Alibaba Cloud
Cloud Enterprise Network

User Guide

Issue: 20190819

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.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

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

Contents

1 Manage CEN instances

After creating a Cloud Enterprise Network (CEN) instance, you can attach networks to the CEN instance, buy bandwidth packages, and set the cross-region interconnection bandwidth to build a secure, reliable, and enterprise-class global network.

Create a CEN instance

To create a CEN instance, follow these steps:

1. Log on to the CEN console.
2. On the Instances page, click Create CEN instance.
3. Configure the CEN instance according to the following information:

Configuration	Description
Name	Enter a name for the CEN instance. The name must be 2 to 128 characters in length and can contain letters, Chinese characters, numbers, hyphens (-), and underscores (_). It must start with a letter or a Chinese character. It cannot start with `http://` or `https://`.
Description	Enter a description for the CEN instance. The description must be 2 to 256 characters in length. It cannot start with `http://` or `https://`.
Attach networks	You can attach networks of your account or other accounts to a CEN instance. For more information, see #unique_4.

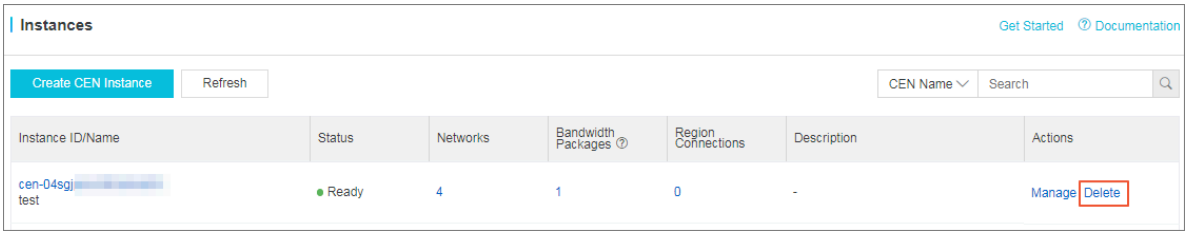
Delete a CEN instance

Before you delete a CEN instance, make sure that no bandwidth package or network is attached to the CEN instance.

To delete a CEN instance, follow these steps:

1. Log on to the CEN console.

2. Find the target CEN instance and click Delete in the Actions column.



3. In the displayed dialog box, click OK.

2 Attach a network in a different account

To attach a network that belongs to a different account, you must obtain permissions.

Cross-account authorization for a VPC

1. Log on to the VPC console by using the credentials of the account to which the target VPC belongs.
2. In the left-side navigation pane, click VPCs.
3. Click the ID of the target VPC, and then in the CEN cross account authorization information section, click CEN Cross Account Authorization.
4. In the displayed dialog box, enter the ID of the account to which the target CEN instance belongs and the ID of the CEN instance, and then click OK.

Cross-account authorization for a VBR

1. Log on to the Express Connect console by using the credentials of the account to which the target Virtual Border Router (VBR) belongs.
2. In the left-side navigation pane, choose Physical Connections > Virtual Border Routers (VBRs).
3. Click the ID of the target VBR, and then click the CEN Authorization tab. Click Authorize CEN of Another Account to Load Instance.
4. In the displayed dialog box, enter the ID of the account to which the target CEN instance belongs and the ID of the CEN instance, and then click OK.

3 Networks

After you create a CEN instance, you must add networks that need to communicate with one another to the CEN instance. Currently, you can add VPCs, Virtual Border Routers (VBRs), and Cloud Connect Networks (CCNs) to a CEN instance.

You can attach networks in the same account or a different account to a CEN instance. To attach a network in a different account, authorization is required. For more information, see #unique_7.

Attach a network in the same account

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

1. Log on to the CEN console.
2. Click the ID of the target CEN instance.
3. Click the Networks tab and then click Attach Network.
4. Click the Your Account tab, and attach a network according to the following information.

Configuration	Description
Network Type	Select the type of the network to attach: · VPC: Attach a VPC. · Virtual Border Router (VBR): Attach an on-premises data center associated with the VBR. · Cloud Connect Network (CCN): Attach a local branch added to the CCN.
Region	Select the region of the network.
Networks	Select the network. Note: You cannot select a network that is already attached to a CEN instance or uses Express Connect.

5. Click OK.

Attach a network in a different account

To attach a network that belongs to a different account, you must grant permissions to the CEN instance by using the account of the network. For more information, see #unique_7.

To attach a network in a different account, follow these steps:

1. Log on to the CEN console.
2. Click the ID of the target CEN instance.
3. Click the Networks tab and then click Attach Network.
4. Click the Different Account tab, and attach a network according to the following information.

Configuration	Description
Owner Account	Enter the ID of the account that owns the network to attach.
Network Type	Select the type of the network to attach.
Region	Select the region of the network to attach.
Networks	Enter the ID of the network to attach.

5. Click OK.

Attach VPCs or VBRs from the details page

You can attach VPCs or VBRs to a CEN instance directly from the VPC or VBR details page.

- On the VPC details page, click Attach to CEN in the upper-right corner, and then select the target CEN instance. Click OK.
- On the VBR details page, click Join CEN, and then select the target CEN instance. Click OK.

Detach a network

To detach a network from a CEN instance, follow these steps:

1. Log on to the CEN console.
2. Click the ID of the target CEN instance. Click the Networks tab.
3. Find the target network and click Detach in the Actions column.
4. In the displayed dialog box, click OK.

4 Cross-region connection bandwidth

To connect networks in different regions, you must set cross-region connection bandwidth after buying a bandwidth package. The total bandwidth value set for all the connected regions of a bandwidth package cannot exceed the bandwidth value of the bandwidth package. By default, 1 Kbit/s bandwidth is provided for connected regions so that you can perform connectivity tests. To run normal business, you must buy a bandwidth package and set a proper connection bandwidth.

For example, you bought a bandwidth package of 20 Mbit/s for a CEN instance and the interconnection 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 value set for all the interconnected regions cannot exceed 20 Mbit/s.

Set a cross-region connection bandwidth

1. Log on to the CEN console.
2. On the Instances page, click the ID of the target CEN instance.
3. Click the Region Connections tab, and then click Set Region Connection.
4. Configure the cross-region connection bandwidth, and then click OK.

Configuration	Description
Bandwidth Package	Select the bandwidth package attached to the CEN instance.
Connected Regions	Select the regions to connect.
Bandwidth	Enter the required bandwidth.

Modify a cross-region connection bandwidth

1. Log on to the CEN console.
2. On the Instances page, click the ID of the target instance.
3. Click the Region Connections tab, find the target cross-region connection, and then click Modify in the Bandwidth column.
4. In the displayed dialog box, enter a new bandwidth value, and click OK.

Delete a cross-region connection bandwidth

1. Log on to the CEN console.

2. On the Instances page, click the ID of the target instance.
3. Click the Region Connections tab, find the target cross-region connection, and then click Delete in the Actions column.
4. In the displayed dialog box, click OK.

