Alibaba Cloud
云企业网

Quick Start

Issue: 20200316

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequent**

ial, exemplary, incidental, 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 contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

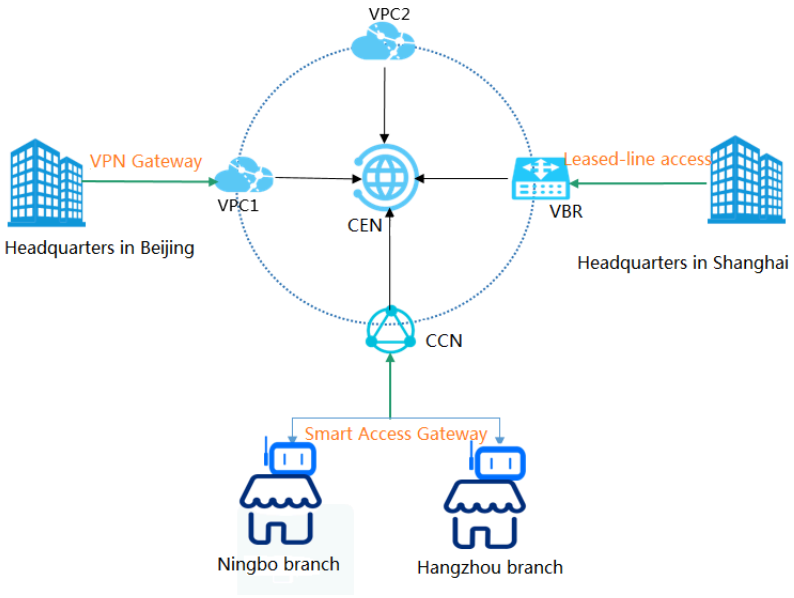
Style	Description	Example
	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 **Danger:** Resetting will result in the loss of user configuration data.
	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
	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.
	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]`

Style	Description	Example
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

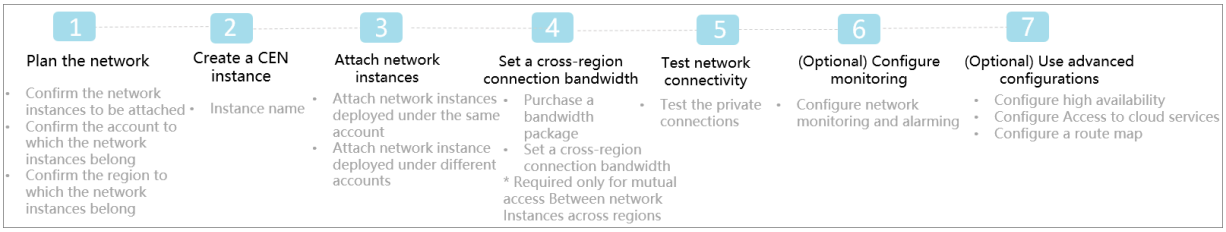
Contents

1 Tutorial overview

This topic provides an overview of Cloud Enterprise Network (CEN) tutorials. When you use a CEN, you can build a global network that consists of interconnected hybrid clouds and distributed service systems. You can attach network instances to a CEN instance so that the network instances can communicate with each other.



Typically, the configurations shown in the following figure are required when a CEN is used for network interconnection. However, these configurations may vary depending on the region and account to which network instances belong. Such network instances include VPCs, VBRs associated with on-premises data centers, CCNs associated with local branches or headquarters. Therefore, we recommend that you use these configurations selectively according to your specific business needs and network resources.



This tutorial uses the following two ECS instances deployed in different zones under different accounts as an example to describe how to establish intranet communication through a CEN.

Configuration	ECS1	ECS2
Private IP address	192.168.1.41	192.168.136.60
Region	China (Shanghai)	China (Hangzhou)
Account	123157908xxxx123	1954105xxxx83124
VPC	vpc-uf6w8bk8dx xxxfj0b7k94	vpc-bp1dylcs2x xxxnkckxxxx

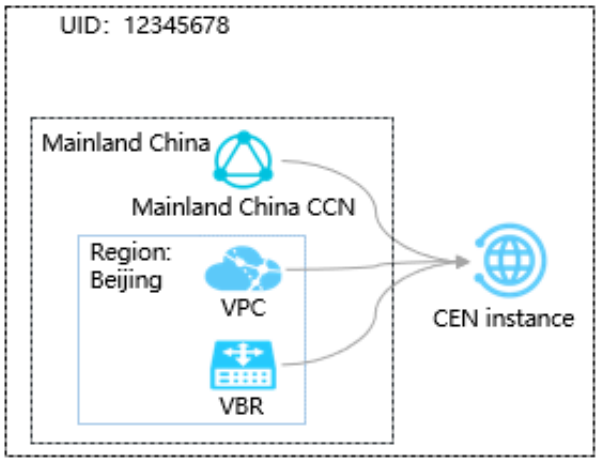
2 Step 1: Network planning

This topic describes how to use a Cloud Enterprise Network (CEN) to interconnect network instances, such as VPCs, VBRs associated with on-premises data centers, and CCNs to which local branches or headquarters is added. The procedure varies depending on the specific regions and accounts. Before using a CEN to configure network interconnection, you must specify the accounts and regions of the networks.

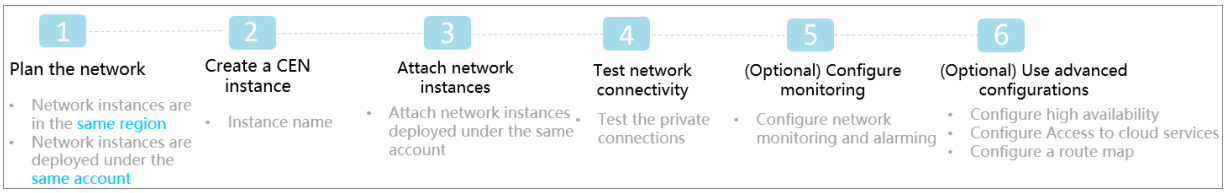
Interconnect network instances under the same account in the same region

To interconnect network instances under the same account in the same region, you need to attach these network instances to a CEN instance.

