Alibaba Cloud
Virtual Private Cloud

Flow logs

Issue: 20190902

Legal disclaimer

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

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

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

Contents

1 Flow log overview

This topic provides an overview of the flow log function of VPCs. By using this function, you can capture the inbound and outbound traffic over the Elastic Network Interface (ENI) in your VPC. With flow logs, you can check access control rules, monitor network traffic, and troubleshoot network faults.

 Note:
The flow log function is only supported in China (Hohhot), Malaysia (Kuala Lumpur), Indonesia (Jakarta), UK (London), and India (Mumbai).

Features

You can capture the traffic of an ENI, a VPC, or a VSwitch. If you create a flow log for a VPC or VSwitch, you can capture the traffic of all ENIs in the VPC or VSwitch, including the ENIs created after the flow log function is enabled.

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

The traffic data captured by flow logs is written to Log Service as flow log records . Each flow log record includes specified quintuple network streams in a capture window. A capture window is about 10 minutes. During this period, traffic data is aggregated and then released to the flow log record.

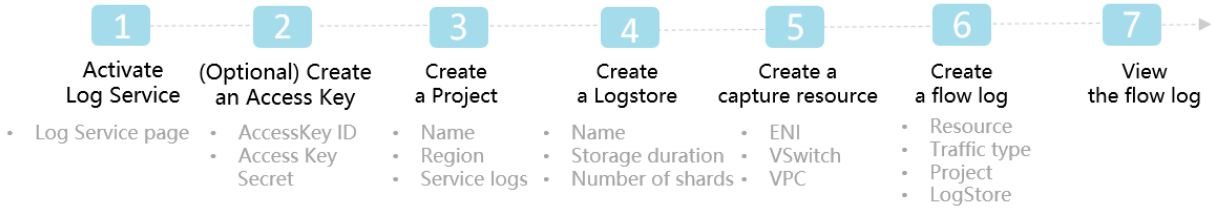
The following table describes the fields of a flow log record.

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 with which the ENI is associated.
vpc-id	The ID of the VPC instance 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 IANA protocol number of the traffic. For more information, see Internet Protocol Numbers.
direction	The direction of the traffic. · in: indicates inbound traffic. · out: indicates outbound traffic.
packets	The number of data packets.
bytes	The data packet size.
start	The start time of the capture window.
end	The end time of the capture window.
log-status	The status of the recorded flow log. · 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 during the capture window.
action	The action associated with the traffic. · ACCEPT: the traffic that security groups allow to record. · REJECT: the traffic that security groups do not allow to record.

Procedure

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



1. Activate Log Service.

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

2. Optional. Create an Access Key.

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

3. Create a Project.

   You must create a Project in Log Service. For more information, see #unique_4/unique_4_Connect_42_section_ahq_ggx_ndb.

4. Create a Logstore.

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

5. Create a capture resource.

   Before you create a flow log, you must create a resource whose logs you want to capture. You can capture logs of a specified ENI, VPC, or VSwitch. For more information, see #unique_6 ,#unique_7 and #unique_8.

6. Create a flow log.

   After you create a flow log, you can capture the traffic data among instances in different regions of the specified CEN. For more information, see #unique_9.

7. View the flow log.

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

Limits

You can create up to 10 flow log instances in each region. To increase the quota, open a ticket.

2 Create a flow log

This topic describes how to create a flow log. After you create a flow log, you can capture the inbound and outbound traffic over the Elastic Network Interface (ENI) in your VPC. With flow logs, you can check access control rules, monitor network traffic, and troubleshoot network faults.

Prerequisites

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

- Log Service is activated. For more information, see Log Service page.
- A Project and a Logstore are created to store traffic data. For more information, see #unique_4/unique_4_Connect_42_section_ahq_ggx_ndb and Create a Logstore.
- A capture resource is created. For more information, see #unique_6, #unique_7, and #unique_8.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click FlowLog.
3. Optional: If it is the first time that you use the flow log function, click Confirm Authorization Policy to authorize VPC to write data to your Logstore.

   Notice:
   The authorization is required only when the primary account uses the flow log function for the first time.
4. Select the region in which you want to create a flow log.
5. On the FlowLog page, click Create FlowLog.

