

Alibaba Cloud Cloud Enterprise Network

User Guide

Issue: 20190906

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, consequential, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK.
<code>Courier</code> font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Manage CEN instances.....	1
1.1 Create a CEN instance.....	1
1.2 Delete a CEN instance.....	1
2 Manage networks.....	3
2.1 Attach a VPC or VBR to a CEN instance through the instance details page....	3
2.2 Cross-account authorization.....	3
2.3 Attach networks.....	7
2.4 Detach a network instance from a CEN instance.....	10
3 Bandwidth package management.....	12
3.1 Purchase a bandwidth package.....	12
3.2 Associate a bandwidth package with a CEN instance.....	13
3.3 Disassociate a bandwidth package from a CEN instance.....	14
3.4 Modify the bandwidth of a bandwidth package.....	14
3.5 Renew a Subscription bandwidth package.....	15
4 Manage cross-region connection bandwidth.....	16
4.1 Configure a cross-region connection bandwidth.....	16
4.2 Modify a cross-region connection bandwidth.....	17
4.3 Delete a cross-region connection bandwidth.....	18
5 Manage routes.....	19
5.1 Enable overlapping routing.....	19
5.2 Publish a route to CEN.....	20
5.3 Withdraw a route from CEN.....	22
5.4 View routes.....	23
5.4.1 View CEN routes in the CEN console.....	23
5.4.2 View CEN routes in the VPC route table.....	25
5.4.3 View CEN routes in the VBR route table.....	25
6 Routing policies.....	26
6.1 Route map overview.....	26
6.2 Add a route map.....	38
6.3 Modify a route map.....	41
6.4 Delete a route map.....	41
7 Access to cloud services.....	42
7.1 PrivateZone overview.....	42
7.2 PrivateZone.....	42
7.2.1 Configure PrivateZone access.....	42
7.2.2 Grant permissions to CCN.....	44

8 Health check.....	52
8.1 Configure the health check function.....	52
8.2 Delete health check settings.....	52
8.3 Modify health check settings.....	53
9 Monitoring.....	54
9.1 Set alarms.....	54
9.2 View the monitoring data of a CEN instance.....	56
10 Flow logs.....	58
10.1 Flow log overview.....	58
10.2 Create a flow log.....	61
10.3 View flow logs.....	62
10.4 Start a flow log.....	62
10.5 Stop a flow log.....	63
10.6 Modify a flow log.....	63
10.7 Delete a flow log.....	64
11 Increase the quota of a cloud resource.....	65

1 Manage CEN instances

1.1 Create a CEN instance

This topic describes how to create a CEN instance for private 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 <code>http ://</code> or <code>https ://</code> .
Description	Enter a description for the CEN instance. The description must be 2 to 256 characters in length. It cannot start with <code>http ://</code> or <code>https ://</code> .
Attach Network	You can attach network instances under the same account to the CEN instance. For more information, see #unique_5 .

1.2 Delete a CEN instance

This topic describes how to delete a 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 [#unique_7](#).
- If a bandwidth package is associated with the CEN instance, disassociate the bandwidth package first. For more information, see [#unique_8](#).

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 Cloud Enterprise Network Instance dialog box, click OK.

2 Manage networks

2.1 Attach a VPC or VBR to a CEN instance through the instance details page

You can attach a VPC or a Virtual Border Router (VBR) to a Cloud Enterprise Network (CEN) instance of the same account directly from the instance details page.

Attach a VPC through the details page

To attach a VPC to a CEN instance through the details page, follow these steps:

1. Log on to the [VPC console](#).
2. Select the region of the target VPC.
3. On the VPCs page, find the target VPC and click Actions in the Manage column.
4. On the VPC Details page, click Attach to CEN.
5. In the Attach to CEN dialog box, select a CEN instance and click OK.

Attach a VBR through the details page

To attach a VBR to a CEN instance through the details page, follow these steps.

1. Log on to the [Express Connect console](#).
2. In the left-side navigation pane, choose Physical Connections > Virtual Border Routers (VBRs).
3. Select the region of the target VBR.
4. On the Virtual Border Routers (VBRs) page, find the target VBR and click the VBR ID.
5. In the Basic Information section, click Join CEN.
6. In the Join CEN dialog box, select a CEN instance and click OK.

2.2 Cross-account authorization

Before you attach a network of a different account to a Cloud Enterprise Network (CEN) instance, you must obtain permissions from the network. After obtaining

permissions, you must obtain the ID of the account to which the network belongs and the instance ID of the network.

Prerequisites

- The ID of the target CEN instance is obtained.
- The ID of the account to which the target CEN instance belongs is obtained.

Obtain permissions from a VPC

To obtain permissions from a VPC, follow these steps:



Notice:

If you grant permissions to another account, this account can attach your networks to its CEN instances and gain access to your networks. Therefore, we recommend that you exercise caution when you grant permissions to other accounts.

1. Log on to the [VPC console](#) by using the credentials of the account to which the target VPC belongs.
2. Select the region of the target VPC.
3. On the VPCs page, find the target VPC, and click Actions in the Manage column.
4. In the CEN cross account authorization information section, click CEN Cross Account Authorization.
5. In the displayed Attach to CEN dialog box, enter the account ID of the target CEN instance and the ID of the target CEN instance, and then click OK.

VPC Details
Detach CEN
Enable ClassicLink
Refresh
Delete

VPC Details

ID vpc-bp1r1...yzaa
IPv4 CIDR Block 192.168.0.0/16
Status Available
Default VPC No
Instance Attachment Details CEN ID :
Owner Account :
Status : attached
Resource Group 默认资源组

Name VPC_Rick_Song
Created At 06/09/2019, 21:58:48
Description - Edit
ClassicLink Disabled
Region China (Hangzhou)

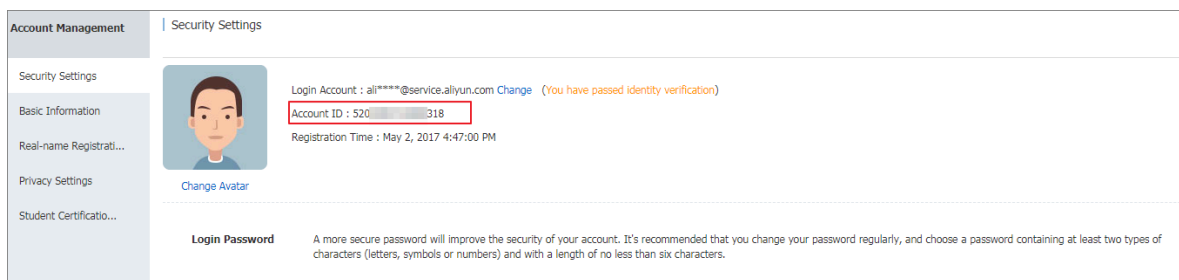
VRouter Basic Information

ID vrt-bp1r1...05c83
Created At 06/09/2019, 21:58:48
Name - Edit
Description - Edit

CEN cross account authorization information
CEN Cross Account Authorization

Peer Account UID	Peer Account CEN ID	Authorized At	Actions
1231...9123	cen-7qth...4gsu	08/21/2019, 13:56:00	Unauthorize

- Record the VPC ID and the account ID of the VPC. You can view the account ID on the [Account Management](#) page.



Obtain permissions from a VBR

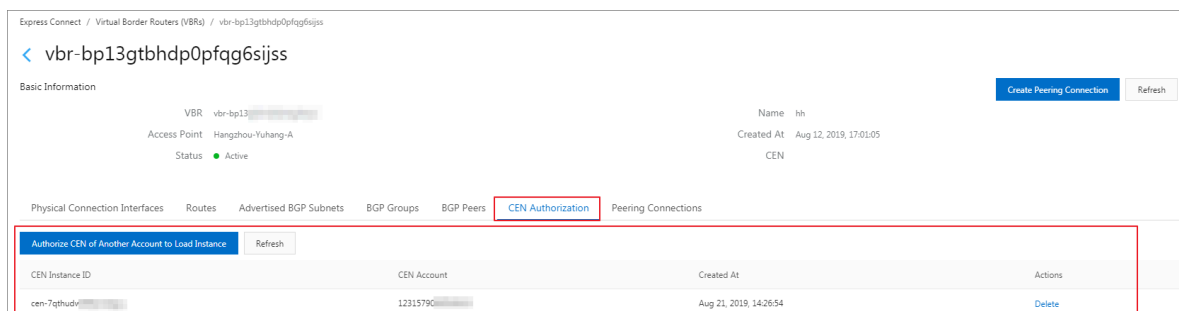
To obtain permissions from a VBR, follow these steps:



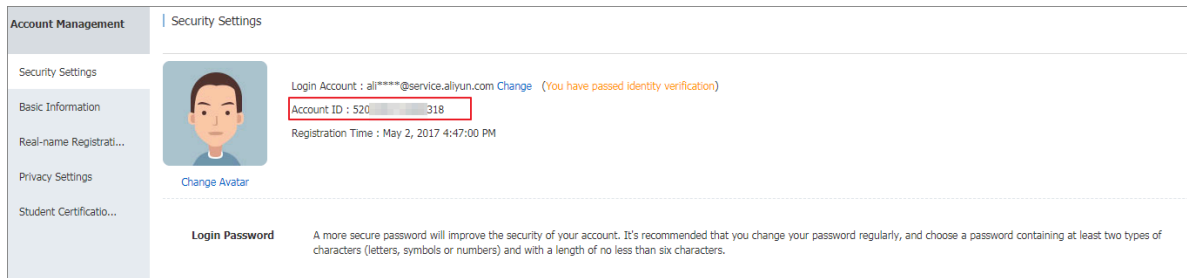
Notice:

If you grant permissions to another account, this account can attach your networks to its CEN instances and gain access to your networks. Therefore, we recommend that you exercise caution when you grant permissions to other accounts.

- Log on to the [Express Connect console](#) by using the credentials of the account to which the target VBR belongs.
- In the left-side navigation pane, choose Physical Connections > Virtual Border Routers (VBRs).
- Select the region of the VBR.
- On the Virtual Border Routers (VBRs) page, find the target VBR and click the VBR ID.
- Click the CEN authorization tab, and then click Authorize CEN of Another Account to Load Instance.
- In the Authorize CEN of Another Account to Load Instance dialog box, enter the ID of the target CEN instance and the account ID of the target CEN instance, and click OK.



