

云点播-混合云版

快速入门

产品文档



腾讯云

【版权声明】

©2013-2024 腾讯云版权所有

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

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

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

快速入门

最近更新時間：2024-01-30 16:32:14

本文將指引您如何開通云點播-混合云版，並創建一個可用的云點播-混合云版應用。

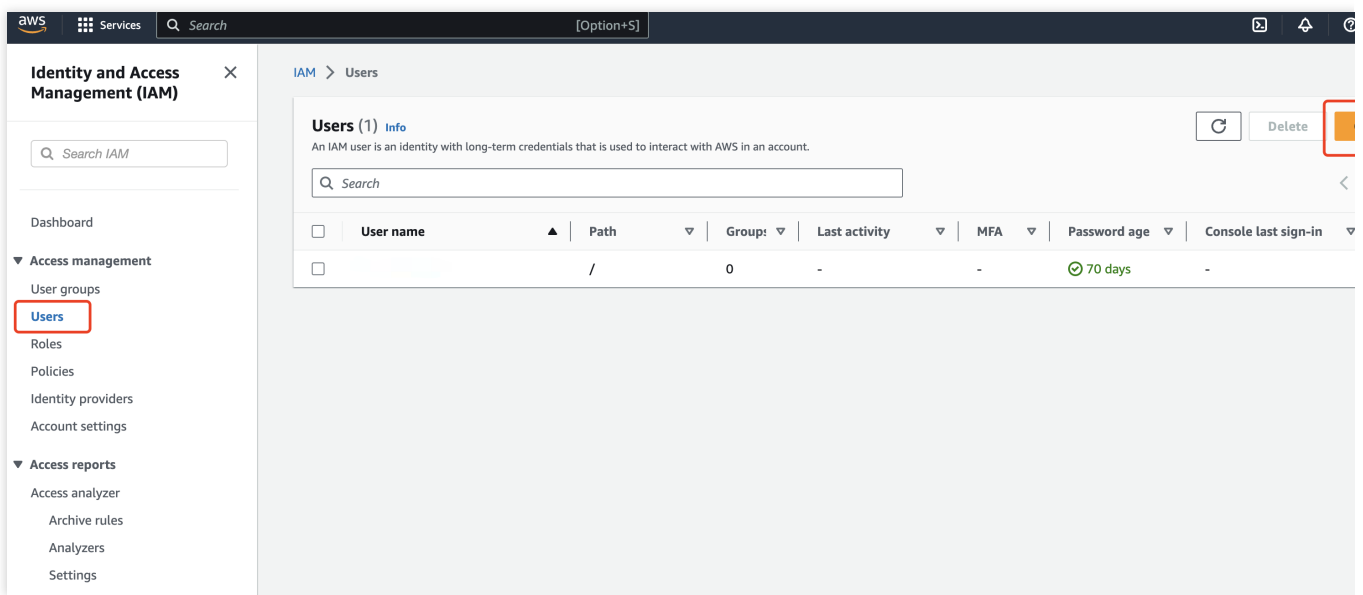
准备工作

已完成註冊的騰訊雲賬號

已完成註冊的第三方存儲服務，並準備好一個已上傳媒體文件數據的存儲桶，以 AWS 的 S3 存儲服務為例：已有一個可用的 AWS S3 存儲桶，存儲桶名為 BucketforVodeo，存儲桶地域為 Asia Pacific (Sydney) ap-southeast-2。

步骤一：创建AWS子用户并保存用户密钥

1. 进入 [Identity and Access Management \(IAM\)](#) 界面单击 **Users**，再单击 **Create user** 添加用户。



2. 輸入 **User name**，单击右下角 **Next**。

Specify user details

User details

User name

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☐ Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

i If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel

3. 选择 **Attach policies directly**，在搜索框中输入 S3 搜索，在搜索结果中找到 **AmazonS3FullAccess** 并勾选，单击右下角 **Next**。

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☐ Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

☒ Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policy instead. Then, add the user to the appropriate group.

Permissions policies (1/1121)

Choose one or more policies to attach to your new user.

Filter by Type

All types

11 matches

<input type="checkbox"/>	<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	<input type="checkbox"/>	AmazonDMSRedshiftS3Role	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	0
<input type="checkbox"/>	<input type="checkbox"/>	AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	0
<input type="checkbox"/>	<input type="checkbox"/>	AmazonS3OutpostsFullAccess	AWS managed	0
<input type="checkbox"/>	<input type="checkbox"/>	AmazonS3OutpostsReadOnlyAccess	AWS managed	0
<input type="checkbox"/>	<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed	0
<input type="checkbox"/>	<input type="checkbox"/>	AWSBackupServiceRolePolicyForS3Backup	AWS managed	0
<input type="checkbox"/>	<input type="checkbox"/>	AWSBackupServiceRolePolicyForS3Restore	AWS managed	0
<input type="checkbox"/>	<input type="checkbox"/>	IVSRecordToS3	AWS managed	0
<input type="checkbox"/>	<input type="checkbox"/>	QuickSightAccessForS3StorageManagement...	AWS managed	0
<input type="checkbox"/>	<input type="checkbox"/>	S3StorageLensServiceRolePolicy	AWS managed	0

