ALIBABA CLOUD

Alibaba Cloud

Log Service

Quick Start

Document Version: 20201110

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.

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
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.
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.
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 list --instanceid` *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.Quick start

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

Prerequisites

- An Alibaba Cloud account is created and real-name verification is passed. For more information, see Sign up with Alibaba Cloud.
- Log Service is activated.

  When you log on to the Log Service console for the first time, you must activate Log Service as prompted.
- An ECS instance is available in the region where you want to create a project. For more information, see Create an ECS instance.

Step 1: Create a project and a Logstore

Before you collect logs, you must 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 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.
Description	The description of the project.
Region	The region to which the project belongs. We recommend that you select a region based on the log source. For example, to collect logs of ECS instances, you can select the region where the ECS instances reside. 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. For more information about the endpoints of different regions, see Endpoints.

   iii. Click **OK**.
3. Create a Logstore.After you create a project, you are prompted to create a Logstore. The following table describes the parameters that you can specify when you create a Logstore.

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.
WebTracking	Specifies whether to enable web tracking. If you enable this feature, Log Service collects logs from web browsers and mobile apps that run on iOS or Android. This feature is disabled by default.
Permanent Storage	Specifies whether to enable permanent storage. If you enable this feature, Log Service permanently stores the collected logs. This feature is disabled by default. **Note** If you call the API to set the data retention period to 3650, the data is permanently saved.
Data Retention Period	The retention period of the collected logs. If you disable the **Permanent Storage** feature, you must specify the **Data Retention Period** parameter. Valid values: 1 to 3000. Unit: days. Logs are automatically deleted after the specified data retention period expires.
Shards	Select the number of shards in the Logstore. You can create up to 10 shards for each Logstore. You can create up to 200 shards for each project.
Automatic Sharding	Specifies whether to enable automatic sharding. If you enable this feature, Log Service increases the number of shards if the number of read and write requests exceed the capacity of the existing shards. This feature is enabled by default. For more information, see Manage shards.
Maximum Shards	The maximum number of shards. This parameter is required if you enable the **Automatic Sharding** feature. Maximum value: 64.
Log Public IP	Specifies whether to enable the log public IP feature. If you enable this feature, Log Service adds the following information to the tag field of the collected logs: ◦ __client_ip__: the public IP address of the log source. ◦ __receive_time__: the time when Log Service receives the log. The time is a UNIX timestamp.

Step 2: Collect logs

This section describes how to collect delimiter-separated values (DSV) formatted logs.

1. In the **Import Data** section, select **Delimiter Mode - Text Log**.
2. In the **Specify Logstore** step, select the project and Logstore, and then click **Next**. You can also click **Create Now** to create a project and a Logstore.
3. In the **Create Machine Group** step, create a machine group.
   - If a machine group is available, click **Using Existing Machine Groups**.
   - This section uses ECS instances as an example to describe how to create a machine group. To

create a machine group, perform the following steps:

a. Install Logtail on ECS instances. For more information, see Install Logtail on ECS instances.

If Logtail is installed on the ECS instances, click **Complete Installation**.

> **Note** If you need to collect logs from user-created clusters or servers of third-party cloud service providers, you must install Logtail on these servers. For more information, see Install Logtail in Linux or Install Logtail in Windows.

b. After the installation is complete, click **Complete Installation**.

c. On the page that appears, specify the parameters for the machine group. For more information, see Create an IP address-based machine group or Create a custom ID-based machine group.

4. In the **Machine Group Settings** step, apply the configurations to the machine group.Select the created machine group and move it from **Source Server Groups** to **Applied Server Groups**.

5. In the **Logtail Config** step, create a Logtail configuration file. The following table describes the parameters in the Logtail configuration file.