7. Record the VBR ID and the account ID of the VBR. You can view the account ID on the [Account Management](#) page.



Obtain permissions from a CCN

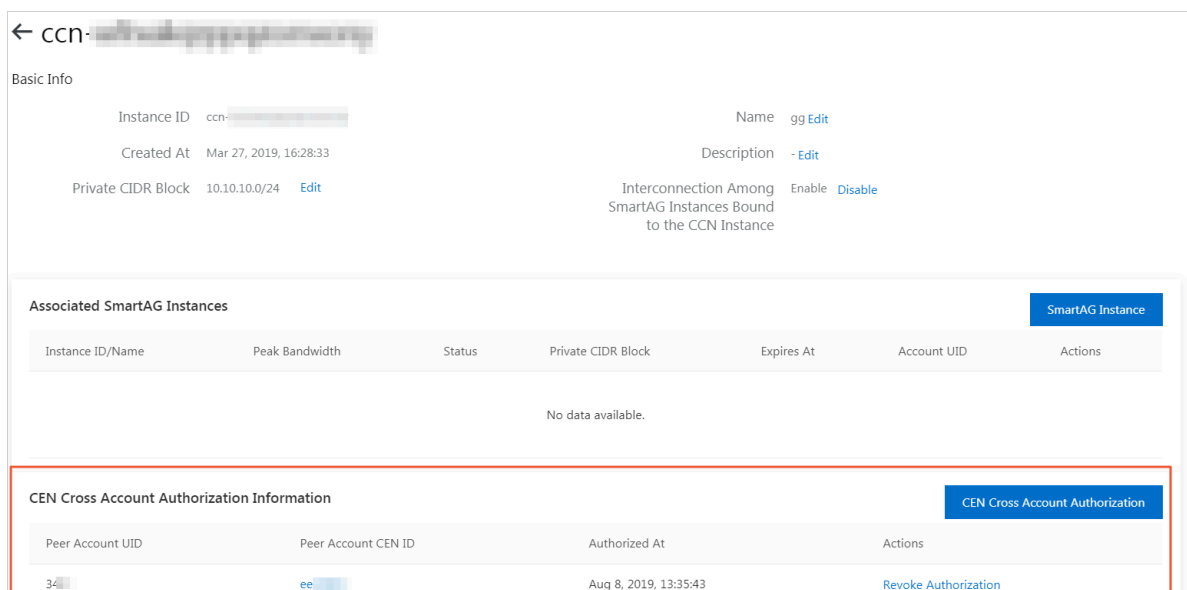
To obtain permissions from a CCN, follow these steps:



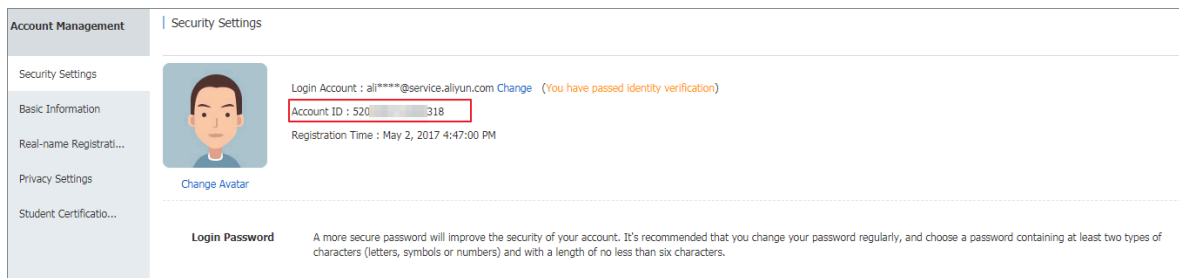
Notice:

If you grant permissions to another account, this account can attach your networks to its CEN instances and gain access to your networks. Therefore, we recommend that you exercise caution when you grant permissions to other accounts.

1. Log on to the [Smart Access Gateway console](#) by using the credentials of the account to which the target CCN belongs.
2. In the left-side navigation pane, click CCN, find the target CCN, and click the instance ID of the CCN.
3. Click CEN Cross Account Authorization, enter the account ID of the target CEN instance and the ID of the CEN instance, and click OK.



- Record the CCN instance ID and the account ID of the CCN. You can view the account ID on the [Account Management](#) page.



What's next

[#unique_5](#)

2.3 Attach networks

You can attach the networks (VPCs, VBRs, and CCNs) that need to communicate with each other to a Cloud Enterprise Network (CEN) instance. CEN automatically learns the routes of the attached networks to achieve intranet communication.

Prerequisites

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

- [#unique_13](#).
- The networks to be attached are not attached to other CEN instances.

Attach a network in the same account

To attach a network in the same account, follow these steps:

- Log on to the [CEN console](#).
- On the Instances page, find the target CEN instance and click the instance ID.
- Click the Networks tab and then click Attach Network.
- Click the Your account tab.
- Network Type: Select the type of the network to be attached.

You can attach VPCs, Virtual Border Routers (VBRs), and Cloud Connect Networks (CCNs).

- Region: Select the region of the network.

7. Networks: Select the instance to be attached.

Attach Network

?

×

Your Account

Different Account

?

Note: You cannot attach networks that are already attached to the CEN instance.

• Network Type

?

VPC

▼

• Region

?

China (Hangzhou)

▼

• Networks

?

vpc-k

...

▼

Contact Us

OK

Cancel

8. Click OK.

Attach a network in a different account



Notice:

Before you attach a network of 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.

For more information, see:

- [#unique_14/unique_14_Connect_42_section_mkn_v7p_lgn](#)

- [#unique_14/unique_14_Connect_42_section_2kc_03o_0us](#)
- [#unique_14/unique_14_Connect_42_section_gs1_agk_3o9](#)

To attach a network in a different account, 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.
6. Network Type: Select the type of the network to be attached.
You can attach VPCs, Virtual Border Routers (VBRs), and Cloud Connect Networks (CCNs).
7. Region: Select the region of the network.

8. Networks: Enter the instance ID of the network to be attached.

Attach Network

Your Account

Different Account

Note: Go to the VPC console, in the properties page of the VPC or virtual border router, authorize the related CEN instance to attach that network. Networks already attached to the CEN instance cannot be attached again.

Owner Account

195 14/128

Network Type

VPC

Region

China (Hangzhou)

Networks

vpc- 22/128

Contact Us

OK

Cancel

9. Click OK.

2.4 Detach a network instance from a CEN instance

This topic describes how to detach a network instance from a CEN instance. After you detach a network instance from a CEN instance, the network instance cannot communicate with other network instances in the CEN instance.

Procedure

1. Log on to the [CEN console](#).

10

Issue: 20190906

2. On the Instances page, find the target CEN instance, and then click Manage in the Actions column.
3. On the Networks tab page, find the target network instance, and then click Detach in the Actions column.
4. In the Detach Network dialog box, click OK.

3 Bandwidth package management

3.1 Purchase a bandwidth package

This topic describes how to purchase a bandwidth package for a CEN instance. After you purchase a bandwidth package, you can set a cross-region bandwidth value to allow mutual access between network instances in different regions. Mutual access between two instances in the same region does not require a bandwidth package.

Context

The bandwidth package of a Cloud Enterprise Network (CEN) instance consists of an interconnection bandwidth and interconnected areas. When you purchase a bandwidth package, you must specify the areas to be interconnected. An area consists of one or more Alibaba Cloud regions.



The following table describes the areas and their respective regions.

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

Procedure

1. Log on to the [CEN console](#).
2. On the Instances page, find the target CEN instance, and then click Manage in the Actions column.
3. On the CEN page, click the Bandwith Packages tab, and then click Buy Bandwidth Package(Subscription).

4. Set the bandwidth package parameters, and then click Buy Now to complete the payment. The following table describes the parameters.

Configuration	Description
CEN ID	Select the CEN instance for which you want to purchase a bandwidth package.
Area	Select one area to be interconnected.  Note: You cannot modify the interconnected areas after you purchase the bandwidth package.
Area	Select the other area to be interconnected.  Note: You cannot modify the interconnected areas after you purchase the bandwidth package.
Bandwidth	Set a bandwidth value for the bandwidth package.
Name	Enter a name for the bandwidth package.
Duration	Select a validity period for the bandwidth package.



Note:

You cannot delete the bandwidth package after you purchase it unless you [open a ticket](#).

3.2 Associate a bandwidth package with a CEN instance

This topic describes how to associate a bandwidth package with a CEN instance. After you purchase a bandwidth package, you must associate it with a CEN instance so that you can configure cross-region interconnection bandwidth.

Prerequisites

The CEN instance is not associated with any bandwidth package between two regions in the same area or in two different areas. For example, if a CEN instance is associated with a bandwidth package between two regions in the Mainland China area, you cannot associate the CEN instance to a bandwidth package between another two regions in the Mainland China area. However, you can associate the CEN instance with a bandwidth package between Mainland China to North America.

Procedure

1. Log on to the [CEN console](#).
2. On the Instances page, find the target CEN instance, and then click Manage in the Actions column.
3. On the CEN page, click Bandwidth Packages tab, find the target bandwidth package, and then click Bind in the Actions column.
4. In the Bind Bandwidth Package dialog box, click OK.

3.3 Disassociate a bandwidth package from a CEN instance

This topic describes how to disassociate a bandwidth package from a CEN instance. After you disassociate a bandwidth package from a CEN instance, you can associate the bandwidth package with another CEN instance.

Prerequisites

The cross-region interconnection bandwidth is deleted from the bandwidth package. For more information, see [#unique_20](#).

Procedure

1. Log on to the [CEN console](#).
2. On the Instances page, find the target CEN instance, and then click Manage in the Actions column.
3. On the CEN page, click the Bandwidth Packages tab, find the target bandwidth package, and then click Unbind in the Actions column.
4. In the Unbind Bandwidth Package dialog box, click OK.

After the bandwidth package is disassociated from the CEN instance, the bandwidth package is still in the available state and incurs fees. To delete the bandwidth package, [open a ticket](#).

3.4 Modify the bandwidth of a bandwidth package

This topic describes how to modify the bandwidth of a bandwidth package that is associated with a Cloud Enterprise Network (CEN) instance. After you modify the bandwidth of a bandwidth package, the new bandwidth takes effect immediately.

Procedure

1. Log on to the [CEN console](#).

2. On the Instances page, find the target CEN instance, and then click Manage in the Actions column.
3. On the CEN page, click the Bandwidth Packages tab, find the target bandwidth package, and then click Downgrade or Upgrade in the Bandwidth column.

**Note:**

Cross-border bandwidth packages (from Mainland China to areas outside Mainland China) do not support bandwidth downgrades.

4. In the Configuration Upgrade area, select a new bandwidth and click Pay.

3.5 Renew a Subscription bandwidth package

This topic describes how to renew a Subscription bandwidth package of a Cloud Enterprise Network (CEN) instance before the bandwidth package expires.

Context

Pay-As-You-Go bandwidth packages cannot be renewed.

Procedure

1. Log on to the [CEN console](#).
2. On the Instances page, find the target CEN instance, and then click Manage in the Actions column.
3. On the CEN page, click the Bandwidth Packages tab, find the target bandwidth package, and then click Renew in the Actions column.
4. On the Renew page, select a renewal duration, click Pay, and then complete the payment.

4 Manage cross-region connection bandwidth

4.1 Configure a cross-region connection bandwidth

This topic describes how to configure a cross-region connection bandwidth. To connect networks in different regions, you must configure a cross-region connection bandwidth after purchasing a bandwidth package.

Context

The sum of all cross-region connection bandwidth values cannot exceed the bandwidth of the bandwidth package. By default, 1 Kbit/s bandwidth is provided for cross-region connections. This default bandwidth is provided for you to perform connectivity tests. To run normal services, you must buy a bandwidth package and set a proper cross-region connection bandwidth.

Assume that you have bought a bandwidth package of 20 Mbit/s for a Cloud Enterprise Network (CEN) instance and the connected areas are Mainland China and North America. You can set a cross-region connection bandwidth between US (Virginia) and China (Hangzhou), China (Shanghai), China (Shenzhen), or other regions. However, the total bandwidth values set for all cross-region connections cannot exceed 20 Mbit/s.

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. Click the Region Connections tab, and click Set Region Connection.
4. In the displayed Set Region Connection dialog box, configure the cross-region connection bandwidth and click OK.

Configuration	Description
Bandwidth Package	Select the bandwidth package attached to the CEN instance.
Connected Regions	Select the regions to be connected.

Configuration	Description
Bandwidth	<p>Enter the required bandwidth value for the connected regions.</p> <p>The sum of all cross-region connection bandwidth values cannot exceed the bandwidth of the bandwidth package.</p> <p>Assume that you have bought a bandwidth package of 20 Mbit/s for a CEN instance and the connected areas are Mainland China and North America. You can set a cross-region connection bandwidth between US (Virginia) and China (Hangzhou), China (Shanghai), China (Shenzhen), or other regions. However, the total bandwidth values set for all the cross-region connections cannot exceed 20 Mbit/s.</p>

4.2 Modify a cross-region connection bandwidth

This topic describes how to modify a cross-region connection bandwidth. After you configure a cross-region connection bandwidth, you can modify the cross-region connection bandwidth value as needed.

