ALIBABA CLOUD

Alibaba Cloud

Virtual Private Cloud

Flow logs

Document Version: 20200902

Alibaba Cloud

Legal disclaimer

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

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

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

Table of Contents

1.Flow log overview

This topic describes the flow log feature of Virtual Private Cloud (VPC) network. You can use flow logs to capture information about inbound and outbound traffic transmitted through Elastic Network Interfaces (ENIs) over your VPC network. Based on the information captured in flow logs, you can verify access control rules, monitor network traffic, and troubleshoot network faults.

> **Note** The flow log feature is available for public preview. You can submit a ticket to apply for public preview.
>
> - The flow log feature is not covered by the terms of service level agreement (SLA) during the public preview.
> - During the public preview period, the flow log feature is applicable in China (Hohhot), China (Shenzhen), Malaysia (Kuala Lumpur), Indonesia (Jakarta), UK (London), and India (Mumbai).

Features

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

The traffic information captured by the flow log feature is written to flow log records in Log Service. Each flow log record includes a five-tuple of a traffic flow captured within the specified capture window. The maximum capture window is approximately 10 minutes. During the capture window, statistics about a traffic flow are captured and aggregated into a flow log record.

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

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 ECS instance to which the ENI is bound.
vpc-id	The ID of the VPC network 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.
dstaddr	The destination IP address.
dstport	The destination port.

Field	Description
protocol	The Internet Assigned Numbers Authority (IANA) protocol number of the traffic flow. For more information, see Internet protocol numbers.
direction	The direction of the traffic flow. Valid values: • in: inbound traffic • out: outbound traffic
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 status of the flow log. Valid values: • OK: The data is recorded. • NODATA: No inbound or outbound traffic is transmitted over the ENI during the capture window. • SKIPDATA: Some flow log records are skipped within the capture window.
action	Actions associated with the traffic flow: • ACCEPT: the traffic that security groups and ACLs allow to record. • REJECT: the traffic that security groups and ACLs forbid to record.

Billing method

You can only analyze flow logs in Log Service. The fee of flow logs includes the fee of log collection and the fee of Log Service.

- Log collection fee

  The log collection fee is charged based on the amount of the collected logs.

  > Note No log collection fee is charged during the public preview.

- The fee of Log Service

  The logs generated by the flow log feature are stored in Log Service. You can view and analyze the logs in Log Service. You are charged for log storage and retrieval when you use Log Service.

Limits

The limits of flow logs are listed in the following table.

Item	Limit	Quota increase supported
The maximum number of flow logs that can be created in a region	10	Submit a ticket.
VPCs that do not support flow logs	VPCs that contain instances of the following instance families: ecs.c1, ecs.c2, ecs.c4, ecs.ce4, ecs.cm4, ecs.d1, ecs.e3, ecs.e4, ecs.ga1, ecs.gn4, ecs.gn5, ecs.i1, ecs.m1, ecs.m2, ecs.mn4, ecs.n1, ecs.n2, ecs.n4, ecs.s1, ecs.s2, ecs.s3, ecs.se1, ecs.sn1, ecs.sn2, ecs.t1, and ecs.xn4.	Upgrade or release an Elastic Compute Service (ECS) instance that does not support advanced network features. • For more information, see 包年包月实例升级配置 and Change the instance type of a pay-as-you-go instance. • For more information, see Release an instance. Note If the VPC network to which a specified VSwitch or ENI belongs contains instances of the specified instance families, and the flow logs feature is enabled, you must upgrade or release the instance for flow logs to work properly. For more information, see Overview of VPC advanced features.
VSwitches that do not support flow logs	VPCs to which VSwitches belong contain instances of the following instance families: ecs.c1, ecs.c2, ecs.c4, ecs.ce4, ecs.cm4, ecs.d1, ecs.e3, ecs.e4, ecs.ga1, ecs.gn4, ecs.gn5, ecs.i1, ecs.m1, ecs.m2, ecs.mn4, ecs.n1, ecs.n2, ecs.n4, ecs.s1, ecs.s2, ecs.s3, ecs.se1, ecs.sn1, ecs.sn2, ecs.t1, and ecs.xn4.	
ENIs that do not support flow logs	The VPC network to which ENIs belong contains instances of the following instance families: ecs.c1, ecs.c2, ecs.c4, ecs.ce4, ecs.cm4, ecs.d1, ecs.e3, ecs.e4, ecs.ga1, ecs.gn4, ecs.gn5, ecs.i1, ecs.m1, ecs.m2, ecs.mn4, ecs.n1, ecs.n2, ecs.n4, ecs.s1, ecs.s2, ecs.s3, ecs.se1, ecs.sn1, ecs.sn2, ecs.t1, and ecs.xn4.	

