

# Cloud Security Center

## Operation Guide

### Product Documentation



## Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

## Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

## Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

# Contents

## Operation Guide

- Access Permissions Management

- Multi-Cloud Multi-Account Management

  - Multi-Cloud Connection

  - Multi-Account Management

- Breach and Attack Simulation

- Log Shipping

- Managing Assets

- Health Checks

  - Product Features

  - Operation Guide

  - Adding IPs to an Allowlist

  - FAQs

- User Behavior Analytics (UEBA)

# Operation Guide

## Access Permissions Management

Last updated : 2024-08-02 10:14:18

This document will guide you on how to view and use permissions for specific resources in Cloud Security Center (CSC), and how to use policies for specific sections of the CSC console.

### Overview

You can grant a user permission to view and use specific resources in the CSC console by using a Cloud Access Management (CAM) policy.

#### SOC Full Access Policy

If you want users to have **Management Permissions** to the CSC, you can grant them the policy named QcloudSSAFullAccess. This policy allows users to have management permissions for all resources in CSC. To authorize users with the preset policy QcloudSSAFullAccess, see [directions](#).

#### SOC Read-Only Policy

If you want users to have **query** permissions to the CSC, but don't have the creation, deletion and processing permissions, you can grant them the policy named QcloudSSAReadOnlyAccess. To authorize users with the preset policy QcloudSSAReadOnlyAccess, see [directions](#).

#### Policy For SOC-related Resources

If you want users to have **usage** permissions to the CSC cloud assets, compliance management, cloud security configuration, response center, and UBA, you can grant them the policy named QcloudAuditFullAccess. This policy allows users to have operational permissions for all resources in CloudAudit, thereby achieving their goals. To authorize users with the preset policy QcloudSSAReadOnlyAccess, see [directions](#).

### Directions

1. Log in to the [CAM console](#). In the left sidebar, click **Policies** to enter the policy page.
2. On the search box on the policy page, enter the policy name (search as needed), such as by entering QcloudCCNFullAccess to search.
3. In the action bar on the right side of the QcloudSSAFullAccess policy, click **Associate User/User Group/Role**.

Create Custom Policy Delete All Policies Preset Policy Custom Policies Qcl

<input type="checkbox"/>	Policy Name	Service Type	Description	Last Modified
<input type="checkbox"/>	QcloudCCNFullAccess	vpc	QcloudCCNFullAccess	2019-10-09 19

0 selected, 1 in total 10

4. On the associating user/user group/role page, select the sub-user that needs permission configuration, and click OK.

### Associate User/User Group/Role

Select a User (1 Total) (1) selected

Support multi-keyword search by user name/ID/SecretId/mob

<input checked="" type="checkbox"/>	Users	Switch to User Groups ...
<input checked="" type="checkbox"/>	[blurred]	Users

Name	Type
[blurred]	Users

Support for holding shift key down for multiple selection

OK Cancel

# Multi-Cloud Multi-Account Management

## Multi-Cloud Connection

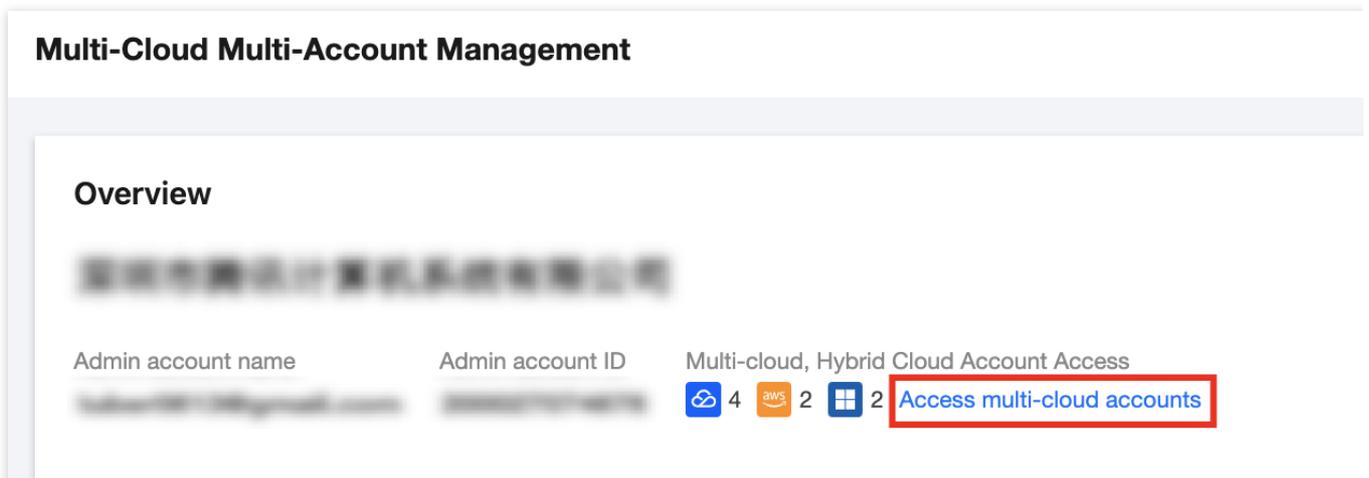
Last updated : 2024-08-02 10:14:18

### Feature Overview

When user operations are deployed simultaneously on Tencent Cloud and third-party cloud vendors, Tencent Cloud CSC supports centralized management of multi-cloud resources (currently supporting Amazon Web Services (AWS) and Microsoft Azure). By connecting to multi-cloud accounts, transparency and visualization of multi-cloud security management are achieved and the real-time monitoring of the security protection status, risks, and other information on third-party clouds are enabled.

### Directions

1. Log in to the [CSC console](#). In the left sidebar, click **Multi-Cloud Multi-Account Management**.
2. On the multi-cloud multi-account management page, click **Access multi-cloud accounts**.



3. In the configure multi-cloud, outside cloud, and hybrid cloud accounts page, select the account type as [Azure account](#) or [AWS account](#), and configure the relevant parameters, then click **OK**.

### Configure Multi-cloud, Outside Cloud, and Hybrid Cloud Accounts

Choose the account type

[Azure Account](#)   [AWS Account](#)   [Tencent Cloud Sub-account](#)

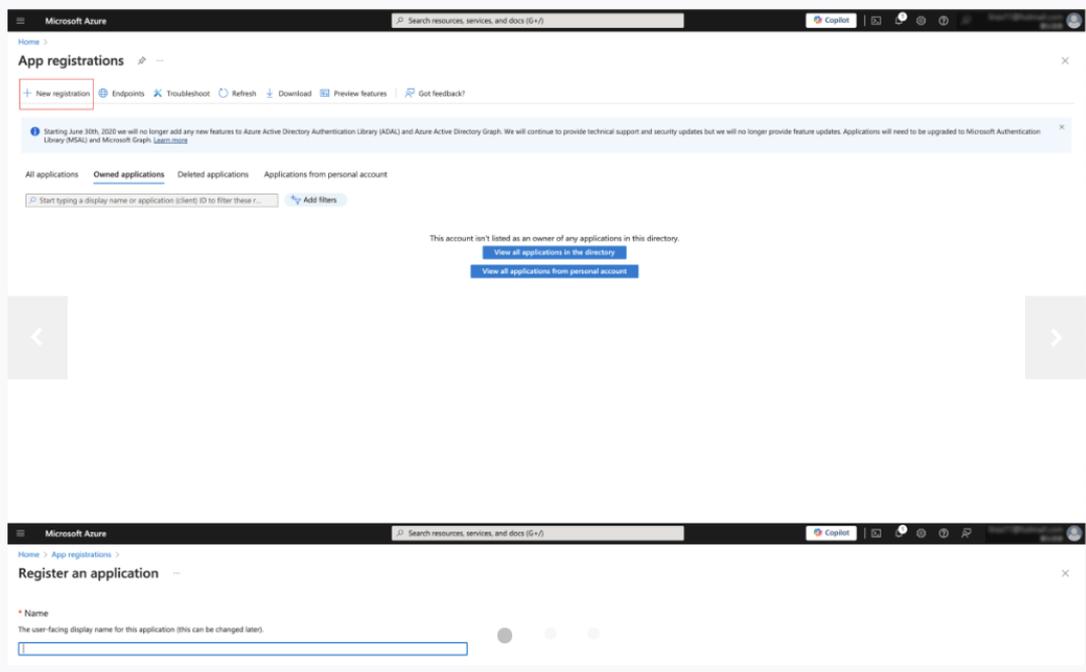
[Tencent Cloud account, go to Group Account Configuration](#)

Methods to create sub-accounts

**Configure Manually** Complete in 5 minutes, need to create "Application Registration" and "Client Password", b "subscription", and assign "Reader" permissions.

[Collapse Configuration Guide](#)   [View in document](#)

◀ Step1/3 ▶ Please visit [www.azure.com/xxx](http://www.azure.com/xxx) to create an application registration and choose the supported account type as needed.



The screenshot shows two parts of the Azure portal. The top part is the 'App registrations' page with a 'New registration' button highlighted. The bottom part is the 'Register an application' form with a text input field for the application name.

Subscription ID

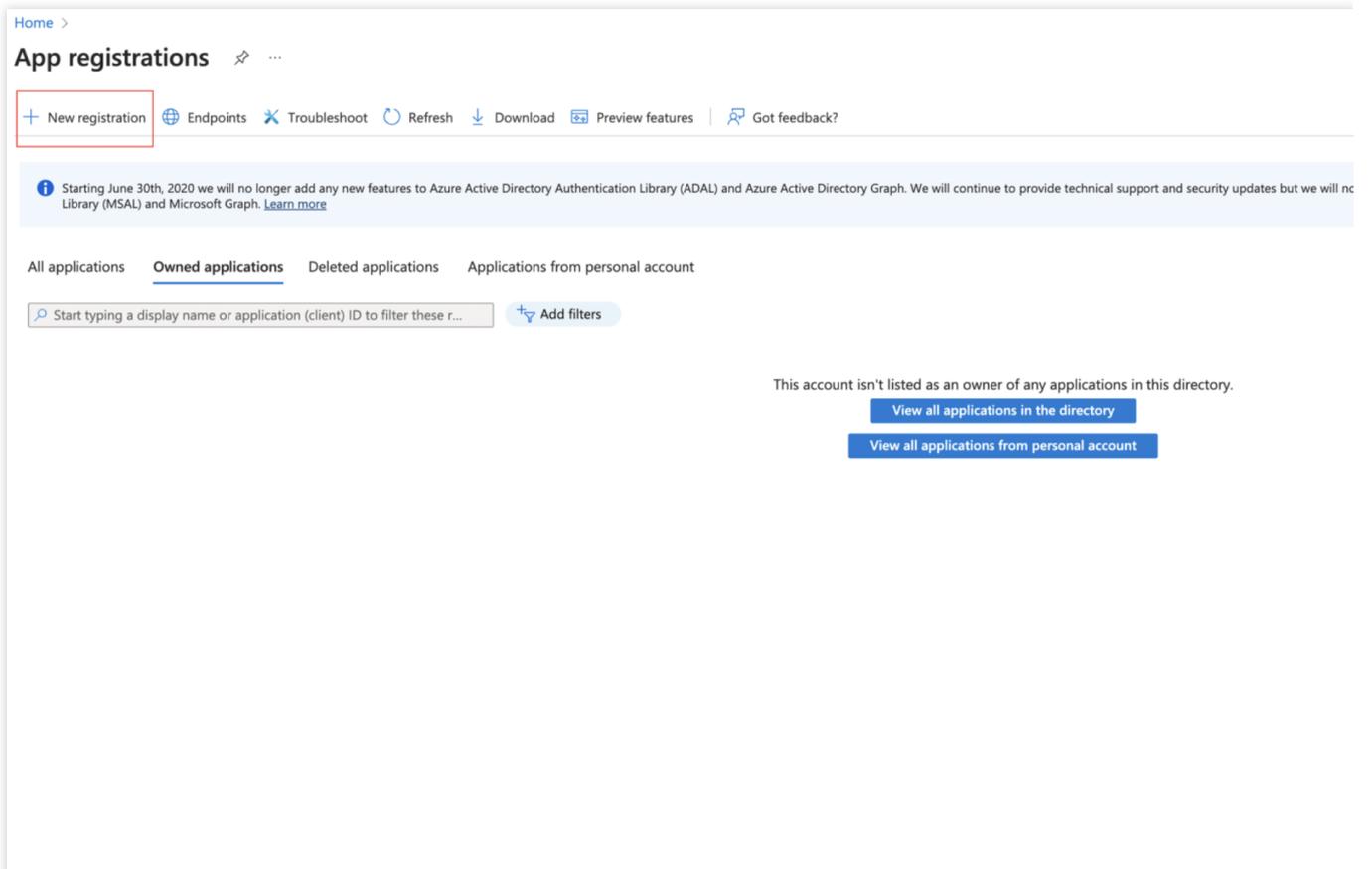
AppId

Client ID

## Azure Account

### Step 1: Application Registration

1. Log in to Azure, then go to the application registration page, and click **New registration** (if you already have an application registered, skip to Step 2.).



2. On the register an application page, fill in the application's Name and select the Supported Account Types according to your needs, and click **Register**.

Microsoft Azure

Search resources, services, and docs (G+)

Home > App registrations >

## Register an application

\* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (默认目录 only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

## Step 2: Obtaining a Subscription ID

1. On the subscription list page, select the subscription to be connected (an application registration can be bound to multiple subscriptions), and click **Subscription name**.

Home > Subscriptions >

## Subscriptions

默认目录

+ Add Manage Policies View Requests View eligible subscriptions

Global administrators can manage all subscriptions in this list by updating their policy setting [here](#).

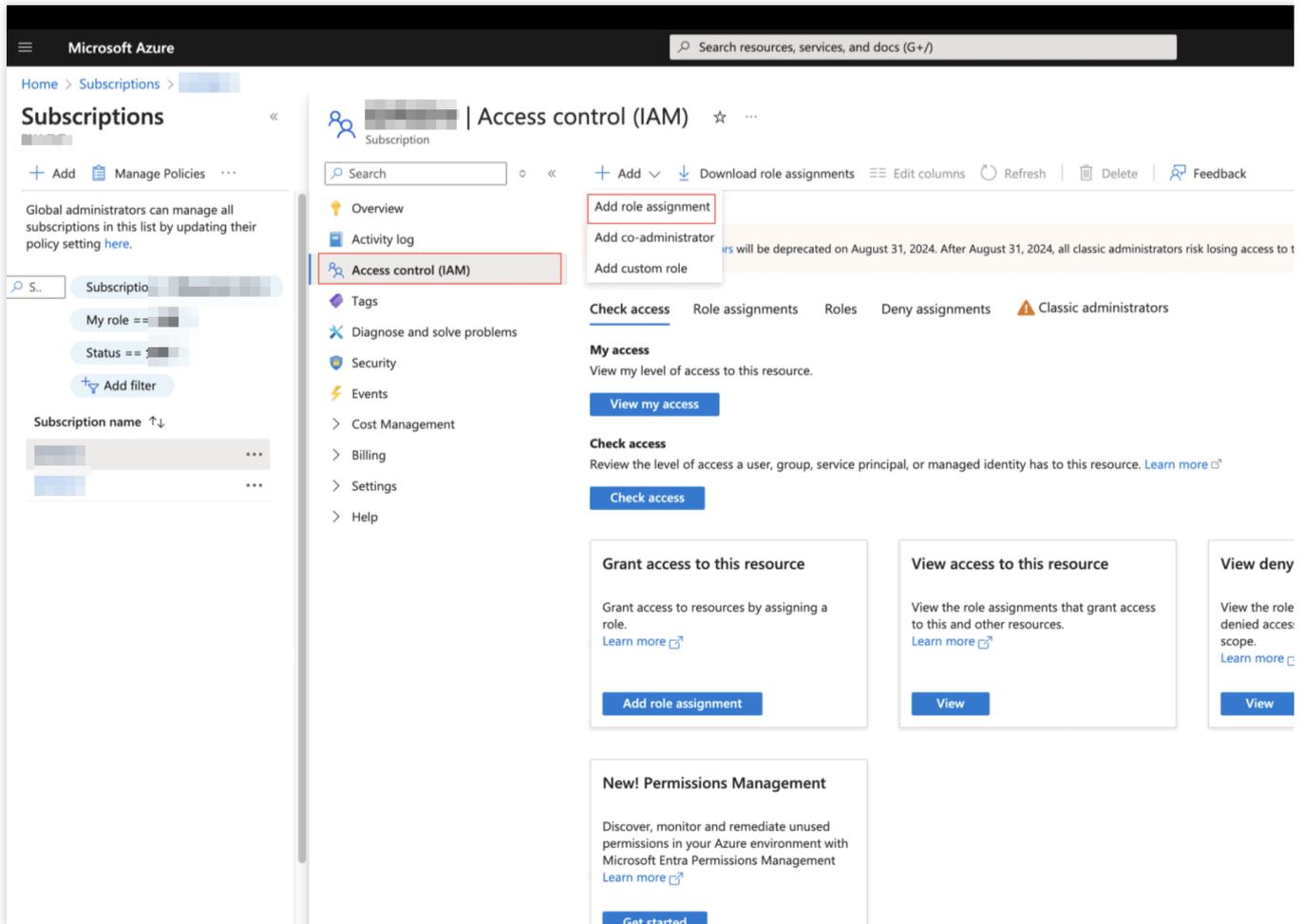
Search for any fi... Subscriptions: Filtered (2 of 2) My role == Status == Add filter

Subscription name ↑↓	Subscription ID ↑↓	My role ↑↓	Current cost	Secure Score ↑↓	Parent subscription
		Account admin	\$355.11	-	
		Account admin	0.00	-	

2. On the subscription details page, click **Overview** to obtain the **Subscription ID**.

The screenshot displays the Microsoft Azure Subscriptions management interface. On the left, the 'Subscriptions' page title is visible, along with navigation options like 'Add' and 'Manage Policies'. A search bar is present above the 'Overview' tab, which is highlighted with a red box. The 'Essentials' section contains key subscription details, with the 'Subscription ID' field also highlighted in red. Below the essentials, three data visualization cards are shown: 'Latest billed amount' displays a value of \$927.48; 'Invoices over time' features a bar chart with a total amount of \$927.48; and 'Spending rate and forecast' includes a line chart showing a current cost of \$355.11 and a forecast of \$1.30 K.

3. Select **Access Control**, click **Add**, and select **Add role assignment**.



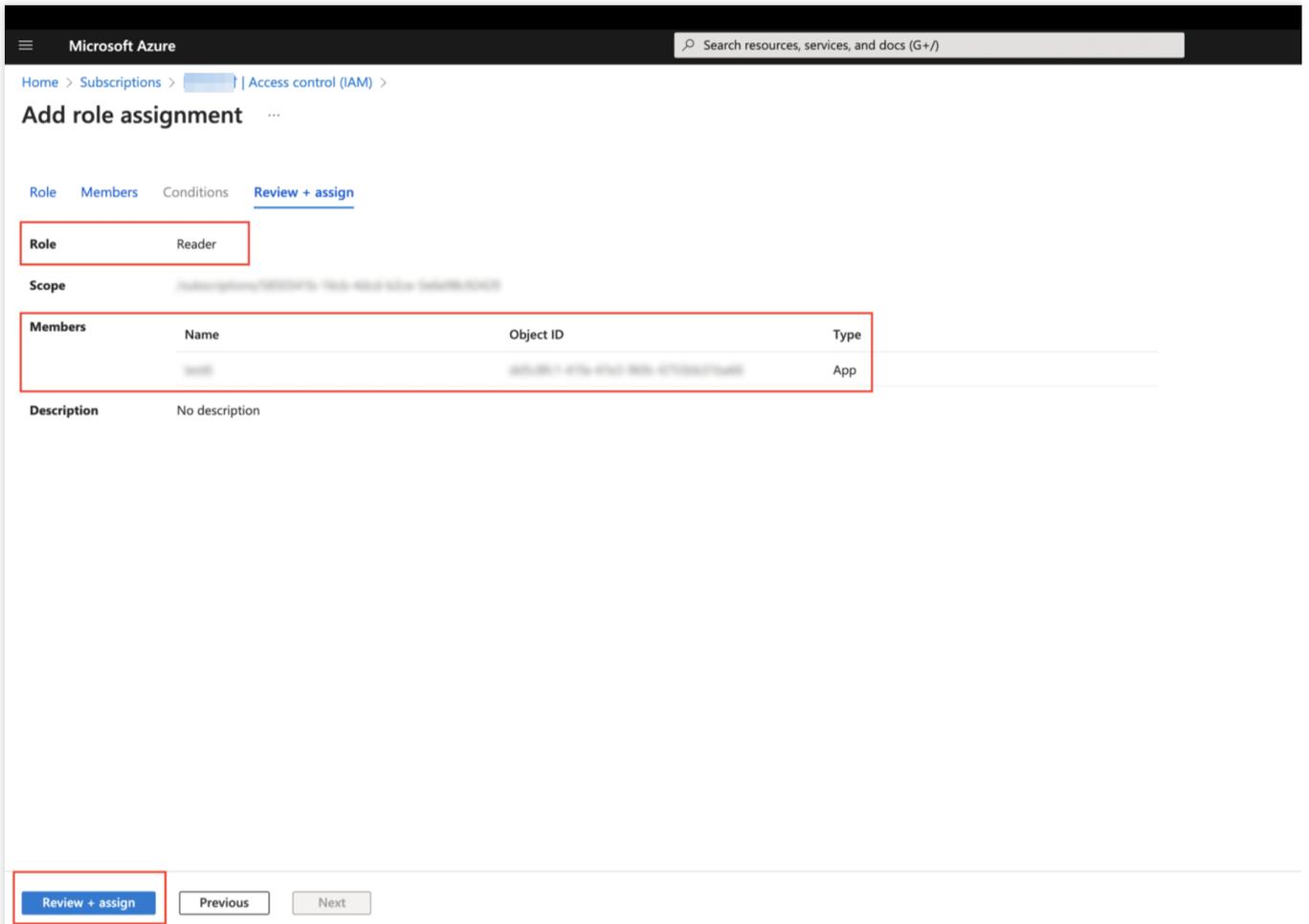
4. Select the role to be **Assigned**. It is recommended to select Reader and Azure Kubernetes Service Cluster User Roles in sequence. Click **Next**.

The screenshot shows the 'Add role assignment' page in the Microsoft Azure portal. The page is titled 'Add role assignment' and has tabs for 'Role', 'Members', 'Conditions', and 'Review + assign'. Below the tabs, there is a search box and filters for 'Type' and 'Category', both set to 'All'. A table lists various roles with columns for 'Name', 'Description', and a status indicator. The 'Reader' role is highlighted with a red box. Below the table, there are three buttons: 'Review + assign', 'Previous', and 'Next', with the 'Next' button also highlighted with a red box.

Name ↑↓	Description ↑↓	
Reader	View all resources, but does not allow you to make any changes.	Bi
ACR Registry Catalog Lister	Allows for listing all repositories in an Azure Container Registry.	Bi
ACR Repository Contributor	Allows for read, write, and delete access to Azure Container Registry repositories, but excluding catalog listing.	Bi
ACR Repository Reader	Allows for read access to Azure Container Registry repositories, but excluding catalog listing.	Bi
ACR Repository Writer	Allows for read and write access to Azure Container Registry repositories, but excluding catalog listing.	Bi
AcrDelete	acr delete	Bi
AcrImageSigner	acr image signer	Bi
AcrPull	acr pull	Bi
AcrPush	acr push	Bi
AcrQuarantineReader	acr quarantine data reader	Bi
AcrQuarantineWriter	acr quarantine data writer	Bi
Advisor Recommendations Contributor (Assessments and Re...	View assessment recommendations, accepted review recommendations, and manage the recommendations lifecycle (mark recommendations as completed,...	Bi
Advisor Reviews Contributor	View reviews for a workload and triage recommendations linked to them.	Bi
Advisor Reviews Reader	View reviews for a workload and recommendations linked to them.	Bi
AgFood Platform Dataset Admin	Provides access to Dataset APIs	Bi

5. Add the user to be assigned, click **Select Members**, enter the name of the Application Registration to be added in the search box, select the **Application Registration**, and click **Next**.

6. Confirm the roles and members, and click **Review + assign**.



### Step 3: Getting a Tenant ID, a Client ID, and a Client Key

1. Go to the page of the newly bound application registration, click **Overview**, and get ① Application (Client) ID and ② Directory (Tenant) ID.

Microsoft Azure

Search resources, services, and docs (G+)

Home > App registrations > test6

Search

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Support + Troubleshooting

Essentials

Display name : test6

Application (client) ID : 1

Object ID : 2

Directory (tenant) ID : 2

Supported account types : My organization only

Client credentials : Add a client secret

Redirect URIs : Add a redirect URI

Application ID URI : Add an application ID URI

Managed application in localized display name : test6

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support for these libraries, but you will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started Documentation

### Build your application with the Microsoft identity

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create applications that use the Microsoft identity platform to access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

**Call APIs**

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

[View API permissions](#)

**Sign in users in 5 minutes**

Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app.