5 Bandwidth package

5.1 Manage bandwidth packages

To connect networks in different regions, you must buy a bandwidth package and set a cross-region bandwidth value.

What is a bandwidth package?

A Cloud Enterprise Network (CEN) bandwidth package is an abstracted object that includes an interconnection bandwidth and interconnection areas. To buy a bandwidth package, you must specify the areas to connect. An area consists of one or more Alibaba Cloud regions.

The relationship between an area and a region is shown in the following table:

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)

Buy a bandwidth package

To connect networks in different regions, you must buy a bandwidth package and set a cross-region bandwidth value. Connecting networks in the same region does not require a bandwidth package.

Note:
To delete a bandwidth package, you must open a ticket.

To buy a bandwidth package, follow these steps:

1. Log on to the CEN console.
2. Click the ID of the target CEN instance.

3. On the CEN page, click the Bandwidth Packages tab and then click Buy Bandwidth Package (Subscription).
4. Configure the bandwidth package according to the following information:

Configuration	Description
Cloud Enterprise Network	Select the CEN instance that requires a bandwidth package.
Area	Select the area to connect.
Area	Select the area to connect.
Bandwidth	Set a bandwidth value for the bandwidth package. Note: You cannot modify the interconnected areas after the bandwidth package is purchased.
Name	Enter a name for the bandwidth package.
Duration	Select a validity period for your Subscription.

Disassociate a bandwidth package

You can disassociate a bandwidth package from a CEN instance and associate this bandwidth package with other CEN instances.

Notice:

- Before you disassociate a bandwidth package, delete region connections using the bandwidth package.
- The bandwidth package is still charged after it is disassociated from a CEN instance. To delete a bandwidth package, open a ticket.

To disassociate a bandwidth package, follow these steps:

1. Log on to the CEN console.
2. Click the ID of the target CEN instance.
3. On the CEN page, click the Bandwidth Packages tab.
4. Find the target bandwidth package and click Unbind in the Actions column.
5. In the displayed dialog box, click OK.

Associate a bandwidth package

You can associate a disassociated bandwidth package to another CEN instance.

To associate a bandwidth package, follow these steps:

1. Log on to the CEN console.
2. Click the ID of the target CEN instance.
3. On the CEN page, click the Bandwidth Packages tab.
4. Find the target bandwidth package and click Bind in the Actions column.
5. In the displayed dialog box, click OK.

Modify the bandwidth

You can change the bandwidth value of a bandwidth package at any time, and the change takes effect immediately.

To modify the bandwidth, follow these steps:

1. Log on to the CEN console.
2. Click the ID of the target CEN instance.
3. On the CEN page, click the Bandwidth Packages tab.
4. Find the target bandwidth package and 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.
5. In the Configuration Upgrade section, modify the bandwidth, click Pay, and complete the payment.

Renew a bandwidth package

To renew a bandwidth package, follow these steps:

1. Log on to the CEN console.
2. Click the ID of the target CEN instance.
3. On the CEN page, click the Bandwidth Packages tab.
4. Find the target bandwidth package and click Renew in the Actions column.
5. Select the renewal duration and complete the payment.

References

#unique_11

6 Health check

CEN provides the health check function for you to monitor the network conditions of local data centers connected to the attached VBRs.

Configure health check

To configure the health check, complete 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 CEN instance and click Set healthcheck.
4. On the displayed page, configure the health check:

Configuration	Description
Instances	Select the CEN instance to which the VBR is attached.
Virtual Border Router (VBR)	Select the VBR to monitor.
Source IP	Any unused IP address in the VPCs attached to the CEN instance.
Target IP	The Interface IP address of the customer premises equipment connected to the VBR.

View monitoring data

To view the monitoring data after configuring the health check, complete these steps:

1. Log on to the CEN console.
2. In the left-side navigation pane, click Health Check.
3. Click the monitoring icon to view the monitoring data:
   - Egress bandwidth: The bandwidth of data transmission from Alibaba Cloud to the local data center.
   - Ingress bandwidth: The bandwidth of data transmission from the local data center to the Alibaba Cloud.
   - Packet loss: The loss rate of data transmitted between the Alibaba Cloud and the local data center.

Delete health check

To delete a health check configuration, complete 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 CEN instance.
4. Find the target health check configuration and then click Delete.
5. In the displayed dialog box, click OK.

7 Manage routes

7.1 Enable overlapping routing

Cloud Enterprise Network (CEN) automatically learns routes from attached networks. If two routes overlap, the conflicted routes will be denied. With overlapping routing enabled, CEN can learn overlapping routes that have the same prefix but different netmasks.

> Note:
> For CEN instances that are created after March 1, 2019, the overlapping routing function is enabled by default.

Before overlapping routing is enabled

The following CEN and VPC are used: VPC-A is attached to a CEN instance. A custom route entry with the destination CIDR block of 192.168.1.0/24 and next hop of an ECS instance is added to VPC-A. By default, all routes with IP address 192.168.1.0/x (1<=x <=3) that are published by other networks and learnt by CEN will be denied.

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 <= x <= 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 <= x <= 32).

After overlapping routing is enabled

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

For example, 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 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.

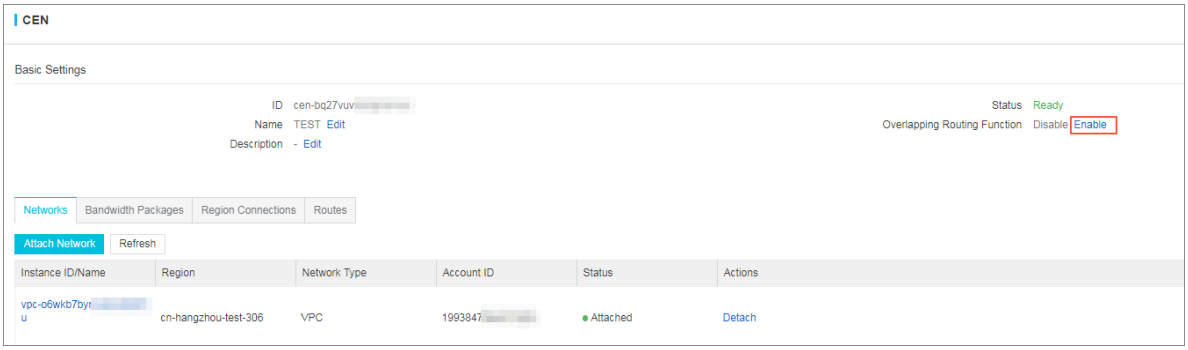
Exception

After the overlapping routing function is enabled, VPC does not accept routes that are subsets of a VSwitch. For example, the CIDR block of a VSwitch is 10.0.0.0/16, then the VPC to which the VSwitch belongs will not accept the routes with the CIDR block 10.0.0.0/24 but will accept the 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. Click the ID of the target CEN instance.
3. In the Basic Settings section, click Enable next to Overlapping Routing Function.