Procedure

To configure a flow log, follow these steps:

1. Activate Log Service

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

2. Optional. Create an AccessKey pair

   If you want to write data through the 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 set of resources created for 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. Create a resource to capture logs

   Before you create a flow log, you must create a resource for which logs are captured. You can capture logs of a specified ENI, VPC network, or VSwitch. For more information, see Create an ENI, Create a VPC, and Create a VSwitch.

6. Create a flow log

   After you create a flow log, the flow log can capture the traffic data among instances in different regions of the specified Cloud Enterprise Network (CEN). For more information, see Create a flow log.

7. View flow logs

   After you create a flow log, you can view the flow log. You can use the captured traffic data to analyze cross-region data transmission, optimize costs, and troubleshoot network faults. For more information, see View a flow log.

2.Create a flow log

This topic describes how to create a flow log. Flow log is a feature of Virtual Private Cloud (VPC). It is used to capture inbound and outbound network traffic that is transmitted through Elastic Network Interfaces (ENIs). This helps diagnose access control list (ACL) rules, monitor network traffic, and deal with network problems. To use this feature to capture network traffic, you must first create a flow log.

Prerequisites

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

- Log Service is activated. Visit the Log Service product page.
- A project and a Logstore are created to store log data. For more information, see Create a project and Create a Logstore.
- A capture resource is created. For more information, see Create an ENI, Create a VPC, and Create a VSwitch.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Flow Log**.
3. (Optional)If this is first time you use the flow log feature, click **Authorize** and **Confirm**. You must complete the authorization so that flow logs can be imported to Log Service.

   > **Notice** You only need to perform this authorization once during the first time you use the flow log feature with your Alibaba Cloud account.

4. In the top menu bar, specify the region where you want to create the flow log.
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
Name	Specify a name for the flow log. The name must be 2 to 128 characters in length and can contain letters, Chinese characters, digits, hyphens (-), and underscores (_). The name must start with a letter or Chinese character and cannot start with `http://` or `https://`.

Parameter	Description
Resource Type	Select the type of resource for which you want to capture traffic before you select a resource. Supported resource types: ○ **Network Interface**: captures traffic from the specified ENI. ○ **VSwitch**: captures traffic from all ENIs attached to the specified VSwitch. ○ **VPC**: captures traffic from all ENIs in the specified VPC network. If the VPC to which a specified VSwitch or ENI belongs contains Elastic Compute Service (ECS) instances of the following instance families, you cannot create a flow log for the VPC network, VSwitch, or ENI. ecs.c1, ecs.c2, ecs.c4, ecs.ce4, ecs.cm4, ecs.d1, ecs.e3, ecs.e4, ecs.ga1, ecs.gn4, ecs.gn5, ecs.i1, ecs.m1, ecs.m2, ecs.mn4, ecs.n1, ecs.n2, ecs.n4, ecs.s1, ecs.s2, ecs.s3, ecs.se1, ecs.sn1, ecs.sn2, ecs.t1, and ecs.xn4. You must upgrade or release the ECS instances before you can create flow logs. ○ For more information about how to upgrade an ECS instance, see 包年包月实例升级配置 and Change the instance type of a pay-as-you-go instance. ○ For more information about how to release an ECS instance, see Release an instance. Note If the VPC network to which a specified VSwitch or ENI belongs contains ECS instances of the preceding instance families, and flow logs are already created, you must upgrade or release the ECS instance for the flow flogs to work as expected. For more information, see Overview of VPC advanced features.
Traffic type	Select the type of traffic to be captured. Options: ○ **All**: all types of traffic. ○ **Allow**: traffic that is accepted by security group rules of the specified resource. ○ **Drop**: traffic that is denied by security group rules of the specified resource.
Project	Specify a project to store the traffic captured.
Logstore	Specify a Logstore to store the log data captured.
Turn on FlowLog Analysis Report Function	You can 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. Log Service indexing is billed based on data usage but dashboards are free of charge. For more information, see Log Service billing. Note This option is available only when the analysis report feature of the specified Logstore is disabled.

Parameter	Description
Description	Enter a description for the flow log. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://`.