[View all quickstart guides](#)

**Configure application policies**

Assign policies to your application. Enter your application ID and select the policies you want to assign.

[Configure application policies](#)

2. Click **Certificates & secrets** > **New client secret**, fill in the **Description**, select expires as **730 days (24 months)**, and click **Add**.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > App registrations > test6

test6 | Certificates & secrets

Search

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

**Certificates & secrets** ①

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)

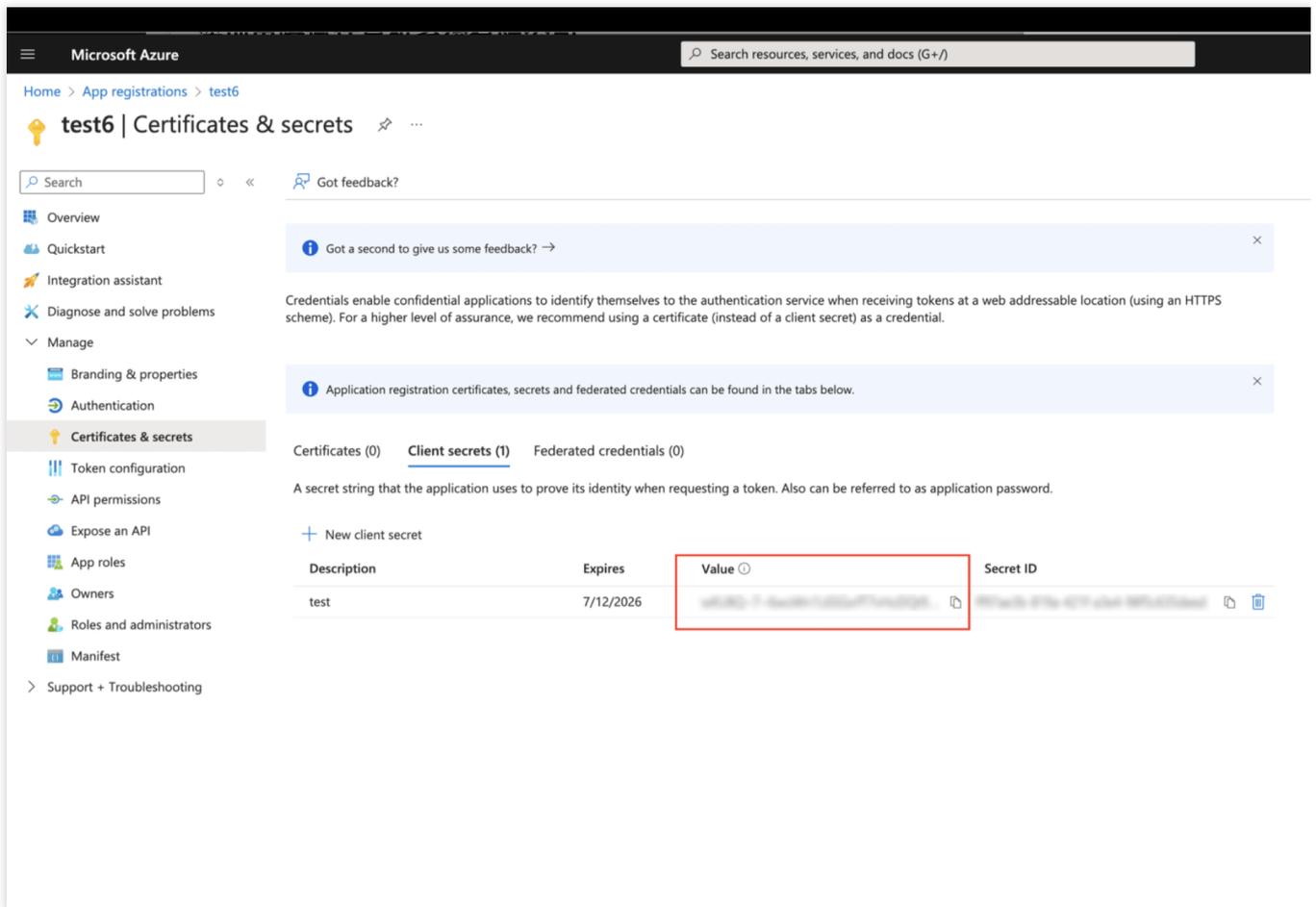
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret ②

Description	Expires	Value	Secret ID
-------------	---------	-------	-----------

No client secrets have been created for this application.

3. On the certificates and keys page, get the **Client Secret**.



Microsoft Azure

Search resources, services, and docs (G+)

Home > App registrations > test6

test6 | Certificates & secrets

Search

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

**Certificates & secrets**

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
test	7/12/2026		 

## AWS Account

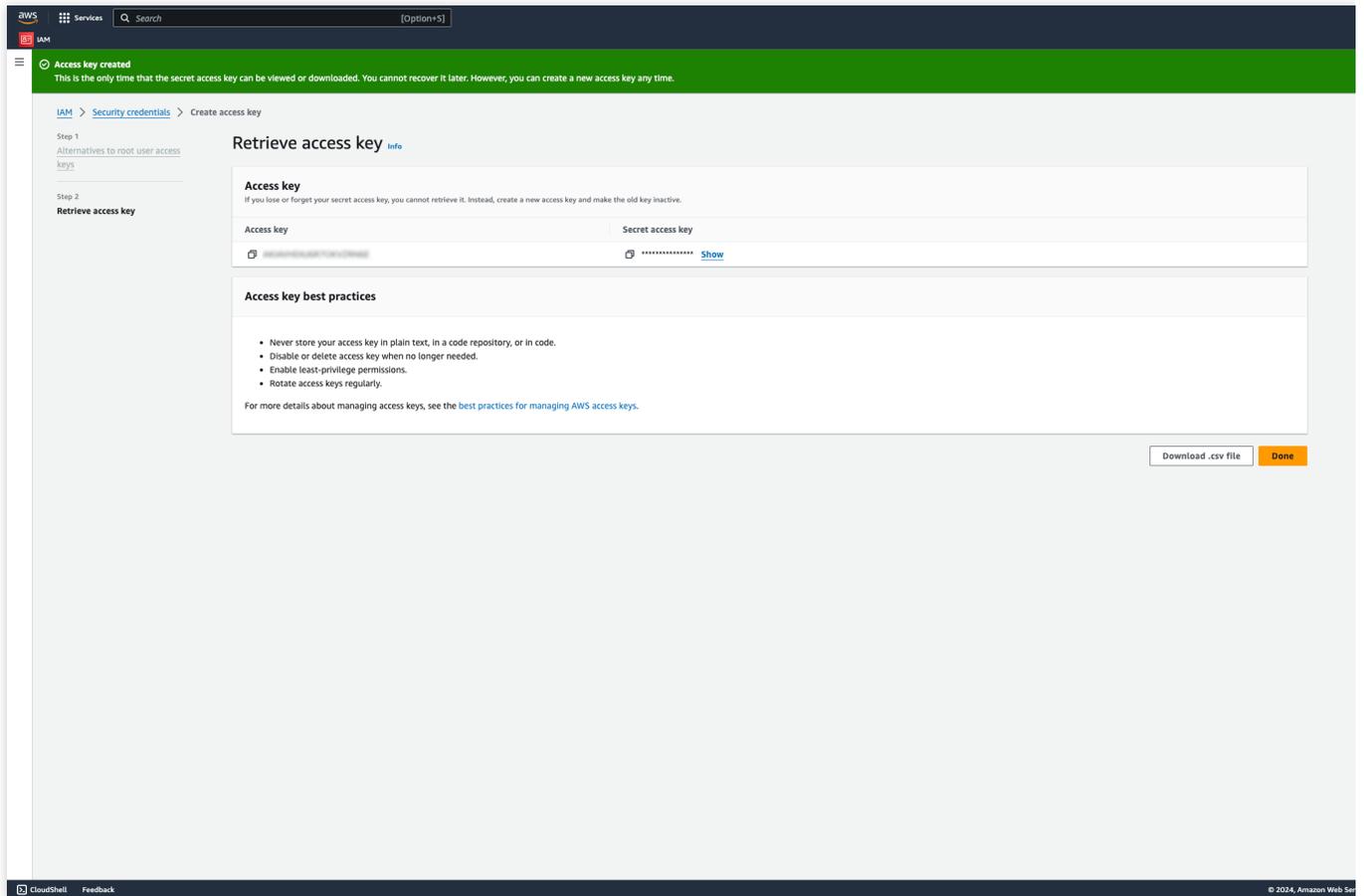
### Quick Configuration

The completion time is approximately 1 minute, but due to the need for higher permissions, the root account's AK should be configured. After that, CSC will automatically create a sub-account AK to connect to assets and grant read-only permissions to all assets.

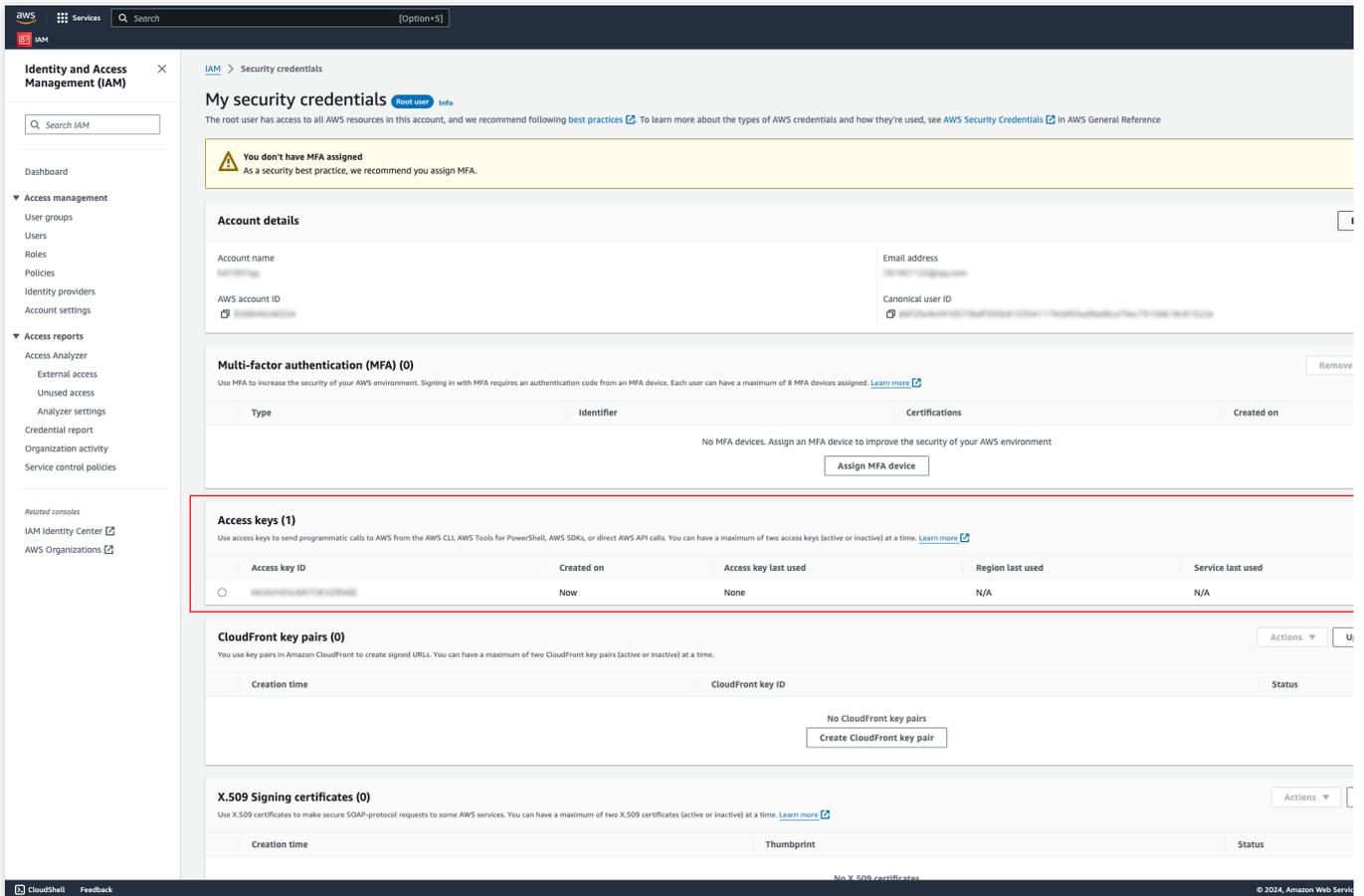
1. Log in to AWS and then go to [my security credentials](#) page. Click **Create access key** to generate an Access Key and Secret Access Key that can be used to monitor or manage AWS resources.

The screenshot shows the AWS IAM console interface. The left sidebar contains navigation options for Identity and Access Management (IAM), including Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), Access reports (Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies), and Related consoles (IAM Identity Center, AWS Organizations). The main content area is titled 'My security credentials' for the 'Root user'. It includes a warning that MFA is not assigned. Below this are sections for Account details, Multi-factor authentication (MFA) (0), Access keys (0), CloudFront key pairs (0), and X.509 Signing certificates (0). The 'Access keys (0)' section is highlighted with a red border and contains a 'Create access key' button. The 'CloudFront key pairs (0)' section contains a 'Create CloudFront key pair' button. The 'X.509 Signing certificates (0)' section contains a 'Create X.509 signing certificate' button.

2. On the retrieve access key page, view or download the Access Key and Secret Access Key.



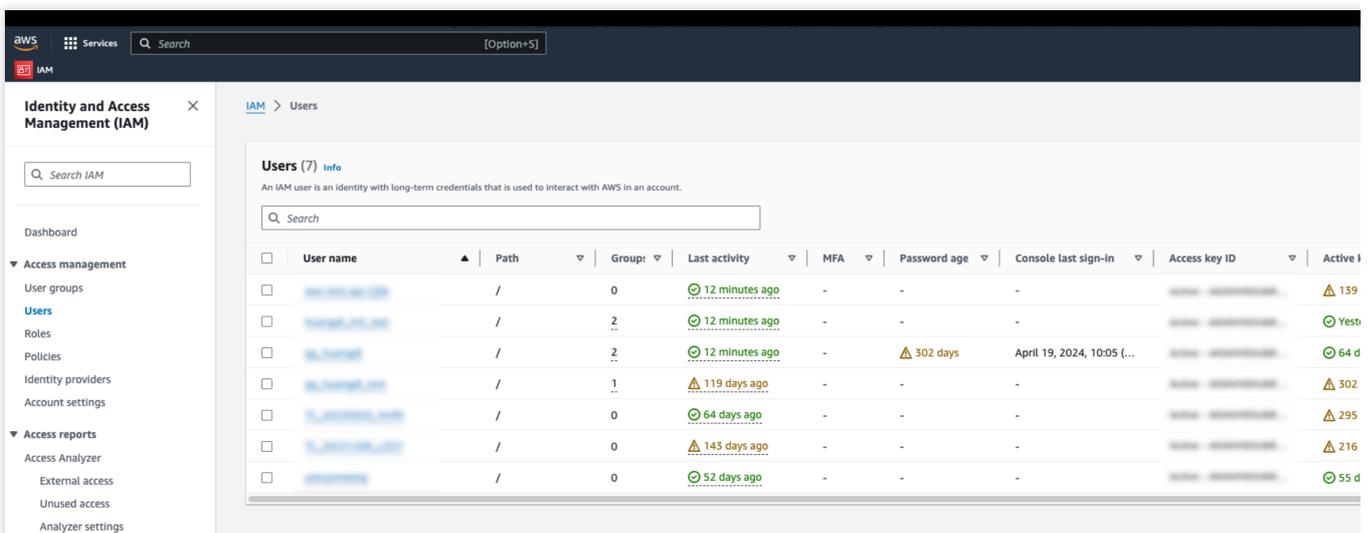
3. Ensure that the Access Key status is active, then fill in the Access Key and Secret Access Key in Root Account SecretID and Root Account SecretKey.



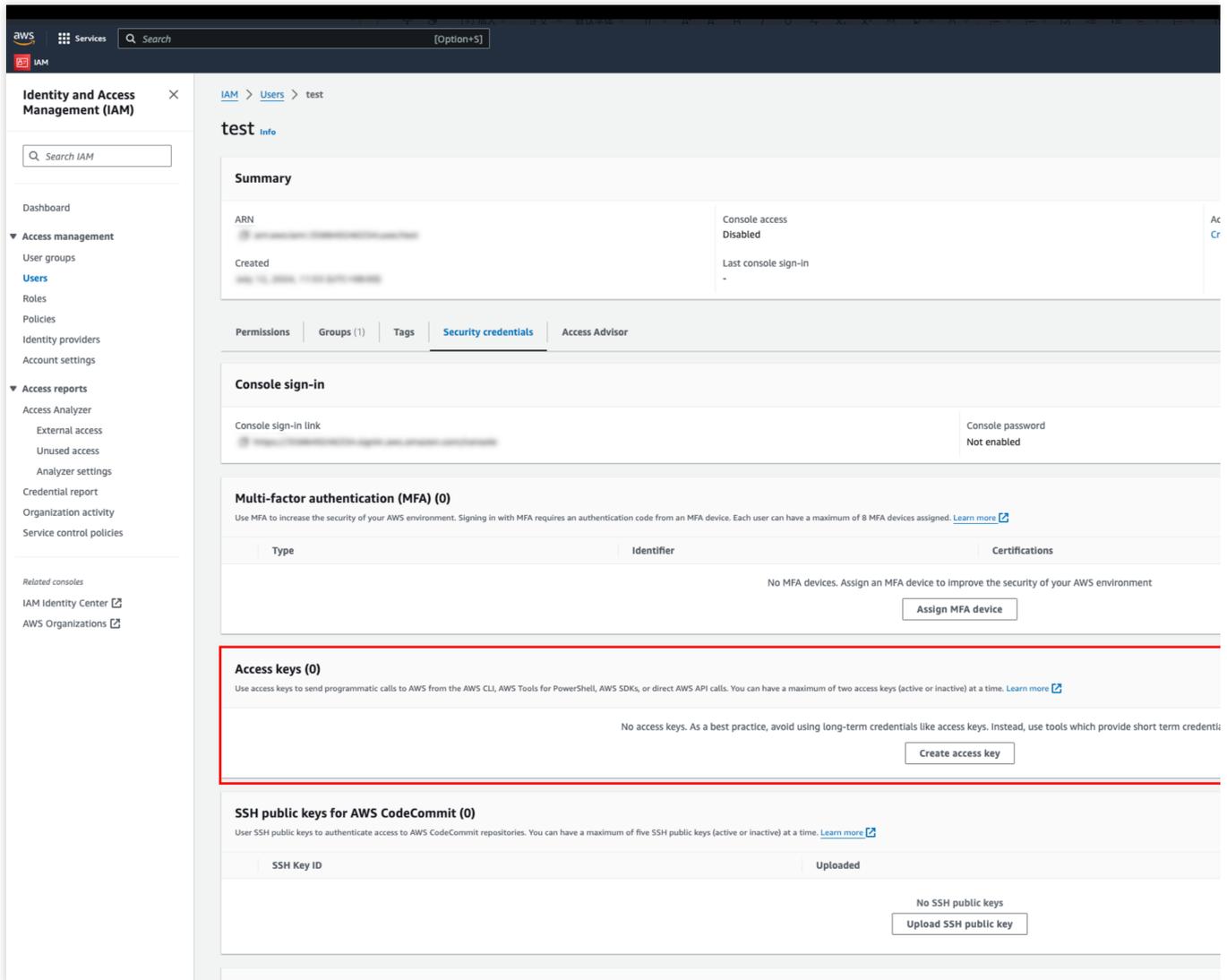
## Configuring Manually

The completion time is approximately 5 minutes, but permission configuration is relatively complex. You need to configure the Access Key for the created sub-account to more flexibly control the range of permissions.

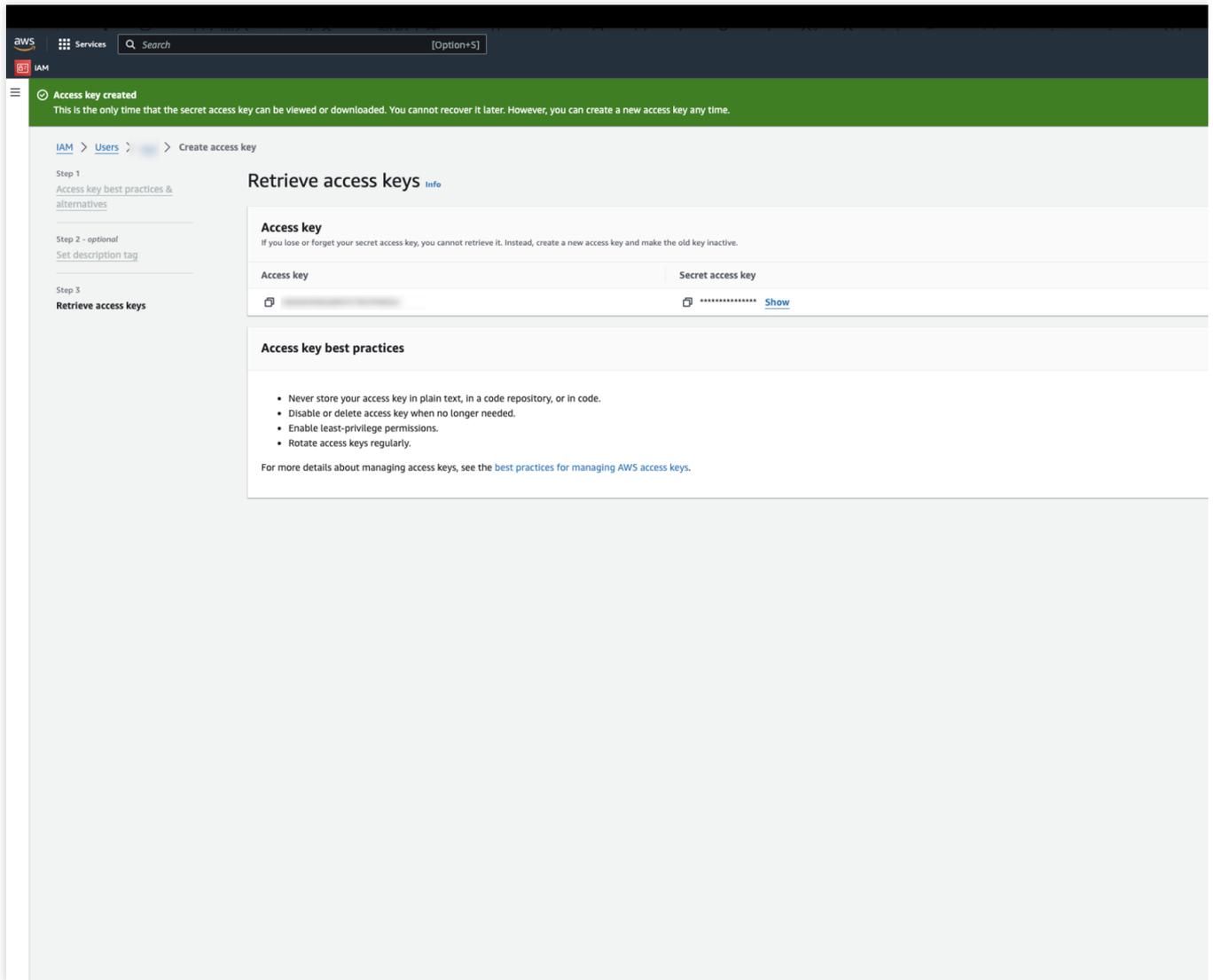
1. Log in to AWS and then go to [IAM > users](#) page, and click **Create User** to create a sub-account for interacting with AWS in your account.



2. Go to the details of the sub-user, click **Create access key** to generate an Access Key and Secret Access Key that can be used to monitor or manage AWS resources.



