

ALIBABA CLOUD

Alibaba Cloud

云企业网

Quick Start

Document Version: 20220322

 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 <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1. Use CEN to enable intra-region network communication	05
2. Use CEN to enable inter-region network communication	10

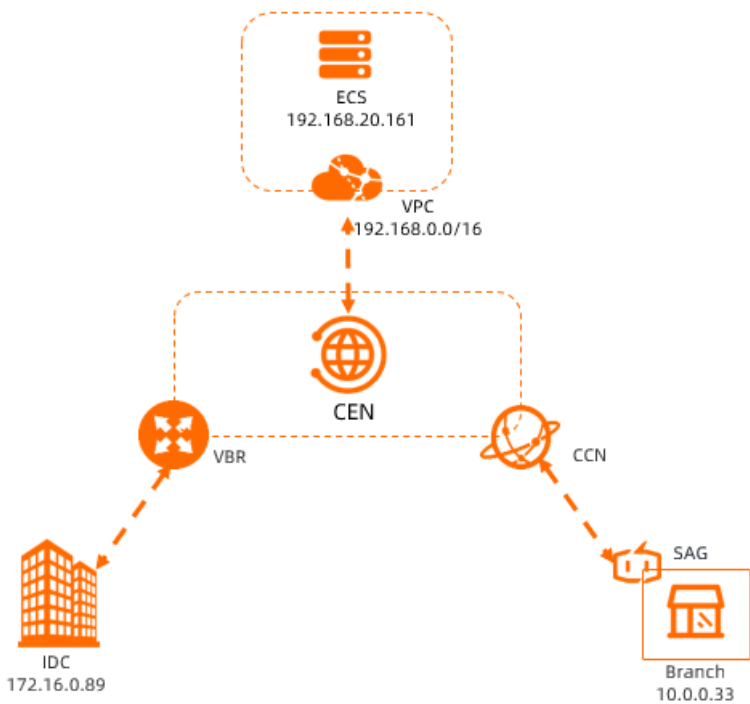
1. Use CEN to enable intra-region network communication

Cloud Enterprise Network (CEN) allows you to build a global network that consists of hybrid clouds and distributed systems. You can attach virtual private clouds (VPCs), virtual border routers (VBRs), and Cloud Connect Network (CCN) instances to the same CEN instance to enable network communication. This topic describes how to use CEN to enable intra-region network communication.


Scenario

The following scenario is used in this topic. A company has a data center in Hangzhou. The data center is connected to Alibaba Cloud through Express Connect circuits and VBRs. The company has a branch office in Hangzhou, whose network is connected to Alibaba Cloud through Smart Access Gateway (SAG) and CCN. The company has a VPC in the China (Hangzhou) region. Elastic Compute Service (ECS) instances are deployed in the VPC.

Due to business growth, the company wants to use CEN to enable network communication between the data center and the VPC, and between the branch office and the VPC.



The following table describes the CIDR blocks that are allocated to the networks.

 **Notice** Make sure that the CIDR blocks do not overlap.

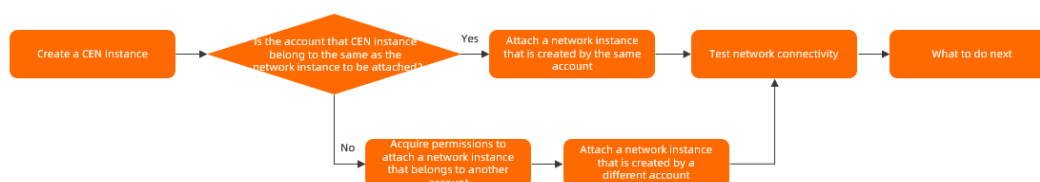
Item	VPC	VBR	Data center	Branch office
------	-----	-----	-------------	---------------

Item	VPC	VBR	Data center	Branch office
CIDR block	192.168.0.0/16	<ul style="list-style-type: none"> VLAN ID: 0 IPv4 CIDR block at the Alibaba Cloud side: 172.16.1.2/30 IPv4 CIDR block at the customer side: 172.16.1.1/30 	Data center CIDR block: 172.16.0.0/16	Branch office CIDR block: 10.0.0.0/16
Server IP address	ECS instance IP address: 192.168.20.161	N/A	IP address of a server in the data center: 172.16.0.89	IP address of a server in the branch office: 10.0.0.33

Procedure

The following figure shows the procedure for enabling intra-region network communication.

