ALIBABA CLOUD

Alibaba Cloud

云企业网

User Guide

Document Version: 20220511

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Manage CEN instances

1.1. Create a CEN instance

This topic describes how to create a Cloud Enterprise Network (CEN) instance for internal network communication. When you create a CEN instance, you can attach network instances under the same account to the CEN instance.

Procedure

1. Log on to the CEN console.
2. On the **Instances** page, click **Create CEN Instance**.
3. On the **Create CEN Instance** page, set the parameters, and then click **OK**. The following table describes the parameters.

Configuration	Description
Name	Enter a name for the CEN instance. The name must be 2 to 128 characters in length. It can contain letters, numbers, hyphens (-), and underscores (_). It must start with an English letter, but cannot start with `http://` or `https://`.
Description	Enter a description for the CEN instance. The description must be 2 to 256 characters in length. It cannot start with `http://` or `https://`.
Attach Network	You can attach network instances under the same account to the CEN instance. For more information, see Attach a network instance.

1.2. Delete a CEN instance

This topic describes how to delete a Cloud Enterprise Network (CEN) instance. After you delete a CEN instance, network instances cannot be attached to the CEN instance.

Prerequisites

No bandwidth package or network instance exists under the CEN instance.

- If a network instance is attached to the CEN instance, detach the network instance first. For more information, see Detach a network instance.
- If a bandwidth package is associated with the CEN instance, disassociate the bandwidth package first. For more information, see Disassociate a bandwidth plan from a CEN instance.

Procedure

1. Log on to the CEN console.
2. On the **Instances** page, find the target CEN instance, and then click **Delete** in the **Actions** column.
3. In the **Delete CEN Instance** dialog box, click **OK**.

2.Manage networks

2.1. Attach a network instance to a CEN instance

This page will no longer be maintained and will be removed. For more information, see Manage network instances.

2.2. Attach a network instance

This page will no longer be maintained and will be removed. For more information, see Manage network instances.

2.3. Detach a network instance

This page will no longer be maintained and will be removed. For more information, see Manage network instances.

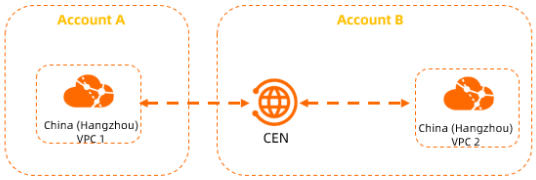
2.4. Manage network instances

After you create a Cloud Enterprise Network (CEN) instance, you can connect the CEN instance to virtual private clouds (VPCs), virtual border routers (VBRs), and Cloud Connect Network (CCN) instances to enable network communication. After you attach network instances to a CEN instance, the CEN instance automatically learns routes of the attached network instances. Then, the network instances can communicate with each other.

Background information

- You can use CEN to connect network instances that belong to the same Alibaba Cloud account or different Alibaba Cloud accounts.

  As shown in the following figure, Account B created a CEN instance. You can attach VPC 1 that belongs to Account A and VPC 2 that belongs to Account B to the same CEN instance to enable network communication between VPC 1 and VPC 2.



- You can use one of the following methods to attach a network instance to a CEN instance:
  - Attach a network instance
  - Attach a network instance to a CEN instance
- If the CEN instance and the network instance that you want to attach to the CEN instance belong to different Alibaba Cloud accounts, you must log on to the network instance and grant the required permissions to the CEN instance. For more information, see Grant permissions on a network instance

that belongs to another account.

> **Notice** After the CEN instance acquires the required permissions, Account B can attach the network instance that belongs to Account A to the CEN instance. Then, the network instance that belongs to Account B and the network instance that belongs to Account A can communicate with each other.

Prerequisites

- A CEN instance is created. For more information, see Create a CEN instance.
- The network instance is not attached to other CEN instances.

Attach a network instance

1. Log on to the CEN console.
2. On the **Instances** page, find the CEN instance that you want to manage and click **Manage** in the **Actions** column.
3. Click the **Networks** tab and then click **Attach Network**.
4. In the **Attach Network** panel, click the **Your Account** or **Different Account** tab, set the following parameters, and then click **OK**.
   - Attach a network instance that is created by the current account
     - **Network Type**: Select the type of network instance.
     - **Region**: Select the region where the network instance is created.
     - **Networks**: Select the network instance that you want to attach.
   - Attach a network instance that is created by a different account
     - **Owner Account**: Enter the ID of the account to which the network instance belongs.
     - **Network Type**: Select the type of network instance.
     - **Region**: Select the region where the network instance is created.
     - **Networks**: Select the network instance that you want to attach.

Attach a network instance to a CEN instance

◉Attach a VPC to a CEN instance○Attach a VBR to a CEN instance○Attach a CCN instance to a CEN instance

1. Log on to the VPC console.
2. In the top navigation bar, select the region where the VPC is deployed.
3. On the **VPCs** page, find the VPC that you want to attach and click the ID of the VPC.
4. On the details page of the VPC, click **Attach to CEN**.
5. In the **Attach to CEN** panel, select the CEN instance to which you want to attach the VPC and click **OK**.

1. Log on to the Express Connect console.
2. In the top navigation bar, select the region where the VBR is created.
3. In the left-side navigation pane, click **Virtual Border Routers (VBRs)**.
4. On the details page of the VBR, click the **Basic Information** tab, and then click **Join CEN**.

5. In the **Join CEN** panel, select the CEN instance to which you want to attach the VBR and click **OK**.

1. Log on to the SAG console.
2. In the top navigation bar, select the region where the CCN instance is deployed.
3. In the left-side navigation pane, click **CCN**.
4. On the **CCN** page, find the CCN instance that you want to attach and click **Bind CEN Instance** in the **Actions** column.
5. In the **Bind CEN Instance** panel, select the CEN instance you want to attach and click **OK**.

   You can use one of the following methods to specify a CEN instance:

   - **Existing CEN**: If you have created CEN instances, you can select an existing CEN instance from the drop-down list.
   - **Create CEN**: If you have not created a CEN instance, enter an instance name. The system then creates a CEN instance and automatically associates it with the CCN instance.

     The name must be 2 to 128 characters in length, and can contain letters, digits, hyphens (-), and underscores (_). It must start with a letter.

Grant permissions on a network instance that belongs to another account

If the CEN instance and the network instance that you want to attach to the CEN instance belong to different Alibaba Cloud accounts, you must log on to the network instance and grant the required permissions to the CEN instance. Before you grant permissions to the CEN instance, obtain the Alibaba Cloud account ID to which the network instance belongs and the Alibaba Cloud account ID to which the CEN instance belongs.

Grant permissions on a VPC

The following steps show how to attach a VPC that belongs to Account A to a CEN instance that belongs to Account B. The CEN instance must first acquire the required permissions from the VPC.

1. Log on to the VPC console with Account A.
2. In the top navigation bar, select the region where the VPC is deployed.
3. On the **VPCs** page, find the VPC that you want to attach and click the ID of the VPC.
4. On the **Authorize Cross Account Attach CEN** tab, click **Authorize Cross Account Attach CEN**.
5. In the **Attach to CEN** dialog box, set the following parameters and click **OK**.

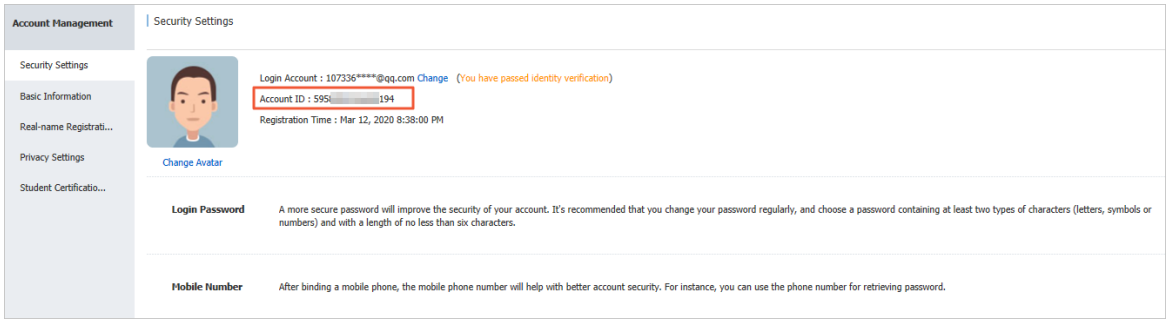
Parameter	Description
Peer Account UID	Enter the ID of the Alibaba Cloud account to which the CEN instance belongs. In this example, the ID of Account B is used.
Peer Account CEN ID	Enter the ID of the CEN instance.

Parameter	Description
Payer	Select the account that pays the fees. ○ **CEN Instance Owner**: The account to which the CEN instance belongs pays the connection fee and data transfer fee. This is the default value. ○ **VPC Owner**: The account to which the VPC belongs pays the connection fee and data transfer fee. **Note** This parameter takes effect only if you use an Enterprise Edition transit router to connect the VPC to the CEN instance in the latest console version.

After you complete the configuration, click OK to grant the permissions. You can view the permission information on the **Authorize Cross Account Attach CEN** tab.

6. Record the ID of Account A and the ID of the network instance for further operations.

   You canview the account ID on the Account Center page.



Grant permissions on a VBR

The following steps show how to attach a VBR that belongs to Account A to a CEN instance that belongs to Account B. The CEN instance must first acquire the required permissions from the VBR.

