# Alibaba Cloud

Cloud Firewall Logs

Document Version: 20210610

C-J 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.

- You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloudauthorized 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 and/or its affiliates Cloud", "Alibaba Cloud. The names owned by Alibaba Cloud and/or its affiliates 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
<u>↑</u> 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.
O 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.
C) 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 listinstanceid 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.L	og audit	05
2.L	.og analysis	07
2	2.1. Overview	07
2	2.2. Billing	08
2	2.3. Enable the Log Analysis feature	09
2	2.4. Collect the log	10
2	2.5. Log analysis	12
2	2.6. Log reports	18
2	2.7. Log fields	25
2	2.8. Export logs	27
2	2.9. Authorize RAM user accounts with Log Analysis function	29
2	2.10. Manage the log storage space	32

# 1.Log audit

All the traffic that passes through Cloud Firewall is recorded as logs and displayed on the **Log Audit** page. The logs are classified into traffic logs, event logs, and operations logs. You can use the logs to audit your network traffic in real time and take measures accordingly. By default, the log audit feature retains logs for seven days.

Cloud Firewall also provides the log analysis feature, which can retain logs for six months. If your business must meet classified protection requirements, we recommend that you enable the log analysis feature. For information about the billing method of the log analysis feature, see Billing.

# **Event logs**

The Event Logs tab displays the logs of events on the Internet firewall and VPC firewalls. You can click the **Internet Firewall** or **VPC Firewall** tab to view information about event logs. The information includes the time an event was detected, the threat type, source IP address, destination IP address, application, severity, and policy action.

Log Audit														
Event Logs	Event Logs Operation Logs													
Internet Fir	irewall VPC Firewall													
Source IP	Enter a keyword.	Destination IP	Enter a keyword.	Туре	All $\checkmark$	Action	Discard $\checkmark$	Time	Apr 14, 2020 1	14:28	- Apr 14, 20	20 15:28	🗎 Search	
Received At	Туре	Module	Policy Name:		Source IP		Destination IP		Destination Port	Direction	Application	Severity	Policy Action	Actions
Apr 14, 2020, 15	5:28:52 -	Access Control	00.00	i.	11 52		39 10		0	Inbound	Unknown	-	Discard 🛇	Obtain Attack Sample
Apr 14, 2020, 15	5:28:52 -	Access Control	176-005	ŀ	11 52		39 16		0	Inbound	Unknown	-	Discard 🛇	Obtain Attack Sample

On the **Event Logs** tab, you can specify the source IP address, destination IP address, threat type, policy action, or time range to search for event logs.

**?** Note The time range must be within the last seven days.

# Traffic logs

The Traffic Logs tab displays the logs of traffic on the Internet firewall and VPC firewalls. You can click the **Internet Firewall** or **VPC Firewall** tab to view information about traffic logs. The information includes the start time and end time of traffic, source IP address, destination IP address, application type, source port, application, protocol, policy action, number of bytes, and number of packets.

Log Audit											
Event Logs Traf	fic Logs Operation	Logs									
Internet Firewall	VPC Firewall										
Source IP Enter a	a keyword. 🖨 De	stination IP Enter a key	word. Application	Select	✓ Apr 14, 202	0 14:30	- Apr 14, 2020 15:30		Search	Show Advanced	Search   🗟 List Configuration
Time	Source IP	Destination IP	Destination Port	Direction	Application	Protocol	Policy Action	Bytes	Packets	Policy Name	Actions
From :Apr 14, 2020.	151 05 0	20 250 (	24248	Inbound	Unknown	TCP	Allow	148 R	2	-	Obtain Attack Sample

On the **Traffic Logs** tab, you can specify the source IP address, destination IP address, application, or time range to search for traffic logs.

**?** Note The time range must be within the last seven days.

To more precisely search for traffic logs, click **Show Advanced Search** in the upper-right corner and specify search conditions such as **Direction**, **Policy Source**, **Port**, and **Region**.

Log Audit	
Event Logs Operation Logs	
Internet Firewall VPC Firewall	
Source IP Enter a keyword. 🕝 Destination IP Enter a keyword. Application Select 🗸 Traffic Type All Traffic Types 🗸 Direction All 🗸	
Policy Action All V IP Protocol All V Policy Source All V Port Enter a keyword Location Select V	Hide Advanced Correls 1. 🔲 List Configuration
Region All V ISP Select V Domain Name Enter a keyword Source Private IP Enter a keyword. URL Enter a keyword.	Hide Advanced Search   Es List Configuration
Apr 14, 2020 14:30 - Apr 14, 2020 15:30 🗎 Search	

Note If traffic hits an access control policy or IPS policy, the name of the policy is displayed in the Policy Name column of the traffic log entry. For traffic that does not hit a policy, the Policy Name column is displayed as a hyphen (-).

# **Operation** logs

The **Operation Logs** tab displays the time, type, severity, and other details about each operation performed on Cloud Firewall.

Lo	og A	Audi	t								
E	event L	_ogs	Traf	fic Logs	Operation Logs						
Sev	erity	All	$\sim$	Log Content	Enter a keyword.		2021-06-09 22:09:02	- 2021-06	-09 23:09:0	02 🛱	Search
Tir	ne			Туре		Sev	erity	Account		Log Cont	ent
Ju	n 9, 20:	21, 22:3	30:16	Operat	ion Logs	Imp	ortant	Alibaba Cloud Acc beaver-test	ount:	Add acce Details:	ss control success UUID:b7066a17-4

On the **Operation Logs** tab, you can select an option from the **Severity** drop-down list to obtain operations logs of a specific severity.

You can also specify a time range within the last seven days to search for operations logs.

# 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 Enable the Log Analysis feature.

### 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. Billing

The log analysis feature in Cloud Firewall uses the subscription billing method and is billed based on the log storage duration and capacity.

