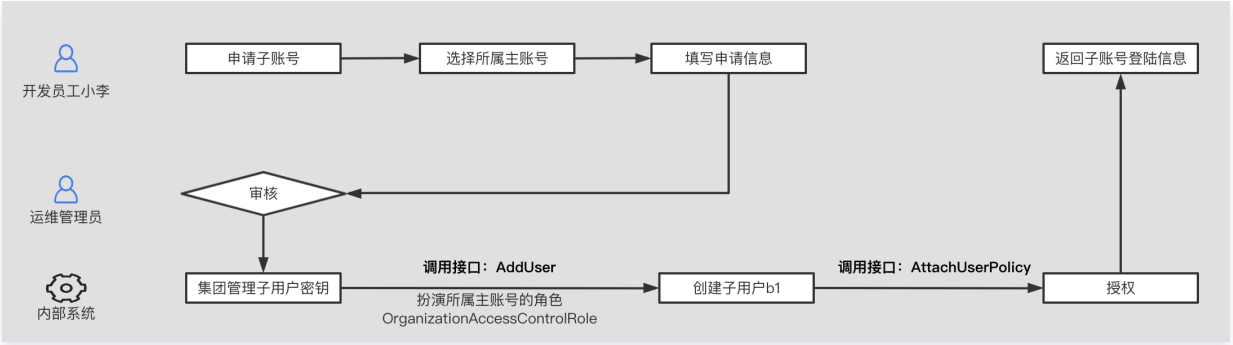
流程说明

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

- 流程1：为新游戏申请主账号



- 流程2：为开发员工小李创建 CAM 子账号并授权



操作步骤

使用管理子用户 Administrator 为新业务创建账号

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

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

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

> **说明**
> 如使用预设策略可以满足授权需要，则可忽略该步骤。

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

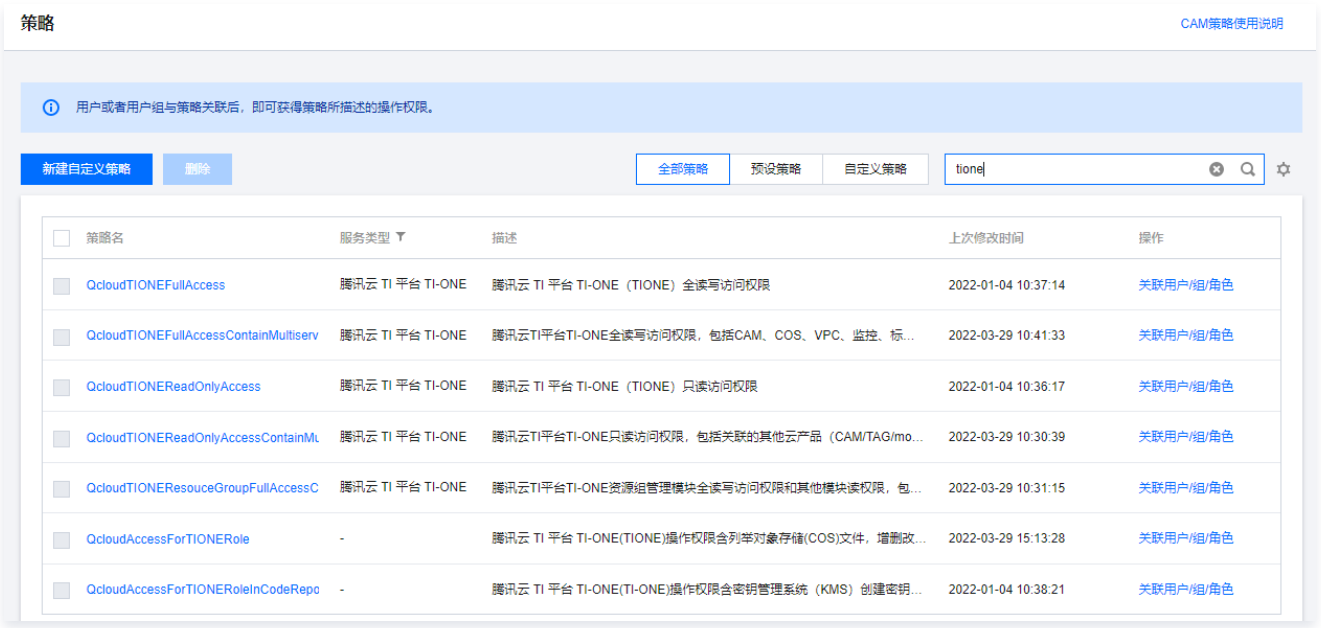
使用管理子用户 Administrator 为员工创建 CAM 子账号

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

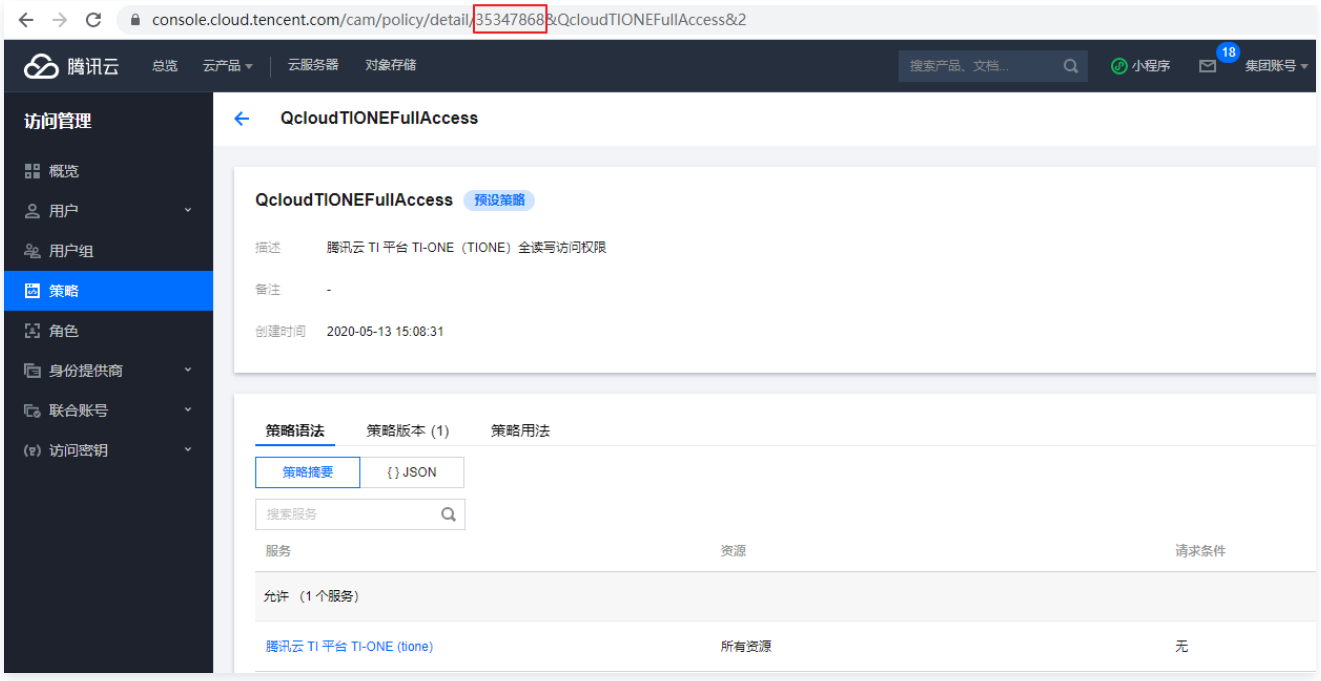
> **说明**
> 子用户的创建需要使用管理员身份，并扮演创建的成员的角色 OrganizationAccessControlRole，API 使用角色的调用请参见 使用角色 文档。

