

# Alibaba Cloud

Virtual Private Cloud

Flow logs

Document Version: 20220527

# Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).
5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please directly contact Alibaba Cloud for any errors of this document.

# Document conventions

Style	Description	Example
 <b>Danger</b>	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 <b>Danger:</b> Resetting will result in the loss of user configuration data.
 <b>Warning</b>	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 <b>Warning:</b> Restarting will cause business interruption. About 10 minutes are required to restart an instance.
 <b>Notice</b>	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 <b>Notice:</b> If the weight is set to 0, the server no longer receives new requests.
 <b>Note</b>	A note indicates supplemental instructions, best practices, tips, and other content.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click <b>Settings</b> > <b>Network</b> > <b>Set network type</b> .
<b>Bold</b>	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click <b>OK</b> .
Courier font	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

# Table of Contents

1. Overview of the flow log feature .....	05
2. Work with flow logs .....	08
3. Examples .....	13
3.1. View the traffic data of an ECS instance in a VPC .....	13
3.2. Query traffic between VPCs .....	17

# 1. Overview of the flow log feature

Virtual Private Cloud (VPC) provides flow logs that record information about inbound and outbound traffic of an elastic network interface (ENI). Flow logs help you verify rules of network access control lists (ACLs), monitor network traffic, and troubleshoot network issues.

## Feature release and supported regions

The flow log feature is in public preview. To use this feature, [submit a ticket](#) apply for the public preview qualification.

The following table describes the regions that support the flow log feature.

Area	Region
Asia Pacific	
Europe and Americas	
Middle East	

## Description

Flow logs can capture information about network traffic of a specified ENI, VPC, or vSwitch. After you enable the flow log feature for a VPC or a vSwitch, traffic information about ENIs in the VPC or vSwitch is captured. Flow logs also capture traffic information about ENIs that are created after the flow log feature is enabled.

The traffic information captured by the flow log feature is written to Log Service as flow log entries. Each flow log entry includes a 5-tuple of a traffic flow captured within the capture window. The capture window is approximately 10 minutes. During the capture window, traffic information is captured and aggregated into a flow log entry.

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

Field	Description
version	The version of the flow log.
vswitch-id	The ID of the vSwitch to which the ENI belongs.
vm-id	The ID of the Elastic Compute Service (ECS) instance with which the ENI is associated.
vpc-id	The ID of the VPC to which the ENI belongs.
account-id	The ID of the account.
eni-id	The ID of the ENI.
srcaddr	The source IP address.
srcport	The source port.

Field	Description
dstaddr	The destination IP address.
dstport	The destination port.
protocol	The Internet Assigned Numbers Authority (IANA) protocol number of the traffic. For more information, see <a href="#">Protocol Numbers</a> .
direction	The direction of the traffic. Valid values: <ul style="list-style-type: none"><li>• in: inbound</li><li>• out: outbound</li></ul>
packets	The number of data packets.
bytes	The size of data packets.
start	The start time of the capture window.
end	The end time of the capture window.
log-status	The logging status of the flow log. Valid values: <ul style="list-style-type: none"><li>• OK: Data is being recorded as expected.</li><li>• NODATA: No inbound or outbound traffic was transmitted through the ENI during the capture window.</li><li>• SKIPDATA: Some flow log entries were skipped during the capture window.</li></ul>
action	The action that was performed on the traffic flow. Valid values: <ul style="list-style-type: none"><li>• ACCEPT: The traffic flow was allowed by security groups or ACLs.</li><li>• REJECT: The traffic flow was rejected by security groups or ACLs.</li></ul>

## Billing and pricing

You can store and analyze flow logs only in Log Service. You are charged for flow log collection and Log Service resources when you use flow logs.

- Flow log collection fee

You are charged a flow log collection fee based on the number of flow logs that are collected.

 **Note** You are not charged a flow log collection fee during the public preview.

- Usage fee of Log Service resources

The traffic information captured by a flow log is stored in Log Service. You can view and analyze the information in Log Service. You are charged for data storage and retrieval when you use Log Service.

## Limits

## Configuration process



### 1. Activate Log Service

The traffic information captured by the flow log feature is stored in Alibaba Cloud Log Service. You must activate Log Service before you create a flow log.

### 2. Optional. Create an AccessKey pair

If you want to write data by using an API or SDK, you must create an AccessKey pair. If you want to collect logs by using Logtail, you do not need to create an AccessKey pair.

### 3. Create a project

You must create a project in Log Service. For more information, see [Create a project](#).

### 4. Create a Logstore

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

### 5. Specify a resource from which traffic information is captured

Before you create a flow log, you must specify the resource from which traffic information is captured. You can capture traffic information from an ENI, VPC, or vSwitch. For more information, see [Create an ENI](#), [创建和管理专有网络](#), and [Work with vSwitches](#).

### 6. Create a flow log

After you create a flow log, the flow log can capture traffic information about network instances that are attached to a Cloud Enterprise Network (CEN) instance in different regions. For more information, see [Work with flow logs](#).

