

Edge Computing Machine

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

Logging in to Linux Instance

Managing Windows Instance

Managing ECM Module

 Creating ECM Module

 Deleting ECM Module

 Configuring Default Module Security Group

Managing Instance

 Creating Instance

 Viewing Instance Details

 Adjusting Network

 Terminating Instance

 Resetting Password

 Viewing Instance Monitoring Data

 Configuring Instance Security Group

Managing Security Group

 Security Group Overview

 Creating Security Group

 Importing Security Group

 Associating Instance with Security Group

 Viewing Security Group

 Removing from Security Group

 Deleting Security Group

 Adjusting the Priorities of Security Groups

Managing Security Group Rule

 Adding Security Group Rule

 Viewing Security Group Rule

 Modifying Security Group Rule

 Deleting Security Group Rule

 Exporting Security Group Rule

 Importing Security Group Rule

Security Group Use Cases

Common Server Ports

Managing Image

Editing Tag

EIP Direct Access

Operation Guide

Logging in to Linux Instance

Last updated : 2023-12-25 17:29:50

Overview

ECM supports the following two login methods:

[Login through VNC](#)

[Login over SSH](#)

After creating an ECM instance successfully, you can log in to it as instructed in this document.

Prerequisites

You have created an ECM instance and obtained its public IP.

You already have the administrator account and password to log in to the instance.

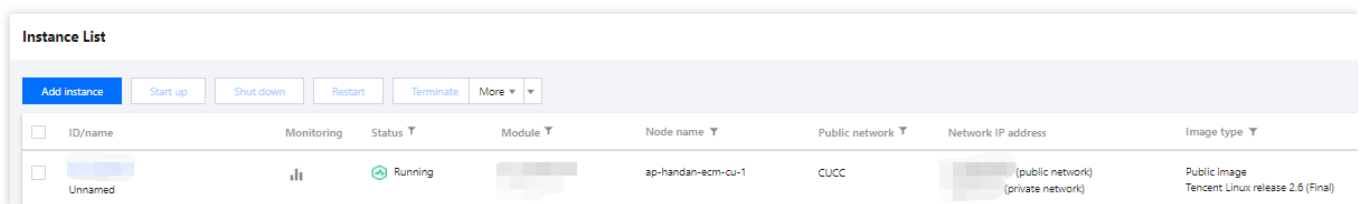
If you forgot your password, you can [reset it](#).

If you want to log in to a Linux instance over SSH, ensure that Xshell has been installed on the local PC.

Directions

Logging in through VNC

1. Log in to the [ECM console](#) and select **Instance List** on the left sidebar.
2. In **Instance List**, select the target Linux instance and click **Login** as shown below:



ID/name	Monitoring	Status	Module	Node name	Public network	Network IP address	Image type
Unnamed		Running		ap-handan-ecm-cu-1	CUCC	(public network) (private network)	Public image Tencent Linux release 2.6 (Final)

3. In the **Log in to Linux Instance** pop-up window, select **Log in Through VNC** and click **Log in Now** as shown below:

登录Linux实例

推荐登录方式

推荐使用您的本地电脑通过SSH方式登录，或使用远程登录软件登录边缘实例公网IP地址，以获得更好的登录体验。

VNC登录

若使用其他方式均无法登录，您可以使用VNC登录到边缘实例进行基本的操作和管理，该方式暂不支持复制粘贴、中文输入。

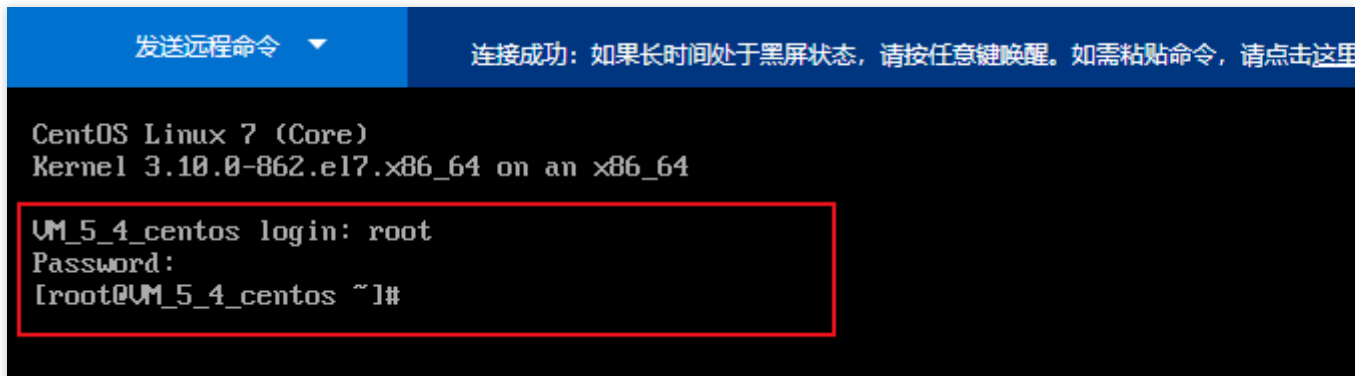
提示：采用VNC方式登录，请务必开启 MFA 二次验证提高安全保障级别。

[立即登录](#)

4. In the pop-up dialog box, enter the username after **login** and press **Enter**.

5. Enter the password after **Password** and press **Enter**.

The entered password is not displayed by default, as shown below:



```
发送远程命令 ▼ 连接成功: 如果长时间处于黑屏状态, 请按任意键唤醒。如需粘贴命令, 请点击这里
CentOS Linux 7 (Core)
Kernel 3.10.0-862.el7.x86_64 on an x86_64
UM_5_4_centos login: root
Password:
[root@UM_5_4_centos ~]#
```

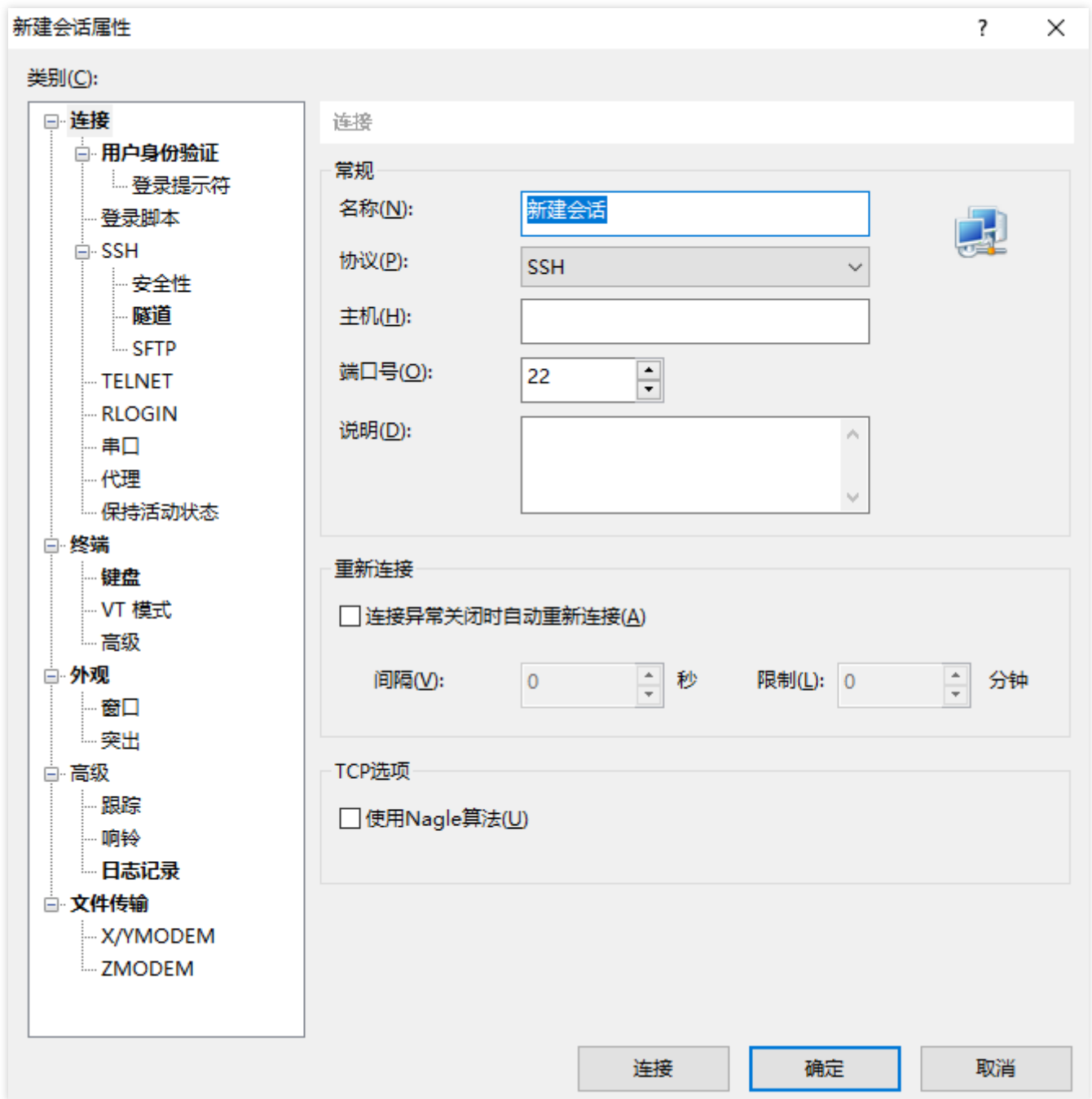
Logging in over SSH

Note:

There are multiple software applications for remote login to a Linux instance, such as PuTTY and Xshell. This document uses Xshell 6 as an example to describe how to use remote login software to log in to a Linux instance on a local Windows PC.

1. Open the Xshell client and click **New**.

2. In the **New Session Properties** window, enter the following content:



Name: enter a session name, such as `test` .

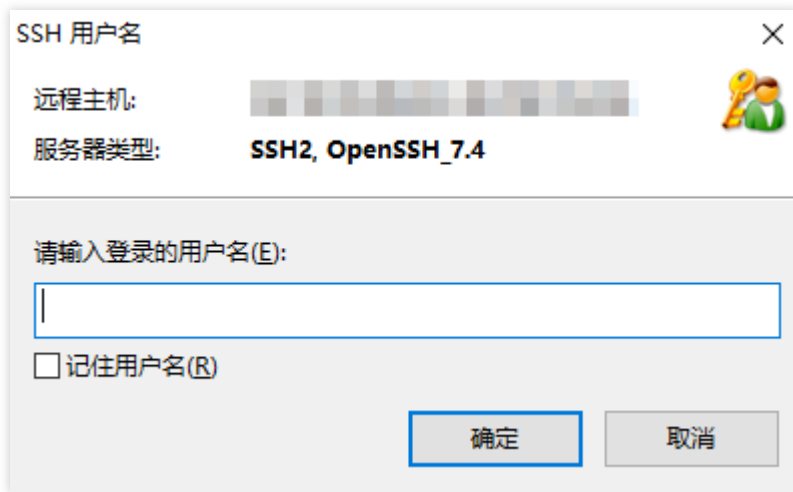
Host: enter the public IP of the ECM instance (log in to the [ECM console](#), and you can get the public IP on the instance list page).

Protocol: select "SSH".

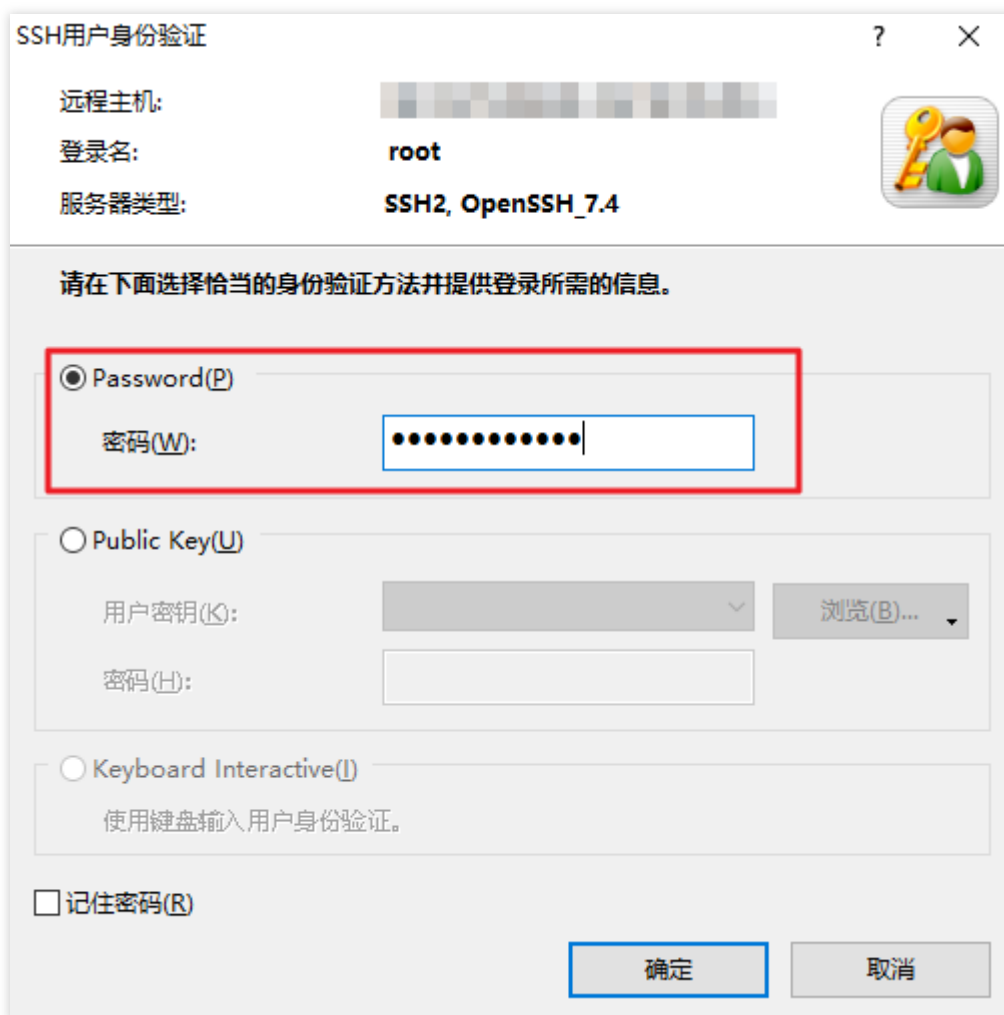
Port Number: enter the port of the ECM instance, which must be set to 22.

3. Click **Connect**.

4. Enter the login username such as `root` and click **OK** as shown below:



5. Enter the login password and click **OK** as shown below:



Once logged in, you can see the information of the ECM instance to which you are currently logged in on the left of the command prompt.

Managing Windows Instance

Last updated : 2023-12-26 09:45:44

Overview

This document describes how to log in to a Windows instance through Remote Desktop Connection on a local Windows computer.

Prerequisites

You have created an ECM instance and obtained its public IP.

You must have the admin account and password for logging in to a Windows instance remotely.

If you forgot your password, you can [reset it](#).

Directions

Note:

The following steps take Windows 10 as an example.

1. On a local Windows PC, right-click



and select **Run**:

2. In the **Run** window, enter **mstsc** and press **Enter** to open the Remote Desktop Connection window .
3. Enter the Windows instance's public IP after **Computer** and click **Connect**.
4. Enter the instance's admin account/password in the **Windows Security** pop-up window .

Note:

If the **Do you trust this remote connection?** window pops up, you can select **Don't ask me again for connections to this computer** and click **Connect**.