2. 获取需要绑定策略的策略 ID。

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



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



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

使用 ABAC 管理员工资源访问权限

ABAC 概述

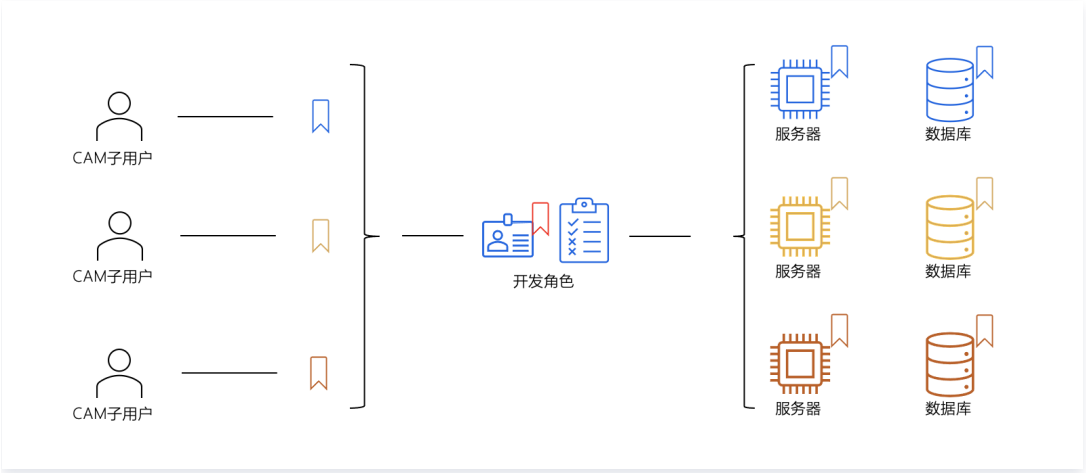
最近更新时间：2024-10-10 17:54:54

ABAC 简介

什么是 ABAC

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

假设有三个项目 GroupA、GroupB 和 GroupC，分别有开发员工 a、b、c，您可以通过以下步骤管理员工资源访问权限：
1. 为三个员工分别创建标签键为 GroupA、GroupB、GroupC 的三个CAM子用户，标签值为 dev，并为三个子用户授予 assumeRole 的权限。
2. 创建开发角色，角色对应的标签的值为 dev。
3. 使用单个策略，允许访问三个项目下的资源，将策略附加给创建好的角色。
4. 员工通过 CAM 子用户代入角色来访问，当员工的标签键和资源的标签值相同时，允许访问。



ABAC 与传统授权方式对比

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

授权方式	ABAC 授权	传统授权
三个项目相同岗位的授权	1. 三个子用户 2. 一个角色 3. 两个策略（三个子用户共用一个角色切换策略，一个角色一个权限管理策略）	1. 三个子用户 2. 三个角色 3. 六个策略（每个子用户一个角色切换策略，每个角色一个权限管理策略）
单个项目添加/减少资源	无需调整授权策略	调整角色对应的权限管理策略
增加新的项目	只需要创建新的子用户	需要创建新的子用户、角色以及关联的两个策略

ABAC 授权的优势

使用 ABAC 管理资源访问权限具备以下优势：

自动扩展资源权限

支持权限随着资源的变更自动扩展，不再需要管理员更新现有策略来允许访问新的资源。
例如：假设您使用 access-project 标签附加到 ABAC 策略。开发人员使用access-project = GroupA 的标签来访问资源。当GroupA项目中的员工需要额外的 CVM 云服务器资源时，开发人员可以使用 access-project = GroupA 标签创建新 CVM 实例。创建后，GroupA 项目中的任何授权员工可以启动和停止这些实例，因为 GroupA 项目的员工对应角色的标签与资源的标签匹配。

减少策略数量

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

方便后续扩展策略

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

实现精细权限控制

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

应用场景

最近更新时间：2024-02-29 15:34:01

操作场景

在腾讯云的实际使用中，通过 ABAC 的授权策略，我们可以使用标签来定义权限。将标签绑定到 CAM 子用户、角色以及具体的云资源，之后可以定义权限策略，这些策略使用标签条件键来根据请求身份的标签向其授予权限。当您使用标签控制对腾讯云资源的访问时，可通过对授权策略进行较少更改来实现团队和资源的变更，操作更加灵活。
本章节将详细说明如何为员工在 CAM 中创建一个带有标签的 CAM 角色，以及支持通过带入角色的属性拥有访问与其标签匹配的资源的权限策略。当员工通过该角色向腾讯云发出请求时，将根据带入的角色标签和资源标签是否匹配来授予权限，实现仅允许员工查看或操作其工作需要的资源。

使用示例

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

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

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

我们根据上述项目和团队，做以下标签定义：
- game-project = web（对应 web 项目）
- game-project = app（对应 app 项目）
- web = dev（对应 web 项目开发人员）
- app = dev（对应 app 的开发人员）
- game=dev（对应 web/app 项目开发人员）

实现原理

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

验证场景

假设有两台云服务器 ins-78qewdr8（标签 game-project:app）和 ins-7txjj4a6（标签 game-project:web），分别属于 app 和 webpage 项目。
- 验证点1：不同项目的员工使用不同的 CAM 子用户登录后，如何实现不同员工只能访问到其所属项目下的云服务器。
- 验证点2：假设员工岗位变更，员工 n 也需要项目 webpage 的权限，如何快速调整权限。
- 验证点3：假设公司新增加一个 H5 类的项目，如何快速为员工授予新项目的权限。