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. Click the Region Connections tab.
4. On the Region Connections tab, find the target cross-region connection, and click Modify in the Bandwidth column.
5. In the displayed Set Region Connection dialog box, enter a new bandwidth value, and click OK.

The sum of all cross-region connection bandwidth values under a bandwidth package cannot exceed the bandwidth of the bandwidth package.

4.3 Delete a cross-region connection bandwidth

This topic describes how to delete a cross-region connection bandwidth. After you delete a cross-region connection bandwidth, the networks in the connected regions cannot communicate with each other any longer.

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. Click the Region Connections tab, find the target cross-region connection, and then click Delete in the Actions column.
4. In the displayed Delete Region Connection dialog box, click OK.

5 Manage routes

5.1 Enable overlapping routing

This topic describes how to enable the overlapping routing function of a Cloud Enterprise Network (CEN) instance. After the overlapping routing function is enabled, CEN can learn overlapping routes that have the same prefix but different netmasks.



Note:

The overlapping routing function is enabled for CEN instances created after March 1, 2019 by default.

Before overlapping routing is enabled

Assume that VPC-A is attached to a CEN instance. A custom route entry with the destination CIDR block of 192.168.1.0/24 and the next hop of an ECS instance is added to VPC-A. By default, CEN will deny all routes with destination IP addresses of 192.168.1.0/x ($1 \leq x \leq 32$) learnt from other attached networks.

Similarly, if a route with the destination CIDR block 192.168.1.0/24 is learnt by VPC-A from CEN, you cannot create any route with the destination CIDR block 192.168.1.0/x ($1 \leq x \leq 32$) in VPC-A, and VPC-A rejects other routes that are sent from CEN with destination CIDR block of 192.168.1.0/x ($1 \leq x \leq 32$).

After overlapping routing is enabled

With overlapping routing enabled, CEN can learn overlapping routes that have the same prefix but different netmasks.

Assume that a custom route with destination CIDR block of 192.168.1.0/24 and the next hop of ECS1 is added to VPC-A which has been attached to a CEN instance. After you enable overlapping routing, routes that are published from other networks in the CEN instance with destination CIDR block of 192.168.0.0/16 can still be accepted by VPC-A.

Also, the routes with the destination CIDR blocks 192.168.1.0/24 and 192.168.0.0/16 can be learned by CEN. CEN uses the longest prefix match algorithm to route traffic.



Note:

After the overlapping routing function is enabled, VPC does not accept routes that are subsets of its VSwitch. Assume that the CIDR block of a VSwitch is 10.0.0.0/16. The VPC to which the VSwitch belongs does not accept routes with the CIDR block 10.0.0.0/24 but accepts routes with the CIDR block 10.0.0.0/8.

Procedure

To enable the overlapping routing function, follow these steps:

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. In the Basic Settings section, click Enable next to Overlapping Routing Function.
4. In the Enable Overlapping Routing dialog box, click OK.



Notice:

After the overlapping routing function is enabled, it cannot be disabled.

5.2 Publish a route to CEN

This topic describes how to publish the route of an attached VPC or Virtual Border Router (VBR) to Cloud Enterprise Network (CEN). After you publish a route of an attached VPC or VBR to a CEN instance, other networks attached to the same CEN instance can learn the route.

Context

The following table lists the route entries that can be published to CEN.



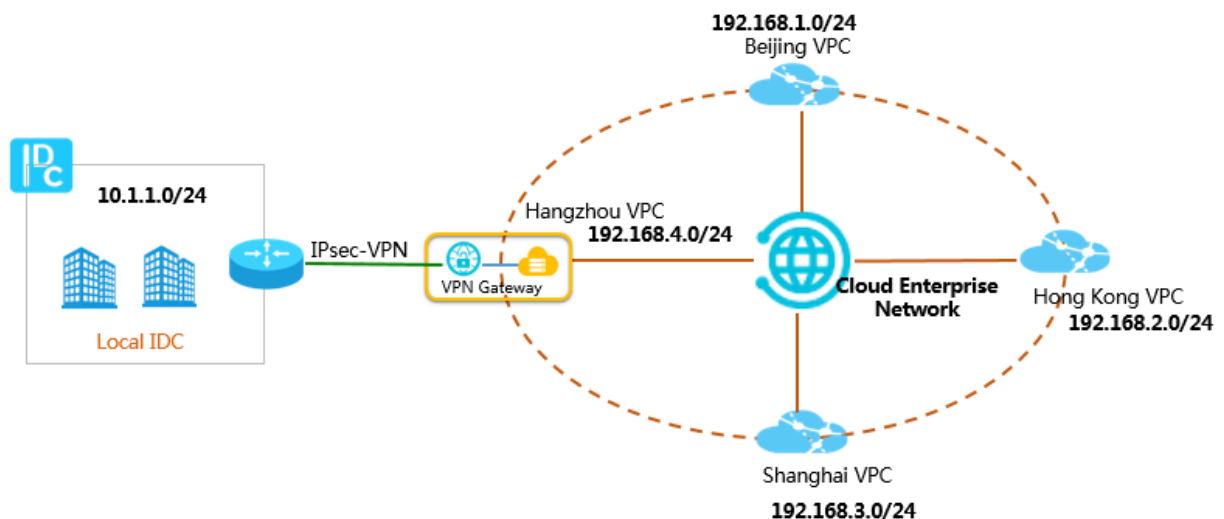
Note:

Currently, the console only supports publishing VPC routes to CEN. If you need to publish VBR routes to CEN, call the PublishRouteEntries API. For more information, see [#unique_30](#).

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

Route entries	Network	Published to CEN by default?
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

As shown in the following figure, four VPCs are attached to a CEN instance. The VPC in the Hangzhou region is configured with a VPN Gateway to connect to the on-premises data center. After you publish the route entry pointing to the VPN Gateway in the Hangzhou VPC to the CEN instance, the other three VPCs learn the route and can also communicate with the on-premises data center.



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 attached 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 Publish in the Route Status in CEN column.
7. In the Publish Route Entry dialog box, 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 [#unique_32](#).

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.

Table 5-1: Region-based route information

Field	Description
Destination CIDR Block	The destination CIDR block of the route.
Type	The type of the route. <ul style="list-style-type: none">· 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.

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

Table 5-2: 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. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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 CEN routes in the VBR route table

This topic describes how to view Cloud Enterprise Network (CEN) routes in the route table of the Virtual Border Router (VBR).

Procedure

1. Log on to the [Express Connect console](#).
2. In the left-side navigation pane, choose Physical Connections > Virtual Border Routers (VBRs).
3. On the Virtual Border Routers (VBRs) page, find the target VBR and click the VBR ID.
4. Click the Routes tab to view CEN routes.

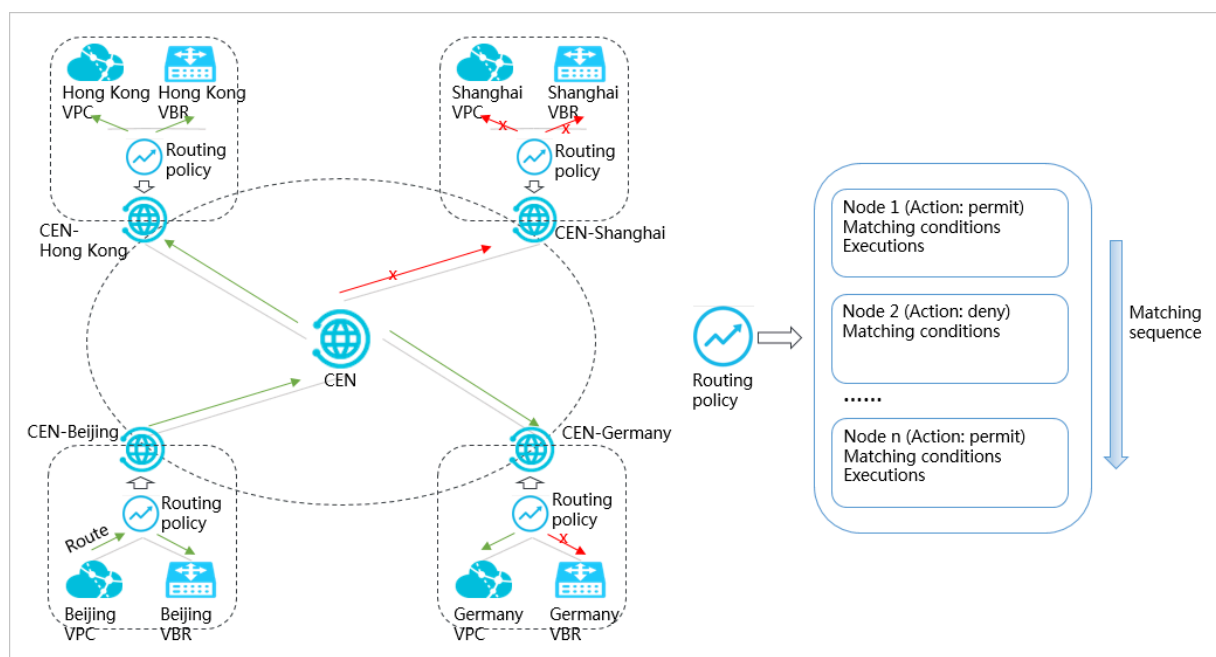
6 Routing policies

6.1 Route map overview

This topic provides an overview of the route map function supported by Cloud Enterprise Networks (CENs). By using the route map function, you can filter route information and modify route attributes to manage the communication between networks attached to a CEN.

Background information

A CEN instance has a regional CEN gateway in each region. The regional CEN gateways allow network instances (VPC, VBR, and CCN instances) attached to the CEN to communicate with each other. Routes can be transmitted to network instances in the same region or different regions through the inbound regional gateway (Import to Regional Gateway) and the outbound regional gateway (Export from Regional Gateway).



You can configure route maps for different regional gateways in a CEN. Each regional gateway can be configured with a route map in the inbound direction and the outbound direction. The corresponding route maps of each gateway consist of a set of conditional statements and executable statements that are sorted in ascending order of priority. When route maps are executed, the system first check whether the route

map with the highest priority matches the conditional statements. The route map permits or denies routes. If a route is permitted, you can modify its attributes.

Elements of a route map

A route map consists of basic information, match conditions, and actions.



Note:


Actions are only supported when the match mode is set to Permit.



- The following table describes the basic information of a route map.

Element	Description
Priority	<p>The priority of the route map. A lower value indicates a higher priority.</p> <p>The priority of route maps in the same region and the same direction must be unique. When route maps are executed, the system first check whether the route map with the highest priority matches the conditional statements. Therefore, we recommend that you specify an appropriate priority for each route map.</p>
Description	The description of the route map.
Region	The region where the route map is applied.
Transmit Direction	<p>The direction of the route map.</p> <ul style="list-style-type: none">- Import to Regional Gateway: the direction in which a route is published to the regional gateway of the CEN. For example, a route is published to the local regional gateway from a local network instance or from another region.- Export from Regional Gateway: the direction in which a route is published from the regional gateway of the CEN. For example, a route is published from a local regional gateway to another network instance in this region or to another regional gateway.