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

7.2 Manage CEN network routes

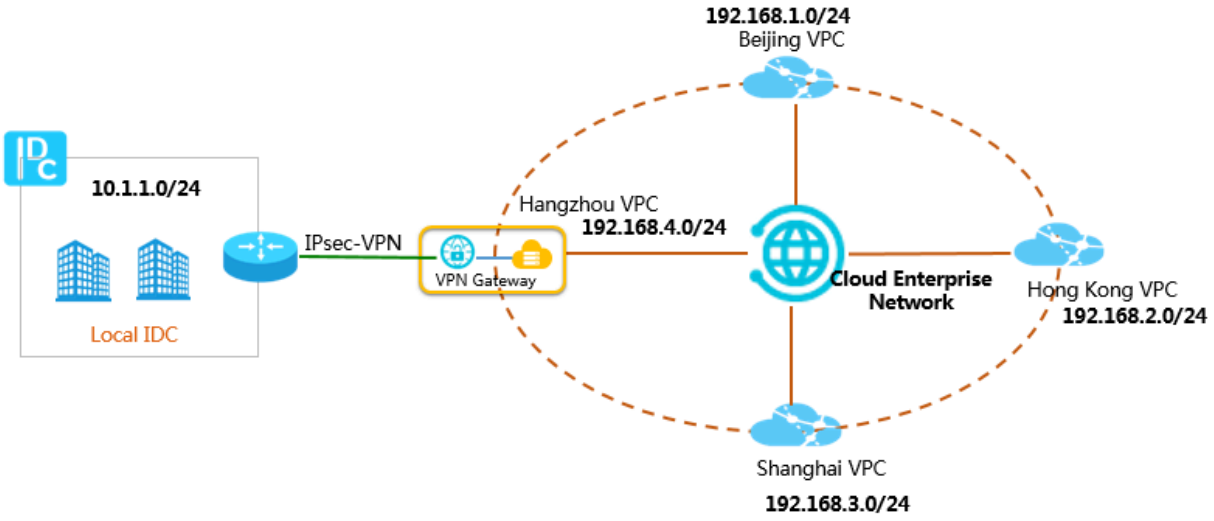
Cloud Enterprise Network (CEN) supports publishing and withdrawing route entries of attached networks. You can publish a route entry of an attached VPC or Virtual Border Router (VBR) to a CEN instance. Then, other networks attached to the same CEN instance can learn the route if there is no route conflict. You can withdraw a published route entry when CEN does not need it any more.

Note:
Currently, the CEN console only supports publishing and withdrawing VPC route entries and does not support publishing and withdrawing VBR route entries. You can publish and withdraw VBR route entries by calling the #unique_16 API.

The following table lists the route entries that can be published to CEN. You can withdraw a route entry that has been published to CEN. After a route entry is withdrawn, it does not exist in the CEN instance anymore. If you have published a custom route entry to a CEN instance and then delete it from the VPC or VBR route table, the route entry is also deleted from the CEN instance.

Route entry	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 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 VPC to the CEN instance, the other three VPCs learn the route and can also communicate with the on-premises data center.



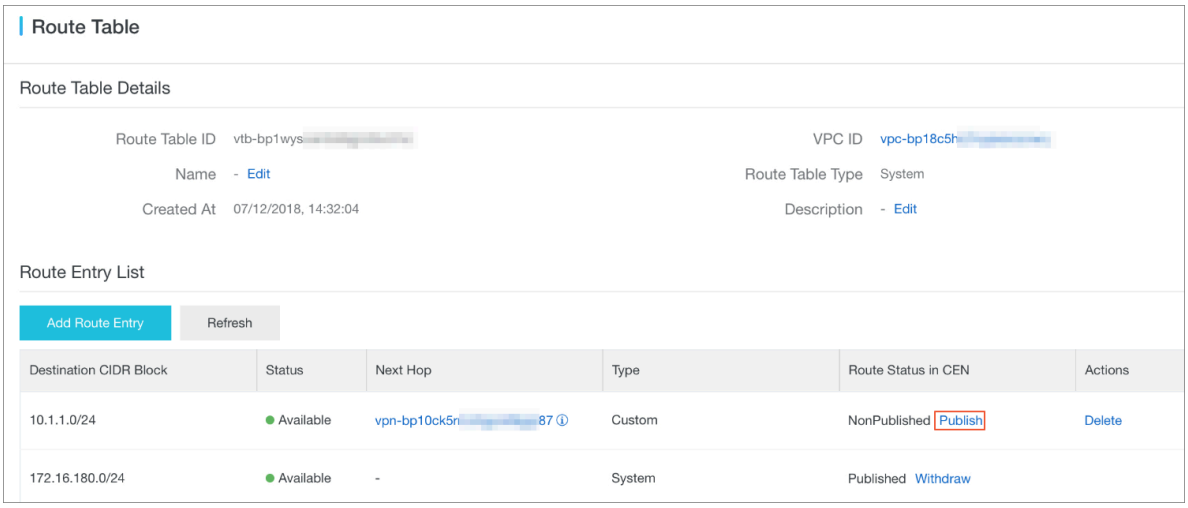
Publish a route entry to CEN

To publish a route entry in a VPC to CEN, follow these steps:

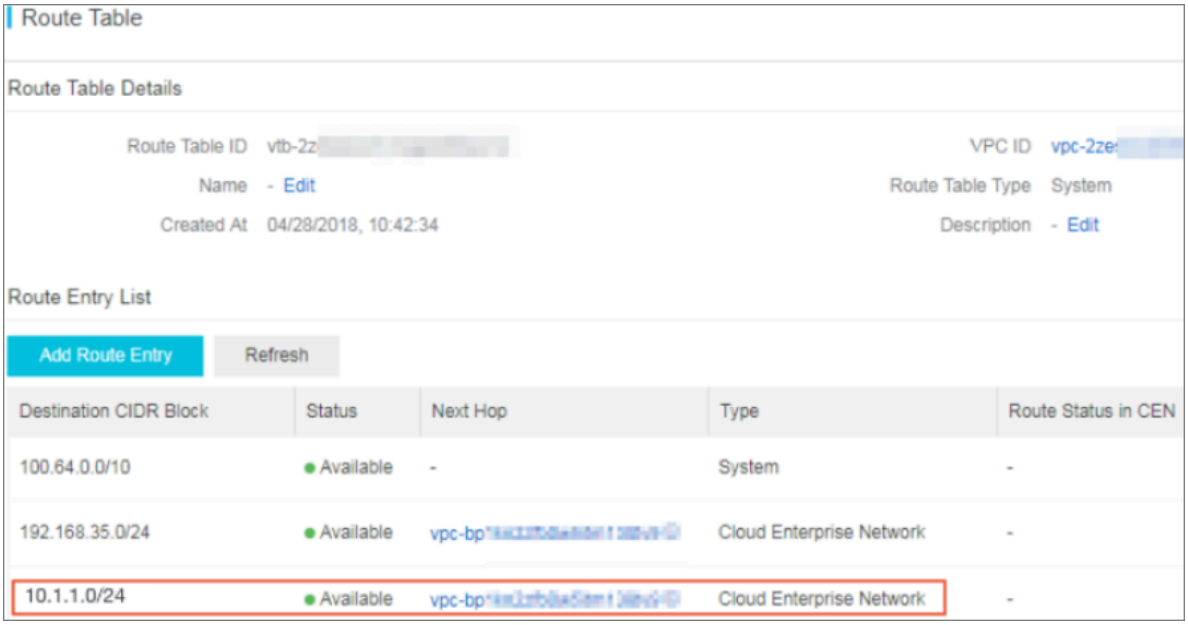
Note:

Make sure that the VPC is attached to a CEN instance.