### 7. View flow logs

After you create a flow log, you can view the flow log. You can analyze inter-region data transmission, control data transfer costs, and troubleshoot network issues based on the captured traffic information. For more information, see [Analyze a flow log](#).

## 2. Work with flow logs

Virtual Private Cloud (VPC) provides the flow log feature to capture information about inbound and outbound traffic of an elastic network interface (ENI). You can use the flow log feature to check access control list (ACL) rules, monitor network traffic, and troubleshoot network errors. This topic describes how to use flow logs.

### Operations

- [Create a flow log](#)
- [View flow logs](#)
- [Modify a flow log](#)
- [Enable a flow log](#)
- [Disable a flow log](#)
- [Delete a flow log](#)

### Create a flow log

Make sure that the following requirements are met:

- Log Service is activated on the [Log Service page](#). [Log Service page](#).
- A project and a Logstore are created to store and manage log data. For more information, see [Create a project](#) and [Create a Logstore](#).
- A resource from which you want to capture traffic information is created. For more information, see [Create an ENI](#), [创建和管理专有网络](#), and [Work with vSwitches](#).

- 1.
- 2.
3. If this is the first time that you use the flow log feature, click **Authorize** and click **Confirm**. You must complete the authorization to ensure that flow logs can be imported to Log Service.
4. In the top navigation bar, select the region where you want to create the flow log.  
For more information about regions that support the flow log feature, see [Feature release and supported regions](#).
5. On the **Flow Log** page, click **Create FlowLog**.
6. In the **Create FlowLog** dialog box, set the following parameters and click **OK**.

Parameter	Description
<b>Name</b>	<p>Specify a name for the flow log.</p> <p>The name must be 2 to 128 characters in length and can contain letters, digits, hyphens (-), and underscores (_). The name must start with a letter and cannot start with <code>http://</code> or <code>https://</code>.</p>

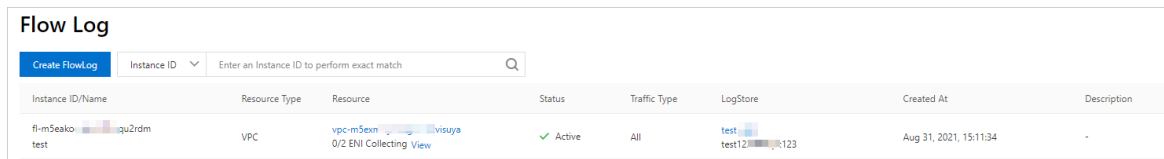


Parameter	Description
<b>Resource Type</b>	<p>Select the type of resource from which you want to capture traffic information, and then select the resource. Supported resource types:</p> <ul style="list-style-type: none"> <li>◦ <b>VPC</b>: captures traffic information from all ENIs in the specified VPC. If the VPC contains Elastic Compute Service (ECS) instances that do not support flow logs, traffic information about ENIs of the ECS instances cannot be captured.</li> <li>◦ <b>VSwitch</b>: captures traffic information from all ENIs associated with the specified vSwitch. If the vSwitch contains ECS instances that do not support flow logs, traffic information about ENIs of the ECS instances cannot be captured.</li> <li>◦ <b>Network Interface</b>: captures traffic information about the specified ENI. If the ENI is associated with an ECS instance that does not support flow logs, traffic information about the ENI cannot be captured.</li> </ul> <p>ECS instances of the following types do not support flow logs:</p> <p>To use flow logs, upgrade the ECS instance. For more information, see <a href="#">Upgrade the instance types of subscription instances</a> and <a href="#">Change the instance type of a pay-as-you-go instance</a>.</p>
<b>Traffic Type</b>	<p>Select the type of traffic information that you want to capture. Valid values:</p> <ul style="list-style-type: none"> <li>◦ <b>All</b>: captures traffic information from the specified resource.</li> <li>◦ <b>Allow</b>: captures information about traffic that is allowed by security group rules and network ACL rules of the specified resource.</li> <li>◦ <b>Drop</b>: captures information about traffic that is denied by security group rules and network ACL rules of the specified resource.</li> </ul>
<b>Project</b>	<p>Specify a project to manage captured traffic information.</p> <ul style="list-style-type: none"> <li>◦ <b>Select Project</b>: Select an existing project to store the captured traffic information.</li> <li>◦ <b>Create Project</b>: Create a project to store captured traffic information.</li> </ul>
<b>Logstore</b>	<p>Specify a Logstore to store captured traffic information.</p> <ul style="list-style-type: none"> <li>◦ <b>Select Logstore</b>: Select a Logstore from an existing project to store the captured traffic information.</li> <li>◦ <b>Create Logstore</b>: Create a Logstore to store captured traffic information.</li> </ul>
<b>Turn on FlowLog Analysis Report Function</b>	<p>Select this option to enable Log Service indexing and create a dashboard for the Logstore. Then, you can consume the log data by using SQL queries or analyze the log data in the dashboard.</p> <p>Log Service dashboards are free of charge. However, Log Service indexing is billed based on data usage. For more information, see <a href="#">Log Service billing</a>.</p>
<b>Description</b>	<p>Enter a description for the flow log.</p> <p>The description must be 2 to 256 characters in length and cannot start with <code>http://</code> or <code>https://</code>.</p>

## View flow logs

After you create a flow log, you can view the information about the flow log and the ENIs from which traffic information is captured.