Notice By default, VBRs cannot grant permissions to CEN instances that belong to another Alibaba Cloud account. You must submit a ticket.

1. Log on to the Express Connect console with Account A.
2. In the top navigation bar, select the region where the VBR is created.
3. In the left-side navigation pane, click **Virtual Border Routers (VBRs)**.
4. On the **Virtual Border Routers (VBRs)** page, click the ID of the VBR that you want to attach.
5. Click the **CEN Authorization** tab, and then click **Authorize CEN of Another Account to Load Instance**.
6. In the **Authorize CEN of Another Account to Load Instance** panel, set the following parameters and click **OK**.

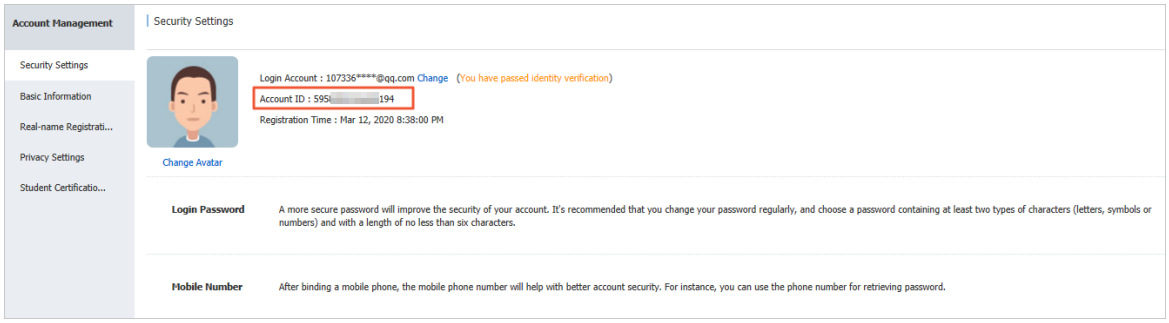
Parameter	Description
Peer Account UID	Enter the ID of the Alibaba Cloud account to which the CEN instance belongs. In this example, the ID of Account B is used.

Parameter	Description
Peer Account CEN ID	Enter the ID of the CEN instance.
Payer	Select the account that pays the fees. ○ **CEN Instance Owner**: The account to which the CEN instance belongs pays the connection fee and data transfer fee. This is the default value. ○ **VBR Owner**: The account to which the VBR belongs pays the connection fee and data transfer fee. **Note** This parameter takes effect only if you use an Enterprise Edition transit router to connect the VBR to the CEN instance in the latest console version.

After you complete the configuration, click OK to grant the permissions. You can view the permission information on the **CEN Authorization** tab.

7. Record the ID of Account A and the ID of the network instance for further operations.

   You canview the account ID on the Account Center page.



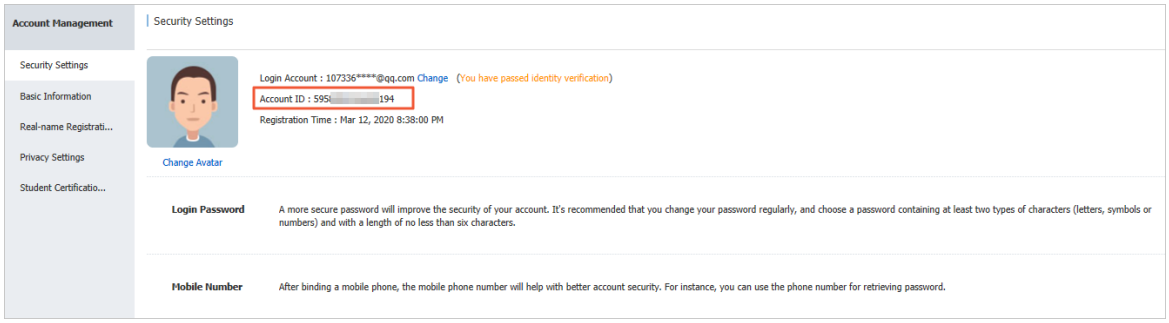
Grant permissions on a CCN instance

The following steps show how to attach a CCN instance that belongs to Account A to a CEN instance that belongs to Account B. The CEN instance must first acquire the required permissions from the CCN instance.

1. Log on to the SAG console with Account A.
2. In the top navigation bar, select the region where the CCN instance is deployed.
3. In the left-side navigation pane, click **CCN**.
4. On the **CCN** page, click the ID of the CCN instance that you want to attach.
5. On the details page of the CCN instance, click the **CEN Cross Account Authorization Information** tab. On the tab, click **CEN Cross Account Authorization**.
6. In the **Attach to CEN** dialog box, enter the ID of Account B and the ID of the CEN instance and click **OK**.

   After you complete the configuration, click OK to grant the permissions. You can view the permission information on the **CEN Cross Account Authorization Information** tab.
7. Record the ID of Account A and the ID of the network instance for further operations.

   You canview the account ID on the Account Center page.



Detach a network instance

You can detach a network instance from a CEN instance. After the network instance is detached, it cannot communicate with other network instances that are attached to the CEN instance.

1. Log on to the CEN console.
2. On the **Instances** page, find the CEN instance that you want to manage and click **Manage** in the **Actions** column.
3. On the **Networks** tab, find the network instance that you want to detach and click **Detach** in the **Actions** column.
4. In the **Detach Network** message, click **OK**.

References

- For more information about how to attach a network instance to a CEN instance, see AttachCenChildInstance.
- For more information about how to query network instances that are attached to a CEN instance, see DescribeCenAttachedChildInstances.
- For more information about how to query regions that allow you to attach network instances to CEN instances, see DescribeChildInstanceRegions.
- For more information about how to query network instances of other Alibaba Cloud accounts that have granted permissions to a CEN instance, see DescribeGrantRulesToCen.
- For more information about how to grant a CEN instance permissions on a VPC, see GrantInstanceToCen.
- For more information about how to grant a CEN instance permissions on a VPC that belongs to another Alibaba Cloud account, see GrantInstanceToCbn.
- For more information about how to detaches a network instance from a CEN instance, see DetachCenChildInstance.

3.Bandwidth package management

3.1. Use a bandwidth plan

To connect network instances in different regions, you must purchase a Cloud Enterprise Network (CEN) bandwidth plan and allocate bandwidth for cross-region communication. Network instances in the same region can communicate with each other after they are attached to the same CEN instance. You do not need to purchase a bandwidth plan.

Purchase a bandwidth plan

1.
2.
3. On the details page of the CEN instance, click the **Bandwidth Plans** tab, and then click **Purchase Bandwidth Plan(Subscription)**.
4.
5.

Disassociate a bandwidth plan from a CEN instance

After you purchase a bandwidth plan, the system automatically associates it with the CEN instance. You can disassociate a bandwidth plan from a CEN instance and associate the bandwidth plan with another CEN instance.

Before you disassociate a bandwidth plan, make sure that the cross-region connections that are associated with the bandwidth plan are deleted. For more information, see Delete bandwidth for cross-region connections.

1.
2.
3. On the details page of the CEN instance, click the **Bandwidth Plans** tab, find the bandwidth plan that you want to disassociate, and then click **Unbind** in the **Actions** column.
4. In the **Disassociate from Bandwidth Plan** message, confirm the bandwidth plan that you want to disassociate and click **OK**.

   You are still charged for disassociated bandwidth plans. The billing of a bandwidth plan stops only after you delete the bandwidth plan. For more information, see .

Associate a bandwidth plan with a CEN instance

After you disassociate a bandwidth plan from a CEN instance, you can associate the bandwidth plan with another CEN instance.

1.
2.
3. On the details page of the CEN instance, click the **Bandwidth Plans** tab, find the bandwidth plan that you want to associate, and then click **Bind** in the **Actions** column.
4. In the **Associate with Bandwidth Plan** message, confirm the bandwidth plan that you want to associate and click **OK**.

References

- Resize a subscription bandwidth plan
- CreateCenBandwidthPackage: creates a bandwidth plan.
- AssociateCenBandwidthPackage: associates a bandwidth plan with a CEN instance.
- UnassociateCenBandwidthPackage: disassociates a bandwidth plan from a CEN instance.
- DescribeCenBandwidthPackages: queries bandwidth plans.

3.2. Associate a bandwidth plan with a CEN instance

The content on this page has been moved. For more information, see Associate a bandwidth plan with a CEN instance. This page will be discontinued and will no longer be maintained.

3.3. Disassociate a bandwidth plan from a CEN instance

The content on this page has been moved. For more information, see Disassociate a bandwidth plan from a CEN instance. This page will be discontinued and will no longer be maintained.

3.4. Resize and renew a bandwidth plan

Cloud Enterprise Network (CEN) allows you to upgrade, downgrade, or renew a bandwidth plan. You can modify the bandwidth value or extend the subscription period of a bandwidth plan based on your business requirements. This topic describes the rules and operations.

Resize a bandwidth plan

After you upgrade or downgrade a bandwidth plan, the new bandwidth value immediately takes effect. Take note of the following rules for upgrades and downgrades:

- **Upgrade rules**

  Upgrade fee = Cost of the upgraded plan - Cost of the original plan

  - Cost of the upgraded plan = Hourly price (Monthly price of the upgraded plan/Number of calendar days in the month/24 hours) × Remaining subscription duration in hours
  - Cost of the original plan = Hourly price (Monthly price of the original plan/Number of calendar days in the month/24 hours) × Remaining subscription duration in hours

  Examples

  On May 1, Alice purchased a subscription bandwidth plan of 2 Mbit/s for three months. The bandwidth plan enables network communication between regions inside the Chinese mainland. In the following examples, one month equals 30 days. The monthly price of the bandwidth plan is USD 68. In this case, the fee for a three-month subscription is USD 204.