1. Log on to the CEN console.
2. On the Instances page, click the ID of the target CEN instance.
3. On the Networks tab, click the ID of the target VPC.
4. On the VPC Details page, click the link to the route table.
5. On the Route Tables page, click the ID of the route table.
6. Find the target route entry and click Publish in the Route Status in CEN column.



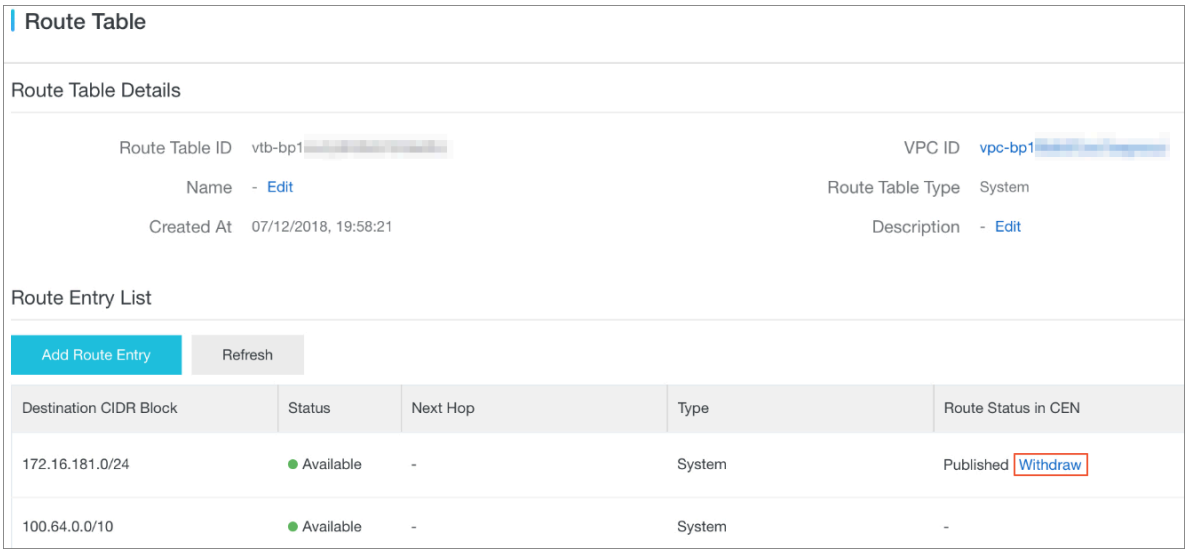
After the route entry is successfully published, you can view the learnt routes in other networks.



Withdraw a route entry from CEN

To withdraw a route entry published to CEN from a VPC, follow these steps:

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



8 Access cloud services

Access cloud services by using Cloud Enterprise Network (CEN).

8.1 Overview of accessing cloud services

PrivateZone is a VPC-based resolution and management service for private domain names. Networks attached to CEN can access the PrivateZone service through CEN. For more information, see #unique_19.

8.2 PrivateZone

8.2.1 Set PrivateZone access

PrivateZone is a VPC-based resolution and management service for private domain names. Networks in a Cloud Enterprise Network (CEN) instance can access the PrivateZone service through CEN.

Prerequisites

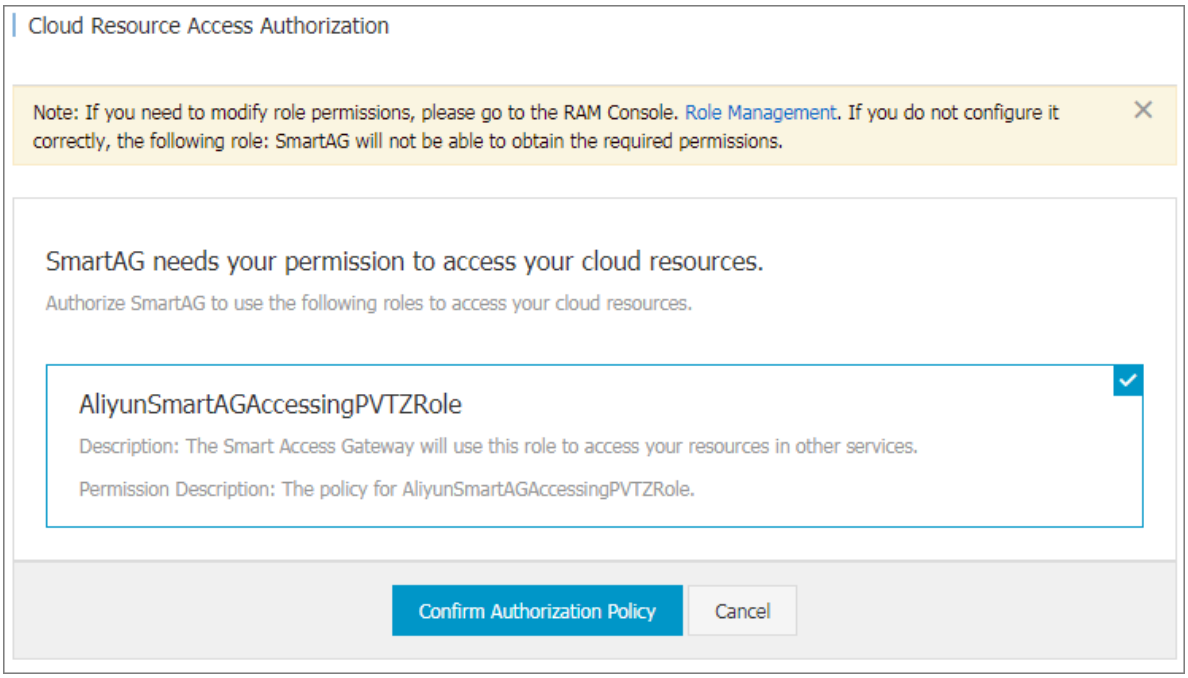
Make sure that the host region and access region have networks (VPC, VBR, and CCN) attached to the CEN instance.

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 Smart Access Gateway only for the first time you configure PrivateZone access.

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



5. Click Set Private Zone and then in the Set Private Zone dialog box, set the following parameters:
   a) Host Region: Select the region to which the VPC configured with PrivateZone belongs.
   b) Host VPC: Select the VPC that is configured with PrivateZone.

      The PrivateZone service can be selected only by selecting the VPC in the host region.
   c) Access Region: Select the region where the access is initiated.

