

Direct Connect

User Guide

Issue 01
Date 2022-04-12



Copyright © Huawei Technologies Co., Ltd. 2022. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Service Overview.....	1
1.1 Overview.....	1
1.2 Product Advantages.....	2
1.3 Network Requirements.....	2
1.4 Constraints and Limitations.....	2
1.5 Permissions Management.....	3
1.6 Basic Concepts.....	5
1.6.1 Connection.....	5
1.6.2 Virtual Gateway.....	5
1.6.3 Virtual Interface.....	5
1.6.4 Region and AZ.....	5
2 Getting Started.....	7
2.1 Process Description.....	7
2.2 Establishing Network Connectivity.....	8
3 Management.....	11
3.1 Managing Connections.....	11
3.1.1 Viewing a Connection.....	11
3.1.2 Modifying a Connection.....	11
3.2 Managing Virtual Gateways.....	12
3.2.1 Viewing a Virtual Gateway.....	12
3.2.2 Modifying a Virtual Gateway.....	12
3.2.3 Deleting a Virtual Gateway.....	12
3.3 Managing Virtual Interfaces.....	13
3.3.1 Viewing a Virtual Interface.....	13
3.3.2 Modifying a Virtual Interface.....	13
3.3.3 Deleting a Virtual Interface.....	13
3.4 Managing Historical Connections.....	14
3.4.1 Viewing a Historical Connection.....	14
3.4.2 Modifying a Historical Connection.....	14
3.5 Managing Operations or Hosted Connections.....	14
3.5.1 Operations Connection.....	15
3.5.2 Hosted Connection.....	15

3.6 Monitoring.....	16
3.6.1 Overview.....	16
3.6.2 Metrics.....	16
3.6.3 Network Quality Metrics (Agent Required).....	18
3.6.4 Installing the Direct Connect Metric Collection Plug-ins.....	19
3.6.5 Setting an Alarm Rule.....	23
3.6.6 Viewing Metrics.....	24
3.7 Permissions.....	24
3.7.1 Creating a User and Granting Permissions.....	24
3.8 Quotas.....	26
4 FAQs.....	27
4.1 Is BGP Routing Supported in Direct Connect?.....	27
4.2 What Are the Network Requirements for Connections?.....	27
5 Change History.....	28

1 Service Overview

1.1 Overview

What Is Direct Connect?

Direct Connect establishes a dedicated connection between your data center and the cloud. You can use one connection to access cloud computing resources in different regions, helping build a secure and reliable hybrid environment.

Application Scenarios

You need a dedicated network connection between your data center and a Virtual Private Cloud (VPC) to ensure high bandwidth, low latency, and robust security.

Components

There are three key components for you to use Direct Connect: connection, virtual gateway, and virtual interface.

- **Connection**

A connection is a dedicated network connection between your on-premises data center and a Direct Connect location over a leased line provided by a carrier. You can request standard connections.

A standard connection provides a port that is exclusive to you and allows you to have multiple virtual interfaces associated.

- **Virtual gateway**

A virtual gateway is a logical gateway for accessing a VPC. A virtual gateway can be associated with only one VPC. Multiple connections can access the same VPC through a single virtual gateway.

- **Virtual interface**

A virtual interface is an entrance for you to access VPCs through a leased line. A virtual interface associates your connection with a virtual gateway, which connects to a VPC so that your network can access the cloud.

1.2 Product Advantages

Direct Connect has the following advantages:

- **High security**
Direct Connect establishes private connectivity between your premises and one or more VPCs while maintaining network isolation between different workloads.
- **Low latency**
A dedicated network is used for data transmission, which brings high network performance, low latency, and excellent user experience.
- **High bandwidth**
A single connection supports up to 10 Gbit/s bandwidth, meeting your connectivity needs today and tomorrow.
- **Great scalability**
By connecting your on-premises network to the cloud, you gain access to virtually unlimited cloud resources for flexible, scalable hybrid deployment.

1.3 Network Requirements

- Your network must use a single-mode fiber with a 1GE or 10GE optical module to connect to the access device in the cloud.
- Auto-negotiation for the port must be disabled.
- Port speed and full-duplex mode must be manually configured.
- 802.1Q VLAN encapsulation must be supported on the entire connection, including intermediate devices.
- If BGP routing is used, your device must support BGP and BGP MD5 authentication.
- (Optional) You can configure Bidirectional Forwarding Detection (BFD) on the network.
- The maximum transmission unit (MTU) supported at the physical layer is 1522 bytes (14-byte Ethernet header + 4-byte VLAN tag + 1500-byte IP datagram + 4-byte frame check sequence).
- Private IP addresses are recommended on the cloud, and IP address ranges for interworking cannot conflict with each other.