Element	Description
Match Mode	<p>The match mode used if a route matches all the matching conditions. The following match modes are supported:</p> <ul style="list-style-type: none"> - Permit: The route is permitted. - Deny: The route is denied.
Preference	<p>The preference of the associated next route map. Optional. Value range: 1 to 100.</p> <ul style="list-style-type: none"> - If this parameter is not set, the current route map is not associated with the next route map. - If this parameter is set to 1, the current route map is associated with the next route map. - If this parameter is set to a value that is not 1, the preference of the associated route map must be greater than that of the current route map. <p>Only route maps whose match mode is set to Permit will be checked whether they match route maps associated with preference after meeting all current match conditions.</p>


- The following table describes the elements of a match condition.

Element	Description
Region	The source region of a matched route.
Instance Type	<p>The instance type of a matched route. The following instance types are supported:</p> <ul style="list-style-type: none"> - The type of the source instance - The type of the target instance <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;">  Note: The type of the target instance is valid only when the Transmit Direction is set to Export from Regional Gateway and the type of the target instance is the type of instances in this region. </div>

Element	Description
Instance ID	<p>The list of instance IDs contained in a matched route. The following instance IDs are supported:</p> <ul style="list-style-type: none">- A list of source instance IDs- A list of target instance IDs <div> Note: The list of target instance IDs is valid only when the Transmit Direction is set to Export from Regional Gateway and the ID of the target instance is the ID of instances in this region.</div> <p>If an instance ID that matches the route is not in the instance ID list of the match condition, the matching succeeds. Otherwise, the matching fails.</p>
Route Table	<p>The route table of a matched route. The following route tables are supported:</p> <ul style="list-style-type: none">- The source route table- The target route table <div> Note: The target route table is valid only when the Transmit Direction is set to Export from Regional Gateway and the target route table is a route table in this region.</div>
Route Type	<p>The type of a matched route. The following route types are supported:</p> <ul style="list-style-type: none">- System: the routes generated by the system.- Custom: the custom routes.- BGP: the routes advertised to BGP.

Element	Description
Route Prefix	<p>The prefix of a matched route. The following match methods are supported:</p> <ul style="list-style-type: none">- Fuzzy Match: If the prefix of a route to be matched is contained in the prefix in the match condition, the route matches the condition. <p>For example, if the prefix in the match condition is set to 1.1.0.0/16 and the match method is set to Fuzzy Match, the route with the prefix of 1.1.1.0/24 matches the condition.</p> - Exact Match: A route matches the condition only when the prefix of the route is the same as the prefix in the match condition. <p>For example, if the prefix in the match condition is set to 1.1.0.0/16 and the match method is set to Exact Match, only the route with the prefix of 1.1.1.0/16 matches the condition.</p>

Element	Description
AS Path	<p>The AS path of a matched route. The following match methods are supported:</p> <ul style="list-style-type: none">- Fuzzy Match: A route matches the condition if the AS path in the route overlaps the AS path in the match condition. <p>For example, if the AS path in the match condition is set to [65001, 65002] and the match method is set to Fuzzy Match, the route with the AS path of [65501, 65001] matches the condition.</p> <ul style="list-style-type: none">- Exact Match: A route matches the condition only when the AS path of the route is the same as the AS path in the match condition. <p>For example, if the AS path in the match condition is set to [65501, 65001, 60011] and the match method is set to Exact Match, only the route with the AS path of [65501, 65001, 60011] matches the condition.</p> <div> Note: The AS path is a well-known mandatory attribute, which describes the numbers of the ASs that a BGP route passes through during transmission.</div>

Element	Description
Community	<p>The community of a matched route. The following match methods are supported:</p> <ul style="list-style-type: none"> - Fuzzy Match: A route matches the condition if the community of the route overlaps the community in the match condition. <p>For example, if the community in the match condition is set to [65001:1000, 65002:2000] and the match method is set to Fuzzy Match, the route with the community of [65501:1000, 65001:1000] matches the condition.</p> <ul style="list-style-type: none"> - Exact Match: A route matches the condition only when the community of the route is the same as the community in the match condition. <p>For example, if the community in the match condition is set to [65001:65001, 65002:65005, 65003:65001] and the match method is set to Exact Match, only the route with the community of [65001:65001, 65002:65005, 65003:65001] matches the condition.</p> <div>  Note: Community is an optional transitive attribute. You can set different community values for different routes. Downstream routers can use community values to match the target routes. </div>

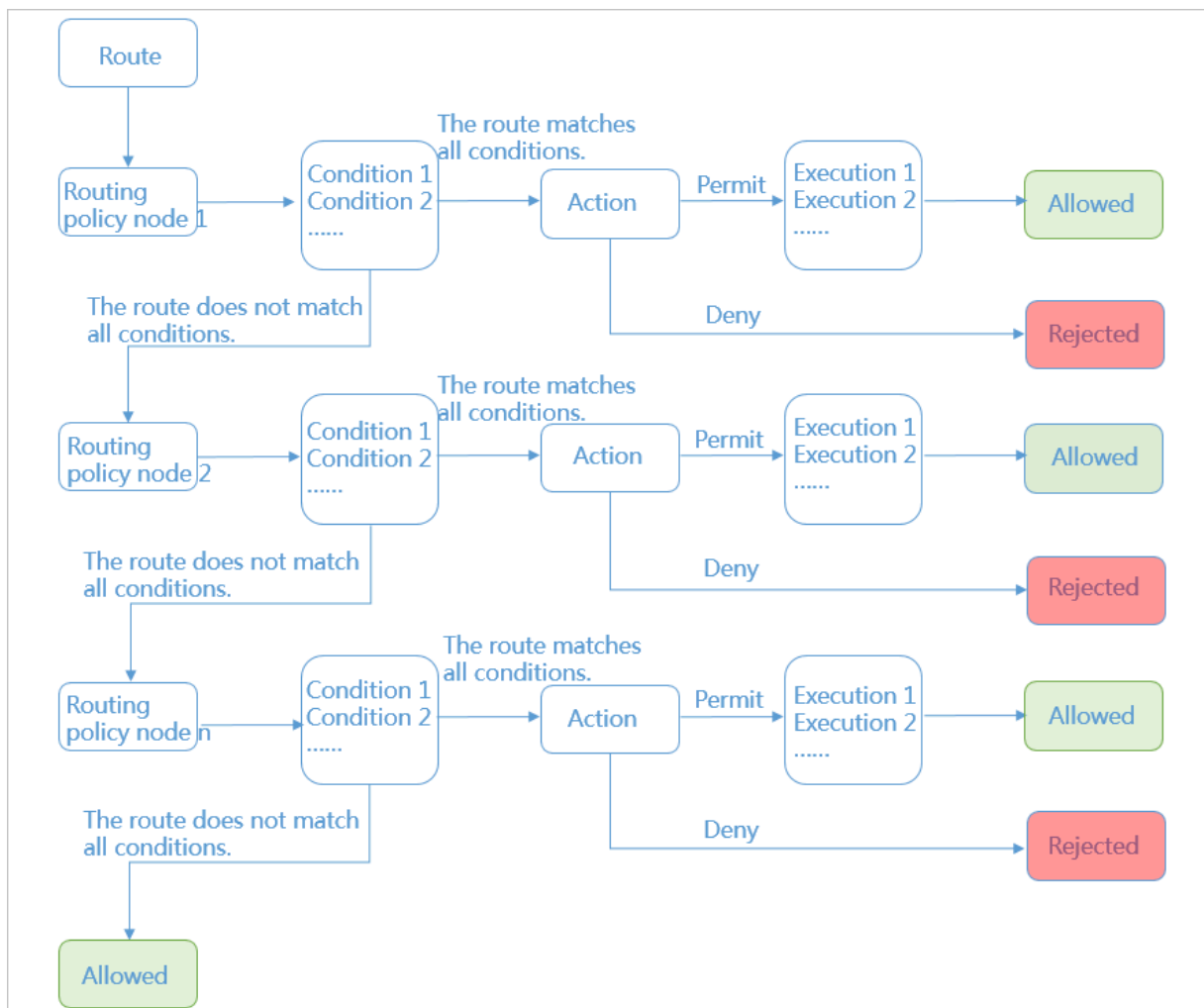
- The following table describes the elements of an action.

Element	Description
Community	<p>Set the community value. The following settings are supported:</p> <ul style="list-style-type: none"> - Additive - Replace
Preference	Set the preference of the permitted routes.

Matching process of route maps

Route maps use the match-action mode. Specifically, actions are performed only after conditions are matched. When route maps are executed, the system first check whether the route map with the highest priority matches the conditional statements.

- If a route meet all the match conditions in the route map, the match mode is then checked.
 - If the match mode is set to Permit, the executable statements in the route map are executed and the route is permitted. By default, the route will not be checked whether it matches the next route map unless the current route map is configured with a preference.
 - If the match mode is set to Deny, the route is denied. By default, the route will not be checked whether it matches the next route map, and the matching process is immediately ended.
- If the route fails to meet any match conditions in the current route map, the route will be checked whether it matches the next route map.
- If the route matches all the match conditions in the next route map, the match mode is then checked.
 - If the match mode is set to Permit, the executable statements in the route map are executed and the route is permitted. By default, the route will not be checked whether it matches the next route map unless the current route map is configured with a preference.
 - If the match mode is set to Deny, the route is denied. By default, the route will not be checked whether it matches the next route map, and the matching process is immediately ended.
- If the route fails to meet any match conditions in the current route map, the route will be checked whether it matches the next route map, and so on.
- If the route fails to meet any match conditions in all route maps, the route is permitted.



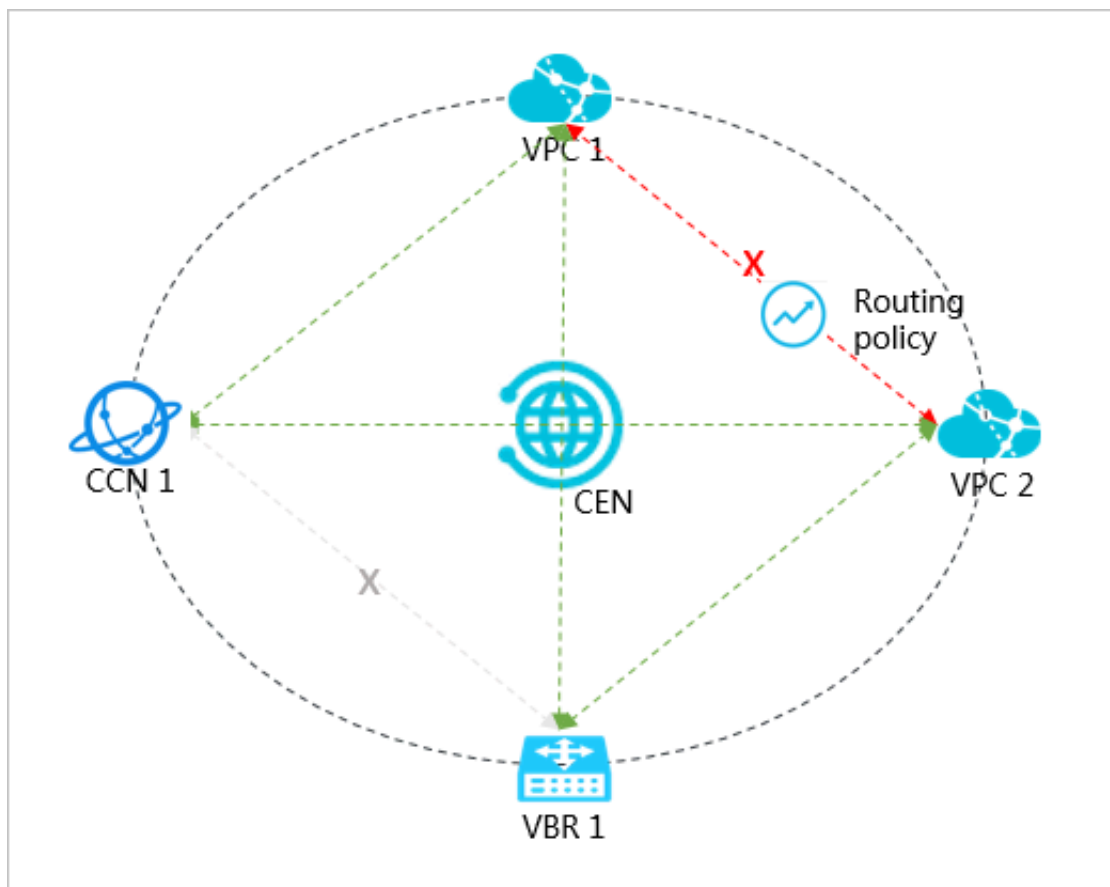
Scenarios

Route maps can be used in the following scenarios:

- Control the communication between two VPCs, or between a VPC and a VBR or a CCN

By default, a VPC can communicate with Virtual Border Routers (VBRs), Cloud Connect Networks (CCNs) and other VPCs that are attached to the same CEN instance. However, you may need to block the communication between two VPCs,

or between a VPC and a VBR or a CCN in some cases, as shown in the following figure.