      Note:

      - The access region can be CCN, or the same region as the host region. Make sure that the network in the selected access region has been attached to the CEN instance.
      - If you select a CCN instance and the CCN instance account is different from that of the VPC instance or CEN instance, you must authorize the instance. For more information, see #unique_22.
   d) Click OK.

8.2.2 Grant permissions to CCN

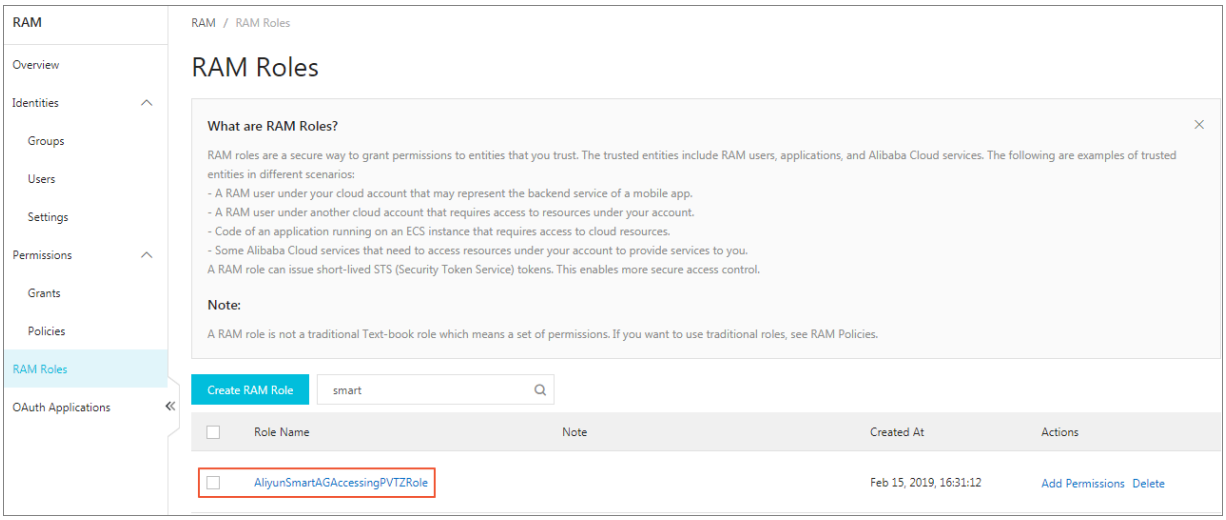
If you need to access the PrivateZone service through local branches of a Cloud Connect Network (CCN) in a Cloud Enterprise Network (CEN) instance, you must grant permissions to the CCN.

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

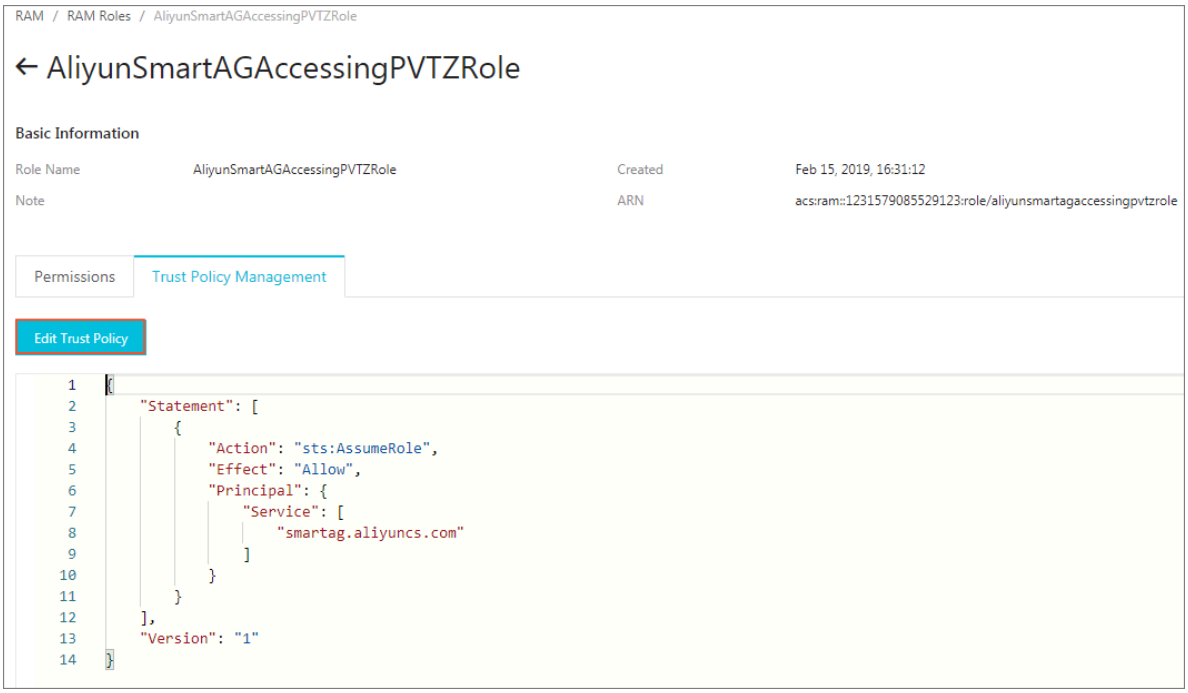
If the CEN instance and the VPC that is configured with PrivateZone belong to the same account, but the CCN belongs to a different account, you need to modify the authorization policy. The following table provides example information of this scenario.

