Log Service

Quick Start

MORE THAN JUST CLOUD | Alibaba Cloud

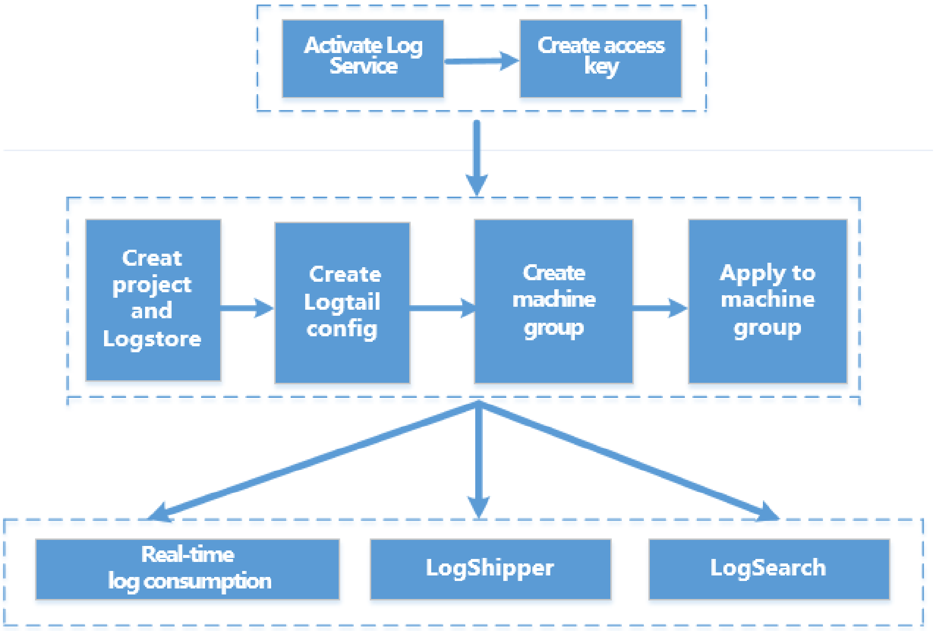
Quick Start

Log Service is a platform service provided by Alibaba Cloud to handle massive log collection, storage, and query. You can use Log Service to collect logs from the service cluster. Log Service also supports real-time consumption, real-time query and shipping logs to OSS+Spark or MaxCompute (coming soon) for further analysis.

The following sample introduces how to collect text logs by using Logtail, preview logs, query the logs collected and ship logs to OSS.

Workflow

The basic workflow of using Log Service is as follows.



1. Preparations

1.1 Create an Alibaba Cloud account

For details, refer to FAQ about account management.

1.2 Activate Log Service

Use a registered Alibaba Cloud account to log on to the Log Service product page and click **Get it Free**.

1.3 Create an Access Key

> **Note:** Logtail requires an access key to collect log data.

On the Log Service console, move the cursor above your username in the upper-right corner and click **accesskeys** in the displayed menu.

In the pop-up confirmation box, click **Continue to manage AccessKey**.

On the **Access Key Management** page, click **Create Access Key** in the upper-right corner.

In the pop-up box, click **Agree and create**.

2 Create project

2.1 Create a project

When you first log on to the Log Service console, the system will prompt you to create a project. To create projects on subsequent logins, click **Create Project** in the upper-right corner.

> **Note:** For details about creating a project, refer to Create a project.

When creating a project, you must specify the **Project Name** and **Region**.

2.2 Create a Logstore

After creating a project, you will be prompted to create a Logstore. You can also go to the project and click **Create** in the upper-right corner.

> **Note:** For details about creating a Logstore, refer to Create a Logstore.

When creating a Logstore, you must specify how you are going to use these logs.

3 Collect logs

Log Service supports various log sources and collection modes; for details, refer to Collection modes.

3.1 Install the Logtail client

Download the installation package.

Download the Logtail installation package onto the ECS instance. The download address of Windows installation package is http://logtail-release.oss-cn-hangzhou.aliyuncs.com/win/logtail_installer.zip.

For your relevant installation method, please refer to the Install Logtail on Windows or Install Logtail on Linux.

Install Logtail.

Unzip the installation package into the current directory and enter the logtail_installer directory. Run cmd as the administrator and run the installation command .\logtail_installer.exe install cn_hangzhou.