6. On the Create FlowLog page, set the parameters, and then click OK.

Configuration	Description
Name	Enter a name for the flow log. The name must be 2 to 128 characters in length. It can contain letters, numbers, hyphens (-), and underscores (_). It must start with an English letter or a Chinese character, but cannot start with `http://` or `https://`.
Resource Type	Select the type of the resource for which you want to capture traffic, and then select a resource. Options: · `ENI` : Captures traffic for the selected ENI. · `VSwitch` : Captures traffic for all the ENIs in the selected VSwitch. · `VPC` : Captures traffic for all the ENIs in the selected VPC.
Traffic Type	Select the type of the traffic to be captured. Options: · `All` : All traffic of the specified resource is captured. · `Allow` : Only the traffic allowed by the security group rules is captured. · `Drop` : Only the traffic not allowed by the security group rules is captured.
LogStore	Select a Project and a Logstore to store traffic data.

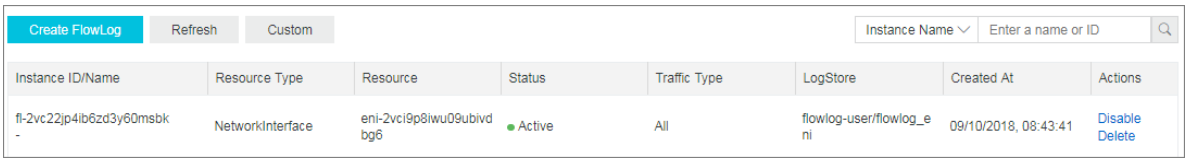
Configuration	Description
Turn on FlowLog Analysis Report Function	If this option is selected, the indexing function is automatically enabled and a dashboard is created for the selected Logstore. You can perform an SQL and visualized analysis of the captured traffic data. The indexing function is charged by traffic. The dashboard is provided free of charge. For more information, see Log Service pricing. Note: This option is displayed only when the report function of the selected Logstore is disabled.
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://`.

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.



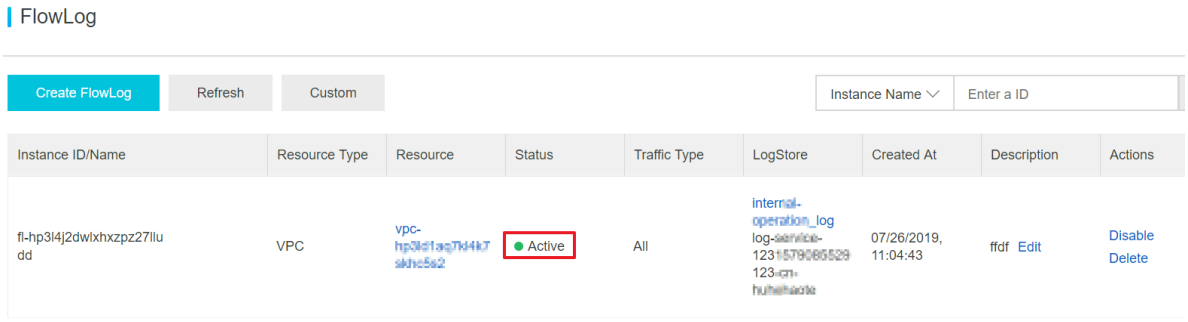
5. In the Log Service console, click Search & Analytics.
   After the flow log is displayed, you can view and analyze its data.

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

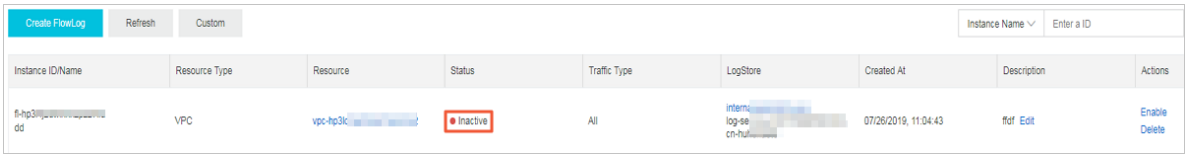
This topic describes how to disable a flow log. You can disable a flow log to stop capturing the traffic information of an Elastic Network Interface (ENI).

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.