操作步骤

步骤1：创建测试 CAM 子用户

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

> **说明**
> 创建 CAM 策略的详细操作，请参见 通过策略语法创建自定义策略。

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

```
            "sts:AssumeRole"
        ],
        "resource": "*",
        "condition": {
            "for_any_value:string_equal": {
                "qcs:resource_tag": [
                    "game&${qcs:principal_tag_value}"
                ]
            }
        }
    },
    {
        "effect": "allow",
        "action": [
            "cam:ListUserTags",
            "cam:ListLoginRoles"
        ],
        "resource": [
            "*"
        ]
    }
 ]
}
```

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

> **说明**
> 创建 CAM 子用户的详细操作，请参见 新建子用户 。

子用户名称	关联标签
m-developer	web=dev
n-developer	app=dev

步骤2：创建 ABAC 策略

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

```
{
 "version": "2.0",
 "statement": [
    {
        "effect": "allow",
        "action": "cvm:*",
        "resource": "*",
        "condition": {
            "for_any_value:string_equal": {
                "qcs:request_tag": [
                   "game-project&${qcs:principal_tag_key}"
                ]
            }
        }
    },
    {
        "effect": "allow",
        "action": "cvm:*",
        "resource": "*",
        "condition": {
            "for_any_value:string_equal": {
```

```
                "qcs:resource_tag": [
                    "game-project&${qcs:principal_tag_key}"
                ]
            }
        }
    },
     {
        "effect": "allow",
        "action": [
            "vpc:DescribeVpcEx",
            "vpc:DescribeSubnetEx",
            "vpc:DescribeNetworkInterfaces",
            "cvm:DescribeDiskSecurityConfigurations",
            "cvm:DescribeCbsStorages",
            "tag:DescribeTagKeys",
            "tag:DescribeTagValues"
        ],
        "resource": [
            "*"
        ]
    }

 ]
}
```

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

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

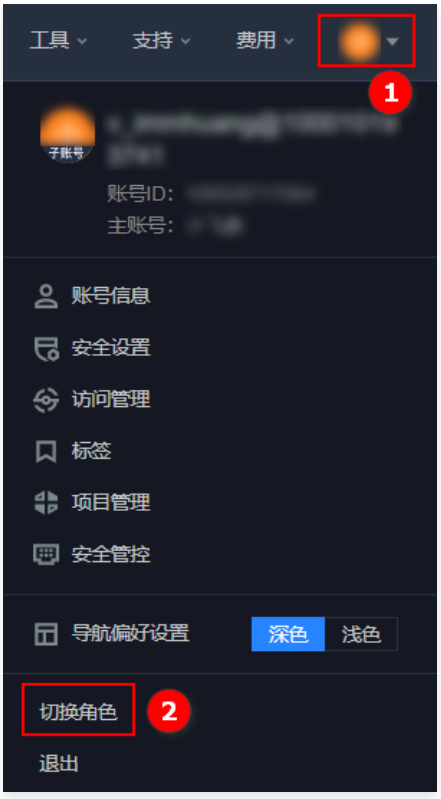
> **说明**
> 创建 CAM 角色的详细操作，请参见 创建角色 。

CAM 角色名称	关联标签
access-developer-role	game=dev

步骤3：场景验证

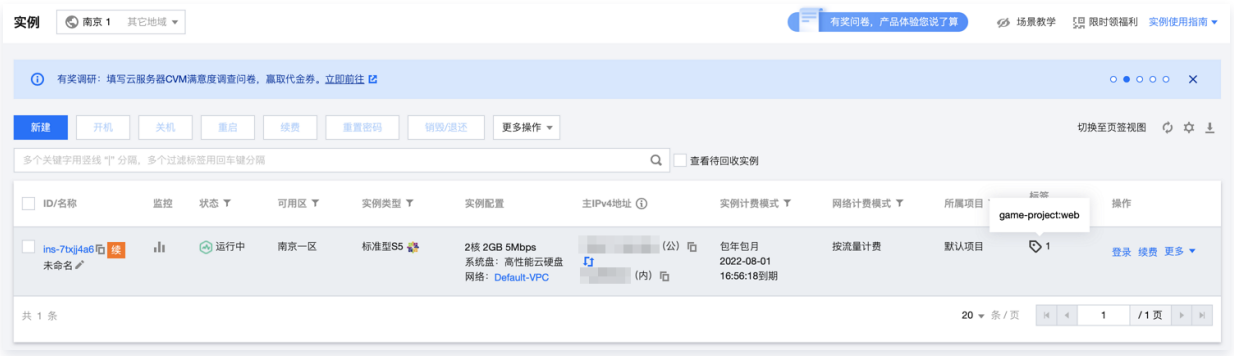
验证点1：使用不同的子用户登录后，只能访问到对应项目下的云服务器

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



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

3. 以角色身份登录腾讯云控制台，进入 CVM **实例** 页面。
在 CVM 产品控制台，若仅可以查看到 ins-7txjj4a6（标签 game-project:web），则符合预期。



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

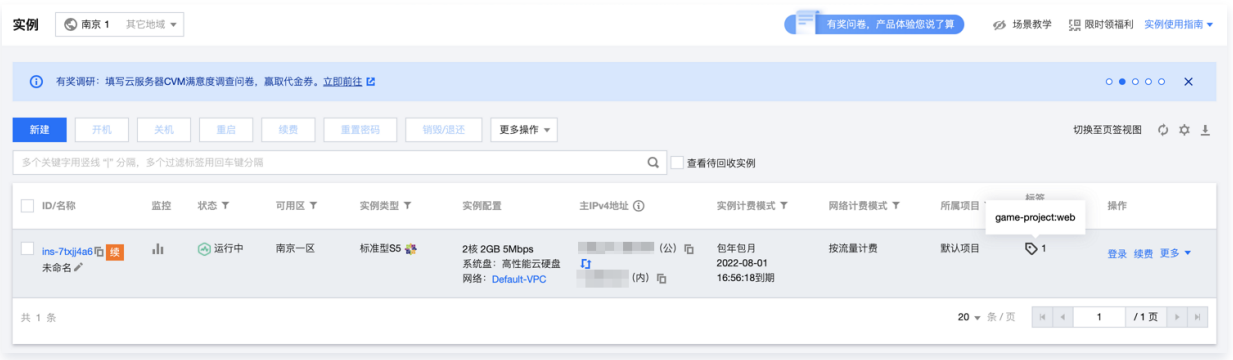
5. 以角色身份进入腾讯云控制台，进入 CVM **实例** 页面。
在 CVM 产品控制台，若仅能查看云服务器 ins-78qewdr8（标签 game-project:app），则符合预期。