► Set permissions boundary - *optional*

Cancel

Pre

4. 单击 **Create user** 即可完成用户的创建。

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name [redacted]	Console password type None	Require password reset No
-------------------------	-------------------------------	------------------------------

Permissions summary

Name	Type	Used as
AmazonS3FullAccess	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

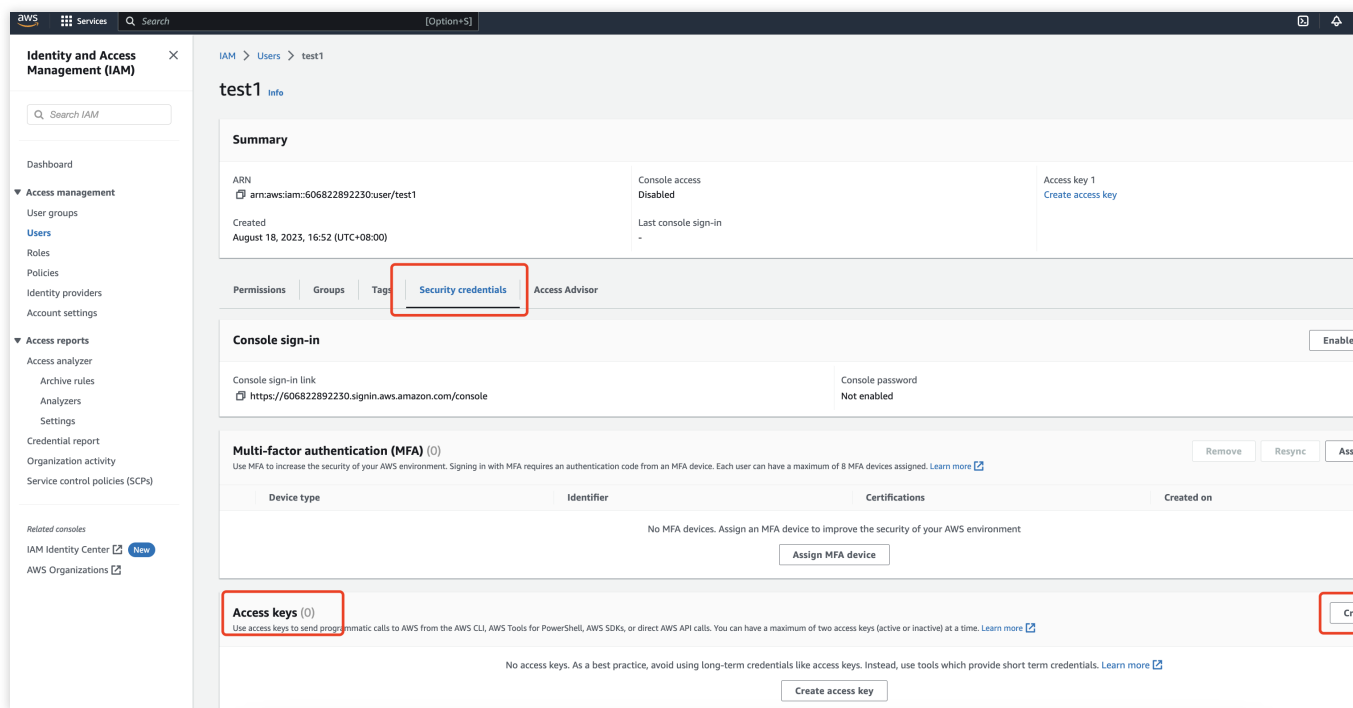
Cancel Previous Create

5. 创建完用户后，在 Users 列表中单击 **已创建好的 User name**。

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with 'Identity and Access Management (IAM)' selected. The main area displays a 'Users (2)' list. The list has columns: User name, Path, Group, Last activity, MFA, Password age, Console last sign-in, and Access key ID. The first user is highlighted with a red box around the 'User name' column header.

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access key ID
[redacted]	/	[redacted]	-	-	71 days	-	Active - AKIAVZSLWQL...
[redacted]	/	[redacted]	-	-	-	-	-

6. 单击 **Security credentials**，找到 **Access keys**，单击 **Create access key**。



7. 在 Use case 中选择 **Other**，单击 **Next** 进行创建，保存好创建的 **Access key ID** 和 **Secret access key**。

注意：

AWS S3 的 Secret access key 后续无法查看，请在创建后妥善复制保管。

Access key best practices & alternatives [Info](#)

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

☐ **Command Line Interface (CLI)**

You plan to use this access key to enable the AWS CLI to access your AWS account.