  One month later, Alice upgraded the bandwidth plan to 4 Mbit/s. The monthly price of a 4 Mbit/s bandwidth plan is USD 136. In this case, the upgrade fee is USD 136. The system calculates the upgrade fee based on the following formula:

Upgrade fee = Hourly price of the upgraded plan (USD 136/30 days/24 hours) × 2 months (60 days × 24 hours) - Hourly price of the original plan (USD 68/30 days/24 hours) × 2 months (60 days × 24 hours) = USD 136.

- **Downgrade rules**

  For more information, see Refund rules for real-time configuration downgrade.

1.
2.
3. On the details page of the CEN instance, click the **Bandwidth Plans** tab, find the bandwidth plan that you want to resize, and then click **Downgrade** or **Upgrade** in the **Bandwidth** column.
4. Set the **Bandwidth** parameter based on your business requirements.
5.

Renew a bandwidth plan

1.
2.
3. On the details page of the CEN instance, click the **Bandwidth Plans** tab, find the bandwidth plan that you want to renew, and then click **Renew** in the **Actions** column.
4. On the **Renew** page, set **Duration**.
5.

In the Billing Management console, you can select manual renewal, auto-renewal, or non-renewal for a bandwidth plan. Before you renew a bandwidth plan, take note of the following rules:

- Expired bandwidth plans support only manual renewal. Auto-renewal and non-renewal are not supported.
- A bandwidth plan that is about to expire within one day supports manual renewal and non-renewal. Auto-renewal is not supported.

1.
2. In the top navigation bar, choose **Expenses > Renewal Management**.
3. In the **Instances** section, Select **CEN Bandwidth Plan**.
4. On the **Manual** tab, find the bandwidth plan and select a renewal method.
   - If you want to manually specify a subscription duration, click **Renew**, specify a subscription duration, select the service agreement check box, and then complete the payment.
   - If you want to enable auto-renewal for a bandwidth plan, click **Enable Auto Renewal**. In the **Enable Auto Renewal** dialog box, select a subscription duration, and click **Auto Renew**.

     > **Note**
     > - After you enable auto-renewal, the auto-renewal feature takes effect the next day.
     > - After auto-renewal is enabled, the system automatically deducts fees from your account balance nine days before your instance expires. Make sure that you have a sufficient balance in your payment account. Auto-renewal supports coupons.

   - If you no longer want to renew a bandwidth plan, click **Nonrenewal**. In the **Set as Nonrenewal** message, click **OK**.

> **Note** After you disable renewal for a bandwidth plan, you will receive only one notification before the bandwidth plan expires. When the subscription duration ends, the bandwidth plan automatically expires. You can change the renewal mode of the bandwidth plan before it expires.

Renew a bandwidth plan in the CEN console

Renew a bandwidth plan in the Billing Management console

3.5. Renew a bandwidth plan

The content on this page has been moved. For more information, see Renew a bandwidth plan. This page will be discontinued and will no longer be maintained.

4.Manage cross-region connection bandwidth

4.1. Manage bandwidth for cross-region connections

To connect network instances in different regions, you must purchase a bandwidth plan and set bandwidth for cross-region connections.

Prerequisites

A bandwidth plan is purchased. For more information, see Purchase a bandwidth plan.

Context

After you attach network instances to a Cloud Enterprise Network (CEN) instance, the system allocates 1 Kbit/s of bandwidth for cross-region connections. You can use the bandwidth to test the connectivity of IPv4 networks. To ensure that your workloads run as expected, purchase a bandwidth plan and set cross-region bandwidth.

The sum of all bandwidth values in different regions cannot exceed the bandwidth value of the bandwidth plan. For example, a CEN instance is associated with a 20 Mbit/s bandwidth plan that connects the Chinese mainland to North America. You can set bandwidth for cross-region connections between the US (Silicon Valley) region and regions in the Chinese mainland such as China (Hangzhou), China (Shanghai), and China (Shenzhen). However, the sum of these bandwidth values cannot exceed 20 Mbit/s.

Configure bandwidth for cross-region connections

1.
2.
3.
4. Click the **Region Connections** tab, and then click **Set Region Connection**.
5. In the **Set Region Connection** panel, set the following parameters and click **OK**.

Parameter	Description
Bandwidth Plans	Select a bandwidth plan.
Connected Regions	Select the regions that you want to connect.
Bandwidth	Enter a bandwidth value for the cross-region connection. Unit: Mbit/s.

Modify bandwidth for cross-region connections

1.

2.
3.
4. On the **Region Connections** tab, find the cross-region connection that you want to manage and click **Modify** in the **Bandwidth** column.
5. In the **Set Region Connection** dialog box, set a new bandwidth value for the cross-region connection and click **OK**.

Delete bandwidth for cross-region connections

1.
2.
3.
4. On the **Region Connections** tab, find the cross-region connection that you want to delete and click **Delete** in the **Actions** column.
5. In the **Delete Region Connection** message, click **OK**.

References

- SetCenInterRegionBandwidthLimit: sets, modifies, or deletes bandwidth for cross-region connections between two regions.
- DescribeCenInterRegionBandwidthLimits: queries bandwidth for cross-region connections among different regions.

4.2. Modify bandwidth for cross-region connections

The content on this page has been moved. For more information, see Modify bandwidth for cross-region connections. This page will be discontinued and will no longer be maintained.

4.3. Delete bandwidth for cross-region connections

The content on this page has been moved. For more information, see Delete bandwidth for cross-region connections. This page will be discontinued and will no longer be maintained.

5.Manage routes

5.1. Enable overlapping routing

Cloud Enterprise Network (CEN) automatically learns the routes of the network instances that are attached to a CEN instance. If the destination CIDR blocks of the routes to be learned overlap with an existing one, the routes conflict with each other. After you enable overlapping routing, CEN can learn routes with destination CIDR blocks that have the same prefix but different subnet mask lengths.

> **Note** By default, overlapping routing is enabled for CEN instances that are created after March 1, 2019 (UTC+8).

Before overlapping routing is enabled

For example, virtual private cloud (VPC) A attached to a CEN instance has a custom route whose destination CIDR block is 192.168.1.0/24 and the next hop is Elastic Compute Service (ECS) instance 1 in VPC A. In this scenario, VPC A cannot learn the routes whose destination CIDR block is 192.168.1.0/x (1 ≤ x ≤ 32) from other network instances attached to the CEN instance.

Similarly, if VPC A learns a route whose destination CIDR block is 192.168.1.0/24 from the CEN instance, you cannot create a custom route whose destination CIDR block is 192.168.1.0/x (1 ≤ x ≤ 32) for VPC A. VPC A cannot learn other routes whose destination CIDR block is 192.168.1.0/x (1 ≤ x ≤ 32) from other network instances attached to the CEN instance.

After overlapping routing is enabled

After you enable overlapping routing, CEN can learn routes with destination CIDR blocks that have the same prefix but different subnet mask lengths.

For example, VPC A attached to a CEN instance has a custom route whose destination CIDR block is 192.168.1.0/24 and the next hop is ECS instance 1 in VPC A. In this scenario, VPC A can learn the routes whose destination CIDR block is 192.168.0.0/16 from other network instances attached to the CEN instance.

The routes whose destination CIDR blocks are 192.168.1.0/24 and 192.168.0.0/16 can be learned at the same time by CEN. CEN learns the routes that match the longest prefix.

> **Note** After you enable overlapping routing, a VPC does not learn the routes whose destination CIDR block is more specific than that of the VPC vSwitch. For example, if the CIDR block of a VPC vSwitch is 10.0.0.0/16, the VPC cannot learn the routes whose destination CIDR block is 10.0.0.0/24 from other network instances. However, the VPC can learn the routes whose destination CIDR block is 10.0.0.0/8 from other network instances.

Procedure

To enable overlapping routing, perform the following steps:

1. Log on to the CEN console.
2. On the **Instances** page, find the CEN instance that you want to manage and click **Manage** in the **Actions** column.
3. In the **Basic Settings** section, click **Enable** after **Overlapping Routing Function**.

4. In the **Enable Overlapping Routing** message, click **OK**.

> **Notice** You cannot disable overlapping routing after you enable it.

5.2. Advertise routes to CEN

Cloud Enterprise Network (CEN) supports route advertisement. You can advertise routes of virtual private clouds (VPCs) and virtual border routers (VBRs) to a CEN instance so that other network instances attached to the CEN instance can learn these routes.

Context

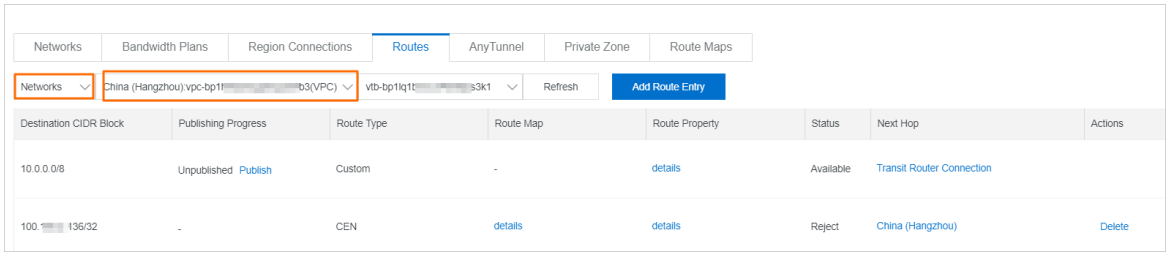
The following table describes the routes that can be advertised to CEN instances.