You can select this feature and specify the log storage duration and capacity as required on the Cloud Firewall buy page. The fee is calculated based on the specified log storage specifications and the subscription duration of your Cloud Firewall instance.

# Log storage specifications

The following table lists prices for different specifications.

Log storage duration	Log storage	Monthly	Decommonded	Cloud Firewall instance in mainland China			
	capacity	bandwidth	edition	Monthly subscripti on	15% discount for annual subscription		
180 days	1 T B	Up to 10 Mbit/s	Premium Edition	USD 80	USD 861		
	5 T B	Up to 50 Mbit/s	Enterprise Edition	USD 400	USD 4,080		
	20 T B	Up to 200 Mbit/s	Ultimate Edition	USD 1,600	USD 16,320		

**Note** We recommend that you increase the log storage capacity by 1 TB for every 10 Mbit/s of bandwidth increase.

#### Increase of storage capacity

If the log storage capacity is used up, the system reminds you to increase the capacity. You can click **Upgrade Storage** to increase the storage capacity.

Log Analysis	Storage Usage 0.49% 485.16 GB/97.66 TB Upgrade Storage Clear   Log Analysis Billing Method Log Fields
Reports Logs	Status 🚺 internet_log 🗸
🕐 report (Belong To c	() Please Select ▼ 🗠 Subscribe () Refresh Reset Time

### ♥ Notice

- The free trial edition of Cloud Firewall does not support the log analysis feature. If you are using the free trial edition, the Cloud Firewall console does not display the log storage capacity. For information about how to enable the log analysis feature, see Enable the Log Analysis feature.
- If you do not increase the log storage capacity when it is used up, Cloud Firewall stops writing new logs to the Logstore of the log analysis feature. Existing logs in the Logstore are retained. Logs are stored for a maximum of 180 days before they are automatically deleted. If the feature has expired and you have not renewed the subscription within seven days, all logs in the Logstore are deleted. Deleted logs cannot be recovered.

# Subscription duration

The subscription duration of the log analysis feature is the same as that of the Cloud Firewall instance.

- **New purchase**: When you buy a Cloud Firewall instance with the log analysis feature enabled, the price of this feature is calculated based on the subscription duration of the instance.
- **Upgrade**: When you upgrade a Cloud Firewall instance with the log analysis feature enabled, the price of this feature is calculated based on the remaining duration (in minutes) of the existing Cloud Firewall instance.

#### Service expiration

If your Cloud Firewall instance expires, the log analysis feature also expires.

- After the feature expires, Cloud Firewall stops writing logs to the Logstore.
- Logs are retained for seven days after the expiration. If you renew the subscription within seven days, you can continue to use the feature. Otherwise, all logs are deleted.

# References

FAQ about Cloud Firewall logs

# 2.3. Enable the Log Analysis feature

After you activate Cloud Firewall, you can enable the Log Analysis feature in the Cloud Firewall console.

# Scenario

The **Log Analysis** feature logs Internet traffic in real time. It retrieves and analyzes log data and displays the results in dashboards. You can specify **Log Storage** when you enable this feature.

**?** Note The Log Analysis feature is available in the Cloud Firewall Pro, Enterprise, and Flagship editions.

# Procedure

- 1. Log on to the Cloud Firewall console.
- 2. In the left-side navigation pane, choose Logs > Log Analysis.
- 3. Click Activate Now.

Log Analysis
Log Analysis supports real-time log search and analysis, and provides a flexible report center. You can use a variety of SQL statements to analyze log data, create custom reports, and set alarms based on your needs.
Activate Nove Learn More

4. Set Log Analysis to Yes and specify Log Storage. Then, pay for the order.

Current Version	Enterprise Edition	Flagship Edition										
Fastures	Ready-to-use. No network co	nfiguration change required.										
Features	Built-in system redundancy a	ind smooth scaling-up.										
	Access control of inbound a	ccess control of inbound and outbound traffic.										
	Access control based on dor	access control based on domain names.										
	Intrusion prevention and inte	lligent blocking of threats.										
	Event log, access log, and sy	stem log.										
	Outbound traffic analysis.											
	Inbound traffic analysis.											
	Blocked traffic analysis.											
	Micro-isolation.											
	Business network topology.											
	Multi-tenant deployment and	resource sharing.										
	Assets: 50 to 1,000.											
	Internet traffic bandwidth: 50	) Mbit/s to 1 Gbit/s.										
	Multi-region deployment. Re	gions in mainland China and H	ong Kong only.									
ssets	- 693 + 台											
Bandwidth (Internet					- 50	+						
Firewall Throughput)	50Mbps	250Mbps	500Mbps	750Mbps	1000Mbps							
	oomopo	Loomspo	000111000	70011300	100011500							
og Analysis	Yes	No										
og Storage	-0				- 3000	+						
	3000GB	25000GB	50000CP	75000CP	100000-8	_						

**?** Note For more information about Log Analysis pricing, see Billing.

5. On the Log Analysis page, select internet\_log and turn on the switch next to Status to enable log collection.

Log Analysis	Storage Usage 0.49% 485.16 GB/97.66 T8 Upgrade Storage Clear   Log Analysis Billing Method Log Fields
Reports Logs	Status 💽 internet_log 🗸
C report (Belong To c	O Pleace Select ▼ □ Subscribe O Refresh Reset Time

The Log Analysis feature collects logs of inbound and outbound Internet traffic and analyzes the log data 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.