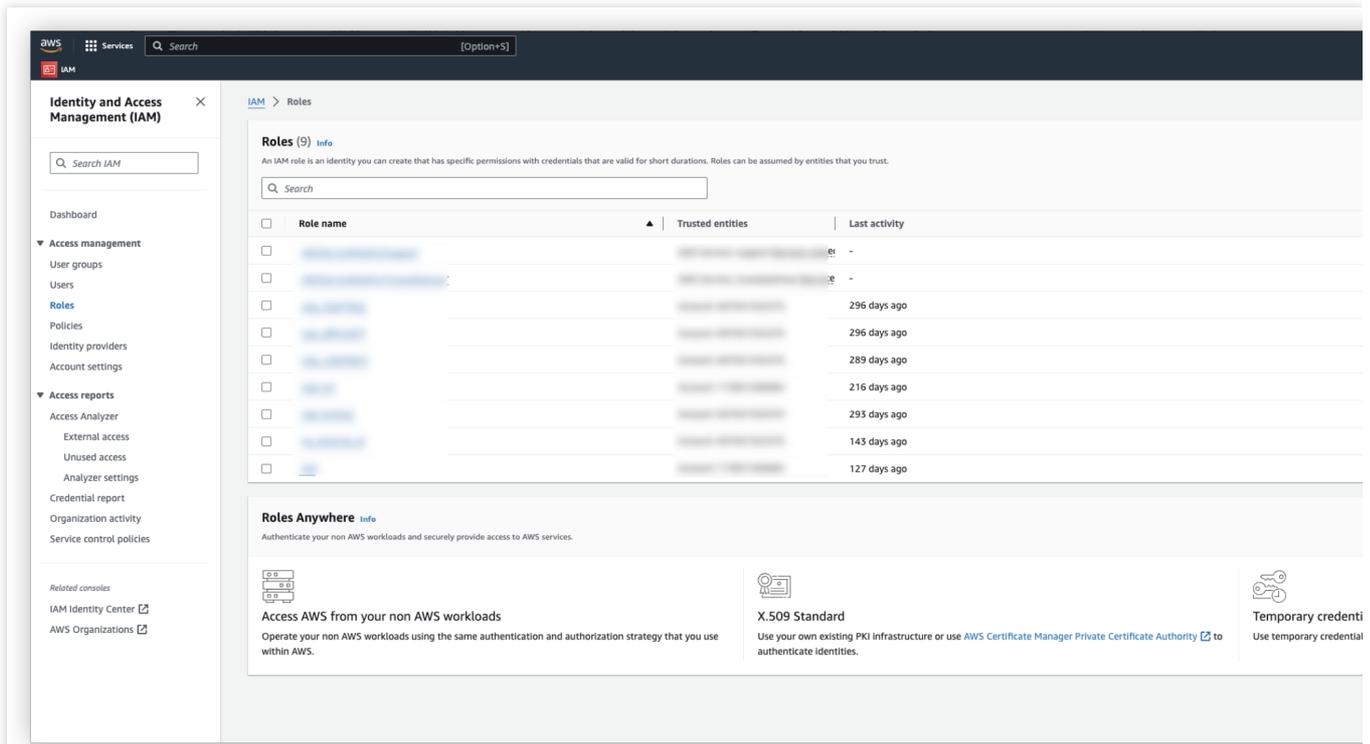
3. View or download the Access Key and Secret Access Key. Ensure that the Access Key status is active, then fill in the Access Key and Secret Access Key in Sub-account SecretID and Sub-account SecretKey.



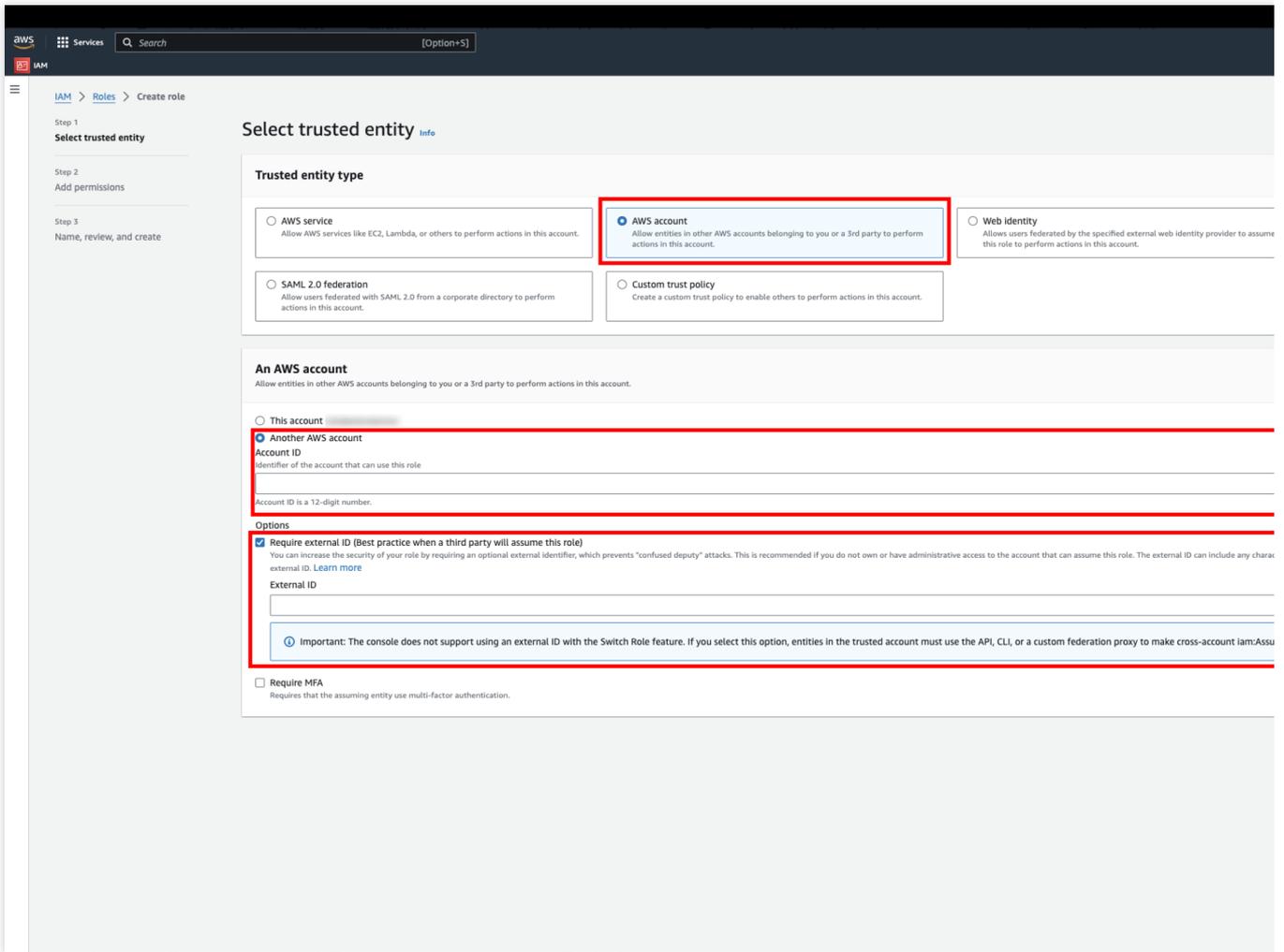
## Advanced Configuration

It is relatively complex, but the range and duration of permissions are controllable. Create a role in AWS using the RoleArn provided by us, and authorize the specified ARN with a UUID to call the sts:AssumeRole API. This API is used to create a temporary access role for the account.

1. Log in to AWS and then go to [IAM > roles](#) page, and click **Create role**. This identity has specific permissions, and the credentials are valid for a short period. The role can be assumed by an entity you trust.



2. After you select AWS Account as the trusted entity type, create the role based on the required permissions.



3. Go to the role details, copy the ARN and paste it into RoleArn.

The screenshot displays the AWS IAM console interface for a role named 'csip\_5QdTXIEg'. The left sidebar contains navigation options under 'Identity and Access Management (IAM)', including 'Access management', 'Access reports', and 'Related consoles'. The main content area is divided into several sections:

- Summary:** Displays role details such as 'Creation date', 'Last activity', and 'Maximum session duration' (1 hour). The 'ARN' field is highlighted with a red rectangular box.
- Permissions:** A tabbed interface showing 'Permissions policies (1)'. A table lists the attached policy: 'ReadOnlyAccess' (AWS managed - job function) with 11 attached entities.
- Permissions boundary:** A section indicating that no boundary is currently set.
- Generate policy based on CloudTrail events:** A section with a 'Generate policy' button and a note stating 'No requests to generate a policy in the past 7 days.'

# Multi-Account Management

Last updated : 2024-08-12 17:26:36

## Overview

The multi-account management feature allows users to have multiple Tencent Cloud root accounts with independent billing and switch the log-in accounts and centrally manage all the accounts. It enables an organization admin to effectively grasp the security information of the organization and learn about the security protection status and risks of the cloud business of each member account in real time. This achieves transparent and visualized security management of the organization.

### Overview

#### Switching Log-in Accounts

You can switch to a member account with one click for secure, efficient and password-free log-in.

#### Centralized Management of Accounts

You can centrally manage all accounts of the organization without deployment. The security protection status of each member account is displayed, and you can set the security management permissions of accounts.

You can perform closed-loop management of handling cloud business risks for multi-accounts of the organization. You can scan the cloud assets of any member account with one click to troubleshoot potential risks.

## 1. Managing Organization Accounts

To use the multi-account management feature provided by CSC, you need to create an organization in Tencent Cloud Organization first. Depending on the status of the current log-in account, go to the step that matches the account status to get started.

### Note

Accounts that have not completed enterprise identity verification, enterprise accounts that have joined other organizations, and existing accounts created for the organization cannot create an organization. For more information, see [Group Organization Settings](#).

### Step 1: For an Account That Has Not Completed Enterprise Identity Verification

On the [Multi-Cloud and Multi-Account Management Page](#), click **verify identity** to go to the [Account Center Console](#), and follow the steps to complete enterprise identity verification. For more information, see [Change Personal Authentication Information - Change to Corporate Real-name Authentication](#).



## Welcome to multi-account management

Create an organizational structure for the organization admin to grasp the security info of the organization transparent and visual security management and to learn the security protection status and risks of business of each member account in real time.

**!** Multi-account management is the exclusive capability of the Ultimate edition of CSC. It can only be used after you activate the Ultimate edition, verify enterprise identity, and create an organization

### 1 Verify enterprise identity

• Not verified

To create or join an organization,

**verify identity** first

### 2 Create organization

• Performance

After creation, you cannot join or delete this organization if it is deleted

Activate now

Learn more

### Step 2: For an Enterprise Account That Has Not Created an Organization Yet

On the [TCO Page](#), click **Create** to create an organization. Under this organization, create member accounts or invite member accounts to join it.

⚠ To create or join an organization, complete enterprise identity verification first. [Verify now](#)

ℹ After you create an organization, you cannot join another organization until the one you create is deleted.

## Organization types: account/resource/finance management

### ✔ Multi-account management

The admin account can create the organization structure and manage member accounts by category

### ✔ Resource sharing management

The admin account can create shared units where member accounts can share resources

### ✔ Finance management

The admin account can check the organization finance overview, view the bills and consumption details of members, allocate

For more information on Tencent Cloud Organization, click to [learn more](#) 

Create

## Step 3: Using Multi-Account Management

An enterprise account with the multi-account management feature enabled can start using it.

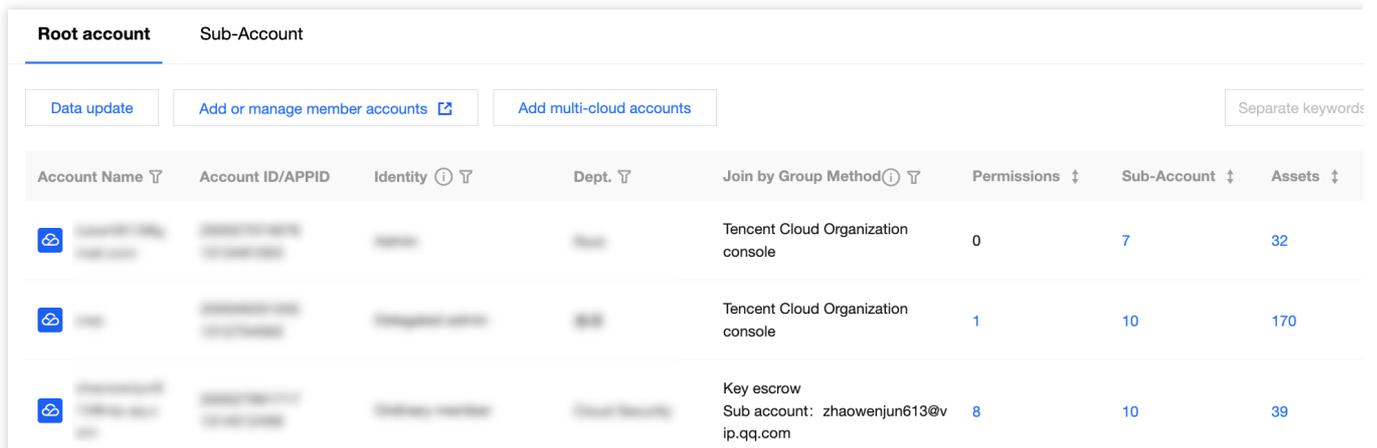
## 2. How to Flexibly Switch Log-in Accounts

### Authorizing Access to Member Accounts

Log in to the [TCO Console](#) to authorize the administrator sub-accounts to log in and manage member accounts. For more information, see [Granting a member the account access](#).

### Switching to a Member Account for Log-in

1. On the [Multi-Cloud and Multi-Account Management Page](#), select the corresponding member account, and click **Log in**.



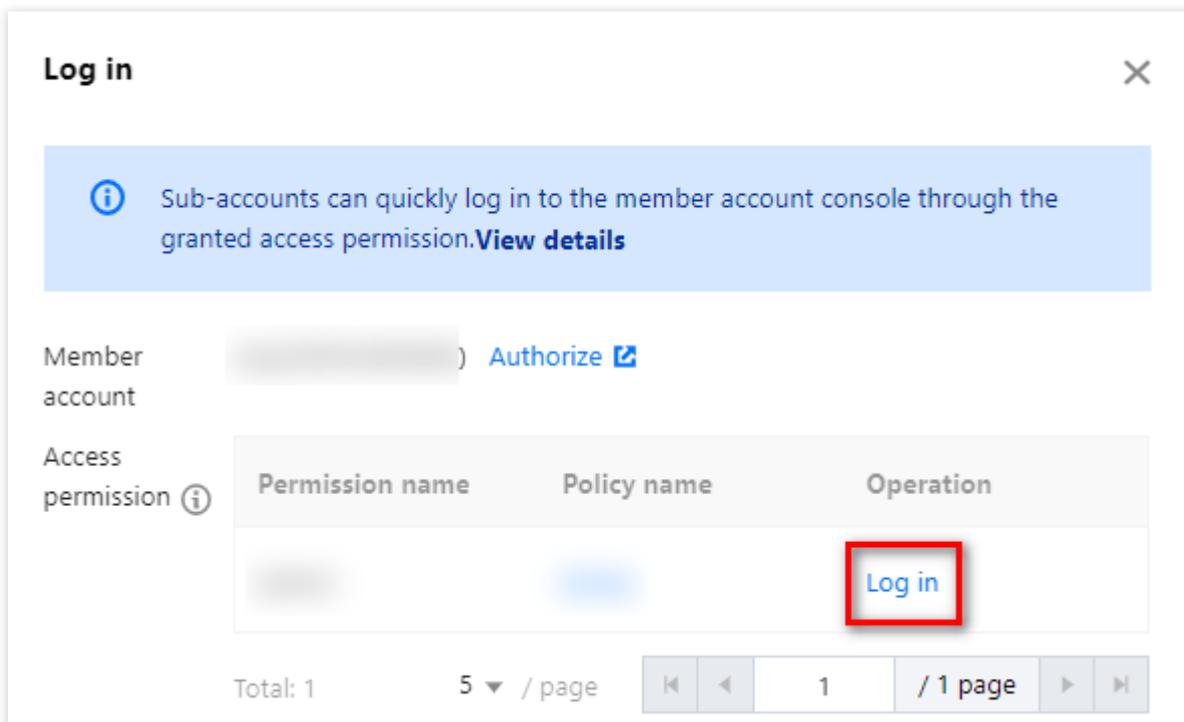
The screenshot shows the 'Root account' management interface. At the top, there are tabs for 'Root account' and 'Sub-Account'. Below the tabs are three buttons: 'Data update', 'Add or manage member accounts', and 'Add multi-cloud accounts'. A search box labeled 'Separate keywords' is on the right. The main content is a table with the following columns: Account Name, Account ID/APPID, Identity, Dept., Join by Group Method, Permissions, Sub-Account, and Assets. Three rows are visible, each representing a different account type.

Account Name	Account ID/APPID	Identity	Dept.	Join by Group Method	Permissions	Sub-Account	Assets
[Blurred]	[Blurred]	[Blurred]	[Blurred]	Tencent Cloud Organization console	0	7	32
[Blurred]	[Blurred]	[Blurred]	[Blurred]	Tencent Cloud Organization console	1	10	170
[Blurred]	[Blurred]	[Blurred]	[Blurred]	Key escrow Sub account: zhaowenjun613@vip.qq.com	8	10	39

2. In the log-in account pop-up, select the required permission name and policy name, and click the corresponding **Login to Member Account** to switch the log-in account successfully.

### Note

An administrator root account or unauthorized administrator sub-account cannot switch to a member account for log-in, and a member account invited to join the organization is not supported for authorized log-in.



## 3. How to Manage Accounts Centrally and Efficiently

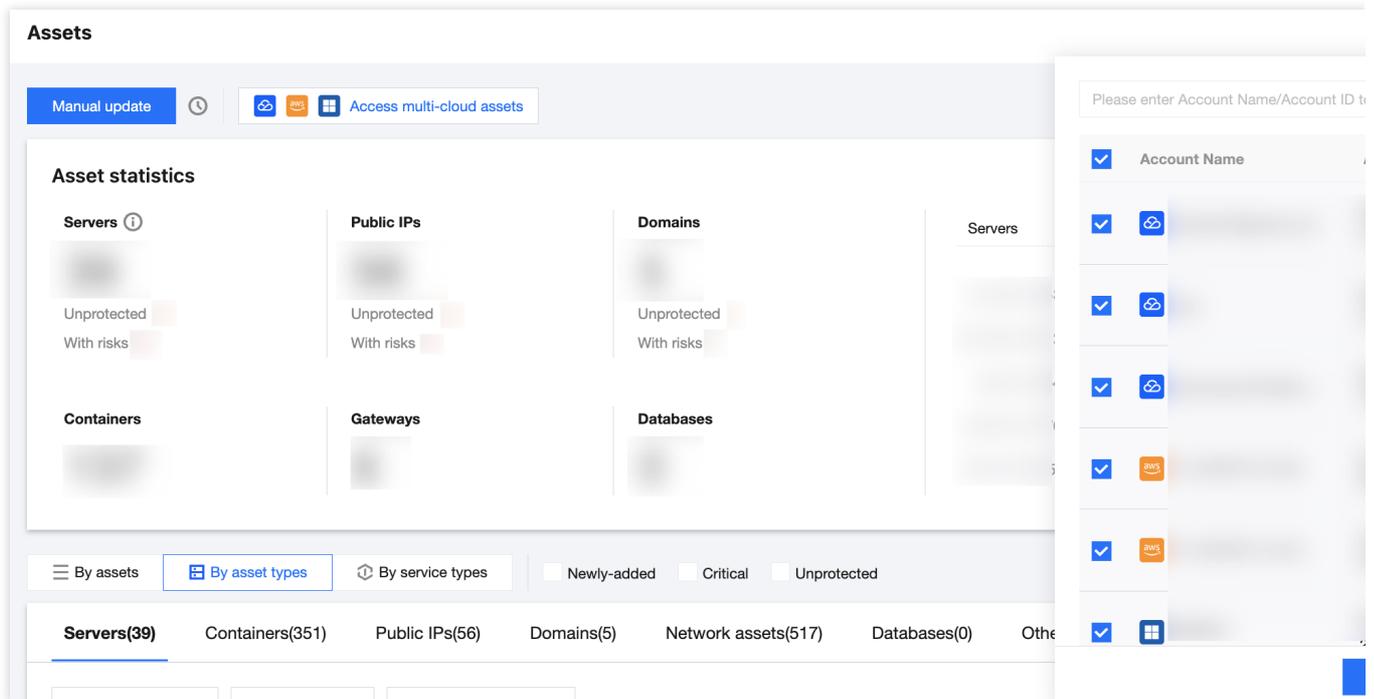
Using the administrator root account and sub-account to log in to the [CSC Console](#) and view the security information of the organization, realizing transparency and visualization of organization security management. You can learn about the security protection status and risks of the cloud business of each member account in real time.

The multi-account management mode has been incorporated into modules such as assets, risks, scan tasks, and report download. This allows you to perform cross-account operations to ensure the security of cloud business assets

for the organization.

## Account Switch

In the upper right corner of each module, click **Multi-account**. In the dropdown filter box, you can search by entering the **Account Name/Account ID/App ID**. After you selecting a member account and click **OK**, the data in the module will switch to all data of the account.



## System Settings - Multi-Account Management

On the [Multi-Cloud and Multi-Account Management Page](#), you can centrally manage all accounts of the organization without deployment. The security protection status of each member account is displayed. You can also switch to a member account with one click for secure, efficient and password-free log-in. The page varies depending on the log-in account you use:

Log-in with an administrator root account

### Multi-Cloud Multi-Account Management

#### Overview

Admin account name      Admin account ID      Multi-cloud, Hybrid Cloud Account Access  
[Icons: 4, 2, 2] [Access multi-cloud accounts](#)

#### Root account

Administrator/Delegated  
Administrator 2

**Root account**      Sub-Account

[Data update](#)      [Add or manage member accounts](#)      [Add multi-cloud accounts](#)

Account Name	Account ID/APPID	Identity	Dept.	Join by Group Method	Permissions	Sub-Account

Log-in with an administrator sub-account

### Multi-Cloud Multi-Account Management

#### Overview

Admin account name      Admin account ID      Multi-cloud, Hybrid Cloud Account Access  
[Icons: 4, 2, 2] [Access multi-cloud accounts](#)

#### Root account

Administrator/Delegated  
Administrator 2

**Root account**      Sub-Account

[Data update](#)      [Add or manage member accounts](#)      [Add multi-cloud accounts](#)

Account Name	Account ID/APPID	Identity	Dept.	Join by Group Method	Permissions	Sub-Account

Log-in with a member root account or sub-account

Multi-Cloud and Multi-Account Management

Overview

Admin account name      Admin account ID      Multi-Cloud and Hybrid Cloud Account Access  
 [blurred]      [blurred]      [cloud icon] [aws icon] [azure icon] Access Multi-Cloud Account

**Root account**      **En**  
 [blurred]  
 Administrator/Delegated  
 Administrator [blurred]

**Root account**      Sub-Account

Data update      Add or manage member accounts [link icon]      Add Multi-Cloud Account

Account Name	Account ID/App ID	Identity	Dept.	Group Join Method	Permissions	Sub-Account
[cloud icon] [blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]
[cloud icon] [blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]

Assets

On the [Asset Page](#), the administrator can manage cloud business assets across accounts, learn about the security protection status of each asset, and scan the cloud assets of any account to troubleshoot potential risks with one click.

Assets

Manual update [refresh icon]      [cloud icon] [aws icon] [azure icon] Access multi-cloud assets

Asset statistics

Servers	Public IPs	Domains	Servers	Containers	Public IPs	Domains
Unprotected [blurred] With risks [blurred]	Unprotected [blurred] With risks [blurred]	Unprotectec [blurred] With risks [blurred]	[blurred]	[blurred]	[blurred]	[blurred]
Containers [blurred]	Gateways [blurred]	Databases [blurred]	[blurred]	[blurred]	[blurred]	[blurred]

Vulnerabilities and Risks

The [Vulnerability and Risk Center Page](#) incorporates the capabilities of linking various products for users to perform one-stop management of the risks of cloud business assets, such as port, vulnerability, weak password, configuration, and content risks. The administrator can handle the potential risks of the cloud business assets across accounts.

**Vulnerability and Risk Center** 1 tasks are being

Full check | All assets | All reports

**Asset risks** ⓘ Apache Struts Code Injection Vulnerability (CVE-2020-17530) [Check now](#) [Details](#)

Category	07-13	07-14	07-15
Vulnerabilities	34	34	53
Port risks	2	2	13
Weak passwords	1	1	4
Content risks	0	0	0
Configuration risks	382	382	208
Exposed risk services	0	0	0

### Health Check

The [Health check tasks Page](#) displays the information of all scan tasks for all accounts under the organization and provides the execution status of each task in real time. The administrator can efficiently manage each asset scan task across accounts and can edit, delete, and stop the scan tasks of each account.

**Health check tasks**

Health check tasks		Number of health checks consumed / Total quota	
Health Check Tasks / Total Quota ⓘ		Purchased Upgrade Quota	<a href="#">View report</a>
Scheduled checks 0 In progress 0			

Start time	Task name
20:...	...
20:...	...
20:...	...

### Report Download

On the [Reports Page](#), linking the vulnerability scan service, the administrator can download reports corresponding to each scan task across accounts and receive reports anytime and anywhere by following the service account.

**Reports** 1 tasks are b...

**Report overview**

**Report Count** **Report Templates**

To be reviewed items Create now

**Download history**

Generation time	Task name	Report

**Reports** Report Templates

One-click download Separate keyword

<input type="checkbox"/>	Report name	Report Type	Included assets	Risks	Task ID/name	Generation time
<input type="checkbox"/>						
<input type="checkbox"/>						

## 4. FAQs

### What Are the Billing Standards After Using Multi-Account Management?

Please stay tuned with the product news for the future billing standards of the new version of CSC.