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

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

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

3. 以角色身份登录腾讯云控制台，进入 CVM **实例** 页面。
   在 CVM 产品控制台，若仅能查看云服务器 ins-7txjj4a6（标签 game-project:web），则符合预期。



验证点3：假设公司新增加一个 H5 类的项目，该如何调整权限策略适配

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

1. 为 H5 项目的开发同事创建新的子用户。
2. 为子用户绑定 H5 项目对应的标签，关联 access-assume-role 策略即可。

按标签鉴权时支持仅匹配标签键

最近更新时间：2024-10-11 11:55:22

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

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

授予关联某个标签键下所有资源的权限（resource_tag）

操作场景

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

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

操作步骤

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

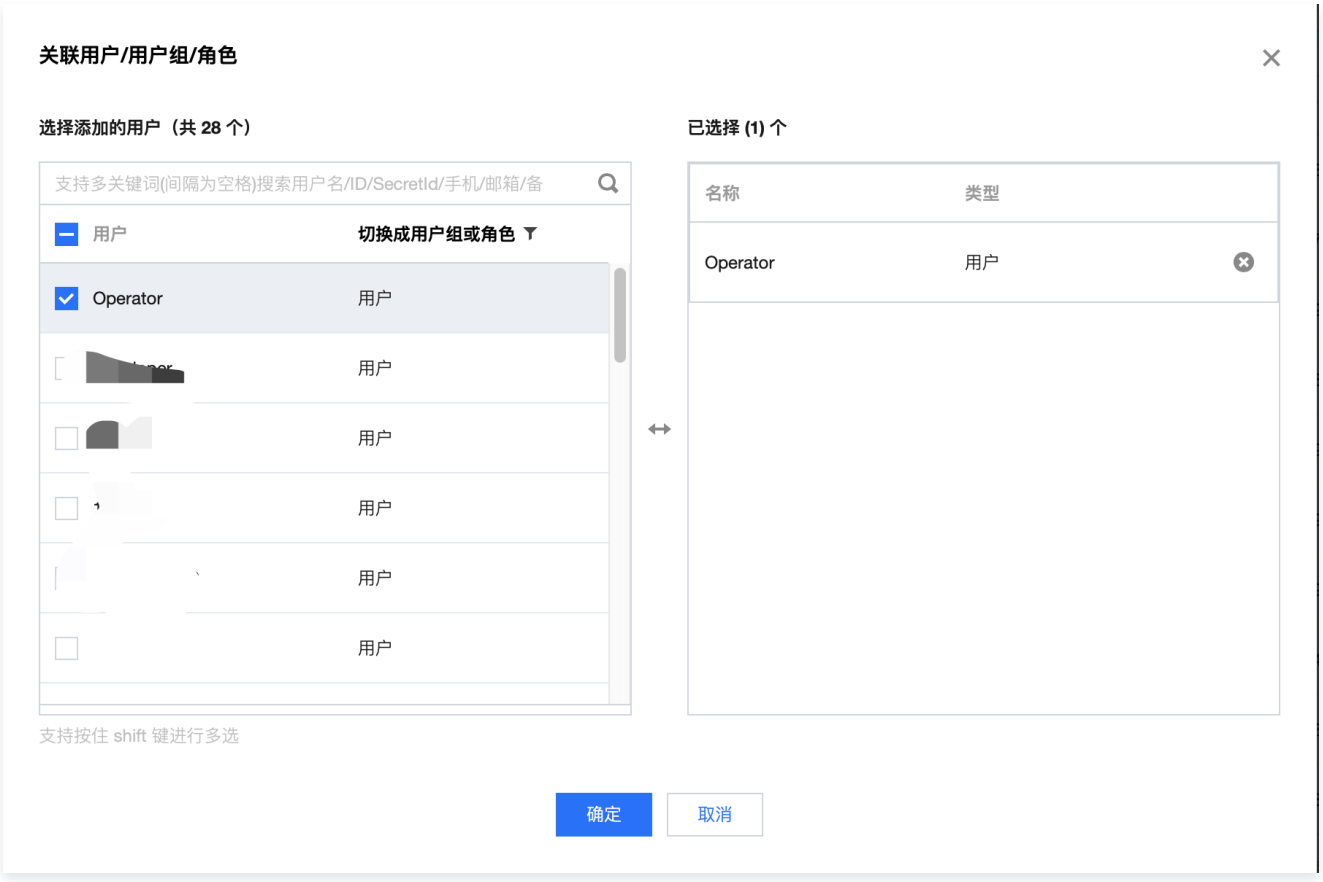
4. 进入编辑策略页面，填写如下表单：
   - 策略名称：默认为 `policygen-当前日期` ，推荐您自行定义一个不重复且有意义的策略名称，例如 Operator-resource_tag 。
   - 描述：可选，自行编写。
   - 策略内容：复制以下内容并填写。其中，运营 为标签键名称，可为中文和英文， `false` 为固定的标签值。

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

```
            "resource": "*",
            "condition": {
                "null_equal": {
                    "qcs:resource_tag/运营": "false"
                }
            }
        }
    ]
}
```