5. Click **OK** to log in to the Windows instance.

Managing ECM Module

Creating ECM Module

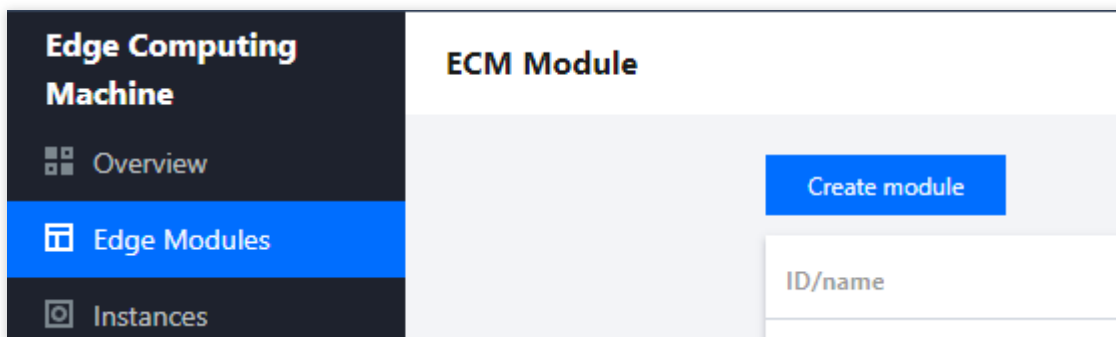
Last updated : 2023-12-26 09:47:53

Overview

This document describes how to create an ECM module in the console. An ECM module is the basic module for edge service management and composed of ECM instances. All instances in it use the same computing, network, and image configuration and provide the same service. By managing an ECM module, you can simplify scaling operations, which makes it easier for you to adjust the regional deployment of your business subsequently.

Directions

1. Log in to the [ECM console](#) and select **ECM Module** on the left sidebar.
2. On the ECM module page, click **Create Module**.



3. On the module creation and instance configuration page, configure the following information as prompted:

←
Create module and configure instance

Configure basic information

Module name Up to 60 characters can be entered. 60 more characters allowed.

Instance basic configuration

Model All models Standard

Instance type ① Latest model first Standard S5 Standard S4 Standard SN3ne

CPU cores 4-core 8-core 16-core 24-core 32-core

MEM 8G 16G 32G

Default image No images selected [Select an image](#)

System disk storage Default system disk size: 50GB (Size cannot be modified)

Data disk storage

0GB

25GB

50GB

100GB

Local storage is vulnerable to data loss, and is not suitable for use cases that do not have a data redundancy structure

Instance network and security configuration

Public IP Assign a public IPv4 address

Public network bandwidth cap

25Mbps

100Mbps

500Mbps

1G

Default security group Select a security group A security group is a virtual firewall to control the network access of inst

[Advanced settings](#) ▶

OK
Cancel

Module Name: it is the custom name of the ECM module to be created.

Instance Type: currently, **High I/O IT5Standard S4**, **High Private Network Bandwidth S4**, and **Standard SN3ne** models are supported. The performance of a model may vary slightly by scenario. For the specific performance differences, see [Instance Specification](#).

To make model selection during instance creation easier, we recommend you select **New Model First**. If this policy is enabled, the system will create an instance of the latest available model on your selected edge node. If there is no available latest model on the selected node, the system will create an instance in another available model.

CPU Cores: select a value as needed.

Memory: select a value as needed.

Default Image: Tencent Cloud provides public and custom images. We recommend new Tencent Cloud users select a public image.

System Disk Storage: it is 50 GB by default and cannot be adjusted.

Data Disk Storage: efficient and reliable storage devices are provided to expand the storage capacity of the ECM module. The default value is 0 GB, and the maximum value is 100 GB.

Default Network Bandwidth Cap: if the network bandwidth exceeds this cap, packets will be discarded by default. The default value is 25 Mbps, and the maximum value is 1,024 Mbps.

Default Security Group: a security group is a virtual firewall to control the network access of instances. You can go to the [Security Group](#) page in the ECM console to create an ECM security group.

Advanced Settings: you can modify the settings of default IP direct access and default tags as needed:

Default IP Direct Access: the IP direct access feature is applicable for scenarios where the public IP needs to be viewed in edge CVM instances; for example, private network traffic and public network traffic need to be forwarded to different IP addresses.

Note:

When you create a Linux ECM instance, the system will enable IP direct access by default (you can also disable it during instance creation in **Advanced Settings**). After an instance is created, the IP direct access status cannot be changed. If you create a Windows ECM instance, the system will not enable IP direct access by default (as Windows currently doesn't support IP direct access).

Default Tags: you can set default tags to manage instances in the ECM module by group. During instance creation, the default tags set in the ECM module will be used as the recommended tag key-value pairs, and you can also modify them as needed.

Note:

This configuration item only modifies the tag key-value pairs of the ECM module but doesn't automatically sync changes to those of successfully created instances.

4. Click **OK**.

Note:

If the ECM module configuration provided in the console cannot meet your requirements, [submit a ticket](#) for assistance, and a dedicated Tencent Cloud rep will contact you.

Deleting ECM Module

Last updated : 2023-12-26 09:49:33

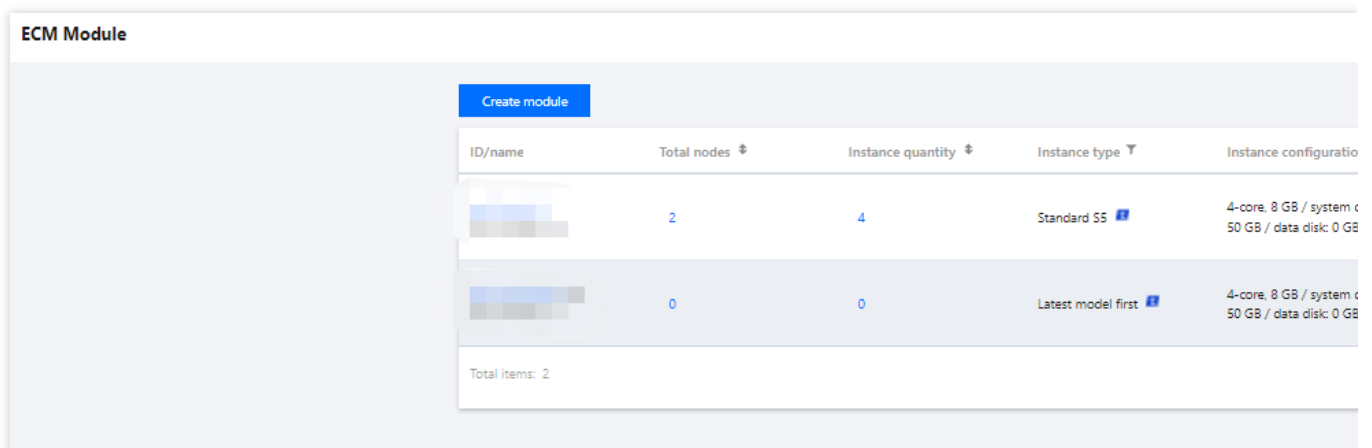
Overview

This document describes how to delete an EMC module that is no longer needed in the ECM console.

Directions

1. Log in to the [ECM console](#) and select **ECM Module** on the left sidebar.
2. On the ECM module page, select the ECM module to be deleted and click **Delete** in the **Operation** column.

Note: Before performing this operation, check whether there is any instance created under this module, and if so, it cannot be deleted.



The screenshot shows the 'ECM Module' page in the Tencent Cloud console. It features a 'Create module' button and a table with the following columns: ID/name, Total nodes, Instance quantity, Instance type, and Instance configuration. Two modules are listed, both with 0 instances. The first module has 2 total nodes and 4 instances of type 'Standard SS'. The second module has 0 total nodes and 0 instances of type 'Latest model first'. A 'Total items: 2' summary is shown at the bottom of the table.

ID/name	Total nodes	Instance quantity	Instance type	Instance configuration
[blurred]	2	4	Standard SS	4-core, 8 GB / system c 50 GB / data disk: 0 GB
[blurred]	0	0	Latest model first	4-core, 8 GB / system c 50 GB / data disk: 0 GB

Total items: 2

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

Configuring Default Module Security Group

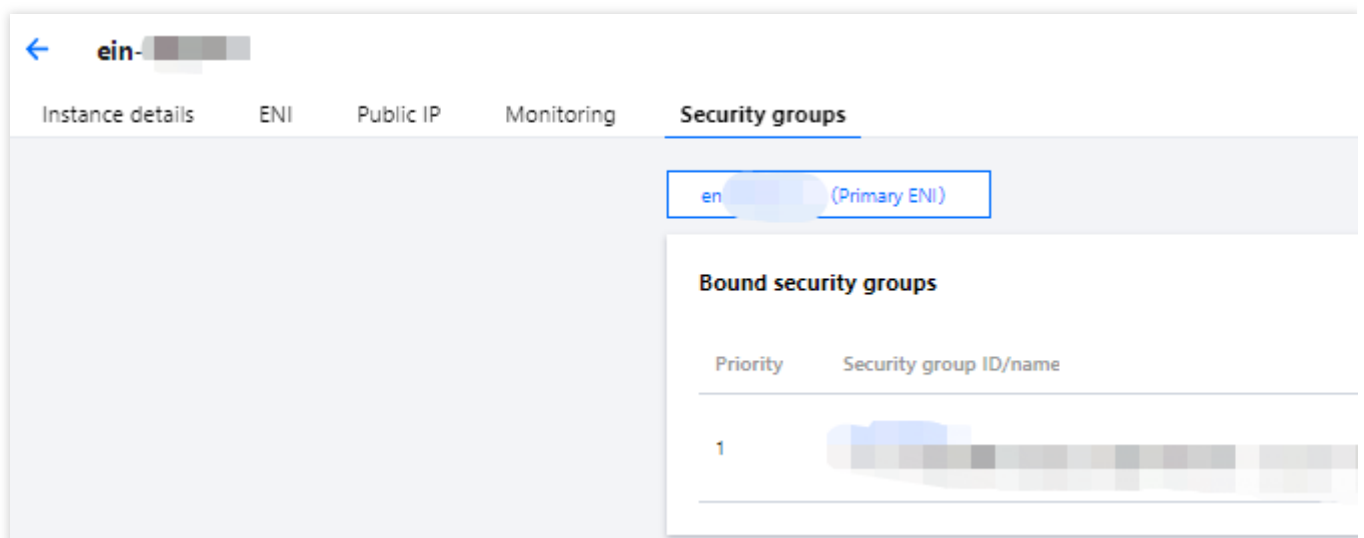
Last updated : 2023-12-26 09:53:41

Overview

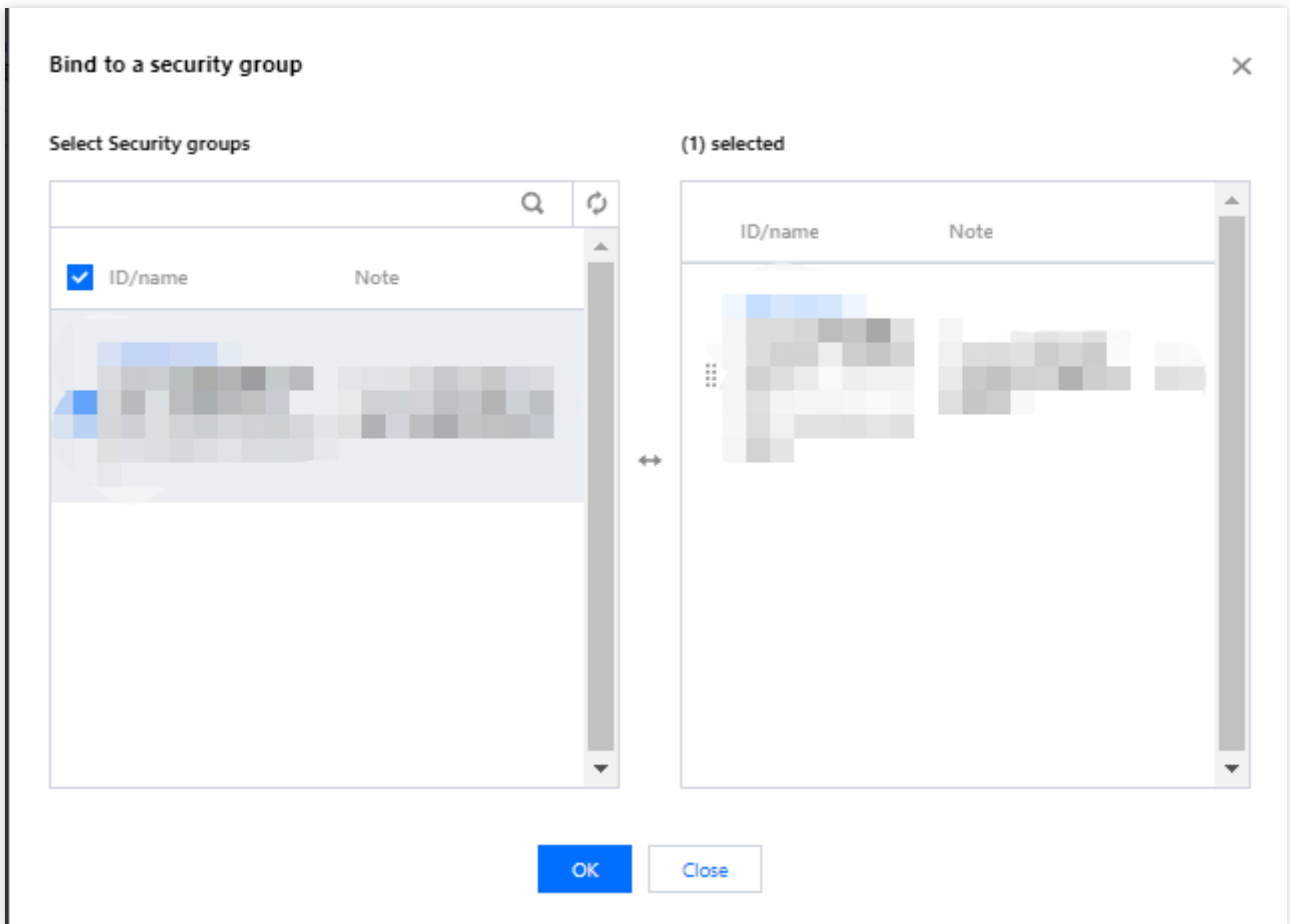
A security group is a virtual firewall that can filter stateful data packets. As an important means for network security isolation provided by Tencent Cloud, it can be used to set network access controls for one or more ECM instances. When creating an ECM module, you must configure the default security group for it, which will be used as the default security group configuration when you create instances in it. You can change the default security group as instructed in this document. In addition, Tencent Cloud allows you to replace the security group of an ECM instance after instance creation. For more information, see [Configuring Instance Security Group](#).

Directions

1. Log in to the ECM console and select **ECM Module** on the left sidebar to enter the **ECM Module** page.
2. On the **ECM Module** page, click the ID of the ECM module for which you want to configure a security group to enter the module details page.
3. On the module details page, select the **Security Group** tab and click **Bind** in the **Bound Security Groups** section as shown below:



4. In the **Bind to a Security Group** pop-up window, select the name of the security group to be bound based on your actual needs and click **OK** as shown below:



Managing Instance

Creating Instance

Last updated : 2023-12-26 09:56:18

Overview

This document describes how to create an ECM instance.

Prerequisites

Before creating an ECM instance, you must complete the following operations:

[Sign up for a Tencent Cloud account](#) and complete [identity verification](#).

[Create an ECM module](#).

If you want to use a Windows image, [submit a ticket](#) for application or contact your Tencent Cloud rep.