- If the CEN instance and the network instances that you want to attach to the CEN instance belong to the same Alibaba Cloud account, you can attach the network instances to the CEN instance.
- If the CEN instance and the network instances that you want to attach to the CEN instance belong to different Alibaba Cloud accounts, you must grant permissions to the accounts before you can attach the network instances. After the required permissions are granted to the accounts, you can attach the network instances to the same CEN instance to enable private network communication.



Prerequisites

- The data center is connected to Alibaba Cloud through Express Connect circuits and VBRs. For more information, see [Connect to an ECS instance from a data center by using an Express Connect circuit](#).
- The network of the branch office is connected to Alibaba Cloud through SAG and CCN. For more information, see [SAG Tutorials](#).
- A VPC is deployed in the China (Hangzhou) region. ECS instances are deployed in the VPC. For more information, see [Create an IPv4 VPC](#).
- You are aware of the security group rules of the ECS instance that is deployed in the VPC, and the access control rules of the data center and the branch office. Make sure that the security rules and access control rules allow the VPC to communicate with the data center and branch office network. For more information, see [Query security group rules](#) and [Add security group rules](#).
- Make sure that the network instances are not attached to another CEN instance.


Step 1: Create a CEN instance

When you create a CEN instance, you can select a network instance that belongs to the same account as the CEN instance and attach the network instance to the CEN instance.

1. Log on to the [CEN console](#).
2. On the **Instances** page, click **Create CEN Instance**.
3. In the **Create CEN Instance** panel, set the following parameters and click **OK**.
 - **Name**: Enter a name for the CEN instance.
The name must be 2 to 128 characters in length and can contain digits, hyphens (-), and underscores (_). It must start with a letter.
 - **Description**: Enter a description for the CEN instance.
The description must be 2 to 256 characters in length, and cannot start with `http://` or `https://`. You can leave this parameter empty.
 - **Attach Network**: Attach network instances that belong to the same Alibaba Cloud account to the CEN instance.
 - **Network Type**: Select the type of network instance. **VPC** is selected in this example.
 - **Region**: Select the region where the network instance is created. In this example, **China (Hangzhou)** is selected.
 - **Networks**: Select the network instance that you want to attach.

Step 2: Attach network instances to the CEN instance

Attach the network instances that need to communicate with each other to the same CEN instance. 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.

 **Note** In this example, a VPC is attached to the CEN instance in [Step 1: Create a CEN instance](#). You must also attach the VBR and CCN instance 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 the instance ID.
3. Click the **Networks** tab and then click **Attach Network**.
4. In the **Attach Network** panel, click the **Your Account** tab.
5. Set the following parameters to attach the network instance to the CEN instance and click **OK**:
 - **Network Type**: Select the type of network instance that you want to attach. In this example, **Virtual Border Router (VBR)** is selected.
 - **Region**: Select the region where the network instance is created. In this example, **China (Hangzhou)** is selected.
 - **Networks**: Select the VBR that you want to attach.
6. Repeat this step to attach the CCN instance to the CEN instance.

You must acquire the required permissions from the account of the network instance that you want to attach. After you acquire the permissions, you must obtain the account ID and the ID of the network instance that you want to attach.

- You must acquire the required permissions from the Alibaba Cloud account to which the VPC belongs before you attach the VPC. For more information, see [VPC authorization](#).
- You must acquire the required permissions from the Alibaba Cloud account to which the VBR belongs before you attach the VBR. For more information, see [VBR authorization](#).
- You must acquire the required permissions from the Alibaba Cloud account to which the CCN instance

belongs before you attach the CCN instance. For more information, see [CCN instance authorization](#).

1. Log on to the [CEN console](#).
2. On the **Instances** page, find the CEN instance that you want to manage and click the instance ID.
3. Click the **Networks** tab and then click **Attach Network**.
4. In the **Attach Network** panel, click the **Different Account** tab.
5. Set the following parameters to attach the network instance to the CEN instance and click **OK**:
 - **Owner Account**: Enter the ID of the account to which the network instance belongs.
 - **Network Type**: Select the type of network instance to attach. In this example, **Virtual Border Router (VBR)** is selected.
 - **Region**: Select the region where the network instance is created. In this example, **China (Hangzhou)** is selected.
 - **Networks**: Select the VBR that you want to attach.
6. Repeat this step to attach the CCN instance to the CEN instance.