Network instances:



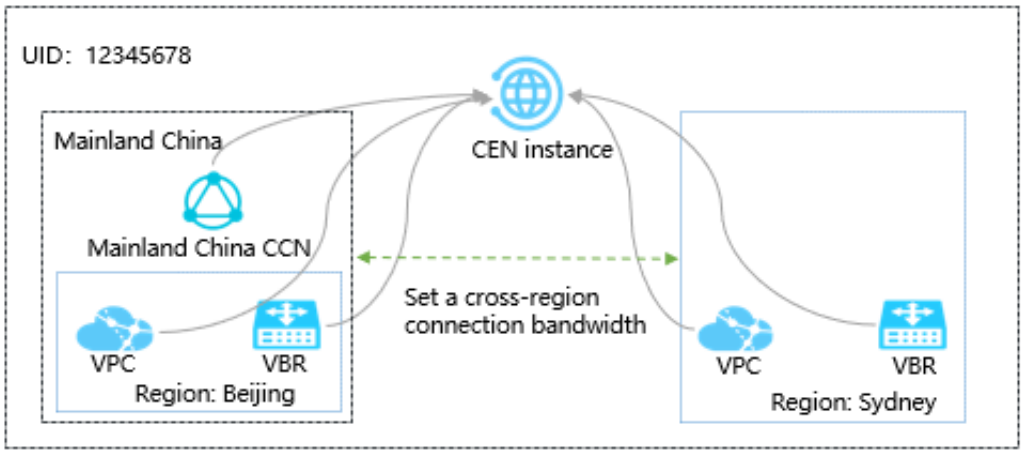
Procedure:



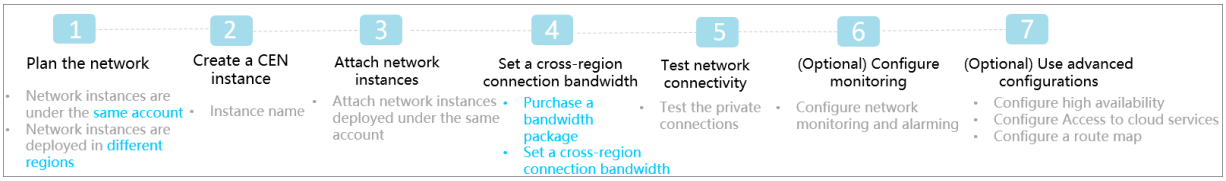
Interconnect network instances under the same account in different regions

To interconnect network instances under the same account in different regions, you need to attach these network instances to a CEN instance and set a cross-region connection bandwidth.

Network instances:



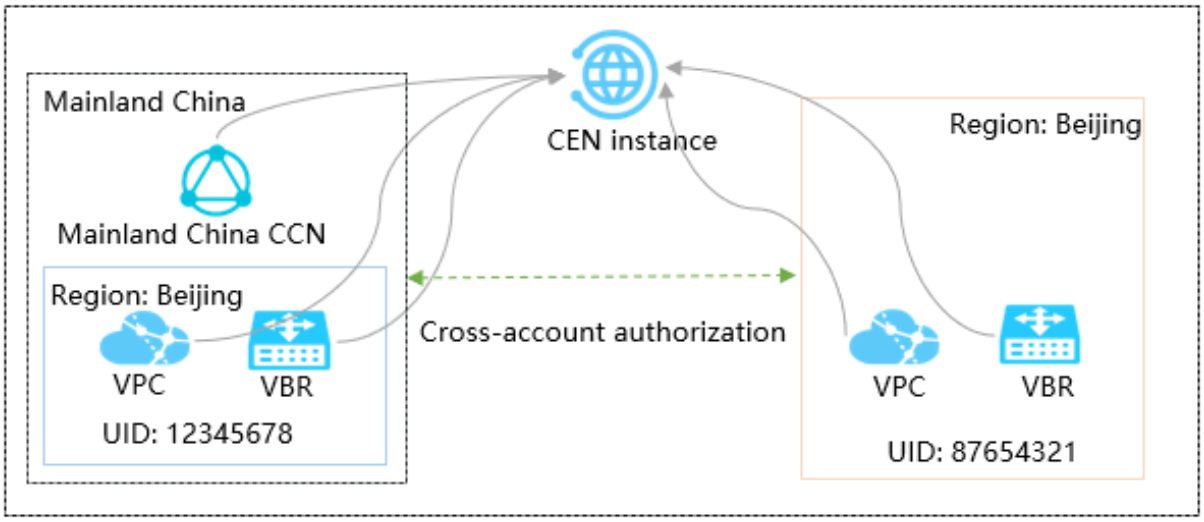
Procedure:



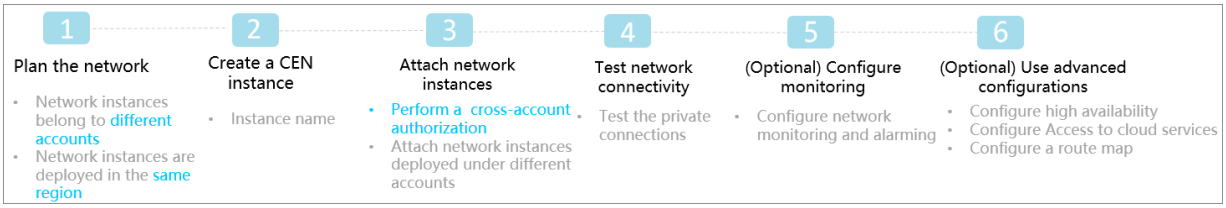
Interconnect network instances under different accounts in the same region

To interconnect network instances under different accounts in the same region, you need to perform a cross-account authorization and then attach these network instances to a CEN instance.