Parameter	Description
Config Name	The name of the Logtail configuration file. After you create the Logtail configuration file, you cannot modify the name of the file. You can also click **Import Other Configuration** to import a Logtail configuration file from another project.
Log Path	Specify the directory and names of the log files. The file names can be complete names or names that contain wildcards. For more information, visit Wildcard matching. The log files in all levels of subdirectories under a specified directory are monitored if the log files match the specified pattern. Examples: ◦ */apsara/nuwa/ ... /*.log* indicates that the files whose extension is *.log* in the */apsara/nuwa* directory and its subdirectories are monitored. ◦ */var/logs/app_* ... /*.log** indicates that each file that meets the following conditions is monitored: The file name contains *.log*. The file is stored in a subdirectory (at all levels) of the */var/logs* directory. The name of the subdirectory matches the *app_** pattern. **Note** ◦ Each log file can be collected by using only one Logtail configuration file. ◦ You can include only asterisks (*) and question marks (?) as wildcard characters in the log path.

Parameter	Description
Docker File	Specifies whether the Logtail configuration file is a Docker file. If it is a Docker file, you can configure the log path and container tags. Logtail monitors the creation and destruction of containers, and collect logs of the specified containers based on the tags. For more information, see Use the console to collect Kubernetes text logs in DaemonSet mode.
Blacklist	Specifies whether to enable the blacklist feature. After you enable this feature, you can configure the blacklist in the **Add Blacklist** field. You can configure a blacklist to skip the specified directories or files when you collect logs. The directories and files in the blacklist support exact match and wildcard match. Examples: ◦ If you select **Filter by Directory** from the Filter Type drop-down list and enter */tmp/mydir* in the Content column, all files in the directory are skipped. ◦ If you select **Filter by File** from the Filter Type drop-down list and enter */tmp/mydir/file* in the Content column, only the specified file is skipped.
Mode	Select a mode. **Delimiter Mode** is selected by default. For information about other modes, see Overview.
Sample Log	Enter a sample log. The delimiter mode applies only to single-line logs.
Delimiter	Select a delimiter based on the log format. Otherwise, Log Service may fail to parse logs. **Note** If you select **Hidden Characters** as the delimiter, you must enter the character in the following format: `0x`*the hexadecimal ASCII code of the non-printable character*. For example, to use the non-printable character whose hexadecimal ASCII code is 01, you must enter 0x01.
Quote	Select a quote based on the log format. Otherwise, Log Service may fail to parse logs. **Note** If you select **Hidden Characters** as the quote, you must enter the character in the following format: `0x`*the hexadecimal ASCII code of the non-printable character*. For example, to use the non-printable character whose hexadecimal ASCII code is 01, you must enter 0x01.
Extracted Content	Specify the key and value of the 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.

Parameter	Description
Incomplete Entry Upload	Specifies whether to upload incomplete log entries. The switch indicates whether to upload a log entry whose number of parsed fields is less than the number of the specified keys. If you enable this feature, the log entry is uploaded. Otherwise, the log entry is dropped. For example, if you set the delimiter to the vertical bar (|), the log entry 11|22|33|44|55 is parsed into the following fields: 11, 22, 33, 44, and 55. You can set the keys to A, B, C, D, and E, respectively. ◦ If you enable the **Incomplete Entry Upload** feature, 55 is uploaded as the value of the D key when Log Service collects the log entry 11|22|33|55. ◦ If you disable the **Incomplete Entry Upload** feature, Log Service drops the log entry because the fields and keys do not match.
Use System Time	◦ Specifies whether to use the system time. If you enable the **Use System Time** feature, the timestamp of a log entry is the system time of the server when the log entry is collected. ◦ If you disable the **Use System Time** feature, you must find the value that indicates the time in the **Extracted Content** and configure a key named time for the value. Specify the value and then click **Auto Generate** in the **Time Conversion Format** field to automatically parse the time. For more information, see Time formats.
Drop Failed to Parse Logs	◦ Specifies whether to drop logs that fail to parse. If you enable the **Drop Failed to Parse Logs** feature, logs that fail to parse are not uploaded to Log Service. ◦ If you disable the **Drop Failed to Parse Logs** feature, raw logs are uploaded to Log Service if the raw logs fail to parse.
Maximum Directory Monitoring Depth	Enter the maximum depth at which the specified log directory is monitored. Valid values: 0 to 1000. The value 0 indicates that only the directory specified in the log path is monitored.