1.4 Constraints and Limitations

Resource	Quota
Number of connections that can be created for an account in each region	10

Resource	Quota
Number of virtual interfaces that can be created for an account in each region	50
Number of routes for BGP sessions on a virtual interface	100
Number of static routes on a virtual interface	50

1.5 Permissions Management

If you need to assign different permissions to employees in your enterprise to access your Direct Connect resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your resources.

With IAM, you can use your account to create IAM users, and assign permissions to the users to control their access to specific resources. For example, some software developers in your enterprise need to use Direct Connect but should not be allowed to delete other Direct Connect resources or perform any other high-risk operations. In this scenario, you can create IAM users for the software developers and grant them only the required permissions.

Skip this part if your account does not require individual IAM users for permissions management.

IAM is free. You pay only for the resources in your account.

For more information, see [IAM Service Overview](#).

Direct Connect Permissions

By default, new IAM users do not have any permissions assigned. To assign permissions to these new users, add them to one or more groups, and attach permissions policies or roles to these groups.

Direct Connect is a project-level service deployed and accessed in specific physical regions. To assign permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing Direct Connect, the users need to switch to a region where they have been authorized to use this service.

Table 1-1 lists all system-defined roles supported by Direct Connect.

Table 1-1 Direct Connect roles

Role Name	Description	Type	Dependency
Direct Connect Administrator	Has all permissions for Direct Connect resources. For permissions of this role to take effect, users must also have the Tenant Guest and VPC Administrator permissions.	System-defined role	Tenant Guest and VPC Administrator <ul style="list-style-type: none"> • VPC Administrator: project-level policy, which must be assigned in the same project as the Direct Connect Administrator policy • Tenant Guest: project-level policy, which must be assigned in the same project as the Direct Connect Administrator

Table 1-2 lists common operations supported by each system-defined role or policy of Direct Connect.

Table 1-2 Common operations and required system-defined permissions

Operation	Direct Connect Administrator
Creating a connection	√
Viewing a connection	√
Modifying a connection	√
Deleting a connection	√
Creating a virtual gateway	√
Viewing a virtual gateway	√
Modifying a virtual gateway	√
Deleting a virtual gateway	√
Creating a virtual interface	√
Viewing a virtual interface	√
Modifying a virtual interface	√
Deleting a virtual interface	√
Creating an operations connection	√
Viewing an operations connection	√

Operation	Direct Connect Administrator
Modifying an operations connection	√
Deleting an operations connection	√
Creating a hosted connection	√
Viewing a hosted connection	√
Modifying a hosted connection	√
Deleting a hosted connection	√

Helpful Links

- [IAM Service Overview](#)
- [Creating a User and Granting Permissions](#)

1.6 Basic Concepts

1.6.1 Connection

A connection is a dedicated network connection between your on-premises data center and a Direct Connect location over a leased line provided by a carrier. You can request standard connections.

A standard connection provides a port that is exclusive to you and allows you to have multiple virtual interfaces associated.

1.6.2 Virtual Gateway

A virtual gateway is a logical gateway for accessing a VPC. A virtual gateway can be associated with only one VPC. Multiple connections can access the same VPC through a single virtual gateway.

1.6.3 Virtual Interface

A virtual interface is an entrance for you to access VPCs through a leased line. A virtual interface associates your connection with a virtual gateway, which connects to a VPC so that your network can access the cloud.

1.6.4 Region and AZ

Concept

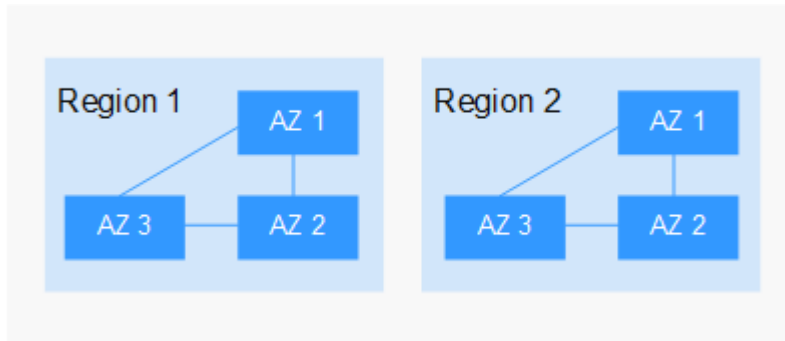
A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.

- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in one AZ will not affect others.

Figure 1-1 shows the relationship between regions and AZs.