> **Note:** You must run different installation commands according to the network environment and the region of Log Service. This quick start uses China East 1 (Hangzhou) and classic network as an example. For the installation commands of other regions, refer to Install Logtail on Windows.

3.2 Create a Logtail configuration

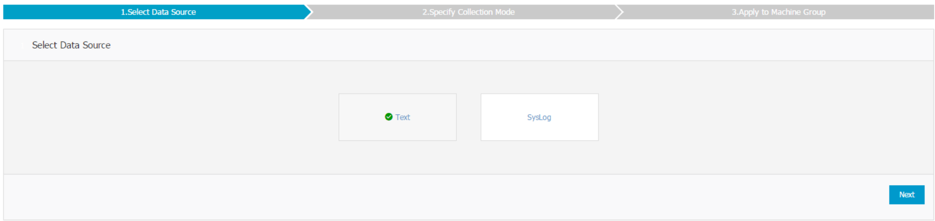
Log on to the Log Service Console.

Select the desired project, and click the project name or click **Manage** on the right.

Select the desired Logstore and click Logtail Config **Manage**.

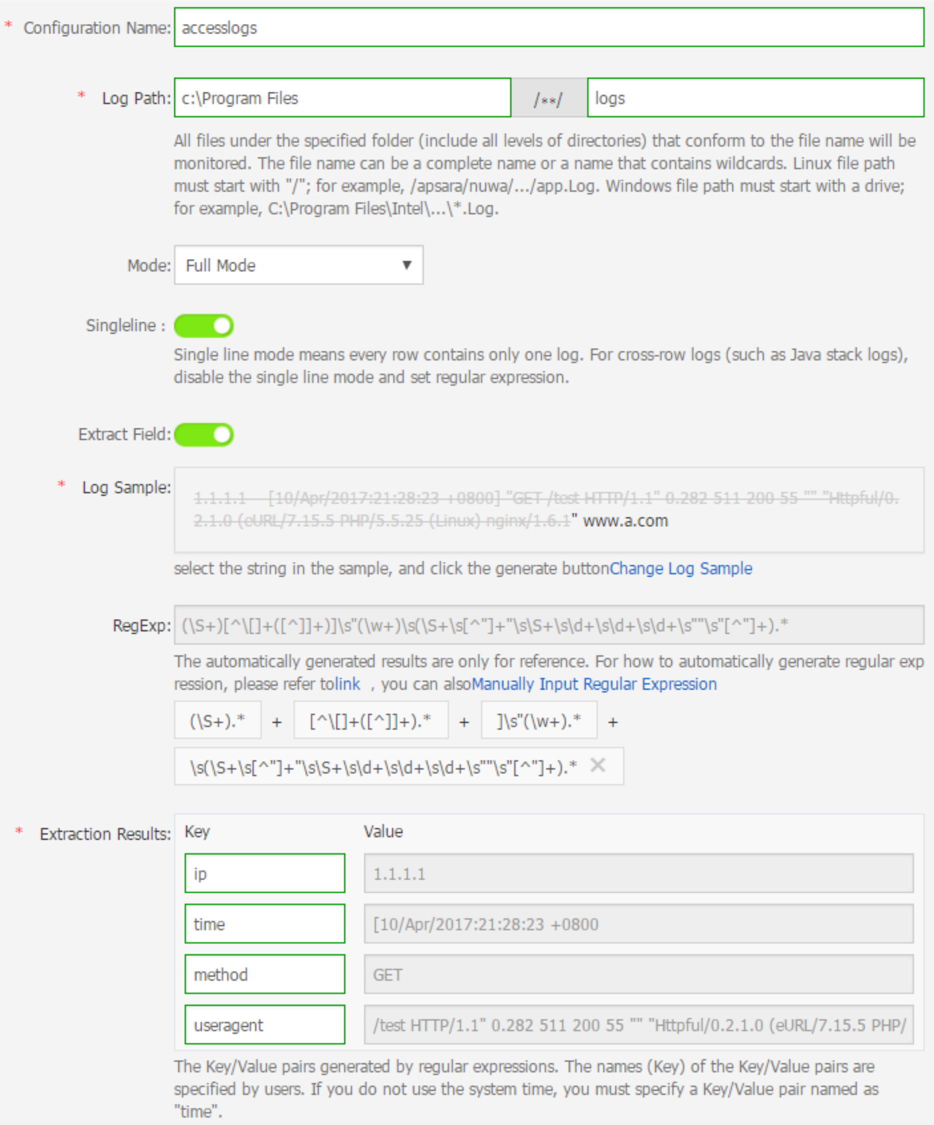
Click **Create** in the upper-right corner.