Cloud firewall	Log Analysis						Storage Usage	0.09% 85.93 GB	/97.66 TB Upgrade Storage	Clear   Log Analy	vsis Billing Method	d Log Fields
Overview	internet_log $\checkmark$										Stat	tus 🌔
Traffic Analysis	cloudfirewall-logstore	e								③ 15Minutes(Relat	ive) 🔻 Saved a	as Alarm
<ul> <li>Business Visualization</li> </ul>	1 log_type:internet_log	5								6	Search &	Analysis
<ul> <li>Security Policies</li> </ul>	SOk											
Firewalls	25k											
Logs	19:57:16	19:58:45	20:00:15	20:01:45	20:03:15	20:04:45	20:06:15	20:07:45	20:09:15	20:10:45	2	:0:12:01
▶ Tools	Raw Logs Gra	ph			,				Display Co	ntent Column	Column Settings	٤
Advanced Heatures	Quick Analysis	<	Time 🛋 🕶	Content								
Log Analysis	_topic	1	May 30, 20:12:01	source: log topic: cloue	_service dfrewall_access_log							
	aliuid 💿			aliuid : 1 app_name : Unk	nown							

# Default configuration item Description The log analysis project created by Cloud Firewall. The project name is determined according to the region of your Cloud Firewall instance. • If the Cloud Firewall instance is deployed in a Mainland China region, the project name is: cloudfirewall-project-Alibaba Cloud account ID-cn-hangzhou . • If the Cloud Firewall instance is deployed in the Finance Cloud Project (Hangzhou) region, the project name is: cloudfirewall-project-Al ibaba Cloud account ID-cn-hangzhou-finance . • If the Cloud Firewall instance is deployed in other regions, the project name is: cloudfirewall-project-Alibaba Cloud account IDap-southeast-1. The default Logstore is cloudfirewall-logstore . Logstore All log data retrieved by Cloud Firewall is stored in this Logstore. • If the Cloud Firewall instance is deployed in a Mainland China region, the project is saved in the China (Hangzhou) region by default. Region • If the Cloud Firewall instance is deployed in other regions, the project is saved in the Singapore region by default.

# Default log analysis configuration

Default configuration item	Description
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 it ems 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 Authorize RAM user accounts with Log Analysis function.

# 2.5. Log analysis

Could 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.

Cloud Firewall	Log Analysis	Storage Usage 000% 08:97.66.18 Upgrade Storage Clear   Log Analysis Billing Method Log Fields
Overview	internet_log ~	Satus 💽
Firewall Settings 3		
Traffic Analysis	@ cloudfirewall-logstore	O 15Minutes(Relative) ▼ Saved as Alarm
	<pre>i log_type:internet_log</pre>	🗇 🚱 Search & Analytics
<ul> <li>Security Policies</li> </ul>	25k Sing type internet ing Fireida	
Access Control		
Intrusion Prevention	09:48:16 09:49:45 09:51:15	09-52-45 09-54-15 09-53-45 10-01-15 10-01-45 10-03-01
▼ Loos		Log Entries343,030 Search StatusThe results are accurate.
	Raw Logs Graph	Display Content Column Column Settings
Log Audit	Quick Analysis < Time 🖛	Content
Log Analysis		_source_ tan annuan _topic ck
<ul> <li>Business Visualization</li> </ul>	alluid	aluid: 18320

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

Cloud Firewall	Log Analysis Storage Usage 600% 68/97.66 T8 Upgrade Storage Clear   Log Analysis Billing Method Log Felds
Overview	stant_log 🗸
Firewall Settings 3	<b>0</b>
Traffic Analysis	Q. cloudfirewall-logstore         0 15Mnute(Releve)         Seved as Airm
<ul> <li>Security Policies</li> </ul>	1 log_type:
Access Control	238. ● tog_type internet_tog 历史记录
Intrusion Prevention	094816 094945 095115 095245 095415 095545 095715 095845 10.00.15 10.0145 10.0201
▼ Logs	Log Entries/343,030 Search Status/The results are accurate.
	Raw Logs Graph Display Content Column Settings
Log Audit	Quick Analyzis < Time
Log Analysis	topic0 1 Sep 5,100.02Newce

### 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.

Once 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.

Log Analysis		Storage Usage 0.00	0% 08/97.66 TB Upgrade Storage Clea	r   Log Analysis Billing Method Log I	, Field
internet_log $\checkmark$				Status 🚺	)
@ cloudfirewall-logstore			01	SMinutes(Relative) ▼ Saved as Alarm ② ② Search & Analytics	n
25k 0 08.59.21 10.00.45 10.02.15 10.03.45	10:05:15 10:06:45	10:08:15 10:09:45	10:11:15	10:12:45	26
	Lon Entries 338 217 Search Status The results a	re arcurate			

• 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.

Cloud Firewall	Log Analysis				Storage Usage	0.00% 0	18/97.66 TB Upgrade Storage	Clear   Log Analysi	s Billing Method L	.og Fields
Overview	internet_log $\checkmark$								Status 🧲	D
Firewall Settings 3									_	
Traffic Analysis	@ cloudfirewall-logstore							③ 15Minutes(Relative)	Saved as A	larm
▼ Security Policies	1 log_type:internet_log and source: log_service	e						© Ø	Search & Anal	rtics
Access Control										
Intrusion Prevention	10:09:59 10:11:15 10:	12:45 10:14:15	10:15:45	10:17:15	10:18:45	10:20:15	10:21:45	10:23:15	10:2	4:44
▼ Logs	Raw Logs Graph		Log Entries:348,186 Se	earch Status:The results are accu	urate.		Display Co	ntent Column Co	lumn Settings	4
Log Audit	Quick Analysis < Th	me 🛋 🕶 Content								
Log Analysis	topic 0 1 Se	ep 5, 10:24:59source topic : r	log_service ess_log							
Business Visualization	aliuid	aliuid : 1832								

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\_service 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.