- 
- 
- 
4. You can view flow logs on the **Flow Log** page.



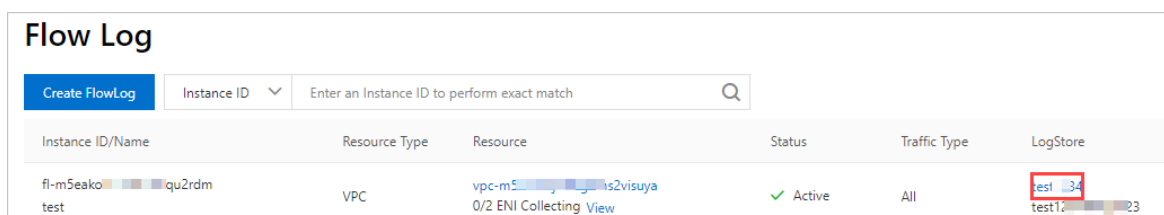
Flow Log							
<a href="#">Create FlowLog</a> Instance ID <input type="text" value="Enter an Instance ID to perform exact match"/>							
Instance ID/Name	Resource Type	Resource	Status	Traffic Type	LogStore	Created At	Description
fl-m5eako-qu2rdm-test	VPC	vpc-m5eak-visuya-0/2 ENI Collecting <a href="#">View</a>	✓ Active	All	test-123	Aug 31, 2021, 15:11:34	-

- 
- 
- 
- 
5. On the **Flow Log** page, find the flow log that you want to view and click **View** in the **Resource** column.
6. In the **Flow Log Collection Details** panel, view the basic information about the flow log including the ID, status, and capture scope.
7. In the **Flow Log Collection Details** panel, click the **ENIs with Flow Logs Unsupported** or **All ENIs** tab to view the information about the ENIs.
  - **ENIs with Flow Logs Unsupported**: The ENIs from which traffic information cannot be captured.
  - **All ENIs**: All the ENIs that belong to the capture scope. For example, if flow logs capture traffic information about a VPC, this section displays all the ENIs in the VPC, including the ENIs from which traffic information can be captured and cannot be captured.

## Analyze a flow log

You can check ACL rules, monitor network traffic, and troubleshoot network errors by analyzing a flow log.

- 
- 
- 
4. On the **Flow Log** page, find the flow log that you want to analyze, and click the name of the Logstore.



Flow Log						
<a href="#">Create FlowLog</a> Instance ID <input type="text" value="Enter an Instance ID to perform exact match"/>						
Instance ID/Name	Resource Type	Resource	Status	Traffic Type	LogStore	
fl-m5eako-qu2rdm-test	VPC	vpc-m5eak-visuya-0/2 ENI Collecting <a href="#">View</a>	✓ Active	All	test-34-test12-23	

- 
- 
- 
- 
5. In the Log Service console, click **Search & Analyze**.  
After the flow log appears, you can view and analyze the data.

## Modify a flow log

After you create a flow log, you can modify the name and description of the flow log.

1. Log on to the [VPC console](#).
- 2.
- 3.
4. On the **Flow Log** page, find the flow log that you want to modify, and click the



icon in the **Instance ID/Name** column to modify the name of the flow log.

The name must be 2 to 128 characters in length and can contain letters, digits, underscores (\_), and hyphens (-). The name must start with a letter.

5. Click



in the **Description** column to modify the description of the flow log.

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

## Enable a flow log

You can enable a flow log that is in the **Inactive** state. After you enable the flow log, the flow log starts to capture traffic information about ENIs.

1. Log on to the [VPC console](#).
- 2.
- 3.
4. On the **Flow Log** page, find the flow log and click **Enable** in the **Actions** column. After the flow log is enabled, the status of the flow log changes to **Active**.

Instance ID/Name	Resource Type	Resource	Status
fl-m5eakol...3qu2rdm t...t	VPC	vpc-m5exn...ms2visuya 0/2 ENI Collecting <a href="#">View</a>	✓ Active

## Disable a flow log

You can temporarily stop a flow log from capturing traffic information about ENIs by disabling the flow log. After you disable the flow log, the flow log is not deleted. You can enable a flow log that is in the **Inactive** state to start to capture traffic information about ENIs again.

1. Log on to the [VPC console](#).
- 2.
- 3.
4. On the **Flow Log** page, find the flow log that you want to disable and click **Disable** in the **Actions** column. After the flow log is disabled, the status of the flow log changes to **Inactive**.

Instance ID/Name	Resource Type	Resource	Status
fl-m5eakol...3qu2rdm t...t	VPC	vpc-m5exn...ms2visuya 0/2 ENI Collecting <a href="#">View</a>	✓ Inactive

## Delete a flow log

You can delete a flow log that is in the **Active** or **Inactive** state. After you delete the flow log, you can still view captured traffic information in the Log Service console.

