

Alibaba Cloud Cloud Firewall

Logs

Issue: 20190912

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.
<code>Courier font</code>	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Log Audit.....	1
2 Log analysis.....	4
2.1 Overview.....	4
2.2 Log analysis billing method.....	6
2.3 Enable the log analysis service.....	8
2.4 Collect the log.....	9
2.5 Log analysis.....	12
2.6 Fields in the log entry.....	19
2.7 Advanced Settings.....	22
2.8 Export log entries.....	23
2.9 Authorize RAM user accounts with Log Analysis function.....	24
2.10 Manage log storage.....	28

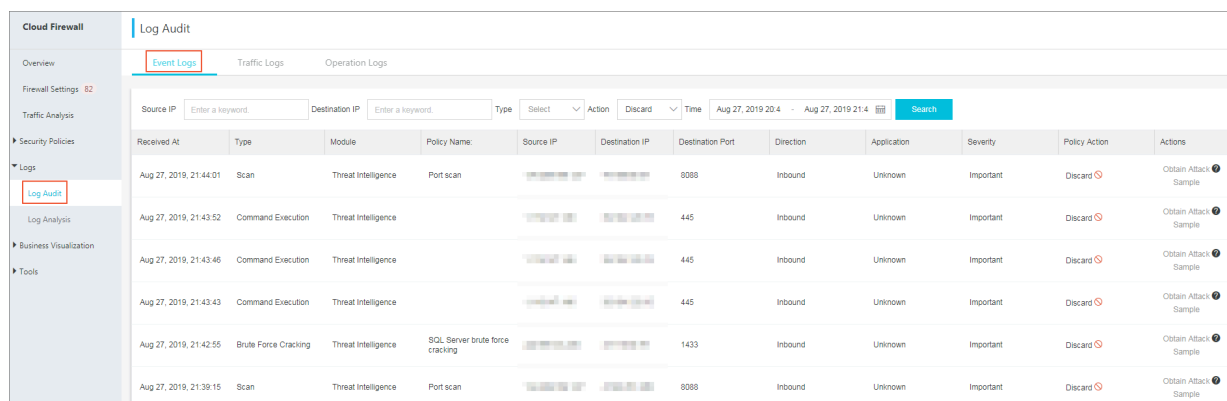
1 Log Audit

All traffic passing through Cloud Firewall is recorded on the Log Audit page. The logs are classified into traffic logs, event logs, and operation logs. You can use the logs to audit your network traffic in real time and take actions accordingly. By default, Cloud Firewall logs are retained for 7 days.

Cloud firewall also provides the Log Analysis function to store log data within six months. If you need classified protection compliance, we recommend that you activate the Log Analysis service. For more information on the cost of log analysis, see [#unique_4](#).

Event logs

The Event logs record the information of each event, including the event detection time, threat type, traffic direction (inbound or outbound), source IP address, destination IP address, application type, severity, and policy action.



Received At	Type	Module	Policy Name	Source IP	Destination IP	Destination Port	Direction	Application	Severity	Policy Action	Actions
Aug 27, 2019, 21:44:01	Scan	Threat Intelligence	Port scan	192.168.1.1	192.168.1.2	8088	Inbound	Unknown	Important	Discard	Obtain Attack Sample
Aug 27, 2019, 21:43:52	Command Execution	Threat Intelligence		192.168.1.1	192.168.1.2	445	Inbound	Unknown	Important	Discard	Obtain Attack Sample
Aug 27, 2019, 21:43:46	Command Execution	Threat Intelligence		192.168.1.1	192.168.1.2	445	Inbound	Unknown	Important	Discard	Obtain Attack Sample
Aug 27, 2019, 21:43:43	Command Execution	Threat Intelligence		192.168.1.1	192.168.1.2	445	Inbound	Unknown	Important	Discard	Obtain Attack Sample
Aug 27, 2019, 21:42:55	Brute Force Cracking	Threat Intelligence	SQL Server brute force cracking	192.168.1.1	192.168.1.2	1433	Inbound	Unknown	Important	Discard	Obtain Attack Sample
Aug 27, 2019, 21:39:15	Scan	Threat Intelligence	Port scan	192.168.1.1	192.168.1.2	8088	Inbound	Unknown	Important	Discard	Obtain Attack Sample

You can specify the source IP address, destination IP address, threat type, action, or other information to search for an event log.

You can also specify a time range to search for relevant event logs.



Note:

The custom time range must be within the previous 7 days.

Traffic logs

The Traffic logs record traffic information including the access start time and end time, direction (inbound or outbound), source IP address, destination IP address,

application type, source port number, application, protocol, policy action, byte count, and packet count.

Cloud Firewall

Overview

Firewall Settings 82

Traffic Analysis

Security Policies

Logs

Log Audit

Log Analysis

Business Visualization

Tools

Log Audit

Event Logs

Traffic Logs

Operation Logs

Internet Firewall

Source IP

Enter a keyword.

Destination IP

Enter a keyword.

Application

Aug 27, 2019 20:4 - Aug 27, 2019 21:4

Search

Show Advanced Search

List Configuration

Time	Source IP	Destination IP	Destination Port	Direction	Application	Protocol	Policy Action	Bytes	Packets	Policy Name	Actions
From :Aug 27, 2019, 21:48:32 To :Aug 27, 2019, 21:48:32			8096	Inbound	Unknown	TCP	Allow	148 B	2		Obtain Attack Sample
From :Aug 27, 2019, 21:48:28 To :Aug 27, 2019, 21:48:28			0	Inbound	Unknown	ICMP	Allow	140 B	2		Obtain Attack Sample
From :Aug 27, 2019, 21:48:28 To :Aug 27, 2019, 21:48:28			7053	Inbound	Unknown	TCP	Allow	148 B	2		Obtain Attack Sample
From :Aug 27, 2019, 21:48:25 To :Aug 27, 2019, 21:48:25			62461	Inbound	Unknown	TCP	Allow	148 B	2		Obtain Attack Sample
From :Aug 27, 2019, 21:48:25 To :Aug 27, 2019, 21:48:25			23	Inbound	Unknown	TCP	Allow	148 B	2		Obtain Attack Sample

You can specify the source IP address, destination IP address, application, or other information to search for a traffic log.

You can also specify a time range to search for relevant traffic logs.



Note:

The custom time range must be within the previous 7 days.

To search for traffic logs more precisely, you can click **Show Advanced Search** next to the search bar and specify advanced conditions such as **Direction**, **Policy Source**, **Port**, and **Region**.