Directions

1. Log in to the [ECM console](#) and select **Instance List** on the left sidebar.
2. On the instance list page, click **Add Instance** to enter the **Create and Deploy Instance** page.
3. Configure the following information as prompted by the page:

←
Create and deploy instance

1
Password, image and bandwidth

>

2
Region deployment

Select a module ▼

Default instance configuration is as follows

Instance type: Standard S5 | CPU cores: 4C | MEM: 8GB | System disk storage: 50GB | Data disk storage: 0GB

Default image Select an image

OS: Tencent Linux release 2.6 (Final)

Image ID: img-evtcb0z

Image name: Tencent Linux release 2.6 (Final)

Public IP Assign a public IPv4 address

Public network bandwidth cap - 25 +

25Mbps

100Mbps

500Mbps

1024Mbps

Security groups Select a security group A security group is a virtual firewall to control the ne

Selected security group ▶ esg-

Advanced settings ▶

Instance name Name the instances in batches sequentially or by specifyi

Password
Key pair

Set password

Confirm password

Enter the password again

Next
Cancel

Select Module: select a module as needed.

Default Image: Tencent Cloud provides public and custom images. The image used by the module is selected by default. You can select an image as needed.

Default Network Bandwidth Cap: if the network bandwidth exceeds this cap, packets will be discarded by default. The default value is 25 Mbps, and the maximum value is 1,024 Mbps.

Security Group: a security group is a virtual firewall to control the network access of instances. The security group used by the module is selected by default. You can change the security group settings as needed.

Advanced Settings: you can modify the settings of default IP direct access and default tags as needed:

IP Direct Access: the IP direct access feature is applicable for scenarios where the public IP needs to be viewed in edge CVM instances; for example, private network traffic and public network traffic need to be forwarded to different IP

addresses.

Note:

When you create a Linux ECM instance, the system will enable IP direct access by default (you can also disable it during instance creation in **Advanced Settings**). After an instance is created, the IP direct access status cannot be changed. If you create a Windows ECM instance, the system will not enable IP direct access by default (as Windows currently doesn't support IP direct access).

Tags: you can set default tags to manage instances in the ECM module by group. During instance creation, the default tags set in the ECM module will be used as the recommended tag key-value pairs, and you can also modify them as needed.

Note:

This configuration item only modifies the tag key-value pairs of the ECM module but doesn't automatically sync changes to those of successfully created instances.

Instance Name: it is the custom name of the instance to be created.

Set Password and **Confirm Password:** set the custom password for instance login.

4. Click **Next**.

5. On the **Region Deployment** tab of the **Create and Deploy Instance** page, configure the following information as prompted:

←
Create and deploy instance

✓ Password, image and bandwidth

2 Region deployment

Default instance configuration is as follows

Instance type: Standard S5 | CPU cores: 4C | MEM: 8GB | System disk storage: 50GB | Data disk storage: 0GB | Image: Tencent Linux release 2.

Region deployment

Save as node template
Load node template

Node location	Node ↔	Node type	Network type	Virtual Private Cloud
Please select... ▾	Please select... ▾		Please select ▾	Please select...

+ Add node

Free security reinforcement: Install components to activate the basic version of cloud workload protection. [Learn more](#)

Free Cloud Monitor: Activate free monitoring, analysis and alarming features of Tencent Cloud service, and install components to obtain ser

Estimated cost:

Configuration fee: 0 USD/Days (fee details)

Bandwidth fee: For bandwidth fee, see [pricing for different regions](#)

Back
Confirm purchase
Cancel

Node Province: we recommend you select the province closest to your end users to minimize the access latency and accelerate the access.

Node Region: select a region as needed.

Network Type: select a public network ISP as needed.

Instance Quantity: enter the number of ECM instances to be purchased.

Activate CWPP for Free: it is selected by default to help you build a server security protection system to prevent data leakage.

Activate CM for Free: it is selected by default to activate CM free of charge. The CM agent will be installed to get the server monitoring metrics and display them as a monitoring icon, and you can customize the alarm thresholds.

6. Click **Confirm Purchase**.

After an instance is successfully created, its relevant information will be sent to you through the notification channel you subscribe to. You can also view the newly created resource in the [Instance List](#).

Viewing Instance Details

Last updated : 2023-12-26 09:58:17

Overview

After creating an ECM instance, you can view its details in the console.

Directions

1. Log in to the [ECM console](#).
2. On the left sidebar, select **Instance List**.
3. On the instance list page, find the target instance and click its ID/instance name to enter the instance details page.

Note:

You can also click **More > Details** on the row of the target instance to enter the instance details page.

The screenshot displays the 'Instance details' page for an Edge Computing Machine (ECM) instance. The page is organized into several sections:

- Basic information:**
 - Instance name: Unnamed
 - Instance ID: ein-XXXXXX
 - UUID: XXXXXXXXXXXXXXXXXXXXXXXXX
 - Instance status: Running
 - Module ID: XXXXXXXX
 - Module name: XXXXXXXX
 - Bind key: -
 - Created at: 2022-03-08 17:32:52
 - Tag: None
- Instance configuration:**
 - Instance type: Standard S5
 - CPU cores: 4-core
 - MEM: 8GB
 - System disk storage: 50GB
 - Data disk storage: 0
 - Image: Public image: XXXXXXXX
- Node information:**
 - Node: Hebei/Handan
 - Node name: ap-handan-ecm-cu
 - Node type: Single-connection
- Network information:**
 - Network: [Link]
 - Subnet: [Link]
 - Public network bandwidth cap: [Link]
 - IP address information: [Link]

On the instance details page, you can view instance information such as basic information, instance configuration, node information, and network information.

Adjusting Network

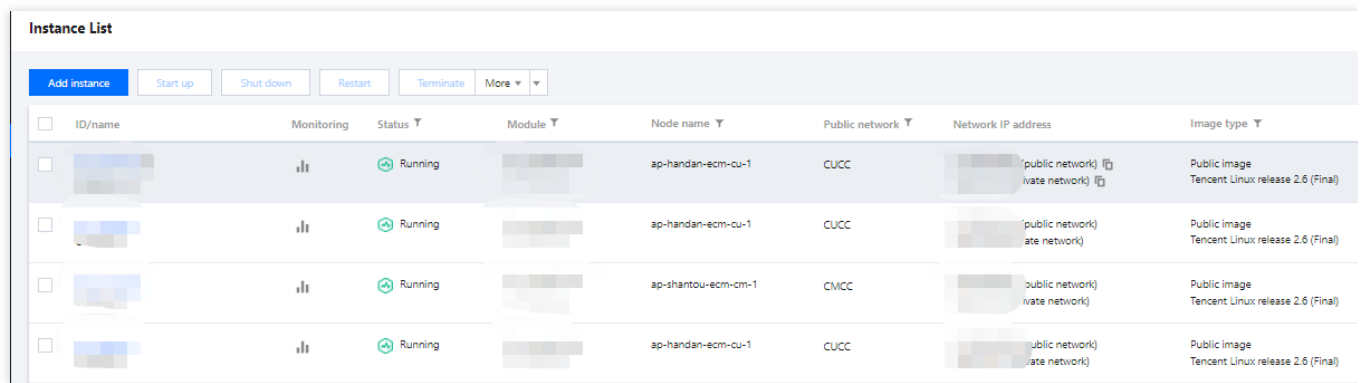
Last updated : 2023-12-26 09:59:23

Overview

This document describes how to modify the bandwidth cap of an instance.

Directions

1. Log in to the [ECM console](#).
2. On the left sidebar, select **Instance List**.
3. On the instance list page, select the target instance and click **More > Adjust Network**.



<input type="checkbox"/>	ID/name	Monitoring	Status	Module	Node name	Public network	Network IP address	Image type
<input type="checkbox"/>	[blurred]	[bar chart]	Running	[blurred]	ap-handan-ecm-cu-1	CUCC	[blurred] (public network) [blurred] (private network)	Public image Tencent Linux release 2.6 (Final)
<input type="checkbox"/>	[blurred]	[bar chart]	Running	[blurred]	ap-handan-ecm-cu-1	CUCC	[blurred] (public network) [blurred] (private network)	Public image Tencent Linux release 2.6 (Final)
<input type="checkbox"/>	[blurred]	[bar chart]	Running	[blurred]	ap-shantou-ecm-cm-1	CMCC	[blurred] (public network) [blurred] (private network)	Public image Tencent Linux release 2.6 (Final)
<input type="checkbox"/>	[blurred]	[bar chart]	Running	[blurred]	ap-handan-ecm-cu-1	CUCC	[blurred] (public network) [blurred] (private network)	Public image Tencent Linux release 2.6 (Final)


4. In the pop-up window, set the bandwidth cap and click **OK**.


Note:

The default instance bandwidth cap is 1 Gbps. If it cannot meet your needs, [submit a ticket](#) for assistance.

Adjust network

You have selected  [View details](#) ▼

Instance name	Instance ID	Node	Current image
Unnamed		ap-handan-ecm-cu-1	Tencent Linux rele Image ID: img-evit Name: Tencent Lin

New bandwidth  25 Mbps

25Mbps 100Mbps 500Mbps 1024Mbps

Terminating Instance

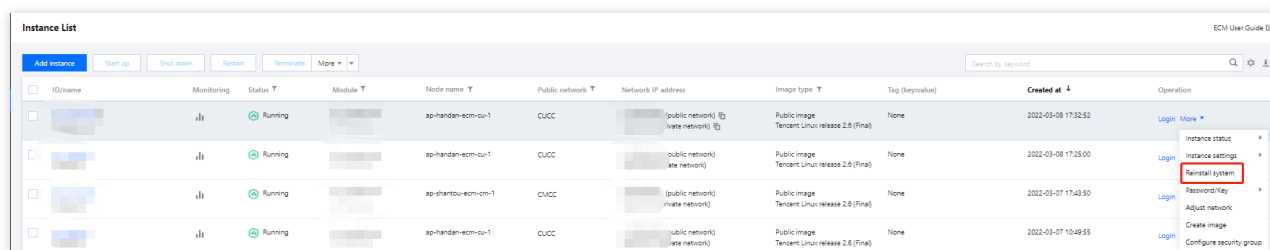
Last updated : 2023-12-25 17:19:33

Overview

This document describes how to terminate an ECM instance that is no longer needed.

Directions

1. Log in to the [ECM console](#).
2. On the left sidebar, select **Instance List**.
3. On the instance list page, select the instance to be terminated and click **More > Terminate** as shown below:



4. In the pop-up window, select **Terminate now** or **Terminate at scheduled time** based on your actual needs and click **Next** as shown below:

Reinstall system ✕

You have selected [blurred] [View details](#) ▼

Instance name	Instance ID	Node	Current image
Unnamed	ein- [blurred]	ap-handan-ecm-cu-1	Tencent Linux release 2.6 (Final) Image ID: img-evitcbqz Name: Tencent Linux release 2.6 (Final)

i Note: After reinstallation, all data in the data disk are cleared.

Reinstall the image as No images selected [Select image](#)

- Free security reinforcement: Install components to activate the basic version of cloud workload protection. [Learn more](#)
- Free Cloud Monitor: Activate free monitoring, analysis and alarming features of Tencent Cloud service, and install components to obtain server monitoring metrics. [Learn more](#)

Username

Password

Confirm password

OK Cancel

Terminate now: the instance data will be cleared immediately and cannot be recovered.

Terminate at scheduled time: you need to specify the termination time. The instance will be terminated at the scheduled time, and the data cannot be recovered.

5. Check the actual and relevant resources to be terminated and click **Start Termination**.

Resetting Password

Last updated : 2023-12-25 17:19:47

Overview

This document describes how to reset your instance login password in the ECM console.

Notes

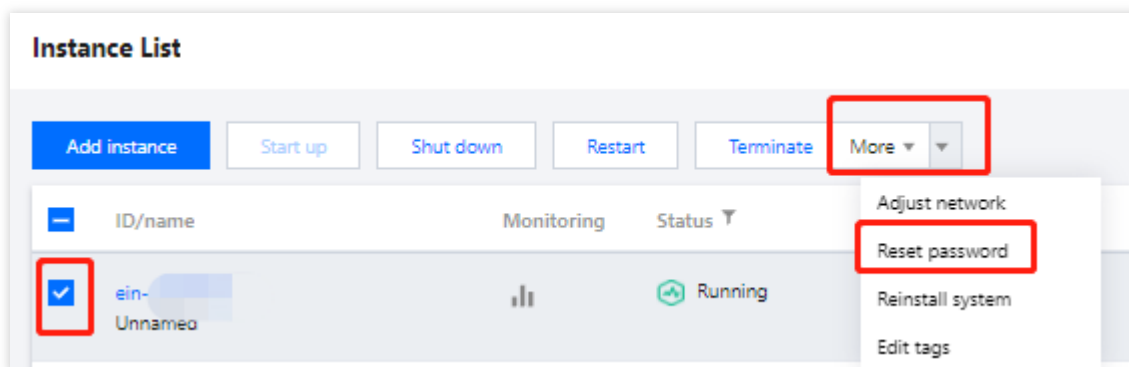
The server will be shut down during password reset. Schedule the time in advance to avoid data loss. We recommend you perform the operation during off-peak hours to minimize the impact.

Requirements of the new password for Linux instance: the password must contain 8–30 characters in at least three of the following character types: uppercase letters, lowercase letters, digits, and special symbols and cannot start with "/".

Requirements of the new password for Windows instance: the password must contain 12–30 characters in at least three of the following character types: uppercase letters, lowercase letters, digits, and special symbols and cannot start with "/" or contain the username.

Directions

1. Log in to the [ECM console](#).
2. On the left sidebar, select **Instance List**.
3. On the instance list page, select the target instance and click **More > Reset Password**.



4. In the pop-up window, confirm the username for which you want to reset the password (for example, the username is `root` in a Linux instance and is `Administrator` in a Windows instance), enter the new password in **New Password** and **Confirm Password**, and click **Next** as shown below:

Reset password

You have selected [redacted] [View details](#) ▼

Instance name	Instance ID	Node	Current image
Unnamed	[redacted]	ap-handan-ecm-cu-1	Tencent Linux release 2.6 (Final) Image ID: img-evitcbqz Name: Tencent Linux release 2.6 (Final)

Username:

New password:

Note: Your password satisfies the current policy. However we still suggest you to set a stronger password, which has a length of at least 12 characters, including at least 4 types of [a-z], [A-Z], [0-9] and special characters ([()~!@#%&^*~+=_{}|:;<>.,?/]), and at least 2 different characters of each type.

Confirm password:

5. Select **Agree to a forced shutdown** and click **Reset Password** as shown below:

Reset password ✕

You have selected [blurred] [View details](#) ▼

Instance name	Instance ID	Node	Current image
Unnamed	[blurred]	ap-handan-ecm-cu-1	Tencent Linux release 2.6 (Final) Image ID: img-evitcbqz Name: Tencent Linux release 2.6 (Final)

1. Shut down the instance before resetting password to avoid data loss. Note that shutting down the instance will interrupt your business.
2. Forced shutdown may lead to data loss or damage to file systems. You can also reset the password after a manual shutdown.
3. Forced shutdown may take a while. Please wait.