Log Analysis Storage Usage	ge 0.00% 08/97.66 TB Upgrade Storage Clear   Log Analysis Billing Method	Log Fields
internet_log V	Status	
∅ cloudfirewall-logstore	O 15Minutes(Relative) ▼ Saved a	s Alarm
<pre>1 log_type:internet_log and source: log_service</pre>	😳 🔞 Search & A	nalytics
0 10:09:59 10:11:15 10:12:45 10:14:15 10:15:45 10:17:15 10:18:45	10:20:15 10:21:45 10:23:15 1	0:24:44
Log Entries348,186 Search Status:The results are accurate.		
Raw Logs Graph		

• 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 <u>Quick analysis</u>.

Cloud Firewall	Log Analysis						Storage Usage	0.00% 08	/97.66 TB Upgrade Storage	Clear   Log Analysis	Billing Method Log Fields
Overview	internet_log	~									Status 🚺
Firewall Settings 3	[ _										
Traffic Analysis		gstore								③ 15Minutes(Relative) ▼	Saved as Alarm
<ul> <li>Security Policies</li> </ul>	1 log_type:inter	net_log								© ଡ	Search & Analytics
Access Control	258										
Intrusion Prevention	0 10:35:47	10:37:15	10:38:45	10:40:15	10:41:45	10:43:15	10:44:45	10:46:15	10:47:45	10:49:15	10:50:32
▼ Logs	Raw Logs	Graph			Log Entries:319,734	Search Status: The results an	e accurate.		Display Cor	tent Column Colum	nn Settings 📳
Log Audit	Quick Analysis	<	Time 🛋 🔻	Content							
Log Analysis	topic	<ul> <li>1</li> </ul>	Sep 5, 10:50:33	source: lo	g_service						
Business Visualization	aliuid	•		aliuid: 1835							
▶ Tools	app_name	٢		direction : ir domain :							
	direction	•		dst_ip: 47. dst_port: 3							
	domain	٢		end_time : in_bps : 212							
	dst_ip	•		in_packet_bytes in_packet_count	1: 266 1: 3						
	dst_port	•		in_pps : 3 ip_protocol : tcp	)						
	end_time	•		out_bps : 752	meClog						
Technical Support	in_bps	۲		out_packet_ovte out_packet_cou out_pps: 1	nt: 1						
	Lin nacket huten	0		region id : cours	ochoni						

# 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

Туре	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.

Onte 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 , err or , 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

Onte 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\_time\_msec > 5000 and request\_time\_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 Could 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



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. Log reports

Log reports in Cloud Firewall provide data collected by Log Analysis, such as basic traffic metrics, inbound and outbound traffic distribution. You can specify a time range, subscribe to log reports, and set a refresh frequency to view data in the dashboards.

## Prerequisites

The **Status** switch in the upper-right corner of the **Log Analysis** page must be **turned on**. If the switch is **turned off**, Log Analysis is disabled, and you cannot view log reports.

I	Log Analysis	Storage Usage	0.49% 485.22 GB/97.66 TB Upgrade Storage	Clear   Log Analysis Billing Method Log Fields
ſ	Reports Logs			Status internet_log V
	Preport (Belong To cloudfirewall-project-1832006554254177-cn-hangzhou )		③ Please Select ▼	🕬 🗹 Subscribe 🗘 Refresh Reset Time

# Procedure

- 1. Log on to the Cloud Firewall console.
- 2. In the left-side navigation pane, choose Log Analysis > Log Analysis.
- 3. In the upper-right corner of the Reports tab, click Please Select.

Log Analysis	Storage Usage 0.49% 485.22 GB/97.66 TB Upgrade Storage	Clear   Log Anal	lysis Billing Me	ethod Log Fields
Reports Logs		Status 🚺	internet_log	~
(9 report (Belong To cloudfremation	③ Please Select ▼	new ⊠ Subscribe	() Refresh	Reset Time
Cloud Firewall Report				
Displays the information about Cloud Firewall, such as the basic indicators, inbound traffic sources, outbound traffic distribution, and system stability				
Basic Indicators				

4. On the **Time** page, specify a time range for displaying reports of Internet traffic logs. You can specify a time range in the **Relative**, **Time Frame**, or **Custom** section.

Time ×	
Nov 20, 2019, 10:54:44 ~ Nov 20, 2019, 11:09:44	
> Relative	
1Minute 5Minutes 15Minutes	
1Hour 4Hours 1Day Today	
1Week 30Days This Month	
Custom	
> Time Frame	
1Minute 15Minutes 1Hour	
4Hours 1Døy 1Week 30Døys	
Today Yesterday	
The Day before Yesterday This Week	
Previous Week This Month This Quarter	
This Year Custom	
> Custom	
2019-11-20 10:54~2019-11-20 11:09	
ОК	
Minutes are used as the time precision of the current query time.	
your SQL statement. Example: "   select " from log where	
_tme_>1558013658 and _time_< 1558013660	
_tme_>1558013658 and _time_< 1558013660	
bme_>133011868 andbme_<155011860	Description
Section	Description Displays log data collected within a specified time range going back from the current time. This time range is accurate to seconds. Assume that the current time is 2019-10-17 23:08:00. The value 2019-10-17 23:07:00~2019-10-17 23:08:00 indicates that log data collected in the last minute is displayed. You can specify a time range in days, hours, minutes, or seconds.
Section Relative	DescriptionDisplays log data collected within a specified time range going back from the current time. This time range is accurate to seconds. Assume that the current time is 2019-10-17 23:08:00. The value 2019-10-17 23:07:00~2019-10-17 23:08:00 indicates that log data collected in the last minute is displayed. You can specify a time range in days, hours, minutes, or seconds.
Section Relative Time Frame	DescriptionDisplays log data collected within a specified time range going back from the current time. This time range is accurate to seconds. Assume that the current time is 2019-10-17 23:08:00. The value 2019-10-17 23:07:00~2019-10-17 23:08:00 indicates that log data collected in the last minute is displayed. You can specify a time range in days, hours, minutes, or seconds.Displays log data collected within a specified time range. For example, the value 2019-10-10 00:00:00~2019-10-17 00:00:00 indicates that log data was collected for the week starting from 2019-10-10 00:00:00.
Section Relative Time Frame	DescriptionDisplays log data collected within a specified time range going back from the current time. This time range is accurate to seconds. Assume that the current time is 2019-10-17 23:08:00. The value 2019-10-17 23:07:00~2019-10-17 23:08:00 indicates that log data collected in the last minute is displayed. You can specify a time range in days, hours, minutes, or seconds.Displays log data collected within a specified time range. For example, the value 2019-10-10 00:00:00~2019-10-17 00:00:00 indicates that log data was collected for the week starting from 2019-10-10 00:00:00. You can specify a time range in days, hours, or minutes.