> **Note** The CEN console allows you to advertise only VPC routes to CEN. To advertise VBR routes to CEN, you must call the `PublishRouteEntries` API operation. For more information, see PublishRouteEntries.

Route	Network instance	Published to CEN by default
Routes that route network traffic to Elastic Compute Service (ECS) instances	VPC	No
Routes that route network traffic to VPN gateways	VPC	No
Routes that route network traffic to high-availability virtual IP addresses (HAVIPs)	VPC	No
System routes of VPCs	VPC	Yes
Routes that route network traffic to data centers	VBR	Yes
Border Gateway Protocol (BGP) routes	VBR	Yes

Advertise routes to CEN

1.
2. On the **Instances** page, find the CEN instance that you want to manage and click its ID.
3. On the **CEN** page, click the **Routes** tab, select **Networks** from the drop-down list, and then select the network instance that you want to manage.

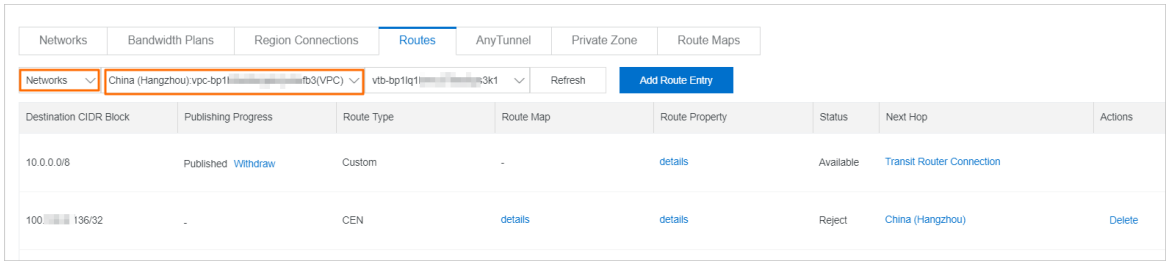


4. Find the route that you want to manage and click **Publish** in the **Publishing Progress** column.

5. In the **Publish Route** message, click **OK**.

Withdraw routes from CEN

1.
2. On the **Instances** page, find and click the CEN instance that you want to manage.
3. On the **CEN** page, click the **Routes** tab, select **Networks** from the drop-down list, and then select the network instance that you want to manage.



4. Find the route that you want to withdraw and click **Withdraw** in the **Publishing Progress** column.
5. In the **Withdraw Route** message, click **OK**.

5.3. Withdraw a route from CEN

This topic describes how to withdraw a route from Cloud Enterprise Network (CEN). You can withdraw a route that has been published to CEN. After the route is withdrawn, other networks attached to the same CEN instance cannot learn the route. If you publish a custom VPC or Virtual Border Router (VBR) route entry to a CEN instance and then delete the route from the VPC or VBR route table, the route entry is also deleted from CEN.

Context

The following table lists the route entries that can be withdrawn from CEN.

> **Note** Currently, the console only supports withdrawing VPC routes from CEN. If you need to withdraw VBR routes, call WithdrawPublishedRouteEntries. For more information, see WithdrawPublishedRouteEntries.

Route entries	Network	Published to CEN by default?
A route entry pointing to an ECS instance	VPC	No
A route entry pointing to a VPN Gateway	VPC	No
A route entry pointing to a High-Availability Virtual IP Address (HaVip)	VPC	No
A VPC system route entry	VPC	Yes
A route entry pointing to an on-premises data center	VBR	Yes
A BGP route entry	VBR	Yes

Procedure

1. Log on to the CEN console.
2. On the **Instances** page, find the target CEN instance and click **Manage** in the **Actions** column.
3. On the **CEN** page, click the **Networks** tab. Find the target VPC and click the VPC ID.
4. On the **VPC Details** page, click the link to the route table.
5. On the **Route Tables** page, find the target route table, and click **Manage** in the **Actions** column.
6. On the **Route Entry List** tab, find the target route entry, and click **Withdraw** in the **Route Status in CEN** column.
7. In the **Withdraw Published Route Entry** dialog box, click **OK**.

5.4. View routes

5.4.1. View CEN routes in the CEN console

This topic describes how to view CEN routes in the Cloud Enterprise Network (CEN) console. You can view the route details in the CEN console.

Procedure

1. Log on to the CEN console.
2. On the **Instances** page, find the target CEN instance and click **Manage** in the **Actions** column.
3. On the **CEN** page, click the **Routes** tab, and then filter the route information you want to view.

   Region-based route information

Field	Description
Destination CIDR Block	The destination CIDR block of the route.
Type	The type of the route. ○ **CEN**: Routes that are learned from CEN. ○ **System**: Routes that are automatically added by the system.
Routemap	Whether the route matches the configured route map. If the route matches a route map, you can click **details** to view the matched route map.
Route Property	The attributes of the route. To view details of the route attributes, such AS Path, Community, and priority, click **details**.
Status	The status of the route.
Next Hop	The region to which the next hop of the route belongs.
To other region route map	The matched route map to other regions.

Field	Description
To other region status	The status of the route to other regions.

Network-based route information

Field	Description
Destination CIDR Block	The destination CIDR block of the route.
Publish Status	Whether the route has been published to CEN. ○ **Published**: The route has been published to CEN. Other networks in the same CEN instance can learn the route. ○ **NonPublished**: The route is not published to CEN. Other networks in the same CEN instance cannot learn the route.
Type	The type of the route. ○ **CEN**: Routes that are learned from CEN. ○ **System**: Routes that are automatically added by the system.
Routemap	Whether the route matches the configured route map. If the route matches a route map, you can click **details** to view the matched route map.
Route Property	The attributes of the route. To view details of the route attributes, such AS Path, Community, and priority, click **details**.
Status	The status of the route.
Next Hop	The region to which the next hop of the route belongs.

5.4.2. View CEN routes in the VPC route table

This topic describes how to view Cloud Enterprise Network (CEN) routes in the VPC route table.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Route Tables**.
3. Select the region to which the target route table belongs.
4. On the **Route Tables** page, find the target route table, and click **Manage** in the **Actions** column.
5. On the **Route Entry List** tab, view CEN routes.

5.4.3. View routes learned from CEN in a VBR route table

Cloud Enterprise Network (CEN) automatically advertises and learns routes. This improves the network quality and accelerates the convergence of routes. You can view routes learned from CEN in the route table of a specific virtual border router (VBR).

Procedure

1. Log on to the Express Connect console.
2. In the left-side navigation pane, click **Virtual Border Routers (VBRs)**.
3. On the **Virtual Border Routers (VBRs)** page, click the ID of the VBR.
4. Click the **Routes** tab to view CEN routes.

6.Route maps

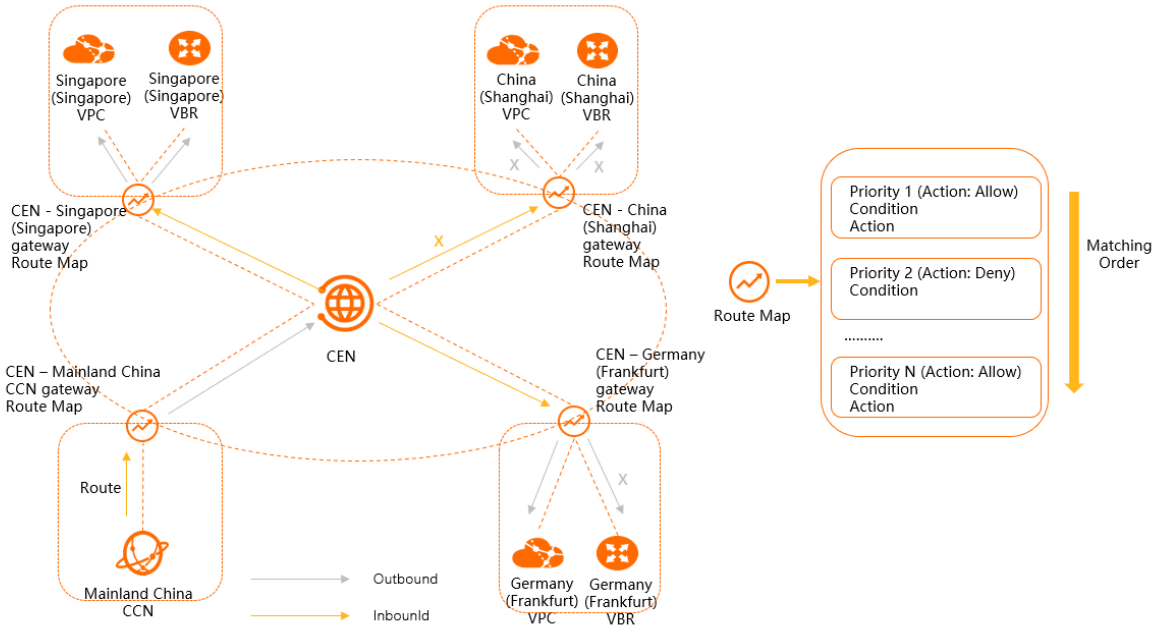
6.1. Routing policy overview

Cloud Enterprise Network (CEN) supports routing policies. You can configure routing policies to filter and modify routes. This allows you to manage network communication in the cloud.