Agree to a forced shutdown

Reset password Cancel

Viewing Instance Monitoring Data

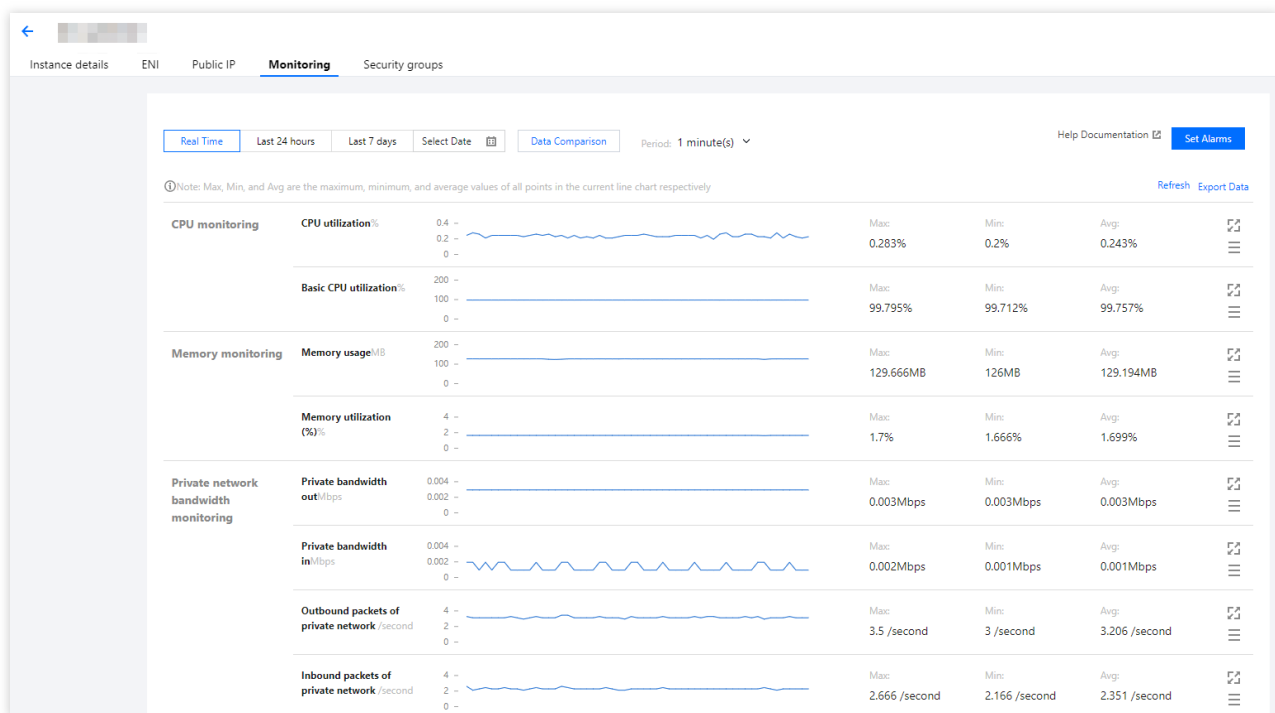
Last updated : 2023-12-25 17:20:01

Overview

This document describes how to view the monitoring data of the current instance in the ECM console.

Directions

1. Log in to the [ECM console](#).
2. On the left sidebar, select **Instance List**.
3. On the instance list page, find the desired instance and click the ID/instance name to enter the instance details page.
4. Select the **Monitoring** tab to enter the monitoring page, and you can view ECM instance monitoring information such as CPU, memory, private and public network bandwidths, and disk usage as shown below:



On the monitoring page, you can filter and export data by time to manage ECM instances more easily.

Configuring Instance Security Group

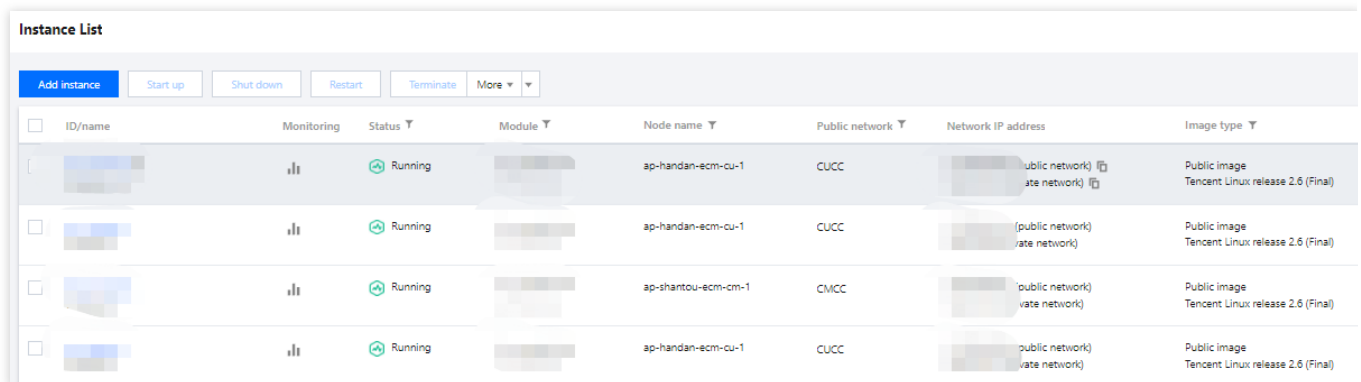
Last updated : 2023-12-25 17:20:12

Overview

A security group is a virtual firewall that can filter stateful data packets. As an important means for network security isolation provided by Tencent Cloud, it can be used to set network access controls for one or more ECM instances. When creating an ECM instance, you must configure a security group for it. If the module's security group that your created instance uses by default or the custom security group cannot meet the requirements of your business scenarios, you can replace it as instructed in this document.

Directions

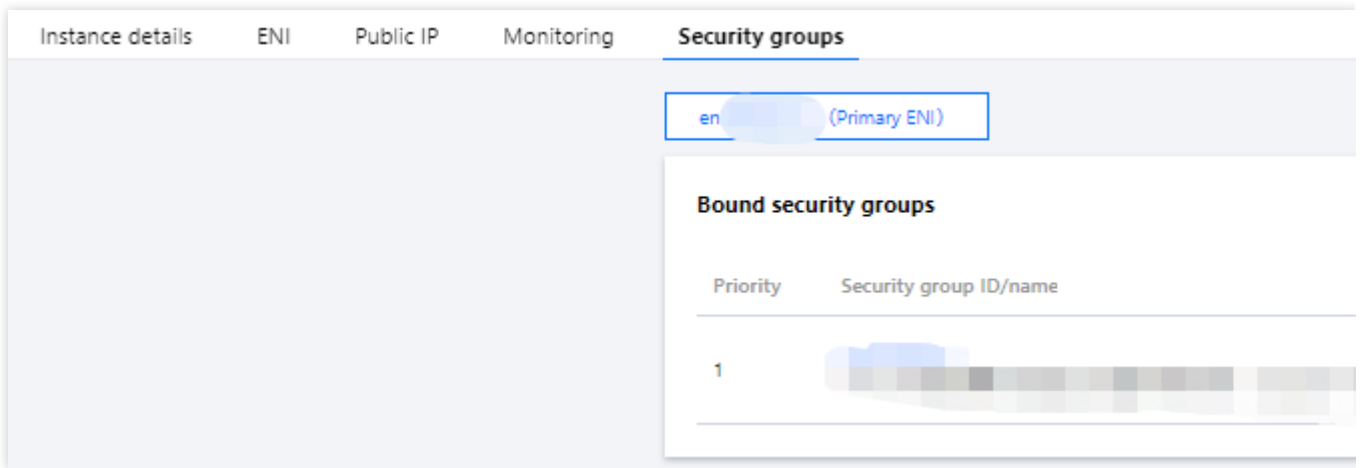
1. Log in to the [ECM console](#).
2. On the left sidebar, select **Instance List** to enter the **Instance List** page.
3. On the **Instance List** page, find the target instance and select **More > Configure Security Group** on the right of the row as shown below:



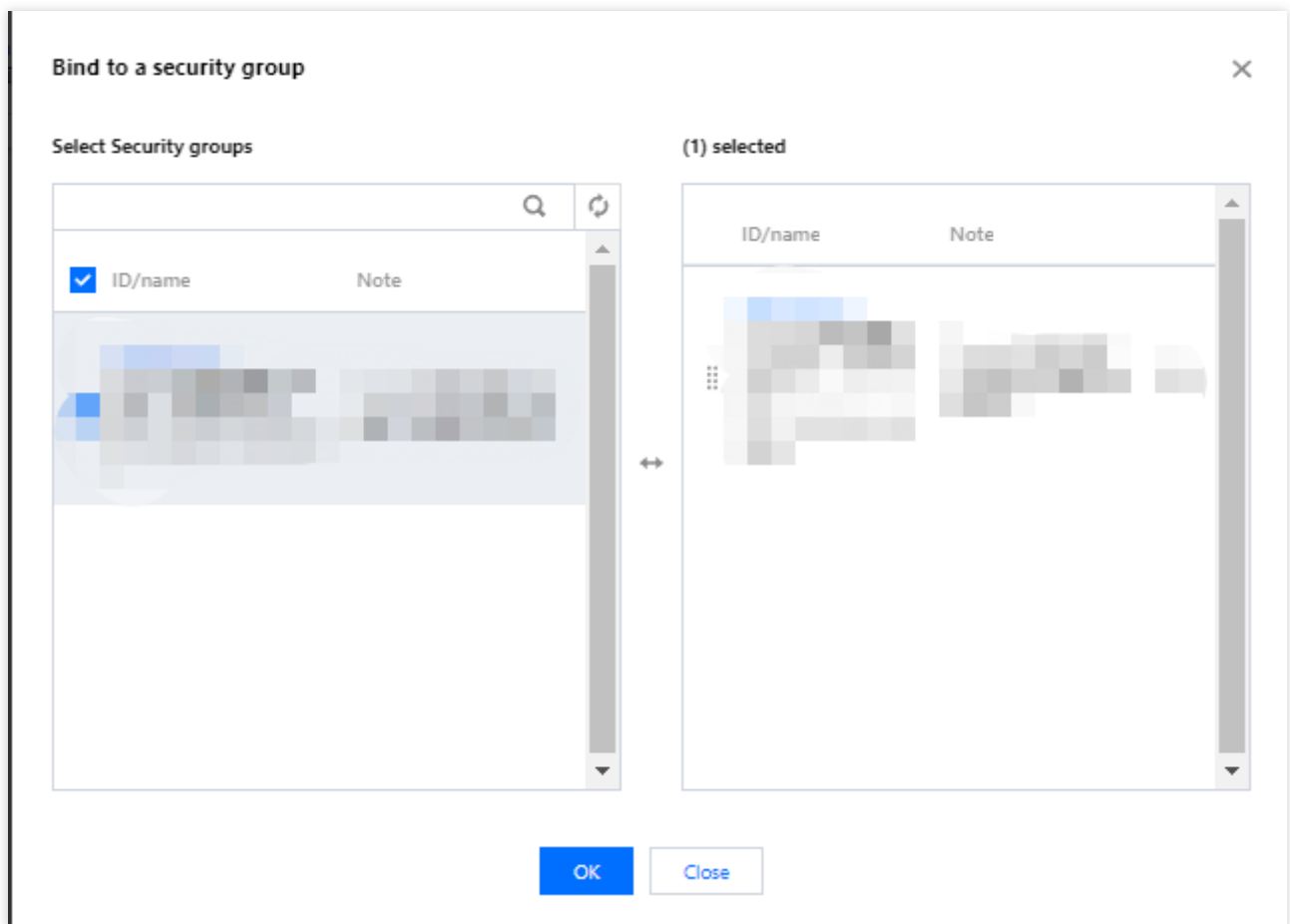
<input type="checkbox"/>	ID/name	Monitoring	Status	Module	Node name	Public network	Network IP address	Image type
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Running	[REDACTED]	ap-handan-ecm-cu-1	CUCC	[REDACTED] public network) [REDACTED] vate network)	Public image Tencent Linux release 2.6 (Final)
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Running	[REDACTED]	ap-handan-ecm-cu-1	CUCC	[REDACTED] (public network) [REDACTED] vate network)	Public image Tencent Linux release 2.6 (Final)
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Running	[REDACTED]	ap-shantou-ecm-cm-1	CMCC	[REDACTED] (public network) [REDACTED] vate network)	Public image Tencent Linux release 2.6 (Final)
<input type="checkbox"/>	[REDACTED]	[REDACTED]	Running	[REDACTED]	ap-handan-ecm-cu-1	CUCC	[REDACTED] (public network) [REDACTED] vate network)	Public image Tencent Linux release 2.6 (Final)

Then, you will be redirected to the **Security Group** tab on the instance management page to bind a security group.

4. In **Bound Security Groups** on the **Security Group** tab, click **Bind** as shown below:



5. In the **Bind to a Security Group** pop-up window, select the name of the security group to be bound based on your actual needs and click **OK** as shown below:



Managing Security Group

Security Group Overview

Last updated : 2023-12-25 17:20:26

A security group is a virtual firewall that can filter stateful data packets. As an important means for network security isolation, it can be used to set network access controls for ECM, ELB, ENI, and other resources while controlling their outbound and inbound traffic.

You can configure security group rules to allow or reject inbound and outbound traffic of instances within the security group.

The security group feature of ECM is logically isolated from the public security group feature in the central cloud. Central cloud products such as CVM cannot be associated with a security group in ECM, and ECM resources such as ECM module, ECM instance, and ELB cannot be directly associated with a public security group in the central cloud. If you have already created a public security group, you can [import its data](#), and a security group data record for ECM will be automatically generated after the import.

Note:

Central cloud refers to various products in Tencent Cloud regions and AZs. For more information, see [CVM Overview](#), [Regions and AZs](#), and [Security Group](#).

Security Group Features

Resources such as ECM instances, ELB instances, and ENIs with the same network security isolation requirements can be put into the same logical security group.

By default, instances in the same security group are not interconnected, unless you allow them by specifying rules.

A security group is stateful. If it has no rules after being created, it will reject all traffic by default. For the allowed inbound/outbound traffic, it will allow the traffic to be flowed automatically, and vice versa.

You can modify security group rules at any time, and the new rules will take effect immediately.

Usage Limits

ECM security group use limits and quotas are as detailed below:

Feature Description	Quantity
Maximum number of created security groups	200
Maximum number of outbound (inbound) rules per security group	100

Maximum number of ECM instances associated with each security group	2,000
Maximum number of ECM modules associated with each security group	100
Maximum number of security groups associated with each ECM resource (such as instance and ENI)	5
Maximum number of security groups associated with each ECM module	5
Maximum number of security group IDs that can be referenced by a security group	10

Security Group Rules

Components

A security group rule consists of:

Source: IP address of the source data (inbound) or target data (outbound)

Protocol Type and Protocol Port: protocol type, such as TCP, UDP, HTTP, etc.

Policy: **Allow** or **Reject**.

Rule priorities

The rules in a security group are prioritized from top to bottom. The rule at the top of the list has the highest priority and will take effect first, while the rule at the bottom has the lowest priority and will take effect last.

If there is a rule conflict, the rule with the higher priority will prevail by default.

If there is inbound/outbound traffic to/from an instance bound to a security group, the rules in the security group will be matched one by one from top to bottom. If a rule is matched successfully, the traffic hitting the rule will not match lower rules.

Multiple security groups

An instance can be bound to one or multiple security groups. When it is bound to multiple security groups, the security group rules will be matched sequentially from top to bottom. You can adjust the priorities of security groups at any time.