After you specify a time range, all dashboards on the Reports tab are refreshed to display data within this time range.

Displays log data collected within a custom time range. The start and end

For more information about the dashboards, see Log report dashboards.

time is accurate to minutes.

**Note** The specified time range is only valid on the current page. The next time you open the Reports tab, the time range of the dashboards is restored to the default.

5. (Optional)On the Reports tab, perform operations on a dashboard. In the upper-right corner of

the target dashboard, click the 👔 icon to show the menu.

The menu of a dashboard supports the following operations:

• Select Time Range: The dashboard displays basic metrics within the specified time range. You can specify a relative time range, time frame, or custom time range. For more operations, see the descriptions in step 4.

Custom

- Download Log: Select this option to save the logs as an Excel file to your computer.
- $\circ~$  Download Chart : Select this option to save the dashboard as a PNG file to your computer.
- Preview Query Statement: Click the 💿 icon to view the query statement of the log metrics

in the dashboard. You can use the statement to query the log data on the Logs tab. For more information about log queries, see Log analysis.

Log Analysis			Storage Usage	0.49% 485.22 GB/97.66 TB Upgrade Storage	Clear   Log Analysis Billing Method Log Fields
Reports Logs					Status 🚺 internet_log 🗸 🗸
Preport (Belong To cloudfirewall-project-	-1832006554254177-cn-hangzhou )			③ Please Select ▼	Subscribe () Refresh Reset Time
Cloud Firewall Report					
Displays the information about Cloud Firewa	all, such as the basic indicators, inbound traffic so	urces, outbound traffic distribution, and system	stability		
Basic Indicators					
Total number of Intercepting 1 Ho	Inbound Traffic 1 Hour(Relative)	Inbound Traffic 1 Hour(Relative)	SSH Access 1 Hour(Relative)	RDP Access 1 Hour(Relative)	FTP Access 1 Hour(Relative)
1,913 times	2.32MB	4.67MR Preview Query Statement	425 times ×	4 times	57 times
Inbound Traffic		<ul> <li>*   select count(1) as drop_</li> </ul>	count from log where rule_result='drop'		
Intercept trend 1 Hour(Relative)	:	Ŭ		Sources - Global 1 Hour(Relative)	:
500			ок		
400					81.4
300			MySQL	San Alignet	A State of the second s
200	• drop_count		• IDP • SSH		
100			• Unknown • HTTP	7K- 3.5K-7K 1.75K-3.5K 875-1.75K 330-875	
18:56:00 19:07:00 19:06:00 19:17:00 19:27:00	19.26.00 19.31.00 19.36.00 19.41.00 19.46.00 19.51.00 19.56.00	99.42%		70-175 0-70	

6. (Optional)Subscribe to log reports. You can specify the frequency at which the system sends log data notifications by email or DingTalk chatbot.

In the upper-right corner of the Reports tab, click **Subscribe**. On the **Create Subscription** page that appears, subscribe to Internet traffic log reports.

Parameter	Description
Subscription Name	The name of the log report subscription. A default name is provided, but you can change it as needed.
Frequency	<ul> <li>The frequency at which log report notifications are sent. Valid values:</li> <li>Hourly: A notification is sent every hour.</li> <li>Daily: A notification is sent each day at a specified hour between 00:00 and 23:00.</li> <li>Weekly: A notification is sent each week on a specified day at a specific hour between 00:00 and 23:00.</li> <li>Fixed Interval: A notification is sent at a specified interval. You can select Days or Hours.</li> <li>Cron: Use a cron expression to customize the frequency. The time specified in a cron expression is accurate to minutes and is in the 24-hour notation. You can refer to the examples in the console to write a cron expression.</li> </ul>
Add Watermark	The address that sends the notification is attached to the image as a watermark. It can be an email address or a webhook URL of the DingTalk chatbot.

### i. In **Subscription Configuration**, configure the following parameters.

ii. Click **Next** to set a notification type.

WebHook-DingTalk Bot $\times$	^
Email  VebHook-DingTalk Bot	
0/	256
t] reportReport 33/	100
t	WebHook-DingTalk Bot × Email WebHook-DingTalk Bot 0/1 1] reportReport 333/

Notification type	Parameter	Description
Empil	Recipients	The email address of the recipient. You can add more than one recipient.
Email	Subject	The subject of the email. A default subject is provided, but you can change it as needed.
WebHook- DingTalk Bot	Request URL	The webhook URL requested. For more information about how to obtain the webhook URL, see Configure DingTalk chatbot notifications.
	Title	The title of the webhook. A default title is provided, but you can change it as needed.