Select a data source.



Specify the collection mode.

This example uses full mode. For details about Logtail configuration, refer to Use logtail to collect text files.



* Configuration Name: accesslogs

* Log Path: c:\Program Files /**/ logs

All files under the specified folder (include all levels of directories) that conform to the file name will be monitored. The file name can be a complete name or a name that contains wildcards. Linux file path must start with "/"; for example, /apsara/nuwa/.../app.Log. Windows file path must start with a drive; for example, C:\Program Files\Intel\...*.Log.

Mode: Full Mode ▼

Singleline : ●

Single line mode means every row contains only one log. For cross-row logs (such as Java stack logs), disable the single line mode and set regular expression.

Extract Field: ●

* Log Sample: ~~1.1.1.1 [10/Apr/2017:21:28:23 +0800] "GET /test HTTP/1.1" 0.282 511 200 55 "" "Httpful/0.2.1.0 (cURL/7.15.5 PHP/5.5.25 (Linux) nginx/1.6.1~~" www.a.com

select the string in the sample, and click the generate buttonChange Log Sample

RegExp: `(\S+)[^\[]+([^]]+)]\s"(\w+)\s(\S+\s[^"]+"\s\S+\s\d+\s\d+\s\d+\s""\s"[^"]+).*`

The automatically generated results are only for reference. For how to automatically generate regular expression, please refer tolink , you can alsoManually Input Regular Expression

`(\S+).*` + `[^\[]+([^]]+).*` + `]\s"(\w+).*` +

`\s(\S+\s[^"]+"\s\S+\s\d+\s\d+\s\d+\s""\s"[^"]+).*` ✕

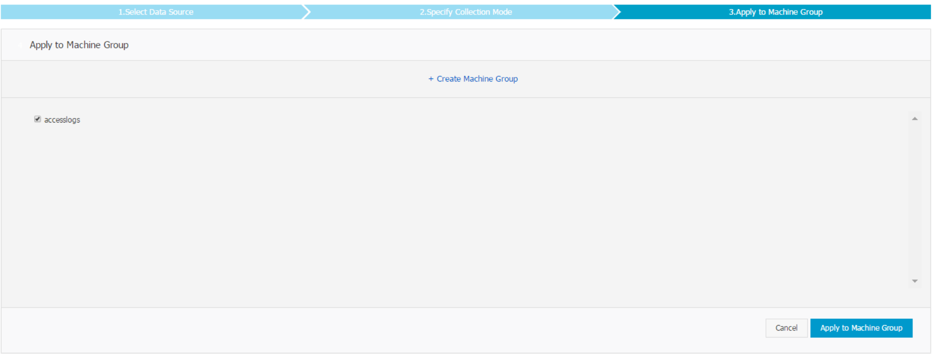
* Extraction Results:

Key	Value
ip	1.1.1.1
time	[10/Apr/2017:21:28:23 +0800
method	GET
useragent	/test HTTP/1.1" 0.282 511 200 55 "" "Httpful/0.2.1.0 (eURL/7.15.5 PHP/

The Key/Value pairs generated by regular expressions. The names (Key) of the Key/Value pairs are specified by users. If you do not use the system time, you must specify a Key/Value pair named as "time".

Apply the configuration to a machine group.

Note: If no machine group is available, you must first create a machine group.



Apply to Machine Group

☑ accesslogs

Note:

- It can take up to 3 minutes for the Logtail configuration to take effect.
- If you need to collect IIS access logs, you must first refer to the IIS Log collection best practices to configure IIS.

Use API to write logs

Log Service provides the RESTful API to help write logs. You can use the API’ s PostLogStoreLogs interface to write data. For complete API references, refer to API Reference.