Network instances:



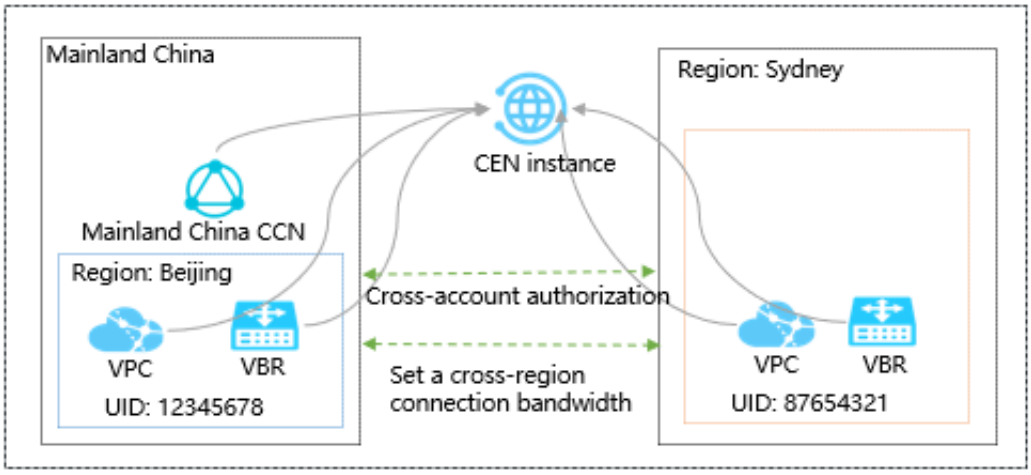
Procedure:



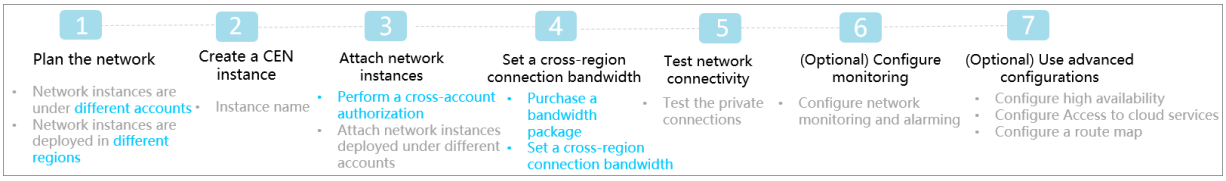
Interconnect network instances under different accounts in different regions

To interconnect network instances under different accounts in different regions, you need to perform a cross-account authorization, attach these network instances to a CEN instance, and then set a cross-region connection bandwidth.

Network instances:



Procedure:



3 Step 2: Create a CEN instance

Before you use Cloud Enterprise Network (CEN) for internal network communication, you must create a CEN instance. When you create a CEN instance, you can directly attach networks 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. **In the Create a CEN instance dialog box, configure the CEN instance according to the following information:**
   a) **Enter a name for the CEN instance to be created.**

      The name must be 2 to 128 characters in length and can contain letters, numbers, underscores (_), and hyphens (-). It must start with an English letter.
   b) **Optional: Enter a description for the CEN instance.**

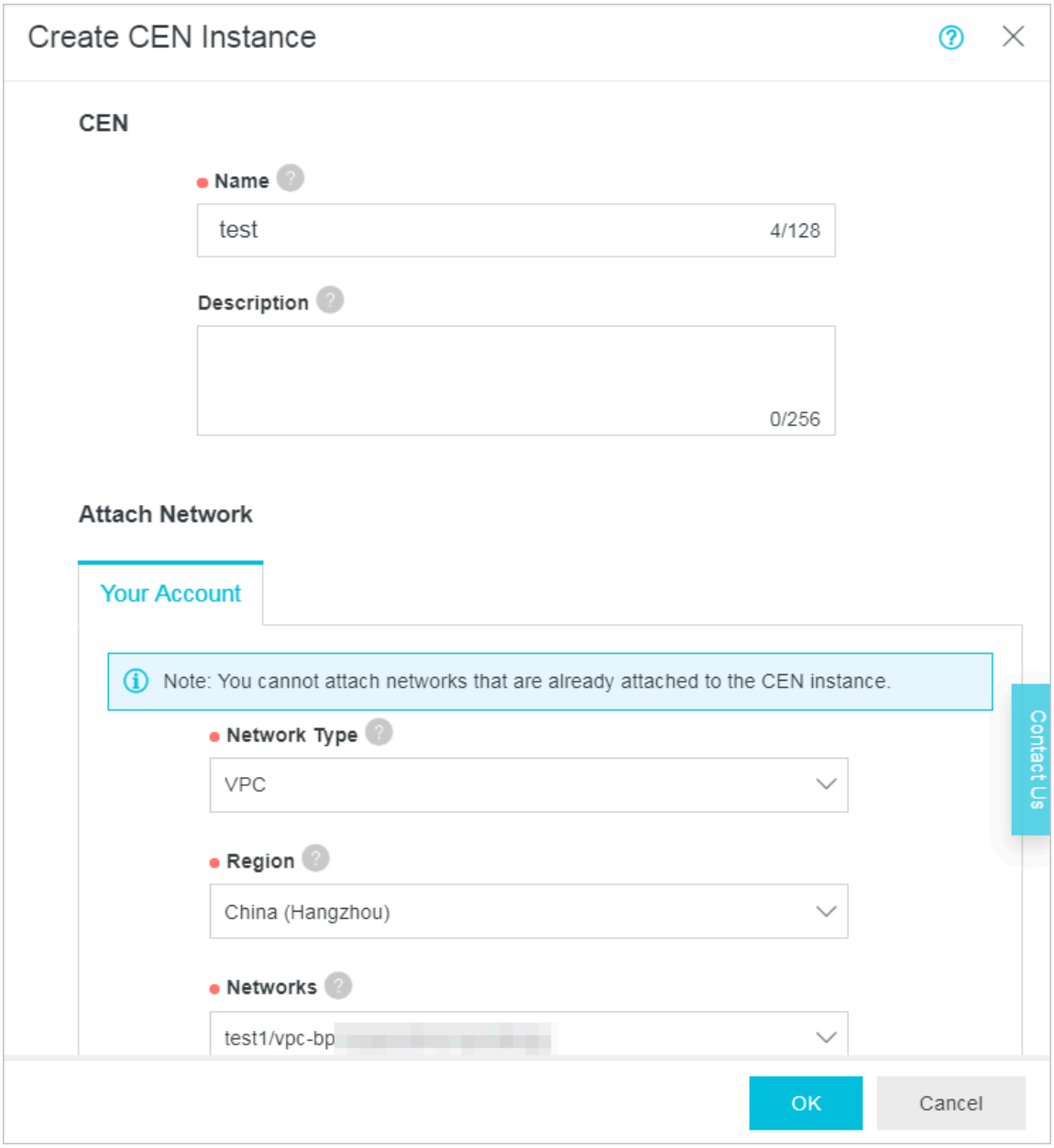
      The description must be 2 to 256 characters in length and cannot start with `http://` or `http://`.
   c) **Attach a network under the same account to the CEN instance.**