#### iii. Click Submit .

iv. In the dialog box that appears,  ${\rm click}\,{\rm OK}.$ 

After the subscription is created, you can move the pointer over the **Subscribe** button on the

**Reports** tab to view the subscription.

You can also click **Subscribe** to **modify** the subscription configurations and notification type or **cancel** the subscription.

	to to opgrade storage, crear, i tog knarysis, binning method, tog herds
Reports Logs	Status 🚺 internet_log 🗸
report (Relong To doudfrewal-project-1833006554254177-on-hangshou )      Basic Indicators	Please Sidect      C3 Subscribe     O Refresh Reset Time     Modity
Total number of Intercepting Houri, Inbound Traffic Hour(Relative) : Inbound Traffic Hour(Relative) : SSH Access Hour(Relative) : RDP Access Hour	(Relative) :

**?** Note You can only create one subscription. To create a new subscription, you must cancel the existing one.

7. (Optional)In the upper-right corner of the **Reports** tab, click **Refresh** to set the frequency to refresh log reports.

Log Analysis Storage Usage 0.12% 119.90 GB/97.66 TB Upgrade Storage Clear   Log Analysis Billing Method Log Fields					
Reports Logs Status 🔵 internet_Jog					Status 🚺 internet_log 🗸
report (Belong To cloudfirewall-project-18     Basic Indicators	832006554254177-cn-hangzhou )			③ Please Select ▼	C Refresh Reset Time
Total number of Intercepting Hear(ž. 703 times	Inbound Traffic Hour(Relative) : 438.47MB	Inbound Traffic Hour(Relative) : 1.11GB	SSH Access Hocur(Relative) : 1.151K times	RDP Access 11Hour(Relative) :	60Seconds Auto Refresh > : 5Minutes 15Minutes 0 times
Frequency		Description			
Once		Trigger a refresh immediately.			
Auto Refresh		Specify a refre seconds, 60 se	sh frequency. You conds, 5 minutes	a can set it to 15 , or 15 minutes.	

# Log report dashboards

Log reports provide a global view of Internet traffic, including basic traffic metrics, inbound and outbound traffic trends, and traffic distribution. The following table describes all dashboards supported by Cloud Firewall.

Dashboard	Туре	Default time range	Description	Exampl e
Total number of Intercepting	Numeri c value	1 hour (relative)	The number of Internet access requests blocked by Cloud Firewall for a specified time range.	10
Inbound Traffic	Numeri c value	1 hour (relative)	The volume of inbound traffic from the Internet for a specified time range.	10 MB
Outbound Traffic	Numeri c value	1 hour (relative)	The volume of outbound traffic to the Internet for a specified time range.	10 GB
SSH Access	Numeri c value	1 hour (relative)	The number of SSH access requests for a specified time range.	10

#### Logs · Log analysis

Dashboard	Туре	Default time range	Description	Exampl e
RDP Access	Numeri c value	1 hour (relative)	The number of RDP access requests for a specified time range.	10
FTP Access	Numeri c value	1 hour (relative)	The number of FTP access requests for a specified time range.	10
Interception trend	Line chart	1 hour (relative)	The trend for the number of times inbound traffic is blocked for a specified time range.	-
Intercepted Source Applications	Pie chart	1 hour (relative)	The top 10 applications (such as HTTP, SNMP, SIP, and SSH) requested by blocked inbound traffic for a specified time range.	-
Sources - Global	World map	1 hour (relative)	The geographical distribution of inbound traffic sources for a specified time range.	-
Source Applications – Top 10	Pie chart	1 hour (relative)	The top 10 applications (such as HTTP and SSH) requested by inbound traffic for a specified time range.	-
Source Regions – Top 10	Pie chart	1 hour (relative)	The top 10 source regions with the most inbound traffic for a specified time range.	-
Source Ports – Top 20	T reem ap chart	1 hour (relative)	The top 20 ports that are accessed by inbound traffic for a specified time range.	-
Interception trend	Line chart	1 hour (relative)	The trend for the number of times outbound traffic is blocked for a specified time range.	-
Intercepted External Applications	Pie chart	1 hour (relative)	The top 10 applications (such as HTTP and SSH) requested by blocked outbound traffic for a specified time range.	_
External Ports – Top 20	T reem ap chart	1 hour (relative)	The top 20 ports accessed by outbound traffic for a specified time range.	-
External IP Addresses – Top 10	Pie chart	1 hour (relative)	The top 10 IP addresses requested by outbound traffic for a specified time range.	-
External Domains – Top 10	T reem ap chart	1 hour (relative)	The top 10 domain names requested by outbound traffic for a specified time range.	-

Dashboard	Туре	Default time range	Description	Exampl e
External Applications – Top 10	Pie chart	1 hour (relative)	The top 10 applications (such as HTTP and SSH) requested by outbound traffic for a specified time range.	-

# 2.7. Log fields

Cloud Firewall logs record both inbound and outbound traffic. Each log entry contains multiple fields. You can use these fields to search and analyze logs.

Field name	Description	Example
time	The time when the operation is performed.	2018-02-27 11:58:15
_topic_	The topic of the log entry. The value is fixed as <b>cloudfirewall_access_log</b> , which indicates that the log entry records traffic controlled by Cloud Firewall.	cloudfirewall_access_log
log_type	The type of the log entry. The value is fixed as <b>internet_log</b> , which indicates the log entry records Internet traffic.	internet_log
aliuid	The ID of the Alibaba Cloud account.	1233333333****
app_name	The application to which the traffic belongs. The valid values include HTTPS , NTP , SIP , SMB , NFS , DNS , and Unknown .	HTTPS
direction	<ul> <li>The direction of the traffic. Valid values:</li> <li>in : inbound traffic to your Elastic Compute Service (ECS) instances from other ECS instances in the internal network or from servers on the Internet.</li> <li>out : outbound traffic from your ECS instances to other ECS instances in the internal network or to servers on the Internet.</li> </ul>	in
domain	The domain name of the traffic.	www.aliyun.com
dst_ip	The destination IP address of the traffic.	1.XX.XX.1
dst_port	The destination port of the traffic.	443
end_time	The time when the session ends. This value is a UNIX timestamp. Unit: seconds.	1555399260
in_bps	The rate of inbound traffic. Unit: bit/s.	11428