Security Group Templates

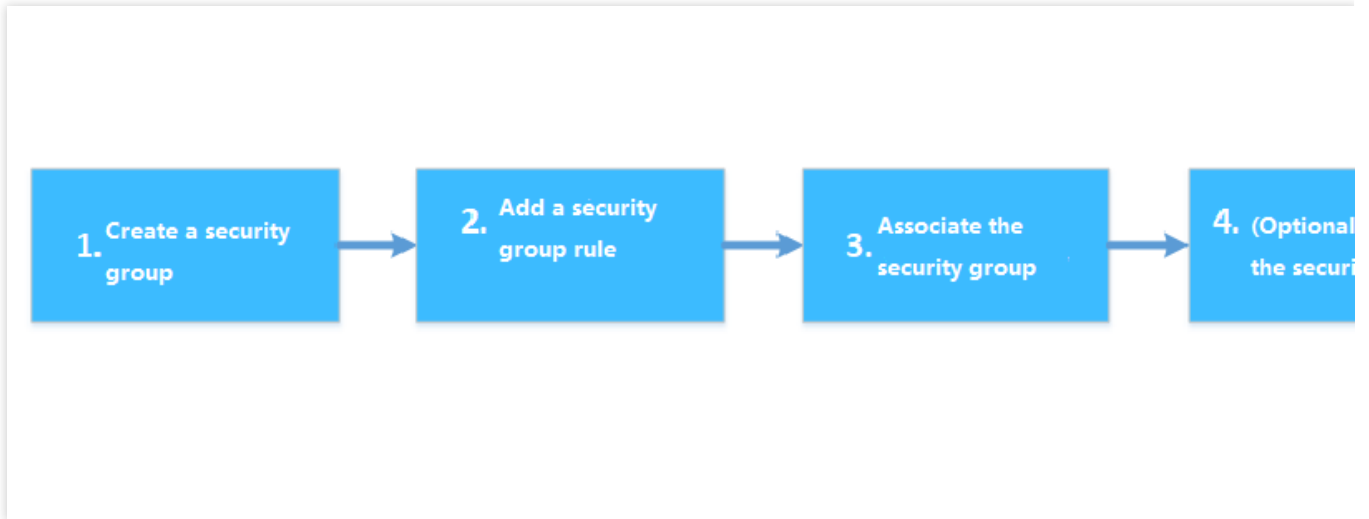
When creating a security group, you can select one of the two security group templates provided by Tencent Cloud:

Open all ports: all inbound and outbound traffic will be allowed to pass.

Open major ports: port TCP 22 (for Linux SSH login), ports 80 and 443 (for web service), port 3389 (for Windows remote login), the ICMP protocol (for ping commands), and the private network will be open to the internet.

Directions

The following figure shows you how to use a security group:



Creating Security Group

Last updated : 2023-12-25 17:20:52

Overview

Security groups act as virtual firewalls for ECM instances. Each ECM instance must be associated with at least one security group. If you haven't created a security group when creating an ECM instance, Tencent Cloud provides two templates (**Open all ports** and **Open ports 22, 80, 443, and 3389 and ICMP protocol**) for quick security group creation. For more information, see [Security Group](#).

This document describes how to create a security group in the ECM console.

Directions

1. Log in to the ECM console and select **Edge Network** > **Security Group** on the left sidebar.
2. On the **Security Group** management page, click **Create**.
3. In the **Create ECM Security Group** pop-up window, configure the options as shown below:

Create ECM security group ✕

Template

Name *

Note

[Advanced Options](#) ▶

[Display template rule](#) ▶

Template: select an appropriate template based on the service to be deployed in the ECM instance in the security group, which simplifies the security group rule configuration, as shown below:

Template	Description	Scenario
Open all ports	All ports are open. May present security issues.	-
Open ports 22, 80, 443, and 3389 and ICMP protocol	Ports 22, 80, and 443 and 3389, and the ICMP protocol are open. All ports are open internally.	Suitable for instances with web services.
Custom	You can create a security group and then add custom rules. For detailed directions, see Adding Security Group Rule .	-

Name: name of the security group.

Notes: a short description of the security group.

Advanced Settings: you can add tags for the security group after expanding.

Display Template Rules: you can view the existing rules in the security group after expanding.

4. Click **OK**.

Importing Security Group

Last updated : 2023-12-25 17:21:04

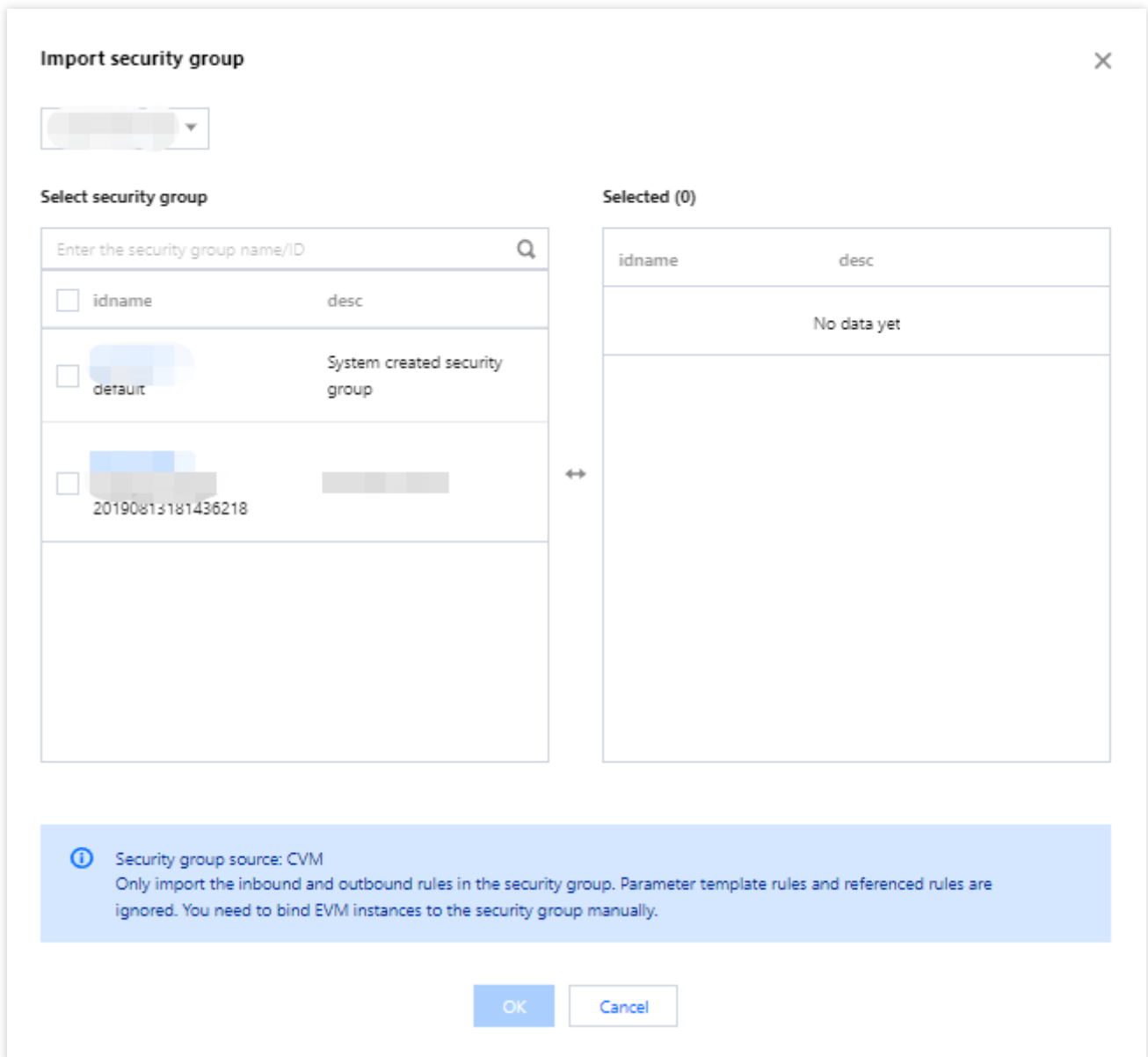
Overview

The security group feature of ECM is logically isolated from the public security group feature in the central cloud. Central cloud products such as CVM cannot be associated with a security group in ECM, and ECM resources such as ECM module, ECM instance, and ELB cannot be directly associated with a public security group in the central cloud. If you have already created a public security group, you can import its data, and a security group data record for ECM will be automatically generated after the import.

You can also create a security group by yourself. For more information, see [Creating Security Group](#).

Directions

1. Log in to the ECM console and select **Edge Network** > **Security Group** on the left sidebar.
2. On the **Security Group** management page, click **Import**.
3. In the **Security Group** pop-up window, perform the operations as shown below:



1. Select the central cloud region, and all security groups in this region will be displayed.
2. Select the security group data to be imported.

Note:

Currently, you cannot import the security group data in finance zones or regions outside the Chinese mainland. Only inbound rules in the security group are imported, while the parameter template rules and nested rules will be filtered out.

3. Click **OK** to import the public security group in the central cloud, and new data will be generated in the ECM security group management list.

Associating Instance with Security Group

Last updated : 2023-12-25 17:21:15

Note:

A security group can be associated with resources such as ECM instance, ELB instance, and ENI. This document uses an ECM instance as an example to describe how to associate a security group.

Overview

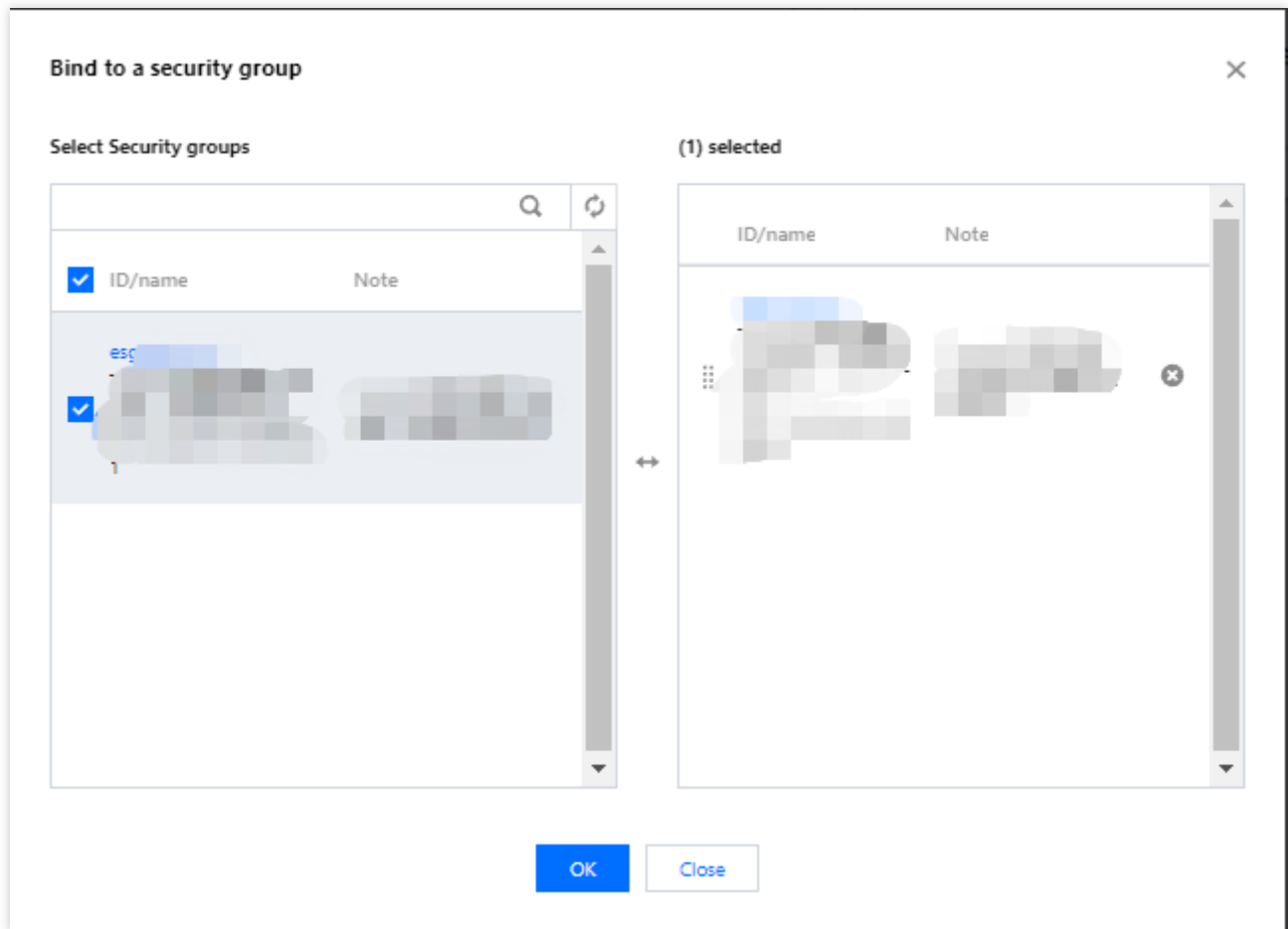
As an important means for network security isolation, a security group can be used to set network access controls for one or more ECM instances. You can associate your ECM instance with one or more security groups as needed. This document describes how to associate an ECM instance with a security group in the ECM console.

Prerequisites

You have created an ECM instance.

Directions

1. Log in to the ECM console and select **Edge Network** > **Security Group** on the left sidebar.
2. On the **Security Group** management page, select **More** > **Manage Instance** on the right of the instance to be associated.
3. On the **Associate Instance** page, click **Associate**.
4. In the **Associate Instance** pop-up window, perform the operations as shown below:



5. Filter out the node region, and the page will display all ECM instances in this region. The instance data in all regions is displayed by default.
6. Filter out the module, and the page will display all ECM instances under this module. The instance data under all modules is displayed by default.
7. Select the instance ID/name of the ECM instance to be associated.
8. Click **OK**.

Subsequent Operations

If you want to view all created security groups, query the security group list and filter groups by resource attribute.

For detailed directions, see [Viewing Security Group](#).

To disassociate an ECM instance from one or more security groups, remove it from the security groups.

For detailed directions, see [Removing Instance from Security Group](#).

If you no longer need a security group, you can delete it. Once a security group is deleted, all rules within it are also deleted.

For detailed directions, see [Deleting Security Group](#).

Viewing Security Group

Last updated : 2023-12-25 17:21:36

Overview

This document describes how to view the list of all created security groups.

Directions

Viewing security group

1. Log in to the ECM console and select **Edge Network** > **Security Group** on the left sidebar.
2. On the **Security Group** management page, view all created security groups.

Searching for security group

You can also use the search bar on the security group management page to quickly filter a specific security group.

1. Log in to the ECM console and select **Edge Network** > **Security Group** on the left sidebar.
2. In the top-right corner of the list on the **Security Group** management page, click the search bar and use one of the following fields to search for a security group.

Select **Security Group Name**, enter a security group name, and click



to filter the corresponding security group.

Select **Security Group ID**, enter a security group ID, and click



to filter the corresponding security group.

Select **Security Group Tag**, enter a tag, and click



to filter all security groups with the tag.

Other Operations

For more information on the syntax for viewing the specified security group, you can click



on the search bar.

Removing from Security Group

Last updated : 2023-12-25 17:21:46

Overview

To disassociate an ECM instance from one or more security groups, remove it from the security groups based on your business needs.

Prerequisites

Your ECM instance is bound to two or more security groups.

Directions

1. Log in to the ECM console and select **Edge Network** > **Security Group** on the left sidebar.
2. On the **Security Group** management page, select **More** > **Manage Instance** on the right of the target security group.
3. Select the instances to be removed and click **Remove Selected**.
4. In the pop-up window, click **OK**.

Deleting Security Group

Last updated : 2023-12-25 17:21:57

Overview

If you no longer need a security group, you can delete it. Once a security group is deleted, all rules within it are also deleted.

Prerequisites

Before deleting a security group, you must remove all associated instances. Otherwise, the operation will fail. For more information, see [Removing Instance from Security Group](#).

Directions

1. Log in to the ECM console and select **Edge Network** > **Security Group** on the left sidebar.
2. On the **Security Group** management page, select **More** > **Delete** on the right of the security group to be deleted.
3. In the pop-up window, click **OK**.

Adjusting the Priorities of Security Groups

Last updated : 2023-12-25 17:22:08

Overview

You can bind one or more security groups to an ECM instance. If you have bound multiple security groups, they are executed based on their priorities. You can adjust the priorities as follows.

Prerequisites

Your ECM instance is bound to two or more security groups.

Directions

1. Log in to the ECM console and select **Instance List** on the left sidebar to enter the **Instance List** page.
2. On the **Instance List** page, click the ID of the ECM instance to enter the details page.
3. Select the **Security Group** tab to enter the security group management page.
4. In the **Bound Security Groups** section on the right, click **Sort**. Click the



icon on the right to drag the security groups up or down to adjust their priorities. The security group at the top has the highest priority.

