Log Service

Quick Start

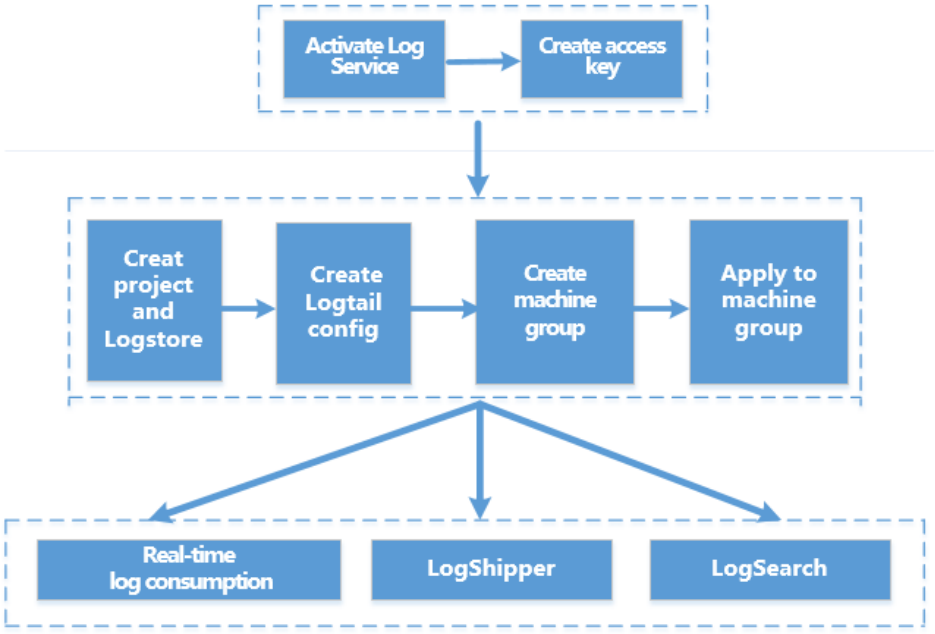
Quick Start

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 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.



Preparations

1 Activate Log Service

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

2 Create an Access Key

Access Key is a requirement for Logtail to collect logs. Before you use Log Service, create Access Key first.

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 dialog box, click **Continue to manage Access Key**. On the **Access Key Management** page, click **Create Access Key** in the upper-right corner. In the dialog box, click **Agree and create**.

Create project and Logstore

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**.

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.

Collect logs

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

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, 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.

Create a Logtail configuration.

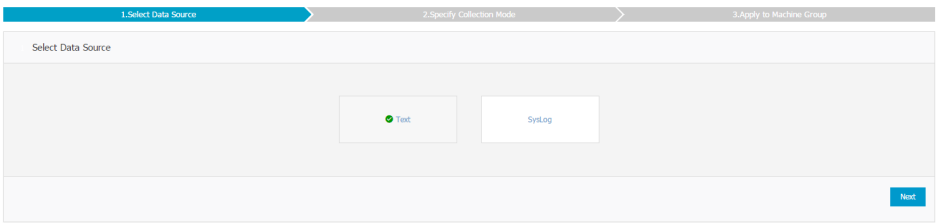
Log on to the Log Service Console. Click the Project name to enter the Logstore List. Click Logstore name to enter the Logtail Configuration List.

Click **Create** in the upper-right corner to enter the Logtail configuration process.

Logtail configuration process includes the following steps: select data source, specify collection mode, and apply to Machine Group.

Select data source.

Click to select a data source. This document was based on collecting text logs. For more information about Logtail collecting syslog, refer to Use Logtail to collect syslog.



Specify collection mode.

Specify the configuration name and log path.

Enter the configuration name, log path, and log file name. Log file name can be a full name, and support fuzzy matching at

the same time.

Specify the log collection mode.

Log Service support Simple Mode, Delimiter Mode, JSON Mode, Full Mode and Alibaba Cloud Custom Mode. This document is based on collecting logs in Delimiter Mode. For more information about collection mode, refer to Other Information.

Enter the sample log.

In Delimiter Mode or Full Mode, you need to enter the sample log. When collecting logs using Logtail, Log Service support parse the logs based on you choosen mode. If fail, you need to modify the delimiter config and regular expressions. Enter the sample log in the corresponding positions.

Specify the delimiters.

You can specify tabs, bars, spaces, or custom seperators as delimiters. Choose the corresponding delimiters based on your log format, or the Logtail will fail to parse the log.