      When you create a CEN instance, you can directly attach a network under the same account to the CEN instance. The network can be a VPC, a Virtual Border Router (VBR), or a Cloud Connect Network (CCN). The networks attached to the CEN instance can communicate with each other through the internal network.

      Note:

Make sure that the network to attach is not attached to other CEN instances.

d) Click OK.



4 Step 3: Attach networks

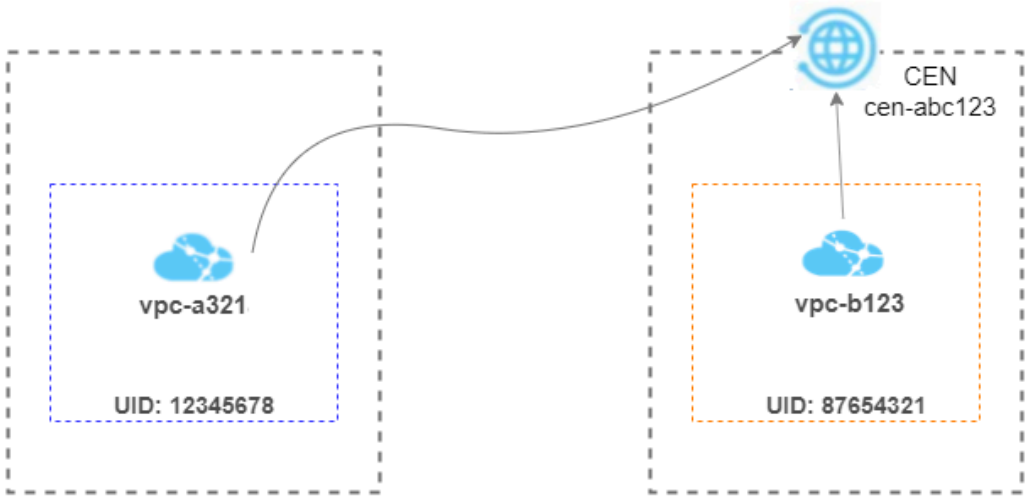
You can attach the networks that need to communicate with each other to a Cloud Enterprise Network (CEN) instance. The networks could be Virtual Private Cloud instances (VPCs), Virtual Border Routers (VBRs), and Cloud Connect Networks (CCNs). CEN automatically learns the routes of the attached networks to achieve internal network communication.

Prerequisites

Before you attach networks, make sure the following conditions are met:

- **You have created a CEN instance. For more information, see *Step 2: Create a CEN instance*.**
- **The networks to be attached are not attached to other CEN instances.**

Context



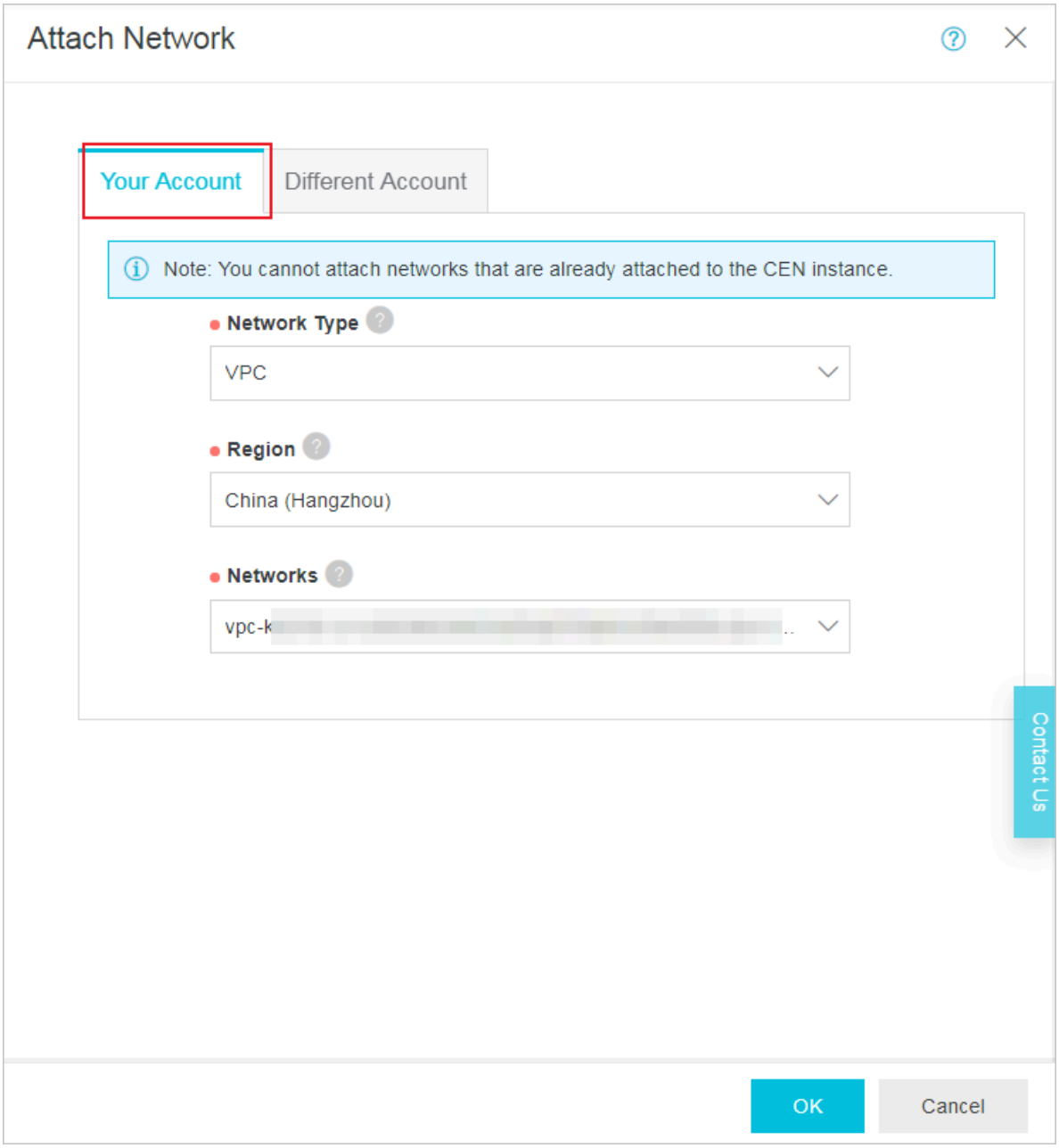
As shown in the figure, a CEN cen-abc123 is created under the account that is identified by the UID 87654321. You can attach network vpc-b123, which is under the same account, and network vpc-a321, which is under a different account, to cen-abc123, and thus interconnect vpc-b123 and vpc-a321.