Field name	Description	Example
in_packet_byte s	The total number of bytes in inbound traffic.	2857
in_packet_cou nt	The total number of packets in inbound traffic.	18
in_pps	The packet throughput of inbound traffic. Unit: packet/s.	9
ip_protocol	The IP protocol of the traffic. Valid values: TCP and UDP.	ТСР
out_bps	The rate of outbound traffic. Unit: bit/s.	27488
out_packet_by tes	The number of bytes in outbound traffic.	6872
out_packet_co unt	The number of packets in outbound traffic.	15
out_pps	The packet throughput of outbound traffic. Unit: packet/s.	7
region_id	The region ID of the traffic. For more information about region IDs, see Regions that are supported by Cloud Firewall.	cn-beijing
rule_result	<ul> <li>The processing result of the traffic that matches the access control policy. Valid values:</li> <li>pass : Cloud Firewall allows the traffic.</li> <li>alert : Cloud Firewall allows the traffic and generates an alert.</li> <li>drop : Cloud Firewall drops the traffic, which indicates that the traffic cannot pass Cloud Firewall.</li> </ul>	pass
src_ip	The source IP address of the traffic.	1.XX.XX.1
src_port	The source port of the traffic.	47915
start_time	The time when the session starts. This value is a UNIX timestamp. Unit: seconds.	1555399258
start_time_min	The time when the session starts. The value of this field is rounded up to the next minute. This value is a UNIX timestamp. Unit: seconds.	1555406460
tcp_seq	The TCP serial number.	3883676672
total_bps	The total rate of inbound and outbound traffic. Unit: bit/s.	38916

#### > Document Version: 20210610

Field name	Description	Example
total_packet_ bytes	The total number of bytes in inbound and outbound traffic. Unit: byte.	9729
total_packet_c ount	The total number of packets in inbound and outbound traffic.	33
total_pps	The total packet throughput of inbound and outbound traffic. Unit: packet/s.	16
vul_level	<ul> <li>The risk level of the vulnerability. Valid values:</li> <li>1 : low-risk vulnerabilities</li> <li>2 : medium-risk vulnerabilities</li> <li>3 : high-risk vulnerabilities</li> </ul>	1
url	The URL of the Internet website that your ECS instance accesses.	http://www.test.com/index.htm l
src_private_ip	The private IP address of the source ECS instance in outbound traffic.	192.168.0.0
acl_rule_id	The ID of the access control list (ACL) rule that matches the traffic.	073a1475-6e11-43e2-8b28- 98cee9c688c0
ips_rule_id	The ID of the intrusion prevention system (IPS) rule that matches the traffic.	073a1475-6e11-43e2-8b28- 98cee9c688c0
ips_ai_rule_id	The ID of the AI rule that matches the traffic.	073a1475-6e11-43e2-8b28- 98cee9c688c0
ips_rule_name	The Chinese name of the IPS rule that matches the traffic.	Mining activities of hosts
ips_rule_name _en	The English name of the IPS rule that matches the traffic.	Mining behavior on the host
attack_type_n ame	The Chinese name of the attack type that is detected in the traffic.	Mining activities
attack_type_n ame_en	The English name of the attack type that is detected in the traffic.	Mining Behavior

# 2.8. Export logs

The log analysis feature allows you to export log query results to your local disk. You can download logs on a specific page as a CSV file or download all logs as a TXT file. This topic describes how to export logs in the Cloud Firewall console.

## Procedure

1. Log on to the Cloud Firewall console.

ГIJЛ

- 2. In the left-side navigation pane, choose Log Analysis > Log Analysis.
- 3. Click Logs and Raw Logs. In the upper right corner, click

•					
Log Analysis		Storage Usage	0.49% 485.22 GB/97.66 TB Upg	rade Storage Clear   Log Analysis	Billing Method Log Fields
Reports Logs				Status 🚺 int	ernet_log ~
@ cloudfirewall-logstore				() 15 Minutes(Relative) 💙 Auto Re	fresh Save as Alert
log_type:internet_log				ି (	Search & Analyze
500					
250					
0 19:04:48 19:06:15 19:07:45	19:09:15 19:10:45	19:12:15 19:13:45	19:15:15	19:16:45 19:18:15	19:19:33
	Log Entries:3,999	Search Status: The results are accurate.			
Raw Logs Graph				Display Content Column Col	umn Settings 📳
Quick Analysis < Time 🛋 Content					
Search Q 1 Apr 14, 19:19:44source: log topic : cloud	service firewall access log				

- 4. In the Log Download dialog box that appears, select a method to download logs.
  - Select Download Log in Current Page and click OK.

Log Download		×
Download Log in Current Page	O Download All Logs with Cloud Shell	O Download All Logs Using Command Line Tool
	OK Cancel	

Logs on the current page are downloaded in a CSV file.

• Select Download All Logs with Cloud Shell.

Log Download	F
O Download Log in Current Page   O Download All Logs with Cloud Shell   Download All Logs Using Command Line Tool	
<ul> <li>Notes:</li> <li>1. After you click "OK", the log is automatically downloaded through Cloud Shell.</li> <li>2. After the log is downloaded, a dialog box appears. You must select a local directory to save the log.</li> <li>3. Cloud Shell is deployed in the China (Shanghai) region, but the current Logstore is</li> </ul>	
not deployed in this region. Therefore, an extra Internet traffic fee will be charged for downloading the log from the Logstore. For more information, see Log Service Pricing         OK       Cancel	

- a. Click OK to go to the Cloud Shell command line.
- b. Follow the instructions that appear on the page to enter the required information.
- c. Specify a local path where you want to store the log file.

All logs are downloaded.