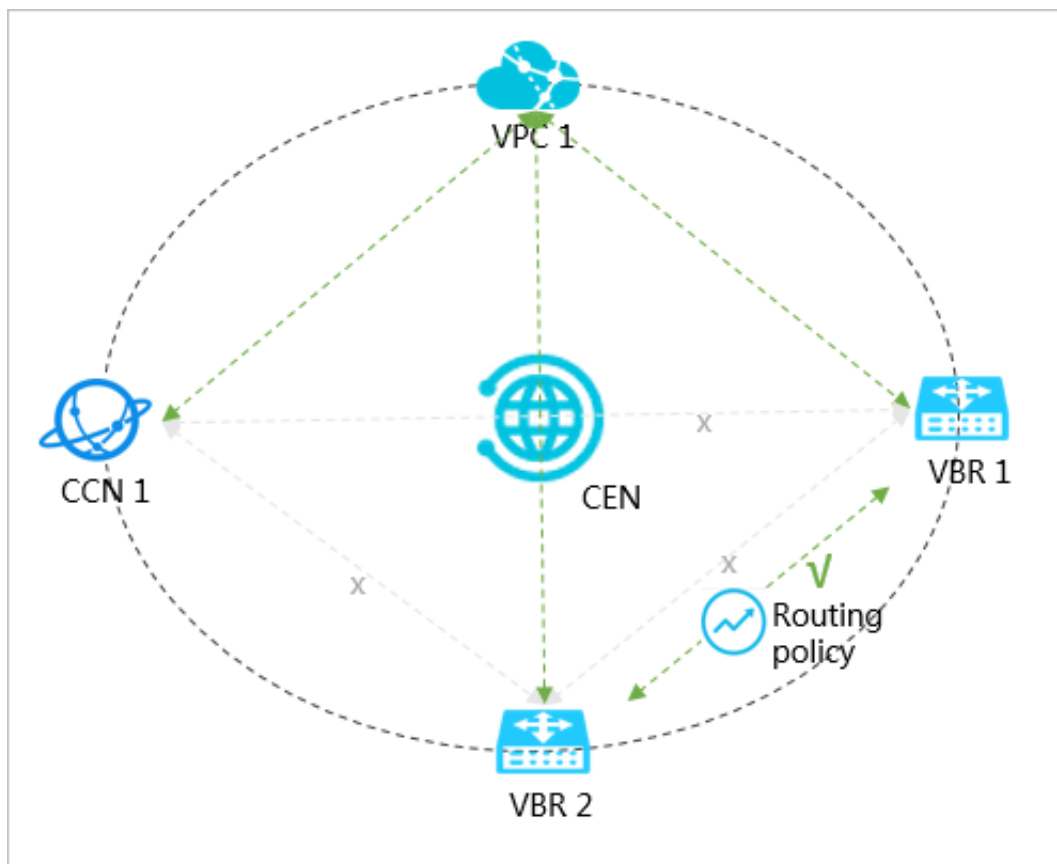


You can use the route map function to block the communication between VPC1 and VPC2 while maintaining the communication between VPC1 and CCN1 or VBR1, or between VPC2 and CCN1 or VBR1.

- Control the communication between two VBRs, or between a VBR and a VPC or a CCN

By default, a VBR cannot communicate with CCNs or other VBRs that are attached to the same CEN instance. However, you may need to enable the communication

between two VBRs or between a VBR and a CCN in some cases, as shown in the following figure.

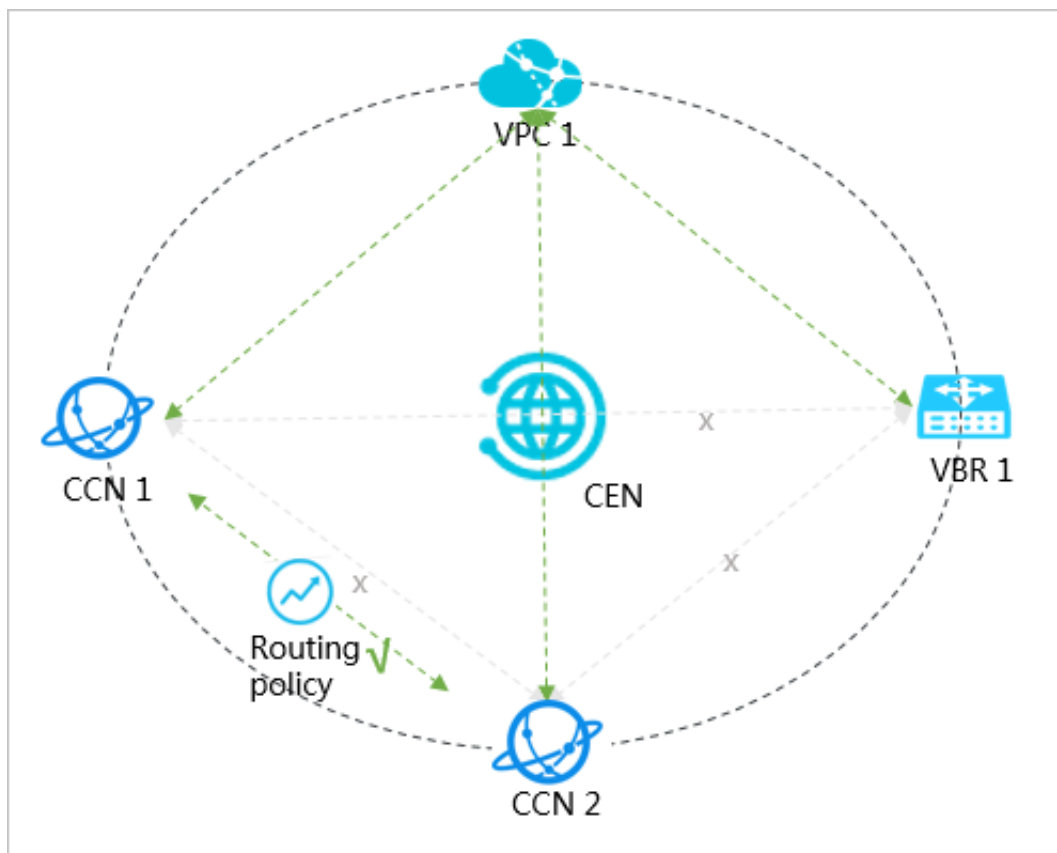


You can use the route map function to enable the communication between VBR1 and VBR2 while blocking the communication between VBR1 and CCN1 and between VBR2 and CCN1.

- Control the communication between two CCNs, or between a CCN and a VPC or a VBR

By default, a CCN cannot communicate with VBRs or other CCNs that are attached to the same CEN instance. However, you may need to enable the communication

between two CCNs or between a VBR and a CCN in some cases, as shown in the following figure.



You can use the route map function to enable the communication between CCN1 and CCN2 while blocking the communication between VBR1 and CCN1 and between VBR1 and CCN2.

Limits

The following table describes the limits that apply when you use the route map function.

Item	Limit	Quota increase supported?
Number of route maps that can be created in the inbound gateway direction in each region	100	Not supported.
Number of route maps that can be created in the outbound gateway direction in each region	100	Not supported.

Documentation

[#unique_39](#)

[#unique_40](#)

[#unique_41](#)

[Route map APIs](#)

6.2 Add a route map

This topic describes how to add a route map to a CEN instance. Before you can use the route map function, you must add a route map. After you add a route map to a CEN instance, you can filter route information and modify route attributes to manage the communication between networks attached to the CEN.

Context

You can configure route maps for different regional gateways in a CEN. Each regional gateway can be configured with a route map in the inbound direction and the outbound direction. Each route map is a set of conditional statements and executable statements. Route maps are sorted in ascending order of priority. When route maps are executed, the system first check whether the route map with the highest priority matches the conditional statements. The route map permit or deny routes. If a route is permitted, you can modify its attributes. For more information, see [#unique_44](#).

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 then 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, set the parameters, and then click OK. The following table describes the parameters.

Configuration	Description
Priority	<p>The priority of the route map. A lower value indicates a higher priority.</p> <p>The priority of route maps in the same region and the same direction must be unique. When route maps are executed, the system first check whether the route map with the highest priority matches the conditional statements. Therefore, we recommend that you specify an appropriate priority for each route map.</p>
Description	Enter a description for the route map.
Region	The region where the route map is applied.
Transmit Direction	<p>The direction of the route map.</p> <ul style="list-style-type: none">• Import to Regional Gateway: Routes are imported to the regional gateway of the CEN. For example, a route is published to the local regional gateway from a local network instance or from another region.• Export from Regional Gateway : Routes are exported from the regional gateway of the CEN. For example, a route is published from a local regional gateway to another network instance in this region or to another regional gateway.
Match condition	<p>The match conditions of the route map.</p> <p>Click + Add Match Value to add one or more matching conditions. For more information, see Match conditions.</p>

Configuration	Description
Match Mode	<p>Select a match mode for the route map.</p> <ul style="list-style-type: none">· Permit: All routes that meet the match conditions are permitted. <p>If you set the match mode to Permit, the following actions are supported:</p> <ul style="list-style-type: none">- Preference: Set the preference of the permitted route.- Community: Set the Community attribute, which can be Additive or Replace. <ul style="list-style-type: none">· Deny: All routes that meet the match conditions are denied. <p>If you set the match mode to Deny, no other actions are supported.</p>
Preference	<p>The preference of the associated next route map. Optional. Value range: 1 to 100.</p> <ul style="list-style-type: none">· If this parameter is not set, the current route map is not associated with the next route map.· If this parameter is set to 1, the current route map is associated with the next route map.· If this parameter is set to a value that is not 1, the preference of the associated route map must be greater than that of the current route map. <p>Only route maps whose match mode is set to Permit will be checked whether they match route maps associated with preference after meeting all current match conditions.</p>

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 condition, match mode, and preference.

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 then 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 condition, match mode, and preference as needed, and then click OK.

6.4 Delete a route map

This topic describes how to delete a route map from a CEN instance. After you delete a route map from a CEN instance, the CEN will no longer execute the 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 then click Manage in the Actions column.
4. On the CEN page, click the Route Maps tab, find the target route map, and then click Delete in the Actions column.
5. In the Delete Route Map dialog box, click OK.

7 Access to cloud services

7.1 PrivateZone overview

PrivateZone can also be defined as a VPC-based service that resolves and manages private domain names. Network instances attached to a CEN can access the PrivateZone service through the CEN. For more information, see [#unique_49](#).

