

# Alibaba Cloud

Log Service  
Quick Start

Document Version: 20201231

# 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 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 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 directly contact Alibaba Cloud for any errors of this document.

# Document conventions

Style	Description	Example
 <b>Danger</b>	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 <b>Danger:</b> Resetting will result in the loss of user configuration data.
 <b>Warning</b>	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 <b>Warning:</b> Restarting will cause business interruption. About 10 minutes are required to restart an instance.
 <b>Notice</b>	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 <b>Notice:</b> If the weight is set to 0, the server no longer receives new requests.
 <b>Note</b>	A note indicates supplemental instructions, best practices, tips, and other content.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click <b>Settings</b> > <b>Network</b> > <b>Set network type</b> .
<b>Bold</b>	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click <b>OK</b> .
<code>Courier font</code>	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[ ] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

# Table of Contents

1.Quick Start	05
---------------	----

# 1. Quick Start

This topic describes how to collect logs of Alibaba Cloud Elastic Compute Service (ECS) instances in the Log Service console. This topic also describes how to query and analyze the collected logs.

## Prerequisites

- An ECS instance is available. For more information, see [ECS quick start](#).
- Logs are available on the ECS instance.

In this example, the logs are stored in the `/var/log/nginx/access.log` file and the sample log is `127.0.0.1|#|-|#|13/Apr/2020:09:44:41 +0800|#|GET /1 HTTP/1.1|#|0.000|#|74|#|404|#|3650|#|-|#|curl/7.29.0 .` **Delimiter mode** is used in this example to collect the sample log.

## Step 1: Create a project and a Logstore

1. Log on to the [Log Service console](#).
2. Create a project.
  - i. In the **Projects** section, click **Create Project**.
  - ii. In the **Create Project** dialog box, set the parameters. The following table describes the required parameters. You can use the default values for other parameters.

Parameter	Description
Project Name	The name of the project. The name must be unique in a region and cannot be modified after the project is created.
Region	The data center of the project. We recommend that you select the region where the ECS instance resides. Then, you can use the internal network of Alibaba Cloud to accelerate log collection.  After you create a project, you cannot migrate the project to another region or modify the region to which the project belongs.

- iii. Click **OK**.

3. Create a Logstore. After you create a project, you are prompted to create a Logstore.


In the **Create Logstore** dialog box, set the parameters. The following table describes the required parameters. You can use the default values for other parameters.

Parameter	Description
Logstore Name	The name of the Logstore. The name must be unique in the project to which the Logstore belongs. After the Logstore is created, the name cannot be modified.


Parameter	Description
Shards	Log Service uses shards to read and write data.  Each shard supports a write capacity of 5 MB/s and 500 times/s and a read capacity of 10 MB/s and 100 times/s. If one shard can meet your business requirements, you can set the <b>Shards</b> parameter to 1. No fees are incurred if you only create one Logstore and use one shard.
Automatic Sharding	If you enable this feature, Log Service increases the number of shards if the number of read and write requests exceeds the capacity of the existing shards.  You can turn off the <b>Automatic Sharding</b> switch if the existing number of shards can meet your business requirements.

## Step 2: Collect logs



1. In the **Import Data** section, select **Delimiter Mode - Text Log**.
2. Select the project and Logstore that you have created and click **Next**.
3. Install Logtail.
  - i. On the **ECS Instances** tab, select the destination ECS instance and click **Execute Now**.
  - ii. Confirm that the **Execution Status** is **Success** and click **Complete Installation**.
4. Create an IP address-based machine group and click **Next**. The following table describes the required parameters. You can use the default values for other parameters.

Parameter	Description
Name	The name of the machine group. The name must be unique in a project and cannot be modified after the machine group is created.
IP addresses	The IP address of the ECS instance. Separate multiple IP addresses with line feeds.  <div>  <b>Notice</b> Windows and Linux servers cannot be added to the same machine group.         </div>

5. Select and move the destination machine group from **Source Server Groups** to **Applied Server Groups**, and then click **Next**.

 **Notice** If you want to apply a machine group immediately after it is created, the heartbeat status of the machine group may be **FAIL**. This is because the machine group has not been connected to Log Service. In this case, you can click **Automatic Retry**. If the problem persists, see [What can I do if the Logtail client has no heartbeat?](#)

6. Create a Logtail configuration file and click **Next**. The following table describes the required parameters. You can use the default values for other parameters.