Cloud Firewall

Overview

Firewall Settings 82

Traffic Analysis

Security Policies

Logs

Log Audit

Log Analysis

Business Visualization

Tools

Log Audit

Event Logs

Traffic Logs

Operation Logs

Internet Firewall

Source IP

Enter a keyword

Destination IP

Enter a keyword

Application

Traffic Type

All Traffic Types

Direction

All

Policy Action

Discard

IP Protocol

All

Policy Source

All

Port

Enter a keyword

Location

Region

China (Qingdao)

ISP

Domain Name

abc.com

Source Private IP

Enter a keyword

Aug 27, 2019 20:4

Aug 27, 2019 21:4

Search

Time	Source IP	Destination IP	Destination Port	Direction	Application	Protocol	Policy Action	Bytes	Packets	Policy Name	Actions
From :Aug 27, 2019, 21:48:32 To :Aug 27, 2019, 21:48:32			8096	Inbound	Unknown	TCP	Allow	148 B	2		Obtain Attack Sample
From :Aug 27, 2019, 21:48:28 To :Aug 27, 2019, 21:48:28			0	Inbound	Unknown	ICMP	Allow	140 B	2		Obtain Attack Sample
From :Aug 27, 2019, 21:48:28 To :Aug 27, 2019, 21:48:28			7053	Inbound	Unknown	TCP	Allow	148 B	2		Obtain Attack Sample

Hide Advanced Search

List Configuration

For the traffic that matches an access control policy or IPS policy, the name of the matching policy is displayed in the Policy Name column of the traffic log. For the traffic that does not match any policy, the Policy Name column is empty.

Operation logs

The Operation logs record the time, type, severity, and details about each operation in Cloud Firewall.

Cloud Firewall

Overview

Firewall Settings 82

Traffic Analysis

Security Policies

Logs

Log Audit

Log Analysis

Business Visualization

Tools

Log Audit

Event Logs

Traffic Logs

Operation Logs

Severity

Please select ▾

Aug 12, 2019 20:52 - Aug 16, 2019 21:52

Search

Time	Type	Severity	Account	Description
Aug 16, 2019, 17:34:10	Operation Logs	Low	Alibaba Cloud Account : beaver-test	Successfully completed the operation.
Aug 16, 2019, 17:34:05	Operation Logs	Low	Alibaba Cloud Account : beaver-test	Successfully completed the operation.
Aug 16, 2019, 10:52:49	Operation Logs	Low	Alibaba Cloud Account : beaver-test	Successfully completed the operation.
Aug 16, 2019, 10:52:26	Operation Logs	Low	Alibaba Cloud Account : beaver-test	Successfully completed the operation.
Aug 16, 2019, 10:48:53	Operation Logs	Low	Alibaba Cloud Account : beaver-test	Successfully completed the operation.
Aug 16, 2019, 10:41:11	Operation Logs	Low	Alibaba Cloud Account : beaver-test	Successfully completed the operation.
Aug 16, 2019, 10:40:32	Operation Logs	Low	Alibaba Cloud Account : beaver-test	Successfully completed the operation.
Aug 16, 2019, 10:39:45	Operation Logs	Low	Alibaba Cloud Account : beaver-test	Successfully completed the operation.
Aug 16, 2019, 10:39:33	Operation Logs	Low	Alibaba Cloud Account : beaver-test	Successfully completed the operation.
Aug 16, 2019, 10:38:42	Operation Logs	Low	Alibaba Cloud Account : beaver-test	Successfully completed the operation.

Prev

1

2

3

4

...

20

Next >

1/20

Go To Page

Go

You can select a value from the Severity drop-down list on the Operation Logs tab page to search for the operation logs of the specified severity

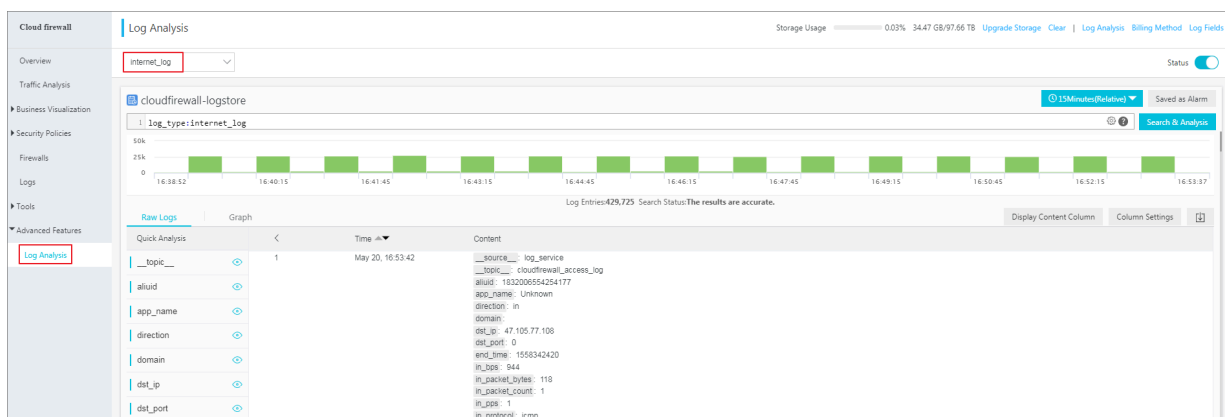
You can also specify a time range to search for relevant operation logs. The custom time range must be within the previous 7 days.

2 Log analysis

2.1 Overview

The Log Analysis service of Cloud Firewall provides internet traffic logs and real-time log analysis.

The Log Analysis service of Cloud Firewall can automatically collect and store real-time log of both inbound and outbound traffic. It outputs query analysis, reports, alarms, and downstream computing interconnection and provide you with detailed analysis result.



Benefits

The Log Analysis service of Cloud Firewall has the following benefits:

- **Classified Protection compliance:** Log Analysis provides log storage duration of six months to help your website meet the requirements of classified protection compliance.
- **Easy configuration:** Easy configuration allows you to collect Internet traffic logs in real time.
- **Real-time analysis:** Integrated with the Simple Log Service (SLS), the Log Analysis service provides the real-time log analysis service and report center. With the help of log analysis, you can view all the traffic and user's visits going through Cloud Firewall.
- **Real-time alarms:** Log Analysis supports you to customize real-time monitoring and alerts based on specific indicators. This ensures you receive real-time alerts when there is any threats detected in the critical business.

Prerequisites

Before you begin to use the service of Log Analysis, the following prerequisite must be available:

- You have purchased and activated the Log Analysis service of Cloud Firewall (Log Analysis is available in Pro, Enterprise, and Flagship editions). For details, refer to [#unique_7](#).

Restrictions

The logstore of Cloud Firewall is an exclusive logstore with the following restrictions:

- You cannot write data into logstore with APIs or SDKs, or modify the attributes of the logstore (such as the storage cycle).



Note:

Other general logstore features (such as query, statistics, alarms, and stream consumption) are supported, and there is no difference with the general logstore.

- Alibaba Cloud's Log Service (SLS) does not charge for the exclusive logstore of Cloud Firewall, but SLS itself must be available (not overdue).
- Built-in reports provided by Log Analysis of Cloud Firewall may be updated and upgraded automatically.