### Data Handling of Existing Users

CSC will notify users of the end of the activity one month before the end of the free trial. Data of unpaid users will be cleared, and data of paid users will be migrated to the new version of CSC.

### How Can I Implement Multi-Account Management? Do I Need to Adjust the Network Architecture?

Multi-account management is achieved by integrating system data of security products, and there is no need to adjust the network architecture.

### How to Contact You If I Have Any Questions?

Thank you for your trust and support. If you have any questions during the usage of our products, you can [submit a ticket](#) to contact us, and we will get back to you as soon as possible.

# Breach and Attack Simulation

Last updated : 2024-08-02 10:14:18

## Feature Overview

By imitating hackers' thinking and working methods, automated simulations of combat skills and tactics based on the MITRE ATT&CK framework allow users to view various cloud security threats from an attacker's perspective. This enables the identification of different potential attack paths and the most impactful security threats for users. It also helps in discovering any shortcomings in security protection products and whether the corresponding security policies are properly configured, allowing for the rational use of security resources to minimize cloud risks.

## Use Cases

### Efficient Penetration Testing

By automated execution of simulated attack tasks, numerous known attacks can be tested extensively, making operations easy and practical, thus reducing the workload for Ops personnel. The system provides penetration testing scripts based on the MITRE ATT&CK framework by default, including tactics such as information collection, vulnerability scanning, vulnerability exploitation, permission maintenance, and lateral movement, effectively imitating the behaviors of malicious hackers and real-world adversaries.

### Accurate Comparison of Security Protection Product Reliability

After the simulation of attacks on the target system, go to the existing security protection products to check the corresponding alarm information. Compare the detection rates of multiple security protection products to test their reliability.

## Installing the Attack Simulation Toolkit

### Step 1: Querying the Toolkit Installation Status Corresponding to the Asset

1. Log in to the [CSC console](#). In the left sidebar, click **Assets**.
2. On the assets page, select **Servers** to view the installation status of the simulation toolkit on the asset.

**Assets**

Manual update 🕒 🔗 📦 📄 Access multi-cloud assets

**Asset statistics**

**Servers** **Public IPs** **Domains** **Containers** **Gateways** **Databases**

Unprotected With risks : Unprotected With risks Unprotected With risks

Servers Containers **Public IPs**

0bps 0bps 0bps 0bps

By assets **By asset types** By service types  Newly-added  Critical  Unprotected

**Servers(39)** Containers(351) Public IPs(56) Domains(5) Network assets(517) Databases(0) Other cloud resources(127)

Enable protection Tag as Critical Remove from Critical

ID/name	Vulnerabilities	Configuration risks	Time	BAS toolkit	Protecti
				• Not installed	• Not it
				• Installed	• Activ
				• Not installed	• Not it

## Step 2: Installing the Attack Simulation Toolkit

For assets without the attack simulation toolkit installed, you can see the following three installation methods:

### Method 1: Manually Executing the Command

Log in to the target server and execute the corresponding command to download and run the attack simulation toolkit.

### Method 2: Downloading and Running the Attack Simulation Toolkit via Tencent Cloud TAT by Executing Commands

Only assets with the Tencent Cloud TAT client installed are supported. After the command is executed via TAT, the attack simulation toolkit will be downloaded and run on the server.

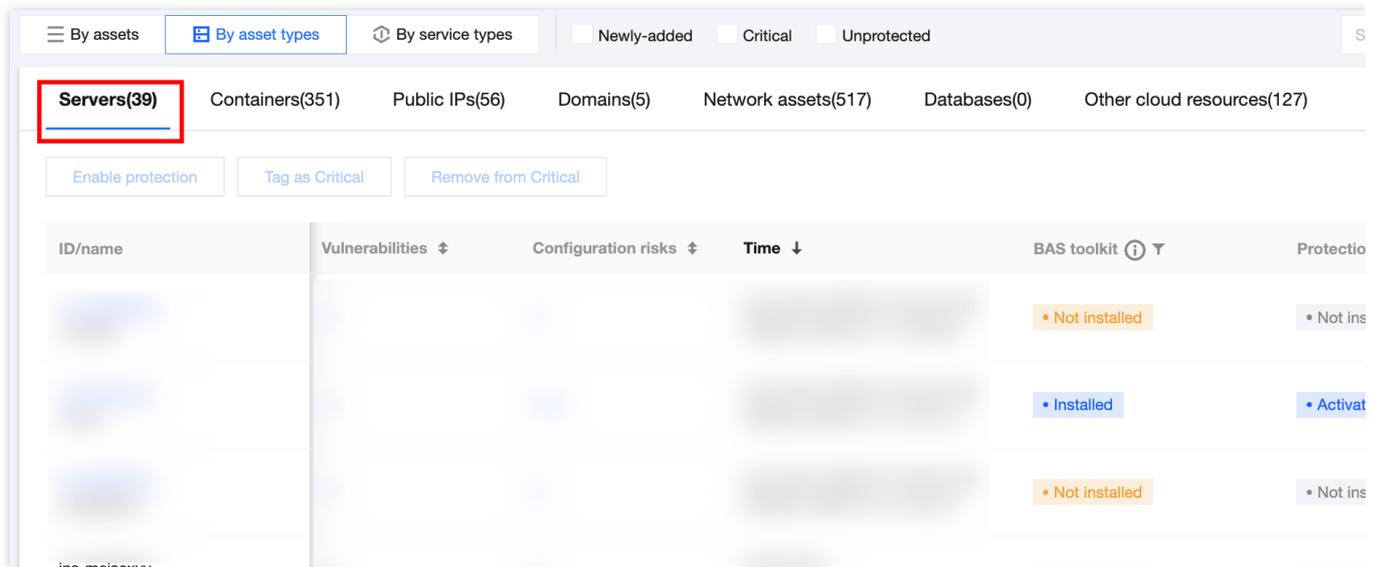
### Method 3: Downloading and Running the Attack Simulation Toolkit via CWPP Agent by Executing Commands

Only assets with the CWPP agent installed are supported. After the command is executed via CWPP agent, the attack simulation toolkit will be downloaded and run on the server.

On the assets page, select the target server assets. In the action bar, click **More > Install toolkit**.

**Note:**

Currently, only servers with Tencent Cloud's Linux operating systems are supported.



### Step 3: How to Conduct Efficient Penetration Testing

#### Viewing Penetration Testing Scripts

On the [breach and attack simulation page](#), you can view penetration testing scripts. The system provides multiple scripts by default, including tactics for information collection, vulnerability scanning, vulnerability exploitation, permission maintenance, and lateral movement, effectively imitating the behaviors of malicious hackers and real-world adversaries.

Breach and attack simulation (BAS)

**Attack Script Overview** Recent attack: 2024-07-18 18:01:03

**Playbooks**

Custom

**Assets available** ⓘ

Assets without toolkit installed

**Tactics | Techniques**

**History**

Attacks

73

- Attack stopp
- Attack succe
- Attack anom

**Attack Script**
Attack Records

Start attack
Custom
Delete
Sep...

MITRE ATT&CK Framework

3  
Reconnaissance

3  
Resource Development

5  
Initial Access

11  
Execution

7  
Persistence

8  
Privilege Escalation

9  
Defense Evasion

5  
Credential Access

6  
Discovery

1  
Lateral M

	Playbook name	Script Source	Server Attack Actions	Network attack actions	Associat...	Execution
<input type="checkbox"/>	-	Custom	Tactics:11 item(s) including Resource Development Combat Technology:23 item(s) including Develop Capabilities	Request Method:POST URI:/report/script/login.php Request Header:{"Host": "111" ... Request Body:clsMode=cls_m...	0	<span style="color: green;">✔</span> Succer
<input type="checkbox"/>	Infected with Xmirg Monero...	System default ...	Tactics:11 item(s) including Resource Development Combat Technology:23 item(s) including Develop Capabilities	-	0	<span style="color: green;">✔</span> Succer
<input type="checkbox"/>	APT Attack 1	System default ...	Tactics:11 item(s) including Resource Development Combat Technology:37 item(s) including Develop Capabilities	-	0	<span style="color: green;">✔</span> Succer

On the [breach and attack simulation page](#), click **ATT&CK matrix** to understand the tactics and techniques associated with each script at the upper right corner, or to learn about the scripts associated with a particular tactic or technique.

### Breach and attack simulation (BAS)

**Attack Script Overview** Recent attack: 2024-07-18 18:01:03

**Playbooks** Custom

**Assets available** Assets without toolkit installed

**Tactics | Techniques**

**History**  
Attacks: **73**  
● Attack stopp  
● Attack succe  
● Attack anom

**Attack Script** | **Attack Records**

Start attack Custom Delete Sepe

MITRE ATT&CK Framework

**Network attack action details**

Request Method: POST

URI: /report/script/login.php

Request Header: {"Host": "111", "Upgrade-Insecure-Requests": "1", "User-Agent": "python-requests/2.31.0", "Accept-Encoding": "gzip,deflate", "Accept": "\*", "Connection": "close", "Sec-Fetch-Dest": "document", "Sec-Fetch-Mode": "navigate", "Sec-Fetch-Site": "cross-site", "Te": "trailers", "Content-Length": "126", "Content-Type": "application/x-www-form-urlencoded"}

Request Body: clsMode=cls\_mode\_login&index=index&log\_type=report&page=login&rnd=0.7550103466497915&userID=admin {placeholder} &userPsw=tmbhuisq

Defense Evasion | Credential Access | Discovery | Lateral M

Network attack actions | Associat... | Execution

Request Method:POST  
URI:/report/script/login.php  
Request Header:{"Host": "111"...  
Request Body:clsMode=cls\_m... 0 Success

Request Method:POST  
URI:/report/script/login.php  
Request Header:{"Host": "111"...  
Request Body:clsMode=cls\_m... 0 Success

Request Method:POST  
URI:/report/script/login.php  
Request Header:{"Host": "111"...  
Request Body:clsMode=cls\_m... 0 Success

Tactics:11 item(s) including Resource Development  
Combat Technology:37 item(s) including Develop Capabilities

▶ **APT Attack 1** System default ...

### Selecting Scripts and the Scope of Assets for Simulated Attacks

1. On the [breach and attack simulation page](#), select one or more scripts, and click **Start attack**.

### Breach and attack simulation (BAS)

**Attack Script Overview** Recent attack: 2024-07-18 18:01:03

**Playbooks** **Assets available** **Tactics | Techniques**

Custom Assets without toolkit installed

**History**

Attacks **55**

- Attack stopp
- Attack succe
- Attack anom

**Attack Script** **Attack Records**

**Start attack** Custom Delete Sepe

MITRE ATT&CK Framework

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral M

	Playbook name	Script Source	Server Attack Actions	Network attack actions	Associat...	Execution
<input type="checkbox"/>	-	Custom	Tactics:11 item(s) including Resource Development Combat Technology:23 item(s) including Develop Capabilities	Request Method:POST URI:/report/script/login.php Request Header:{"Host": "111"... Request Body:clsMode=cls_m...	0	✔ Succeed
<input checked="" type="checkbox"/>	Infected with Xmirg Monero...	System default ...	Tactics:11 item(s) including Resource Development Combat Technology:23 item(s) including Develop Capabilities	-	0	✔ Succeed
<input type="checkbox"/>	APT Attack 1	System default ...	Tactics:11 item(s) including Resource Development Combat Technology:37 item(s) including Develop Capabilities	-	0	✔ Succeed

2. In the simulated attack script pop-up window, select the scope of assets for this simulated attack. Check the Letter of Commitment, and click **OK**.

**Note:**

You can only execute simulated attack scripts on assets with the toolkit installed.

### Execute BAS playbook (i) ×

Playbooks **Infected with Xmirg Monero mining trojan**

Scope (i)  Select from existing  Exclude assets

All assets (219) [Select assets \(0\)](#)

---

Agree and authorize for BAS [View details](#)

I hereby acknowledge that the assets are owned by current enterprise account. The account owner shall bear the legal responsibility for unauthorized usage of the assets.

#### Viewing the Simulated Attack Record of the Script

On the [breach and attack simulation](#) > **Simulated Attack Record** page, you can check the execution status of the current script (successful, exceptional, stopped) through the script execution status, stop ongoing simulated attacks, and resimulate attacks.

Breach and attack simulation (BAS)

**Attack Script Overview** Recent attack: 2024-07-18 18:01:03

**Playbooks**

Custom

**Assets available** ⓘ

Assets without toolkit installed

**Tactics | Techniques**

**History**

- Attack stopp
- Attack succe
- Attack anom

Attack Script
**Attack Records**

Re-attack
Stop attack
All statuses ▼
Sepa

	Attack Time ↕	Attack Script	Server Attack Actions	Network attack actions	Attacke... ↕	Attack result
<input type="checkbox"/>		-	Tactics:11 item(s) including Resource Development Combat Technology:23 item(s) including Develop Capabilities	Request Method:POST URI:/report/script/login.php Request Header:{"Host": "111"... Request Body:clsMode=cls_m...	1	🛡️ Attack stopped
<input type="checkbox"/>		Python rebound shell ...	Tactics:Execution Combat Technology:Command and Scripting Interpreter	-	1	🛡️ Attack stopped
<input type="checkbox"/>		ew intranet traversal	Tactics:Lateral Movement Combat Technology:Lateral Tool Transfer	-	1	✅ Attack succeeded

### Step 4: How to Accurately Compare the Reliability of Security Protection Products

After a successful script attack simulation, you can go to the existing security protection products to view the corresponding execution results of the attack simulation, such as [T-Sec CWP](#). By checking the alarm content detected by the security protection products, you can identify any shortcomings and determine whether the corresponding security policies are properly configured. By comparing the number of alarms detected and the accuracy of the alarm content among multiple security protection products, you can evaluate their reliability.

## FAQs

### Why Did the Installation of the Attack Simulation Toolkit Fail?

**Firewall interception:** It is recommended to allow CSC backend server access addresses in the firewall policy. The public domain names are bas.tencentcs.com and csc-1300616671.cos.ap-guangzhou.myqcloud.com. The public network ports are 8001 and 443.

**Network issues:** It is recommended to check whether the network connection is normal, and try using another network. The attack simulation toolkit needs to be downloaded from the internet. If the network is unstable or the download speed is too slow, it may cause the installation to fail.

**Permission issues:** It is recommended to log in to the system using an administrator account or use the option Run As An Administrator to download/run the attack simulation toolkit. Downloading/running the attack simulation toolkit

requires the administrator permissions. If the current user does not have sufficient permissions, it may cause the installation to fail.

System compatibility issues: Check the System requirements of the attack simulation toolkit to ensure that the current operating system and other software version meet the requirements. The attack simulation toolkit may not be compatible with the current operating system or other software, leading to running failure.

### What Is the Source for the System Default Script?

The system default script is based on the tactical phase in ATT&CK. You can see [MITRE ATT&CK](#) for more information. MITRE ATT&CK is a globally accessible knowledge base of opponent tactics and techniques based on real-world observation. The ATT&CK knowledge base is used as a foundation for developing specific threat models and methods by the private sector, government, and cybersecurity product and service communities.

## System Default Script (Continuously Updated)

Script Name	Script Content
Python base64 command attack	A simulator simulates a hacker using Python to decode a base64-encoded text string, which can be used to execute malicious code or steal sensitive information.
Examine password complexity policies	A simulator simulates a hacker checking the password complexity policy on a Linux system's console to understand the password requirements and limitations, which might be used to crack passwords or obtain access to the system.
Shiro deserialization attack	A simulator simulates a hacker exploiting a Shiro deserialization vulnerability to obtain remote command execution permissions on the target system, executing malicious commands to obtain system access or steal sensitive information.
DNS log information collection	A simulator simulates a hacker obtaining visitor IP addresses through DNS logs to track target user activities or perform other malicious behaviors.
Port forwarding attack	A simulator simulates a hacker collecting information about the target system's weaknesses and vulnerabilities, installing malicious software or exploiting vulnerabilities to maintain access to the target system and using the Netcat tool with port forwarding techniques to bypass firewalls and other security products to execute commands or transfer files on the target system.
Private network lateral movement attack	A simulator simulates a hacker collecting host SSH information to understand the target system's SSH configuration and security, and using the Exploit Writing Toolkit (EW) to further attack other systems by exploiting an already compromised target system to obtain more sensitive information or control more systems within the private network.
User permission	A simulator simulates a hacker transferring sensitive data from the target system to a

persistence attack	server controlled by the simulator or elsewhere to obtain illegal benefits or cause losses. After reading sensitive information, the simulator writes malicious code to maintain access permissions to the target system, and clears various history records in the target system to hide attack traces or mislead investigators.
Malicious file execution attack	A simulator simulates a hacker writing malicious code into a file and executing the file to carry out the attack. The simulator collects SUID information on the target system and executes a Python reverse shell script on the target system. Upon receiving the connection from the target system, she or he performs lateral movement to obtain more system permissions. Subsequently, tamper with the file timestamps to hide attack traces or mislead investigators.
NC reverse shell attack	A simulator simulates a hacker collecting CWPP process information on the target system to attempt killing CWPP relevant processes. The simulator uses the Netcat tool to execute a reverse shell command on the target system, connecting the target system's shell to the simulator's machine. Upon receiving the connection from the target system, the simulator can execute commands or obtain system permissions.
Python reverse shell attack	A simulator simulates a hacker understanding the vulnerabilities and weaknesses of the target system by collecting information. Execute a Python reverse shell script on the target system, connecting the target system's shell to the simulator's machine. Upon receiving the connection from the target system, the simulator can execute commands or obtain system permissions.
Malicious lateral movement	A simulator simulates a hacker understanding the vulnerabilities and weaknesses of the target system by collecting information. The simulator uses the iox malicious tool for port traffic forwarding to control the target system. Then, using the permissions and features of the target system, she or he further attacks other systems to ultimately obtain more sensitive information or control more systems.

# Log Shipping

Last updated : 2024-08-12 17:28:05

## Feature Background

Centralize and normalize logs from multiple CSC products and deliver them to message queues via the console. This facilitates data storage or integration with other systems to consume data, aiding in extracting the value of log data and meeting users' log operation and maintenance needs. Once log delivery is enabled, the collected logs will be delivered to the corresponding message queues.

## Application Scenario

### Log storage

According to the Cybersecurity Law of the People's Republic of China and the Information Security Grade Protection Management Measures, enterprises are required to record and store cybersecurity incidents, and the Log Storage Duration must be at least 6 months. This is to ensure the information security and network security of enterprises and to prevent the occurrence and proliferation of security incidents.

### Offline Analysis

After delivering logs to Kafka/CLS, enterprises can integrate other systems for offline analysis. This helps to manage raw logs, assists in deep analysis and research of security incidents, uncovering the root causes and vulnerabilities, and improves the processing capability and level of handling security incidents.

## Log Delivery to Kafka

On the log analysis page, you can configure different log types accessed by CSC to be delivered to different Topics of specified CKafka instances.

### Preconditions:

To deliver logs to the message queue, you need to purchase the CSC Flagship Version and integrate relevant product logs into CSC. If you need to use either the CKafka Public Domain Name or CKafka Supporting Environment network access method, you must first [go to create a Tencent Cloud Message Queue CKafka instance](#).

### CKafka Public Domain Name Access

1. Log in to [CSC Console](#), in the left navigation pane, click **Log Analysis**.

2. On the Log Analysis page, click **Log shipping** > **Ship to Kafka**.

3. On the Ship to Kafka page, CSC automatically retrieves your Tencent Cloud message queue CKafka instance, for logs already integrated with CSC, select **CKafka (public domain)** and configure the related parameters.

### Log shipping

**Ship to Kafka** Ship to CLS
Go to C

**i** 1. Purchase a CKafka instance. Select the instance specification according to the volume of logs to ship.

2. Enable the allowlist as instructed in the CKafka documentation to achieve public domain access or supporting environment access.

3. Complete the log shipping configuration as instructed below. Note that you can only ship logs with the same Kafka username.

#### Log destination

Log destination  CKafka (public domain)  CKafka (supporting environment)  External Kafka (public network)

TLS Encryption

The Account to Which the TDMQ Belongs **i**

Kafka instance

Public domain

Username **i**

Password

#### Log shipping rules

Log source	Log type	Account source	Topic ID/name <b>i</b>	Op
<input type="text" value="CFW"/>	<input type="text" value="All"/>	<input type="text" value="All accounts"/>	<input type="text" value="Select a topic name"/>	De
<input type="text" value="WAF"/>	<input type="text" value="All"/>	<input type="text" value="All accounts"/>	<input type="text" value="Select a topic name"/>	De
<input type="text" value="CWPP"/>	<input type="text" value="All"/>	<input type="text" value="All accounts"/>	<input type="text" value="Select a topic name"/>	De
<input type="text" value="CSC"/>	<input type="text" value="All"/>	<input type="text" value="All accounts"/>	<input type="text" value="Select a topic name"/>	De
<input type="text" value="CloudAudit"/>	<input type="text" value="All"/>	<input type="text" value="All accounts"/>	<input type="text" value="Select a topic name"/>	De

**+** Add log shipping configuration

OK

Cancel

Parameter name	Description
Log destination	CKafka (public domain).
TLS Encryption	Select whether to enable TLS encryption.
The Account to Which the TDMQ Belongs	Target account for shipping
Kafka instance	CSC automatically retrieves your Tencent Cloud message queue Ckafka instance. Select the required message queue instance.
Public domain	Select the required public domain name.
Username	Please enter the selected message queue instance's username.
Password	Please enter the selected message queue instance's password.
Log source	Supports selecting logs from CWPP, CFW, WAF, CSC, Anti-DDoS, SaaS Bastion Host, CloudAudit, and Network HoneyPot.
Log type	The log type varies depending on the chosen log source.
Topic ID/Name	Select the required Topic.
Operation	<p>Add: click <b>Add log shipping configuration</b>, multiple log sources can be added.</p> <p>Delete: click <b>Delete</b> in the log operation column of the target log. After second confirmation, the log delivery task corresponding to the log type of this log source can be deleted.</p> <p>Edit: If it is not the first time configuring log delivery, you can click <b>Modify Configuration</b> on the log delivery page to modify the related log delivery.</p>

4. After confirming that everything is correct, click **OK** to deliver the collected logs to the corresponding message queue.

5. On the Log Delivery page, you can view details of synchronous access method, access object, message queue status, username, and other message queue details, as well as log source, log type, account source (under multiple accounts), Topic ID/Name, Topic delivery status, delivery switch, and other information. It also allows modifications to message queue and Topic configurations, and viewing the status of the message queue and each Topic.

### CKafka Supporting Environment Access

1. Log in to [CSC Console](#), in the left navigation pane, click **Log Analysis**.
2. On the Log Analysis page, click **Log shipping > Ship to Kafka**.
3. On the Ship to Kafka page, CSC automatically retrieves your Tencent Cloud message queue CKafka instance and the log source already integrated with CSC. Select **CKafka (supporting environment)** and configure the related parameters.

#### Log shipping

**Ship to Kafka** Ship to CLS
Go to

**i** 1. Purchase a CKafka instance. Select the instance specification according to the volume of logs to ship.

2. Enable the allowlist as instructed in the CKafka documentation to achieve public domain access or supporting environment access.

3. Complete the log shipping configuration as instructed below. Note that you can only ship logs with the same Kafka username.

#### Log destination

Log destination  CKafka (public domain)  CKafka (supporting environment)  External Kafka (public network)

TLS Encryption

The Account to Which the TDMQ Belongs **i**

Kafka instance

Supporting environment

#### Log shipping rules

Log source	Log type	Account source	Topic ID/name <b>i</b>
<input type="text" value="CFW"/>	<input type="text" value="All"/>	<input type="text" value="All accounts"/>	<input type="text" value="Select a topic name"/>
<input type="text" value="WAF"/>	<input type="text" value="All"/>	<input type="text" value="All accounts"/>	<input type="text" value="Select a topic name"/>
<input type="text" value="CWPP"/>	<input type="text" value="All"/>	<input type="text" value="All accounts"/>	<input type="text" value="Select a topic name"/>
<input type="text" value="CSC"/>	<input type="text" value="All"/>	<input type="text" value="All accounts"/>	<input type="text" value="Select a topic name"/>
<input type="text" value="CloudAudit"/>	<input type="text" value="All"/>	<input type="text" value="All accounts"/>	<input type="text" value="Select a topic name"/>

[+ Add log shipping configuration](#)

OK

Cancel

Parameter name	Description
Log destination	CKafka (supporting environment).
TLS Encryption	Select whether to enable TLS encryption.
The Account to Which the TDMQ Belongs	Target account for shipping
Kafka instance	CSC automatically retrieves your Tencent Cloud message queue Ckafka instance. Select the required message queue instance.
Supporting environment	Select the required supporting environment.
Log source	Supports selecting logs from CWPP, CFW, WAF, CSC, Anti-DDoS, SaaS Bastion Host, CloudAudit, and Network Honeypot.
Log type	The log type varies depending on the chosen log source.
Topic ID/Name	Select the required Topic.
Operation	<p>Add: click <b>Add log shipping configuration</b>, multiple log sources can be added.</p> <p>Delete: click <b>Delete</b> in the log operation column of the target log. After second confirmation, the log delivery task corresponding to the log type of this log source can be deleted.</p> <p>Edit: If it is not the first time configuring log delivery, you can click <b>Modify Configuration</b> on the log delivery page to modify the related log delivery.</p>

4. After confirming that everything is correct, click **OK** to deliver the collected logs to the corresponding message queue.