Figure 1-1 Regions and AZs



Selecting a Region

Select a region closest to your target users for lower network latency and quick access.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

2 Getting Started

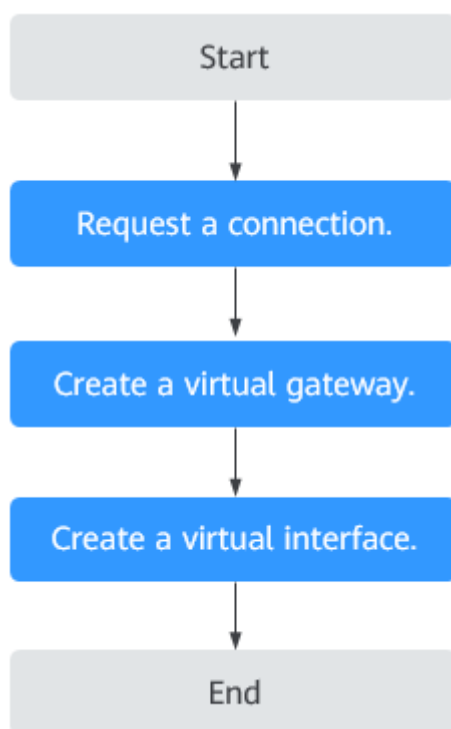
2.1 Process Description

Establish network connectivity to enable ECSs in your VPC to communicate with your data center or private network.

To do so, you first need to apply for a connection to reserve the port used to connect your on-premises data center to the Direct Connect location you select. After that, create a virtual gateway and associate it with a VPC, and finally create a virtual interface to connect to the VPC.

Figure 2-1 shows the whole process for connecting your on-premises data center to the cloud.

Figure 2-1 Enabling Direct Connect



2.2 Establishing Network Connectivity

Scenarios

Establish network connectivity using Direct Connect if cloud servers in your VPC need to communicate with your on-premises data center.

Procedure

1. Apply for a connection from your account manager. If you do not have an account manager, contact customer service.
2. Log in to the management console.
3. In the service list, choose **Network > Direct Connect**.
4. In the navigation pane on the left, choose **Direct Connect > Virtual Gateways**.
5. Click **Create Virtual Gateway**.
6. Configure the parameters.

Table 2-1 Parameter description

Parameter	Description
Name	Specifies the virtual gateway name. The name can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
VPC	Specifies the VPC to be associated with the virtual gateway.
Subnet CIDR Block	Specifies the CIDR blocks of subnets in the VPC to connect to the on-premises network.
Description	Provides supplementary information about the virtual gateway. You can enter 0 to 128 characters.

7. Click **OK**.
8. In the navigation pane on the left, choose **Direct Connect > Virtual Interfaces**.
9. Click **Create Virtual Interface**.
10. Set the parameters as prompted and then click **Create Now**.

Table 2-2 Parameter description

Parameter	Description
Region	Select the region of the VPC that needs to communicate with the on-premises data center.

Parameter	Description
Name	Specifies the virtual interface name. The name can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
Connection	Specifies the connection with which the virtual interface is to be associated. A virtual interface can be associated with only one connection.
Virtual Gateway	Select the virtual gateway with which the virtual interface is to be associated. A virtual interface can be associated with only one virtual gateway.
VLAN	Specifies the virtual interface VLAN ID. You need to configure the VLAN if you create a standard connection. The VLAN for a hosted connection will be allocated by the carrier or partner. You do not need to configure the VLAN.
Bandwidth	Specifies the virtual interface bandwidth in the unit of Mbit/s. If the selected connection is a hosted connection, the virtual interface exclusively uses the connection bandwidth.
Local Gateway	Specifies the IP address for connecting to the cloud network.
Remote Gateway	Specifies the IP address for connecting to your on-premises network.
Remote Subnet	Specifies the subnets used by the on-premises network. Specifies the remote subnet using CIDR notation. You can enter a maximum of 50 subnets. Ensure that each subnet is unique and separate every two subnets with commas (,).
Routing Mode	Specifies the routing mode. Two options are available, Static and BGP . If there are two or more connections, select BGP routing.
BGP ASN	Specifies the autonomous system number (ASN) of the BGP peer.
BGP MD5 Authentication Key	Specifies the MD5 password of the BGP peer.

Parameter	Description
Description	Provides supplementary information about the virtual interface. You can enter 0 to 128 characters.

3 Management


3.1 Managing Connections

3.1.1 Viewing a Connection

Scenarios

View details of a connection.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network > Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect > Connections**.
4. In the connection list, locate the target connection and click  before its name to view the details.

3.1.2 Modifying a Connection

Scenarios

Modify the name and description of a connection.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network > Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect > Connections**.
4. In the connection list, locate the connection and click **Modify** in the **Operation** column.
5. Modify the connection and click **OK**.


3.2 Managing Virtual Gateways

3.2.1 Viewing a Virtual Gateway

Scenarios

View details of a virtual gateway.

Procedure

1. In the service list, choose **Network > Direct Connect**.
2. In the navigation pane on the left, choose **Direct Connect > Virtual Gateways**.
3. Locate the virtual gateway you want to view and click  before its name to view the details.