7.2 PrivateZone

7.2.1 Configure PrivateZone access

This topic describes how to configure PrivateZone access for a Cloud Enterprise Network (CEN) instance. After you configure PrivateZone access for a CEN instance, the network instances attached to the CEN instance can access the PrivateZone service that resolves and manages private domain names.

Prerequisites

At least one VPC, VBR, or CCN instance in the host region and the access region is attached to the CEN instance.

Procedure

1. Log on to the [CEN console](#).
2. Click the ID of the target CEN instance.
3. Click the PrivateZone tab, and then click Authorization.



Note:

You need to grant permissions to the Smart Access Gateway only when you configure PrivateZone access for the first time.

4. On the Cloud Resource Access Authorization page, click **Confirm Authorization Policy** to allow local branches associated with a CCN (a component of the Smart Access Gateway) in the CEN instance to access the PrivateZone service.

Cloud Resource Access Authorization

Note: If you need to modify role permissions, please go to the RAM Console. [Role Management](#). If you do not configure it correctly, the following role: SmartAG will not be able to obtain the required permissions.

SmartAG needs your permission to access your cloud resources.
Authorize SmartAG to use the following roles to access your cloud resources.

AliyunSmartAGAccessingPVTZRole

Description: The Smart Access Gateway will use this role to access your resources in other services.
Permission Description: The policy for AliyunSmartAGAccessingPVTZRole.

Confirm Authorization Policy

Cancel

5. Click **Set Private Zone**, and then set the following parameters on the **Set Private Zone** page:
 - a) **Host Region**: Select the region to which the VPC configured with the PrivateZone service belongs.
 - b) **Host VPC**: Select the VPC configured with the PrivateZone service.

The PrivateZone service can be accessed only after the VPC in the host region is selected.

- c) **Access Region**: Select the region where access is initiated.



Note:

- The access region can be the host region or a CCN. The target network instance in the selected access region must be attached to the CEN instance.
- If you select a CCN whose account is different from that of the VPC or CEN, you must authorize the CCN. For more information, see [#unique_52](#).

- d) Click **OK**.

7.2.2 Grant permissions to CCN

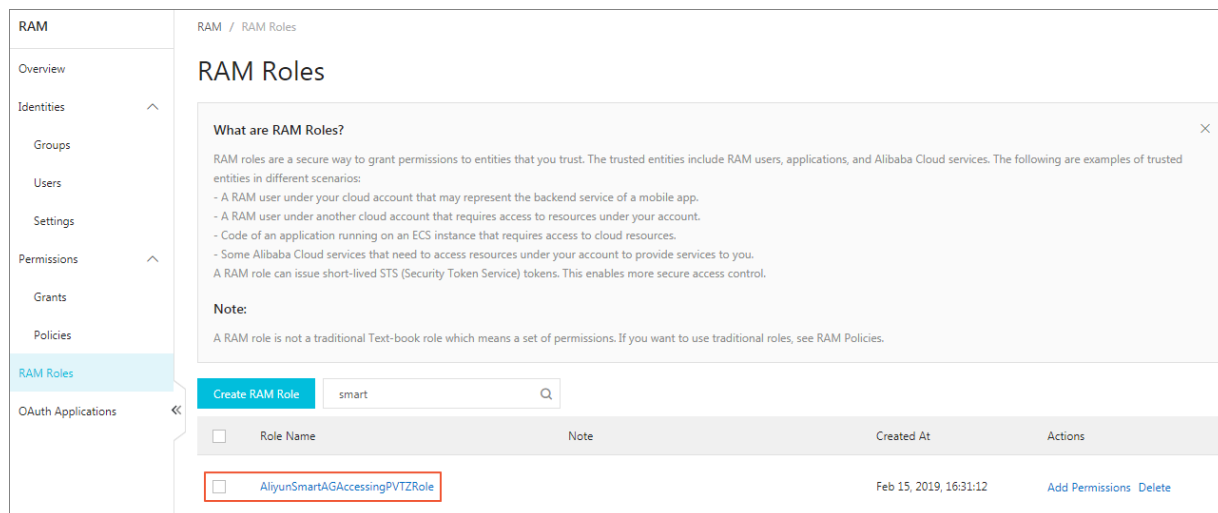
If you need to access the PrivateZone service through local branches of a Cloud Connect Network (CCN) in a Cloud Enterprise Network (CEN) instance, you must grant permissions to the CCN.

Same CEN, VPC, and CCN account

If the CCN, the VPC that is configured with PrivateZone, and the CEN instance all belong to the same account, you need to click **Authorization** on the PrivateZone tab, and grant permissions to CCN by following the prompts. The following table provides example information of this scenario.

Resource	User ID
CEN	111111
VPC	111111
CCN	111111

After you grant permissions to the CCN, the system automatically creates a RAM role named `AliyunSmartAGAccessingPVTZRole`. You can view the RAM role on the RAM Roles page of the [RAM console](#).



Same CEN and VPC account, but different CCN account

If the CEN instance and the VPC that is configured with PrivateZone belong to the same account, but the CCN belongs to a different account, you need to modify the authorization policy. The following table provides example information of this scenario.

Resource	User ID
CEN	111111
VPC	111111
CCN	333333

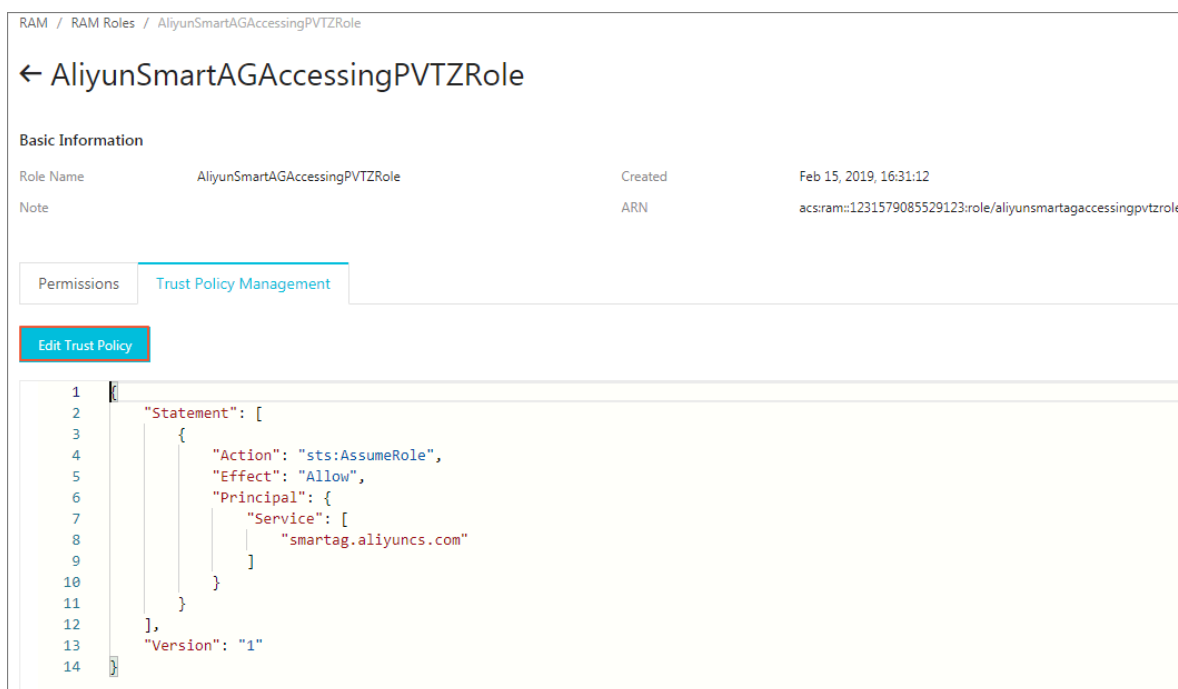
To grant permissions to the CCN, follow these steps:



Notice:

You need to use the account to which the VPC belongs.

1. Log on to the [CEN console](#).
2. Click the ID of the target CEN instance.
3. Click the PrivateZone tab, and then click Authorization. Grant permissions to the CCN by following the prompts.
4. Go to the [RAM console](#).
5. In the left-side navigation pane, click RAM Roles.
6. In the search box, enter AliyunSmartAGAccessingPVTZRole and click the displayed role name.
7. Click the Trust Policy Management tab and then click Edit Trust Policy.



8. In Service , add a record of account ID of the CCN@smartag.aliyuncs.com and click OK.

Same CCN and VPC account, but different CEN account

If the CCN and the VPC that is configured with PrivateZone belong to the same account, but the CEN instance belongs to a different account, you need to create a RAM role and grant it permissions by using the account of the VPC. The following table provides example information of this scenario.

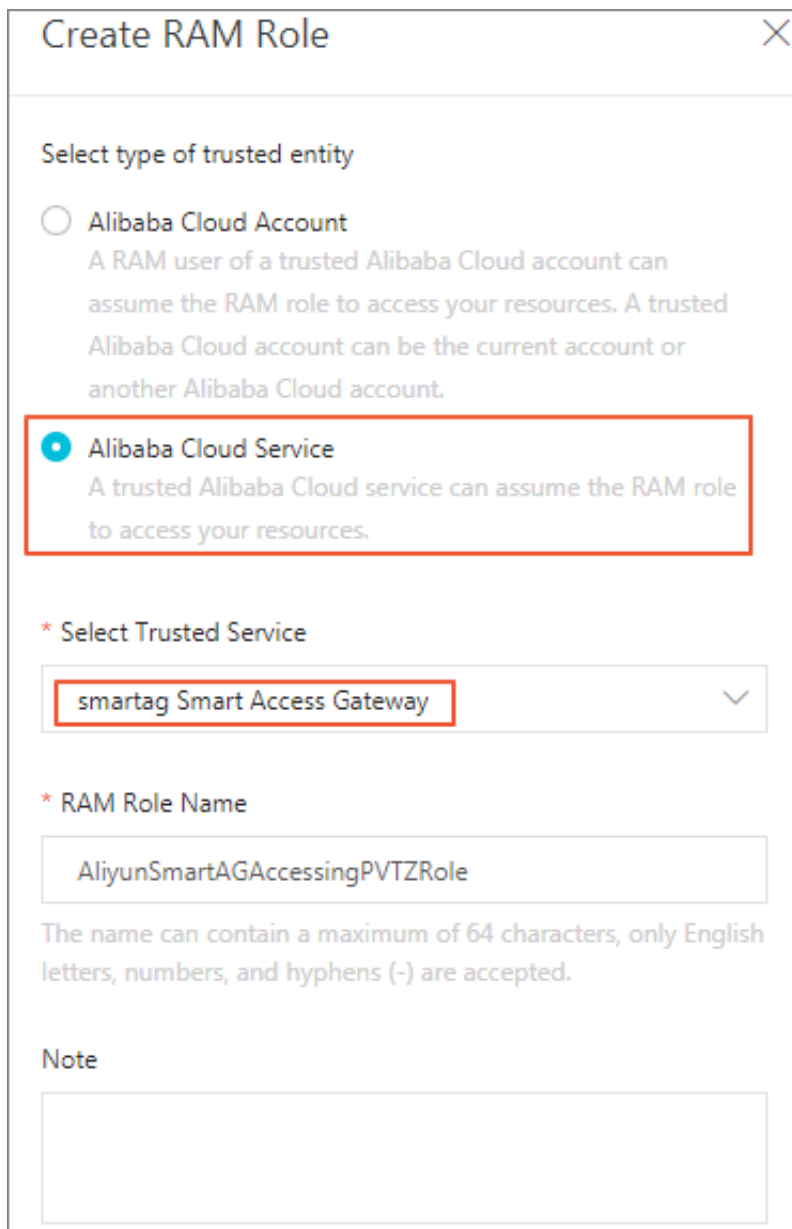
Resource	User ID
CEN	333333
VPC	111111
CCN	111111

To grant permissions to the CCN, follow these steps:

1. Log on to the [RAM console](#) by using the credentials of the account to which the VPC belongs.
2. In the left-side navigation pane, click RAM Roles.