Use SDKs to write logs

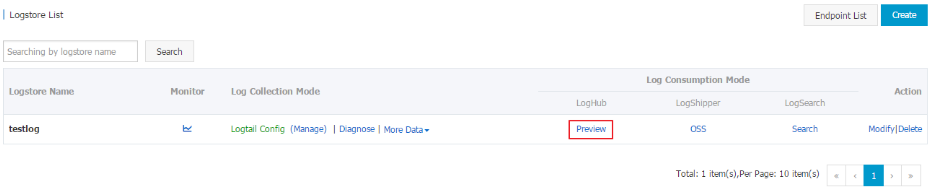
In addition to APIs, Log Service also provides SDKs in multiple languages (Java, .NET, PHP, and Python) to facilitate log writes. For a complete SDK reference, refer to SDK Reference.

4 Consume logs

Log service provides various ways to consume your collected logs, including previewing, querying, shipping logs to other products.

4.1 Preview logs

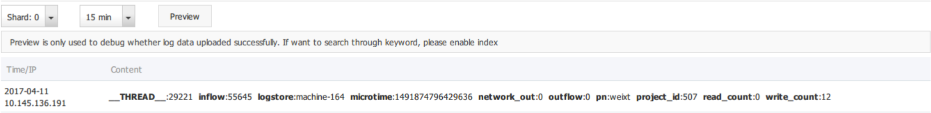
After you collect log data through Log Service, you can preview the collected logs. By specifying the Shard ID and time, you can preview the first 10 packets.



Logstore Name	Monitor	Log Collection Mode	Log Consumption Mode			Action
			LogHub	LogShipper	LogSearch	
testlog		Logtail Config (Manage) | Diagnose | More Data	Preview	OSS	Search	Modify|Delete

Total: 1 item(s),Per Page: 10 item(s)

In the following example, the preview Shard ID is 0 and the time range is the first 10 packets from the previous 15 minutes.



Shard: 0

15 min

Preview is only used to debug whether log data uploaded successfully. If want to search through keyword, please enable index

Time/IP	Content
2017-04-11 10.145.136.191	**__THREAD__**:29221 **inflow**:55645 **logstore**:machine-164 **microtime**:1491874796429636 **network_out**:0 **outflow**:0 **pn**:weixt **project_id**:507 **read_count**:0 **write_count**:12

API log consumption

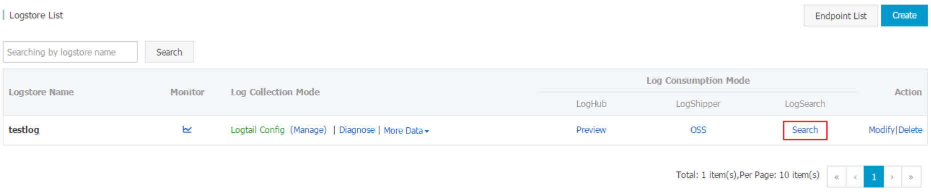
Similar to log writing, API also provides log consumption interfaces GetCursor and PullLogs. For a complete API reference, refer to API Reference.

SDK log consumption

In addition to APIs, Log Service also provides SDKs in multiple languages (Java, .NET, PHP, and Python) that allow you to easily consume logs. For a complete SDK reference, refer to Log Service SDKs.

4.2 Query logs

After you collect log data in Log Service, you can click **Search** in the Log Consumption Mode column to go to the query interface.

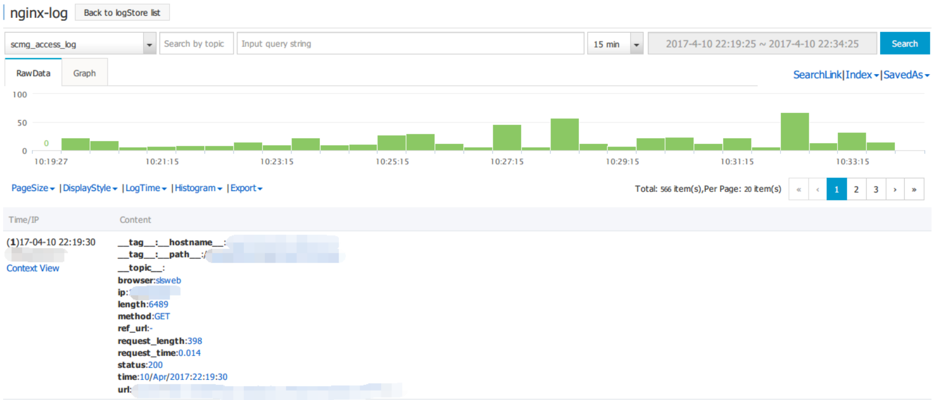


Logstore Name	Monitor	Log Collection Mode	Log Consumption Mode			Action
			LogHub	LogShipper	LogSearch	
testlog		Logtail Config (Manage) | Diagnose | More Data	Preview	OSS	Search	Modify|Delete

Total: 1 item(s),Per Page: 10 item(s)

Queries are performed by the specified log topic (at present, only logs written using API have topics), keyword, or time. In the histogram, green indicates that the data are precise during this time period, and yellow indicates the data are imprecise. You can click on or drag the yellow portion to perform further queries. Imprecise log data will not be returned in “Match Logs” .