How it works

CEN has a gateway in each Alibaba Cloud region. Regional gateways are one of the basic components that CEN uses to establish communication between networks. CEN uses regional gateways to pass routes to networks that are attached to CEN.

You can configure routing policies for inbound network traffic or outbound network traffic. Each routing policy is a collection of conditional statements and execution statements. Routing policies are sorted by priority. A smaller value indicates a higher priority. Routes are matched against match conditions specified in routing policies in descending order of policy priority. Routes that meet all match conditions are permitted or denied based on the specified policy action. You can modify the priority, autonomous system (AS) path, and community value of a route that is permitted. Routes that do not match all match conditions are matched against the next routing policy by default. If a route does not match any routing policy, the route is permitted by default.



Components

A routing policy consists of three components: basic information, match conditions, and policy values. The following tables describe the details of each component.

> **Note** You can set **Policy Value** and **Routing Policy Priority** only when **Routing Policy Action** is set to **Permit**.

Basic information

Parameter	Description
Routing Policy Priority	The priority of the routing policy. Valid values: 1 to 100. A smaller value indicates a higher priority. You cannot specify the same priority for routing policies that apply in the same region and direction. The system compares routes against the match conditions of routing policies in descending order of priority. A smaller value indicates a higher priority. Therefore, set appropriate values to sort the routing policies in the desired order.
Description	Enter a description for the routing policy. The description cannot start with `http://` or `https://`. It must start with a letter and can contain letters, digits, hyphens (-), periods (.), and underscores (_).
Region	Select the region in which the routing policy applies.
Direction	The direction in which the routing policy is applied. • **Import to Regional Gateway**: If you select this option, the routing policy applies to routes that are advertised to the regional gateway. For example, routes are advertised to a regional gateway from a network instance in the same region, or from a network instance in a different region. • **Export from Regional Gateway**: If you select this option, the routing policy applies to routes that are advertised from the regional gateway. For example, routes are advertised from a regional gateway to a network instance in the same region or to a regional gateway in a different region.
Routing Policy Action	The action to be performed on a route that meets all match conditions. The following actions are supported: • **Permit**: permits routes that are matched. • **Deny**: denies routes that are matched.
Priority of Associated Routing Policy	Specify a priority for the routing policy that you want to associate with the current one. • You can set the parameter only if you set **Permit** to **Routing Action Policy**. Only permitted routes are matched against the routing policies that have the specified priority. • The **region** and **direction** of the routing policy that you want to associate with the current routing policy must be the same as those of the current routing policy. • The priority of the routing policy that you want to associate with the current routing policy must be lower than the priority of the current routing policy.

Match conditions

Parameter	Description
Source Region	The system checks whether routes are advertised from a specified region. The system only checks whether the source regions of the routes meet the specified condition. The destination regions of the routes are not checked.
Source Instance IDs	The system checks whether routes are advertised from specified network instances. The following network instance types are supported: • Virtual private cloud (VPC) • Virtual border router (VBR) • Cloud Connect Network (CCN) instance • Smart Access Gateway (SAG) instance You can select **Exclude Specified IDs** to specify network instance IDs that you want to exclude. If the routes are not advertised from the specified IDs, the routes meet the condition. Otherwise, the routes fail to meet the condition.
Destination Instance IDs	The system checks whether routes are advertised to specified network instances. The following network instance types are supported: • Virtual private cloud (VPC) • Virtual border router (VBR) • Cloud Connect Network (CCN) instance • Smart Access Gateway (SAG) instance You can select **Exclude Specified IDs** to specify network instance IDs that you want to exclude. If the routes are not advertised to the specified IDs, the routes meet the condition. Otherwise, the routes fail to meet the condition. **Note** The destination instance IDs take effect only when **Direction** is set to **Export from Regional Gateway** and the destination instances are deployed in the current region.
Destination Route Table	The system checks whether routes are advertised to specified route tables. **Note** The destination route table IDs take effect only when **Direction** is set to **Export from Regional Gateway** and the destination route tables belong to network instances deployed in the current region.

Parameter	Description
Source Instance Type	The system checks whether routes are advertised from specified network instance types. The following network instance types are supported: • **VPC**: a virtual private cloud (VPC) • **VBR**: virtual border router (VBR) • **CCN**: Cloud Connect Network (CCN) instance
Destination Instance Type	The system checks whether routes are advertised to specified network instance types. The following network instance types are supported: • **VPC**: a virtual private cloud (VPC) • **VBR**: virtual border router (VBR) • **CCN**: Cloud Connect Network (CCN) instance **Note** The destination instance types take effect only when **Direction** is set to **Export from Regional Gateway** and the destination instance types are supported in the current region.
Route Type	The system checks whether routes are of specified types. The following route types are supported: • **System**: routes created by the system. • **Custom**: routes manually added by the user. • **BGP**: routes that are advertised over Border Gateway Protocol (BGP).
Route Prefix	The system filters routes based on the specified route prefixes. The following match methods are supported: • **Fuzzy Match**: If the prefix of a route falls within one of the specified prefixes, the route meets the match condition. For example, if you set the match condition to 10.10.0.0/16 and fuzzy match is applied, the route whose prefix is 10.10.10.0/24 meets the match condition. • **Exact Match**: A route meets the match condition only when the prefix of the route is the same as one of the specified prefixes. For example, if the match value is set to 10.10.0.0/16 and the match method is set to Exact Match, only the route with the prefix 10.10.0.0/16 meets the match condition.

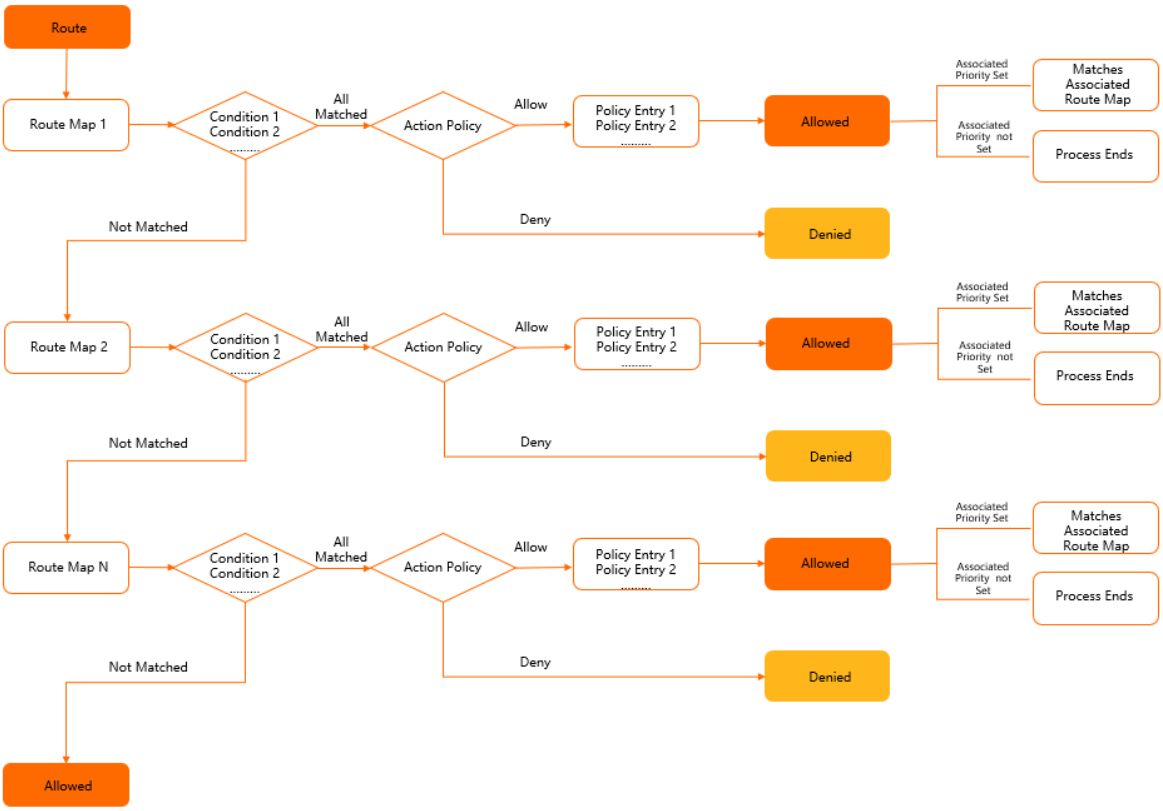
Parameter	Description
AS Path	The system filters routes based on the specified AS path. The following match methods are supported: • **Fuzzy Match**: A route meets the match condition if the AS path of the route overlaps with that specified in the match condition. For example, if you set the AS path to `65001,65002` and the match method to Fuzzy Match, the route whose AS path is `65501,65001` matches the condition because both AS paths contain `65001`. • **Exact Match**: A route meets the match condition only if the AS path of the route is the same as that specified in the match condition. For example, if you set the match condition to `65501,65001,60011` and exact match is applied, only the route whose AS path is `65501,65001,60011` meets the match condition. **Note** AS path is a mandatory attribute, which describes the AS numbers that a BGP route passes through when it is advertised.
Community	The system matches routes based on the community. The following match methods are supported: • **Fuzzy Match**: A route meets the match condition if the community of the route overlaps with that specified in the match condition. For example, if you set the match condition to `65001:1000,65002:2000` and fuzzy match is applied, the route whose community is `65501:1000,65001:1000` meets the match condition, because both communities contain `65501:1000`. • **Exact Match**: A route meets the match condition only if the community of the route is the same as that specified in the match condition. For example, if you set the match condition to `65001:65001,65002:65005,65003:65001` and exact match is applied, only the route whose community is `65001:65001,65002:65005,65003:65001` meets the match condition. **Note** Community is an optional transitive attribute. You can specify a specific community value for a specific route. Downstream routers can filter routes based on the specified community value when routing policies are implemented.