3. Click Create RAM Role, configure it by referring to the following description, and then click OK.

- Select type of trusted entity: Select Alibaba Cloud Service.
- Select Trusted Service: Select smartag Smart Access Gateway.
- RAM Role Name: Enter AliyunSmartAGAccessingPVTZRole.



Create RAM Role [X]

Select type of trusted entity

☐ Alibaba Cloud Account
A RAM user of a trusted Alibaba Cloud account can assume the RAM role to access your resources. A trusted Alibaba Cloud account can be the current account or another Alibaba Cloud account.

☒ Alibaba Cloud Service
A trusted Alibaba Cloud service can assume the RAM role to access your resources.

* Select Trusted Service

smartag Smart Access Gateway [v]

* RAM Role Name

AliyunSmartAGAccessingPVTZRole

The name can contain a maximum of 64 characters, only English letters, numbers, and hyphens (-) are accepted.

Note

4. Click the created RAM role name.

5. On the Permissions tab, click Add Permissions.

6. In the search box, enter `pvtz` and click the displayed `AliyunPvtzReadOnlyAccess` policy.

Add Permissions

Principal

AliyunPvtzReadOnlyAccess@role.aliyun-document.onaliyunservice.com X

Select Policy

System Policy ▼ pvtz × Q Selected (0) Clear

Policy Name	Note
AliyunPvtzFullAccess	Provides full access to Cloud DNS Private Zone via Management Console.
AliyunPvtzReadOnlyAccess	Provides read-only access to Cloud DNS Private Zone via Management Console.

7. Go back to the RAM role details page, and click the Trust Policy Management tab to view the permission information.

RAM / RAM Roles / AliyunPvtzReadOnlyAccess

← AliyunPvtzReadOnlyAccess

Basic Information

Role Name	AliyunPvtzReadOnlyAccess	Created	Feb 15, 2019, 17:22:42
Note		ARN	acsram::1231579085529123:role/aliyunpvtzreadonlyaccess

Permissions Trust Policy Management

Edit Trust Policy

```

1 {
2   "Statement": [
3     {
4       "Action": "sts:AssumeRole",
5       "Effect": "Allow",
6       "Principal": {
7         "Service": [
8           "smartag.aliyuncs.com"
9         ]
10      }
11    }
12  ],
13  "Version": "1"
14 }
```

Three different accounts

If the CCN, the VPC that is configured with PrivateZone, and the CEN instance belong to three different accounts, you need to complete the following tasks:

Resource	User ID
CEN	111111
VPC	222222

Resource	User ID
CCN	333333

1. Use the account of the VPC to create a RAM role and grant it permissions. For more information, see [Same CCN and VPC account, but different CEN account.](#)

RAM / RAM Roles / AliyunPvtzReadOnlyAccess

← AliyunPvtzReadOnlyAccess

Basic Information

Role Name	AliyunPvtzReadOnlyAccess	Created	Feb 15, 2019, 17:22:42
Note		ARN	acs:ram::1231579085529123:role/aliyunpvtzreadonlyaccess

Permissions Trust Policy Management

Edit Trust Policy

```

1 {
2   "Statement": [
3     {
4       "Action": "sts:AssumeRole",
5       "Effect": "Allow",
6       "Principal": {
7         "Service": [
8           "smartag.aliyuncs.com"
9         ]
10      }
11    }
12  ],
13  "Version": "1"
14 }
```

2. Use the account of the VPC to modify the policy associated with the corresponding RAM role by adding the CCN service in the format of `CCN account ID @`

aliyuncs . com . For more information, see [Same CEN and VPC account, but different CCN account](#).



To allow multiple CCNs to access the PrivateZone service, add all the CCNs to the trust policy, as shown in the following figure.

Resource	User ID
CEN	111111
VPC	222222
CCN	333333
CCN	444444
CCN	555555

Edit Trust Policy

×

RAM Role Name

AliyunSmartAGAccessingPVTZRole

```
1  {
2    "Statement": [
3      {
4        "Action": "sts:AssumeRole",
5        "Effect": "Allow",
6        "Principal": {
7          "Service": [
8            "smartag.aliyuncs.com",
9            "333333@smartag.aliyuncs.com",
10           "444444@smartag.aliyuncs.com",
11           "555555@smartag.aliyuncs.com"
12         ]
13       }
14     ]
15   },
16   "Version": "1"
```

8 Health check

8.1 Configure the health check function

This topic describes how to configure the health check function of a Cloud Enterprise Network (CEN) instance. After you configure the health check function of a CEN instance, you can monitor the network conditions of on-premises data centers connected to the CEN.

Procedure

1. Log on to the [CEN console](#).
2. In the left-side navigation pane, click Health Check.
3. On the CEN page, select the region to which the target CEN instance belongs, and then click Set Health Check.
4. On the Set Health Check page, set the parameters as needed, and then click OK.

The following table describes the parameters.

Configuration	Description
Instances	Select the CEN instance to which the VBR is attached.
Virtual Border Router (VBR)	Select the VBR that you want to monitor.
Source IP	The source IP address can be any available IP address in the 10.0.0.0/8, 192.168.0.0/16, or 172.16.0.0/12 CIDR block. However, the source IP address cannot conflict with the IP address that it will communicate with in the CEN, or the IP address of the VBR at the Alibaba Cloud side or customer side.
Target IP	The Interface IP address of the customer premises equipment connected to the VBR.

8.2 Delete health check settings

This topic describes how to delete the health check settings of a CEN instance. After you delete the health check settings of a CEN instance, you cannot monitor

the network status of the on-premises data center connected to the VBR of the CEN instance.

Procedure

1. Log on to the [CEN console](#).
2. In the left-side navigation pane, click Health Check.
3. On the CEN page, select the region to which the target CEN instance belongs.
4. Find the target CEN instance, and then click Delete in the Actions column.
5. In the Delete Healthcheck dialog box, click OK.

8.3 Modify health check settings

This topic describes how to modify the source IP address and target IP address of the health check function.

Procedure

1. Log on to the [CEN console](#).
2. In the left-side navigation pane, click Health Check.
3. On the CEN page, select the region to which the target CEN instance belongs.
4. Find the target CEN instance, and then click Edit in Actions column.
5. On the Set Health Check page, modify the source IP address and target IP address, and then click OK.
 - Source IP: The source IP address can be any available IP address in the 10.0.0.0/8, 192.168.0.0/16, or 172.16.0.0/12 CIDR block. However, the source IP address cannot conflict with the IP address that it will communicate with in the CEN, or the IP address of the VBR at the Alibaba Cloud side or customer side.
 - Target IP: The interface IP address of the customer premises equipment connected to the VBR.

9 Monitoring


9.1 Set alarms

You can set alarm rules for physical connections, bandwidth packages and region connection traffic to monitor the usage of these resources and avoid the influence on services when any resource limit is reached.

Set alarm rules for a physical connection

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 of the target CEN instance and click Set Alarm.

CEN	CEN						Get Started	Documentation
Instances	<div>China North 2 (Beijing) Set healthcheck Refresh</div>							
Health Check								
	CEN ID/Name	VBR ID	Monitor	Source IP	Target IP	Actions		
	cen-nh98vzx8gfhlwngl76	vbr-2zentl26m5o5wdhtb9d0g	<div> Set Alarm</div>	172.16.0.2	10.0.0.0	Edit Delete		

4. Configure one or more alarm rules.

You can set alarm rules for latency, packet loss, inbound bandwidth, or outbound bandwidth and customize the thresholds that trigger the alarms.

Create Alarm Rule
Back to

1
Related Resource

Products : CEN-Router

Resource Range : Instances

Instances : 云企业网 Totally1unit

VBRInstances : vbr-2zentl26m5o5wdhtb9d0g Totally1unit

2
Set Alarm Rules

Alarm Rule :

Rule Describe : Healthy Check Latency

1mins

Value

>=

Threshold

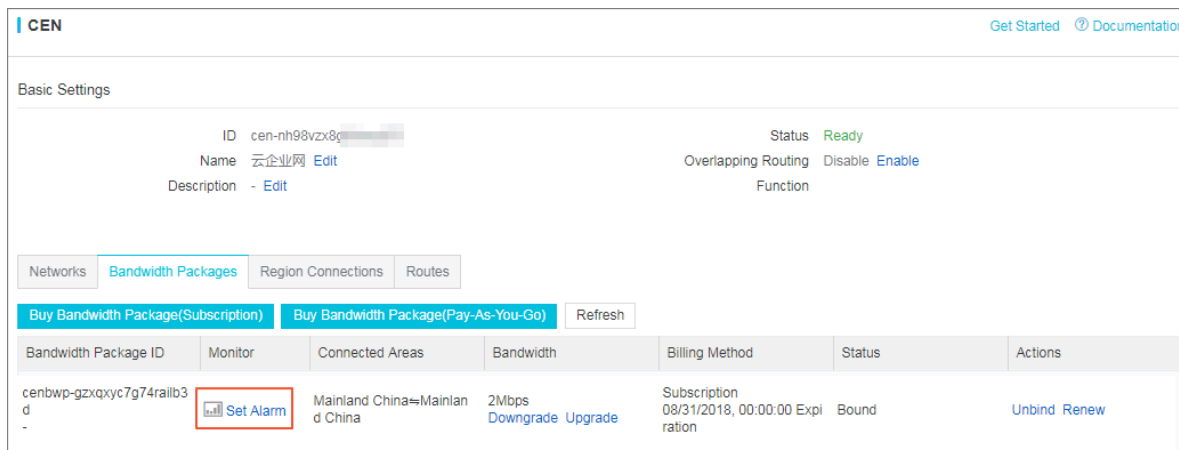
ms

Add Alarm Rule

Set alarm rules for a bandwidth package

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

1. Log on to the [CEN console](#).
2. Click the ID of the target CEN instance and then click the Bandwidth Packages tab.
3. Find the target bandwidth package and then click Set Alarm.



4. Configure one or more alarm rules.

You can set alarm rules for area-to-area connection bandwidth or area-to-area connection bandwidth ratio, and customize the thresholds that trigger the alarms.

The screenshot shows the 'Create Alarm Rule' form. It has a 'Back to' button at the top left. The form is divided into two main sections: '1 Related Resource' and '2 Set Alarm Rules'. In the 'Related Resource' section, there are dropdown menus for 'Products' (set to 'CEN-Area'), 'Resource Range' (set to 'Instances'), 'Instances' (set to '云企业网 Totally1unit'), and 'PackageId' (set to 'cenbwp-be7ojvicb7zwdcxnji(north-america_china) Totally1unit'). In the 'Set Alarm Rules' section, there is a text input for 'Alarm Rule', a dropdown for 'Rule Describe' (set to 'Area Internet Out Rate Percent'), a dropdown for '1mins', a dropdown for 'Value', a dropdown for '>=' (set to '>='), and a text input for 'Threshold' followed by a '%' symbol. At the bottom, there is a '+Add Alarm Rule' button.