Scenarios

- Track Internet traffic logs to trace security threats.
- Allow you to view Internet request activities in real time, and check the security status and trend of your assets.
- Provide you with quick understanding of security operation efficiency and handling the risks in a timely manner.
- Output logs to your self-built data and computing centers.

2.2 Log analysis billing method

Cloud Firewall Log Analysis service charges fees based on the selected log storage duration and log storage capacity. Log Analysis is charged by monthly and annual subscription.

Enable Activate Log Service and select the log storage period and the log storage size. Then, the price is automatically calculated based on the log store specification of your choice.

Log storage specification

Different log storage specifications of Cloud Firewall are charged as follows:

Log storage duration	Log storage size	Applicable bandwidth	Recommended version	Monthly subscription fee	Annual subscription fee
180 days	1TB	Applicable to business scenarios with monthly bandwidth not higher than 10 Mbps	Pro Edition	To be released.	To be released.
	5TB	Applicable to business scenarios with monthly bandwidth not higher than 50 Mbps	Enterprise Edition	To be released.	To be released.
	20TB	Applicable to business scenarios with monthly bandwidth not higher than Mbps	Flagship Edition	To be released.	To be released.

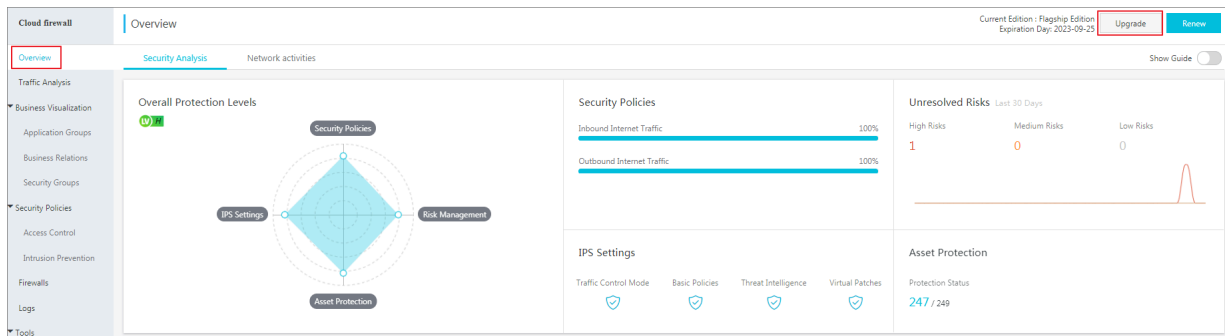


Note:

To increase the bandwidth, we recommend that you expand with 1TB log storage for every 10 Mbps increase.

Upgrade storage capacity

If you have no log storage left, a notification appears to remind you to expand the storage size. You can click Upgrade on the console to expand the storage size.



Notice:

If you fail to upgrade the log storage capacity when the storage capacity is full, Cloud Firewall will stop writing new log data to the exclusive logstore of log analysis service, the stored log data in the logstore is retained. Log data is deleted automatically if it is stored for more than 180 days or is not renewed after the Log Analysis service expires for 7 days. Once the log data is deleted, it cannot be recovered.

Duration

The purchase duration of Cloud Firewall log service is bound to the subscription instance of the Cloud Firewall you purchased.

- **Buy:** When you buy a Cloud Firewall subscription and enable Log Analysis, the price of Log Service is calculated based on the validity of the subscription.
- **Upgrade:** When you enable Log Service by upgrading an existing Cloud Firewall subscription, the price of Log Service is calculated based on the log storage size.

Service expiration

If the purchased Cloud Firewall instance is about to expire, Log Analysis service will also expire.

- When the service expires, Cloud Firewall stops writing log entries to the exclusive logstore in Log Service.

- The log entries recorded by Cloud Firewall Log Analysis are retained within seven days after the service expires. If you renew the service within seven days after the service expires, you can continue to use Log Analysis service. Otherwise, all stored log entries are deleted.

2.3 Enable the log analysis service

After you activate Cloud Firewall, you can enable the Log Analysis service in the Cloud Firewall console. Log Analysis provides you with the real-time log search and analysis features.

Features

After the Log Analysis service is activated, real-time logs of the internet traffic through Cloud Firewall can be collected automatically. You can also perform real-time log search and analysis with Log Analysis service, and check the results in log dashboards. You need to set the storage duration and storage capacity when you enable the Cloud Firewall log analysis service.

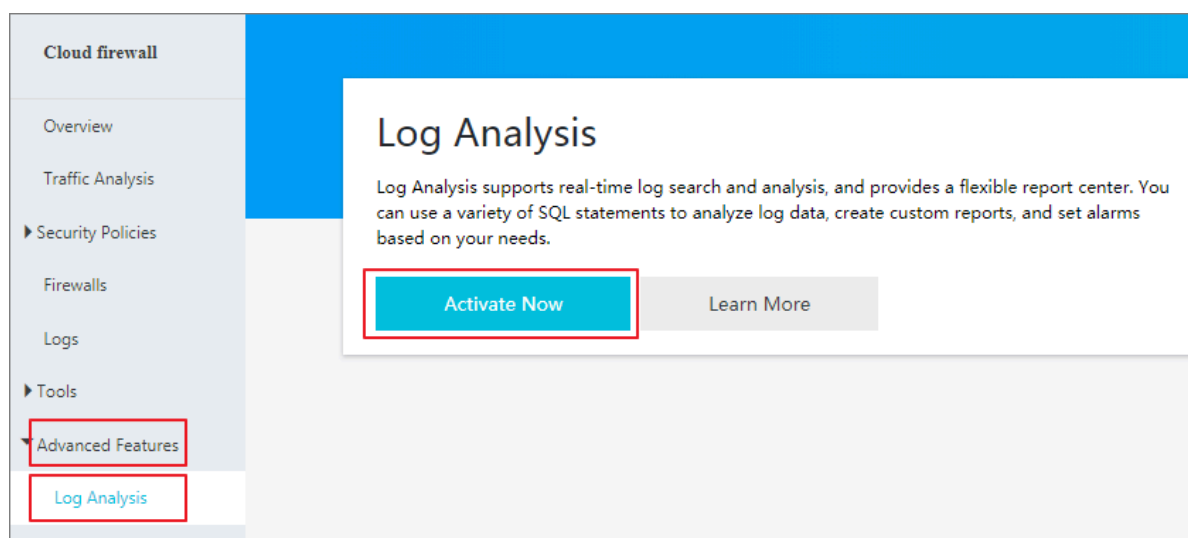


Note:

The log analysis service is available in the Cloud Firewall Pro, Enterprise, and Flagship editions.