5. After completing the adjustment, click **Save**.

Managing Security Group Rule

Adding Security Group Rule

Last updated : 2023-12-25 17:22:24

Overview

Security groups are used to manage traffic to and from public and private networks. For the sake of security, most inbound traffic is denied by default. If you selected **Open all ports** or **Open ports 22, 80, 443, 3389 and ICMP protocol** as the template when creating a security group, rules are automatically created and added to the security group to allow traffic on those ports. For more information, see [Security Group](#).

This document describes how to add security group rules to allow or reject traffic to and from public or private networks for ECM instances and resources.

Prerequisites

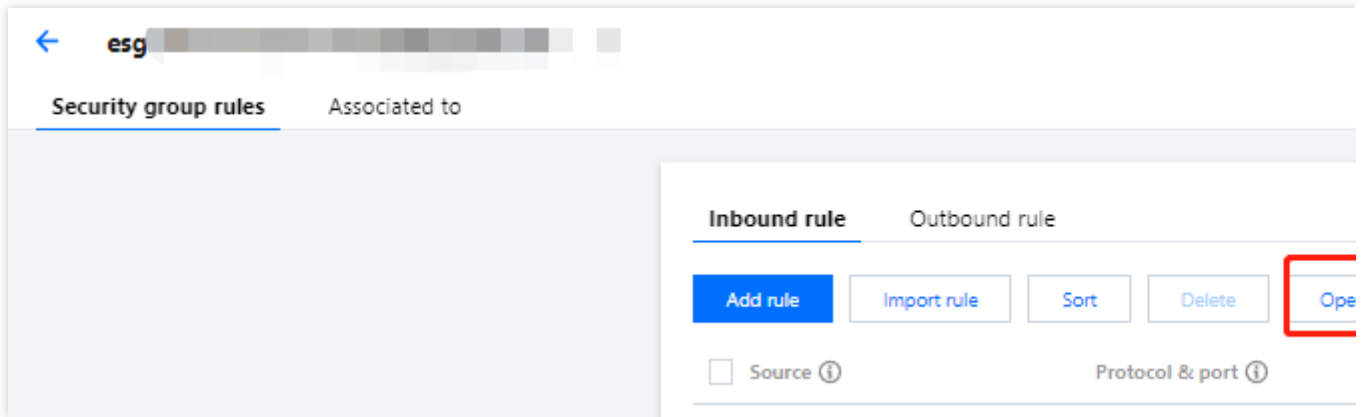
You should have an existing security group. If you do not, refer to [Creating a Security Group](#) for details.

You should know which traffic is allowed or rejected for your ECM instance. For more information on security group rules and their use cases, see [Security Group Use Cases](#).

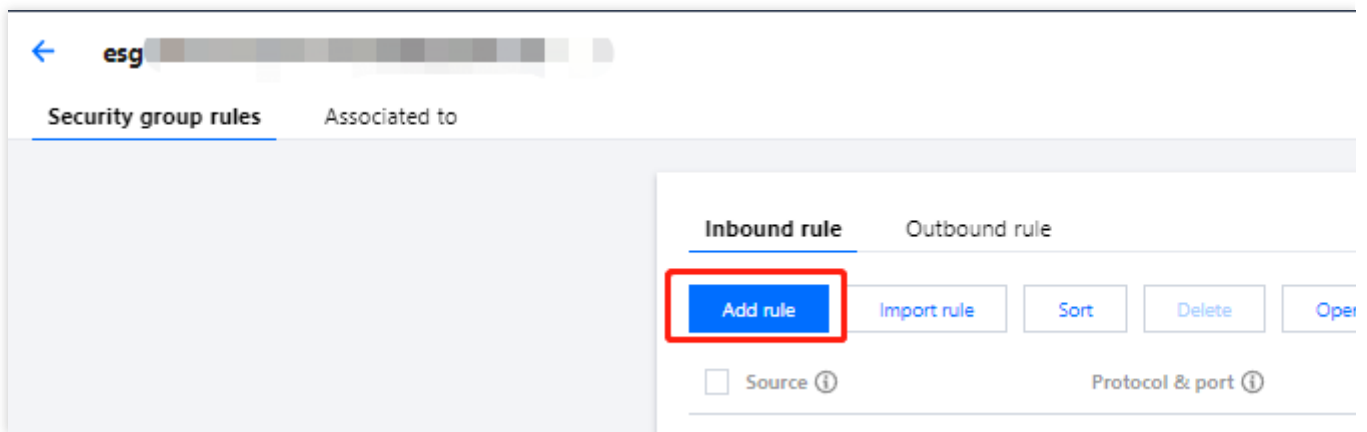
Directions

1. Log in to the ECM console and select **Edge Network** > [Security Group](#) on the left sidebar.
2. On the **Security Group** management page, select **Modify Rule** on the right of the target security group.
3. On the **Security Group Rule** tab, click **Inbound Rule** or **Outbound Rule** and select one of the following methods to add a rule:

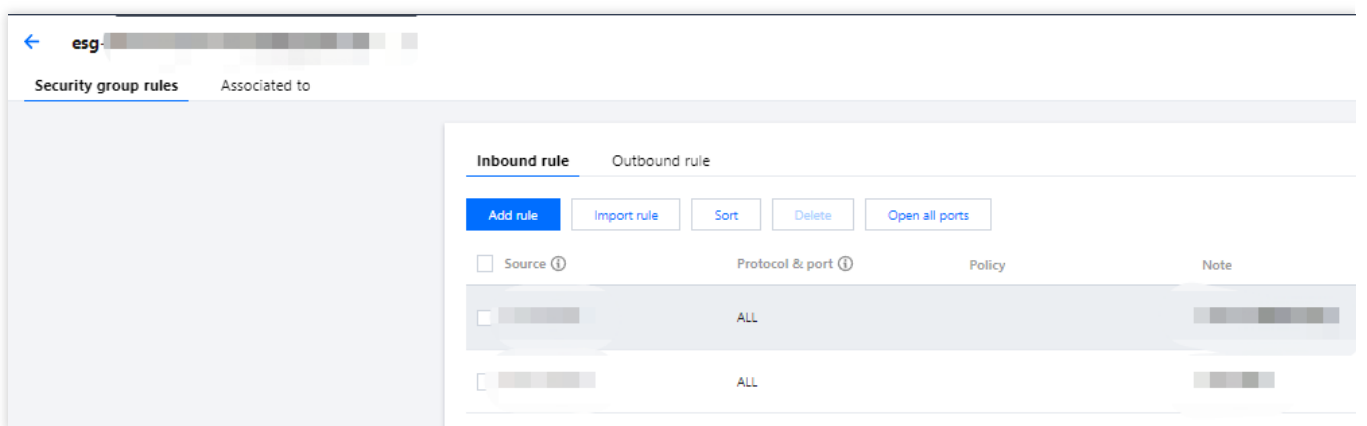
Method 1: click **Open all ports** and confirm the operation in the pop-up window. This method is ideal if you do not need custom ICMP rules and all traffic goes through ports 20, 21, 22, 80, 443, and 3389 and the ICMP protocol as shown below:



Method 2: click **Add Rule** and configure the rule in the pop-up window. For more information, see [step 5](#). This method is ideal if you need to set multiple communication protocols such as ICMP as shown below:



Method 3: on the security group rule page, you can modify inbound/outbound rules based on your needs. Select **Inbound Rule** or **Outbound Rule** and add a rule position as needed. Click **Insert > Insert Row Above** or **Insert Row Below** on the right of a rule and quickly configure it as instructed in [step 5](#) as shown below:



4. The main parameters for adding a rule are as detailed below:

Type: **Custom** is selected by default. You can also choose another system rule template including **Login Windows CVMs (3389)**, **Login Linux CVMs (22)**, **Ping, HTTP (80)**, **HTTPS (443)**, **MySQL (3306)**, and **SQL Server (1433)**.
Source or **Destination:** traffic source (inbound rules) or destination (outbound rules). You need to specify one of the following options:

Source/Destination	Description
A single IPv4 address or an IPv4 range	In CIDR notation, such as 203.0.113.0, 203.0.113.0/24 or 0.0.0.0/0, where 0.0.0.0/0 indicates all IPv4 addresses will be matched.

Protocol Port: enter the protocol type and port range such as **UDP:53** and **TCP:80,443**.

Policy: **Allow** or **Refuse**. **Allow** is selected by default.

Allow: traffic to this port is allowed.

Reject: data packets will be discarded without any response.

Notes: a short description of the rule for easier management.

5. Click **Complete**.

6. To add an outbound rule, click **Outbound Rule** and refer to [step 4](#) to [step 5](#).

Viewing Security Group Rule

Last updated : 2023-12-25 17:22:35

Overview

After adding a security group rule, you can view its details in the console.

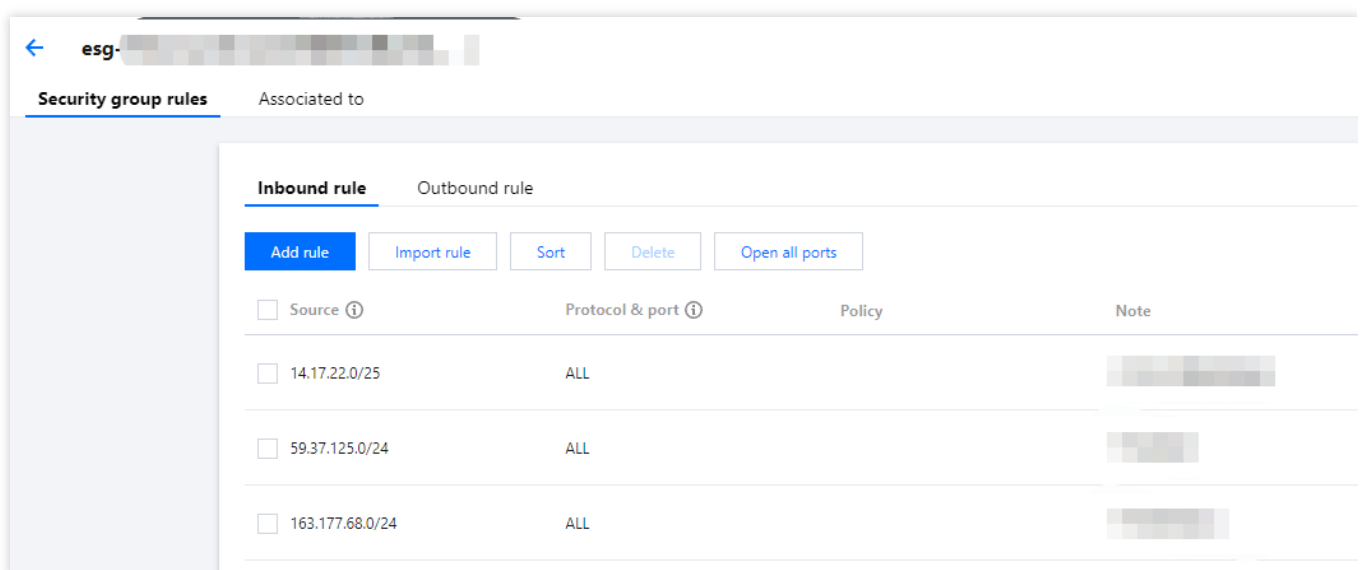
Prerequisites

You have created a security group and added at least one rule.

For information on how to create a security group and add security group rules to it, see [Creating a Security Group](#) and [Adding Security Group Rules](#).

Directions

1. Log in to the ECM console and select **Edge Network** > **Security Group** on the left sidebar.
2. On the **Security Group rule** management page, click the ID/name of the target security group or click **Modify Rule** on the right to enter the security group rule page.
3. On the security group rule page, click the **Inbound Rule** or **Outbound Rule** tab to view the inbound or outbound rules of the security group as shown below:



Modifying Security Group Rule

Last updated : 2023-12-25 17:23:29

Overview

This document describes how to modify a security group rule. Rules are important because they protect you ECM instance from malicious attacks. For example, they can protect certain ports from being abused.

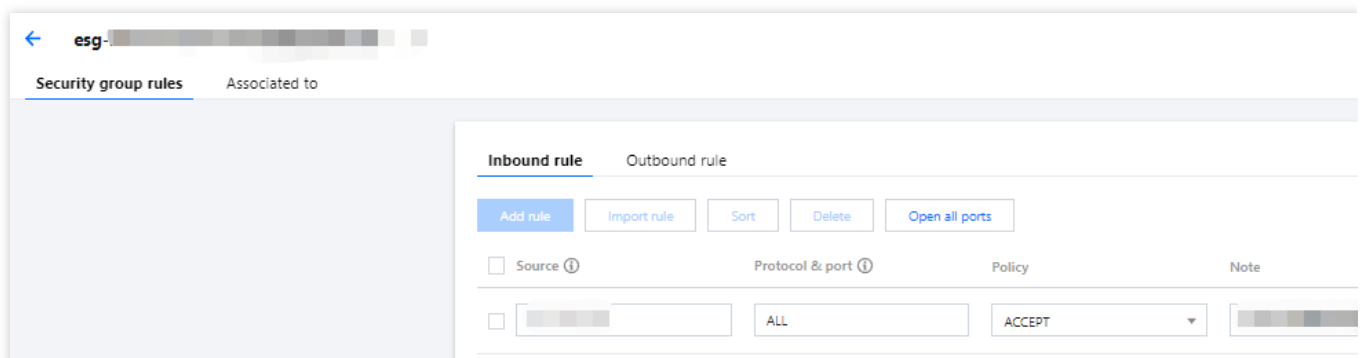
Prerequisites

You have created a security group and added at least one rule.

For information on how to create a security group and add security group rules to it, see [Creating a Security Group](#) and [Adding Security Group Rules](#).

Directions

1. Log in to the ECM console and select **Edge Network** > **Security Group** on the left sidebar.
2. On the **Security Group rules** management page, click the ID/name of the target security group or click **Modify Rule** on the right to enter the security group rule page.
3. Use **Inbound Rule** and **Outbound Rule** to switch between inbound and outbound security group rules.
4. Find the target rule and click **Edit** on the right.
5. You can modify the rule as instructed in [Rule Parameter Description](#) and click **Save** after modification as shown below:



Deleting Security Group Rule

Last updated : 2023-12-25 17:23:41

Overview

This document describes how to delete a security group rule that is no longer needed.

Prerequisites

You have created a security group and added at least one rule to it.

For information on how to create a security group and add security group rules to it, see [Creating a Security Group](#) and [Adding Security Group Rules](#).

You have confirmed the public or private networks whose access the ECM instance doesn't need to allow/reject.

Directions

1. Log in to the ECM console and select **Edge Network** > **Security Group** on the left sidebar.
 2. On the **Security Group** management page, click **Modify Rule** on the right of the security group rule to be deleted to enter the security group rule page.
 3. Use **Inbound Rule** and **Outbound Rule** to switch between inbound and outbound security group rules.
 4. Find the target rule and click **Delete** on the right.
- You can also select the boxes on the left of multiple rules and click **Delete** at the top of the page to batch delete them.
5. In the pop-up window, click **OK**.