Parameter	Description
Config Name	The name of the Logtail configuration file. The name must be unique in a project and cannot be modified after the file is created.
Log Path	<p>The directory and name of the log file.</p> <p>The file names can be complete names or names that contain wildcards. For more information, visit <a href="#">Wildcard matching</a>. The log files in all levels of subdirectories under a specified directory are monitored if the log files match the specified pattern. Examples:</p> <ul style="list-style-type: none"> <li>◦ <code>/apsara/nuwa/.../*.log</code> indicates that the files whose extension is <code>.log</code> in the <code>/apsara/nuwa</code> directory and its subdirectories are monitored.</li> <li>◦ <code>/var/logs/app_*/*.log</code> indicates that each file that meets the following conditions is monitored: The file name contains <code>.log</code>. The file is stored in a subdirectory (at all levels) of the <code>/var/logs</code> directory. The name of the subdirectory matches the <code>app_*</code> pattern.</li> </ul> <div> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>◦ By default, each log file can be collected by using only one Logtail configuration file.</li> <li>◦ You can include only asterisks (*) and question marks (?) as wildcard characters in the log path.</li> </ul> </div>
Log Sample	<p>Enter a valid sample log entry that is collected from an actual scenario. Example:</p> <pre>127.0.0.1 # - # 13/Apr/2020:09:44:41 +0800 # GET /1 HTTP/1.1 # 0.000 # 74  # 404 # 3650 # - # curl/7.29.0</pre>
Delimiter	<p>Select a delimiter based on the log format. Example: <code> # </code>.</p> <div> <p> <b>Note</b> If you select <b>Hidden Characters</b> as the quote, you must enter a character in the following format: <code>0xthe hexadecimal ASCII code of the non-printable character</code>. For example, to use the non-printable character whose hexadecimal ASCII code is 01, you must enter <code>0x01</code>.</p> </div>
Extracted Content	Log Service extracts the log content based on the specified sample log and delimiter. The extracted log content is delimited into values. You must specify a key for each value.

Click **Next** to complete the configuration and use Logtail to collect logs.

**Note**

- The Logtail configurations require at most 3 minutes to take effect.
- If an error occurs when you use Logtail to collect logs, see [Diagnose collection errors](#).

7. Preview the data and click **Next**. By default, Log Service enables the Full Text Index to query and analyze logs. For more information, see [Enable and configure the index feature for a Logstore](#).

**Note**

- The index is applicable only to the log data that is newly written.
- To query and analyze logs, you must enable the Full Text Index or Field Search. If you enable both of them, the settings of Field Search prevail.

## Step 3: Query and analyze logs

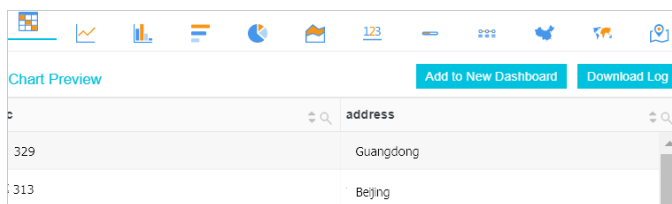
1. In the **Projects** section, click the project in which you want to query and analyze logs.
2. On the **Log Storage > Logstores** tab, click the Logstore where logs are stored.
3. Enter a query statement in the search box, set a time range, and then click **Search & Analyze**. Example: You can run the following query statement to view the location of IP addresses of the previous day. You can also display the query result on a chart.

- Query statement

```
* | select count(1) as c, ip_to_province(remote_addr) as address group by address limit 100
```

- Query result

The following figure shows that 329 IP addresses were located in Guangdong province and 313 IP addresses were located in Beijing on the previous day. Log service allows you to display the query result on a chart. For more information, see [Chart overview](#).



	address
329	Guangdong
313	Beijing

## What to do next

- Ship logs: You can ship collected logs to Object Storage Service (OSS), MaxCompute, and other storage or computing services. For more information, see [LogShipper](#).
- Consume logs: You can consume collected logs. For more information, see [Log consumption](#).
- Data transformation: You can perform multiple operations on the collected logs. For example, you can standardize, enrich, distribute, and aggregate the collected logs. For more information, see [Data transformation](#).