5. On the Log Delivery page, you can view details of synchronous access method, access object, message queue status, username, and other message queue details, as well as log source, log type, account source (under multiple

accounts), Topic ID/Name, Topic delivery status, delivery switch, and other information. It also allows modifications to message queue and Topic configurations, and viewing the status of the message queue and each Topic.

### Other Kafka Public Network Access

1. Log in to [CSC Console](#), in the left navigation pane, click **Log Analysis**.
2. On the Log Analysis page, click **Log shipping > Ship to Kafka**.
3. In the Ship to Kafka page, select **External Kafka (public network)** and configure the related parameters.

#### Log shipping

**Ship to Kafka** Ship to CLS
Go

**i** 1. Purchase a CKafka instance. Select the instance specification according to the volume of logs to ship.

2. Enable the allowlist as instructed in the CKafka documentation to achieve public domain access or supporting environment access.

3. Complete the log shipping configuration as instructed below. Note that you can only ship logs with the same Kafka username.

#### Log destination

Log destination  CKafka (public domain)  CKafka (supporting environment)  External Kafka (public network)

TLS Encryption

Public network

Username **i**

Password

#### Log shipping rules

Log source	Log type	Account source	Topic name <b>i</b>
<input type="text" value="CFW"/>	<input type="text" value="All"/>	<input type="text" value="All accounts"/>	<input type="text" value="Enter a topic name"/>
<input type="text" value="WAF"/>	<input type="text" value="All"/>	<input type="text" value="All accounts"/>	<input type="text" value="Enter a topic name"/>
<input type="text" value="CWPP"/>	<input type="text" value="All"/>	<input type="text" value="All accounts"/>	<input type="text" value="Enter a topic name"/>
<input type="text" value="CSC"/>	<input type="text" value="All"/>	<input type="text" value="All accounts"/>	<input type="text" value="Enter a topic name"/>
<input type="text" value="CloudAudit"/>	<input type="text" value="All"/>	<input type="text" value="All accounts"/>	<input type="text" value="Enter a topic name"/>

[+ Add log shipping configuration](#)

OK

Cancel

Parameter name	Description
Log destination	External Kafka (public network).
TLS Encryption	Select whether to enable TLS encryption.
Public network	Enter the public network information based on actual needs.
Username	Please enter the selected message queue instance's username.
Password	Please enter the selected message queue instance's password.
Log source	Supports selecting logs from CWPP, CFW, WAF, CSC, Anti-DDoS, SaaS Bastion Host, CloudAudit, and Network Honeypot.
Log type	The log type varies depending on the chosen log source.
Topic name	Enter the desired Topic name.
Operation	<p>Add: click <b>Add log shipping configuration</b>, multiple log sources can be added.</p> <p>Delete: click <b>Delete</b> in the log operation column of the target log. After second confirmation, the log delivery task corresponding to the log type of this log source can be deleted.</p> <p>Edit: If it is not the first time configuring log delivery, you can click <b>Modify Configuration</b> on the log delivery page to modify the related log delivery.</p>

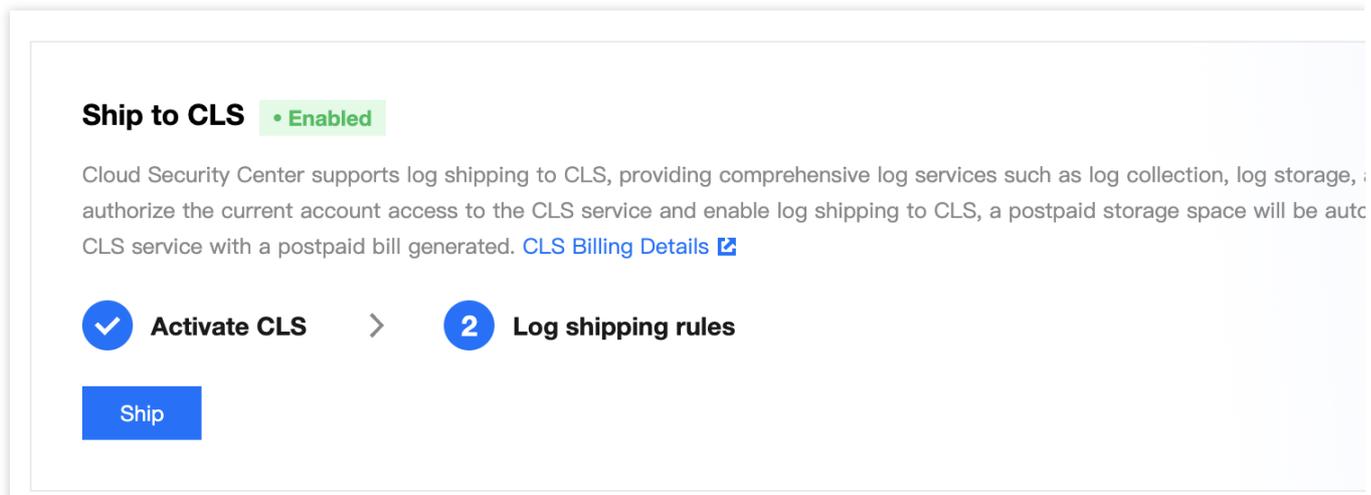
4. After confirming that everything is correct, click **OK** to deliver the collected logs to the corresponding message queue.

5. On the log delivery page, you can view details such as synchronous access method, access object, message queue status, username, log source, log type, account source (under multiple accounts), Topic name, Topic delivery status, delivery switch, etc., and you are allowed to modify the message queue and Topic configuration.

## Shipping Logs to CLS

On the log analysis page, you can configure different types of logs connected to CSC and ship them to different specified log topics in CLS respectively.

1. Click the **Log shipping** at the top left corner to open the log shipping configuration pop-up. If the CLS service has not been activated before, you need to click [Go to Authorization](#), agree to service authorization, and create a service role to proceed with more log shipping configurations.



**Note:**

CSC supports shipping logs to CLS, enabling comprehensive CLS services like log collection, log storage, and log search. After the current account authorizes access to CLS and enables shipping logs to CLS, a pay-as-you-go storage space will be automatically created in CLS, along with a pay-as-you-go bill. For details, see [CLS Billing Information](#).

2. After the authorization is completed, you can configure different log topics for logs to be shipped. (Logs not to be shipped do not need to be configured.)

**Log shipping**

Ship to Kafka **Ship to CLS**

**i** Once you authorize the current account access to the CLS service and enable log shipping to CLS, a postpaid storage space will be created in the CLS service with a postpaid bill generated. [CLS Billing Details](#)

**Delivery account**

Target Account for Shipping

**Delivery content**

Log source

Log type

Log Source Account

**Shipping object** **i**

Target Region

Logset Operation  Select the existing logset  Create Logset

Logset

Log Topic Operation  Select existing log topic  Create Log Topic

Log Topic

Parameter	Description
Target account for shipping	Target account for shipping
Log source	Supports selecting logs from CWPP, CFW, WAF, CSC, Anti-DDoS, SaaS Bastion Host, CloudAudit, and Network Honeypot.
Log type	The log type varies depending on the selected log source.
Log source account	Names of multi-accounts corresponding to the selected log source.

Target region	Enter the target region for shipping.
Logset operation	Select to ship to an existing logset or create a logset for shipping.
Logset	Enter the name of the new logset. / Select an existing logset.
Log topic operation	Select to ship to an existing log topic or create a log topic for shipping. CLS only supports shipping to log topics created in CSC.
Log topic	Enter the name of the new log topic. / Select an existing log topic.

- After everything is confirmed, you can click **OK** to ship the collected logs to the corresponding log topic.
- On the log shipping page, you can view the account name/ID, department, log source, log type, source account (under multi-account), log topic, shipping status, shipping switch, and other information. It also allows you to edit shipped tasks, (batch) delete tasks, (batch) enable/disable tasks, (batch) refresh, and perform log search.

**Log shipping**

Ship to Kafka    **Ship to CLS**

---

**Shipping Account**

Account Name/ID

Dept.

---

**Log shipping configurations**

<input type="checkbox"/>	Log source	Log type	Source Account	Log Topic ⓘ	Status	SI
<input type="checkbox"/>	CSC	Port Risk Logs	Multiple (3)		• Normal	(

Total: 1 10 / page

## Delivery and Delivering Objects

### Multi-account management

After enabling the [Multi-account Management](#) feature, multi-account and multi-product log delivery is supported.

- Log in to [CSC Console](#), in the left navigation pane, click **Log Analysis**.

2. On the Log Analysis page, click **Multi-account Management** at the top right.

**Log Analysis** Mut

---

**Log Overview**

Access Log Source

# 13

[Configure log sources](#)

Log shipping

# 0

[Log shipping](#)

Log capacity usage

# 0/0

 GB
 [Expand now](#)

No product logs are accessed.

Log Trend Last 7 days ▾

07-24      07-26

3. On the Multi-account Management page, select the required account, click **OK**.

Q

	Account name	Account ID/App ID	Dept. ▾
<input type="radio"/>	tcss	200026291205 1312704563	邀请
<input type="radio"/>	tuber0613@gmail.com	200027074678 1313461053	Root
<input checked="" type="radio"/>	zhaowenjun613@vip.qq.com	200027991717 1314512458	邀请

OK
Cancel

Scenario Description	Not configured	Configuration completed
----------------------	----------------	-------------------------

<p>The Administrator/Delegated Administrator unifies the delivery of multiple product logs from all accounts into a single Kafka.</p>	<p>After selecting all accounts in the upper right corner to configure log delivery, under both Public Domain Access and Supporting Environment Access for CKafka, the <b>Administrator's</b> CKafka will be automatically retrieved. You can select the required Tencent Cloud Message Queue.</p>	<p>Displays the Administrator's message queue status, user information, and other message queue details, along with synchronized configured log sources, log types, account sources, and delivery status.</p>
<p>The Administrator/Delegated Administrator manages other accounts' logs by configuring multiple product log deliveries for other accounts.</p>	<p>After selecting other accounts in the upper right corner to configure log delivery, under both Public Domain Access and Supporting Environment Access for CKafka, the <b>other account's</b> CKafka will be automatically retrieved. You can select the required Tencent Cloud Message Queue.</p>	<p>Displays other accounts' message queue status, user information, and other message queue details, along with synchronized configured log sources, log types, and delivery status.</p>
<p>The Administrator/Delegated Administrator manages the current account's (Administrator/Delegated Administrator) logs by configuring multiple product log deliveries for the current account.</p>	<p>After selecting the current account (Administrator/Delegated Administrator) in the upper right corner to configure log delivery, under both Public Domain Access and Supporting Environment Access for CKafka, the CKafka for <b>the current account (Administrator/Delegated Administrator)</b> will be automatically retrieved. You can select the required Tencent Cloud Message Queue.</p>	<p>Displays the current account's (Administrator/Delegated Administrator) message queue status, user information, and other message queue details, along with synchronized configured log sources, log types, and delivery status.</p>

## Single account management

Only supports multi-product log delivery for the current account.

Not configured: When configuring log delivery, CKafka for the current account will be automatically retrieved under both CKafka Public Domain Access, and CKafka Supporting Environment Access network access methods. You can select the required Tencent Cloud Message Queue.

### Note:

If the current account is managed by an Administrator/Delegated Administrator, the Administrator/Delegated Administrator may edit the log delivery configuration of the current account.

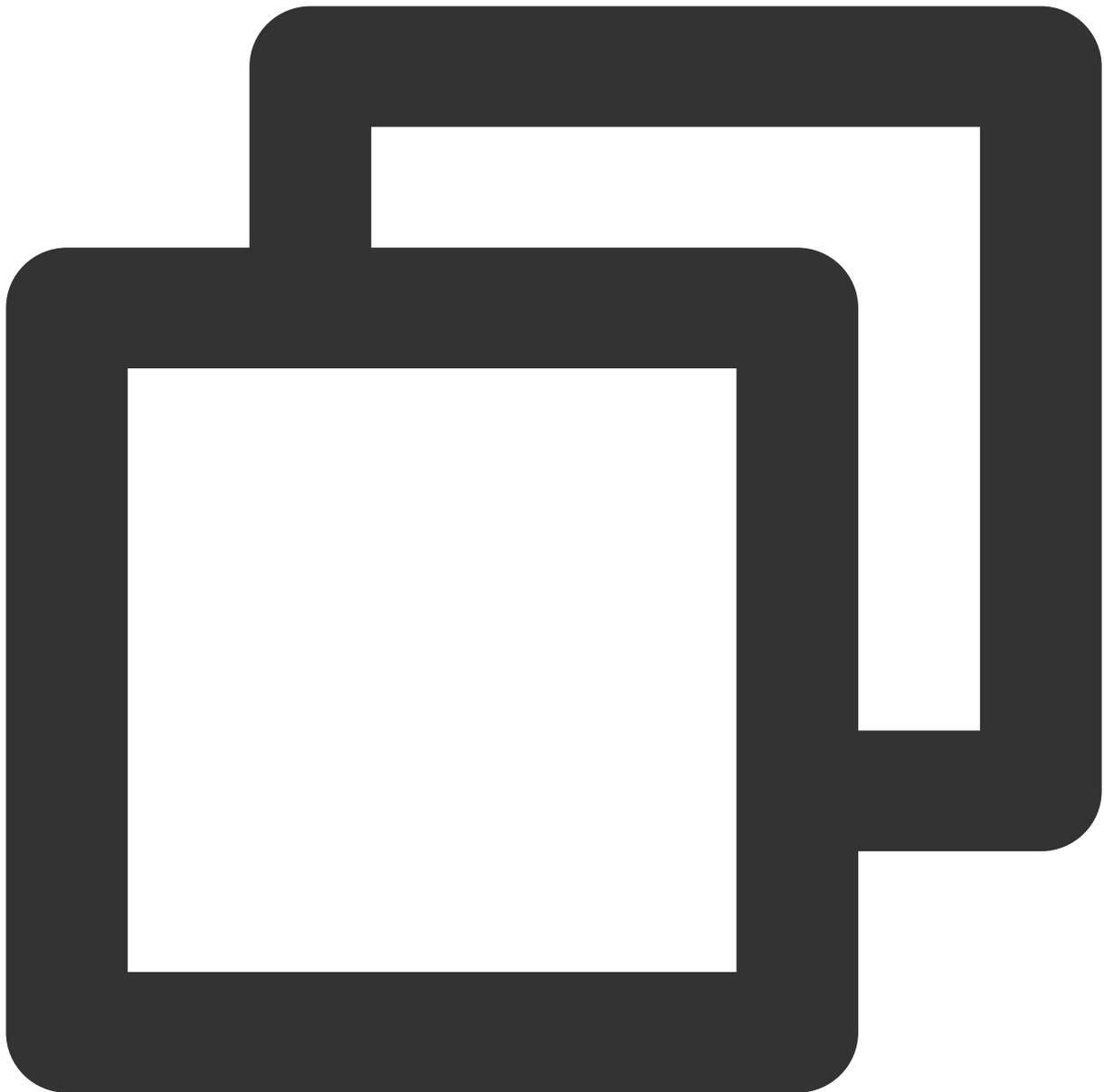
After configuration: Displays the current account's message queue status, user information, and other message queue details, along with synchronized configured log sources, log types, delivery status, and other log delivery details.

## FAQs

### **How is log delivery charged?**

Log Delivery is exclusive to CSC Enterprise Edition. You can [purchase Log Delivery](#).

### **Public Network Log Delivery Egress IP allowlist**



```
106.55.200.0/24
106.55.201.0/24
106.55.202.0/24
81.71.5.0/24
134.175.239.0/24
193.112.130.0/24
193.112.164.0/24
193.112.221.0/24
111.230.173.0/24
111.230.181.0/24
129.204.232.0/24
```

193.112.129.0/24  
 193.112.153.0/24  
 106.52.11.0/24  
 106.55.52.0/24  
 118.89.20.0/24  
 193.112.32.0/24  
 193.112.60.0/24  
 106.52.106.0/24  
 106.52.67.0/24  
 106.55.254.0/24  
 42.194.128.0/24  
 42.194.133.0/24  
 106.52.69.0/24  
 118.89.64.0/24  
 129.204.249.0/24  
 182.254.171.0/24  
 193.112.170.0/24  
 106.55.207.0/24  
 119.28.101.0/24  
 150.109.12.0/24

### Which products and log types does Log Delivery support?

Product	Log type	Log type
Cloud Firewall	Access control log	CFW Rule Hit Logging is generated based on access control rules configured by users in Internet Border Firewall, NAT Boundary Firewall, VPC-to-VPC Firewall, and Enterprise Security Group.
	Zero Trust Protection Log	Zero Trust Protection Log in CFW includes Remote Operation and Maintenance Login, Web Service Access, and Database Access, along with log in to and access service details.
	Intrusion Defense Log	CFW Based on the "Observation Mode" and "Interception Mode", all security events generated and recorded include four lists: "External Intrusion, Host Compromise, Lateral Movement, Network Honeypot". They allow for the examination of inbound and outbound security event details.
	Flow Logs	CFW Internet Border Firewall and NAT Boundary Firewall monitor north-south traffic generated by inbound and outbound actions and east-west traffic between VPCs.
	Operations logs	In CFW, all operational behaviors and details based on the security policies and switch pages within the account are recorded.

Web Application Firewall	Attack Logs	WAF provides attack logs that record the attack time, attack source IP, attack type, and attack details.
	Access Log	WAF records access log information for the protected domain.
Cloud Workload Protection Platform	Intrusion Detection Log	CWPP provides security logs for multi-dimensional intrusion detection, including Trojans, high-risk commands, local privilege escalation, and all log in to behavior events.
	Vulnerability Management Log	CWPP security logs for detailed situations of vulnerability security events.
	Advanced Defense Log	CWPP logs for Advanced Defense, including Java Memory Horse and attack detection.
	Client-related logs	CWPP detected that the client was offline abnormally for over 24 hours and did not come back online. The client was Uninstall (for servers running Linux System) logs.

# Managing Assets

Last updated : 2024-08-02 10:14:18

CSC automatically synchronizes the security status of connected Tencent Cloud assets. You can also manually add non-Tencent Cloud IPs/domains for unified management. See below of the list of supported Tencent Cloud assets:

Asset types	Assets
Servers	CVMs
	External servers
	Lighthouse instances
	Edge Compute Machine instances
Containers	Containers
	Local images
	Repository images
	Nodes
	Clusters
	Pods
Public IPs	IPs
	High-availability virtual IPs
	EIPs
	External IPs
	Elastic IPv6 addresses
	Anycast IPs
Domains	Tencent Cloud domains
	External domains
Network assets - Gateways	NAT gateways
	VPN gateways

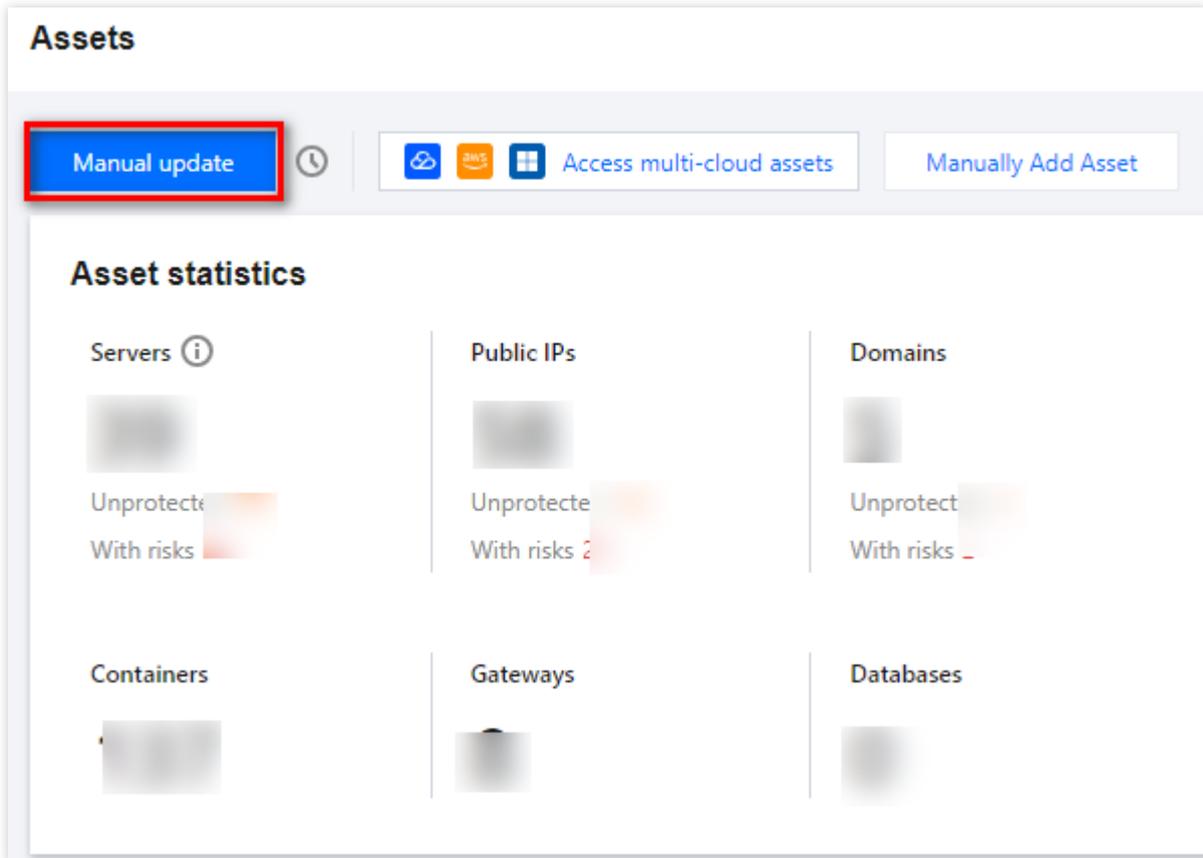
	CLBs
	NAT firewalls
	Probes
Network assets - ENIs	ENIs
Private networks	VPCs
	Subnets
Databases	TencentDB for MySQL
	TencentDB for Redis
	TencentDB for MariaDB
	TencentDB for PostgreSQL
	TencentDB for MongoDB
Other cloud resources	Cloud Block Storage
	Cloud Object Storage
	Cloud File Storage
	Message Queue
	Elasticsearch Service

## Updating assets

On the [Assets](#) page, click **Manual update** in the upper left corner. CSC automatically obtains and lists data of Tencent Cloud assets. This process may take 3 to 5 minutes if there are many assets. It takes even longer for updating container assets.

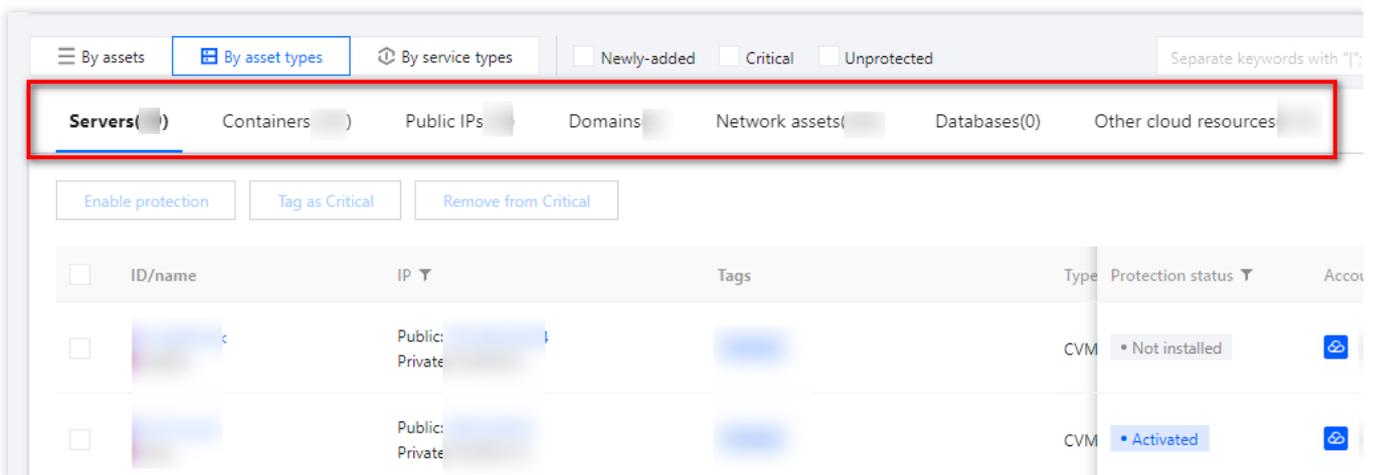
**Note:**

Data of Tencent Cloud assets are automatically synchronized. For external assets, see [Adding External Assets](#).