Attach a network under the same account

To attach vpc-b123, a network under the same account, to the CEN instance cen-abc123, follow these steps.

1. Log on to the *CEN console*.
2. On the Instances page, find the target CEN instance and click the instance ID.
3. Click the Networks tab and then click Attach Network.
4. Click the Your Account tab.
5. Network Type: Select the type of the network to be attached.

   You can attach VPCs, VBRs, and CCNs.
6. Region: Select the region of the network.
7. Networks: Select the instance to be attached. In this example, select vpc-b123.



8. Click OK.

Attach a network under a different account

Notice:

Before you attach a network under a different account, you must obtain permissions from this account. After obtaining permissions, you must obtain the ID of this account and the instance ID of the network to be attached.

For more information, see:

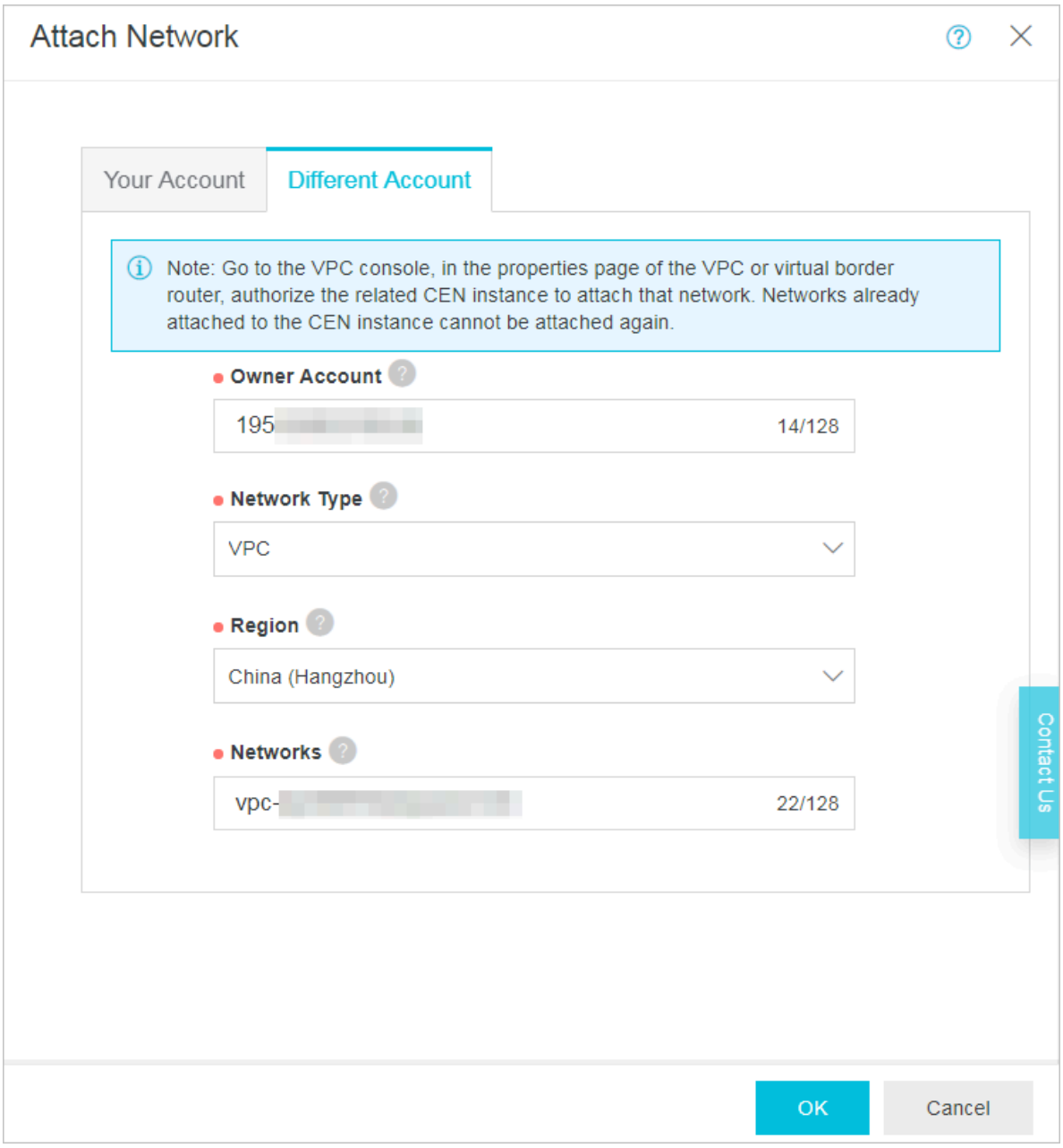
- *#unique_7/unique_7_Connect_42_section_mkn_v7p_lgn*
- *#unique_7/unique_7_Connect_42_section_2kc_03o_0us*
- *#unique_7/unique_7_Connect_42_section_gs1_agk_3o9*

To attach vpc-a321, a network under a different account, to the CEN instance cen-abc123, follow these steps.