Policy values

Parameter	Description

Parameter	Description
Preference	Specify a priority for the routes that are permitted. Valid values: 1 to 100. Default value: 50. A smaller value indicates a higher priority.
Community	Specify a community value for routes. The following methods are supported: • **Add**: adds the specified community value to matched routes. • **Replace**: replaces the community values of matched routes with the specified community value.
Appended AS Path	The AS paths that are prepended by using an action statement when regional gateways receive or advertise routes. For routing policies that are used in different directions, the requirements for AS paths that are prepended are different: • If the direction of a routing policy is set to **Import to Regional Gateway** and you want to specify appended AS paths, you must specify source instance IDs and source region in match conditions. The source region that you specify must be the same region to which the routing policy applies. • If the direction of a routing policy is set to **Export from Regional Gateway** and you want to specify appended AS paths, you must specify destination instance IDs in match conditions.

Matching process



CEN matches routes against routing policies in match-action mode. Actions are performed after conditions are matched. The system matches routes against match conditions in descending order of routing policy priority.

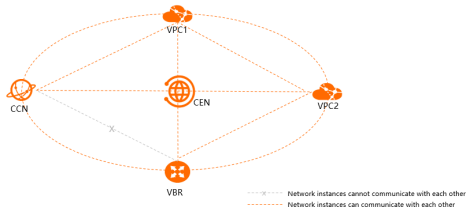
- If a route meets all the match conditions in a routing policy, the specified action is performed on the route.
  - If you set Routing Policy Action to Permit, the route is permitted. By default, the system does not match a matched route against the next routing policy. However, if you set a priority for the associated routing policy, the system matches the route against the routing policy that has the specified priority. If you do not set a priority, the matching process ends.
  - If you set Routing Policy Action to Deny, the route is denied. By default, the system stops matching the route against the next routing policy and the matching process ends.
- If a route does not meet a match condition specified in a routing policy, the current matching process ends and the system matches the route against the next routing policy.
- If the route meets all the match conditions specified in the next routing policy, the action specified in the routing policy is performed on the route.
  - If you set Routing Policy Action to Permit, the route is permitted. By default, the system does not match a matched route against the next routing policy. However, if you set a priority for the associated routing policy, the system matches the route against the routing policy that has the specified priority. If you do not set a priority, the matching process ends.
  - If you set Routing Policy Action to Deny, the route is denied. By default, the system stops matching the route against the next routing policy and the matching process ends.
- If a route does not meet a match condition specified in a routing policy, the current matching process ends and the system matches the route against the next routing policy. The preceding processes are repeated until the system matches the route against the last routing policy.

- If the route does not meet a match condition specified in the last routing policy, the route is permitted.

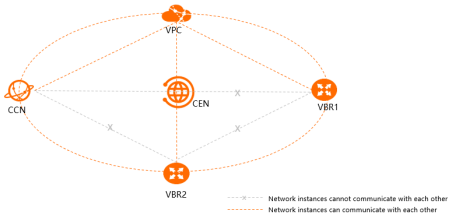
Default routing policy

If a VBR or CCN instance is attached to a CEN instance, the system automatically adds a routing policy whose priority is 5000, action is Deny, and direction is Export from Regional Gateway to the regional gateway. This routing policy disallows the VBR or CCN instance from communicating with the other VBRs or CCN instances that are attached to the CEN instance. The following rules describe whether VPCs, VBRs, and CCN instances that are attached to the same CEN instance can communicate with each other.

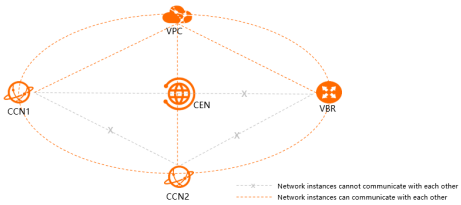
- A VPC that is attached to a CEN instance can communicate with other VPCs, VBRs, and CCN instances that are attached to the CEN instance.



- A VBR that is attached to a CEN instance cannot communicate with other VBRs or CCN instances that are also attached to the CEN instance.



- A CCN instance that is attached to a CEN instance cannot communicate with VBRs or other CCN instances that are also attached to the CEN instance.



Limits

Resource	Limit	Adjustable
Number of routing policies that can be created in the Import to Regional Gateway direction for each regional gateway	100	Not supported
Number of routing policies that can be created in the Export to Regional Gateway direction for each regional gateway	100	Not supported

References

The routing policy feature allows you to flexibly manage network communication in the cloud. For more information, see the following topics:

- Stop the communication between a VPC and other networks attached to a CEN instance
- Stop the communication between a VPC and a CIDR block in CEN
- Connect data centers through CEN
- Connect branches to a data center through CEN
- Configure active/standby static routes for VBRs in the same region by using route maps
- Use route maps to allow specified VPCs to communicate with each other

6.2. Add a route map

This topic describes how to add a route map to a Cloud Enterprise Network (CEN) instance. To use the route map function, you must first add a route map. After you add a route map to a CEN instance, you can filter routes and modify route attributes to manage the communication between networks attached to the CEN.

Context

A route map is a set of conditional statements and executable statements. You can configure route maps for different regional gateways in a CEN instance. Each regional gateway can be configured with one or more route maps in the inbound and the outbound directions. The sequence of route maps of each gateway is ordered based on their priorities. When route maps are executed to evaluate a route, the system first checks whether the route matches the conditional statements of the route map with the highest priority. The route map permits or denies routes based on the configured match conditions. If a route is permitted, you can modify its attributes. For more information, see Routing policy overview.

Procedure

1. Log on to the CEN console.
2. In the left-side navigation pane, click **Instances**.
3. On the **Instances** page, find the target CEN instance and click **Manage** in the **Actions** column.
4. On the **CEN** page, click the **Route Maps** tab and then click **Add Route Map**.
5. On the **Add Route Map** page, configure the route map according to the following information and then click **OK**.

Configuration	Description

Configuration	Description
Route Map Priority	The priority of the route map. A lower value indicates a higher priority. After configuring a route map with a specific priority value, you cannot set the same priority value for another route map that is applied in the same region and in the same direction. When route maps are executed to evaluate a route, the system first checks whether the route matches the conditional statements of the route map with the highest priority. Therefore, we recommend that you specify an appropriate priority for each route map.
Description	The description of the route map.
Region	The region where the route map is applied.
Transmit Direction	The direction in which the route map is applied. ○ Import to Regional Gateway: The direction in which routes are imported to the regional gateway of the CEN. For example, routes are imported to the regional gateway from an instance in the current region or another region. ○ Export from Regional Gateway: The direction in which routes are exported from the regional gateway of the CEN. For example, routes are exported from the regional gateway of the current region to an instance in the same region, or to the regional gateway in another region.
Match Conditions	The match conditions of the route map. Click **+ Add Match Condition** to add one or more match conditions. For more information, see Match conditions.

Configuration	Description
Action Policy	The action that is performed to a route if the route matches all the match conditions. ○ **Permit**: Permit the route. After you set the Action Policy to Permit, you can add the following policy entries: ■ **Route Preference**: Set the preference for the permitted routes. Value range: 1 to 100. The default route preference is 50. A lower value indicates a higher priority. ■ **Community**: Set the community value. Two settings are supported: Add and Replace. ■ **Prepended AS Path** : An AS path is prepended when the regional gateway receives or advertises a route. The requirements for configuring this policy entry vary depending on the application direction of the route map. The requirements are described as follows: ■ If the Transmit Direction of a route map is set to Import to Regional Gateway and you want to configure the Prepended AS Path as a policy entry, the match conditions must include the Source Instance IDs and the Source Region. Furthermore, you must specify the same value for the Source Region and the Region parameters. ■ If the Transmit Direction of a route map is set to Export from Regional Gateway and you want to configure the Prepended AS Path as a policy entry, the match conditions must include the Destination Instance IDs. ○ **Deny**: Deny the route. If you set the Action Policy to Deny, policy entries are not supported.

Configuration	Description
Associated Priority	Optional. The priority of the next route map that is associated with the current route map. Value range: 1 to 100. ○ If **Associated Priority** is not set, the current route map is not associated with any route map that is ordered next to the current route map. ○ If the value is set to 1, the current route map is associated with the next route map. ○ If the value is set to a number other than 1, the priority of the associated route map must be lower than the priority of the current route map, that is, the value of Associated Priority must be greater than the value of Route Map Priority. Only when the Action Policy is set to Permit for the current route map, the routes which match all the match conditions will be evaluated by the associated route map that is configured with a specific priority value.

Related information

- CreateCenRouteMap

6.3. Modify a route map

This topic describes how to modify a route map of a CEN instance. After you create a route map, you can modify its priority, description, transmit direction, match conditions, action policy, and associated priority.

Context

You cannot modify the default route map whose priority is greater than 1000. However, you can add a custom route map to overwrite the default route map.