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

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



授予子账号只能绑定某个标签键的权限（request_tag）

操作场景

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

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

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

操作步骤

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

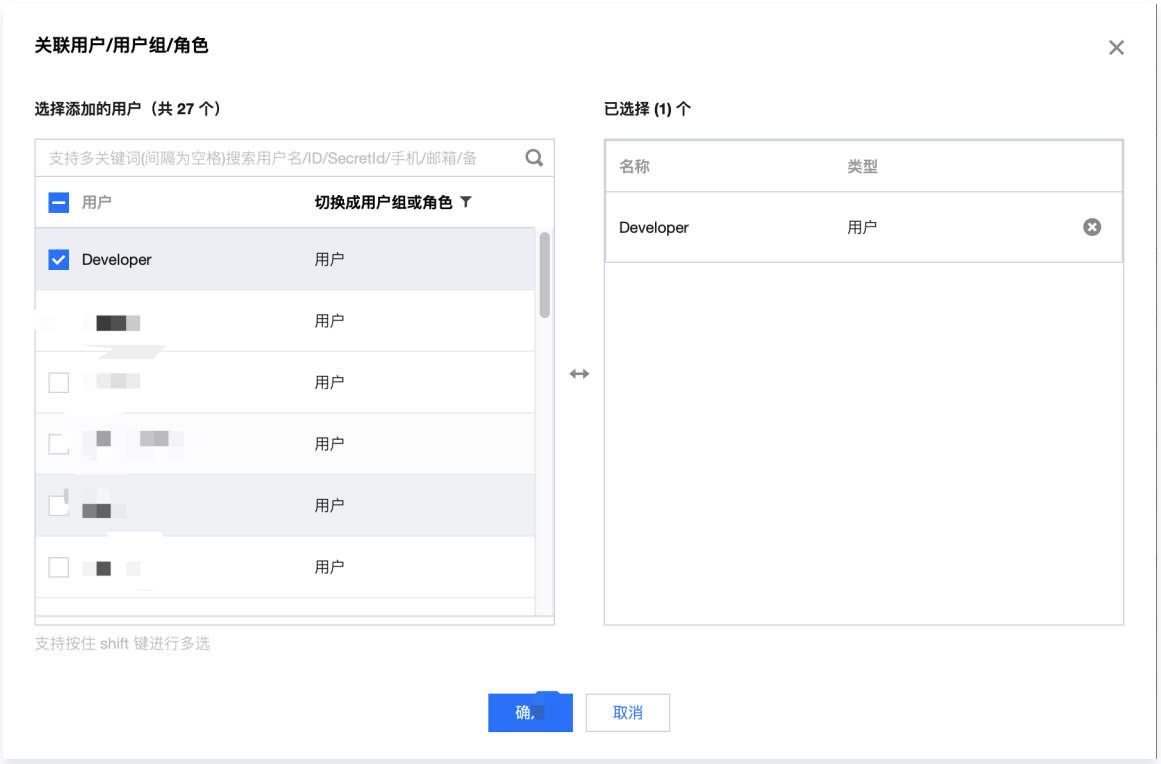
4. 进入编辑策略页面，填写如下表单：
   - 策略名称：默认为 `policygen-当前日期` ，推荐您自行定义一个不重复且有意义的策略名称，例如 Developer-request_tag。
   - 描述：可选，自行编写。
   - 策略内容：复制以下内容并填写。其中，开发 为标签键名称，可为中文和英文， `false` 为固定的标签值。

```
{
"version": "2.0",
 "statement": [
   {
       "effect": "allow",
       "action": "*",
       "resource": "*",
       "condition": {
           "null_equal": {
               "qcs:request_tag/开发": "false"
           }
       }
   }
 ]
}
```

5. 单击**完成**，完成策略的创建。新建的策略将显示在策略列表页。

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

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



关联文档

如果您想了解如何将资源和标签建立关联关系，请参见 管理标签 。

创建资源时强制绑定固定标签键值

最近更新时间：2024-11-28 11:21:41

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

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

操作场景：

若您希望您的子账号（Operator ）在购买云服务器（CVM）资源时，只能绑定某个标签键值的权限。
假设存在以下条件：
企业账号 CompanyExample 下有个子账号 Operator 。
企业账号 CompanyExample 下有个为（App&Dev）的标签键值。
企业账号 CompanyExample 希望给子账号 Operator 授予只能绑定（App&Dev）标签键值的权限。