Specify the Key in Extraction result.

After you enter the sample log and choose delimiters, Log Service extracts log fields based on your choosen delimiters, and define it as Value. You need to specify the corresponding Key for the Value.

Apply to Machine Group.

If you have not created a machine group before, create a machine group based on the page prompt, and then apply the Logtail configuration to the machine group.

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

After completing the above steps, the Log Service begins to collect logs from Ali Cloud ECS immediately. You can consume collected logs real-time on the console and API/SDK.

Note:

- It can take up to 3 minutes for the Logtail configuration to take effect.

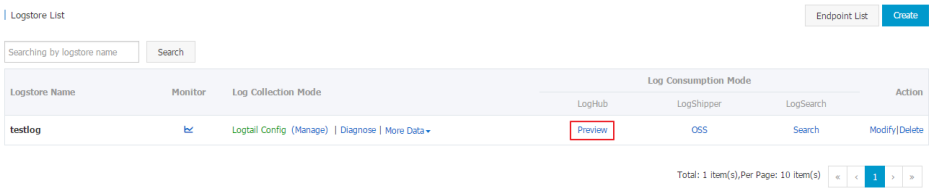
- If you need to collect IIS access logs, you must first refer to the IIS Log collection best practices to configure IIS.

Consume logs

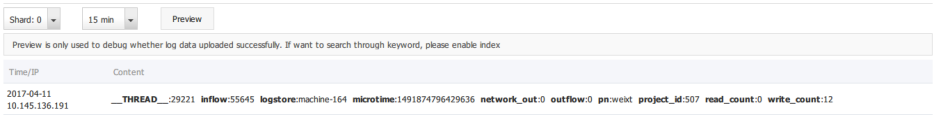
Log service provides various ways to consume your collected logs, including previewing, querying, shipping logs to other products.

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.

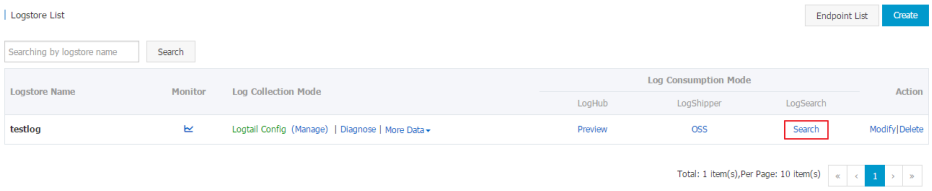


In the following example, the preview Shard ID is 0 and the time range is the first 10 packets from the previous 15 minutes.



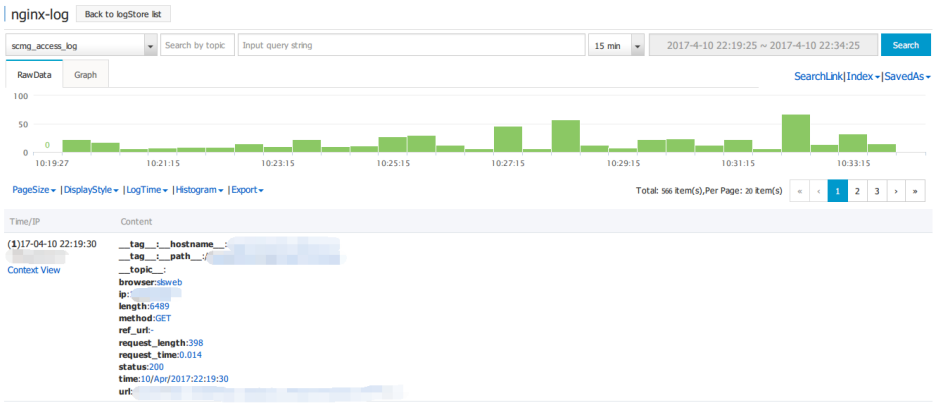
Query logs

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



Queries are performed by the specified log topic, keyword, or time. In the histogram, green indicates that the search results are precise during this time period, and yellow indicates the search results are imprecise. You can click on or drag the yellow portion to perform further queries. Imprecise search results 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.



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.

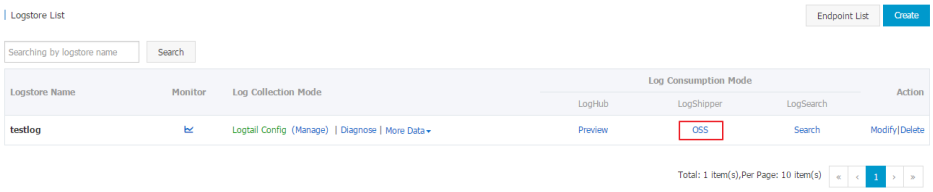
Activate the OSS service.