3.2.2 Modifying a Virtual Gateway

Scenarios

Modify the name, subnet CIDR block, and description of a virtual gateway.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network > Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect > Virtual Gateways**.
4. Locate the virtual gateway you want to modify, click **Modify** in the **Operation** column, and modify the virtual gateway.
5. Modify the parameters and click **OK**.

3.2.3 Deleting a Virtual Gateway

Scenarios

Delete a virtual gateway if you no longer need it. Before deleting the virtual gateway, you need to delete all associated virtual interfaces.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network > Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect > Virtual Gateways**.

4. Locate the virtual gateway you want to delete and click **Delete** in the **Operation** column.
5. Click **Yes**.


3.3 Managing Virtual Interfaces

3.3.1 Viewing a Virtual Interface

Scenarios

View details of a virtual interface.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network > Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect > Virtual Interfaces**.
4. Locate the virtual interface you want to view and click  before its name to view the details.

3.3.2 Modifying a Virtual Interface

Scenarios

Modify the name, remote subnet, description, of a virtual interface.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network > Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect > Virtual Interfaces**.
4. Locate the virtual interface you want to modify and click **Modify** in the **Operation** column.
5. Modify the virtual interface and click **OK**.

3.3.3 Deleting a Virtual Interface

Scenarios

Delete a virtual interface if you no longer need it.

Procedure

1. Log in to the management console.

2. In the service list, choose **Network > Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect > Virtual Interfaces**.
4. Locate the virtual interface you want to delete and click **Delete** in the **Operation** column.
5. Click **Yes**.


3.4 Managing Historical Connections

3.4.1 Viewing a Historical Connection

Scenarios

View details of a connection that you requested through email or phone call.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network > Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect > Historical Connections**.
4. Locate the connection you want to view and click  before its name to view the details.

3.4.2 Modifying a Historical Connection

Scenarios

Modify the name and remote subnets of a historical connection.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network > Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect > Historical Connections**.
4. Locate the connection you want to modify and click **Modify** in the **Operation** column.
5. Modify the parameters and click **OK**.

3.5 Managing Operations or Hosted Connections

3.5.1 Operations Connection

Viewing an Operations Connection

Scenarios

View details of an operations connection you created as a partner.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network > Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect > Connections**.
4. Locate the operations connection you want to view and click its name.
5. View detailed information about the operations connection.

Modifying an Operations Connection

Scenarios

Modify an operations connection you created as a partner.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network > Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect > Connections**.
4. Locate the operations connection you want to modify, click **Modify** in the **Operation** column.
5. Modify the parameters and then click **OK**.


3.5.2 Hosted Connection

Viewing a Hosted Connection

Scenarios

View details of a hosted connection you created as a partner.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network > Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect > Connections**.
4. Locate the operations connection on which the hosted connection is created and click **Manage Hosted Connection** in the **Operation** column.
5. Locate the hosted connection you want to view and click  before its name to view the details.

Modifying a Hosted Connection

Scenarios

Modify the name, bandwidth, and description of a hosted connection you created as a partner.

Procedure

1. Log in to the management console.
2. In the service list, choose **Network > Direct Connect**.
3. In the navigation pane on the left, choose **Direct Connect > Connections**.
4. Locate the operations connection on which the hosted connection is created and click **Manage Hosted Connection** in the **Operation** column.
5. Locate the hosted connection you want to modify and click **Modify** in the **Operation** column.
6. Modify the parameters and click **OK**.

3.6 Monitoring

3.6.1 Overview

Monitoring is key to ensuring the performance, reliability, and availability of a service. Monitoring data lets you keep track of the status of your resources. Cloud Eye collects and displays monitoring data for you in a visualized manner. You can use Cloud Eye to automatically monitor connections in real time and manage alarms and notifications, helping you keep track of the connection performance.

To learn more information, see the following topics:

- [Metrics](#)
- [Network Quality Metrics \(Agent Required\)](#)
- [Installing the Direct Connect Metric Collection Plug-ins](#)
- [Setting an Alarm Rule](#)
- [Viewing Metrics](#)

3.6.2 Metrics

Description

Table 3-1 describes the metrics reported by Direct Connect to Cloud Eye as well as their namespaces and dimensions. You can use the management console to query the metrics of the monitored objects and alarms generated for Direct Connect.

