Flow Logs

Getting Started

Product Documentation

©2013-2019 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Getting Started

Last updated : 2020-11-12 11:53:16

After a flow log is created for the ENI, you can store and analyze the network traffic in real time, making FL fit for troubleshooting, compliance audit, security and other use cases. This document describes how to create a flow log in the private network.

Prerequisites

- The FL service is currently in beta. If you want to try it out, please submit a ticket.
- Ensure that the CVM is included in the FL's supported list.
- You have created a logset and log topic. For more information on how to add a logset and log topic, please see Logset Actions and Log Topic Actions.

Background

CVM A (10.16.0.22) and CVM B (10.16.0.40) reside in the same VPC. If you log in to the CVM A and run the ping command to connect the CVM B, the CVM A will receive the following response. If a flow log is created for the ENI on the CVM A, the flow log also records the response to the ping operation.

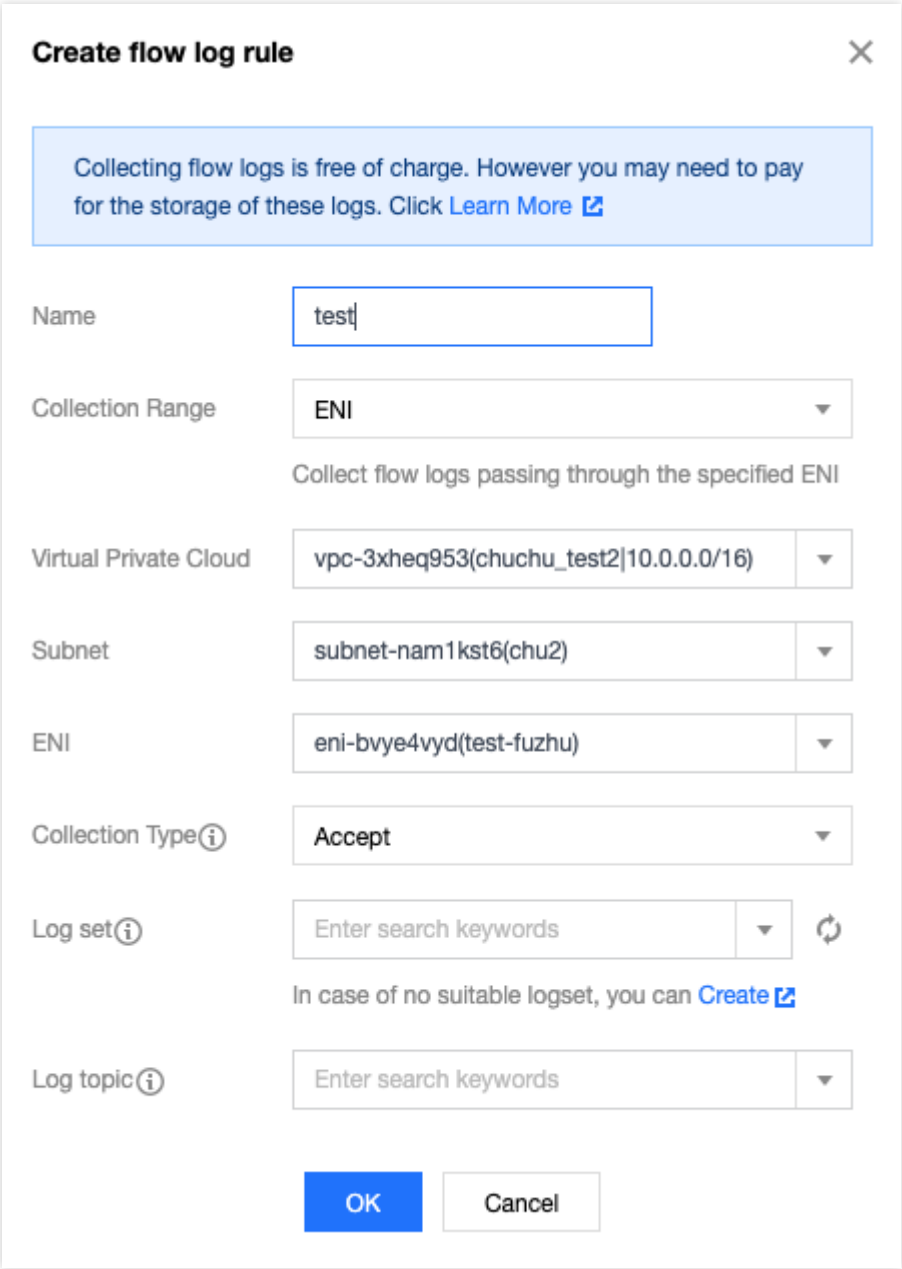
```
[root@VM-0-22-centos ~]# ping 10.16.0.40
PING 10.16.0.40 (10.16.0.40) 56(84) bytes of data.
64 bytes from 10.16.0.40: icmp_seq=1 ttl=64 time=0.490 ms
64 bytes from 10.16.0.40: icmp_seq=2 ttl=64 time=0.449 ms
64 bytes from 10.16.0.40: icmp_seq=3 ttl=64 time=0.437 ms
64 bytes from 10.16.0.40: icmp_seq=4 ttl=64 time=0.429 ms
64 bytes from 10.16.0.40: icmp_seq=5 ttl=64 time=0.471 ms
64 bytes from 10.16.0.40: icmp_seq=6 ttl=64 time=0.665 ms
64 bytes from 10.16.0.40: icmp_seq=7 ttl=64 time=0.682 ms
64 bytes from 10.16.0.40: icmp_seq=8 ttl=64 time=0.451 ms
64 bytes from 10.16.0.40: icmp_seq=9 ttl=64 time=0.415 ms
```

Directions

1. Log in to the VPC console and select **Diagnostic Tools** -> **Flow Log** in the left sidebar.

©2013-2019 Tencent Cloud. All rights reserved.

2. At the top left of the **Flow Log** page, choose the region where you want to create a flow log. Click **+New** and configure the following parameters in the pop-up dialog box.



Field	Description
Name	The name of the flow log to be created
Collection Range	Only **ENI** is supported currently
VPC	VPC where the source CVM resides
Subnet	Subnet where the source CVM resides

©2013-2019 Tencent Cloud. All rights reserved.

Collection Type	Specifies the type of traffic to be collected by the flow log: all traffic, or the traffic rejected or accepted by security groups or ACL.
Logset	Specifies the storage location in CLS for flow logs. Select an existing logset, or click **Create** to add a logset in the CLS console.
Log topic	Specifies the minimum dimension of log storage, which is used to distinguish log types, such as `Accept` log. Select an existing log topic, or go to the CLS console to add a log topic.
Tag key	You can enter or select a tag key for the identification and management of the flow log.
Key value	You can enter or select a key value, or leave it empty.

3. Click **OK**.

> ⚠ **Note :**
>
> - You can view the record of a newly created flow log in CLS after 15 minutes upon the creation (10 minutes for the capture window and 5 minutes for data publishing).
> - FL is free of charge, but the data stored in CLS is charged at standard prices.

Result Validation

After 15 minutes, locate the flow log you've created on the **Flow Log** page and click **Check** to access the **Search Analysis** page. Select a time range and enter the IP of the CVM B in the search bar to search. The result is the same as the response received by the CVM A.

©2013-2019 Tencent Cloud. All rights reserved.