**Note** Currently, Cloud Shell is deployed in the China (Shanghai) region. If the current Logstore is not in the China (Shanghai) region, downloading log data incurs data consumption fees. Click **Log Service Pricing** to learn more about the pricing of data usage.

• Select Download All Logs Using Command Line Tool.

Log Download	×
Download Log in Current Page     Download All Logs with Cloud Shell     O     Download All Logs Using Command Line To     I. Install the command line tool	100
For information about the command line tool installation, see Documentation 2. View the AccessKeyId and AccessKeySecret of the current user Address:Security information management	
3. Use the command line tool	
<pre>aljyuulog log get.log_allproject="sas-log-103200655425417-cn-hangzhou"logstore="sas-log"query=topic_:aegis-log-crack"from_time="2019- 11-86 22:27:43+08:00"region-endpoi nt="cn-hangzhou.log.ellyuncs.com"format-output=no_escapejmes-filter ="join('\n', map(&amp;to_string(@), @))"access-id=" [AccesskeyId obtained in step 2]"access-key=" [AccesskeySecret obtained in step 2]" &gt;&gt; ./downloa ded_data.txt</pre>	
Switch to Internal Endpoint () Copy Comman	d
4. Modify the AccessKeyId and AccessKeySecret in the command	
After the command is executed, the search result is automatically downloaded to download_data.bd under the current directory where the command was executed. Click OK to view the detailed information about the command line tool usage.	
OK Cancel	

- a. Click **Documentation** in the Log Download dialog box to learn how to install a command line tool.
- b. Install the command line tool.
- c. Click **Security information management** to view and copy the AccessKey ID and AccessKey secret of the current user.
- d. Click Copy Command and replace the AccessKey ID in step 2 and AccessKey secret in step 2 with those of the current user.
- e. Run the command in the CLI command line tool.

After the command is executed, all logs are downloaded to the **download\_data.txt** file in the directory where the command is executed.

# 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> <li>Alibaba Cloud account</li> <li>A RAM user account with AliyunLogFullAccess permission</li> <li>A RAM user account with the customized permission of log writing</li> </ul>
Use the Log Analysis function.	<ul> <li>Alibaba Cloud account</li> <li>A RAM user account with AliyunLogFullAccess permission</li> <li>A RAM user account with the customized permissions</li> </ul>

#### 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 AliyunLogFullAccess 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 <b>AliyunLogReadOnlyAccess</b> 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.

Image: The second sec

```
{
    "Version": "1",
```

Cloud Firewall

"Statement": [ { "Action": "log:GetProject", "Resource": "acs:log:\*:\*:project/\${Project}", "Effect": "Allow" }, { "Action": "log:CreateProject", "Resource": "acs:log:\*:\*:project/\*", "Effect": "Allow" }, { "Action": "log:ListLogStores", "Resource": "acs:log:\*:\*:project/\${Project}/logstore/\*", "Effect": "Allow" }, { "Action": "log:CreateLogStore", "Resource": "acs:log:\*:\*:project/\${Project}/logstore/\*", "Effect": "Allow" }, { "Action": "log:GetIndex", "Resource": "acs:log:\*:\*:project/\${Project}/logstore/\${Logstore}", "Effect": "Allow" }, { "Action": "log:CreateIndex", "Resource": "acs:log:\*:\*:project/\${Project}/logstore/\${Logstore}", "Effect": "Allow" }, { "Action": "log:UpdateIndex", "Resource": "acs:log:\*:\*:project/\${Project}/logstore/\${Logstore}", "Effect": "Allow" }, { "Action": "log:CreateDashboard", "Resource": "acs:log:\*:\*:project/\${Project}/dashboard/\*", "Effect": "Allow" }, { "Action": "log:UpdateDashboard", "Resource": "acs:log:\*:\*:project/\${Project}/dashboard/\*", "Effect": "Allow" }, { "Action": "log:CreateSavedSearch", "Resource": "acs:log:\*:\*:project/\${Project}/savedsearch/\*", "Effect": "Allow" }, { "Action": "log:UpdateSavedSearch", "Resource": "acs:log:\*:\*:project/\${Project}/savedsearch/\*",

"Effect": "Allow" } ] }		
Create Authorization Policy		$\times$
Step 1: Select an authorizat	ion 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       {       "Statement": [         3       4	
	Previous Create Authorization Policy Car	cel

- 5. Click Create Authorization Policy.
- 6. 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 the log storage space

After you enable the log analysis feature, log storage space is allocated based on the storage capacity you specify. You can view log storage usage on the Log Analysis page in the Cloud Firewall console.

### View log storage usage

You can view log storage usage on the Log Analysis page.

**Note** Log storage usage is updated every two hours in the Cloud Firewall console. We recommend that you upgrade your log storage before it is used up.

1. Log on to the Cloud Firewall console.

- 2. In the left-side navigation pane, choose Logs > Log Analysis.
- 3. In the upper-right corner of the Log Analysis page, view log storage usage.

Log Analysis	Storage Usage	0.49% 485.21 GB/97.66 TB	Upgrade Storage	Clear   Log A	nalysis Billing Method	l Log Fields
Reports Logs				Status 🦲	) internet_log	~

# Upgrade log storage

On the top of the **Log Analysis** page, click **Upgrade Storage**. Configure a larger storage capacity and pay for the order.

**?** Note If you do not upgrade your log storage space before it is used up, Cloud Firewall cannot store new log entries to the dedicated Logstore.

# Clear your log storage space

You can delete log entries stored in the Logstore. For example, you can delete all log entries generated during the test phase to save space for log entries that are generated during service production.

On the top of the Log Analysis page, click Clear to delete all log entries.

🗘 Notice

- Deleted log entries cannot be recovered. Exercise caution when you perform this operation.
- You can clear the log storage space only a few times.