Enable the Log Analysis service of Cloud Firewall

1. Log on to the [Cloud Firewall console](#).
2. In the left-side navigation pane, select Advanced Features > Log Analysis.
3. Click Activate Now on the Log Analysis page.



4. Select your log storage capacity, and then click Pay to complete the payment.

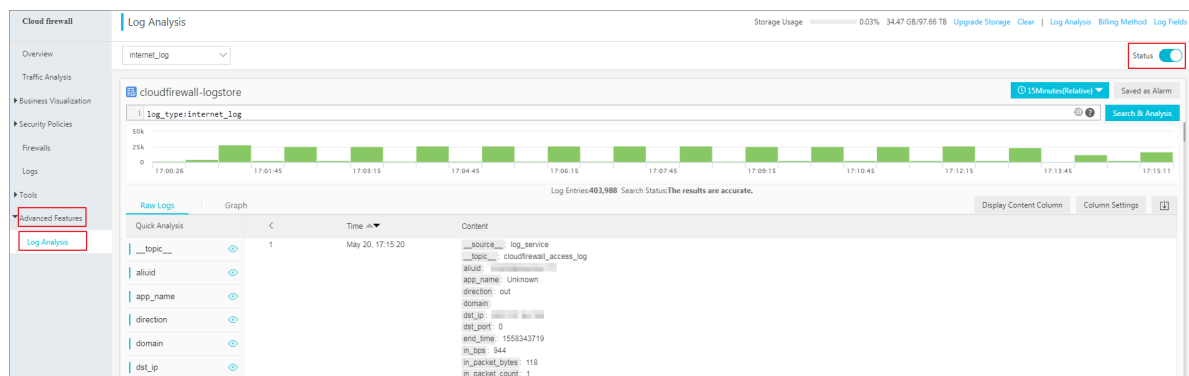


Note:

For more information about log analysis pricing, refer to [#unique_4](#).

5. Go back to Log Analysis page in Cloud Firewall console.

6. Click the Status switch on the right side to enable the Log Analysis service.



Log Analysis service retrieves records of both inbound and outbound Internet traffic flowing through Cloud Firewall. You can use the retrieved records to detect threats in real time.

2.4 Collect the log

You can enable the log collector function for Cloud Firewall in the Cloud Firewall console.

Prerequisites

- You have activated Cloud Firewall.
- You have activated Alibaba Cloud Log Service.

Context

The log collector function retrieves log data of inbound and outbound Internet traffic for Alibaba Cloud Firewall in real time. The retrieved log data can be searched and analyzed in real time, and the returned results are displayed in dashboards. Based on the log data, you can analyze visits to and attacks on your websites and help the security engineers develop protection strategies.

After you enable the Cloud Firewall log analysis function, the log analysis function automatically creates a dedicated Logstore named `cloudfirewall-logstore` under your account. Cloud Firewall automatically imports log entries to this dedicated Logstore

in real time. For more information about the default configuration of the dedicated Logstore, see [Default configuration](#).

Procedure

1. In the left-side navigation pane, locate Log Analysis.
2. Click the Status switch on the right side to enable the log collector function.

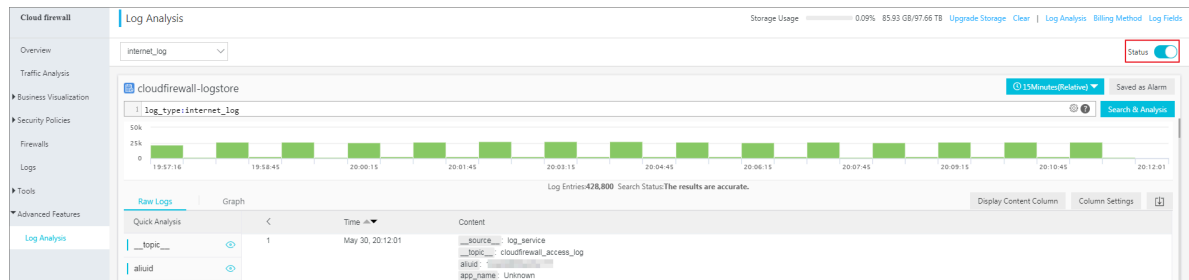


Table 2-1: Default log analysis configuration

Default configuration item	Description
Project	<p>The log analysis project created by Cloud Firewall. The project name is determined according to the region of your Cloud Firewall instance.</p> <ul style="list-style-type: none"> • If the Cloud Firewall instance is deployed in a Mainland China region, the project name is: <code>cloudfirewall-project-Alibaba Cloud account ID-cn-hangzhou</code>. • If the Cloud Firewall instance is deployed in the Finance Cloud (Hangzhou) region, the project name is: <code>cloudfirewall-project-Alibaba Cloud account ID-cn-hangzhou-finance</code>. • If the Cloud Firewall instance is deployed in other regions, the project name is: <code>cloudfirewall-project-Alibaba Cloud account ID-ap-southeast-1</code>.
Logstore	<p>The default Logstore is <code>cloudfirewall-logstore</code>.</p> <p>All log data retrieved by Cloud Firewall is stored in this Logstore.</p>

Default configuration item	Description
Region	<ul style="list-style-type: none">· If the Cloud Firewall instance is deployed in a Mainland China region, the project is saved in the China (Hangzhou) region by default.· If the Cloud Firewall instance is deployed in other regions, the project is saved in the Singapore region by default.
Shard	By default, two shards are created and the Automatic shard splitting function is enabled.
Dashboards	A dashboard is created by default.

**Note:**

The default log analysis configuration items cannot be modified.

Restrictions and guidelines

- After you enable the Log Analysis function, the system automatically creates a Logstore named cloudfirewall-logstore in the Log Service console. The Logstore is dedicated to Cloud Firewall and stores all log entries of Cloud Firewall. Do not delete this Logstore.
- Other data cannot be written into the dedicated Logstore.

Log entries generated by Cloud Firewall are stored in the dedicated Logstore. You cannot write other data into this Logstore by using the API, SDK, or other methods.

**Note:**

The dedicated Logstore has no restrictions in search, statistics, alerts, streaming consumption, and other functions.

- Basic configurations, such as the log storage period, cannot be modified.
- The dedicated Logstore is not billed.

To use the dedicated Logstore, you must activate Log Service for your account.

**Note:**

When your Log Service is overdue, the Cloud Firewall log collector function is suspended until you pay the bills.

- Do not delete or modify the configurations of the default project, Logstore, index, and dashboards created by Log Service. Log Service will update the Cloud Firewall log analysis function. The index of the dedicated Logstore and the default report are also updated.
- If you want to use the Cloud Firewall log analysis function with a RAM user account, you must grant the required Log Service permissions to the RAM user account. For more information, see [#unique_13](#).