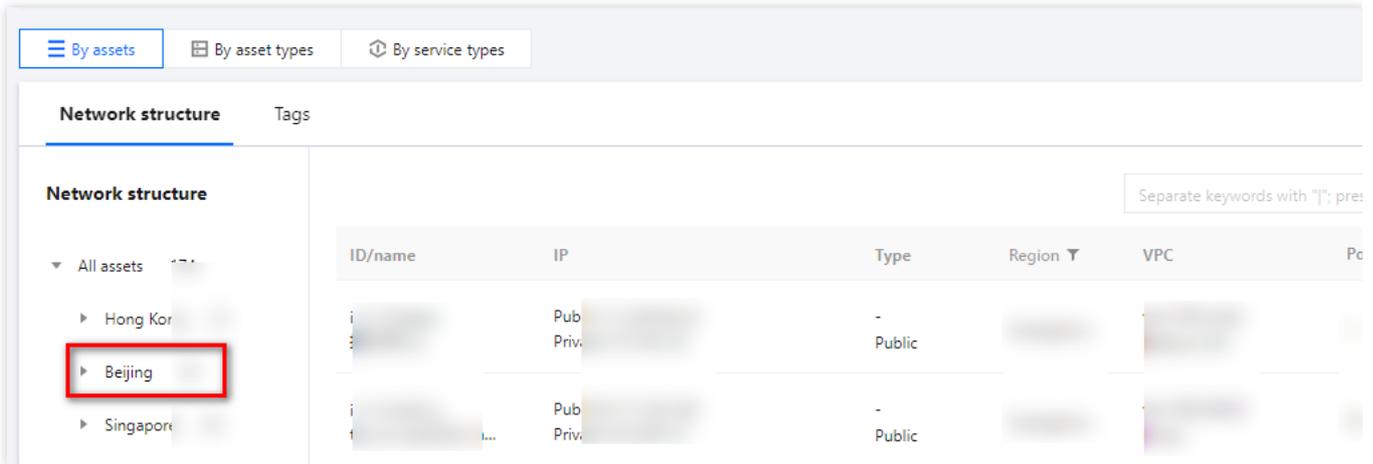


## Searching for assets

On the [assets](#) page, select **By asset types** to query servers, containers, domains, and public IPs assets under the account.



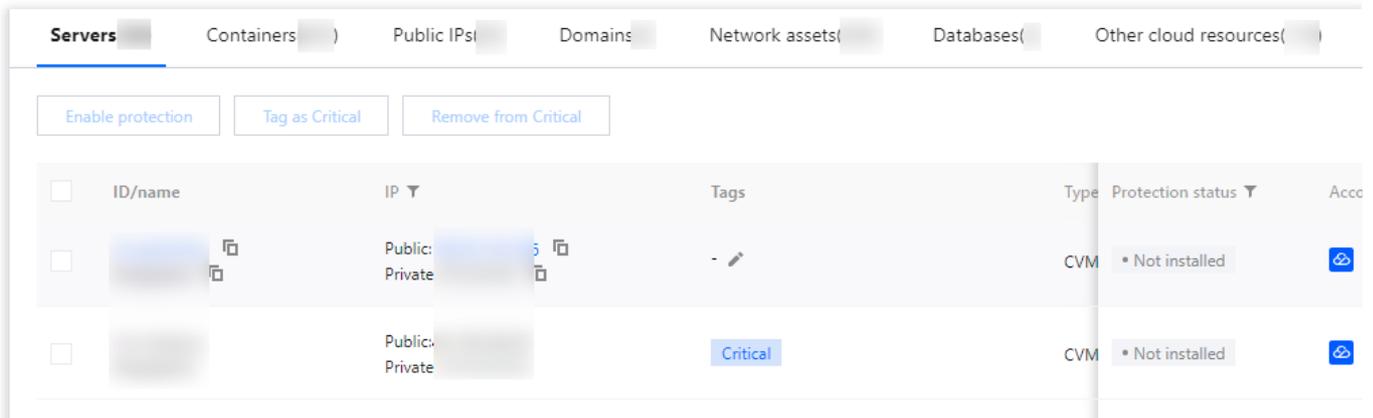
On the [assets](#) page, select **By assets** to query which VPCs are available in each region, and which assets are located within each VPC from a network structure perspective.



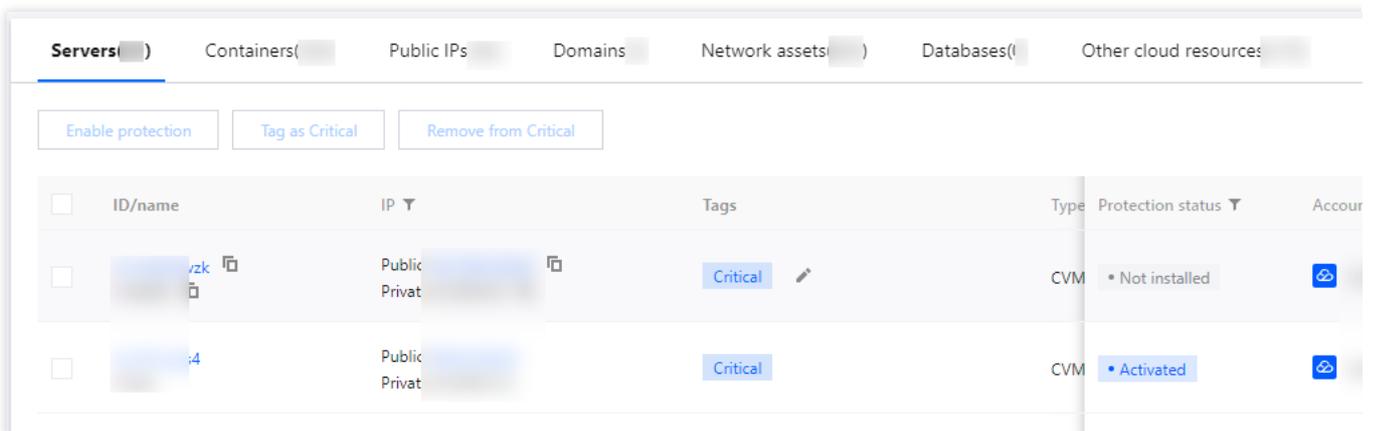
## Tagging critical assets

Common critical assets are automatically tagged. You can also manually tag critical assets of your services as needed.

On the [assets](#) page, select the target non-critical asset, and click **More > Tag as Critical**. Tag the asset, and the tag appears to the right of the asset name.



On the [assets](#) page, select the target critical asset, and click **More > Remove from Critical**.



On the [Assets](#) page, you can filter out critical/non-critical assets. You can also check the status of security product related with an asset.

Servers are protected by CWPP.

IPs are protected by CFW.

Domains are protected by WAF.

**Note:**

Keep checking the security status of your critical assets and make sure they are protected.

## Adding custom tags for assets

1. On the [Assets](#) page, select the target asset, and click



in the tag column to add a custom tag.

2. In the tag editing window, select the tag key and tag value, and click **OK**.

**Edit Tag** ×

Tags are used to manage resources by category in different dimensions. If the existing tags don't meet your requirements, you can [manage tags](#).

1 resource(s) selected

Tag Key ▼ Tag Value ▼ ×

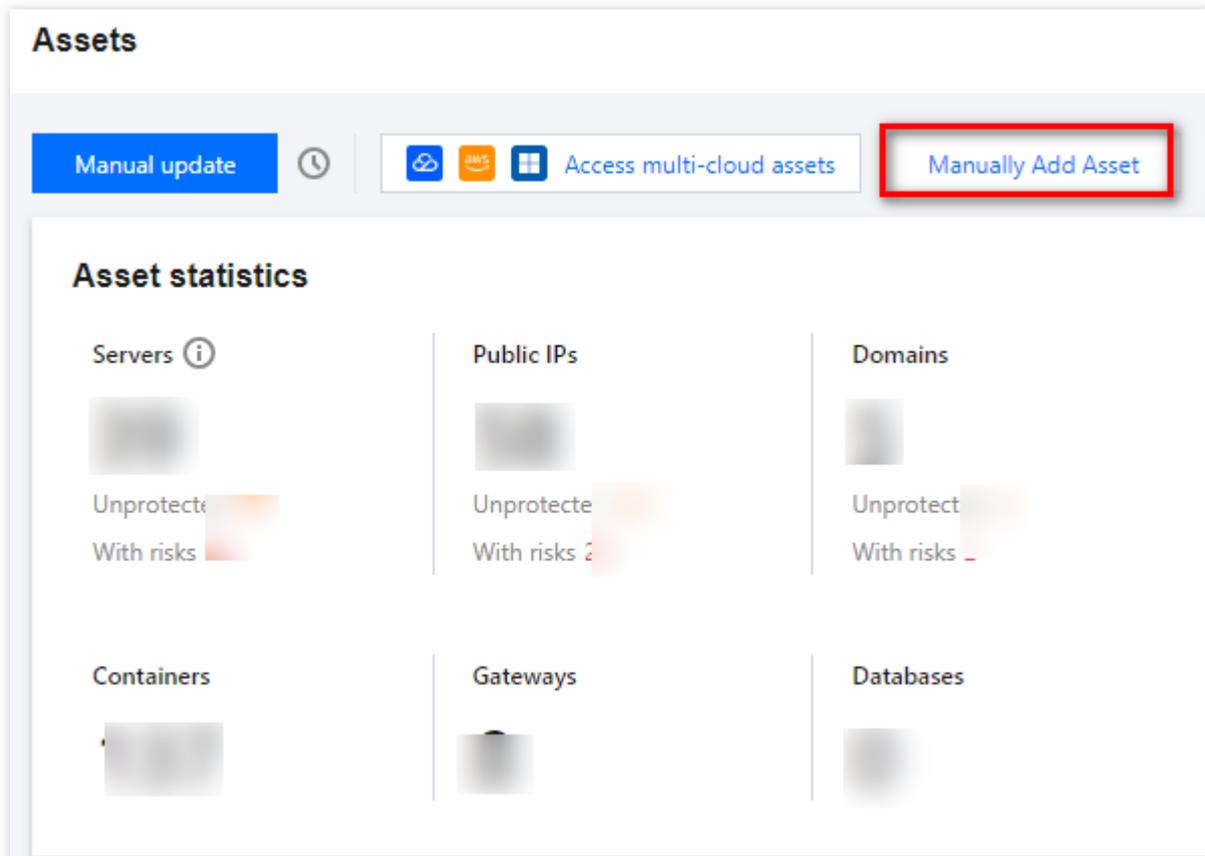
[+ Add](#)

**OK** Cancel

3. After adding tags, click **Tags** to view assets by custom tags.

## Adding external assets

1. If you need to manage the non-Tencent Cloud assets, click **Manually Add Asset** at the upper right corner on the [assets](#) page.



2. In the manual asset addition window, enter public IPs and domains outside Tencent Cloud, check the acknowledgment, and click **OK**.

**Note:**

This feature is now only available to beta users. To try it out, please [submit a ticket](#).

Make sure that the assets to add are owned by the current organization. The account owner shall bear the legal responsibility for unauthorized usage of the assets.

### Manually Add Asset

You can add public IPs and domains outside Tencent Cloud.

Options  Manual input  Import

Address

1 .

Enter public IPs, website domains, and API domains. For manual input, one address per line. Up to 1000 addresses allowed. For copying and pasting multiple addresses, separate them with ",". CIDR blocks are not supported. Duplicate IPs are automatically merged.

I hereby acknowledge that the assets to check are owned by current enterprise account. The account owner shall bear the legal responsibility for unauthorized usage of the assets. [View details](#)

## Managing assets under multiple accounts

Click **Multi-account** in the upper right corner and select one or more accounts of members under the same organization. You can view assets of the selected accounts. For more information, see [Multiple Account Management](#).

Multi-account

Please enter Account Name/Account ID to search

<input type="checkbox"/>	Account Name	Account ID/APPID	Dept. ▾
<input checked="" type="checkbox"/>	[Tencent Cloud Icon]	[Blurred]	[Blurred]
<input checked="" type="checkbox"/>	[Tencent Cloud Icon]	[Blurred]	[Blurred]
<input checked="" type="checkbox"/>	[Tencent Cloud Icon]	[Blurred]	[Blurred]
<input type="checkbox"/>	[AWS Icon]	[Blurred]	[Blurred]
<input type="checkbox"/>	[AWS Icon]	[Blurred]	[Blurred]
<input type="checkbox"/>	[Blurred]	[Blurred]	[Blurred]

OK Cancel

# Health Checks

## Product Features

Last updated : 2023-09-21 17:41:24

### Feature overview

Cloud Security Center (CSC) provides security health checks to discover six types of major risks on your cloud assets. This helps address the challenges of network attacks and data breaches, and enhance the security capabilities of enterprises.

### Use cases

#### Routine security health checks

Customers can initiate security health checks on a periodic basis to assess their enterprise security status, identify potential security issues, and take appropriate measures to enhance the security level of the enterprise.

### Feature details

#### Health check items

Item	Description	Related product
Port risks	Detect port risks on public IPs and domains utilizing the port exposure detection capability provided by CSC and CFW.	CSC
Vulnerabilities	Scan for vulnerabilities based on a rich vulnerability database. It covers OWASP TOP 10 vulnerabilities, such as SQL injection, XSS, CSRF, and weak passwords. The system can also detect zero-day/one-day/n-day vulnerabilities.	CSC, CWPP and TCSS
Weak passwords	Check weak passwords on servers, public IPs and domains.	CSC, CWPP
Configuration risks	Check for configuration risks on CVM, TKE, COS, TencentDB and CLB instances.	CSC, CWPP and TCSS
Risk exposure	Provide an internet attack surface mapping feature to identify exposed ports, services, and components of cloud assets visible on the Internet.	CSC

Website content risks	Identify sensitive images and texts on websites, and support detection of trojans, hidden links, spam advertisements, mining pools and more.	CSC
-----------------------	--	-----

**Note:**

To detect vulnerabilities, weak passwords, and exposed risky services, we need to scan ports of the target system. For example, if port 80 (HTTP services) is found open on the target server, it may be exposed to web application vulnerabilities.

**Checked assets**

Asset	Item
CVM, Lighthouse, Edge Computing Machine (ECM)	Vulnerabilities, weak passwords, configuration risks
Authorized local images and repository images	Vulnerabilities
Cluster with the scanner running properly	Vulnerabilities, configuration risks
Public IPs, domain names	Ports, vulnerabilities, weak passwords, website content risks
CLB, subnets, TencentDB for MySQL, TencentDB for Redis, TencentDB for MariaDB, TencentDB for PostgreSQL, TencentDB for MongoDB, CBS, COS, Elasticsearch Service	Configuration risks

**Note:**

Risk exposure is available on CSC Enterprise and Ultimate. It does not consume the health check quota. Also, the detection of configuration risks on subnets and CBS instances does not consume the health check quota.

**Quota consumption**

Asset	Item	Consumed quota
Public IPs, domain names	Vulnerabilities, weak passwords, website content risks	Quota consumed per health check = Number of checked assets
CVM, CLB, TencentDB for MySQL, TencentDB for Redis, TencentDB for MariaDB, TencentDB for	Configuration risks	

PostgreSQL, TencentDB for MongoDB, Elasticsearch Service, COS		
---	--	--

## Comparison of CSC editions

Item	Free edition	Premium edition	Enterprise edition	Ultimate edition
Port risks	✓	✓	✓	✓
Emergency vulnerabilities	✓	✓	✓	✓
Vulnerabilities	-	✓	✓	✓
Weak passwords	-	✓	✓	✓
Configuration risks	-	✓	✓	✓
Risk exposure	-	-	✓	✓
Website content risks	-	-	✓	✓
Health check quota	20 times	400 times/month (scalable)	1,200 times/month (scalable)	4,800 times/month (scalable)
Task quota	1 task	10 tasks	20 tasks	50 tasks (scalable to unlimited)

CSC provides different check items for different editions. Each security check consumes different quota usage.

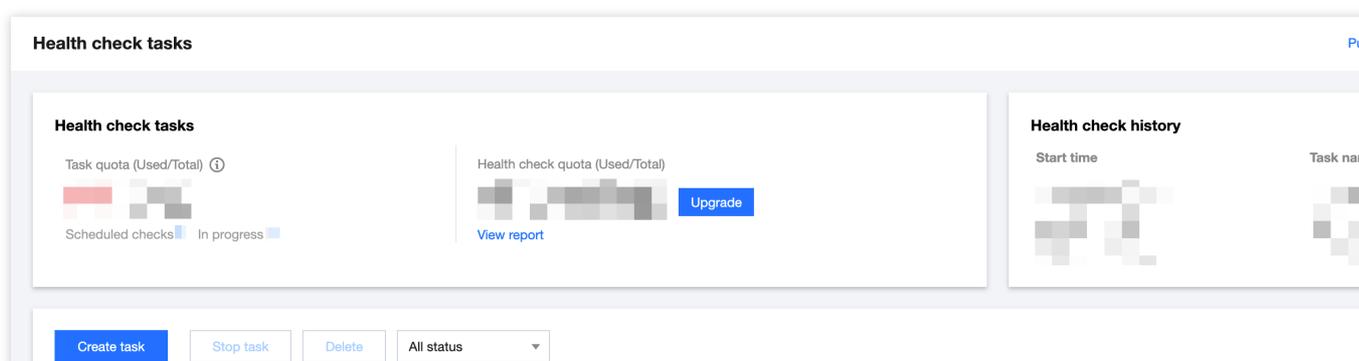
# Operation Guide

Last updated : 2023-09-21 17:41:05

## Health check options

### Health Check Tasks

On the [Health check tasks page](#), you can check the exposed ports, sensitive information and services, find potential vulnerabilities, weak passwords, cloud resource configuration risks and other security threats. Multiple health check modes are supported. The health check is integrated with Cloud Security Center, Cloud Workload Protection Platform and Tencent Container Security Service.



### Full check

On the [Overview - Security Center](#), the four modules, including "Security products", "Assets", "High risks" and "High-risk alerts", provide a one-stop solution for product trial, asset authorization, risk processing and alert disposal.

### Solid protection

On the [Solid protection](#) page, click **Quick scan** to scan for urgent vulnerabilities on public IPs and domains.

#### Note:

Each account is granted a free quota of two urgent vulnerability scans.

## Creating tasks

1. Log in to the [Cloud Security Center console](#), and click **Health check tasks** in the left sidebar.
2. On the **Health check tasks page**, click **Create task**.
3. In the pop-up window, configure the required parameters and click **OK**.

**Create task** ⓘ
👤 [User Avatar] ✕

Task name ⓘ

Mode  Basic  Standard  Advanced ⓘ

Plan ⓘ  Immediate  Specified time  Scheduled checks

Daily
🕒

Included assets  All assets ⓘ  Select from existing  Manual input

Import

[Exclude assets \(0\)](#)

Check items ⓘ

Port risks ⓘ

Vulnerabilities ⓘ

Weak passwords ⓘ

Content risks ⓘ

Configuration risks ⓘ

Exposed risk services ⓘ

Estimated duration  minutes

Quota usage ⓘ

---

Agree to Health Check Authorization Agreement. [View details](#)

I hereby acknowledge that the assets to check are owned by current enterprise account. The account owner shall bear the legal responsibility for unauthorized usage of the assets.

OK
Cancel

Parameter	Description
Task name	Enter a custom task name. You can query the task result later by using this name on the <b>Risks</b> page.
Mode	<p><b>Basic:</b> Quickly initiate scans for port risks, urgent vulnerabilities, and exposed risk services.</p> <p><b>Standard:</b> Scan for six types of risks, including port risks, vulnerabilities, weak passwords, configuration risks exposed risk services, and website content risks.</p> <p><b>Advanced:</b> Create an advanced health check task to customize the configurations of health check items. Users can manually enter or import files to add discrete ports for exposed port detection</p>
Plan	<p><b>Immediate:</b> Start a health check immediately when there is a security issue or an apparent security threat.</p> <p><b>Specified time:</b> Start a health check at a specified time. It helps monitor the network security status, identify potential security issues early, and take preventive measures.</p>

	<p>Customers can determine when to run security health checks according to their business situation, security requirements, and security risks of the enterprise.</p> <p><b>Scheduled check:</b> Execute health checks at regular intervals. This allows you to comprehensively assess the network security status, screen potential security risks, and take corresponding measures. Customers can determine the interval to execute the check according to their security standards.</p>
Included assets	Select assets to check as needed.
Check items	Based on port scanning, retrieve the information of open ports and services on the target system, and infer possible vulnerabilities, weak passwords, and exposed risk services. For example, if the target server has port 80 open (HTTP service), there may be a risk of web application vulnerabilities.

## Editing tasks

1. Log in to the [Cloud Security Center console](#), and click **Health check tasks** in the left sidebar.
2. On the **Health check tasks** page, select the target task, and click **Edit**.

### Note:

You cannot edit immediate tasks, pending non-periodic tasks, and ongoing periodic tasks and scheduled tasks.

<input type="checkbox"/>	Task ID/name	Plan	Included...	Check items	Start time	Estimated dura...	Task status	Reports	Mode
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]
<input type="checkbox"/>	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]	[blurred]

3. In the pop-up window, make modification and click **OK**.

### Edit task ⓘ

⌵ ✕

Task name ⓘ

Mode  Basic  Standard  Advanced ⌵

Plan ⓘ  Immediate  Specified time  Scheduled checks

⌵  🕒

Included assets  All assets  Select from existing  Manual input

Import

[Select assets](#)  All assets (  )

Check items ⓘ

<input checked="" type="checkbox"/> Port risks <span>ⓘ</span>	<input checked="" type="checkbox"/> Vulnerabilities <span>ⓘ</span>
<input checked="" type="checkbox"/> Weak passwords <span>ⓘ</span>	<input type="checkbox"/> Content risks <span>ⓘ</span>
<input checked="" type="checkbox"/> Configuration risks <span>ⓘ</span>	<input checked="" type="checkbox"/> Exposed risk services <span>ⓘ</span>

Estimated duration  minutes

Quota usage ⓘ

---

Agree to Health Check Authorization Agreement. [View details](#)

I hereby acknowledge that the assets to check are owned by current enterprise account. The account owner shall bear the legal responsibility for unauthorized usage of the assets.

## Deleting tasks

1. Log in to the [Cloud Security Center console](#), and click **Health check tasks** in the left sidebar.
2. On the **Health check tasks** page, select the target task, and click **Delete**.

<input type="checkbox"/>	Task ID/name	Plan	Included...	Check items	Start time	Estimated dura...	Task status	Reports	Mode
<input type="checkbox"/>									
<input type="checkbox"/>									

3. In the pop-up window, click **OK**.

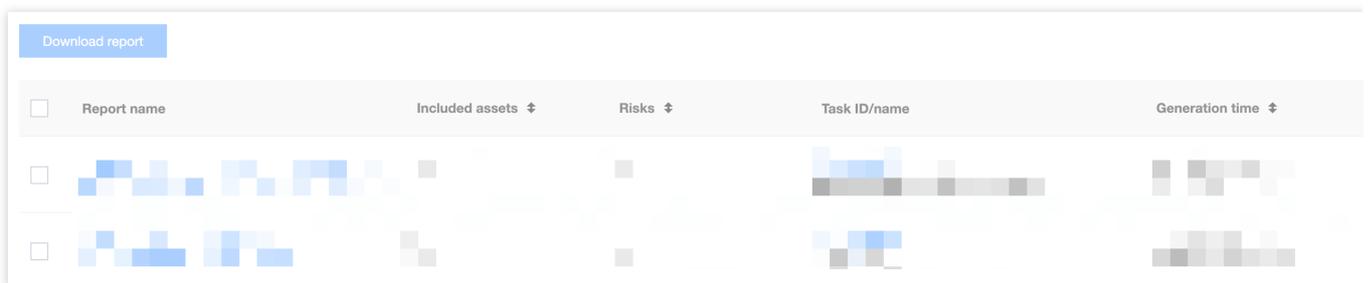
**Note:**

Tasks cannot be recovered after being deleted. But the reports generated before are retained.  
Ongoing tasks cannot be deleted.