Create an OSS bucket and perform the relevant authorization operations.

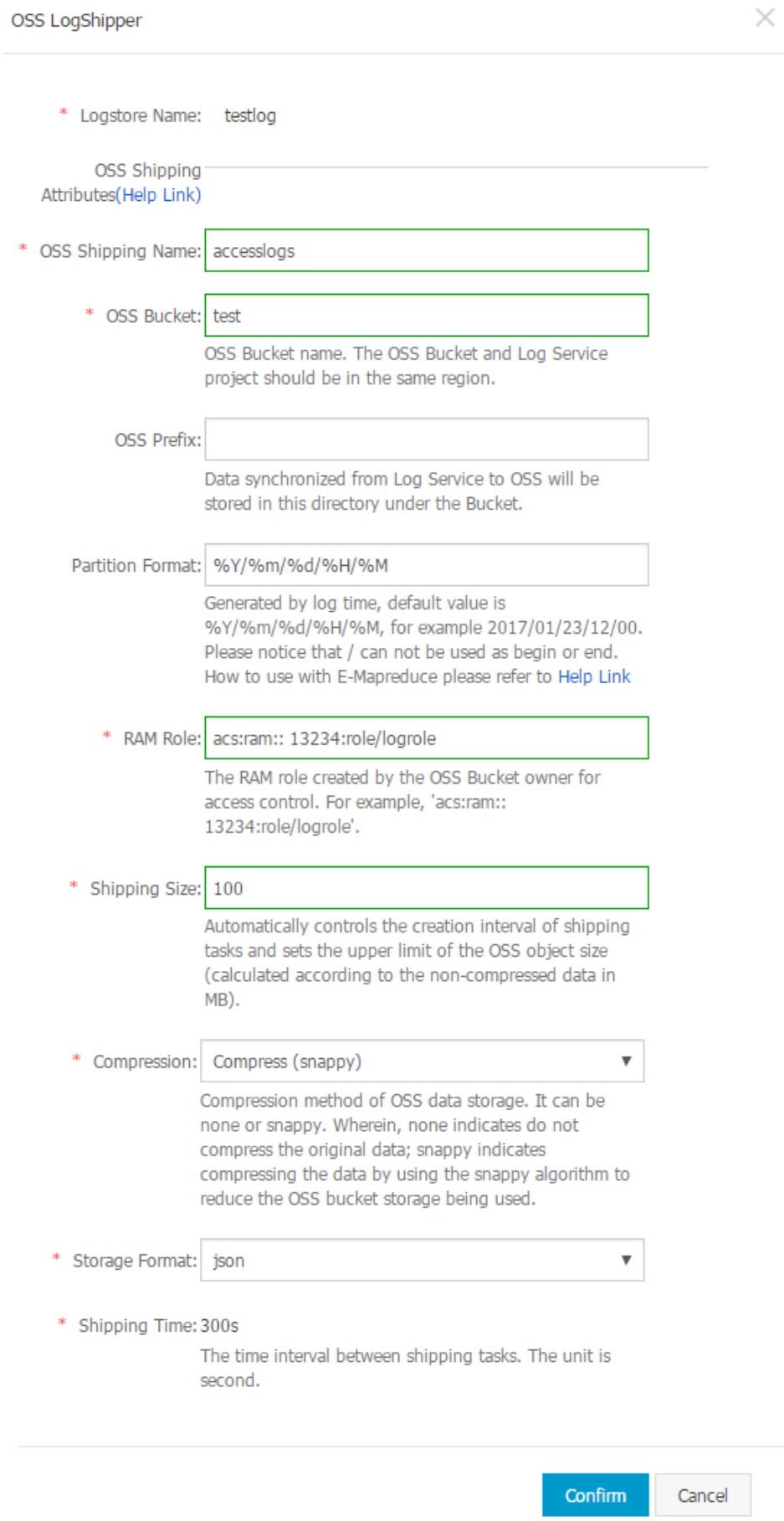
> **Note:** The OSS bucket must be in the same region as the Log Service Project. Data can only be shipped to OSS buckets in the same region as the Log Service project.

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.



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.
Confirm
Cancel

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.