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

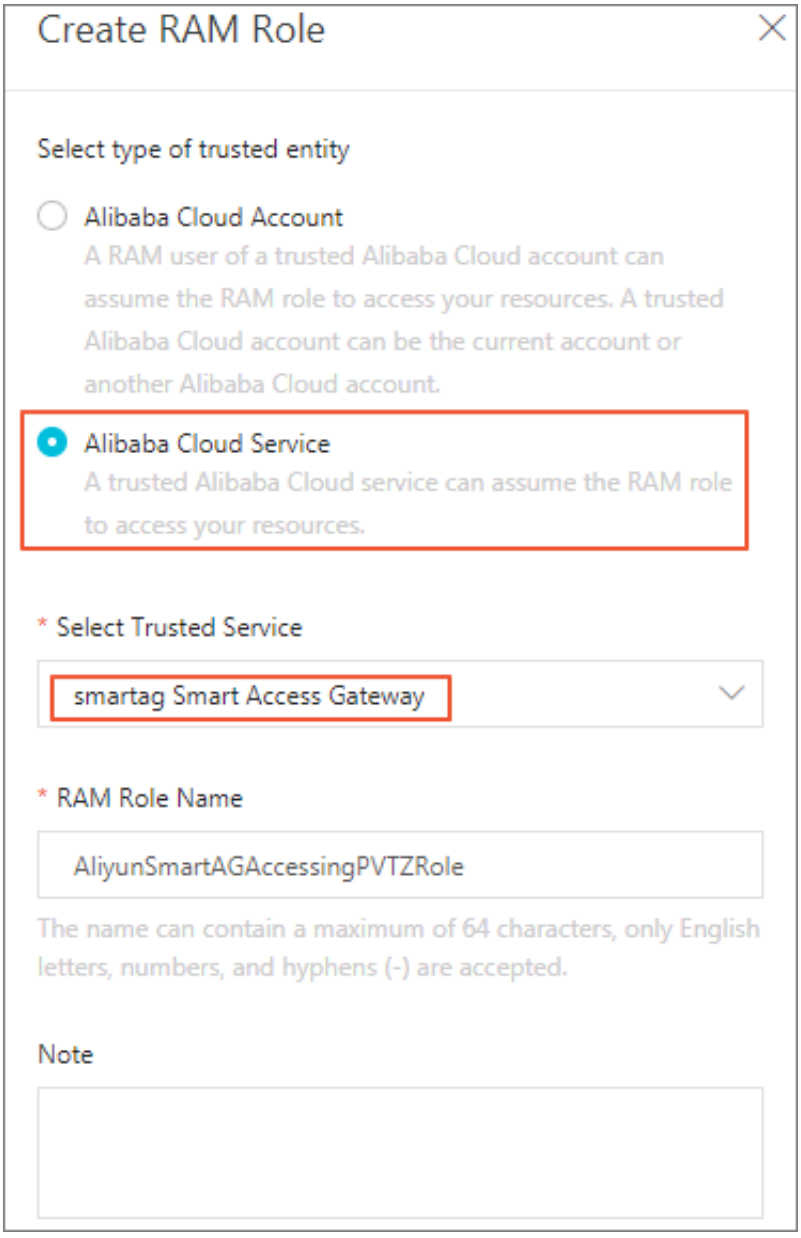
If the CCN and the VPC that is configured with PrivateZone belong to the same account, but the CEN instance belongs to a different account, you need to create a RAM role and grant it permissions by using the account of the VPC. The following table provides example information of this scenario.

Resource	User ID
CEN	333333
VPC	111111
CCN	111111

To grant permissions to the CCN, follow these steps:

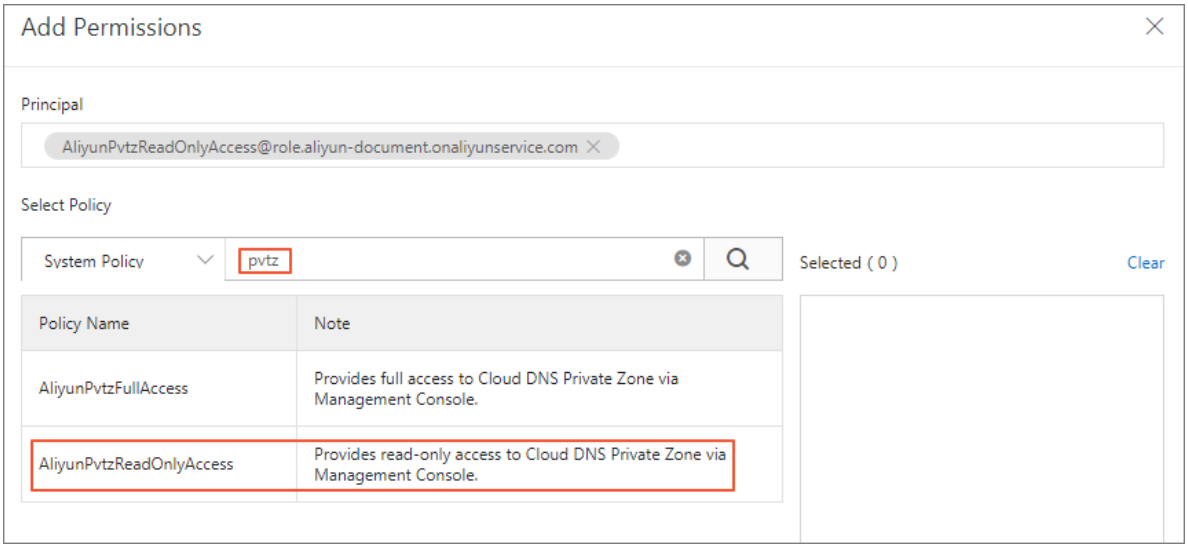
1. Log on to the RAM console by using the credentials of the account to which the VPC belongs.
2. In the left-side navigation pane, click RAM Roles.

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.



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.



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

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

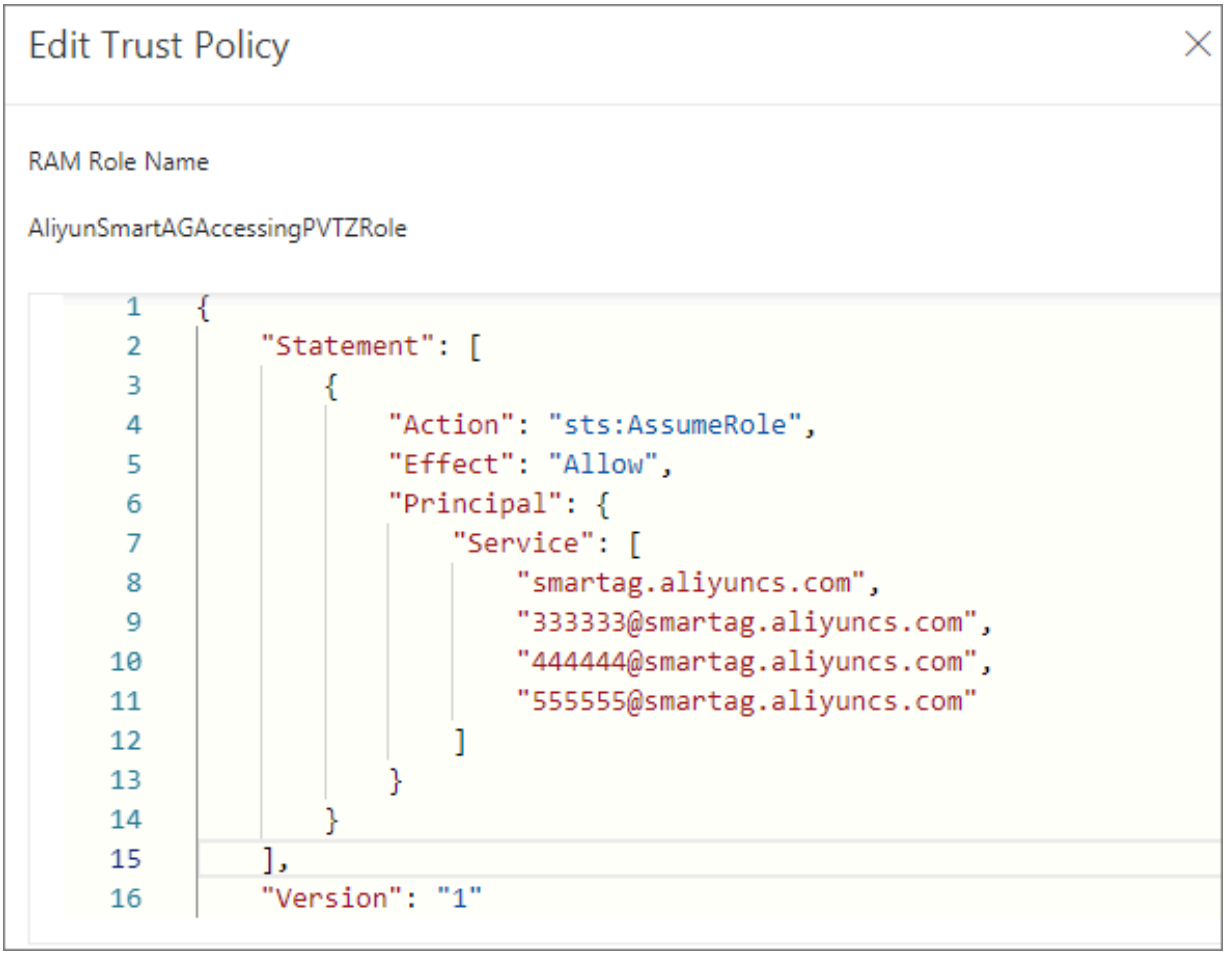
1. Use the account of the VPC to create a RAM role and grant it permissions. For more information, see Same CCN and VPC account, but different CEN account.