## Downloading reports

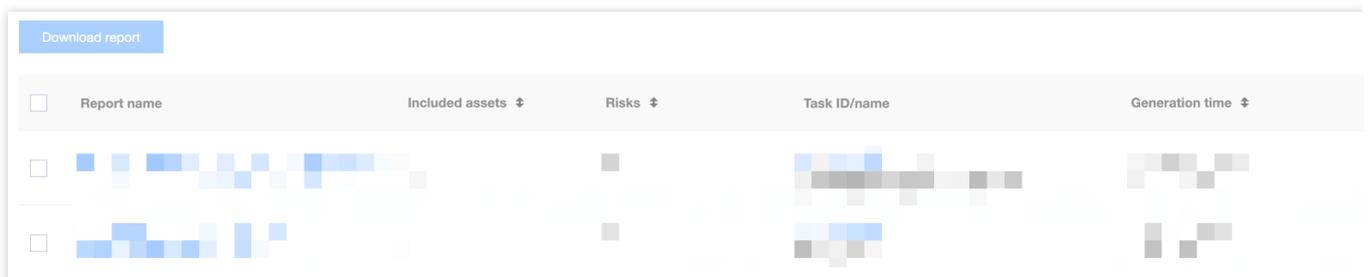
Automatically generate PDF reports after health check tasks are completed. You can preview and download the reports.

1. Log in to the [Cloud Security Center console](#) and click **Reports** in the left sidebar.
2. On the report download page, select the target report, and click **Preview** under **Operation**.

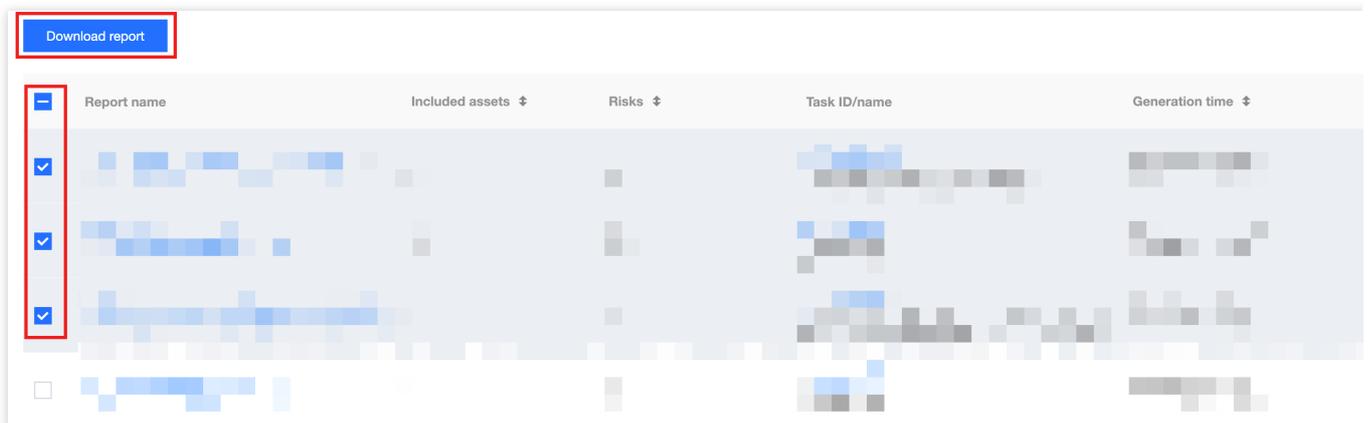


3. You can download one or more reports as needed.

Single report: Select the target report, and click **Download** under **Operation**.



Multiple reports: Select multiple reports and click **Download report** in the top-left corner.



## Multi-account management

Each health check consumes both the health check quota and task quota. In Multi-account mode, the administrator or a delegated administrator can initiate health check tasks under a member account of the organization. In this case, the administrator can specify the consumer account of the health check quota, and the task quota is always consumed by the assigned task owner.

### Editing tasks

Administrators, deligated administrators and members can edit tasks created by their own. Administrators can also edit tasks created by deligated administrators.

### Deleting tasks

All tasks can be deleted by their creators. Administrators and delegated administrators can delete tasks created by the other role. Members can delete tasks created by administrators and delegated administrators under their accounts.

# Adding IPs to an Allowlist

Last updated : 2024-08-02 10:14:18

This document will provide you with a detailed guide on how to add Tencent CSC's monitoring IP to the allowlist.

## Overview

CSC uses simulated hacker intrusion attacks during asset discovery and risk monitoring through the public network. If your server is equipped with security protection or monitoring deployment (such as WAF), it is recommended to add Tencent Cloud CSC's monitoring IP to the allowlist, enabling scan access permissions to ensure the normal running of the monitoring service. The IPs of the CSC scanning node are:

129.211.162.110

129.211.162.87

129.211.163.253

129.211.164.19

129.211.166.123

129.211.167.182

129.211.167.200

129.211.167.70

129.211.162.158

129.211.162.23

129.211.166.134

129.211.167.108

129.211.167.181

129.211.166.142

129.211.166.163

129.211.167.128

129.211.167.166

43.139.244.231

43.139.243.246

If your website requires log-in access, you should first disable the security policy to allow all IPs to access it. Once your cookie's validity has been verified, you can restore the IP limits.

## Directions

**Note**

Applicable to Tencent Cloud WAF. If you are using a different WAF product, add the necessary configurations accordingly.

WAF has been purchased.

You have added a protected domain name and connected it properly. The domain name is under proper protection, and the BOT management rules are enabled. For details, see [getting started](#).

**Method 1: Adding to the Allowlist through IP Query**

1. Log in to the [WAF console](#). In the left sidebar, click **IP Lookup**.
2. On the IP query page, select the domain name to be protected in the upper left corner, enter the IP to be queried, and click **Search**.

The screenshot displays the 'IP Query' interface. At the top left, there is a dropdown menu labeled 'IP Query'. Below it, there are two tabs: 'IP Query' (which is active and underlined) and 'Block Query'. A blue banner with an information icon contains the text: 'Query whether an IP is blocked or added to the blocklist/allowlist, and whether it triggers CC protection or cus'. At the bottom, there is a search input field and a blue 'Search' button.

3. In the query results, you can view the specific IP details. Click **Add to blocklist/allowlist** to manually add to the blocklist/allowlist.

**Search results**

IP	<input type="text"/> <b>Block</b>
Domain name	<input type="text"/>
Valid at	<input type="text"/>
End time	Permanent
Category	Blocklist
Triggered policy name	custom

[Add to blocklist/allowlist](#)

4. On the IP addition to blocklist/allowlist page, you can manually add to the allowlist. Configure the relevant parameters and click **Add** to complete adding to the allowlist.

**Add blocked/allowed IP** ×

Category  Blocklist  Allowlist

IP address

Deadline \*

Remarks

5. Parameter Description:

Category: Select **Allowlist**.

IP Address: Enter the address to be added to the allowlist.

Expire Time: Enter the expiration time for the allowlist.

Remarks: Custom description.

## Method 2: Adding IPs Directly to the Allowlist

Log in to the [WAF console](#). In the left sidebar, click **Configuration Center** > **Blocklist** to choose the domain to be protected in the upper left corner, and click **IP Allowlist** to enter the IP allowlist page.

### Manually Adding to the Allowlist

1. On the IP allowlist page, click **Add address** to enter the add to allowlist page.

The screenshot shows the 'Blocklist/Allowlist' management page. At the top, there is a dropdown menu for selecting a domain. Below it, there are four tabs: 'IP blocklist', 'IP allowlist' (which is selected), 'Custom allow rules', and 'Preset rule exceptions'. The main area contains a toolbar with buttons for 'Add address', 'Delete address', 'Delete all', 'Import data', and 'Export all'. A filter input field is also present. Below the toolbar, a message states: 'A maximum of 20000 IP addresses can be added to a single domain., 19999 remaining'. The main content is a table with the following columns: Rule ID, IP address, Source, Validity, Update time, Status, Remarks, and Creation Time. One row is visible, showing a 'Custom' source, 'Valid' status, and an expiration time of '2024-07-23 11:50:16'. At the bottom, it indicates 'of 1 items selected' and a pagination control set to '50 / page'.

Rule ID	IP address	Source	Validity	Update time	Status	Remarks	Creation Time
		Custom	Valid Expire Time:2024-07-23 11:50:16	2024-07-23 11:33:29	Valid	None	2024-07-23 11:3

2. On the addition to allowlist page, configure the relevant parameters, and click **OK**.

## Add to allowlist

IP address \*

Up to 20 arbitrary IP addresses (such as 10.0.0.10 or FF05::B5) or CIDR addresses (such as 10.0.0.0/16 or FF05:B5::/60). Add one per line

Validity \*

Permanent  Expiration time

Expiration time \*

2024-07-30 11:35:57



Remarks

Up to 50 characters

### Field Description

**IP Address:** Supports any IP address, such as 10.0.0.10 or FF05::B5. Supports CIDR format addresses, such as 10.0.0.0/16 or FF05:B5::/60. Use line breaks for separation, up to 20 entries at a time.

### Note

When you select the domain name as ALL, the added IP addresses or ranges will be added to the global allowlist. The domain name quotas in each edition are as follows: Premium Edition: 1,000 entries/domain name; Enterprise Edition: 5,000 entries/domain name; Ultimate Edition: 20,000 entries/domain. Each IP address or range occupies one entry in the quota.

**Validity:** effective permanently or within the limited time.

**Remarks:** Custom; within 50 characters.

### Batch Importing to the Allowlist

1. On the IP allowlist page, click **Import data**, and the Import IP List window will pop up.
2. In the Import IP List window, click **Import**. Select the allowlist file to import, and after the upload is complete, click **OK**.

## Import IP list

Import

Click to select a file.

### Description:

1. Only .xlsx and .xls files are supported. You can only upload one file at a time.
2. Quantity, up to  rules can be imported at a time. If you need to import a large number of rules, please import them in batches.
3. It must include three columns: category, IP address and end time. For more details, see the exported excel data.
4. The end time must be in the format of YYYY/MM/DD HH:MM:SS, and earlier than 2033/12/31 00:00:00.
5. The content format must be the same as the exported file. For more details, see [IP blocklist](#) and [allowlist](#)

OK

Reset

### Method 3: Adding the Blocked IP to the Allowlist

1. Log in to the [WAF console](#). In the left sidebar, choose **IP Inquiry** > **Block Query**.
  2. On the query blocking page, enter the relevant information, and click **Search** to query the relevant IPs of the CSC.
- This allows you to perform the allowlist operation for the already blocked IPs.

IP Query

IP Query **Block Query**

 You can view IPs being blocked here, or real-time IP blocking records related to CC, bot, and custom CAPTCHA blocking policies

\*Type  Trigger policy  IP address

Creation time     

Validity:  

**Search**

# FAQs

Last updated : 2023-08-29 15:59:14

## How do I choose a health check quota?

To mitigate asset security risks, it is recommended to conduct four automatic checks and one comprehensive manual check each month. Please calculate the number of asset health checks to purchase based on the quantity of your cloud assets.

## Formula for calculating consumed health check quota

In a single security check, selecting one domain and one IP asset each consumes one health check quota, totaling two health check quotas. If you select a cloud resource configuration risk health check project, the consumed health check quota is the number of selected cloud resources.

## Is it abnormal if the health check duration is too long?

If a security health check task involves inspecting a web site, it requires content recognition analysis of your specified URL using crawling technology authorized by you. Moreover, conducting the health check too quickly can easily impact the business, hence a slower health check duration is normal.

## Will a report still be generated after a health check task is terminated?

If a security health check task is terminated, no report will be generated. However, detected risks will still exist in the Risk Center and can be queried based on the report ID.

## Does an abnormal health check task consume health checks and occupy task quotas?

If a security health check task cannot be executed, it occupies the task quota but does not consume the health check quota. If a security health check task begins execution, it immediately consumes the health check quota and occupies the task quota.

## In addition to hosts and containers, what other cloud resources are included in the configuration risk detection?

Check Item Name	Check type	Check target	Risk level	Associated standard	Configuration risk notes
TDSQL for MySQL should not be open to public network access.	Data Security	tdmysql	Medium	Default security standards	Direct exposure of the database to the public network may lead to the leakage of sensitive data in the database, posing a high security risk. This check

					<p>item will inspect TDSQL MySQL Edition, and if public network access is enabled, it does not meet the requirements.</p>
<p>Network ACL should not have all inbound rules allowed.</p>	<p>Network access control</p>	<p>subnet</p>	<p>High</p>	<p>Default security standards</p>	<p>A Network ACL is a subnet-level access control attack. If you use a rule that allows all inbound traffic, i.e., the source in the inbound direction is 0.0.0.0/0 and the action is to allow, it may cause the subnet to be overly exposed, leading to unnecessary exposure of assets. This check item will inspect the inbound rules of the Network ACL service. If there is a rule where the source address is 0.0.0.0/0, all ports are allowed, and the action is to allow, then it does not meet the requirements.</p>
<p>It is not recommended for Network ACL to have inbound rules that allow all non-business ports.</p>	<p>Network access control</p>	<p>subnet</p>	<p>High</p>	<p>Default security standards</p>	<p>A Network ACL is an access control attack at the subnet level. If you use inbound rules that allow all non-business (default: 80,443) traffic, i.e., inbound rules where the source is 0.0.0.0/0, the port is any port other than 80/443, and the action is 'allow', this could potentially lead to an overly broad opening of the subnet, unnecessarily exposing assets. This check will examine the inbound rules of the Network ACL service. There should not be any rules where the source address is 0.0.0.0/0, the port is 'all' or a non-business</p>

					port (default: 80,443), and the action is 'allow'.
The SSL certificate should be within its validity period.	Data Security	ssl	Medium	Default security standards	Check whether the SSL certificate has exceeded its validity period. You need to renew or replace the certificate in a timely manner before it expires. Otherwise, you will not be able to continue using the SSL certificate service, leading to data security risks. The current check scope is all SSL certificates. You need to determine whether to repair or delete unused certificates based on whether the certificate is associated with resources and whether the domain name is still in use.
The permissions for the image repository should be set appropriately.	Data Security	repository	Medium	Default security specifications, technical requirements for level three cybersecurity protection	Repositories are divided into public repositories and private repositories. Public repositories allow all users on the Internet to access and download images. If the image contains sensitive information, it is recommended to configure it as a private repository to prevent information leakage.
High-risk commands should be disabled in TencentDB for Redis.	Data Security	redis	Medium	Default security standards	Databases often have high levels of security protection. If high-risk commands are not disabled (default: flushall, flushdb, keys, hgetall, eval, evalsha, script), it can easily lead to application blocking and data deletion risks. This check will examine the

					Redis instance's command disablement configuration. If high-risk commands are not disabled (default includes: flushall, flushdb, keys, hgetall, eval, evalsha, script), it does not meet the requirements.
The NoSQL database - Redis should enable automatic backup.	Data Security	redis	Medium	Default security specifications, technical requirements for level three cybersecurity protection	To determine if the backup function of the Redis database is abnormal, under normal circumstances, data should be backed up at least once a day.
The NoSQL database - Redis should not be open to all network segments.	Network access control	redis	High	Default security specifications, technical requirements for level three cybersecurity protection	Determining whether the service port of the Redis database is open to all IPs. Under normal circumstances, the database service port should only be open to trusted IPs or ranges.
NoSQL-Redis should be located in the Mainland China region.	Infrastructure Location	redis	Low risk	Technical requirements for Level 3 Cybersecurity Protection	Requirement 8.2.1.1 in GB 22239-2008 stipulates that the cloud computing infrastructure should be located within the Chinese mainland.
It is not recommended to allow public network access to TencentDB for PostgreSQL.	Network access control	postgres	High	Default security standards	Direct exposure of a database to the public network may lead to the leakage of sensitive data within the database, posing a high security risk.
Relational Database - PostgreSQL	Data Security	postgres	Medium	Default security specifications, technical	To determine whether the backup function of the PostgreSQL database is abnormal, under normal

should enable backup.				requirements for level three cybersecurity protection	circumstances, data should be backed up at least once a day.
The relational database - TencentDB for PostgreSQL should be located in the mainland China region.	Infrastructure Location	postgres	Low risk	Technical requirements for Level 3 Cybersecurity Protection	Requirement 8.2.1.1 in GB 22239-2008 stipulates that the cloud computing infrastructure should be located within the Chinese mainland.
NoSQL- MongoDB should be located in the mainland China region.	Infrastructure Location	mongodb	Low risk	Technical requirements for Level 3 Cybersecurity Protection	Requirement 8.2.1.1 in GB 22239-2008 stipulates that the cloud computing infrastructure should be located within the Chinese mainland.
TencentDB for MariaDB should restrict the use of high-risk commands.	Data Security	mariadb	Medium	Default security standards	Databases often have a high level of security protection. If all accounts have global command permissions such as drop and delete, there is a risk of accidental data deletion or malicious deletion. This check will inspect MariaDB. If all users have not prohibited the drop and delete commands, it does not meet the requirements.
It is not recommended to allow public network access to TencentDB for MariaDB.	Network access control	mariadb	High	Default security standards	Direct exposure of a database to the public network may lead to the leakage of sensitive data within the database, posing a high security risk.
TencentDB for MariaDB should not enable access	Network access control	mariadb	High	Default security standards	If a cloud database is configured to allow access from all network segments, it enlarges the attack

for all network segments.					surface of the database, thereby increasing the risk of attacks and data breaches.
Relational Database - MariaDB should enable backup	Data Security	mariadb	Medium	Default security specifications, technical requirements for level three cybersecurity protection	To determine whether the backup function of the MariaDB database is abnormal, under normal circumstances, data should be backed up at least once a day.
The relational database - TencentDB for MariaDB should be located in the mainland China region.	Infrastructure Location	mariadb	Low risk	Technical requirements for Level 3 Cybersecurity Protection	Requirement 8.2.1.1 in GB 22239-2008 stipulates that the cloud computing infrastructure should be located within the Chinese mainland.
Elasticsearch clusters should not be open to public network access.	Data Security	es	High	Default security standards	Elasticsearch clusters often store data. If public network access is enabled, it may expose unnecessary attack surfaces, leading to risks to data integrity, confidentiality, and availability.
The Kibana component of the Elasticsearch cluster should not be open to public network access.	Data Security	es	High	Default security standards	Elasticsearch clusters often store data and can be accessed and controlled via the Kibana component. If public network access is enabled, it may expose unnecessary attack surfaces, leading to risks to data integrity, confidentiality, and availability.
The security group should	Network access	cvm	High	Default security	A security group is a type of virtual firewall. It is

not open any port to all network segments.	control			specifications, technical requirements for level three cybersecurity protection	recommended to configure firewall policies based on the principle of minimal granularity and add trusted IP allowlists for server port access.
The CVM should be located in the Chinese mainland region.	Infrastructure Location	cvm	Medium	Technical requirements for Level 3 Cybersecurity Protection	Requirement 8.2.1.1 in GB 22239-2008 stipulates that the cloud computing infrastructure should be located within the Chinese mainland.
CVM should use key pair login	Identity Verification and Permissions	cvm	Medium	Default security standards	Check whether the CVM is logged in using an SSH key. Compared to traditional password login, SSH key login is more convenient and secure. (Only checks for Linux system machines)
The host security agent on the CVM should operate normally.	Basic Security Protection	cvm	High	Default security specifications, technical requirements for level three cybersecurity protection	Tencent Cloud Workload Protection Platform provides a variety of security features including trojan detection and removal, brute force attack prevention, login behavior auditing, vulnerability management, and asset component identification. Without the installation of the CWPP client, there is a risk of network security breaches and data leakage.
It is recommended to enable bucket replication for the COS bucket.	Data Security	cos	Medium	Default security specifications, technical requirements for level three cybersecurity protection	Cross-region replication is a configuration for storage buckets. By setting up cross-region replication rules, incremental objects can be automatically and asynchronously replicated between storage buckets in different regions. Once

					cross-region replication is enabled, COS will precisely replicate the object content in the source bucket (such as object metadata and version ID) to the target bucket, and the replicated object copies will have completely consistent attribute information. In addition, operations on objects in the source bucket, such as adding or deleting objects, will also be replicated to the target bucket. It is recommended to perform cross-region replication to enhance your data disaster recovery capabilities.
A reasonable bucket policy should be configured for the COS bucket.	Data Security	cos	High	Default security specifications, technical requirements for level three cybersecurity protection	A bucket policy refers to the access policy configured within a bucket, allowing specified users to perform designated operations on the bucket and its resources. It should be configured according to the principle of "minimal permissions". It is not recommended to grant read access to any user, as this poses a risk of file names being traversed or files being downloaded.
The COS bucket should be located in the China Mainland region.	Infrastructure Location	cos	Low risk	Technical requirements for Level 3 Cybersecurity Protection	Requirement 8.2.1.1 in GB 22239-2008 stipulates that the cloud computing infrastructure should be located within the Chinese mainland.
The COS bucket should	Data Security	cos	Medium	Default security	To prevent malicious programs from using

enable the anti-leech feature.				specifications, technical requirements for level three cybersecurity protection	resource URLs to steal public network traffic or employing malicious methods to misappropriate resources, causing unnecessary losses, it is recommended that you configure a blocklist/allowlist through the console's hotlink protection settings to provide security protection for storage objects.
The COS bucket should enable server-side encryption.	Data Security	cos	Medium	Default security specifications, technical requirements for level three cybersecurity protection	Buckets support the application of data encryption protection policies at the object level and automatically decrypt data upon access. Both the encryption and decryption processes are completed on the server side. This server-side encryption feature can effectively protect static data. It is recommended to enable this configuration for sensitive data types.
The COS bucket should have log recording enabled.	Data Security	cos	Medium	Default security specifications, technical requirements for level three cybersecurity protection	The log management feature can record detailed access information for a specified source bucket and save this information in the form of log files in a designated bucket, facilitating better bucket management. The log management feature requires that the source bucket and the target bucket be in the same region, currently supported in Beijing, Shanghai, Guangzhou, Chengdu, and Toronto. If your region supports the log

					management feature, it is recommended to enable this function.
The ACL public permission for the COS bucket should not be set to public read and write.	Data Security	cos	High	Default security specifications, technical requirements for level three cybersecurity protection	The public read and write permissions of a bucket allow data in the bucket to be directly read and written by anonymous identities, posing certain security risks. To ensure the safety of your data, it is not recommended to set the bucket permissions to public read/write or public read/private write. Instead, it is advisable to choose private read/write permissions.
The certificate bound to the CLB should be within its validity period.	Monitoring and Alarms	clb	Medium	Default security standards	Check whether the certificate bound with the CLB has expired. If it has, it needs to be replaced to avoid affecting normal business operations.
The health check status of the CLB backend server group should remain normal.	Monitoring and Alarms	clb	Low risk	Default security standards	The health status of the Tencent Cloud Load Balancer (CLB) service is checked to determine whether there are any anomalies with the backend services of the CLB.
CLB should not forward high-risk ports	Network access control	clb	High	Default security specifications, technical requirements for level three cybersecurity protection	The CLB forwarding strategy should be set based on the "minimum service" principle, forwarding only necessary public service ports (such as 80, 443, etc.), and other ports should not be forwarded.
CLB should not	Network	clb	High	Default	Inspect the access control

enable non-business port access for all network segments.	access control			security specifications, technical requirements for level three cybersecurity protection	configuration of the CLB load balancing instance. There is a potential security risk in opening 0.0.0.0/0 to non-business ports. It is recommended to enable access control for non-http/https services.
TencentDB for MySQL should enable database auditing.	Data Security	cdb	Medium	Default security standards	Databases often store data of high importance. If database auditing is not enabled, it would be difficult to trace back in case of issues such as misoperations or malicious operations. This check item will verify whether database auditing is enabled for the MySQL database. If it is not, it does not meet the requirements.
The network type for TencentDB for MySQL should utilize a private network.	Data Security	cdb	Medium	Default security standards	A VPC can isolate different networks based on tenant requirements. Databases often store data of high importance. If a non-private network is used, precise access control rules need to be maintained. Any oversight or error in maintenance could potentially expose your database unnecessarily. This check item will inspect the MySQL database type. If it is a private network, it meets the requirements; otherwise, it does not.
A password should be set for the admin account in	Network access control	cdb	High	Default security standards	TencentDB for MySQL is a database service. If you have not configured the administrator account and password for the database,

TencentDB for MySQL.					it may be maliciously logged in, leading to data leakage.
A non-root user should be created for use with TencentDB for MySQL.	Data Security	cdb	Medium	Default security standards	Databases often store data of high importance. If a database only has a root account and no other application accounts, it indicates excessive permissions, posing a risk of data security being affected by erroneous or malicious operations. This check item will inspect the user list of the primary instance database of MySQL that has been initialized. If there are no other users besides the root user and the default mysql.* created by Tencent Cloud, it does not meet the requirements.
TencentDB for MySQL database instances should be deployed in different availability zones.	Data Security	cdb	Low risk	Default security standards	TencentDB for MySQL offers various high-availability architectures. Selecting different primary and secondary availability zones (i.e., multi-AZ deployment) can protect the database from failures or AZ interruptions. This check item will inspect the MySQL database. If the primary and secondary instances of the same database are in the same region and availability zone, it does not meet the requirements.
The retention period for TencentDB for MySQL database audit	Data Security	cdb	Medium	Default security standards	Databases often store data of high importance. Based on compliance requirements, database audit logs should be