In the following example, the query conditions are blank and the time range is set to the previous 15 minutes.



scmg_access_log

15 min

2017-4-10 22:19:25 ~ 2017-4-10 22:34:25

Total: 566 item(s),Per Page: 20 item(s)

Time/IP	Content
(1)17-04-10 22:19:30 [redacted]	**__tag__:__hostname__**:[redacted] **__tag__:__path__**:/[redacted] **__topic__**: **browser**:slsweb **ip**:[redacted] **length**:6489 **method**:GET **ref_url**:- **request_length**:398 **request_time**:0.014 **status**:200 **time**:10/Apr/2017:22:19:30 **url**:[redacted]

Use APIs to query logs

Similar to log writing, API also provides the log query interfaces GetLogs and GetHistograms. For a complete API reference, refer to API Reference.

Use SDKs to query logs

In addition to APIs, Log Service also provides SDKs in multiple languages (Java, .NET, PHP, and Python) that allow for easy log querying. For a complete SDK reference, refer to Log Service SDKs.

4.3 Ship logs to OSS (with EMR computing)

Prepare the OSS environment.

In order to ship logs in Log Service to OSS, you must first prepare an OSS environment as explained in the following process.

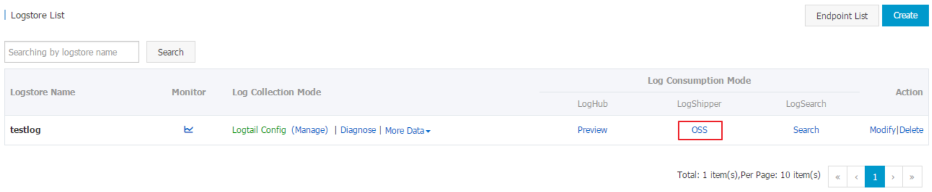
Activate the OSS service.

Create an OSS bucket and perform the relevant authorization operations.

> **Note:** The OSS bucket should be in the same region as the Log Service Project. Data can only be shipped to OSS buckets in the same region as the Log Service project.

Create OSS shipping rules.