Exporting Security Group Rule

Last updated : 2023-12-25 17:23:54

Overview

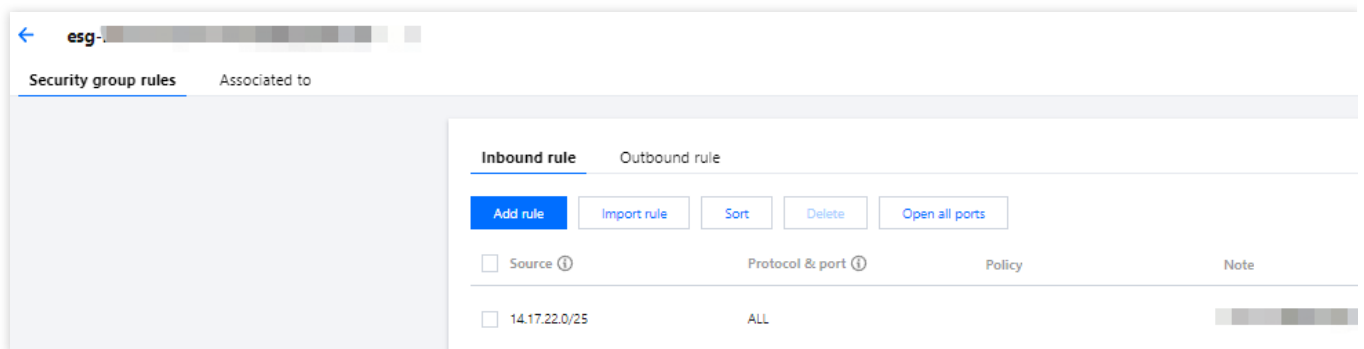
You can export security group rules and save them locally for backup.

Directions

1. Log in to the ECM console and select **Edge Network** > **Security Group** on the left sidebar.
2. On the **Security Group rules** management page, click the name or ID of the target security group to enter the security group rule page.
3. Use **Inbound Rule** and **Outbound Rule** to switch between inbound and outbound security group rules.
4. Click



to export security group rules to a file and save it to your local device as shown below:



Importing Security Group Rule

Last updated : 2023-12-25 17:24:09

Overview

Security group rules can be imported from a file. You can use this feature to quickly restore or create security group rules.

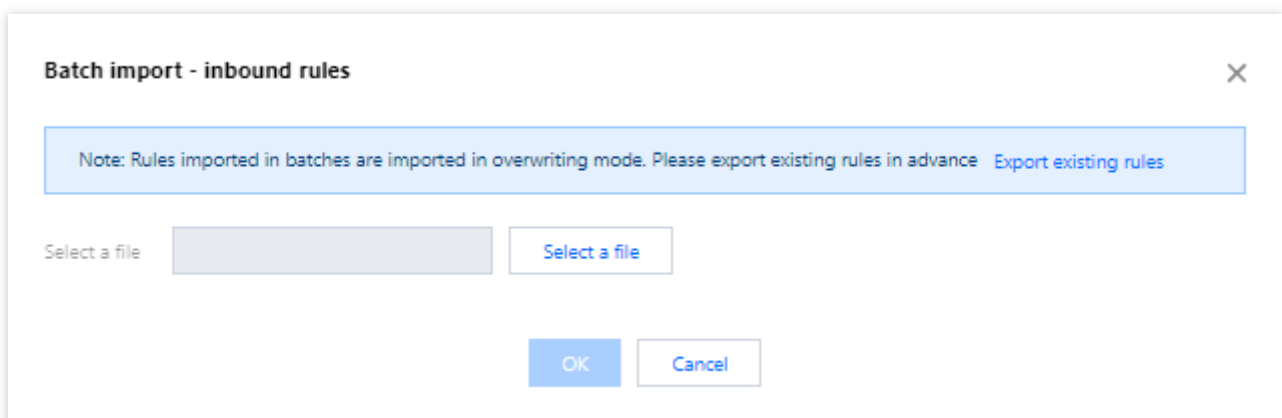
Directions

1. Log in to the ECM console and select **Edge Network** > **Security Group** on the left sidebar.
2. On the **Security Group** management page, click the ID/name of the target security group or click **Modify Rule** on the right to enter the security group rule page.
3. Use **Inbound Rule** and **Outbound Rule** to switch between inbound and outbound security group rules.
4. On the **Inbound Rule** or **Outbound Rule** tab, click **Import Rule**.
5. Click **Browse**, select a rule template file, and click **OK** as shown below:

Note:

As existing rules will be overwritten after importing, we recommend you export the existing rules before importing new ones.

If there are no existing rules in the security group, download a template and edit it before importing it.



After the import, a security group data record for ECM will be generated.

Security Group Use Cases

Last updated : 2023-12-26 10:07:43

By configuring security groups, you can manage access to an ECM instance. You can configure inbound and outbound rules for security groups to specify whether your instance can be accessed by or can access other network resources.

The default inbound and outbound rules for security groups are as follows:

To ensure data security, the inbound rule for a security group is a rejection policy that forbids remote access from external networks. To enable public access to your ECM instances, you need to open the corresponding port to the internet in the inbound rule.

The outbound rule for a security group specifies whether your ECM instance can access external network resources. If you select **Open all ports** or **Open ports 22, 80, 443, and 3389 and the ICMP protocol**, the outbound rule for the security group opens all ports to the Internet. If you select a custom security group rule, the outbound rule blocks all ports by default, and you need to configure the outbound rule to open the corresponding port to the Internet.

Common Use Cases

This document provides several common use cases of security groups. You can directly use its recommended security group configurations if a use case meets your requirements.

Scenario 1: remotely connecting to Linux ECM instance over SSH

Case: you have created a Linux ECM instance and want to remotely connect to it over SSH.

Solution: when [adding a security group rule](#), set **Type** to **Linux login** and open TCP port 22 to the Internet to enable Linux login via SSH.

You can open all IPs or a specified IP (or IP range) to the internet as required. This enables you to configure the source IPs that can remotely connect to the ECM instance over SSH.

Direction	Type	Source	Protocol Port	Policy
Inbound	Linux Login	All IP addresses: 0.0.0.0/0 Specified IP address: enter your specified IP address or IP range	TCP: 22	Allow

Scenario 2: remotely connecting to Windows ECM instance over RDP

Case: you have created a Windows ECM instance and want to remotely connect to it over RDP.

Solution: when [adding a security group rule](#), set **Type** to **Windows Login** and open TCP port 3389 to the Internet to

enable remote login to Windows.

You can open all IPs or a specified IP (or IP range) to the internet as required. This enables you to configure the source IPs that can remotely connect to the ECM instance over RDP.

Direction	Type	Source	Protocol Port	Policy
Inbound	Windows Login	All IP addresses: 0.0.0.0/0 Specified IP address: enter your specified IP address or IP range	TCP: 3389	Allow

Scenario 3: pinging server on internet

Case: you have created an ECM instance and want to test whether it can communicate with other ECM instances normally.

Solution: test the connection by using the `ping` command. Specifically, when [adding a security group rule](#), set **Type to Ping** and open Internet Control Message Protocol (ICMP) ports to the internet to enable other ECM instances to access this instance over ICMP.

You can open all IPs or a specified IP (or IP range) to the internet as required. This allows you to configure the source IP addresses that can access this ECM instance over ICMP.

Direction	Type	Source	Protocol Port	Policy
Inbound	Ping	All IP addresses: 0.0.0.0/0 Specified IP address: enter your specified IP address or IP range	ICMP	Allow

Scenario 4: remotely logging in to ECM instance over Telnet

Case: you want to remotely log in to an ECM instance over Telnet.

Solution: when [adding a security group rule](#), configure the following security group rule:

Direction	Type	Source	Protocol Port	Policy
Inbound	Custom	All IP addresses: 0.0.0.0/0 Specified IP address: enter your specified IP address or IP range	TCP: 23	Allow

Scenario 5: allowing access to a web service through HTTP or HTTPS

Case: you have built a website and want to allow access to your website through HTTP or HTTPS.

Solution: when [adding a security group rule](#), configure the following security group rules as required:

Allow all public IP addresses to access this website

Direction	Type	Source	Protocol Port	Policy
Inbound	HTTP (80)	0.0.0.0/0	TCP: 80	Allow
Inbound	HTTPS (443)	0.0.0.0/0	TCP: 443	Allow

Allow some public IP addresses to visit this website.

Direction	Type	Source	Protocol Port	Policy
Inbound	HTTP (80)	IP address or IP range that is allowed to access your website	TCP: 80	Allow
Inbound	HTTPS (443)	IP address or IP range that is allowed to access your website	TCP: 443	Allow

Scenario 6: allowing an external IP address to access a specified port

Case: you have deployed a service and want the specified service port (such as port 1101) to be externally accessible.

Solution: when [adding a security group rule](#), set **Type** to **Custom** and open TCP port 1101 to the Internet to allow external access to the specified service port.

You can open all IP addresses or a specified IP address (or IP range) to the Internet as required. This allows the source IP address to access the specified service port.

Direction	Type	Source	Protocol Port	Policy
Inbound	Custom	All IP addresses: 0.0.0.0/0 Specified IP address: enter your specified IP address or IP range	TCP: 1101	Allow

Scenario 7: rejecting an external IP address to access a specified port

Case: you have deployed a service and want to prevent external access to a specified service port (such as port 1102).

Solution: when [adding a security group rule](#), set **Type** to **Custom**, configure the TCP port 1102, and set **Policy** to **Reject** to reject external access to the specified service port.

Direction	Type	Source	Protocol Port	Policy
Inbound	Custom	All IP addresses: 0.0.0.0/0	TCP: 1102	Reject

		Specified IP address: enter your specified IP address or IP range		
--	--	---	--	--

Scenario 8: allowing ECM instance to access only specified external IP

Case: you want your ECM instance to access only a specified external IP address.

Solution: add two outbound security group rules as follows.

Allow the instance to access a specified external IP address.

Forbid the instance from accessing any public IP addresses through any protocol.

Note:

The first rule takes priority over the second.

Direction	Type	Source	Protocol Port	Policy
Outbound	Custom	Specified public IP address that the ECM instance can access	Required protocol and port number	Allow
Outbound	Custom	0.0.0.0/0	All	Reject

Scenario 9: prohibiting ECM instance from accessing specified external IP

Case: you don't want your ECM instance to access a specified external IP address.

Solution: add a security group rule as follows.

Direction	Type	Source	Protocol Port	Policy
Outbound	Custom	Specified public IP address that your instance cannot access	All	Reject

Scenario 10: uploading or downloading a file over FTP

Case: you want to allow uploads and downloads over FTP.

Solution: add a security group rule as follows.

Direction	Type	Source	Protocol Port	Policy
Inbound	Custom	0.0.0.0/0	TCP: 20 to 21	Allow

Multi-Scenario Configurations

You can configure multiple security group rules to meet your business requirements. For example, both inbound and outbound rules can be simultaneously configured. An ECM instance can be bound to one or multiple security groups.

When it is bound to multiple security groups, the security group rules will be matched sequentially from top to bottom. You can adjust the priorities of security groups at any time. For more information about the priorities, see [Rule Priorities](#).

Common Server Ports

Last updated : 2023-12-25 17:24:35

The following describes common server ports. For more information about service application ports for Windows, see Microsoft's official documentation ([Service overview and network port requirements for Windows](#)).

Port Number	Service	Description
21	FTP	An open FTP server port for uploading and downloading.
22	SSH	Port 22 is the SSH port. It is used to remotely connect to Linux servers in CLI mode.
25	SMTP	SMTP server's open port for sending emails.
80	HTTP	This port is used for web services such as IIS, Apache, and Nginx to provide external access.
110	POP3	Port 110 is open for the POP3 (email protocol 3) service.
137, 138, 139	NetBIOS protocol	Ports 137 and 138 are UDP ports for transferring files via My Network Places. Port 139: connections over port 139 attempt to access the NetBIOS/SMB service. This protocol is used for file and printer sharing on Windows and SAMBA.
143	IMAP	Port 143 is mainly used for Internet Message Access Protocol (IMAP) v2, a protocol for receiving emails akin to POP3.
443	HTTPS	Web browsing port. This is another type of HTTP that provides encryption and transmission over secure ports.
1433	SQL Server	Port 1433 is the default port for SQL Server. The SQL Server service uses two ports: TCP-1433 and UDP-1434. Port 1433 is used for SQL Server to provide external services, while port 1434 is used to respond to the requester which TCP/IP port is used by SQL Server.
3306	MySQL	Port 3306, the default port for MySQL databases, is used by MySQL to provide external services.
3389	Windows Server Remote Desktop Services	Port 3389 is the service port for the Windows Server remote desktop, through which you can connect to a remote server by using the "Remote Desktop" connection tool.
8080	Proxy	Similar to port 80, port 8080 is used for WWW proxy service for web browsing. Port

	port	number ":8080" is often appended to the URL when the user visits a website or uses a proxy server. In addition, port 8080 is the default service port after the Apache Tomcat web server is installed.
--	------	--

Managing Image

Last updated : 2023-12-26 10:09:22

Overview

ECM provides public images, each of which contains the basic OS and initial components offered by Tencent Cloud for all users. If you want to quickly create multiple instances with the same configuration and applications, you can use the image creation feature to create a custom image and use it to create instances. ECM also allows you to import a custom image from the central cloud AZ to ECM instances. This document describes how to import and manage an image in the console.

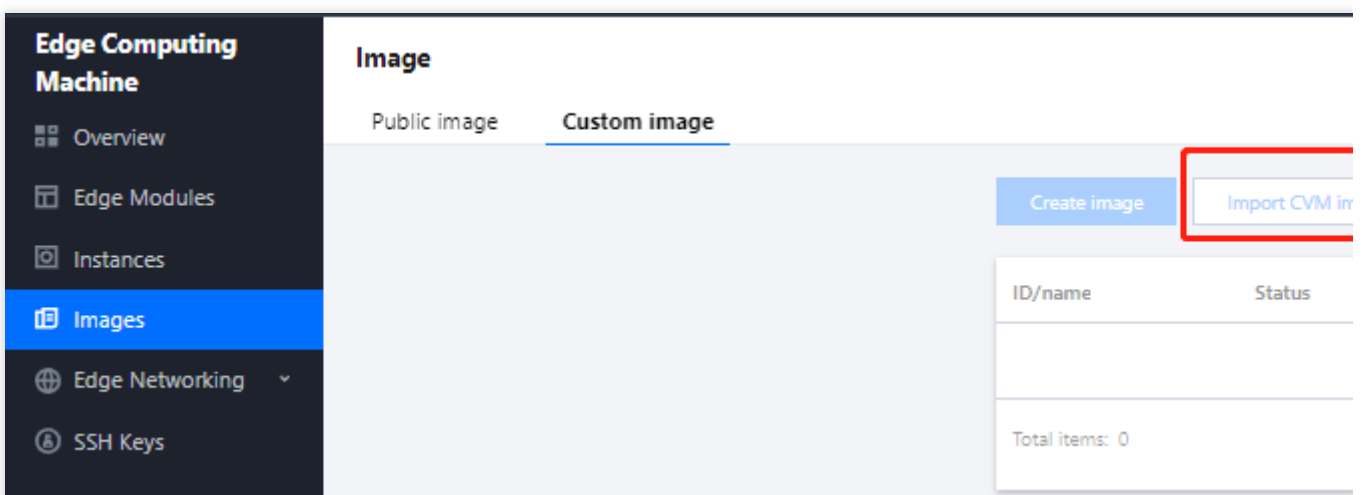
Prerequisites

You have created a custom image in the central cloud (i.e., CVM) AZ.

Directions

Importing image

1. Log in to the [ECM console](#).
2. On the left sidebar, select **Image**.
3. On the image page, click **Import CVM Image** as shown below:



4. In the pop-up window, select the region, OS, system architecture, and ID/name of the image to be imported and click **OK**.

Note:

ECM currently can retain up to 10 custom images.

After the import succeeds, the CVM data will be synced to ECM.

Deleting image

1. Log in to the [ECM console](#).
2. On the left sidebar, select **Image**.
3. On the image page, select the image to be deleted and click **Delete** in the **Operation** column .

Note:

Before performing this operation, check whether there is any ECM module using this image, and if so, it cannot be deleted.