1. **Log on to the *CEN console*.**
2. **On the Instances page, find the target CEN instance and click the instance ID.**
3. **Click the Networks tab and then click Attach Network.**
4. **Click the Different Account tab.**
5. **Owner Account: Enter the ID of the account to which the network to be attached belongs. In this example, enter 12345678.**
6. **Network Type: Select the type of the network to be attached.**

   You can attach VPCs, VBRs, and CCNs.
7. **Region: Select the region of the network.**

8. **Networks: Enter the instance ID of the network to be attached. In this example, enter vpc-a321.**



9. **Click OK.**

5 Step 4: Set a cross-region connection bandwidth

This topic describes how to set a cross-region connection bandwidth to connect network instances across different regions. By doing so, you can achieve internal network communication.

Prerequisites

You have attached the networks to be connected to the same CEN instance. For more information, see *Step 3: Attach networks*.

Context

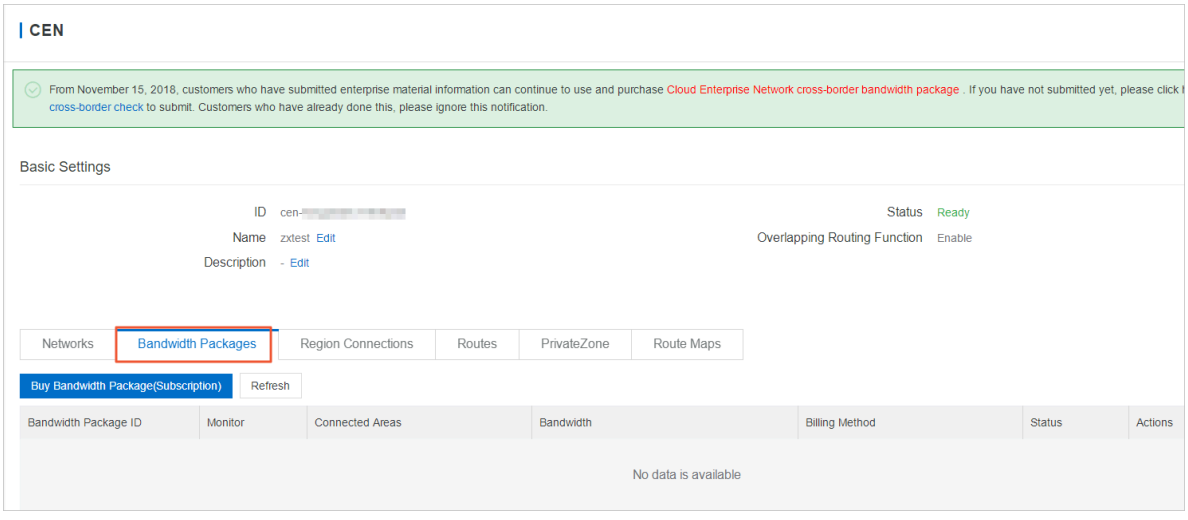
Establishing connection between networks in the same region doesn't require a bandwidth package or incur any costs. However, you must purchase a bandwidth package if you want to connect network instances across different regions.

When you purchase a bandwidth package, you need to specify the areas to be interconnected. An area is a collection of multiple regions. After you purchase a bandwidth package, you need to set a connection bandwidth for the regions to interconnect through the internal network.

Purchase a bandwidth package

To purchase a bandwidth package, follow these steps:

1. **Log on to the *CEN console*.**
2. **On the Instances page, find the target CEN instance and click the instance ID.**
3. **On the CEN page, click Bandwidth Packages.**



4. **Click Buy Bandwidth Package (Subscription).**

5. CEN ID: Select the CEN instance for which you want to purchase a bandwidth packet.
6. Select the areas to be interconnected.

   An area is a collection of regions. Each area contains one or more Alibaba Cloud regions. After you purchase a bandwidth package and set a cross-region interconnection bandwidth for two areas, network instances in the regions of these two areas can communicate with each other.

    **Notice:**
   After you purchase the bandwidth package, the interconnected areas cannot be modified.

Area	Included regions
Mainland China	China (Qingdao), China (Beijing), China (Zhangjiakou), China (Shenzhen), China (Hangzhou), China (Shanghai), China (Hohhot), China (Chengdu)
North America	US (Silicon Valley), US (Virginia)
Asia Pacific	China (Hong Kong), Singapore, Malaysia (Kuala Lumpur), Japan (Tokyo), Indonesia (Jakarta), India (Mumbai)
Europe	Germany (Frankfurt), UK (London)
Australia	Australia (Sydney)

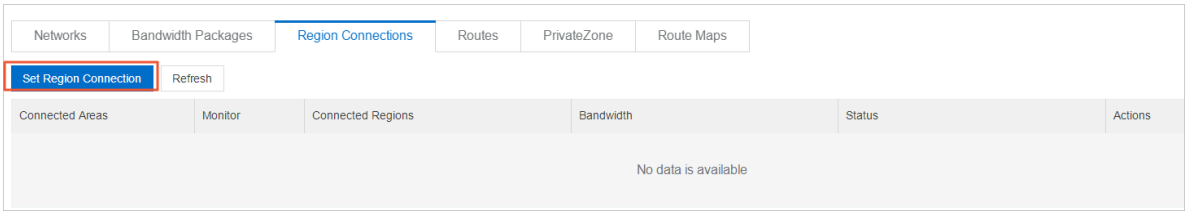
7. Set the bandwidth of the bandwidth package.
8. Enter a name for the bandwidth package.
9. Select a duration, and then select Auto Renew or not.
10. Click Buy Now and complete the payment.