2.5 Log analysis

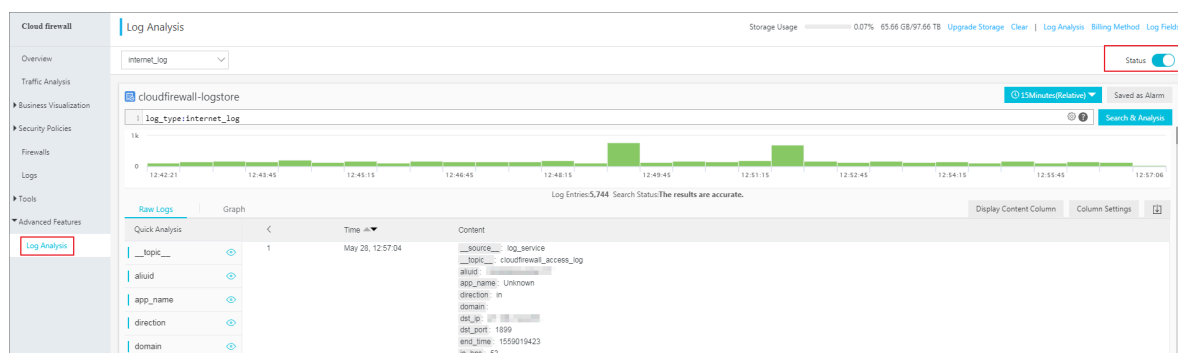
Cloud Firewall console supports the Log Analysis function.

Overview

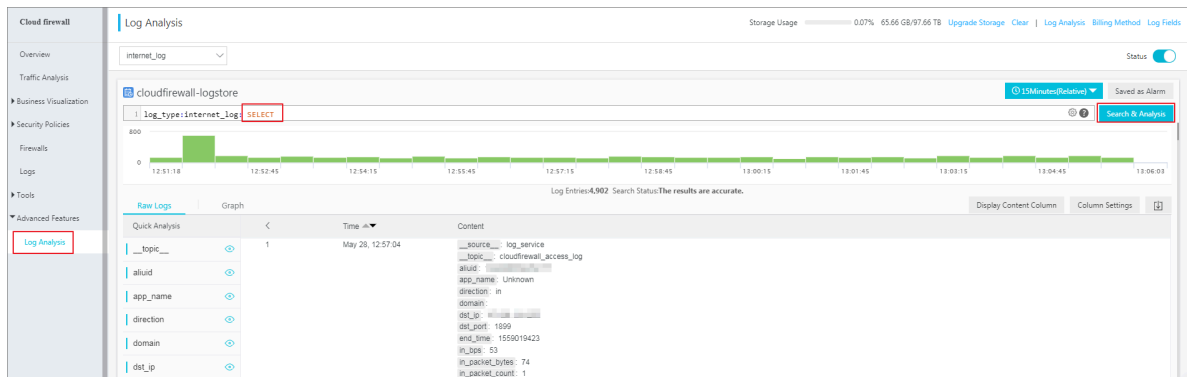
After you enable the Log Analysis function in Cloud Firewall console, you can perform real-time log search and analysis, view or edit dashboards, and set up monitoring and alerts on the Log Analysis page.

Procedure

1. Log on to the [Cloud Firewall console](#).
2. In the left-side navigation pane, select Logs > Log Analysis.
3. Click the Status switch on the right side to enable the Log Analysis function.



4. Enter a search and analysis statement, select a time range, and click Search & Analysis.



More actions

On the Log Analysis page, you can perform the following actions to handle the returned search results:

- Customize search and analysis

The log analysis function provides the search and analysis statements for you to search and analyze log entries in different scenarios. For more information, see [Customize search and analysis](#).

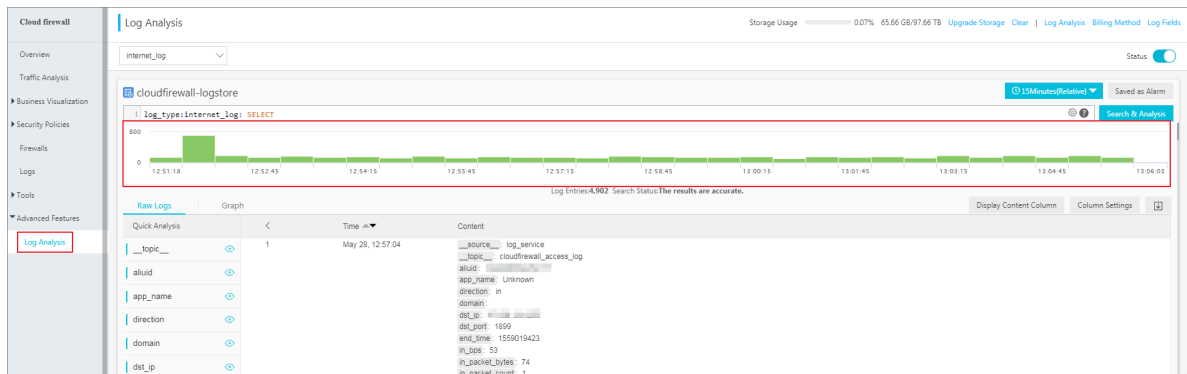
- View the distribution of log entries by time

The histogram under the search box shows the distribution of log entries that are filtered by time and search statement. The horizontal axis indicates the time period, and the vertical axis indicates the number of log entries. The total number of the log entries returned is also displayed.



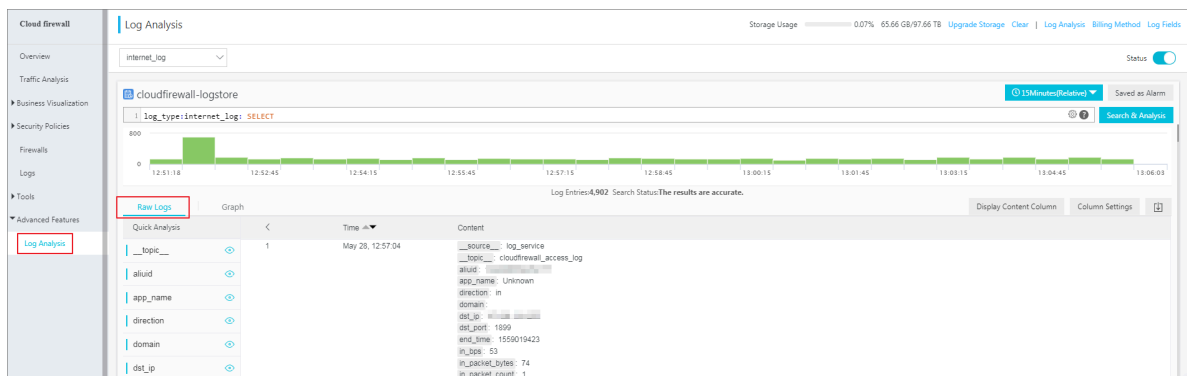
Note:

You can drag the mouse pointer in the histogram to narrow down the time period. The **time picker** automatically updates the time period, and the search results are also updated accordingly.