Namespace

SYS.DCAAS

Metrics

Table 3-1 Direct Connect metrics

ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval
network_incoming_bits_rate	Network Incoming Bandwidth	Bit rate for inbound data to the Direct Connect side of a connection Unit: bit/s	≥ 0 bits/s	Connections and historical connections	1 minute
network_outgoing_bits_rate	Network Outgoing Bandwidth	Bit rate for outbound data from the Direct Connect side of a direct connection Unit: bit/s	≥ 0 bits/s	Connections and historical connections	1 minute
network_incoming_bytes	Network Incoming Traffic	Number of bytes for inbound data to the Direct Connect side of a connection Unit: byte	≥ 0 bytes	Connections and historical connections	1 minute
network_outgoing_bytes	Network Outgoing Traffic	Number of bytes for outbound data from the Direct Connect side of a connection Unit: byte	≥ 0 bytes	Connections and historical connections	1 minute
network_incoming_packets_rate	Network Incoming Packet Rate	Packet rate for inbound data to the Direct Connect side of a connection Unit: Packet/s	≥ 0 packet s/s	Connections and historical connections	1 minute
network_outgoing_packets_rate	Outgoing Packet Rate	Packet rate for outbound data from the Direct Connect side of a connection Unit: Packet/s	≥ 0 packet s/s	Connections and historical connections	1 minute

ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval
network_incoming_packets	Network Incoming Packets	Number of packets for inbound data to the Direct Connect side of a connection Unit: Packet	≥ 0 packets	Connections and historical connections	1 minute
network_outgoing_packets	Network Outgoing Packets	Number of packets for outbound data from the Direct Connect side of a connection Unit: Packet	≥ 0 packets	Connections and historical connections	1 minute

Dimensions

Key	Value
direct_connect_id	Connection
virtual_gateway_id	Virtual gateway
virtual_interface_id	Virtual interface
history_direct_connect_id	Historical connection

3.6.3 Network Quality Metrics (Agent Required)

Direct Connect plug-ins monitor the end-to-end network quality of connections along with two key metrics of remote subnets: network latency and packet loss rate.

There are two plug-ins:

- dc-nqa-collector: monitors the connections created on the Direct Connect console.
- history-dc-nqa-collector: monitors historical connections.

For details, see [Installing the Direct Connect Metric Collection Plug-ins](#).

 NOTE

- Automated connections are requested using the console and can be self-service or full-service connections. Each connection has at least a virtual gateway and a virtual interface, and their routes are automatically advertised.
- Historical connections are requested by email or phone. They do not have virtual gateways and virtual interfaces, and their routes must be configured manually.

Metrics

Table 3-2 Network quality metrics

ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval
latency	Latency	Network latency of a connection Unit: ms	≥ 0 ms	Connections and historical connections	1 minute
packet_loss_rate	Packet Loss Rate	Packet loss rate of a connection Unit: Percent	0~100%	Connections and historical connections	1 minute

Dimensions

Key	Value
virtual_interface_id	Virtual interface (associated with an automated connection)
history_direct_connection_id	Historical connection

3.6.4 Installing the Direct Connect Metric Collection Plug-ins

Direct Connect plug-ins monitor the end-to-end network quality of connections along with two key metrics of remote subnets: network latency and packet loss rate.

There are two plug-ins:

- `dc-nqa-collector`: monitors the connections created on the Direct Connect console.
- `history-dc-nqa-collector`: monitors historical connections.

NOTE

Automated connections are requested using the console and can be self-service or full-service connections. Each connection has at least a virtual gateway and a virtual interface, and their routes are automatically advertised. Connections in most regions are automated.

Historical connections are requested by email or phone. They do not have virtual gateways and virtual interfaces, and their routes must be configured manually. Historical connections exist only in some regions.

Constraints

The plug-ins support only Linux. ECSs where the plug-ins are to be installed must be in the same VPC as the connection.

Prerequisites

- Cloud Eye is available in the current region.
- You have obtained the monitoring plug-ins and one-click installation script from the Direct Connect manager.

Procedure

Step 1 Install the Agent provided by Cloud Eye for server monitoring.

1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. In the navigation pane on the left, choose **Server Monitoring** > **Elastic Cloud Server**.
4. Click **Install and configure the Agent**.
5. Select the Agent based on the server type.
x86 servers are recommended, and the image version must be 7.0 or later.
6. Copy the installation command and run it on the server.

```
root@ecs-dces-ces ~]#  
root@ecs-dces-ces ~]# cd /usr/local && wget --no-check-certificate https://telescope-cn-south-235.obs.guet.edu.cn/scripts/agent  
install.sh && chmod 755 agentinstall.sh && ./agentinstall.sh
```