Set a cross-region connection bandwidth

After purchasing a bandwidth package, complete these steps to set the cross-region connection bandwidth:

1. Log on to the *CEN console*.
2. On the Instances page, find the target CEN instance and click the instance ID.

3. On the CEN page, click Region Connections, and then click Set Region Connection.



4. Bandwidth Packages: Select the bandwidth package that you purchased.
5. Connected Regions: Select two regions to be interconnected.
6. Bandwidth: Set a bandwidth for the selected regions

> **Note:**
> A default bandwidth of 1 kbps is provided for you to conduct connectivity tests. We recommend that you set the bandwidth value according to your specific needs. The sum of all the connection bandwidth values cannot exceed the bandwidth value of the bandwidth package.

7. Click OK.

6 Step 5: Test network connectivity

This topic describes how to test the network connectivity between two network instances attached to a CEN instance.

Prerequisites

Before testing the connectivity, make sure that the following conditions are met:

- A cross-region connection bandwidth is configured for the network instances if the two network instances belong to different regions. For more information, see *Step 4: Set a cross-region connection bandwidth*.
- Security group rules that allow intercommunication between the networks exist in the security group. If not, add security group rules. For more information, see *#unique_10*.

Context

The following table describes two ECS instances (named ECS 1 and ECS 2) that are deployed in China (Hangzhou) and China (Shanghai) respectively.

Configuration	ECS 1	ECS 2
Private IP address	192.xx.1.41	192.xx.136.60
Region	China (Shanghai)	China (Hangzhou)