- View raw logs

On the Raw Logs tab page, each log entry is detailed on an individual page, which includes the time when the log is generated, the content, and the columns in the log entry. You can click **Display Content Column** to set the display mode for the long strings in the content column. The display modes include Full Line and New Line. You can click **Column Settings** to customize the columns to be displayed, or click the **Download** icon to download the search results.



Additionally, you can click a value or a property name in the content column to add a search condition to the search box. For example, if you click **log_servic e**

in the `__source__ : log_service` field, the following search statement is added to the search box:

```
" Former Search Statement " and source : log_service
```

- View analysis graphs

The log analysis function enables you to show the analysis results in graphs. You can select the graph type as needed on the Graph tab page. For more information, see [Analysis graphs](#).

- Quick analysis

The quick analysis function on the Raw Logs tab provides you with a quick interactive search function. You can view the distribution of a property within a specific time period. This function can reduce the time used for indexing key data. For more information, see [Quick analysis](#).

Customize search and analysis

The log analysis function provides the search and analysis statements. Separate the search and analysis statements with a vertical bar (|):

```
$ Search | $ Analytics
```

Type	Description
Search	A keyword, a fuzzy string, a numerical value, or a range can be used as a search condition. You can also combine these search conditions. If the statement is empty or only contains a wildcard character (*), all log entries are searched.
Analytics	Performs calculation and statistics to the search results or all log entries.



Note:

Both the search and the analysis statements are optional.

- When the search statement is empty, all log entries within the specified time period are displayed. Then, the search results are used for statistics.

- When the analysis statement is empty, the search results are returned. No statistical analysis is performed.

Search statements

The search statements of Log Service support full text search and field search. You can set the New Line mode, syntax highlighting, and other functions in the search box.

- Full text search

You can enter keywords without specifying fields to perform the search. You can enter a keyword enclosed in quotation marks (") to query log entries that contain the entire keyword. You can also use spaces or `and` to separate multiple keywords.

Examples

- Search by keyword

The following statements can be used to search for log entries that contain `www`

```
. aliyun . com and error .
```

```
www . aliyun . com error or www . aliyun . com and error .
```

- Search by condition

The following statement can be used to search for log entries that contain `www`

```
. aliyun . com , error , or 404 .
```

```
www . aliyun . com and ( error or 404 )
```

- Search by prefix

The following statement can be used to search for log entries that contain `www`

```
. aliyun . com and start with failed_ .
```

```
www . aliyun . com and failed_ *
```



Note:

The wildcard character (*) can only be added as a suffix. The wildcard character (*) cannot be added as a prefix. For example, the statement cannot be `* _error .`

- Search by field

To narrow down the search results, you can search by field.

You can specify numeric fields. The format is `field name : value or field name >= value` . Moreover, you can use both the `and` and `or` operators in full text search.



Note:

The Cloud Firewall log analysis function supports searching by field. For more information about the definition, type, format, and other information of each field, see [Cloud Firewall log field descriptions](#).

Examples

- Search by specifying multiple fields

If you want to search for log entries about client `1 . 2 . 3 . 4` accessing IP address `1 . 1 . 1 . 1` , set the following search conditions:

```
src_ip : 1 . 2 . 3 . 4 and dst_ip : 1 . 1 . 1 . 1
```



Note:

In this example, the `src_ip` field and `dst_ip` field are log fields created by Cloud Firewall.

- Search by specifying numeric fields

The following statement can be used to search log entries where the response time exceeds five seconds.

```
request_time_msec > 5000
```

Searching by time period is also supported. For example, you can search for log entries where the response time exceeds five seconds and is no greater than ten seconds.

```
request_time_msec in ( 5000 10000 ]
```



Note:

You can get the same result by using the following search statement:

```
request_ti me_msec > 5000 and request_ti me_msec <= 10000
```

- Field search

You can search whether a field exists as follows:

- Search for log entries that include the `total_pps` field.

```
total_pps :*
```

- Search for log entries that include the `ua_browser` field.

```
not total_pps :*
```

For more information about the search statements supported by Log Service, see [Indexes and search](#).

Analysis statements

You can use the SQL/92 statements for log analysis and statistics.

For more information about the statements and functions supported by Log Service, see [Real-time analysis](#).



Note:

- The `from table name part` (the `from log part`) in the standard SQL statements can be omitted.
- The first 100 log entries are returned by default. You can modify the number of the returned log entries by using the [LIMIT statement](#).

Examples of search and analysis

Time-based log search and analysis

Each Cloud Firewall log entry has a `time` field, which is used to indicate the time.

The format of field is `year - month - dayThour : minute : second + time`

`zone`. For example, in `2018 - 05 - 31T20 : 11 : 58 + 08 : 00`, the time zone is `UTC + 8`.

Meanwhile, each log has a built-in field `__time__`. This field also indicates the time when the log entry is generated. The field is used for calculation during the time-based statistics process. The format of this field is `Unix timestamp`, and the

value of this field indicates the amount of seconds that have elapsed since 00:00:00 Coordinated Universal Time (UTC), January 1, 1970. Therefore, if you want to display a calculated result, you must convert the format first.

- Select and display the time
- Calculate the time
- Statistical analysis by group based on a specific time



Note:

You can also display the results with a line graph.

The `date_parse` and `date_format` functions are used to convert the time format. For more information about the functions that can be used to parse the time field, see [Date and time functions](#).

2.6 Fields in the log entry

Cloud firewall records the inbound and outbound traffic logs, including multiple log fields. You can perform query and analysis based on specific fields.

Field Name	Description	Example	Comments
<code>__time__</code>	Time of the operation in Cloud Firewall	2018-02-27 11:58:15	-
<code>__topic__</code>	Log topic	cloudfirewall_access_log	Log topic is unique, which is cloudfirewall for Cloud Firewall.
<code>Log_type</code>	Log types	Internet_log	Internet_log refers to the Internet Traffic Log.
<code>aliuid</code>	User's Alibaba Cloud UID	12333333333333	-

Field Name	Description	Example	Comments
app_name	Protocol of the access traffic	HTTPS	Possible values include HTTPS , NTP, SIP, SMB , NFS, and DNS. Unknown values are Unknown.
direction	Traffic direction	in	<ul style="list-style-type: none"> · in: traffic goes to the ENI · out: traffic goes from the ENI
domain	Domain name	www.aliyun.com	-
dst_ip	Destination IP	1.1.1.1	-
dst_port	Destination port	443	-
end_time	Session end time	1555399260	Unit: Seconds (Unix timestamp)
In_bps	Bps of inbound traffic	11428	Unit: bps
In_packet_bytes	Total number of bytes of inbound traffic	2857	-
In_packet_count	Total number of packet of inbound traffic	18	-
In_pps	Pps of inbound traffic	9	Unit: pps
Ip_protocol	IP protocol type	TCP	Protocol name . TCP and UDP protocol are supported.
Out_bps	Bps of outbound traffic	27488	Unit: bps
Out_packet_bytes	Total number of bytes of outbound traffic	6872	-
Out_packet_count	Total number of packet of outbound traffic	15	-
Out_pps	Pps of outbound traffic	7	Unit: pps
region_id	Region to which the access traffic belongs	cn-beijing	-