Attach a network instance that is created by the same account

Attach a network instance that is created by a different account

Step 3: Test network connectivity

After you attach the network instances to the CEN instance, you can run the `ping` command to test the network connectivity.

1. Log on to the ECS instance. For more information, see [Connection methods](#).
2. Run the `ping` command to test whether the ECS instance is connected to the data center.

```
ping 172.16.0.89
```

If you receive an echo reply packet, it indicates that the ECS instance and the data center are connected.

3. Run the `ping` command to test whether the ECS instance is connected to the branch office.

```
ping 10.0.0.33
```

If you receive an echo reply packet, it indicates that the ECS instance and the branch office are connected.

What to do next

- You can create alert rules in CloudMonitor to monitor the VBRs, bandwidth plans, and bandwidth usage for inter-region connections. Resource exhaustion may disrupt services.
 - For more information about how to set alerts rules for VBRs, see [Monitor Express Connect circuits](#).
 - For more information about how to set alerts rules for bandwidth plans, see [Monitor bandwidth plans](#).
 - For more information about how to set alerts rules for bandwidth usage of inter-region connections, see [Monitor region connections](#).
Alert rules for bandwidth usage of inter-region connections apply only to scenarios in which network instances communicate with each other across regions. For more information, see [Use a bandwidth plan](#) and [Manage bandwidth for cross-region connections](#).

- Network instances that are attached to a CEN instance can access cloud services through the CEN instance. For more information, see [Access cloud services](#) and [PrivateZone overview](#).
- You can configure route policies to filter and modify routes. This allows you to manage network communication in the cloud. For more information, see [Route map overview](#).

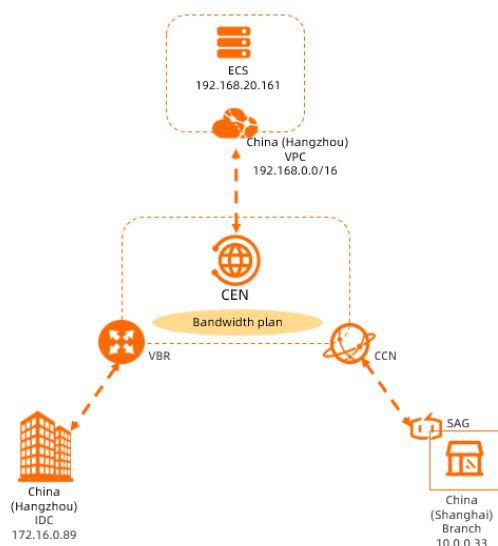
2. Use CEN to enable inter-region network communication

Cloud Enterprise Network (CEN) allows you to build a global network that consists of hybrid clouds and distributed systems. You can attach virtual private clouds (VPCs), virtual border routers (VBRs), and Cloud Connect Network (CCN) instances to the same CEN instance to enable network communication. This topic describes how to use CEN to enable inter-region network communication.

Scenario

The following scenario is used in this topic. A company has a data center in Hangzhou. The data center is connected to Alibaba Cloud through Express Connect circuits and VBRs. The company has a branch office in Shanghai, whose network is connected to Alibaba Cloud through Smart Access Gateway (SAG) and CCN. The company has a VPC in the China (Hangzhou) region. Elastic Compute Service (ECS) instances are deployed in the VPC.

Due to business growth, the company wants to use CEN to enable network communication between the data center and the VPC, and between the branch office and the VPC.



The following table describes the CIDR blocks allocated to the networks.

Notice Make sure that the CIDR blocks do not overlap.

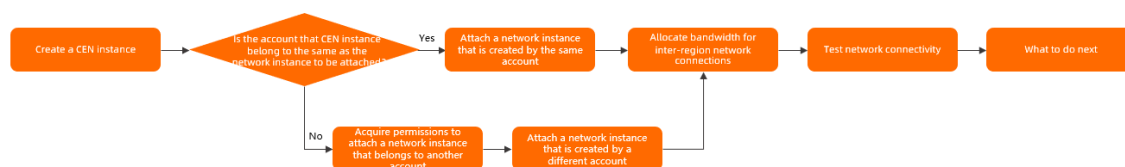
Item	VPC	VBR	Data center	Branch office
Region	China (Hangzhou)	China (Hangzhou)	China (Hangzhou)	China (Shanghai)

Item	VPC	VBR	Data center	Branch office
CIDR block	192.168.0.0/16	<ul style="list-style-type: none"> VLAN ID: 0 IPv4 CIDR block at the Alibaba Cloud side: 172.16.1.2/30 IPv4 CIDR block at the customer side: 172.16.1.1/30 	Data center CIDR block: 172.16.0.0/16	Branch office CIDR block: 10.0.0.0/16
Server IP address	ECS instance IP address: 192.168.20.161	N/A	IP address of a server in the data center: 172.16.0.89	IP address of a server in the branch office: 10.0.0.33

Procedure

The following figure shows the procedure for enabling inter-region network communication.