Set alarm rules for a region connection

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

1. Log on to the [CEN console](#).
2. Click the ID of the target CEN instance and then click the Region Connections tab.

3. Find the target region connection and then click Set Alarm.

The screenshot shows the CEN console interface. At the top, there's a header with 'CEN' and links for 'Get Started' and 'Documentation'. Below is a 'Basic Settings' section with fields for ID, Name, Description, Status, and Function. A navigation bar includes 'Networks', 'Bandwidth Packages', 'Region Connections' (selected), and 'Routes'. Under 'Region Connections', there are buttons for 'Set Region Connection' and 'Refresh'. A table displays the following data:

Connected Areas	Monitor	Connected Regions	Bandwidth	Status	Actions
Mainland China⇒Mainland China	Set Alarm	China North 2 (Beijing)⇒China East 1 (Hangzhou)	1Mbps Modify	● Ready	Delete

4. Configure one or more alarm rules.

You can set alarm rules for outbound bandwidth or outbound bandwidth ratio of connected regions, and customize the thresholds that trigger the alarms.

The screenshot shows the 'Create Alarm Rule' form. It has a 'Back to' button and two main sections:

- 1 Related Resource**
 - Products : CEN-Region
 - Resource Range : Instances
 - Instances : Totally1unit
 - Flow direction : cn-beijing->cn-hangzhou Totally1unit
- 2 Set Alarm Rules**
 - Alarm Rule :
 - Rule Describe : Region Internet Out Rate
 - 1mins
 - Value
 - >=
 - Threshold
 - Mbits/s


At the bottom, there is a '+Add Alarm Rule' button.

9.2 View the monitoring data of a CEN instance

This topic describes how to view the monitoring data of a CEN instance, such as the egress bandwidth, ingress bandwidth, delay, and packet loss.

Procedure

1. Log on to the [CEN console](#).
2. In the left-side navigation pane, click Health Check.
3. On the CEN page, select the region to which the target CEN belongs.

4. Find the target health check task, and then click  in the Monitor column to view the monitoring data.

- **Egress Bandwidth:** the bandwidth of data transmission from Alibaba Cloud to on-premises data centers.
- **Ingress Bandwidth:** the bandwidth of data transmission from on-premises data centers to the Alibaba Cloud.
- **Delay:** the communication delay between Alibaba Cloud and on-premises data centers.
- **Packet loss:** the loss rate of data packets transmitted between Alibaba Cloud and on-premises data centers.

10 Flow logs

10.1 Flow log overview

This topic describes the flow log function of Cloud Enterprise Networks (CENs).

A flow log is used to capture the traffic data of the network instances that belong to different regions associated with a CEN instance. After you enable the flow log function, you can use the data aggregated in flow logs to analyze cross-region traffic flows, minimize traffic costs, and troubleshoot network faults.



Note:

- Flow logs only capture cross-region traffic data of mutual access. Traffic between two VPCs in a region, or traffic among VPCs, VBRs, and on-premises data centers in a region, are not captured.
- The flow log function is supported in China (Hangzhou), China (Shanghai), China (Zhangjiakou), China (Shenzhen), China (Beijing), China (Hohhot), China (Hong Kong), UK (London), US (Silicon Valley), US (Virginia), Germany (Frankfurt), India (Mumbai), Singapore, Indonesia (Jakarta), Australia (Sydney), and Malaysia (Kuala Lumpur).

Background information

Flow logs can be defined as aggregated traffic data that is captured in a capture window of 10 minutes. Each flow log consists of the following traffic data: a source IP address and source port, a destination IP address and destination port, and the protocol that is used.

The captured traffic data is stored in Alibaba Cloud Log Service, where you can view and analyze the traffic data. The flow log function is currently in the beta testing phase. During this phase, you are only charged for the storage and retrieval of traffic data in Log Service.

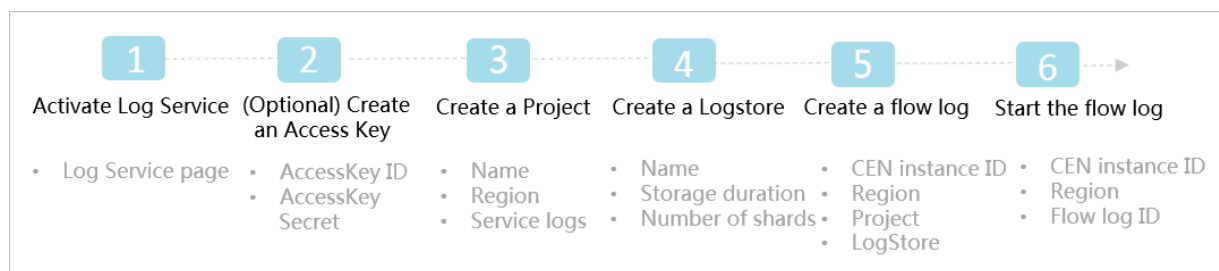
The traffic data captured by the flow log function is written to Log Service as flow log records. Each flow log record captures specified traffic data in a specified capture window, which is about 10 minutes. During this period, data is aggregated and then released to the flow log record.

The following table describes the fields of a flow log record.

Field	Description
account-id	The account ID.
cen-id	The ID of the CEN instance.
srcaddr	The source IP address.
srcport	The source port.
dstaddr	The destination IP address.
dstport	The destination port.
protocol	The protocol type.
direction	The direction of the traffic. <ul style="list-style-type: none"> · in: Indicates inbound traffic. · out: Indicates outbound traffic.
packets	The number of data packets.
bytes	The size of data packets.
rtt	The latency.
start	The start time of the capture window.
end	The end time of the capture window.
log-status	The status of the flow log record. <ul style="list-style-type: none"> · OK: Traffic data was recorded normally. · NODATA: No traffic data was detected during the capture window. · SKIPDATA: Some flow log records were skipped during the capture window.

Procedure

The following figure shows the procedure for configuring the flow log function.



1. Activate Log Service.

The traffic data captured by the flow log function is stored in Alibaba Cloud Log Service. Therefore, you need to activate Log Service before you create a flow log.

2. Optional. Create an Access Key.

If you want to write data to Log Service through APIs or SDKs, you must first create an Access Key (AK). However, if you want to collect logs by using Logtail, you do not need to create an AK.

3. Create a Project.

You must create a Project in Log Service. For more information, see [#unique_63/unique_63_Connect_42_section_ahq_ggx_ndb](#).

4. Create a Logstore.

A Logstore is a collection of resources created in a Project. All data in a Logstore is from the same data source. After creating a Project, you must create a Logstore. For more information, see [Create a Logstore](#).

5. Creates a flow log.

You call create a flow log through the CEN console. For more information, see [#unique_65](#).

6. View the flow log.

You can view the captured traffic data in the flow log. You can use the captured traffic data to analyze cross-region traffic flows, minimize traffic costs, and troubleshoot network faults. For more information, see [#unique_66](#).

Limit

Each CEN instance supports only one flow log.

Related documentation

- [#unique_67](#)
- [#unique_68](#)
- [#unique_69](#)
- [#unique_70](#)
- [Flow log API overview](#)

10.2 Create a flow log

This topic describes how to create a flow log. The flow log function in Cloud Enterprise Network (CEN) is used to record the cross-region traffic data of the networks associated with a CEN instance. To record traffic data, you must create a flow log.

Prerequisites

Before you create a flow log, make sure that the following conditions are met:

- Log Service is activated.
- A Project and a Logstore are created to store the traffic data. For more information, see [#unique_63/unique_63_Connect_42_section_ahq_ggx_ndb](#) and [Create a Logstore](#).

Context

After a flow log is created, the flow log enters the Enabled state, indicating that traffic data is recording.

You can view and analyze the traffic data in Log Service.

Procedure

1. Log on to the [CEN console](#).
2. In the left-side navigation pane, click Flow Logs.
3. Select the region of the flow log to be created.



Note:

- The region of the flow log must be the same as that of the Project.
 - Currently, the flow log function is supported only in the following regions: China (Hangzhou), China (Shanghai), China (Shenzhen), China (Beijing), China (Hohhot), Hong Kong, UK (London), US (Silicon Valley), and US (Virginia).
4. On the CEN page, click Create Flow Log.
 5. On the Create Flow Log page, configure the flow log according to the following information, and then click OK.

Configuration	Description
Name	Enter a name for the flow log to be created.

Configuration	Description
CEN	Select the CEN instance of which you want to record the traffic data.
Project	Select the Project where the recorded traffic data is stored.
LogStoreName	Select the Logstore where the recorded traffic data is stored.
Description	Enter a description for the flow log.

10.3 View flow logs

This topic describes how to view the recorded traffic data in a flow log. You can use the traffic data recorded in flow logs to analyze cross-region traffic flow, optimize traffic costs, and troubleshoot network faults.

Procedure

1. Log on to the [CEN console](#).
2. In the left-side navigation pane, click Flow Logs.
3. Select the region of the target flow log.
4. On the CEN page, find the target flow log and click the Logstore name link.
5. In the Log Service console, set the search conditions and click Search & Analysis.

You can view and analyze the displayed data.

10.4 Start a flow log

This topic describes how to start a flow log that is in the Disabled state. You must start a flow log if you want to record the cross-region traffic data of networks associated with a Cloud Enterprise Network (CEN) instance.

Procedure

1. Log on to the [CEN console](#).
2. In the left-side navigation pane, click Flow Logs.
3. Select the region of the target flow log.
4. On the CEN page, find the target flow log and click Start in the Actions column.

After the flow log is started, the status of the flow log changes to Enabled.

10.5 Stop a flow log

This topic describes how to stop a flow log. If you want to temporarily stop recording traffic data between the networks associated with a Cloud Enterprise Network (CEN) instance, you can stop the corresponding flow log.

Procedure


1. Log on to the [CEN console](#).
2. In the left-side navigation pane, click Flow Logs.
3. Select the region of the target flow log.
4. On the CEN page, find the target flow log and click Stop in the Actions column.

After the flow log is stopped, the status of the flow log changes to Disabled.


10.6 Modify a flow log

This topic describes how to modify the name and description of a flow log.

Procedure

1. Log on to the [CEN console](#).
2. In the left-side navigation pane, click Flow Logs.
3. Select the region of the target flow log.
4. On the CEN page, find the target flow log, rest the pointer over the instance name in the Instance ID/Name column, click the displayed  image, and enter a new name for the flow log.

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

5. To modify the description of the flow log, click the  image in the Description column and enter a new description.

The description must be 2 to 256 characters in length and cannot start with http:// or https://.

10.7 Delete a flow log

This topic describes how to delete a flow log.

Context

You can delete a flow log that is in the Enabled or Disabled state.

Procedure

1. Log on to the [CEN console](#).
2. In the left-side navigation pane, click Flow Logs.
3. Select the region of the target flow log.
4. On the CEN page, find the target flow log and click Delete in the Actions column.
5. In the displayed dialog box, click OK.

11 Increase the quota of a cloud resource

This topic describes how to increase the quota of a cloud resource in the CEN console. If the remaining quota of a cloud resource is insufficient, you can apply for a quota increase.

Procedure

1. Log on to the [CEN console](#).
2. In the left-side navigation pane, click Quotas. The resource usage of the CENs under your account is displayed.
3. Click Apply in the Actions column, and then set the following parameters in the displayed dialog box:
 - Quantity for Application: the resource quota that you need. The quota you apply for must be greater than the current quota. For information about the default resource limits of a CEN, see [#unique_78](#).
 - Reason for Application: your reason for applying for a quota increase. We recommend that you provide details about your specific scenarios.
 - Email: your email address.
4. Click OK.

The system then determines whether the quota increase application is reasonable.

- If the request is unreasonable, the status of the application is Rejected.
- If the request is reasonable, the status of the application is Approved, and the quota is automatically increased to the quota that you applied for.

To view the historical quota applications of a cloud resource, click Application History in the Application History column.