Procedure

1. Log on to ECS 2.
2. Use `ping` command to `ping` the private IP address of ECS 1 to check whether the connection between ECS 1 and ECS 2 is established.

```
C:\Users\Administrator>ping 192.168.1.41

Pinging 192.168.1.41 with 32 bytes of data:
Reply from 192.168.1.41: bytes=32 time<1ms TTL=128
Reply from 192.168.1.41: bytes=32 time<1ms TTL=128
Reply from 192.168.1.41: bytes=32 time<1ms TTL=128
Reply from 192.168.1.41: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.41:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

7 (Optional) Step 6: Set alarms

This topic describes how to set alarm rules for physical connections, bandwidth packages and cross-region connections. By doing so, you can monitor the usage of these resources and avoid service interruptions when any resource limit is reached.

Set alarm rules for a physical connection

Due to system upgrades, the alarm setting function for physical connections will be temporarily disabled from November 22, 2018 to October 1, 2019. Sorry for the inconvenience.

To set alarm rules for a physical connection configured with health checks, follow these steps:

1. **Log on to the *CEN console*.**
2. **In the left-side navigation pane, click Health Check.**
3. **Select the region to which the CEN instance belongs, and then click Set Alarm in the Monitor column.**
4. **On the Create Alarm Rule page, set the parameters as needed, and then click OK.**

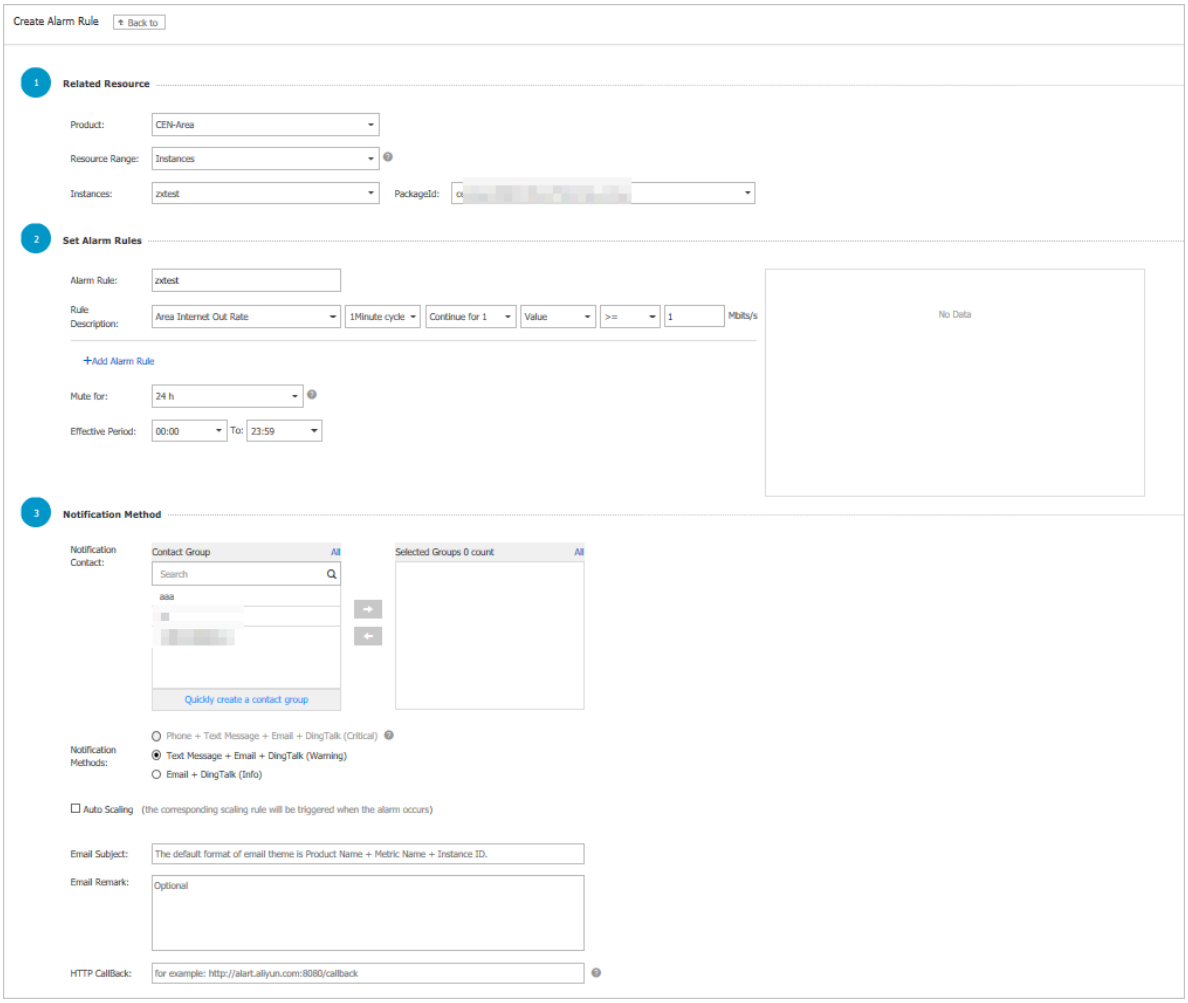
Set alarm rules for a bandwidth package

To set alarm rules for a bandwidth package of a CEN instance, follow these steps:

1. **On the Instances page, find the target CEN instance, and then click Manage in the Actions column.**
2. **Click the Bandwidth Packages tab, find the target bandwidth package, and then click Set Alarm in the Monitor column.**

3. **On the Create Alarm Rule page, set the parameters as needed, and then click OK.**

   You can set alarm rules for the Area Internet Out Rate and the Area Internet Out Rate Percent. You can set the alarm threshold and alarm conditions based on your specific service needs.



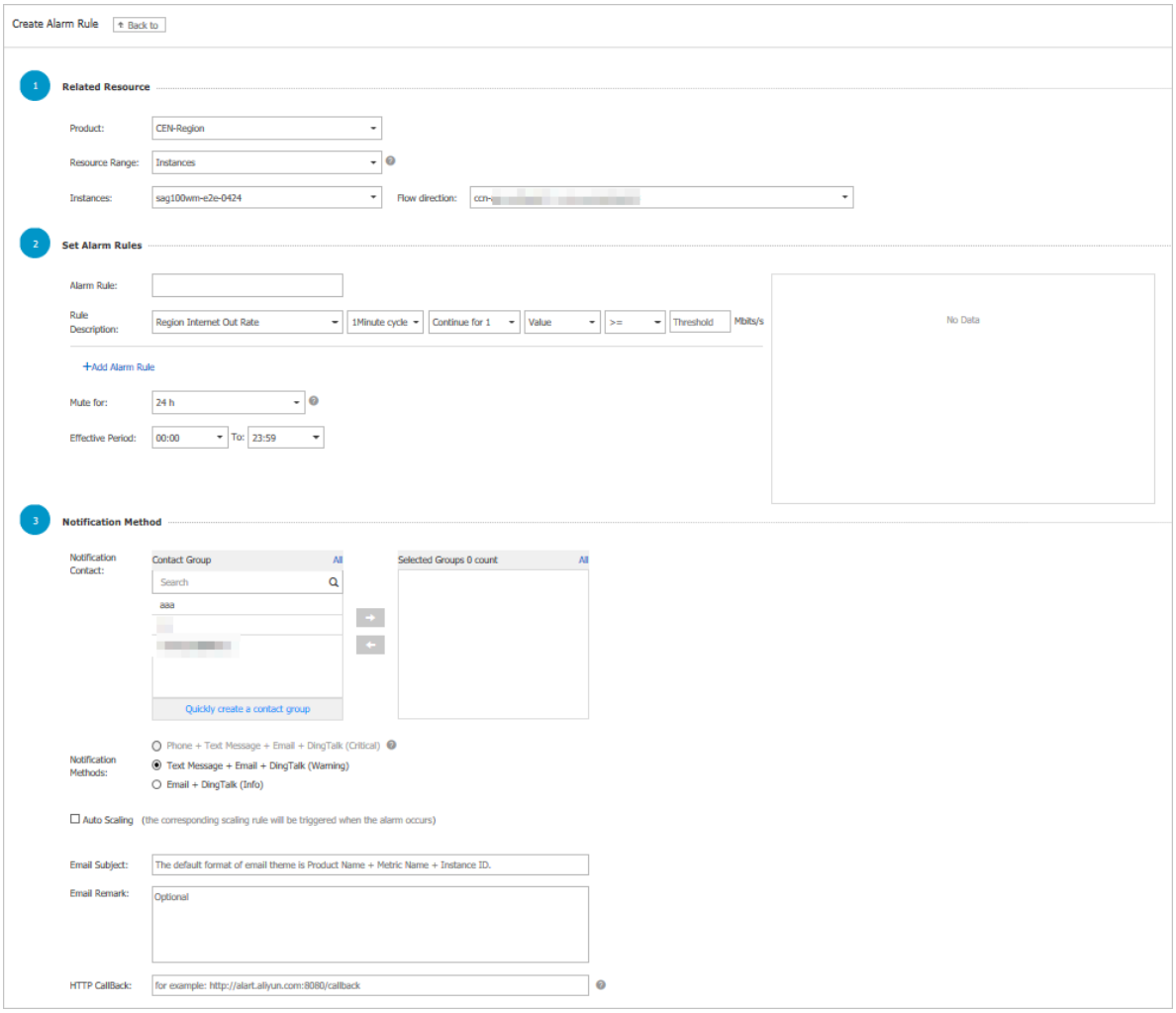
Set alarm rules for a region connection

To set alarm rules for a region connection, follow these steps:

1. **Click the Region Connections tab, find the target connection, and then click Set Alarm in the Monitor column.**

2. **On the Create Alarm Rule page, set the parameters as needed, and then click OK.**

   You can set alarm rules for the Area Internet Out Rate and the Area Internet Out Rate Percent. You can set the alarm threshold and alarm conditions based on your specific service needs.



8 (Optional) Step 7: Advanced configurations

This topic describes the advanced configurations of a Cloud Enterprise Network (CEN). You can use the advanced configurations to manage your private networks.

A CEN provides the following advanced configurations:

- **Access to cloud services**

  Network instances attached to a CEN instance can access the PrivateZone service through the CEN instance. For more information, see *#unique_13*.

- **Route map**

  By using the route map function, you can filter route information and modify route attributes to manage the communication between network instances attached to a CEN instance. For more information, see *#unique_14*.

- **High Availability**

  You can establish high-availability hybrid cloud networks by using health check, physical connections, VPN Gateways, and other Alibaba Cloud products.