操作步骤

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

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

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": "cvm:*",
            "resource": "*",
            "condition": {
                "for_any_value:string_equal": {
                    "qcs:request_tag": [
```

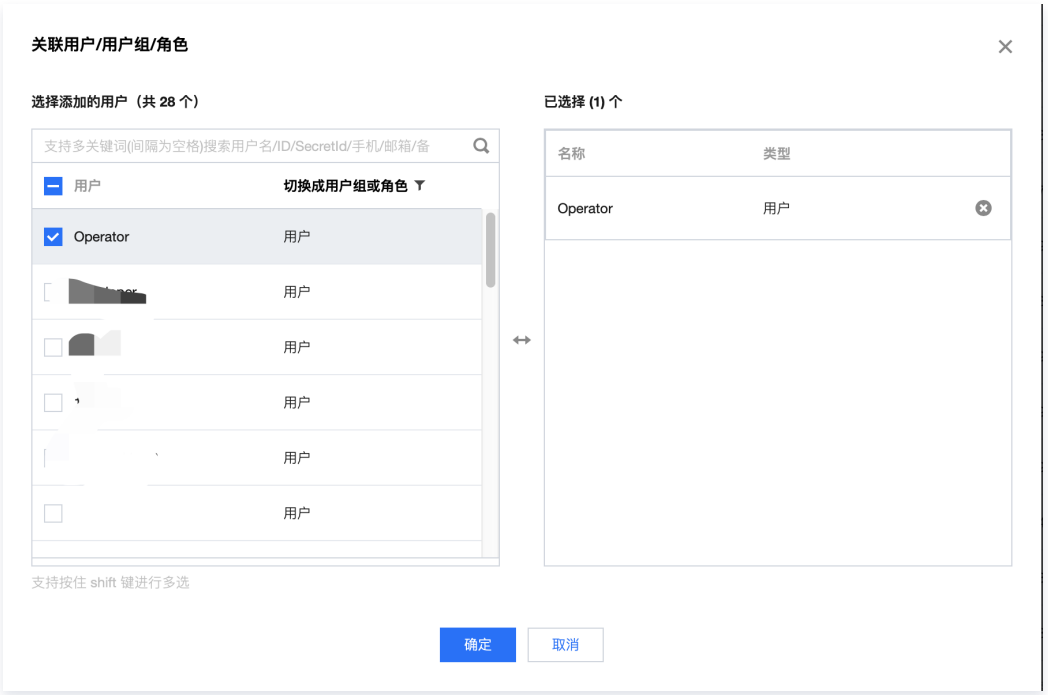
```
                        "App&Dev"
                    ]
                }
            }
        },
        {
            "effect": "allow",
            "action": "cvm:*",
            "resource": "*",
            "condition": {
                "for_any_value:string_equal": {
                    "qcs:resource_tag": [
                        "App&Dev"
                    ]
                }
            }
        },
        {
            "effect": "allow",
            "action": [
            "cvm:CreateSecurityGroup",
            "tag:*",
            "vpc:*"
            ],
            "resource": "*"
        }
    ]
}
```

说明：

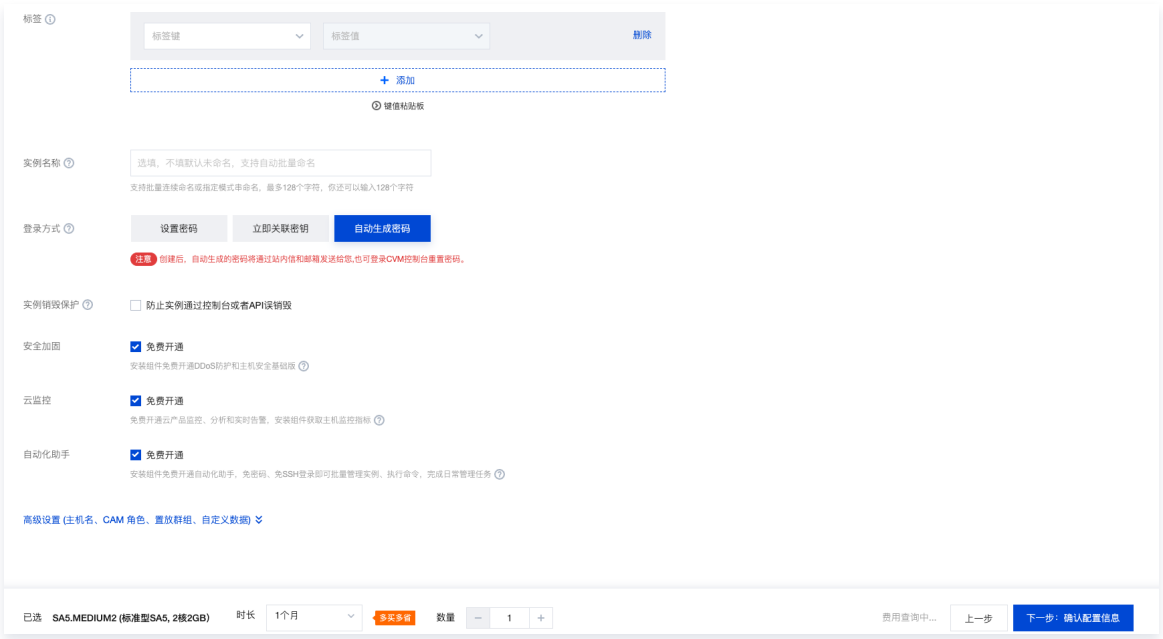
- 通过 qcs:resource_tag 控制：可以访问所有绑定标签（App&Dev）的资源。
- 通过 qcs:request_tag 控制：在创建资源的时候必须绑定标签（App&Dev）才能成功。
- 其他不支持资源级授权的接口需要在最后一个 `effect` 里面附加授予，本策略增加了 cvm:CreateSecurityGroup 和 tag、vpc 权限，可按需添加。

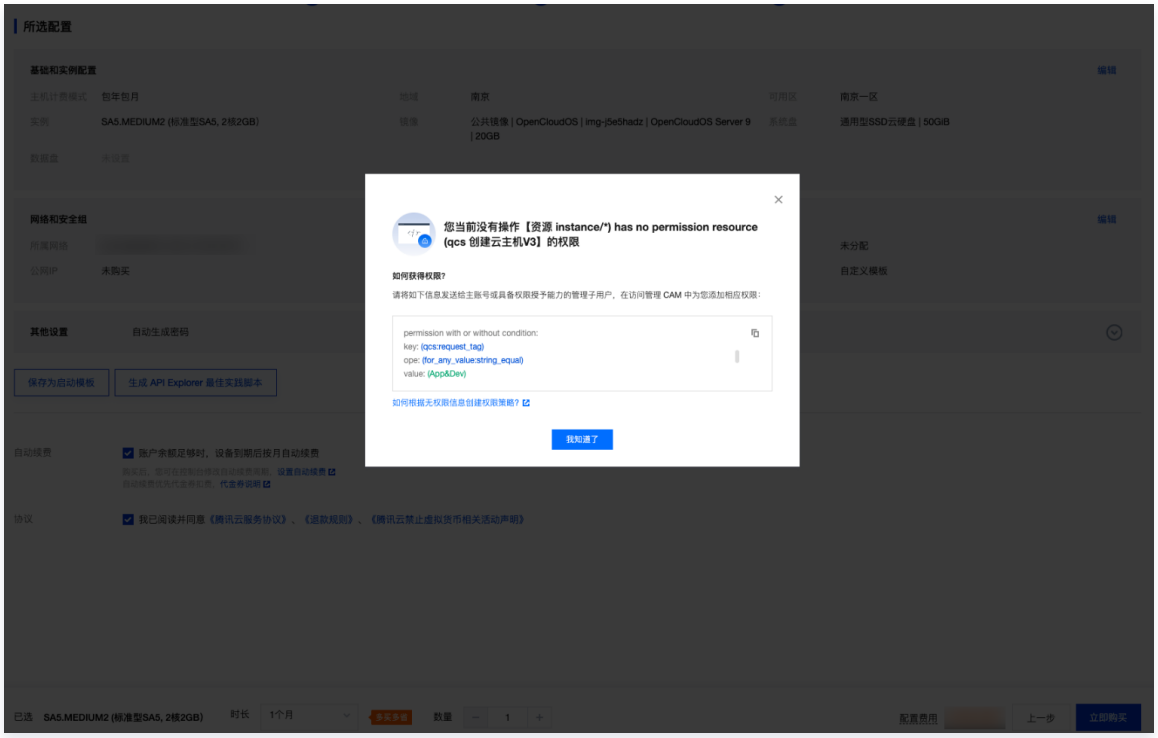
5. 单击**完成**，完成策略的创建。新建的策略将显示在策略列表页。
6. 在策略列表中搜索找到刚才已创建的策略，单击右侧操作列的**关联用户/组/角色**。