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
{
"Statement": [
{
"Action": "sts:AssumeRole",
"Effect": "Allow",
"Principal": {
"Service": [
"smartag.aliyuncs.com",
"333333@smartag.aliyuncs.com",
"444444@smartag.aliyuncs.com",
"555555@smartag.aliyuncs.com"
]
}
}
],
"Version": "1"

9 Flow logs

9.1 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_26/unique_26_Connect_42_section_ahq_ggx_ndb and #unique_27/unique_27_Connect_42_section_v52_2jx_ndb.

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.
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.

9.2 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.

9.3 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.

9.4 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.

9.5 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://.

9.6 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.

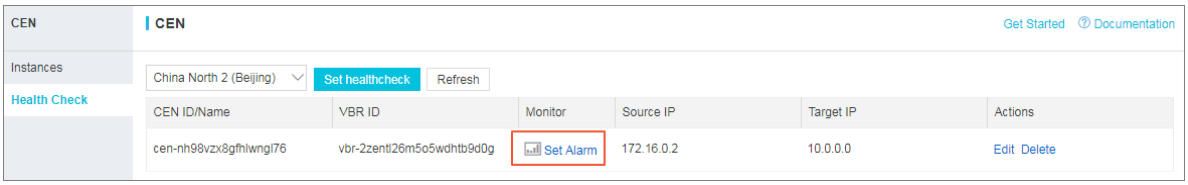
10 Set alarms

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

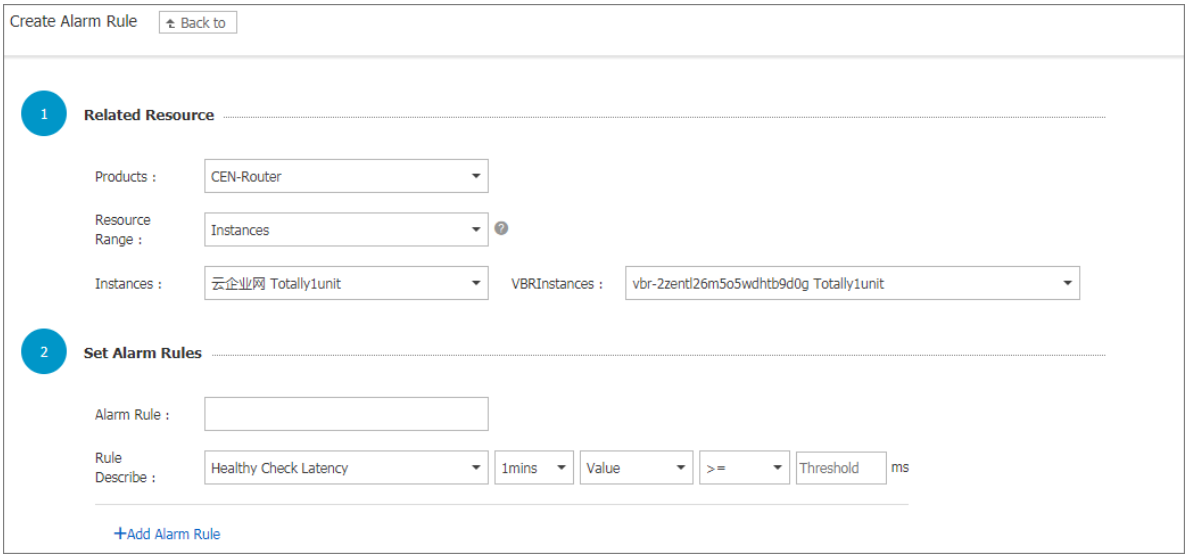
To set alarm rules for a physical connection configured with health checks, follow these steps:

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.



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.