Field Name	Description	Example	Comments
Rule_result	Result of matching with the rules	pass23	<p>The result of matching with the rules. The values are:</p> <ul style="list-style-type: none"> · Pass: The traffic is allowed to pass through Cloud Firewall. · Alert: Cloud Firewall detects threats in the traffic. · Discard: The traffic is not allowed to pass through Cloud Firewall.
src_ip	Source IP	1.1.1.1	-
src_port	The port of the host from which traffic data is sent	47915	-
start_time	Session start time	1555399258	Unit: Seconds (Unix timestamp)
Start_time_min	Session start time, which is an integer in minutes	1555406460	Unit: Seconds (Unix timestamp)
Tcp_seq	TCP serial number	3883676672	-
Total_bps	Total bps of both inbound and outbound traffic	38916	Unit: bps
Total_packet_bytes	Total number of bytes of both inbound and outbound traffic	9729	Unit: byte

Field Name	Description	Example	Comments
Total_packet_count	Total number of packets of both inbound and outbound traffic	33	-
Total_pps	Total number of pps of both inbound and outbound traffic	16	Unit: pps
Src_private_ip	Private IP of the source host	1.1.1.1	
Vul_level	Vulnerability Risk level	High	Vulnerability Risk level: <ul style="list-style-type: none">· 1: Low· 2: Moderate· 3: High

2.7 Advanced Settings

Log Analysis of Cloud Firewall provides you with Advanced Settings. You can set advanced features for Log Service with Advanced Settings. For example, you can set alarms and notifications, real-time log collection and consumption, shipping log data, or provide visual representations with other products.

Steps


1. Log on to [Cloud firewall console](#).
2. Go to the left-side navigation pane **Advanced Functions > Log Analysis**.
3. Click **Advanced Settings** in the upper-right corner.
4. In the dialog box that appears, click **Go** to open the Log Service console.
5. In the Log Service console, you can set the following advanced features for log projects and logstores:
 - [Alarms and notifications](#)
 - [Real-time log collection and consumption](#)
 - [Shipping log data to other Alibaba Cloud storage services in real time](#)
 - [Providing visual representations with other products](#)

2.8 Export log entries

The Log Analysis function of Cloud Firewall allows you to export log entries to your local device.

You can export log entries on the current page to a CSV file, or export all log entries to a TXT file.

Procedure

1. Log on to the [Cloud Firewall console](#).
2. In the left-side navigation pane, select Advanced Features > Log Analysis.
3. On the Raw Logs tab page, click the Download icon  on the right side.



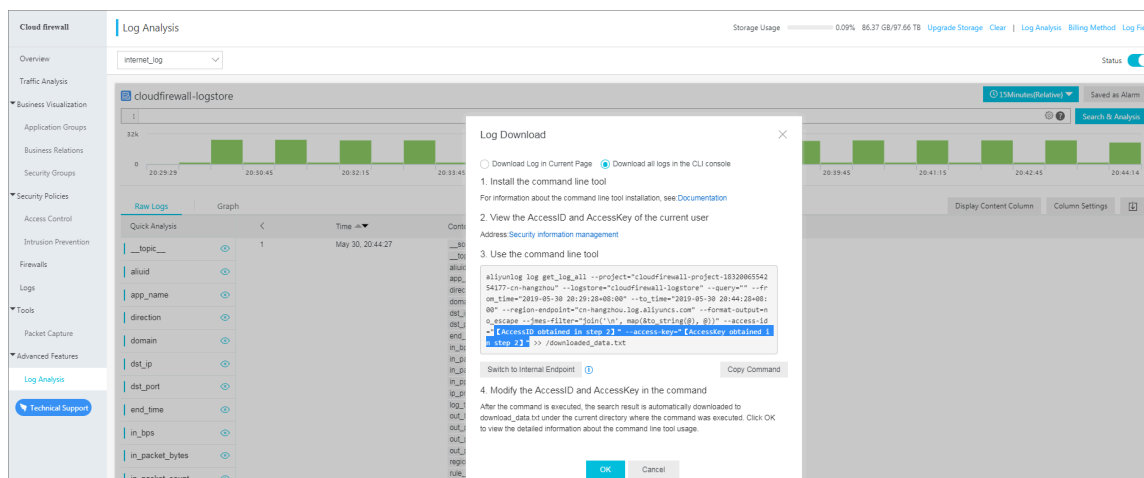
Note:

The download icon does not appear if there's no search result.

4. In the Log Download dialog box, select Download Log in Current Page or Download all logs by the CLI console.
 - Download logs in current page:

Click OK to export the raw log entries on the current page to a CSV file.
 - Download all logs by CLI:
 - a. For more information about installing the CLI, see [CLI guide](#).
 - b. Click [Security Information Management Link](#) to view and record the AccessKey ID and AccessKey Secret of the current user.
 - c. Click Copy Command and paste the command into CLI, replace the `AccessID` obtained in step 2 and `AccessKey Secret`

obtained in step 2 with the AccessKey ID and AccessKey Secret of the current user, and run the command.



After you run the command, all raw log entries created by Cloud Firewall are automatically exported and saved to the file `download_data.txt`.

2.9 Authorize RAM user accounts with Log Analysis function

If you want to use Cloud Firewall's Log Analysis function with a RAM user account, you must first use your Alibaba Cloud account to authorize this RAM user account with the Log Analysis functions of Cloud Firewall.

Context

The following permissions are required for enabling and using Cloud Firewall's Log Analysis function.

Operations	Required account
Enable the Log Analysis function. You only need to perform this operation once.	Alibaba Cloud account
Authorize Cloud Firewall to write the log data into the dedicated Logstore of Log Analysis in real time. You only need to perform this operation once.	<ul style="list-style-type: none">Alibaba Cloud accountA RAM user account with AliyunLogFullAccess permissionA RAM user account with the customized permission of log writing

Operations	Required account
Use the Log Analysis function.	<ul style="list-style-type: none"> Alibaba Cloud account A RAM user account with <code>AliyunLogFullAccess</code> permission A RAM user account with the customized permissions

You can grant permissions to a RAM user account as needed.