If **Telescope process starts successfully** is displayed, the Agent has been installed.


```
Connecting to telescope-cn-south-235.obs.gueta.edu.cn (telescope-cn-south-235.obs.gueta.edu.cn|188.125.32.611:443)
WARNING: cannot verify telescope-cn-south-235.obs.gueta.edu.cn's certificate, issued by "/C=CN/ST=sc/D=hu/OU=hu/CN=
Unable to locally verify the issuer's authority.
WARNING: certificate common name 'obs.huawei.com' doesn't match requested host name 'telescope-cn-south-235.ob
HTTP request sent, awaiting response... 200 OK
Length: 221 (application/gzip)
Saving to: 'agentInstall.sh'
188[=====] 221 --K/s
2021-01-14 19:26:04 (19.1 MB/s) - 'agentInstall.sh' saved [221/221]
--2021-01-14 19:26:04-- http://telescope-cn-south-235.obs.cn-south-235.gueta.edu.cn/agent/telescope_linux_amd64.ta
Resolving telescope-cn-south-235.obs.cn-south-235.gueta.edu.cn (telescope-cn-south-235.obs.cn-south-235.gueta.edu.cn
2.61
Connecting to telescope-cn-south-235.obs.cn-south-235.gueta.edu.cn (telescope-cn-south-235.obs.cn-south-235.gueta.edu.cn
32.611:80:.. connected.
HTTP request sent, awaiting response... 200 OK
Length: 7838529 (7.5M) (application/gzip)
Saving to: 'telescope_linux_amd64.tar.gz'
188[=====] 7,838,529 --K/s
2021-01-14 19:26:05 (283 MB/s) - 'telescope_linux_amd64.tar.gz' saved [7838529/7838529]
telescope_linux_amd64/
telescope_linux_amd64/bin/
telescope_linux_amd64/bin/conf_ces.json
telescope_linux_amd64/bin/logs_config.xml
telescope_linux_amd64/bin/telescope
telescope_linux_amd64/bin/agent
telescope_linux_amd64/bin/conf.json
telescope_linux_amd64/install.sh
telescope_linux_amd64/telescope-1.2.2-release.json
telescope_linux_amd64/telescopeid
telescope_linux_amd64/uninstall.sh
/bin/curl
ces flag NOT FOUND in __support_agent_list
Current user is root.
Current linux release version : CENTOS
Start to install telescope...
In chkconfig
Success to install telescope to dir: /usr/local/telescope.
Starting telescope...
Telescope process starts successfully.
[root@ecs-dces-ces local]#
```

Step 2 Upload the plug-ins to an OBS bucket.

1. Log in to the management console.
2. Choose **Service List > Storage > Object Storage Service**.
3. Click **Create Bucket**.
4. Configure the parameters.

Enter a bucket name and set **Bucket Policy** to **Public Read**.

CAUTION

The public read permission allows any user to read objects in the bucket without identity authentication. To ensure data security, change the bucket policy to **Private** after configuring the plug-ins. You can modify the bucket policy as required.

5. Click **Create Now**.
6. Click the name of the created bucket on the bucket list page.
7. On the **Overview** page of the bucket, copy the access domain name.
8. In the navigation tree on the left, click **Objects**.
9. On the **Objects** page, click **Upload Object**.
10. Decompress the **dc_plugins_x86.rar** and upload the decompressed file to the OBS bucket.

Step 3 Use the one-click installation script dc-installer.sh to configure the plug-ins.

1. Log in to an ECS as user **root**.
2. Create the **user.txt** file in the **/usr/local/** directory and add user information, including the plug-ins download path, monitored resource ID, and remote IP address:

```
cd /usr/local/
vi user.txt
```

The **user.txt** file contains the path of the plug-ins in the OBS bucket, virtual interface ID, and IP address of the remote gateway.

- Path of the plug-ins in the OBS bucket: Select dc-nqa-collector for automated connections. Select history-dc-nqa-collector for historical connections, as shown below:
`https://cesplugin.obs.xxx.edu.cn/dc-nqa-collector`
- Information about monitored resources: Each resource occupies a line, and consists of a resource ID and a remote IP address separated from the resource ID by a comma (,). To add multiple resources, add lines in the same format, as shown below:
`75e09ecf-xxxx-xxxx-xxx-e1295e03e5dc,x.x.x.x`
 - Resource ID: If dc-nqa-collector is used, resource ID is the virtual interface ID, which can be queried on the **Virtual Interfaces** page of the Direct Connect console. If history-dc-nqa-collector is used, resource ID is the historical connection ID, which can be queried on the **Historical Connections** page of the Direct Connect console.
 - Remote IP address: the IP address of the remote gateway or an IP address in the remote subnet, which will be used to ping an IP address in the VPC. If dc-nqa-collector is used, you can query the IP address of the remote gateway on the **Virtual Interfaces** page. If history-dc-nqa-collector is used, you can query the IP address in the remote subnet on the **Historical Connections** page.

NOTE

Ensure that each resource ID matches one remote IP address. You cannot enter multiple IP addresses or CIDR blocks.

After the Agent is installed, if you want to add more resources to be monitored, edit the **user.txt** file by adding new IDs and IP addresses in sequence, and then perform **3**.

3. Run the one-click installation script.

Copy the storage path of the script in the OBS bucket.