- If the CEN instance and the network instances that you want to attach to the CEN instance belong to the same Alibaba Cloud account, you can attach the network instances to the CEN instance.
- If the CEN instance and the network instances that you want to attach to the CEN instance belong to different Alibaba Cloud accounts, you must grant permissions to the accounts before you can attach the network instances. After the required permissions are granted to the accounts, you can attach the network instances to the same CEN instance to enable private network communication.



Prerequisites

- The data center is connected to Alibaba Cloud through Express Connect circuits and VBRs. For more information, see [Connect to an ECS instance from a data center by using an Express Connect circuit](#).
- The branch office is connected to Alibaba Cloud through SAG and CCN. For more information, see [SAG Tutorials](#).
- A VPC is deployed in the China (Hangzhou) region. ECS instances are deployed in the VPC. For more information, see [Create an IPv4 VPC](#).
- You are aware of the security group rules of the ECS instance that is deployed in the VPC, and the access control rules of the data center and the branch office. Make sure that the security rules and access control rules allow the VPC to communicate with the data center and branch office network. For more information, see [Query security group rules](#) and [Add security group rules](#).
- Make sure that the network instances are not attached to another CEN instance.


Step 1: Create a CEN instance

When you create a CEN instance, you can select a network instance that belongs to the same account as the CEN instance and attach the network instance to the CEN instance.

1. Log on to the [CEN console](#).
2. On the **Instances** page, click **Create CEN Instance**.
3. In the **Create CEN Instance** panel, set the following parameters and click **OK**.
 - **Name**: Enter a name for the CEN instance.
The name must be 2 to 128 characters in length and can contain digits, hyphens (-), and underscores (_). It must start with a letter.
 - **Description**: Enter a description for the CEN instance.
The description must be 2 to 256 characters in length, and cannot start with `http://` or `https://`. You can leave this parameter empty.
 - **Attach Network**: Attach network instances that belong to the same Alibaba Cloud account to the CEN instance.
 - **Network Type**: Select the type of network instance. **VPC** is selected in this example.
 - **Region**: Select the region where the network instance is created. In this example, **China (Hangzhou)** is selected.
 - **Networks**: Select the network instance that you want to attach.

Step 2: Attach network instances to the CEN instance

Attach the network instances that need to communicate with each other to the same CEN instance. 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.

 **Note** In this example, a VPC is attached to the CEN instance. You must also attach the VBR and CCN instance 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 the instance ID.
3. Click the **Networks** tab and then click **Attach Network**.
4. In the **Attach Network** panel, click the **Your Account** tab.
5. Set the following parameters to attach the network instance to the CEN instance and click **OK**:
 - **Network Type**: Select the type of network instance that you want to attach. In this example, **Virtual Border Router (VBR)** is selected.
 - **Region**: Select the region where the network instance is created. In this example, **China (Hangzhou)** is selected.
 - **Networks**: Select the VBR that you want to attach.
6. Repeat this step to attach the CCN instance to the CEN instance.

You must acquire the required permissions from the account of the network instance that you want to attach. After you acquire the permissions, you must obtain the account ID and the ID of the network instance that you want to attach.

- You must acquire the required permissions from the Alibaba Cloud account to which the VPC belongs before you attach the VPC. For more information, see [VPC authorization](#).
- You must acquire the required permissions from the Alibaba Cloud account to which the VBR belongs before you attach the VBR. For more information, see [VBR authorization](#).
- You must acquire the required permissions from the Alibaba Cloud account to which the CCN instance

belongs before you attach the CCN instance. For more information, see [CCN instance authorization](#).