Procedure

1. Log on to the CEN console.
2. In the left-side navigation pane, click **Instances**.
3. On the **Instances** page, find the target CEN instance and click **Manage** in the **Actions** column.
4. On the **CEN** page, click the **Route Maps** tab, find the target route map, and then click **Modify** in the **Actions** column.
5. On the **Modify Route Map** page, modify the priority, description, transmit direction, match conditions, action policy, and associated priority as needed, and then click **OK**.

6.4. Delete route maps

This topic describes how to delete route maps that you no longer need. After you delete a route map from a CEN instance, the route map is no longer applied.

Procedure

1. Log on to the CEN console.
2. In the left-side navigation pane, click **Instances**.
3. On the **Instances** page, find the CEN instance that you want to manage and click **Manage** in the **Actions** column.
4. On the **CEN** page, click the **Route Maps** tab, find the route map that you want to delete, click **Delete** in the **Actions** column.
5. In the **Delete Route Map** message, click **OK**.

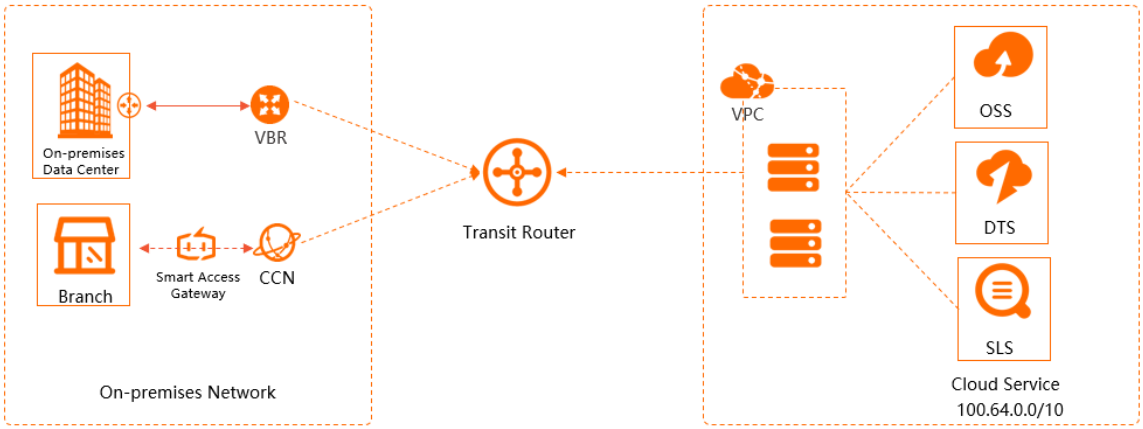
7.Access to cloud services

7.1. Access cloud services

After you attach virtual border routers (VBRs) and Cloud Connect Network (CCN) instances to a Cloud Enterprise Network (CEN) instance, you can configure the on-premises networks connected to the VBRs and CCN instances to access Alibaba Cloud services through the CEN instance.

Context

The cloud services discussed in this topic refer to the Alibaba Cloud services that use the 100.64.0.0/10 CIDR block to provide services, such as Object Storage Service (OSS), Log Service, and Data Transmission Service (DTS). If an on-premises network needs to access a cloud service, you must attach the VBR or CCN instance associated with the on-premises network to a CEN instance, and then attach a virtual private cloud (VPC) to the CEN instance. The VPC and the cloud resource must belong to the same region. This way, your on-premises network can access the VPC and access the cloud service through the VPC.



Limits

An on-premises network associated with a VBR can access only a cloud service that is deployed in the same region by using CEN.

For example, if the cloud service is deployed in the China (Beijing) region, only an on-premises network associated with a VBR in the China (Beijing) region can access the cloud service.

Prerequisites

- A VPC that is deployed in the same region as the cloud service is attached to the CEN instance.
- The VBR or CCN instance associated with your on-premises network is attached to the CEN instance. For more information, see Attach a network instance.

Configure access to the cloud service

1.
2.
3. On the instance details page, click the **AnyTunnel** tab and then click **Configure AnyTunnel**.

4. In the **Configure AnyTunnel** panel, set the following parameters and click **OK**.
   - **Service IP address**: Enter an IP address or CIDR block used by the cloud service. This IP address or CIDR block must fall within 100.64.0.0/10. For example, you can enter 100.118.28.52/32.
   - **Service Region**: Select the region where the cloud service is deployed.
   - **Host VPC**: Select the VPC attached to the CEN instance from the drop-down list.

     After you set the preceding parameters, the on-premises network associated with the VBR or CCN instance can access the cloud service through the VPC.
   - **Access Region**: Select the region where the VBR or CCN instance that needs to access the cloud service is deployed.
   - **Description**: Enter a description for the cloud service.

     The description must be 2 to 256 characters in length, and can contain digits, hyphens (-), periods (.),and underscores (_). It cannot start with `http://` or `https://`.

   > **Note** Typically, a cloud service uses multiple IP addresses or CIDR blocks. Repeat the preceding steps to add routes to all the IP addresses of the cloud service.

Delete cloud service configurations

1.
2.
3. On the details page of the CEN instance, click the **AnyTunnel** tab. Find the cloud service configuration that you want to delete and click **Delete** in the **Actions** column.
4. In the **Delete Route Service** message, click **OK**.

References

- ResolveAndRouteServiceInCen: configures a cloud service.
- DescribeRouteServicesInCen: queries cloud service configurations.
- DeleteRouteServiceInCen: deletes cloud service configurations.

8.Manage tags

8.1. Manage tags

You can add tags to Cloud Enterprise Network (CEN) instances. This allows you to manage and search CEN instances in an easier way.

Prerequisites

A CEN instance is created. For more information, see Create a CEN instance.

Context

Before you add a tag to a CEN instance, take note of the following information:

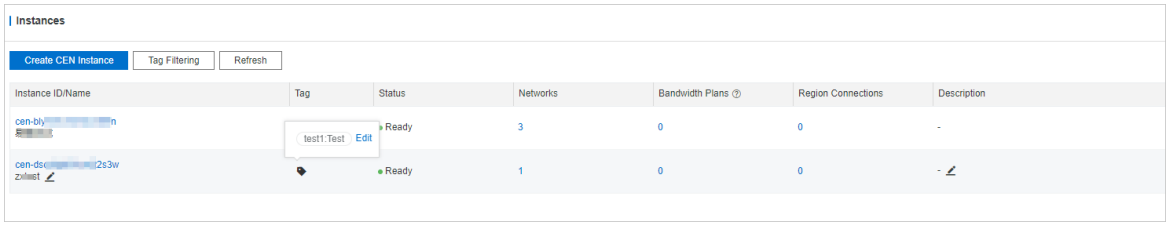
- Each tag consists of a tag key and a tag value. When you add a tag, you must specify the tag key, but you can leave the tag value empty.
- If you want to add multiple tags to a CEN instance, each tag key must be unique.
- You can add at most 20 tags to a CEN instance.

Add tags

1.
2. On the **Instances** page, find the CEN instance, click in the **Tag** column, and then click **Add**.
3. In the **Configure Tags** dialog box, set the following parameters to add one or more tags, and click **OK**.

Parameter	Description
Tag Key	The tag key. The key cannot be an empty string. It can be at most 64 characters in length, and cannot contain `http://` or `https://`. It must not start with `aliyun` or `acs:`.
Tag Value	The tag value. The value can be an empty string. It can be at most 128 characters in length, and cannot contain `http://` or `https://`. It must not start with `aliyun` or `acs:`.

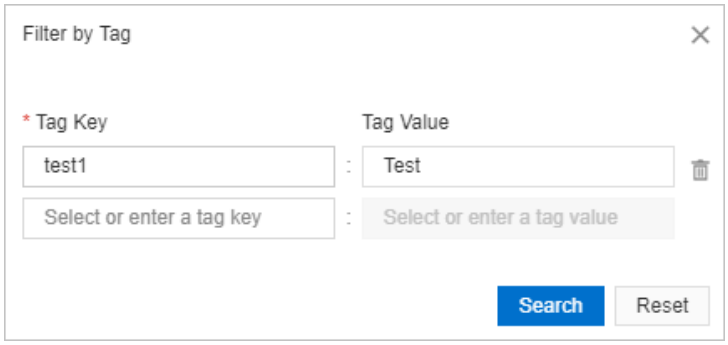
After you add tags, you can move the pointer over to view the tags that are added to the CEN instance.



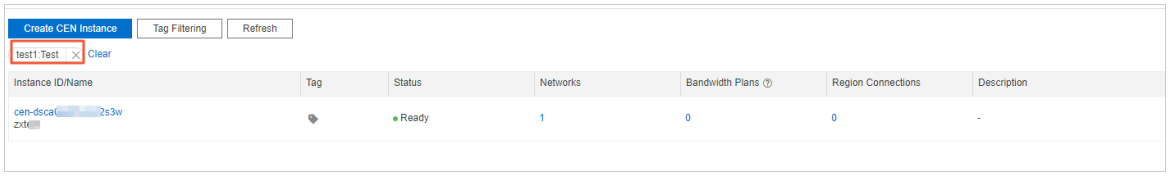
Filter by tag

After you add tags to CEN instances, you can search CEN instances by tag.

1.
2. On the **Instances** page, click **Filter by Tag**.
3. In the **Filter by Tag** dialog box, select one or more tags.



4. Click **Search** to view the CEN instances that have the specified tags.
   In the section below **Create CEN Instance**, you can view the tags that are used to filter CEN instances. You can also click **Clear** to clear the current filter conditions.