1. Log on to the [VPC console](#).
- 2.
- 3.
4. On the **Flow Log** page, find the flow log that you want to delete and click **Delete** in the **Actions** column.
5. In the **Delete FlowLog** message, click **OK**.

## Related information

- [CreateFlowLog](#)
- [DescribeFlowLogs](#)
- [ModifyFlowLogAttribute](#)
- [ActiveFlowLog](#)
- [DeactiveFlowLog](#)
- [DeleteFlowLog](#)

## 3.Examples

### 3.1. View the traffic data of an ECS instance in a VPC

This topic describes how to view the traffic data of an Elastic Compute Service (ECS) instance in a virtual private cloud (VPC) by using flow logs.

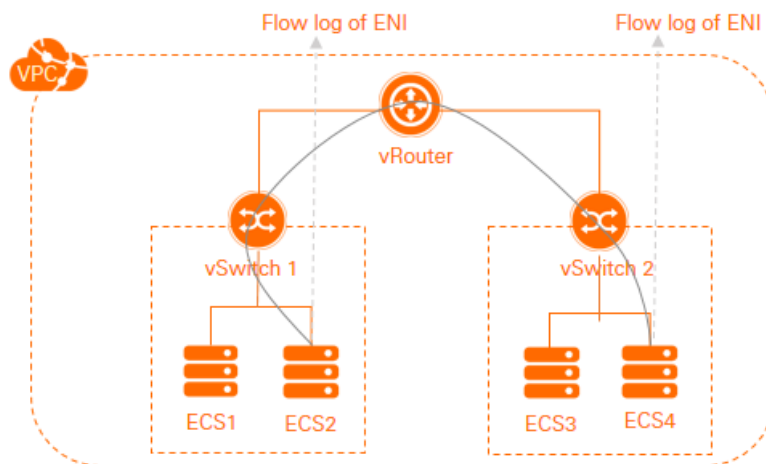
#### Prerequisites

Before you start, make sure that the following requirements are met:

- A VPC is created and two vSwitches are created in the VPC. In this example, the vSwitches are named vSwitch 1 and vSwitch 2. For more information, see [Create an IPv4 VPC](#).
- ECS 1 and ECS 2 are created in vSwitch 1. ECS 3 and ECS 4 are created in vSwitch 2. Applications are deployed on ECS 2 and ECS 4. For more information, see [Create an instance by using the wizard](#).

#### Context

The following scenario is used as an example. ECS 2 and ECS 4 are connected to different vSwitches that belong to the same VPC. Large amounts of data are exchanged between ECS 2 and ECS 4. The IT department wants to view the traffic data in details.



#### Procedure

- 1 2
- Create a flow log View the flow log

#### Step 1: Create a flow log

- 1.
- 2.
3. In the top navigation bar, select the region where you want to create the flow log.



In this example, select the region where the VPC is deployed.

4. On the **Flow Log** page, click **Create FlowLog**.

## Flow Log

Create FlowLog

Instance ID

Instance ID/Name	Resource Type	Resource	Status	Traffic Type
fl-bp1-  -bvgxpd7	ENI	eni-bp1-  -9nmul	✓ Active	All
ECS2_to_ECS4				

5. In the **Create FlowLog** dialog box, set the following parameters and click **OK**:

- o **Name:** Enter a name for the flow log. In this example, `ECS2_to_ECS4` is used.
- o **Resource Type:** Select the type of resource whose traffic data you want to capture, and then select the resource. In this example, **ENI** and the elastic network interface (ENI) of ECS 2 are selected. The flow log captures the traffic data of ECS 2 from its ENI.

If you want to capture the traffic data of ECS 4, specify ENI as the resource type, and then select the ENI of ECS 4.

- **Traffic Type:** Select the type of traffic data that you want to capture. In this example, **All** is selected.
- **Project:** Select the project that is used to store the captured traffic data. In this example, **Create Project** is selected.
- **Logstore:** Select the Logstore that is used to store the captured traffic data. In this example, **Create Logstore** is selected.
- **Turn on FlowLog Analysis Report Function:** In this example, this switch is turned on. After you turn on the switch, Log Service indexing is enabled and a dashboard for the Logstore is created. Then, you can consume the log data by using SQL queries and analyze the log data on the dashboard. Log Service dashboards are free of charge. However, Log Service indexing is billed based on data usage. For more information, see [Log Service billing](#).
- **Description:** Enter a description for the flow log.

Create FlowLog

\* Flow Log Name

ECS2\_to\_ECS412/128

\* Resource Type

ENI

\* Resource Instance

test1-17eni-m5el2whgs

\* Traffic Type

All

\* Project

Select Project

Create Project

Create test1-flow

\* Logstore

Select Logstore

Create Logstore

Create test1-w

☒ Turn on FlowLog Analysis Report Function

1

This function will open the index and establish a dashboard on the log service LogStore to support SQL and visual analysis of data. Fee Tip: Log Service Index is charged by flow, and dashboard is not charged(Billing instruction).