1. Log on to the [CEN console](#).
2. On the **Instances** page, find the CEN instance that you want to manage and click the instance ID.
3. Click the **Networks** tab and then click **Attach Network**.
4. In the **Attach Network** panel, click the **Different Account** tab.
5. Set the following parameters to attach the network instance to the CEN instance and click **OK**:
 - **Owner Account**: Enter the ID of the account to which the network instance belongs.
 - **Network Type**: Select the type of network instance to attach. In this example, **Virtual Border Router (VBR)** is selected.
 - **Region**: Select the region where the network instance is created. In this example, **China (Hangzhou)** is selected.
 - **Networks**: Select the VBR that you want to attach.
6. Repeat this step to attach the CCN instance to the CEN instance.

Attach a network instance that is created by the same account

Attach a network instance that is created by a different account

Step 3: Allocate bandwidth for inter-region network connections


Network instances that are deployed in the same region and attached to the same CEN instance can communicate with each other. If you want to enable network communication between network instances that are deployed in different regions, you must purchase a bandwidth plan and allocate bandwidth for inter-region connections.

Note

- The sum of the bandwidth values set for all the inter-region connections cannot exceed the maximum bandwidth value of the bandwidth plan.
- By default, CEN provides 1 Kbit/s of inter-region bandwidth that you can use to test the connectivity of inter-region IPv4 networks.
- When you purchase a bandwidth plan, you must specify the areas that you want to connect. An area is a collection of Alibaba Cloud regions. For more information about bandwidth plans, see [Work with a bandwidth plan](#).

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. Purchase a bandwidth plan.
 - i. On the details page of the CEN instance, click **Bandwidth Plans**.
 - ii. On the **Bandwidth Plans** tab, click **Purchase Bandwidth Plan (Subscription)**.

- iii. Set the following parameters, click **Buy Now**, and then complete the payment.

Parameter	Description
CEN ID	Select the CEN instance for which you want to purchase a bandwidth plan. After you purchase a bandwidth plan, the system automatically associates the bandwidth plan with the CEN instance.
Area A	Select the areas between which you want to enable inter-region communication.  Notice After you purchase the bandwidth plan, you cannot change the specified areas.
Area B	
Billing Method	Displays the billing method of the bandwidth plan. Default value: By bandwidth .
Bandwidth	Select a bandwidth value. Unit: Mbit/s.
Name	Enter a name for the bandwidth plan.
Duration	Select a subscription duration for the bandwidth plan. You can select Auto-renewal to enable auto-renewal for the bandwidth plan.
Resource Group	Select the resource group to which the bandwidth plan belongs.

4. Set the inter-region connection bandwidth.

- i. On the details page, click the **Region Connections** tab.
- ii. Click the **Region Connections** tab, and then click **Set Region Connection**.
- iii. In the **Set Region Connection** panel, set the following parameters and click **OK**:
 - **Bandwidth Plans**: Select the bandwidth plan that you purchased.
 - **Connected Regions**: Select the regions that you want to connect.
 - **Bandwidth**: Specify the bandwidth that you want to allocate. Unit: Mbit/s.

Step 4: Test the network connectivity

After you attach the network instances to the CEN instance, you can run the **ping** command to test the network connectivity.

1. Log on to the ECS instance. For more information, see [Connection methods](#).
2. Run the `ping` command to test whether the ECS instance is connected to the data center.

```
ping 172.16.0.89
```

If you receive an echo reply packet, it indicates that the ECS instance and the data center are connected.

3. Run the `ping` command to test whether the ECS instance is connected to the branch office.

```
ping 10.0.0.33
```

If you receive an echo reply packet, it indicates that the ECS instance and the branch office are connected.

What to do next

- You can create alert rules in CloudMonitor to monitor the VBRs, bandwidth plans, and bandwidth usage for inter-region connections. Resource exhaustion may disrupt services.
 - For more information about how to set alert rules for VBRs, see [Monitor Express Connect circuits](#).
 - For more information about how to set alert rules for bandwidth plans, see [Monitor bandwidth plans](#).
 - For more information about how to set alert rules for bandwidth usage of inter-region connections, see [Monitor region connections](#).
Alert rules for bandwidth usage of inter-region connections apply only to scenarios in which network instances communicate with each other across regions. For more information, see [Use a bandwidth plan](#) and [Manage bandwidth for cross-region connections](#).
- Network instances that are attached to a CEN instance can access cloud services through the CEN instance. For more information, see [Access cloud services](#) and [PrivateZone overview](#).
- You can configure route policies to filter and modify routes. This allows you to manage network communication in the cloud. For more information, see [Route map overview](#).