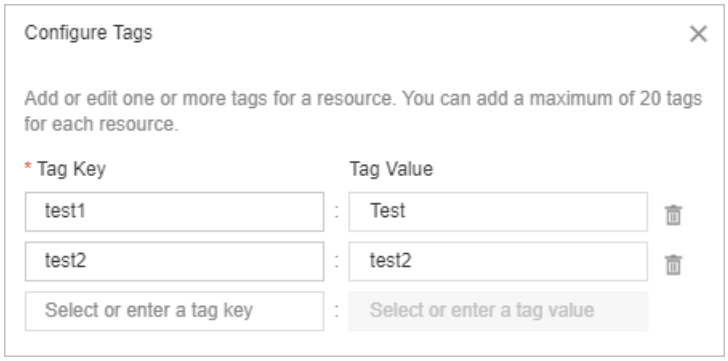


Edit tags

After you add a tag to a CEN instance, you can edit or delete the tag. You can also add more tags to the CEN instance.

> **Note** You can add at most 20 tags to each CEN instance.

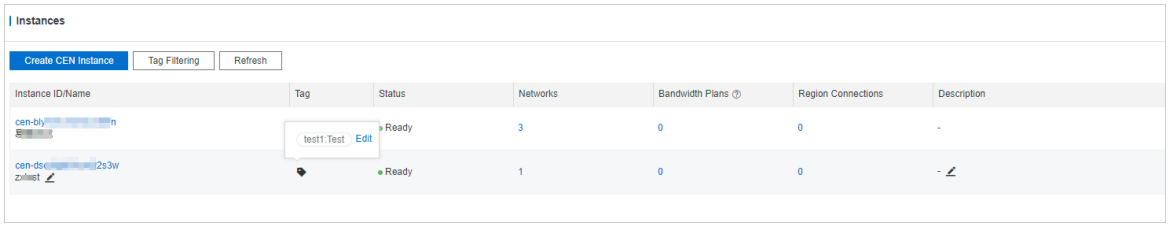
1.
2. On the **Instances** page, find the CEN instance, click in the **Tag** column, and then click **Edit**.
3. In the **Configure Tags** dialog box, you can perform the following operations. After you perform the operations, click **OK**.



   - Add tags: You can add more tags.

- Edit a tag: You can select a tag and modify the tag key or tag value.
- Delete a tag: You can click next to a tag to delete the tag.

After you edit a tag, you can move the pointer over in the **Tag** column to view the tag.



References

- TagResources: adds tags to a specified CEN instance.
- ListTagResources: queries tags added to CEN instances.
- UntagResources: removes tags from a CEN instance.

8.2. Edit tags

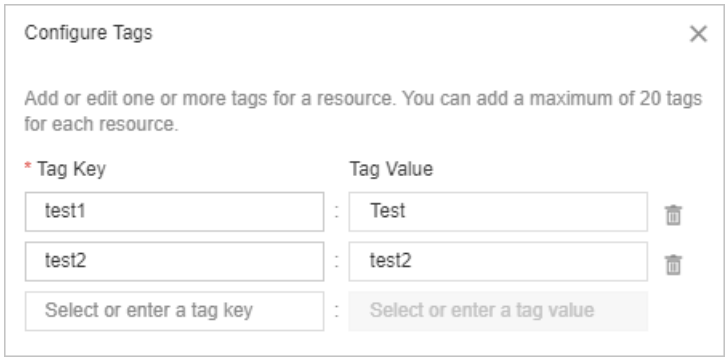
This topic describes how to edit tags. You can edit or delete tags that are attached to a Cloud Enterprise Network (CEN) instance, or attach new tags to the instance.

Prerequisites

Tags are attached to the target CEN instance. For more information, see Manage tags.

Procedure

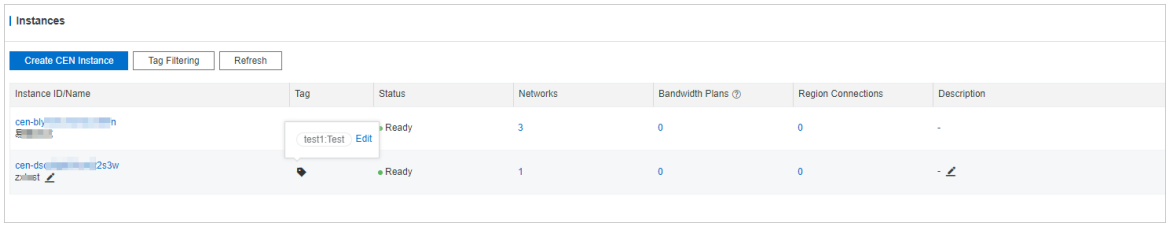
1. Log on to the CEN console.
2. On the **Instances** page, find the target CEN instance.
3. Click the icon in the **Tag** column.
4. Click **Edit**. In the **Configure Tags** dialog box, you can perform the following operations:



- Delete a tag: Click the icon next to a tag to delete the tag.
- Edit a tag: Select a tag, and modify the key and value of the tag.
- Add a tag: Enter a tag key and a tag value in the last row to add a new tag.

5. Click **OK**.

   After you edit tags, you can move your pointer over the icon to view the edited tags.

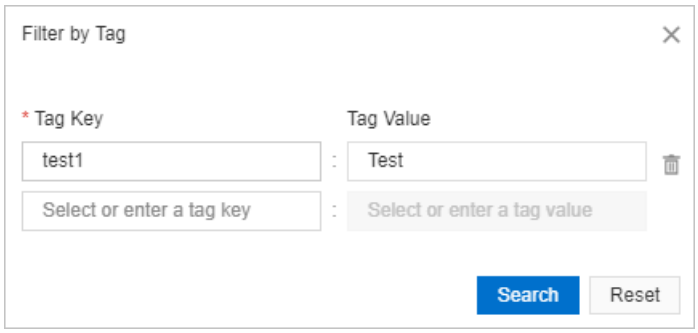


8.3. Filter by tag

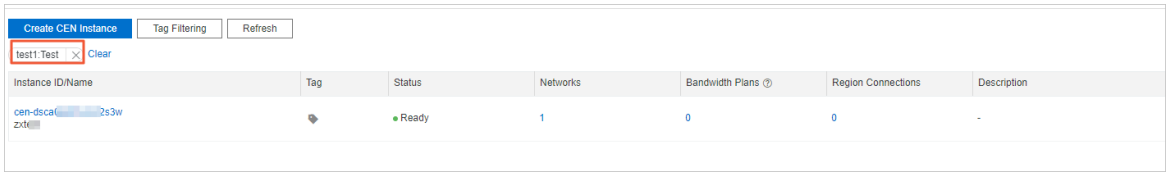
This topic describes how to filter Cloud Enterprise Network (CEN) instances by tag.

Procedure

1. Log on to the CEN console.
2. On the **Instances** page, click **Tag Filtering**.
3. In the **Filter by Tag** dialog box, select one or more tag keys and tag values.



4. Click **Search**, and view the matching instances.
   In the section below **Create CEN Instance**, view the tags that are used to filter CEN instances.



What's next

- In the section below **Create CEN Instance**, click **Clear** to clear the selected tags.
- Click **Tag Filtering** to reselect tags to filter CEN instances.

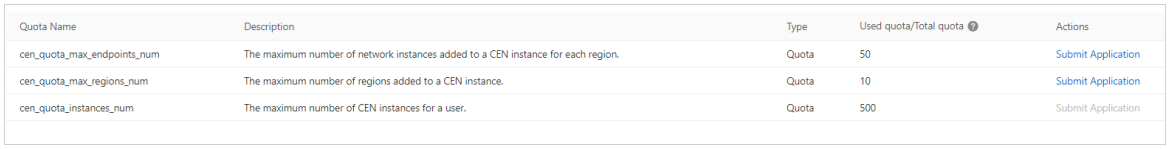
9.Manage resource quotas

This topic describes how to manage resource quotas in the Cloud Enterprise Network (CEN) console. If the quota on a resource cannot meet your business requirements, you can apply for a quota increase.

Apply for a quota increase

You can increase quotas on the following resources on the **Quotas** page: the number of network instances that can be attached to a CEN instance in each region, the number of regions that can be added to a CEN instance, and the number of CEN instances that can be created by each Alibaba Cloud account.

1.
2. In the left-side navigation pane, click **Quotas**. On this page, you can view the resource usage of CEN instances within the current account.



Quota Name	Description	Type	Used quota/Total quota	Actions
cen_quota_max_endpoints_num	The maximum number of network instances added to a CEN instance for each region.	Quota	50	Submit Application
cen_quota_max_regions_num	The maximum number of regions added to a CEN instance.	Quota	10	Submit Application
cen_quota_instances_num	The maximum number of CEN instances for a user.	Quota	500	Submit Application

3. To increase the quota on a resource, click **Submit Application** in the **Actions** column. In the dialog box that appears, set the following parameters and click **OK**:
   - **Requested Value**: Enter a value to which you want to increase the quota. The value must be a number that is greater than the current quota. For more information about default quota limits, see Usage notes on the previous console version.
   - **Reason**: State the reason why you want to increase the quota, including the scenarios and requirements.
   - **Email**: Enter the email address of the applicant.

   After you submit the application, you can click **History** in the **Actions** column to view the application status.

   The system automatically reviews your application.

   - If the requested value exceeds the upper limit, the system automatically rejects the application and the application status changes to **Rejected**.

     If your application is rejected, enter a smaller value and apply again.
   - If the specified value falls within the valid range, the system automatically approves the application and the application status changes to **Approved**. The new quota immediately takes effect.