Description



OK

Cancel

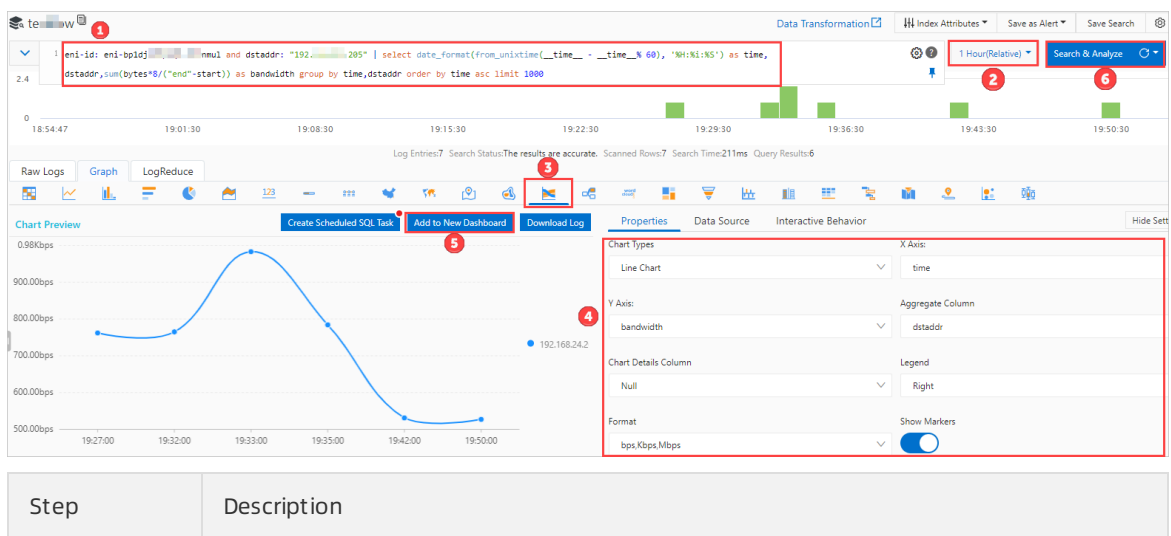
## Step 2: View the flow log


View the traffic data generated when ECS 2 communicates with ECS 4.

1. On the **Flow Log** page, find the flow log and click the name of the LogStore in the **LogStore** column.

Flow Log					
<div> <a href="#">Create FlowLog</a> <div> Instance ID <div>▼</div> <div>Enter an Instance ID to perform exact match</div> <div>Q</div> </div> </div>					
Instance ID/Name	Resource Type	Resource	Status	Traffic Type	LogStore
fl-bp17z-  /bvxpdp7 ECS2_to_ECS4	ENI	eni-bp1-  :09nmul	✓ Active	All	testflow testflow

2. Query the traffic data generated when ECS 2 communicates with ECS 4 by performing the steps in the following figure.



Step	Description
1	<p>Enter the following SQL statement to aggregate and sort the traffic data generated when ECS 2 communicates with ECS 4:</p> <pre>eni-id: eni-bpla69mvjubaw**** and dstaddr: "192.XX.XX.188"   select date_format(from_unixtime(__time__ - __time__% 60), '%H:%i:%S') as time, dstaddr, sum(bytes*8/("end"-start)) as bandwidth group by time, dstaddr order by time asc limit 1000</pre> <p>The SQL statement specifies the following parameters: time, bandwidth (bit/s), and dstaddr (destination address). time and dstaddr are aggregate columns and are sorted in ascending order of time. In this case, 1,000 log entries are retrieved. The following section describes the parameters:</p> <ul style="list-style-type: none"> <li>◦ <code>eni-id</code> : the ENI ID of ECS 2.</li> <li>◦ <code>dstaddr</code> : the private IP address of ECS 4.</li> <li>◦ Set other parameters to the values shown in this example.</li> </ul> <p><b>Note</b> To retrieve traffic data generated when ECS 4 communicates with ECS 2, select ENI and then select ECS 4 when you create the flow log. Then, set <code>eni-id</code> to the ENI ID of ECS 4 and set <code>dstaddr</code> to the private IP address of ECS 2 when you enter the SQL statement, and repeat other steps.</p>
2	Select the time period that you want to query.
3	Click the <b>Graph</b> tab and click  to select a chart type.
4	<p>In the <b>Properties</b> section, set the following parameters:</p> <ul style="list-style-type: none"> <li>◦ <b>Chart Types</b>: <b>Line Chart</b> is selected in this example.</li> <li>◦ <b>X Axis</b>: Set the value to <b>time</b>.</li> <li>◦ <b>Y Axis</b>: Set the value to <b>bandwidth</b>.</li> <li>◦ <b>Aggregate Column</b>: Set the value to <b>dstaddr</b>.</li> <li>◦ <b>Format</b>: Set the value to <b>bps</b>, <b>Kbps</b>, <b>Mbps</b>.</li> </ul> <p>Keep the default settings for other parameters.</p>
5	<p>Click <b>Add to New Dashboard</b> and set the following parameters in the dialog box that appears:</p> <ul style="list-style-type: none"> <li>◦ <b>Operation</b>: <b>Create Dashboard</b> is used in this example.</li> <li>◦ <b>Dashboard Name</b>: Enter a name for the dashboard. In this case, <b>ECS2_to_ECS4</b> is entered.</li> <li>◦ <b>Chart Name</b>: Enter a name for the chart. In this example, <b>Traffic_ECS2_to_ECS4</b> is entered.</li> </ul> <p>You can view information about the flow log on the <b>dashboard</b>.</p>