☐ **Local code**

You plan to use this access key to enable application code in a local development environment to access your AWS account.

☐ **Application running on an AWS compute service**

You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

☐ **Third-party service**

You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

☐ **Application running outside AWS**

You plan to use this access key to enable an application running on an on-premises host, or to use a local AWS client or third-party AWS plugin.

☒ **Other**

Your use case is not listed here.



It's okay to use an access key for this use case, but follow the best practices:

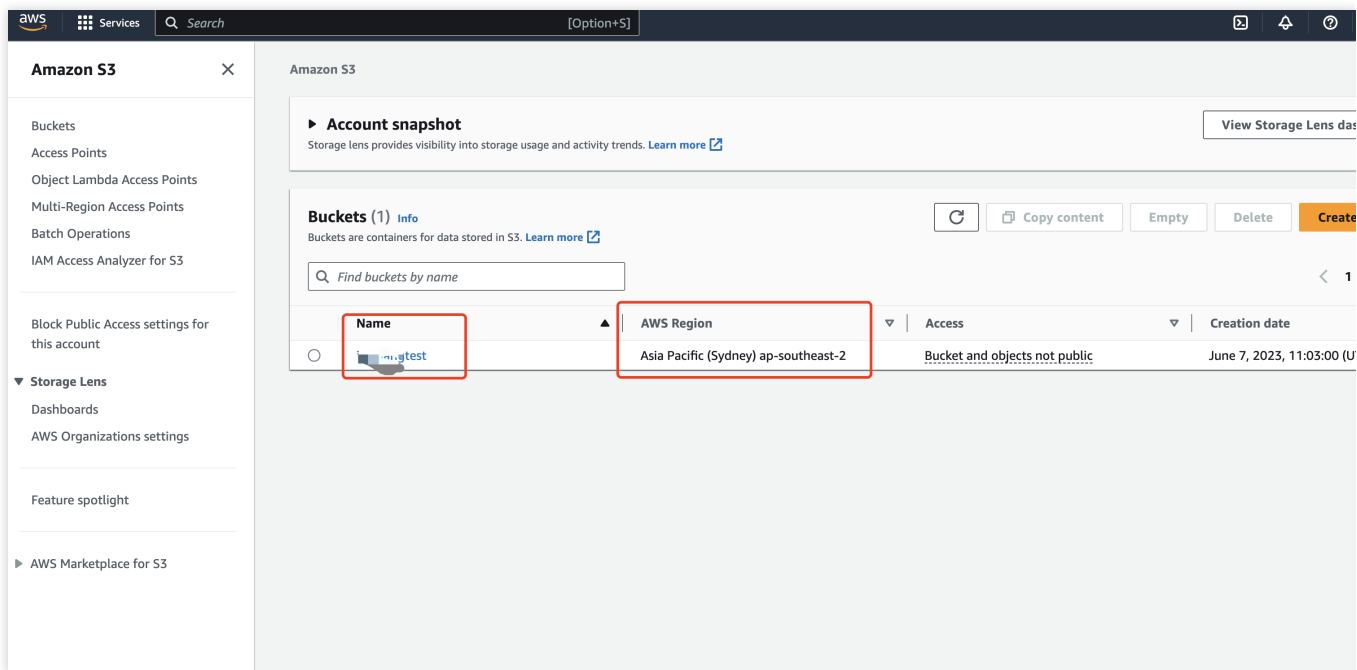
- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access keys when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

Cancel

步骤二：获取 AWS S3 存储桶信息

1. 进入 AWS S3 存储桶列表，复制需要绑定的存储桶名称及地域信息。



步骤三：创建云点播-混合云版应用

1. 进入云点播-混合云版 [控制台](#)，单击**开通并创建应用**。



2. 在创建应用页面，填写应用名称（40字以内）。

3. 填入步骤一创建的 Access key ID、Secret access key 以及步骤二获取的存储桶信息，并选择存储桶对应的区域，单击**创建**即可完成应用创建。

1 应用基本信息

应用名称*

请输入应用名称

应用名称不能超过40个字符

2 绑定存储桶

存储服务商*

腾讯云 COS

AWS S3

创建应用后，可以继续添加存储桶

帐号信息*

AccessKey*

请输入正确的AccessKey

SecretKey*

请输入正确的SecretKey

[存储托管授权指引](#)

选择存储桶*

区域*

US East (N. Virginia)

存储桶名称*

请输入正确的存储桶名称

创建

版权所有：腾讯云计算（北京）有限责任公司

第9 共9页