Example command:

```
cd /usr/local && wget --no-check-certificate https://xxx.cn/dc-installer.sh && chmod 755 dc-installer.sh && ./dc-installer.sh
```

```
[root@ecs-dcs-ces local]# cd /usr/local && wget --no-check-certificate https://cesplugin.obs.cn-south-235.gueta.edu.cn/dc-installer.sh && chmod 755 dc-installer.sh && ./dc-installer.sh
```

```
64 bytes from 1.1.1.1: icmp_seq=4 ttl=254 time=6.91 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=254 time=9.76 ms

--- 1.1.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4886ms
rtt min/avg/max/mdev = 3.863/39.849/176.375/68.389 ms
Ping success. Continue to install dc-nqa-collector
--2021-01-14 19:30:11-- https://cesplugin.obs.cn-south-235.gueta.edu.cn/dc-nqa-collector
Resolving cesplugin.obs.cn-south-235.gueta.edu.cn (cesplugin.obs.cn-south-235.gueta.edu.cn)... 100.125.32.61
Connecting to cesplugin.obs.cn-south-235.gueta.edu.cn (cesplugin.obs.cn-south-235.gueta.edu.cn)|100.125.32.61|:443...
WARNING: cannot verify cesplugin.obs.cn-south-235.gueta.edu.cn's certificate, issued by '/C=cn/ST=sc/0=hw/OU=hw/CN=
Unable to locally verify the issuer's authority.
WARNING: certificate common name 'obs.huawei.com' doesn't match requested host name 'cesplugin.obs.cn-south-235.gueta.edu.cn'
HTTP request sent, awaiting response... 200 OK
Length: 8066624 (7.7M) [application/octet-stream]
Saving to: 'dc-nqa-collector'

100%[=====] 8,066,624  --.-K/s

2021-01-14 19:30:11 (237 MB/s) - 'dc-nqa-collector' saved [8066624/8066624]

--2021-01-14 19:30:11-- https://cesplugin.obs.cn-south-235.gueta.edu.cn/dc-nqa-conf.json
Resolving cesplugin.obs.cn-south-235.gueta.edu.cn (cesplugin.obs.cn-south-235.gueta.edu.cn)... 100.125.32.61
Connecting to cesplugin.obs.cn-south-235.gueta.edu.cn (cesplugin.obs.cn-south-235.gueta.edu.cn)|100.125.32.61|:443...
WARNING: cannot verify cesplugin.obs.cn-south-235.gueta.edu.cn's certificate, issued by '/C=cn/ST=sc/0=hw/OU=hw/CN=LEVEL2-ROOT-C
Unable to locally verify the issuer's authority.
WARNING: certificate common name 'obs.huawei.com' doesn't match requested host name 'cesplugin.obs.cn-south-235.gueta.edu.cn'
HTTP request sent, awaiting response... 200 OK
Length: 90 [application/json]
Saving to: 'dc-nqa-conf.json'

100%[=====] 90  --.-K/s in 8s

2021-01-14 19:30:11 (4.00 MB/s) - 'dc-nqa-conf.json' saved [90/90]

cat: 'dc-nqa-user-conf.json' and '/usr/local/telescope/plugins/dc/dc-nqa-user-conf.json' are the same file
cat: /usr/local/telescope/plugins/conf.json: No such file or directory
Restarting telescope...
Stopping telescope...
Stop telescope process successfully
Starting telescope...
Telescope process starts successfully.
ok, dc-nqa-collector install success!
root@ecs-4e9e-1000:~#
```

Step 4 View monitoring information.

1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. In the navigation pane on the left, choose **Server Monitoring > Elastic Cloud Server**.
Ensure that the Agent is in the **Running** state.
4. In the navigation pane on the left, choose **Cloud Service Monitoring > Direct Connect**.
5. Click the name of the monitored object to view the network delay and packet loss rate.


----End

3.6.5 Setting an Alarm Rule

Scenarios

You can configure alarm rules to customize monitored objects and notification policies and to learn connection status at any time.

Procedure



1. Log in to the management console.
2. Click  in the upper left corner of the management console and select a region and a project.
3. Hover on the upper left corner to display **Service List** and choose **Management & Governance > Cloud Eye**.

4. In the navigation pane on the left, choose **Alarm Management > Alarm Rules**.
5. On the **Alarm Rules** page, click **Create Alarm Rule** to create one. (You can also modify an existing alarm rule.)
6. After configuring the parameters, click **Create**.
After the alarm rule is set, the system automatically notifies you when an alarm is triggered.

 **NOTE**

For more information about Direct Connect alarm rules, see the *Cloud Eye User Guide*.

3.6.6 Viewing Metrics

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Hover on  to display **Service List** and choose **Management & Governance > Cloud Eye**.
4. In the navigation pane on the left, choose **Cloud Service Monitoring > Direct Connect**.
5. Click **View Metric** in the **Operation** column.
You can view data of the last one, three, 12, or 24 hours, or last 7 days.