Step	Description
6	Click <b>Search &amp; Analyze</b> to view the traffic data generated when ECS 2 communicates with ECS 4.

## 3.2. Query traffic between VPCs

Traffic between virtual private clouds (VPCs)

This topic describes how to use flow logs to query traffic between VPCs that are attached to the same Cloud Enterprise Network (CEN) instance in the same region. You can analyze the traffic information to adjust your services or troubleshoot issues.

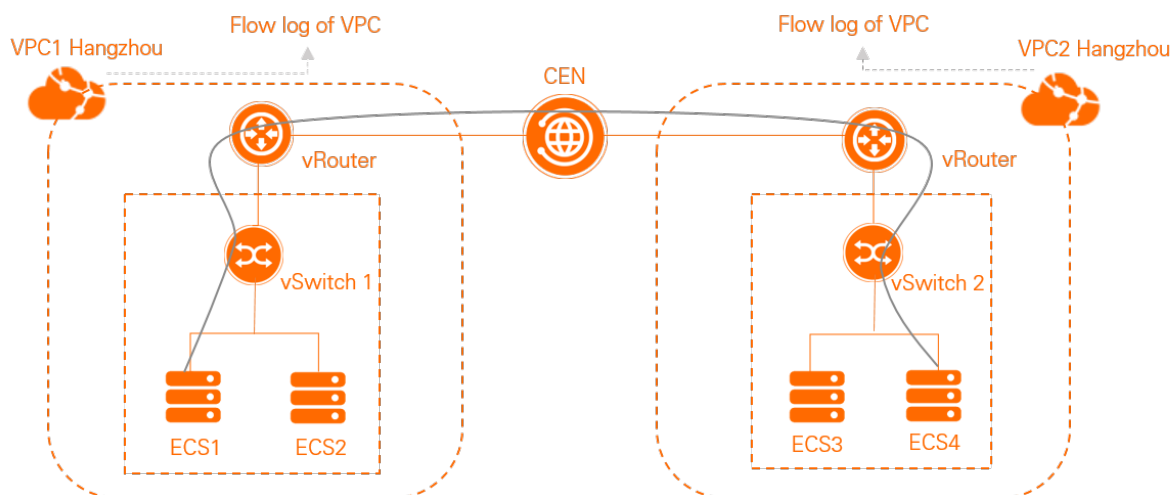
### Prerequisites

- VPC 1 and VPC 2 are deployed in the China (Hangzhou) region. For more information, see [创建和管理专有网络](#).
- Two vSwitches are created in Zone H for VPC 1 and another two vSwitches in Zone I for VPC 2. For more information, see [Work with vSwitches](#).
- ECS instances are created in the four vSwitches and applications are deployed on the ECS instances. For more information, see [Create an instance by using the wizard](#).
- Log Service is activated on the [Log Service product page](#). You are charged for using Log Service. For more information, see [Overview](#).

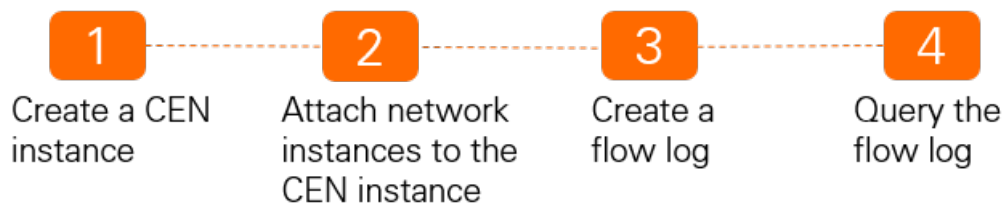
### Scenarios

The following scenario is used as an example. VPC 1 and VPC 2 are created in the China (Hangzhou) region. You want to query traffic between the VPCs. You can use an Enterprise Edition transit router to connect VPC 1 to VPC 2. Then you can query traffic between the VPCs by using flow logs.

This example describes how to view the flow logs generated when VPC 1 accesses VPC 2.



### Procedure



## Step 1: Create a CEN instance

In this example, network instances that belong to the same Alibaba Cloud account and the same region are attached to the same CEN instance. [Step 1: Create a CEN instance](#) and [Step 2: Attach network instances to the same CEN instance](#) are performed in the new CEN console.