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

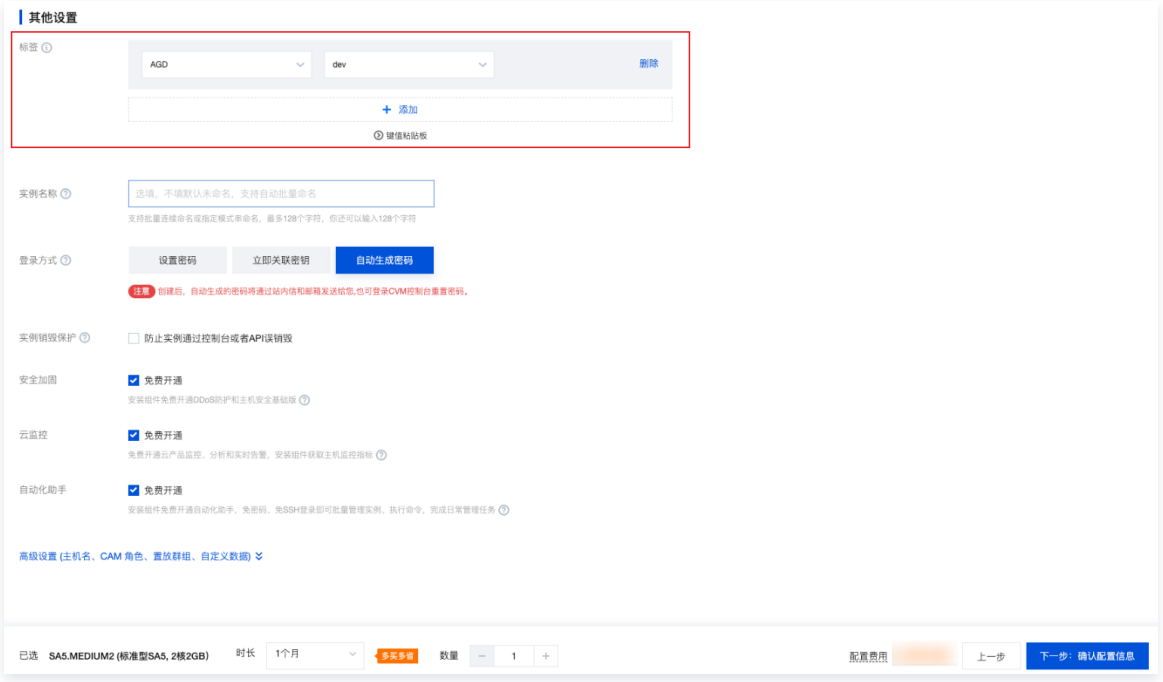


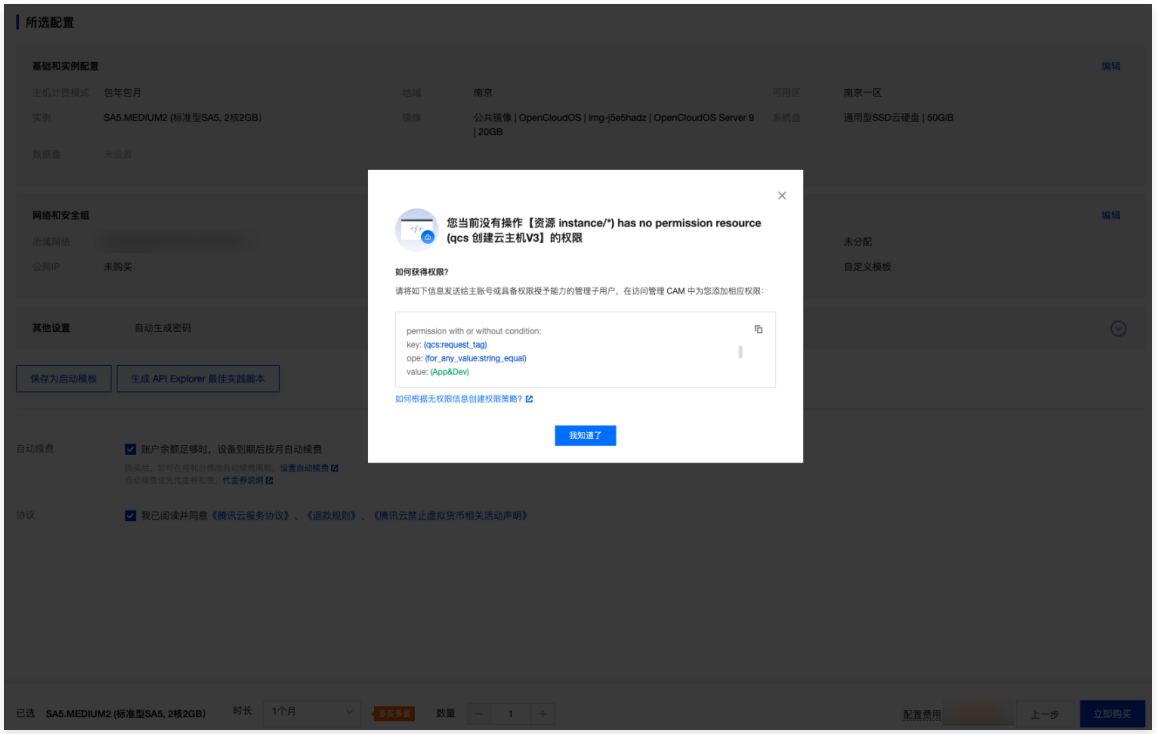
8. 登录子账号 Operator，在不设置标签和不设置对应标签（App&Dev）的情况下，尝试购买服务器。
   - 不设置标签情况下，购买失败。



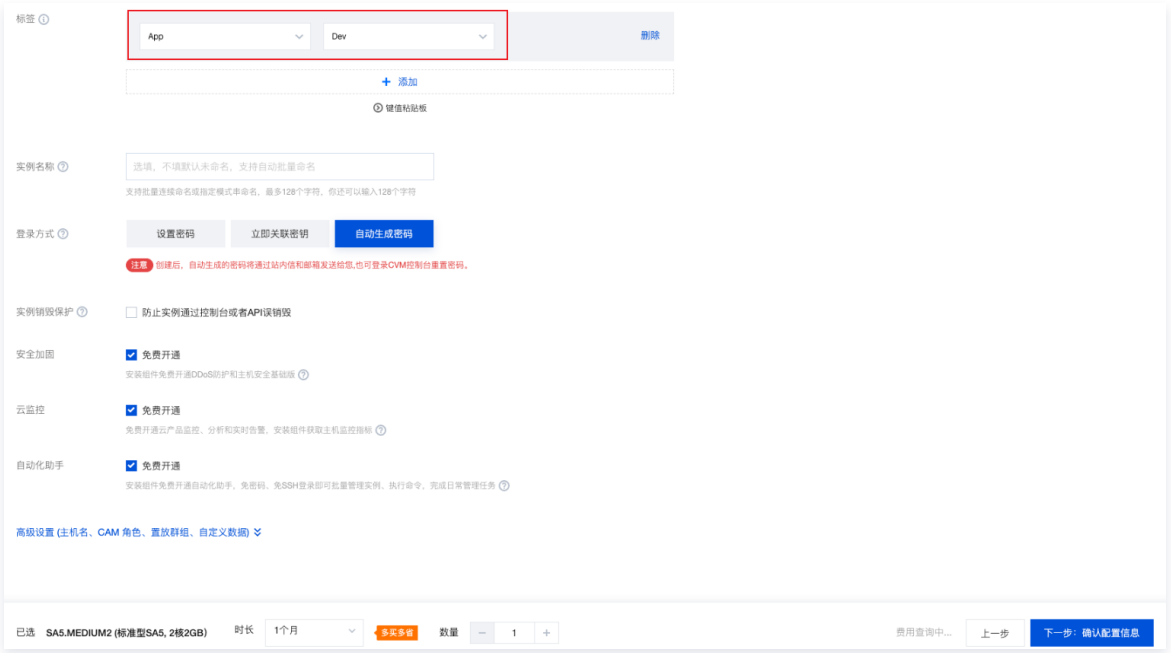


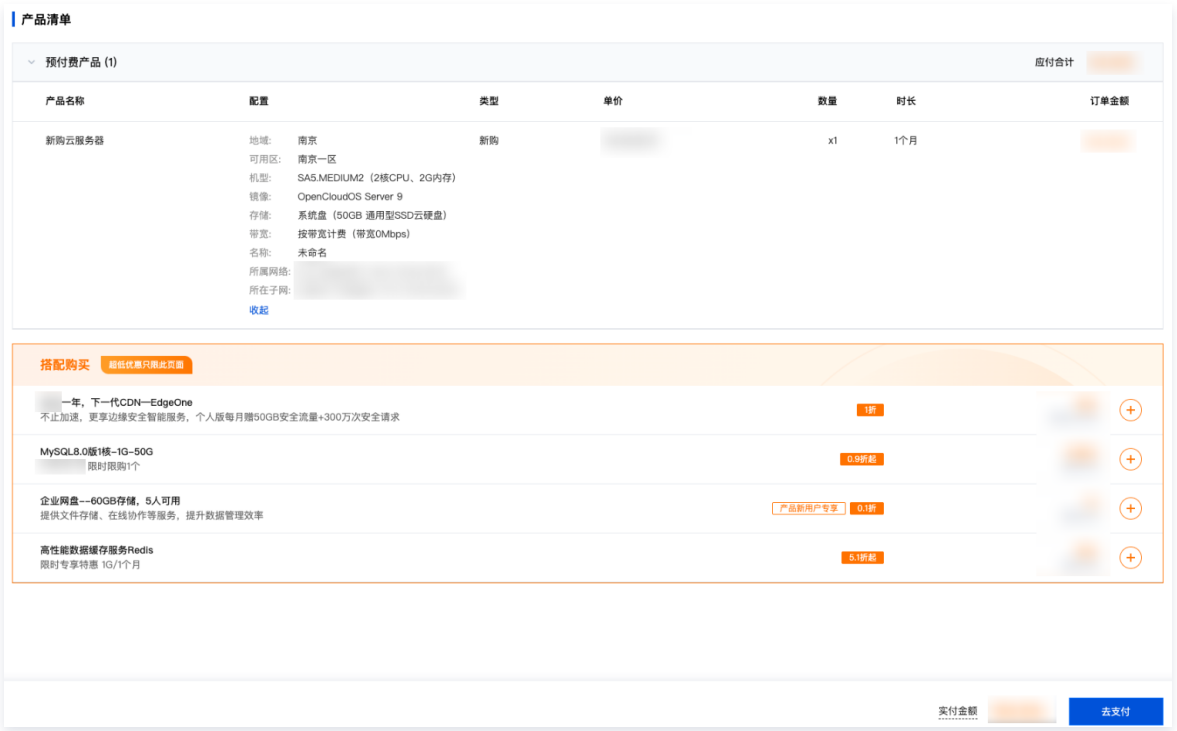
- 不设置对应标签（App&Dev）情况下，购买失败。





- 在设置对应标签（App&Dev）情况下，购买成功。




产品清单
预付费产品 (1)
应付合计
产品名称
配置
类型
单价
数量
时长
订单金额
新购云服务器
地域: 南京
可用区: 南京一区
机型: SA5.MEDIUM2（2核CPU、2G内存）
镜像: OpenCloudOS Server 9
存储: 系统盘（50GB 通用型SSD云硬盘）
带宽: 按带宽计费（带宽0Mbps）
名称: 未命名
所属网络:
所在子网:
收起
新购
x1
1个月
搭配购买
超低优惠只限此页面
一年，下一代CDN—EdgeOne
不止加速，更享边缘安全智能服务，个人版每月赠50GB安全流量+300万次安全请求
1折
MySQL8.0版1核-1G-50G
限时限购1个
0.9折起
企业网盘--60GB存储，5人可用
提供文件存储、在线协作等服务，提升数据管理效率
产品新用户专享
0.1折
高性能数据缓存服务Redis
限时专享特惠 1G/1个月
5.1折起
实付金额
去支付

使用 MFA 保护 API 请求

最近更新时间：2025-04-11 15:17:12

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

操作场景

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

典型场景示例：

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

前提条件

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

注意事项

MFA 设备限制

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

操作步骤

步骤 1：绑定虚拟 MFA 并开启登录保护

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

步骤 2：创建 MFA 保护策略

1. 策略语法

在 CAM 策略中，通过 condition 字段添加 qcs:mfaPresent 条件键，限制 API 调用必须附带 MFA 认证。

示例策略（限制终止 CVM 实例）：