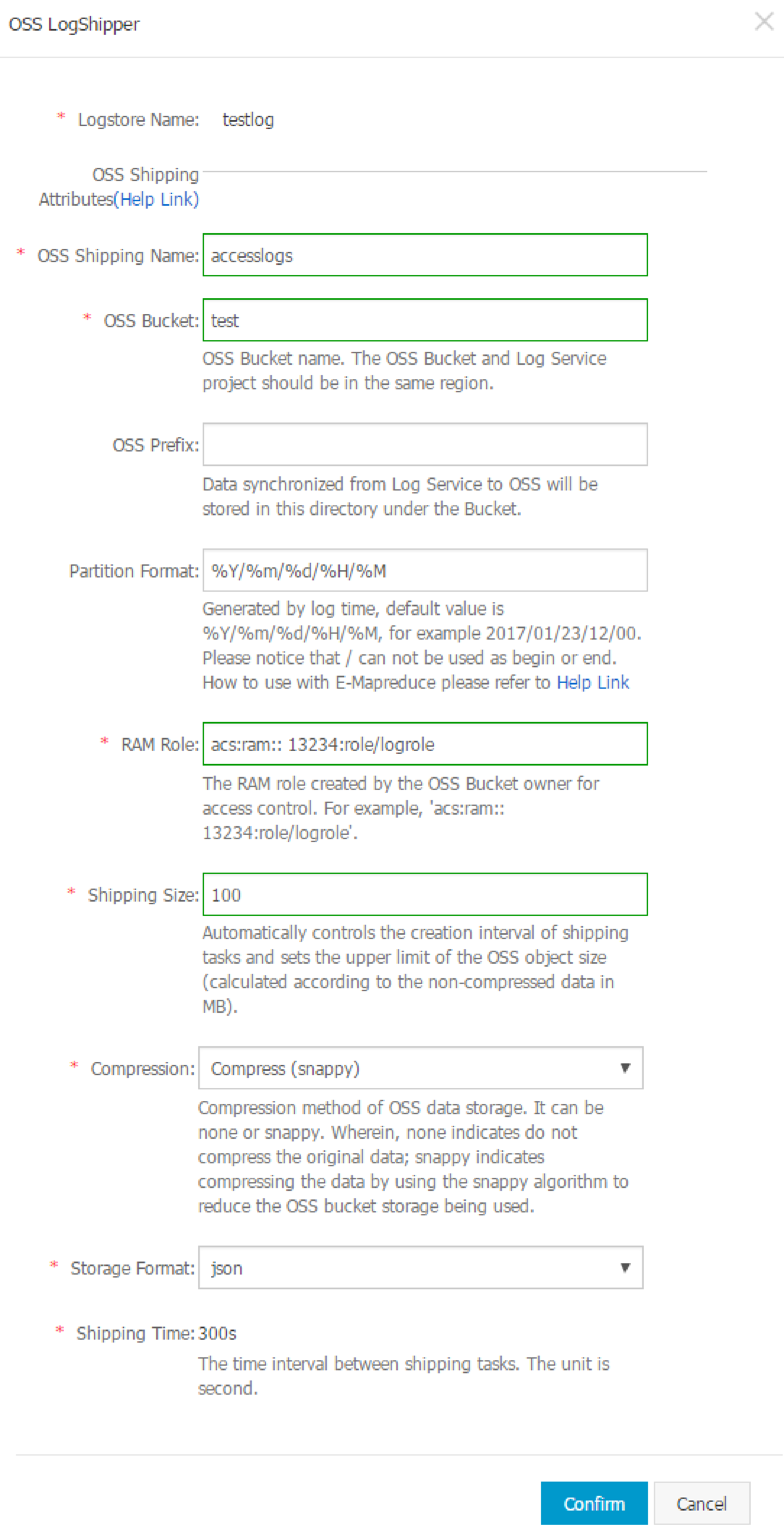
Log Service provides the function to ship log data to OSS. In the Logstore list, click **OSS** in the Log Consumption Mode column, and then click **Enable** to set the OSS shipping rules.



Logstore Name	Monitor	Log Collection Mode	Log Consumption Mode			Action
			LogHub	LogShipper	LogSearch	
testlog		Logtail Config (Manage) | Diagnose | More Data	Preview	OSS	Search	Modify|Delete

Total: 1 item(s),Per Page: 10 item(s)

You must specify the OSS bucket to post to, the permission console role name (ARN), whether or not the data are compressed, and other attributes.



OSS LogShipper

* Logstore Name: testlog

OSS Shipping Attributes(Help Link)

* OSS Shipping Name: accesslogs

* OSS Bucket: test

OSS Bucket name. The OSS Bucket and Log Service project should be in the same region.

OSS Prefix:

Data synchronized from Log Service to OSS will be stored in this directory under the Bucket.

Partition Format: %Y/%m/%d/%H/%M

Generated by log time, default value is %Y/%m/%d/%H/%M, for example 2017/01/23/12/00. Please notice that / can not be used as begin or end. How to use with E-Mapreduce please refer to Help Link

* RAM Role: acs:ram:: 13234:role/logrole

The RAM role created by the OSS Bucket owner for access control. For example, 'acs:ram:: 13234:role/logrole'.

* Shipping Size: 100

Automatically controls the creation interval of shipping tasks and sets the upper limit of the OSS object size (calculated according to the non-compressed data in MB).

* Compression: Compress (snappy)

Compression method of OSS data storage. It can be none or snappy. Wherein, none indicates do not compress the original data; snappy indicates compressing the data by using the snappy algorithm to reduce the OSS bucket storage being used.

* Storage Format: json

* Shipping Time: 300s

The time interval between shipping tasks. The unit is second.

View OSS shipping tasks.

In the OSS shipping task management on the console, you can view the shipping task statuses. After a log has been imported, you can view its data on the OSS console. In addition, the Ship logs to OSS explains how to use the imported data.