- 1.
2. On the **Instances** page, click **Create CEN Instance**.
3. In the **Create CEN Instance** dialog box, set the following parameters and click **OK** to create a CEN instance.
  - i. **Name**: Enter a name for the CEN instance.


The name must be 2 to 128 characters in length and can contain digits, underscores (\_), and hyphens (-). The name must start with a letter.
  - ii. **Description**: Enter a description for the CEN instance.

The description must be 2 to 256 characters in length and cannot start with `http://` or `https://`. You can also leave this parameter empty.

## Step 2: Attach network instances to the same CEN instance

Attach the network instances to be connected to the same CEN instance. After you attach network instances to the same CEN instance, the CEN instance automatically learns routes from the network instances. Then, the network instances can communicate with each other.


- 1.
2. On the **Instances** page, click the ID of the CEN instance that you created in [Step 1: Create a CEN instance](#).
3. On the details page of the CEN instance, click the  icon next to **VPC**.
4. On the **Connection with Peer Network Instance** page, set the following parameters and click **OK**.
  - **Network Type**: Select **VPC**.
  - **Region**: Select the region where the network instances are deployed. In this example, **China (Hangzhou)** is selected.
  - **Transit Router**: The system automatically creates a transit router in the selected region.
  - **Select the primary and secondary zones for the transit router**: Select a primary and secondary zone for the transit router.

 **Note** When you perform this operation, the system automatically creates the service-linked role `AliyunServiceRoleForCEN`. The service-linked role allows the transit router to create elastic network interfaces (ENIs) in the vSwitches of the VPC. ENIs are used to direct network traffic from the VPC to the transit router. For more information, see [AliyunServiceRoleForCEN](#).

- **Resource Owner ID:** Select the Alibaba Cloud account to which the VPC belongs. **Your Account** is selected in this example.
  - **Billing Method:** The default value **Pay-As-You-Go** is used in this example.
  - **Connection Name:** Enter a name for the connection.
  - **Networks:** Select the ID of the VPC to be connected. In this example, VPC 1 is selected.
  - **vSwitch:** Select a vSwitch from the primary zone and secondary zone.
  - **Advanced Settings:** By default, the system automatically enables the advanced features. In this example, the default setting is used for VPC 1.
5. After you attach VPC 1 to the CEN instance, click **Create More Connections**. Then, repeat [Step](#) to attach VPC 2 to the same CEN instance.

### Step 3: Create a flow log

- 1.
2. In the top navigation bar, select the **China (Hangzhou)** region.
- 3.
4. On the **Flow Log** page, click **Create FlowLog**.
5. In the **Create FlowLog** dialog box, set the following parameters and click **OK**.
  - **Flow Log Name:** Enter a name for the flow log. In this example, `VPC_to_each_other` is used.
  - **Resource Type:** Select the type of resource whose traffic you want to capture, and then select the resource. In this example, **VPC** is selected and VPC 2 is selected in the **Resource Instance** drop-down list. In this case, the flow log of VPC 2 is queried.

 **Note** If you want to query the flow log of VPC 1, set **Resource Type** to **VPC** and select VPC 1 from the **Resource Instance** drop-down list. When you enter the SQL statement in [Step 4: Query the flow log](#), set `vpc-xxx` to the ID of VPC 1 and set `srcaddr` to the private CIDR block of VPC 2. Do not change other operations.

- **Traffic Type:** Select the type of traffic data that you want to capture. In this example, **All** is selected.
- **Project:** Select the project that is used to store the captured traffic. In this example, **Create Project** is selected.
- **Logstore:** Select the Logstore that is used to store the captured traffic. In this example, **Create Logstore** is selected.
- **Turn on FlowLog Analysis Report Function:** After you enable this feature, Log Service indexing is enabled and a dashboard is created for the Logstore. Then, you can consume the log data by using SQL queries and analyze the log data in the dashboard. In this example, this feature is enabled.
- **Description:** Enter a description for the flow log.

Step 4: Query the flow log

1.

2.

3. On the **Flow Log** page, find the flow log and click the name of the Logstore in the **LogStore** column.
- fl-m5eb65000mwdf3u8fwh

