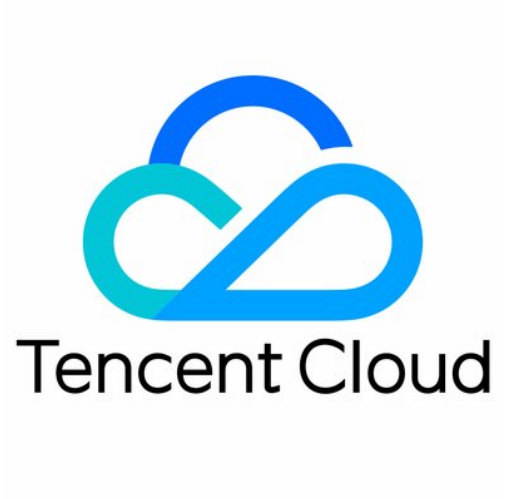
Security Token Service

Getting Started

Product Documentation



Contents

Getting Started
SAML 2.0-based Federation

Last updated：2022-05-20 10:25:44

Overview

Tencent Cloud supports federated authentication based on SAML 2.0 (Security Assertion Markup Language 2.0). If you already have your own account system and users, you can generate temporary security credentials for them to manage Tencent Cloud resources with limited permission, instead of creating a CAM sub-user.

Prerequisite

You already had your own account system and users.

How It Works

1. A user in your enterprise or organization uses a client app to request authentication from your organization's IdP.
2. The IdP authenticates the user against your enterprise's identity authorization system.
3. The user authentication result is returned.
4. The IdP generates a standard SAML 2.0 assertion document based on the user authentication result and sends it back to the client app.
5. The client passes the SAML 2.0 assertion and the resource description of the IdP and the assumed role to sts:AssumeRoleWithSAML for temporary credential.
6. STS verifies the SAML 2.0 assertion.
7. The verification result is returned.
8. The API constructs a temporary credential based on the result, and sends it to the client.

Cross-Account Access Role

Last updated：2023-10-20 15:30:03

Overview

By generating a temporary credential for cross-account access, you can enable one of your Tencent Cloud accounts to play the role of another Tencent Cloud account, and manage Tencent Cloud resources within the scope of authority.

Prerequisite

You already had multiple root accounts. If you want to create one, please refer to register. Assume that you have two Tencent Cloud accounts, Account A and Account B. You want to manage the resources under Account B by using Account B.

Directions

1. Log in with Account A and create the custom role as instructed in Creating Role.
2. Use the access key for account B to generate a temporary security key by invoking sts: AssumeRole through the Cloud API tool.
3. Use the key generated in Step 2 as account A to invoke the API through the Cloud API tool. In this case, you can manage Tencent Cloud resources.