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

Editing Tag

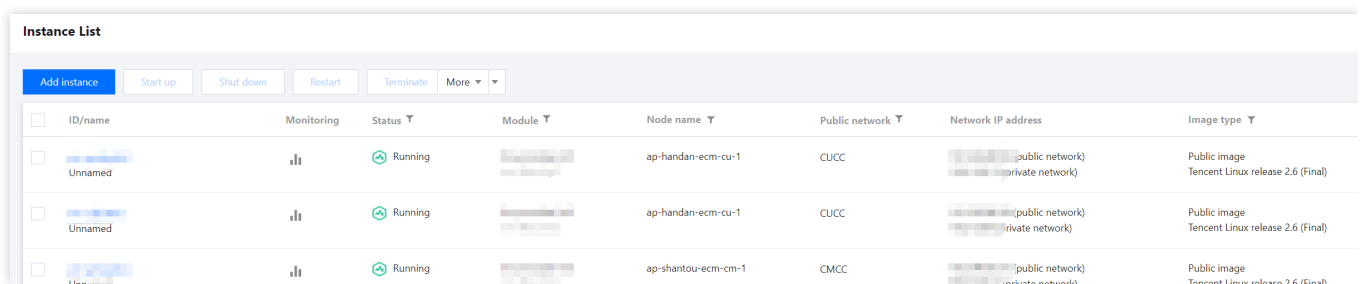
Last updated : 2023-12-25 17:25:01

Overview

Tags can help you easily categorize and manage ECM resources in many dimensions such as business, purpose, and owner. This document describes how to add a tag to an ECM instance in the ECM console.

Directions


1. Log in to the [ECM console](#).
2. On the left sidebar, select **Instance List**.
3. On the instance list page, select the target instance and click **More > Edit Tag**.



ID/name	Monitoring	Status	Module	Node name	Public network	Network IP address	Image type
Unnamed		Running		ap-handan-ecm-cu-1	CUCC	(public network) (private network)	Public image Tencent Linux release 2.6 (Final)
Unnamed		Running		ap-handan-ecm-cu-1	CUCC	(public network) (private network)	Public image Tencent Linux release 2.6 (Final)
Unnamed		Running		ap-shantou-ecm-cm-1	CMCC	(public network) (private network)	Public image Tencent Linux release 2.6 (Final)

4. In the pop-up window, enter a tag key and value as needed and click **OK**.

Edit Tags

The tag is used to manage resources by category from different dimensions. If the tag does not meet your requirements, please go to [Manage Tags](#) 

1 resource selected

Tag key ▼	Tag value ▼	✕
-----------	-------------	---

[+ Add](#)

OK	Cancel
----	--------

EIP Direct Access

Last updated : 2023-12-25 17:25:15

Overview

When you create an ECM instance, EIP direct access is configured by default. If your ECM instance is not configured with EIP direct access, you can run the EIP direct access script for configuration. This document describes how to configure an EIP direct access script for an ECM instance and how to restore the script if you delete it by mistake.

Notes

Currently, you can configure EIP direct access only for Linux instances.
The EIP direct access script must run on CentOS 6 or above or Ubuntu.

Prerequisites

You have created an ECM instance and obtained its public IP.
You have obtained the instance admin account and password.
Both the private IP and EIP of the Linux instance are on the primary ENI (eth0).
If the public IP bound to the primary ENI is not an EIP, you need to convert it to an EIP first.

Directions

Downloading EIP direct access script

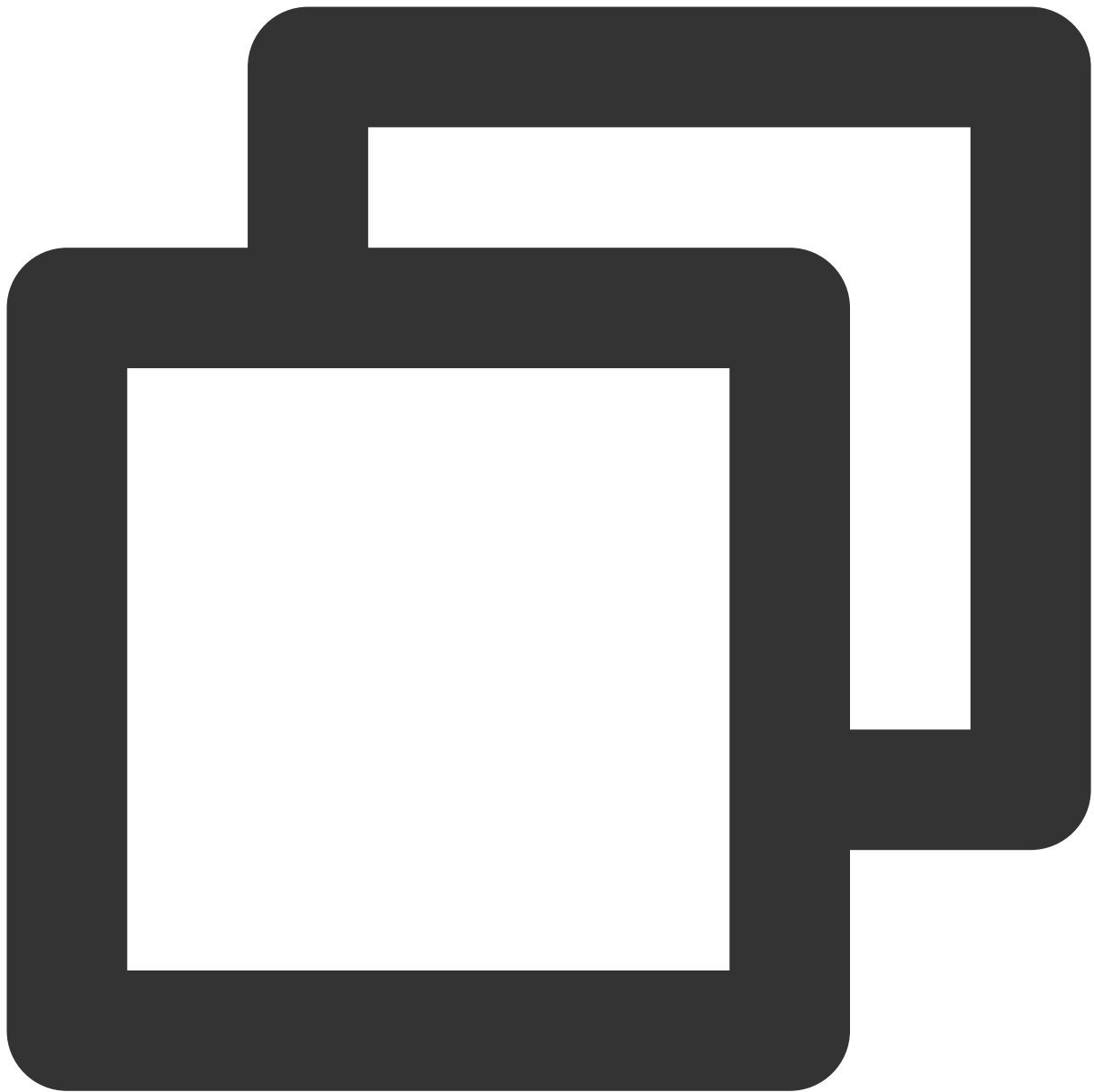
As EIP direct access will interrupt network connection, you need to select a method to save the EIP direct access script to the ECM instance first.

Method 1: upload the script for EIP direct access

- 1.1 Download the EIP direct access script to the local PC.
- 1.2 Upload the downloaded script to the ECM instance requiring EIP direct access.

Method 2: use the command directly

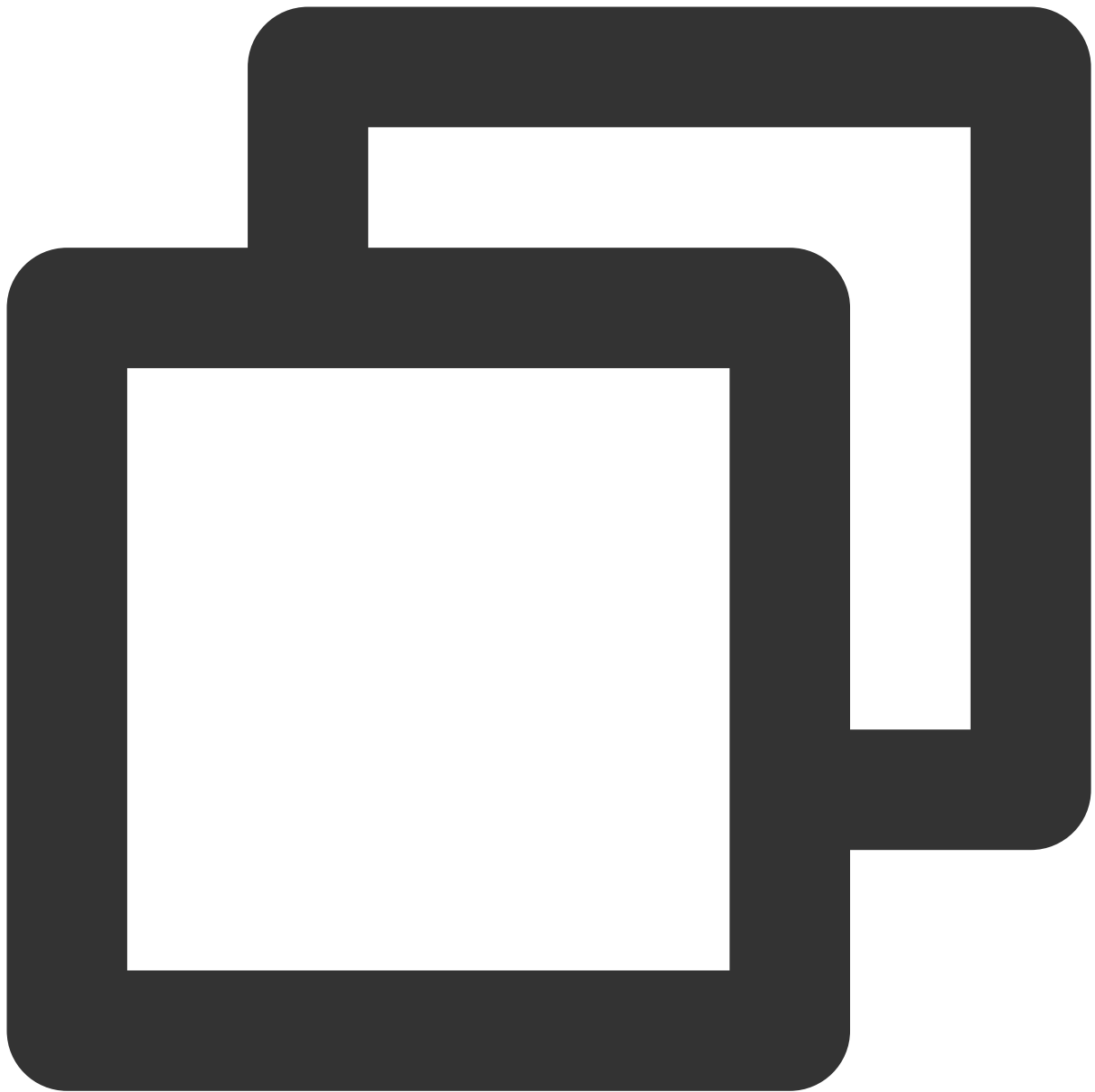
Log in to the ECM instance and run the following command to download the EIP direct access script:



```
wget https://eip-direct-1254277469.cos.ap-guangzhou.myqcloud.com/eip_direct.sh
```

Running EIP direct access script

1. [Log in to a Linux instance.](#)
2. Run the following command to grant the execution permission:



```
chmod +x eip_direct.sh
```

3. Run the following command to run the script:



```
./eip_direct.sh install XX.XX.XX.XX
```

Here, `XX.XX.XX.XX` is the EIP address, which is optional. You can also directly run `./eip_direct.sh install` without entering the address.

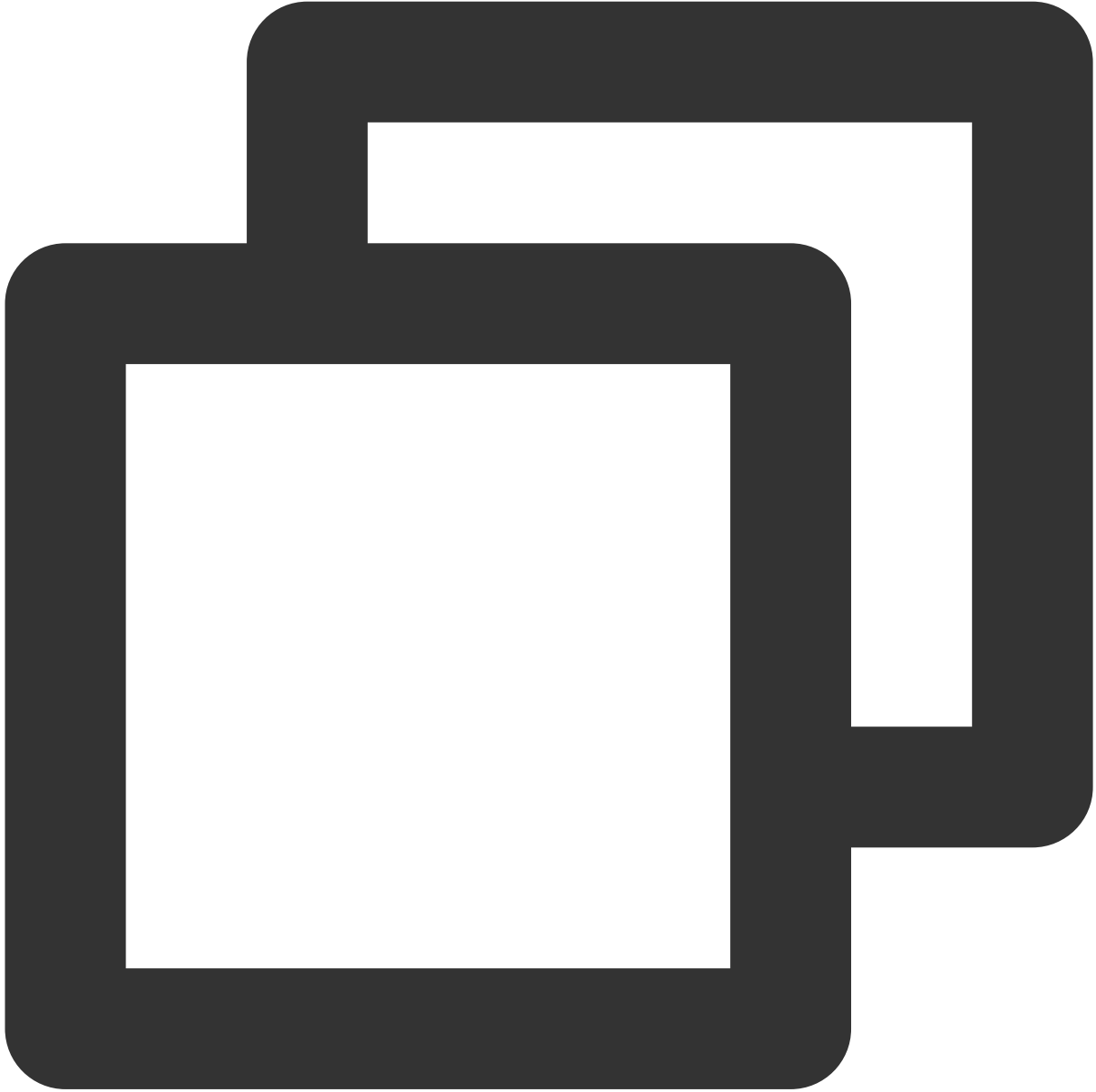
Appendix

If you delete the EIP direct access script by mistake, you can restore it as follows:

1. Upload/Download the EIP direct access script to the ECM instance.

For more information, see [Downloading EIP direct access script](#).

2. Log in to the instance and run the following command to restart it:



```
reboot
```