VPC

vpc-m5e0000gdms2visuya

0/5 ENI Collecting

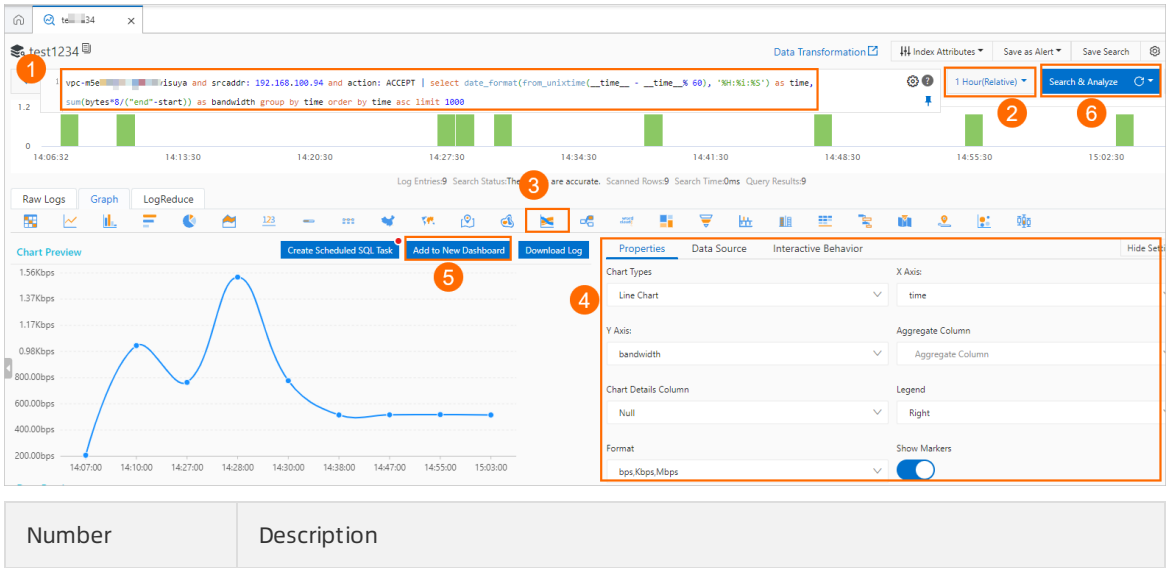
View


Active

All

test1234

pc123
4. Query the traffic generated when VPC 1 accesses VPC 2 based on the procedure described in the following figure.



Number	Description
①	<ul style="list-style-type: none"> <li>Enter the following SQL statement to aggregate and sort the flow log entries and filter the chart that displays the traffic generated when VPC 1 accesses VPC 2.</li> </ul> <pre>vpc-xxx and srcaddr: 172.16.* and action: ACCEPT   select date_format(from_unixtime(__time__ - __time__ % 60), '%H:%i:%S') as time, sum(bytes*8/("end"-start+1)) as bandwidth group by time order by time asc limit 1000</pre> <p>The SQL statement defines the following parameters: time, bandwidth (bit/s), and srcaddr (source address). The parameters are sorted in ascending order of time. In this case, 1,000 log entries are retrieved. The following section describes the parameters:</p> <ul style="list-style-type: none"> <li><code>vpc-xxx</code> : the ID of VPC 2.</li> <li><code>srcaddr</code> : the private CIDR block of VPC 1.</li> <li>Set other parameters to the values shown in this example.</li> </ul> <ul style="list-style-type: none"> <li>Enter the following SQL statement to filter the chart that displays the traffic generated when each ECS instance in VPC 1 accesses VPC 2.</li> </ul> <pre>vpc-xxx and srcaddr: 172.16.* and action: ACCEPT   select date_format(from_unixtime(__time__ - __time__ % 60), '%H:%i:%S') as time, srcaddr,sum(bytes*8/("end"-start+1)) as bandwidth group by time,srcaddr order by time asc limit 1000</pre> <ul style="list-style-type: none"> <li><code>vpc-xxx</code> : the ID of VPC 2.</li> <li><code>srcaddr</code> : the private CIDR block of VPC 1.</li> <li>When the chart is generated, set <b>Aggregate Column</b> to <code>srcaddr</code>.</li> </ul>
②	Select the time period that you want to query.
③	Click the <b>Graph</b> tab and click  to select a chart type.
④	<p>In the <b>Properties</b> section, set the following parameters:</p> <ul style="list-style-type: none"> <li><b>Chart Types</b>: <b>Line Chart</b> is selected in this example.</li> <li><b>X Axis</b>: Set the value to <b>time</b>.</li> <li><b>Y Axis</b>: Set the value to <b>bandwidth</b>.</li> <li><b>Aggregate Column</b>: Leave this parameter empty.</li> <li><b>Format</b>: Set the value to <b>bps, Kbps, Mbps</b>.</li> </ul> <p>Keep the default values for other parameters.</p>

Number	Description
⑤	<p>Click <b>Add to New Dashboard</b> and set the following parameters in the dialog box that appears:</p> <ul style="list-style-type: none"><li>◦ <b>Operation: Create Dashboard</b> is used in this example.</li><li>◦ <b>Dashboard Name:</b> Enter a name for the dashboard. In this example, <b>VPC1_to_VPC2</b> is used.</li><li>◦ <b>Chart Name:</b> Enter a name for the chart. In this example, <b>VPC1_to_VPC2</b> is used.</li></ul> <p>You can view information about the flow log on the <b>dashboard</b>.</p>
⑥	<p>Click <b>Search &amp; Analyze</b> to view the traffic generated when VPC 1 accesses VPC 2.</p>

5. (Optional) To view the chart that displays the traffic generated when VPC 2 accesses VPC 1, you can set **Resource Type** to **VPC** and select VPC 1 from the drop-down list. When you enter the SQL statement, set `vpc-xxx` to the ID of VPC 1 and set `srcaddr` to the private CIDR block of VPC 2. Do not change other operations.