Related information

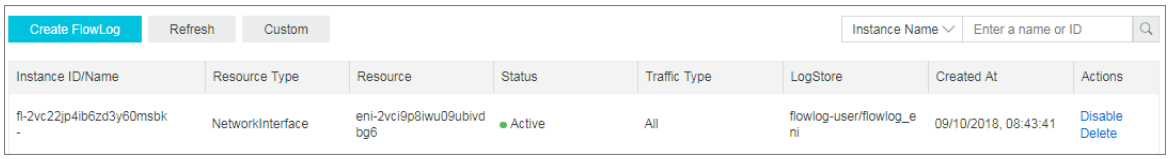
- CreateFlowLog

3.View a flow log

This topic describes how to view a flow log that you have created. By viewing a flow log, you can check access control rules, monitor network traffic, and troubleshoot network faults.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **FlowLog**.
3. Select the region to which the target flow log belongs.
4. On the **FlowLog** page, find the target flow log, and then click the corresponding Logstore link.



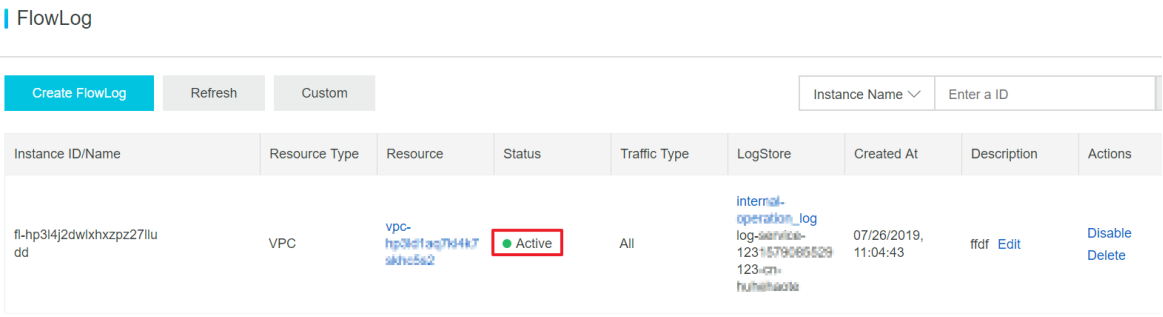
5. In the Log Service console, click **Search & Analytics**.
   After the flow log is displayed, you can view and analyze its data.

4.Enable a flow log

This topic describes how to enable a flow log that is in the **Inactive** state. After you enable a flow log, the flow log will capture the traffic data of the specified ENIs.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **FlowLog**.
3. Select the region to which the target flow log belongs.
4. On the **FlowLog** page, find the target flow log, and then click **Enable** in the **Actions** column. After the flow log is enabled, the status of the flow log changes to **Active**.



5.Disable a flow log

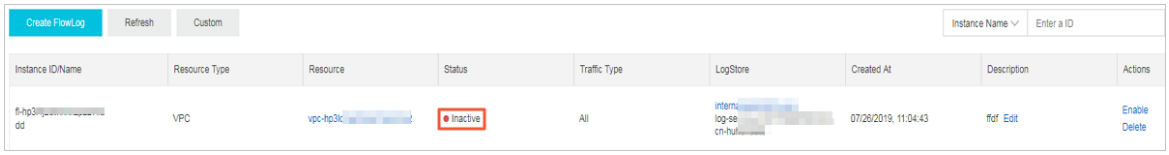
This topic describes how to disable a flow log. You can disable a flow log to stop capturing the traffic information of an Elastic Network Interface (ENI).

Context

After you disable a flow log, it is not deleted. You can enable it whenever necessary.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **FlowLog**.
3. Select the region to which the target flow log belongs.
4. On the **FlowLog** page, find the target flow log, and then click **Disable** in the **Actions** column. After the flow log is disabled, its status changes to **Inactive**.



6.Modify the basic information of a flow log

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

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **FlowLog**.
3. Select the region to which the target flow log belongs.
4. On the **FlowLog** page, find the target flow log, and then click the 
   icon in the **Instance ID/Name** column. The name must be 2 to 128 characters in length and can contain letters, numbers, underscores (_), and hyphens (-). The name must start with a letter.
5. Click **Edit** in the **Description** column to modify the description of the flow log. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://`.

7.Delete a flow log

This topic describes how to delete a flow log. You can delete a flow log that is in the **Active** or **Inactive** state. After you delete a flow log, you can still view the previously captured traffic data in the Log Service console.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **FlowLog**.
3. Select the region to which the target flow log belongs.
4. On the **FlowLog** page, find the target flow log, and then click **Delete** in the **Actions** column.
5. In the **Delete FlowLog** dialog box, click **OK**.