<p>should meet the requirements.</p>					<p>retained for at least six months or more. This check will examine the retention time of MySQL database audits. If the retention time is less than the audit time (default 180 days), it does not meet the requirements.</p>
<p>It is recommended to limit the high-risk command permissions of non-root users in TencentDB for MySQL.</p>	<p>Data Security</p>	<p>cdb</p>	<p>Medium</p>	<p>Default security standards</p>	<p>Non-root database accounts should be subject to permission control. If application accounts have high-risk command permissions, such as drop and delete, there is a risk of accidental or malicious data deletion. This check item will inspect the MySQL database (checking the master instance, not checking read-only instances and disaster recovery instances), and the configuration of users other than the root user. If the configuration allows the execution of commands: drop, delete, then it is not satisfactory. For instances where non-root users do not exist, this check item is satisfactory and other check items are used for compliance checks.</p>
<p>It is not recommended to open TencentDB for MySQL for public network access.</p>	<p>Network access control</p>	<p>cdb</p>	<p>High</p>	<p>Default security standards</p>	<p>TencentDB for MySQL is a database service. If the database is directly exposed to the public network, it may lead to the leakage of sensitive data in the database, posing a high security risk.</p>
<p>Relational</p>	<p>Data</p>	<p>cdb</p>	<p>Medium</p>	<p>Default</p>	<p>To determine whether the</p>

Database - MySQL should enable backup.	Security			security specifications, technical requirements for level three cybersecurity protection	backup function of the MySQL database is abnormal, under normal circumstances, data should be backed up at least once a day.
The relational database - MySQL database should be located in the mainland China region.	Infrastructure Location	cdb	Low risk	Technical requirements for Level 3 Cybersecurity Protection	Requirement 8.2.1.1 in GB 22239-2008 stipulates that the cloud computing infrastructure should be located within the Chinese mainland.
The relational database - MySQL should not be open to all IP ranges.	Network access control	cdb	Medium	Default security specifications, technical requirements for level three cybersecurity protection	Determining whether the service port of the MySQL database is open to all IP addresses. Under normal circumstances, the database service port should only be open to trusted IPs or ranges.
The CBS data disk should be set as an encrypted disk.	Data Security	cbs	Medium	Default security specifications, technical requirements for level three cybersecurity protection	Check whether the data disk of the cloud disk is an encrypted disk. Encrypted disks can not only provide better data confidentiality, but also meet security compliance requirements. (Only non-system disks can be checked)
CBS should enable the scheduled snapshot feature.	Data Security	cbs	Medium	Default security specifications, technical requirements for level three cybersecurity protection	Verify if the automatic scheduled snapshot feature is enabled for the cloud disk. Regular snapshot creation can enhance data security, achieving low-cost and high-disaster tolerance for your business.
Sub-accounts	Basic	cam	Medium	Default	If a sub-account has not

should use MFA for login protection	Security Protection			security standards	bound an MFA device, it cannot use MFA for secondary verification in login protection or operation protection, which poses a risk. This check item will verify whether the sub-account has bound an MFA device. If not, it does not meet the requirements.
Sub-accounts should use MFA for operation protection.	Basic Security Protection	cam	Medium	Default security standards	If a sub-account has not bound an MFA device, it cannot use MFA for secondary verification in login protection or operation protection, which poses a risk. This check item will verify whether the sub-account has bound an MFA device. If not, it does not meet the requirements.
Sub-account passwords should be changed regularly.	Basic Security Protection	cam	Medium	Default security standards	The sub-account password is the primary credential for user access. Not changing the password for a long period (90 days) can increase the risk of password leakage. The account information involved in this check may be subject to synchronization delays, so it is recommended to have an interval of more than 4 hours between checks.
Obsolete sub-accounts should be deleted.	Basic Security Protection	cam	High	Default security standards	If a sub-account is not logged in for a long period (30 days), it is possible that the account has been abandoned. Abandoned accounts may be used by individuals no longer affiliated with your

					organization, leading to unavailability of your assets or data leakage.
Obsolete API keys of sub-accounts should be deleted.	Basic Security Protection	cam	High	Default security standards	If a sub-account API key has not been used for a long period (30 days), it is possible that the API key has been abandoned. Abandoned API keys may be used by members no longer belonging to your organization, leading to unavailability of your assets or data leakage. The account information involved in this check may be subject to synchronization delays, so it is recommended to have a check interval of more than 4 hours.
Obsolete collaborator API keys should be deleted.	Basic Security Protection	cam	High	Default security standards	If a collaborator's API key has not been used for a long period (30 days), it is possible that the API key has been abandoned. Abandoned API keys may be used by members no longer belonging to your organization, leading to unavailability of your assets or data leakage. The account information involved in this check may be subject to synchronization delays, so it is recommended to have a check interval of more than 4 hours.
The API keys of sub-accounts should be	Basic Security Protection	cam	Medium	Default security standards	The API key of a sub-account is the primary credential for programmatic access. Not changing the

regularly updated.					key for a long period (90 days) can increase the risk of key exposure. The account information involved in this check may be subject to synchronization delays, so it is recommended to have a check interval of more than 4 hours.
The API key of the collaborator should be regularly updated.	Basic Security Protection	cam	Medium	Default security standards	The collaborator's API key is a primary credential for programmatic access. Not changing the key for a long period (90 days) can increase the risk of key leakage. The account information involved in this check may be subject to synchronization delays, so it is recommended to have a check interval of more than 4 hours.
Collaborators should use MFA for login protection.	Basic Security Protection	cam	Medium	Default security standards	If a collaborator has not bound an MFA device, they cannot use MFA for secondary verification in login protection or operation protection, which poses a risk. This check item will verify whether the collaborator has bound an MFA device. If not, they do not meet the requirements.
Collaborators should use MFA for operation protection.	Basic Security Protection	cam	Medium	Default security standards	If a collaborator has not bound an MFA device, they cannot use MFA for secondary verification in login protection or operation protection, which poses a risk. This check item will verify whether the collaborator has bound an

					MFA device. If not, they do not meet the requirements.
Collaborators should activate login protection.	Basic Security Protection	cam	Medium	Default security standards	Collaborator accounts do not belong to your account management system and pose uncontrollable security risks. If a collaborator account is compromised, it may lead to the destruction of assets that the collaborator has access to or data leakage. By enabling login protection and implementing multi-factor authentication for collaborator logins, the risk of damage caused by collaborator account leakage can be reduced.
Collaborators should enable operation protection	Basic Security Protection	cam	Medium	Default security standards	Collaborator accounts do not belong to your account management system and their security risks are uncontrollable. If a collaborator account is compromised, it may lead to the destruction of assets that the collaborator has permission to access or data leakage. By enabling operation protection, sensitive operations by collaborators are subject to secondary verification, reducing the risks associated with collaborator account leakage.
Collaborators should not use programming access and user interface	Basic Security Protection	cam	High	Default security standards	If both access methods are enabled for a collaborator account, it may increase the exposure of a single account and potentially lead to the mixed use of

<p>access simultaneously.</p>					<p>automated and manual accounts, increasing the likelihood of malicious use. The account information involved in this check may be subject to synchronization delays, so it is recommended to have an interval of more than four hours between checks.</p>
<p>Collaborators with high-risk permissions should enable login protection.</p>	<p>Basic Security Protection</p>	<p>cam</p>	<p>High</p>	<p>Default security standards</p>	<p>Collaborator accounts do not belong to your account management system and their security risks are uncontrollable. High-permission collaborators have super admin privileges. If a collaborator account is compromised, your cloud assets will face significant security risks. By enabling login protection and implementing secondary verification for collaborator logins, the risk of collaborator account leakage can be reduced.</p>
<p>Operation protection should be enabled for collaborators with high-risk permissions.</p>	<p>Basic Security Protection</p>	<p>cam</p>	<p>High</p>	<p>Default security standards</p>	<p>A collaborator account does not belong to your account management system, and its security risks are uncontrollable. High-permission collaborators have super administrator permissions. If a collaborator account is leaked, your cloud assets will face very high security risks. By enabling operation protection, sensitive operations of collaborators are subject to secondary verification, reducing the</p>

					risks caused by the leakage of collaborator accounts.
It is recommended that a sub-account has no more than one API key.	Basic Security Protection	cam	Low risk	Default security standards	Maintaining multiple API keys for a single sub-account can increase the exposure of the keys and the risk of key leakage. The account information involved in this check may be subject to synchronization delays, so it is recommended to have an interval of more than 4 hours between checks.
Login protection should be enabled for sub-accounts with high-risk permissions.	Basic Security Protection	cam	High	Default security standards	High-privilege sub-accounts possess super administrator permissions. If such high-risk sub-accounts are maliciously logged in, your cloud assets could face significant risks. Login protection provides a second verification for your sub-account logins, reducing the likelihood of high-risk sub-accounts being maliciously logged in.
Operation protection should be enabled for sub-accounts with high-risk permissions.	Basic Security Protection	cam	Medium	Default security standards	A high-privilege sub-account has the authority of a super administrator. If the main account is misused or maliciously operated after being stolen, it may affect all your cloud assets. Operation protection provides a second verification for your sensitive operations, reducing the risk of misuse or malicious operations.
It is not recommended	Basic Security	cam	Low risk	Default security	A high-privilege sub-account has the authority of

<p>to enable API keys for sub-accounts with high-risk permissions.</p>	<p>Protection</p>			<p>standards</p>	<p>a super administrator, and the API key is the identity credential for account programming access. It is often written into the configuration and is prone to leakage. If the API key is leaked, an attacker can use this key to control all your assets in the cloud, posing a high risk. The account information involved in this check may be subject to synchronization delays, so it is recommended to have a check interval of more than four hours.</p>
<p>You cannot simultaneously enable programming access and user interface access for a sub-account.</p>	<p>Basic Security Protection</p>	<p>cam</p>	<p>Medium</p>	<p>Default security standards</p>	<p>Sub-accounts have two access methods. If both are enabled, it may increase the exposure of a single account and potentially lead to the mixed use of automated and manual accounts, increasing the likelihood of malicious account usage. The account information involved in this check may be subject to synchronization delays, so it is recommended to have an interval of more than 4 hours between checks.</p>
<p>The root account should use MFA for login protection.</p>	<p>Basic Security Protection</p>	<p>account</p>	<p>Medium</p>	<p>Default security standards</p>	<p>The primary account inherently possesses all Tencent Cloud resources under the account and has super administrator privileges. If the primary account is compromised, your cloud assets could face significant security risks. Multi-factor authentication (MFA) is a simple and</p>

					<p>effective security authentication method that adds an additional layer of protection beyond the username and password. Login protection can utilize Tencent Cloud's virtual MFA device, reducing the likelihood of malicious logins to the primary account.</p>
<p>The root account should use MFA for operation protection.</p>	<p>Basic Security Protection</p>	<p>account</p>	<p>Medium</p>	<p>Default security standards</p>	<p>The root account by default possesses all Tencent Cloud resources under the account and has super administrator privileges. Misoperation or malicious operation by the root account due to theft may affect all your cloud assets. Multi-factor authentication (MFA) is a simple and effective security authentication method that adds an extra layer of protection beyond the username and password. Enabling virtual MFA in operation protection can provide a second verification for your sensitive operations, reducing the risk of misoperation or malicious operation.</p>
<p>The primary account should activate login protection.</p>	<p>Basic Security Protection</p>	<p>account</p>	<p>High</p>	<p>Default security standards</p>	<p>The root account by default has access to all Tencent Cloud resources under the account and has super administrator permissions. If the root account is compromised, your cloud assets face a high security risk. Login protection provides a second verification for your account</p>

					login, reducing the likelihood of malicious logins to the root account.
The master account should enable operation protection.	Basic Security Protection	account	Medium	Default security standards	The root account by default owns all Tencent Cloud resources under the account and has super administrator privileges. Any misoperation or malicious operation due to the root account being compromised could potentially affect all your cloud assets. Operation protection provides a second verification for your sensitive operations, reducing the risk of misoperation or malicious activities.
It is recommended that the main account enables protection against logins from different locations.	Basic Security Protection	account	Low risk	Default security standards	The root account by default possesses all Tencent Cloud resources under the account and has super administrator permissions. If the root account is compromised, your cloud assets face a very high security risk. Remote login protection provides location verification for your account login. If a remote login is detected, a second verification will be conducted to reduce the likelihood of malicious login to the root account.
The root account should not enable API keys.	Basic Security Protection	account	High	Default security standards	The root account by default has access to all Tencent Cloud resources under the account and has super administrator permissions. The API key is the identity credential for programmatic

					<p>access to the account and is often written into the configuration, making it prone to leakage. If the API key is leaked, an attacker can manipulate all your assets in the cloud using this key, posing a high risk. The account information involved in this check may be subject to synchronization delays, so it is recommended to have a check interval of more than 4 hours.</p>
--	--	--	--	--	--

# User Behavior Analytics (UEBA)

Last updated : 2024-08-02 10:14:18

The User Behavior Analytics (UEBA) feature provides visualized auditing and monitoring of cloud user operation behaviors and TencentCloud API calls. It can detect and alarm on risky behaviors such as exceptional invocation of AKSK, high-risk API invocation, high-risk user operations, unauthorized service usage, and privilege escalation. This identifies security risks caused by exceptional user behaviors and risk API calls.

## Features

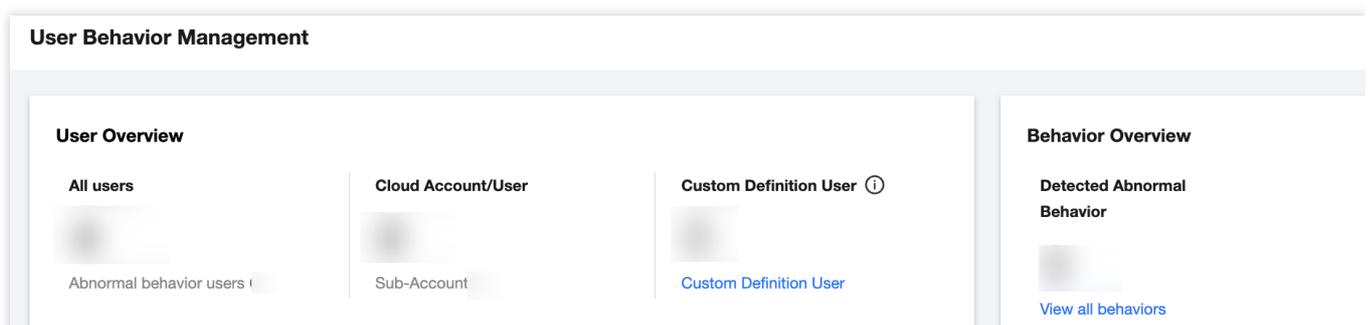
**Audit log connection:** Through the multi-cloud multi-account feature module, you can obtain user lists corresponding to cloud accounts and external user information. By using CloudAudit logs, you can retrieve all cloud user behavior records, and identify user behavior fields. Additionally, it enables visual monitoring and real-time auditing of cloud user operations and TencentCloud API call logs.

**Risk detection:** Detects and alarms on risky behaviors such as AKSK exceptional invocation, high-risk API invocation, high-risk user operations, unauthorized service usage, and privilege escalation. It also supports user-defined enabling or disabling of detection rules, and custom addition of detection policies.

**Security visualization:** Displays risk data detected in the past 7 days from aspects such as exceptional behaviors and exceptional accounts. Customers can quickly understand risk trends through data comparison and carry out timely risk management.

## User Overview

1. Log in to the [CSC console](#). In the left sidebar, click **User Behavior Analytics (UEBA)**.
2. On the UEBA page, it supports behavior analytics for all of your users, including your root account, sub-accounts, and collaborators.



3. Click **Custom Definition User**, you can identify user information in third-party logs by selecting a log type.

**Note:**

To proceed, this operation requires the [log configuration access](#).

4. In the custom definition user dialog box, configure parameters such as log type and user ID.

Parameter Name	Description
Log Type	After completing the <a href="#">log configuration access</a> , users can select the custom users for whom they want to add policies in this section, to audit the required log types. Log types include CFW access control logs, operation logs, traffic logs, intrusion prevention logs, zero trust protection logs, WAF attack logs, access logs, CWPP client-side reporting logs, CSC content risk logs, risk service exposure logs, weak password risk logs, configuration risk logs, vulnerability risk logs, SaaS BH asset log-in logs, product log-in logs, or other custom logs.
User ID	Select the field representing the user ID.
Username	Optional. Select the field representing the username.
Operation object	In the current log fields, select up to three fields to reflect the objects of user actions. It is recommended to select information such as service, product, resource, instance, and API. Fields can be left blank.
Operation Method	In the current log fields, select up to three fields to reflect the method of user actions. It is recommended to select information such as key and AKSK. Fields can be left blank. After configuration, user data in the custom user section will be refreshed based on the configuration information.

5. Click **OK**. After configuration, user data in the custom user section will be refreshed based on the configuration information.

## Behavior Overview

1. Log in to the [CSC console](#). In the left sidebar, click **\*\*User Behavior Analytics (UEBA)\*\***.
2. In the behavior overview module, before using the feature, you need to connect the logs. Click **Access Now**.

### Behavior Overview



**No behavior data, please integrate Cloud Au**

CSC has not yet integrated Cloud Audit Logs; user overview data cannot be provided. Please go to the [page](#) to complete Cloud Audit Log integration, or [/](#)

3. In the connected log source dialog box, you can select log source from operations or custom log source.

### Note:

If these two types of logs are already connected in log analysis, you can skip this configuration in the UEBA feature module and directly add policies.

### Connected Log Source

☰ ☒

Log source: Self-Definition Log Source ▾

Log source name:

Retention period: 7 days 30 days 60 days 90 days 180 days

Access method: Integrated through personal COS bucket ▾

COS Bucket:  ▾ ↻

Write the logs that need to be accessed into the selected COS bucket and configure permissions to allow the CSC service role to read. CSC will automatically read the log files periodically, and you can also choose a customized reading method

Storage Directory

Please select CFS directory Select a compre

To improve read performance, it is recommended to further organize the log file path in the selected directory according to the format **yyyy/mm/dd**. We will automatically read the files for the corresponding natural day based on the calendar; the log format supports JSON format, lines separated by '/n', and supports gzip compression

Log Sample

Please enter other field information of the target resolution file

Sample Parsing

We will perform field parsing based on the input sample. You can further review and choose specific fields and sorting options. This will enhance log reading performance and parsing accuracy

Timestamp

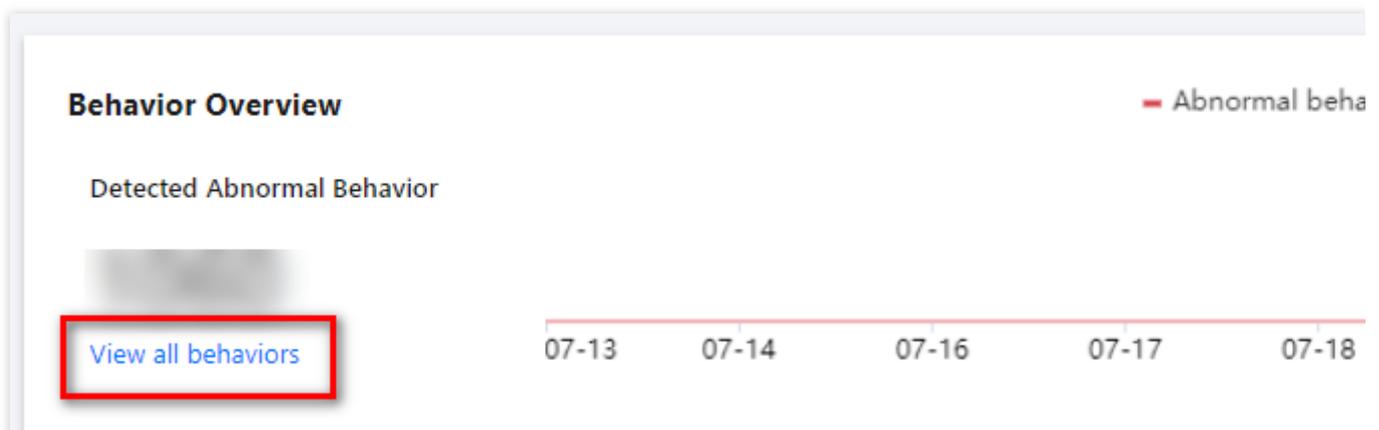
Please input the log s Please select the timestamp format

OK Cancel

Log Source	Parameter Name	Description
CloudAudit	Retention Period	The default is 180 days. You can select 7 days, 30 days, 60 days, 90 days, or 180 days.
	Connection Method	The default method is connected through tracking set.
	Tracking Set	Displays only the available tracking sets that are stored in COS. If disabled, go to the COS product first to enable it.
Custom Log Source	Log Source Name	User-defined log source name required.
	Retention Period	You can select 7 days, 30 days, 60 days, 90 days, or 180 days.

Connection Method	The default method is connected through your own COS bucket.
COS Bucket	Write the required logs into the selected COS bucket and configure privileges to allow the CSC service role to read them. CSC will automatically read log files at scheduled times. You can also <a href="#">submit a ticket</a> to customize the reading method, or visit the COS product page to create a bucket.
Storage Directory	To enhance reading performance, it is recommended to organize log file paths under the selected directory in the format yyyy/mm/dd. We will automatically read files corresponding to the natural calendar date. The log format supports JSON with lines separated by '\n' and supports gzip compression.
Log Sample	It is recommended to input log samples for the system's reference. The system will parse fields based on the input samples. You can further review and select specific fields and sorting operations, which will enhance the reading performance and accuracy of log parsing.
Timestamp	Select log samples and their corresponding timestamp formats.

4. Click **OK**, and the system will complete log connection. Subsequently, system policies and user-defined policies will audit exceptional behaviors and accounts based on the real-time connected logs. If an exceptional behavior is detected, the exceptional behavior data and trend chart below will be updated. Click **View all behaviors** to navigate to log analysis to view log details.



## Viewing Policy

1. Log in to the [CSC console](#). In the left sidebar, click **User Behavior Analytics (UEBA)**.
2. In the user behavior analytics (UEBA) list, system policies are provided to detect exceptional behaviors and exceptional accounts. It can detect and alarm risky behaviors including AKSK exceptional invocations, high-risk API

invocations, high-risk user operations, unauthorized service usage, and privilege escalation.

<input type="checkbox"/>	Policy ID/Name	Policy Type	Alert level	Policy Content	Switch
<input type="checkbox"/>	Suspicious IP calls high-risk interfaces	Preset policy	Critical	IPs that have not appeared in the past 6 months have called high-risk interfaces	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Aksk calls made by the root account	Preset policy	High	The root account uses aksk to call interfaces	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Aksk calls that have not been used for a lon...	Preset policy	High	Long-term use refers to aksk that has not appeared in a month	<input checked="" type="checkbox"/>
<input type="checkbox"/>	High-risk operations by new users	Preset policy	High	New users refer to users created within the last day, and high-risk operations refer to the list of interfaces that call sensitive/have security risks	<input checked="" type="checkbox"/>

Parameter Name	Description
Policy ID	System generated by default.
Policy Name	System policies are defined by the product backend. User-defined policies are defined by the user.
Policy Type	Includes system policies and user-defined policies.
Alarm Level	Includes critical, high, medium, low, and note.
Policy Content	Explain the detection content of the policy.
Enabling/Disabling	Users can enable or disable this policy.
Hits	Statistics for the last 7 days' policy hit records. Click to go to the alarm center to view alarm details. Alarm sources are the UEBA.
Operation	System policies are not allowed to be edited or deleted. User-defined policies can be edited or deleted.

## Adding Policy

1. Log in to the [CSC console](#). In the left sidebar, click **User Behavior Analytics (UEBA)**.
2. On the UEBA page, click **Add Policy** to customize user behavior analytics policy.
3. On the custom policy page, configure the relevant parameters and click **Confirm**.

### Custom Policy

---

Policy name

User type

Occurred  Every 10 minutes  Hourly  Daily  Weekly  Monthly

Event  Query search  Filter search

Alert name

Alert level  Critical  High  Medium  Low  Information

Operator  ⓘ

Operation object  ⓘ

Operation method  ⓘ

Parameter Name	Description
Policy Name	User-defined policy name, no more than 20 characters.
User Type	Cloud account or custom user. When users select cloud account, the log types available include CloudAudit read operation log and CloudAudit write operation log. When users select custom user, the log types available are those configured in the custom user.
Occurrence	Options include every 10 minutes, hourly, daily, weekly, and monthly.
Event	It can be configured by query or filter search.

Alarm Name	Optional. User exceptional behavior.
Alarm Level	It includes critical, high, medium, low, and note.
Operator	In the current log fields, select up to three fields to reflect the operator's information. It is recommended to select fields related to IP, account, and users. Fields cannot be left blank.
Operation Object	In the current log fields, select up to three fields to reflect the objects of user actions. It is recommended to select information such as service, product, resource, instance, and API. Fields can be left blank.
Operation Method	In the current log fields, select up to three fields to reflect the methods of user actions. It is recommended to select information such as key and AKSK. Fields can be left blank.