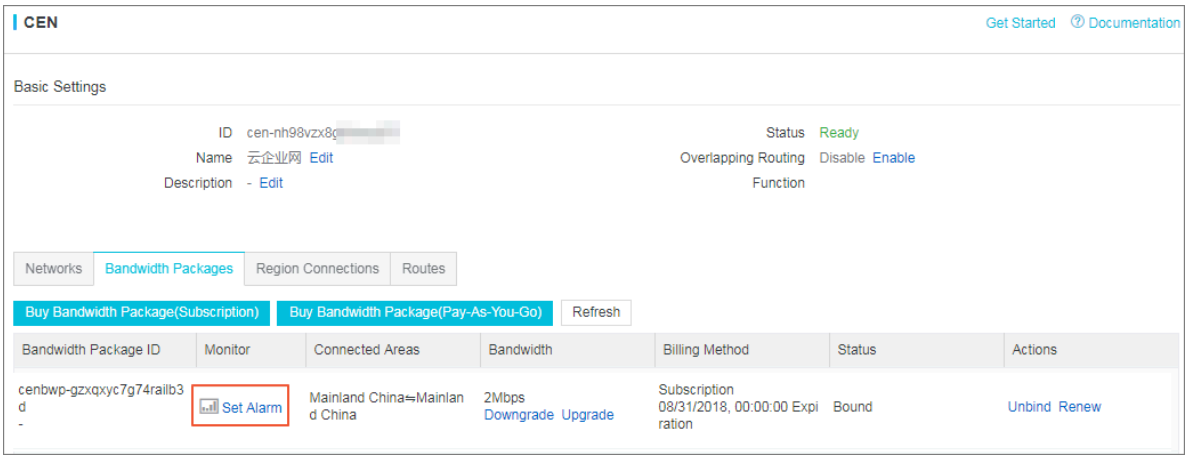


Set alarm rules for a bandwidth package

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

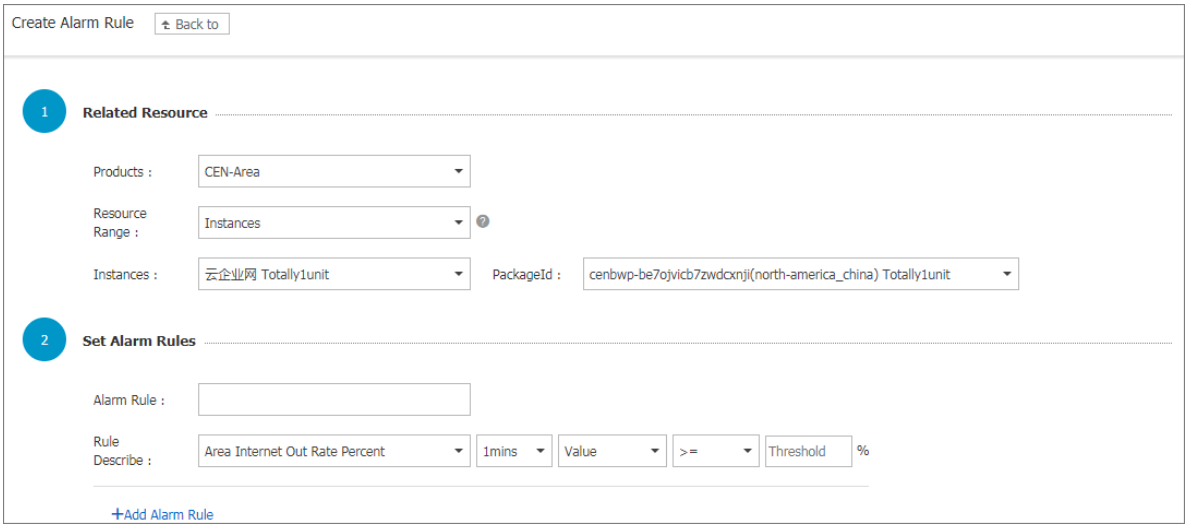
1. Log on to the CEN console.

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.

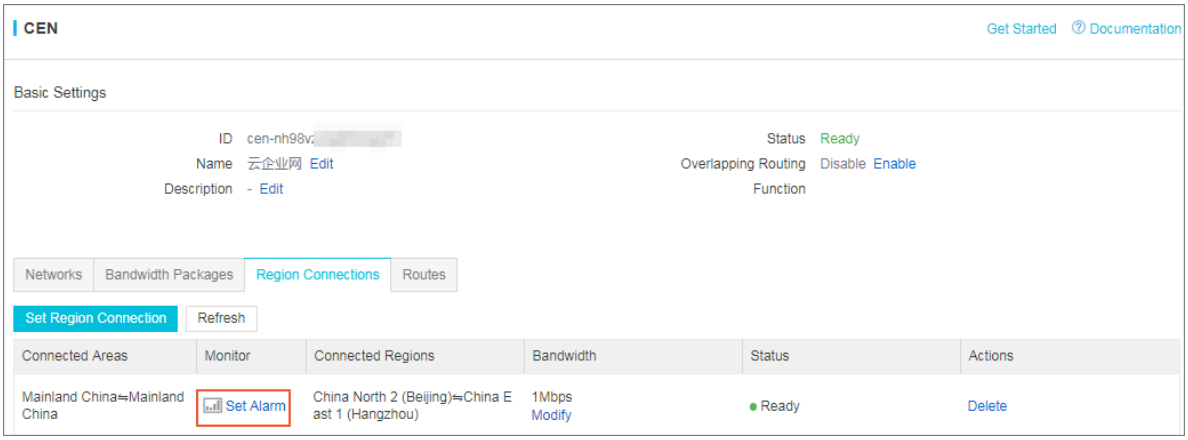


Set alarm rules for a region connection

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

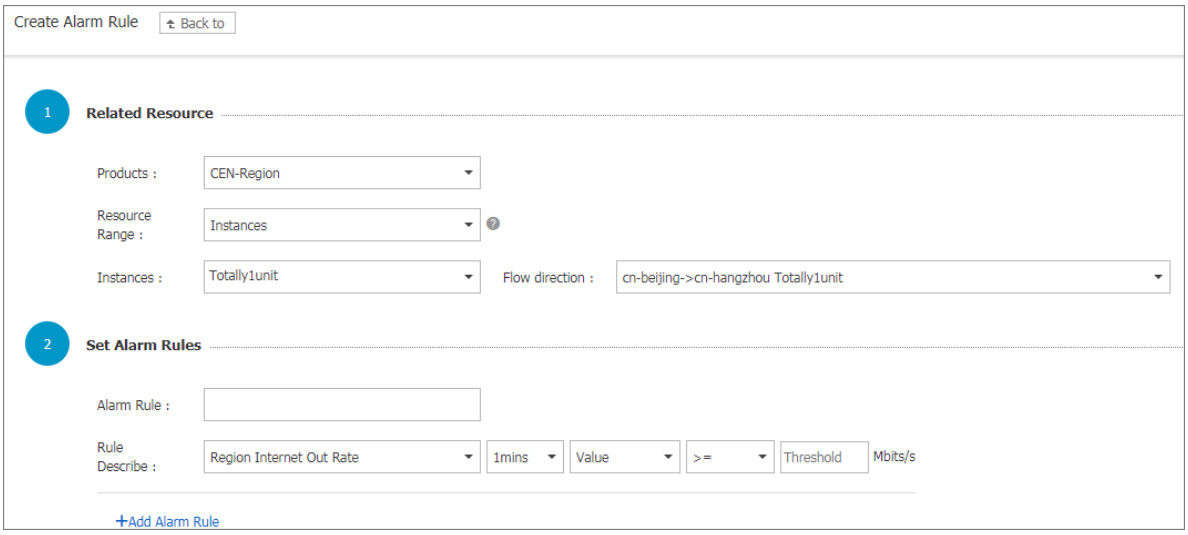
1. Log on to the CEN console.
2. Click the ID of the target CEN instance and then click the Region Connections tab.

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



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.



11 Manage quotas

You can query the number of remaining resources in your quota through the Cloud Enterprise Network (CEN) console. If the remaining quota number is insufficient for your requirements, you can apply to increase the quota.

Procedure

1. Log on to the CEN console.
2. In the left-side navigation pane, click Quota to view the resource usage of the CEN service under your account.
3. To increase your resource quota, click Apply in the Actions column. Then, enter the following information:
   - Quantity for Application: the number of resources you require. You must enter a number that is greater than the current quota. For more information about the resource limits of CEN, see #unique_35.
   - Reason for Application: your reason for applying for an increase to your quota. We recommend that you include details about your specific scenario.
   - Mobile/Landline Phone Number: the mobile or landline phone number of the person to contact.
   - Email: the email address of the person to contact.
4. Click OK.

   The system then determines whether the quota application is reasonable.
   - If the system determines the request is unreasonable, the application enters the Rejected state.
   - If the request is reasonable, the application enters the Approved state, and the quota is automatically upgraded to the applied quota number.

   To view a history of quota applications, click Application History in the Application History column.