```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": "cvm:TerminateInstances",
      "resource": "*",
      "condition": {
        "bool_equal": {
          "qcs:mfaPresent": "true"
        }
      }
```

```
    }
  ]
}
```

2. **策略关联**

将策略关联至目标用户/用户组，确保权限生效。

步骤 3：调用支持 MFA 的 API

用户需通过以下方式获取临时凭证并调用 API：

方式 1：GetSessionToken（获取 MFA 临时凭证）

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

```
curl -X POST <https://sts.tencentcloudapi.com> \
-H "Authorization: TC3-HMAC-SHA256 ..." \
-d '{
  "Action": "GetSessionToken",
  "Name": "temp_token",
  "Policy": "{\"version\":\"2.0\", ...}",
  “SerialNumber”:"qcs::cam:uin/12345678::mfa/softToken", # 输入虚拟MFA序列号
  "MfaCode": "123456"  # 输入虚拟 MFA 动态口令
}'
```

使用示例

场景：强制删除 COS 存储桶前验证 MFA

1. **策略配置**

```
{
"version": "2.0",
"statement": [
  {
    "effect": "allow",
    "action": "cos:DeleteBucket",
    "resource": "qcs::cos:ap-guangzhou:uid/12345678:bucket/example-1250000000/*",
    "condition": {
      "bool_equal": {
        "qcs:mfaPresent": "true"
      }
    }
  }
]
}
```

2. **用户操作**

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

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

方式 2：AssumeRole（角色代入）

- **适用场景：**跨账号访问或角色委托。
- **API 调用示例：**

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