3.7 Permissions

3.7.1 Creating a User and Granting Permissions

Use **IAM** to implement fine-grained permissions control over your Direct Connect resources. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to cloud resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust another account or cloud service to perform professional and efficient O&M on your cloud resources.

Skip this part if your account does not require individual IAM users.

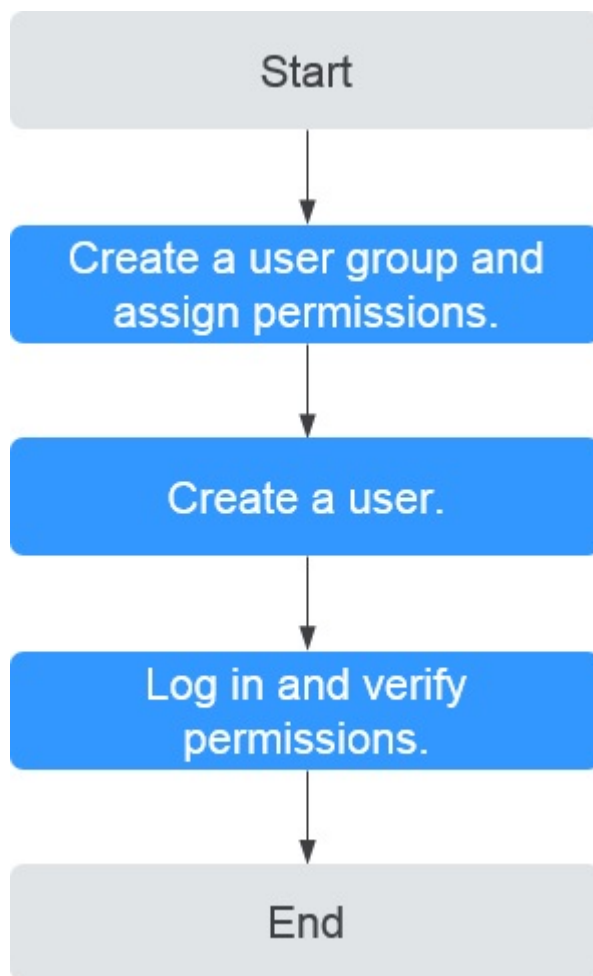
The following is the procedure for granting permissions.

Prerequisites

Before assigning permissions to user groups, you should learn about Direct Connect system policies and select the policies based on service requirements. For details about system permissions of Direct Connect, see [Permissions Management](#). For system permissions of other cloud services, see [Permission Description](#).

Process Flow

Figure 3-1 Process for granting Direct Connect permissions



1. **Create a user group and assign permissions.**
Create a user group on the IAM console and attach the **Direct Connect Administrator** policy to the group, which grants users read-only permissions to Direct Connect resources.
2. **Create a user and add the user to the user group** created in the preceding step.
3. **Log in to the management console as the created user.**
Switch to the authorized region and verify the permissions.
 - Choose **Service List > Network > Direct Connect**. On the displayed page, click **Create Connection**. If the connection fails to be created, the **Direct Connect Administrator** policy has taken effect.
 - Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **Direct Connect Administrator** policy has already taken effect.



3.8 Quotas

What Is Quota?

Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, click  .
The **Service Quota** page is displayed.
4. View the used and total quota of each type of resources on the displayed page.
If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources > My Quotas**.
The **Service Quota** page is displayed.
3. Click **Increase Quota**.
4. On the **Create Service Ticket** page, configure parameters as required.
In **Problem Description** area, fill in the content and reason for adjustment.
5. After all necessary parameters are configured, select **I have read and agree to the Tenant Authorization Letter and Privacy Statement** and click **Submit**.

4 FAQs

4.1 Is BGP Routing Supported in Direct Connect?

Yes. Direct Connect allows you to use BGP for routing.

4.2 What Are the Network Requirements for Connections?

- Your network must use a single-mode fiber with a 1GE or 10GE optical module to connect to the access device in the cloud.
- Auto-negotiation for the port must be disabled. Port speed and full-duplex mode must be manually configured.
- 802.1Q VLAN encapsulation must be supported on the entire connection, including intermediate devices.
- If BGP routing is used, your device must support BGP and BGP MD5 authentication.
- (Optional) You can configure Bidirectional Forwarding Detection (BFD) on the network.
- The maximum transmission unit (MTU) supported at the physical layer is 1522 bytes (14-byte Ethernet header + 4-byte VLAN tag + 1500-byte IP datagram + 4-byte frame check sequence).
- Private IP addresses are recommended on the cloud, and IP address ranges for interworking cannot conflict with each other.

5 Change History

Release On	Description
2022-04-12	This issue is the first official release.