Scenarios	Grant a RAM user account permissions	Procedure
Grant a RAM user account full permission to Log Service.	The <code>AliyunLogFullAccess</code> policy specifies full permission to Log Service.	For more information, see RAM user management .
After you use your Alibaba Cloud account to enable the Cloud Firewall log analysis function and complete the authorization, grant the RAM user account the permission to view logs.	The <code>AliyunLogReadOnlyAccess</code> policy specifies the read-only permission.	For more information, see RAM user management .
Grant the RAM user account the permissions to enable and use the Cloud Firewall log analysis function. Do not grant other permissions to Log Service.	Create a custom authorization policy, and apply the policy to the RAM user account.	For more information, see the following procedure.

Procedure

1. Log on to the [RAM console](#).
2. Open the Create Custom Policy tab page on the Policies page.
3. In the upper-right corner of the page, click Create Authorization Policy.
4. Click Blank Template, enter the Policy Name and the following Policy Content into this template.



Note:

Replace `${ Project }` and `${ Logstore }` in the following policy with the Log Service Project name and Logstore name dedicated for Cloud Firewall, respectively.

```
{
  " Version ": " 1 ",
  " Statement ": [
    {
      " Action ": " log : GetProject ",
      " Resource ": " acs : log :*: project /${ Project }",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : CreateProj ect ",
      " Resource ": " acs : log :*: project /*",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : ListLogSto res ",
      " Resource ": " acs : log :*: project /${ Project }/
logstore /*",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : CreateLogS tore ",
      " Resource ": " acs : log :*: project /${ Project }/
logstore /*",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : GetIndex ",
      " Resource ": " acs : log :*: project /${ Project }/
logstore /${ Logstore }",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : CreateInde x ",
      " Resource ": " acs : log :*: project /${ Project }/
logstore /${ Logstore }",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : UpdateInde x ",
      " Resource ": " acs : log :*: project /${ Project }/
logstore /${ Logstore }",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : CreateDash board ",
      " Resource ": " acs : log :*: project /${ Project }/
dashboard /*",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : UpdateDash board ",
      " Resource ": " acs : log :*: project /${ Project }/
dashboard /*",
      " Effect ": " Allow "
    }
  ]
}
```

```

    },
    {
      " Action ": " log : CreateSave dSearch ",
      " Resource ": " acs : log :*:*: project /${ Project }/
savedsearc h /*",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : UpdateSave dSearch ",
      " Resource ": " acs : log :*:*: project /${ Project }/
savedsearc h /*",
      " Effect ": " Allow "
    }
  ]
}

```

Create Authorization Policy

Step 1: Select an authorization policy

Step 2: Edit permissions and submit.

Policy creation complete.

* Authorization Policy Name:

Names must be 1-128 characters long. They may only contain the letters A-Z, numbers 0-9, and hyphens.

Description:

Provides full access to Alibaba Cloud services and resources.

Policy Content:

```

1 {
2   "Statement": [
3     {
4       "Action": "*",
5       "Effect": "Allow",
6       "Resource": "*"
7     }
8   ],
9   "Version": "1"
10  }

```

Authorization Policy Format

Previous

Create Authorization Policy

Cancel

- Click Create Authorization Policy.
- Go to the Users page, locate the RAM user account, and click Authorize.
- Select the custom authorization policy that you created, and then click OK.

The authorized RAM user account then can enable and use the Log Analysis function. However, this RAM user account is not authorized to use other functions of Log Service.

2.10 Manage log storage

After you enable the Log Analysis function of Cloud Firewall, the log storage space is allocated based on your specified log storage size. You can view the usage of the log storage space on the Log Analysis page in the Cloud Firewall console.

Check the log storage

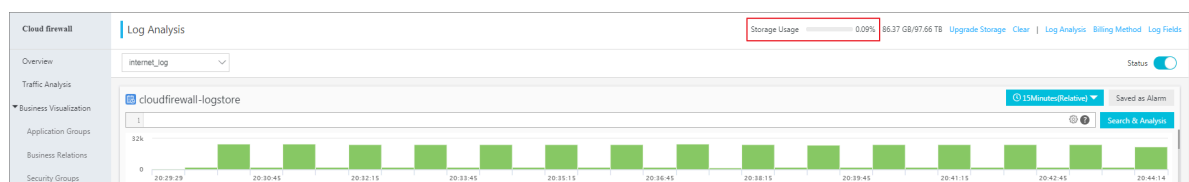
You can view the log storage in the Cloud Firewall console at any time.



Note:

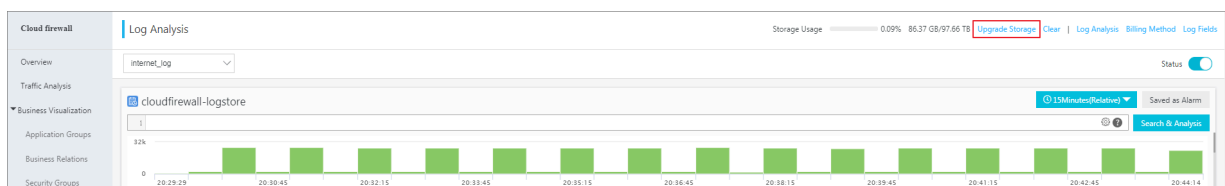
The log storage information in the console is not updated in real time. It takes up to two hours to update the actual storage information to the console. We recommend that you expand the log storage space before it is exhausted.

1. Log on to the [Cloud Firewall console](#).
2. In the left-side navigation pane, select **Advanced Features > Log Analysis**.
3. View the log storage information in the upper-right corner of the Log Analysis page.



Expand log storage

To expand the log storage, click **Upgrade Storage** at the top of the Log Analysis page.



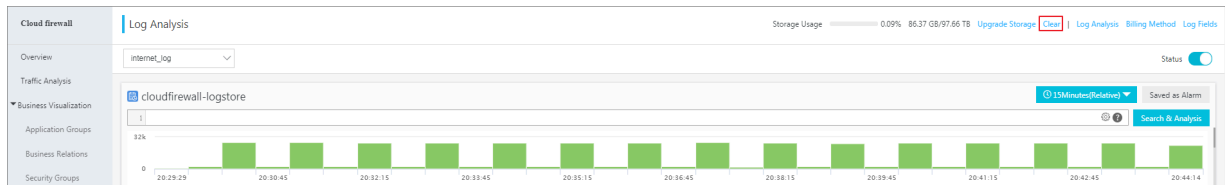
Note:

We recommend that you expand the log storage space before it is exhausted. If no storage space is available, then the new log data cannot be written into the dedicated Logstore.

Clear log storage

You can delete all log entries stored in the Logstore. For example, you can delete the log entries generated during the testing phase and use the log storage space to store log entries that are generated during the production phase only.

Click **Clear** at the top of the Log Analysis page, and confirm to delete all stored log entries.



Notice:

You cannot recover the deleted log entries. This operation is irreversible.



Note:

You only have limited times for clearing the log storage.