You can configure advanced options based on your business requirements. We recommend that you do not modify the settings. The following table describes the parameters in the advanced options.

Parameter	Description
Enable Plug-in Processing	Specifies whether to enable the Logtail processing feature. If you enable this feature, Logtail is used to process logs. For more information, see Process data.
Upload Raw Log	Specifies whether to upload raw logs. If you enable this feature, raw logs are written to the __raw__ field and uploaded together with the parsed logs.

Parameter	Description
Topic Generation Mode	○ **Null - Do not generate topic**: This mode is selected by default. In this mode, the topic field is set to an empty string. You do not need to enter a topic to query logs. ○ **Machine Group Topic Attributes**: This mode is used to differentiate logs that are generated by different servers. ○ **File Path Regex**: In this mode, you must configure a regular expression in the **Custom RegEx** field. The part of a log path that matches the regular expression is used as the topic name. This mode is used to differentiate logs that are generated by different users or instances.
Log File Encoding	○ utf8: indicates that UTF-8 encoding is used. ○ gbk: indicates that GBK encoding is used.
Timezone	The time zone where logs are collected. Valid values: ○ System Timezone: This option is selected by default. It indicates that the time zone where logs are collected is the same as the time zone to which the server belongs. ○ Custom: Select a time zone.
Timeout	The timeout period of log files. If a log file is not updated within the specified period, Logtail considers the file to be timed out. Valid values: ○ Never: All log files are continuously monitored and never time out. ○ 30 Minute Timeout: If a log file is not updated within 30 minutes, Logtail considers the file to be timed out and no longer monitors the file. If you select **30 Minute Timeout**, you must specify the **Maximum Timeout Directory Depth** parameter. Valid values: 1 to 3.
Filter Configuration	The filter conditions that are used to collect logs. Only logs that match the specified filter conditions are collected. Examples: ○ Collect logs that meet a condition: Specify the filter condition to Key:level Regex:WARNING|ERROR if you need to collect logs of only the WARNING or ERROR severity level. ○ Filter out logs that do not meet a condition: ■ Specify the filter condition to Key:level Regex:^(?!. *(INFO|DEBUG)). * if you need to filter out logs of the INFO or DEBUG severity level. ■ Specify the filter condition to Key:url Regex:. *^(?!.*(healthcheck)). * if you need to filter out logs whose URL contains the keyword healthcheck. For example, logs of which the value of the url key is /inner/healthcheck/jiankong.html are not collected. For more examples, visit regex-exclude-word and regex-exclude-pattern.

6. In the **Configure Query and Analysis** step, configure the indexes.Indexes are configured by default. You can re-configure the indexes based on your business requirements. For more

information, see Enable and configure the index feature for a Logstore.

> Note
> - You must configure Full Text Index or Field Search. If you configure both of them, the settings of Field Search prevail.
> - If the data type of the index is long or double, the case sensitive and delimiter settings are unavailable.

After you complete the preceding steps, you can use Log Service to collect logs of the ECS instances.

> Note
> - It may require three minutes for the Logtail configurations to take effect.
> - For more information about how to resolve Logtail errors, see Diagnose collection errors.

Step 3: Query and analyze logs

You can use query statements to query and analyze logs in real time after logs are collected to Log Service.

1. In the **Projects** section, click the destination project.
2. Choose **Log Management > Logstores**, and then click the destination Logstore.
3. Enter a query statement in the search box, set a time range, and then click **Search & Analyze**.
   - Log Service provides the contextual query, saved search, quick analysis, and reindexing features. For more information, see Query syntax.
   - Log Service provides multiple types of charts to visualize analysis results. For more information, see Analysis graph.
   - Log Service allows you to create dashboards that display data analysis results. For more information, see Dashboard.

What to do next

- Ship logs: You can ship collected logs to Object Storage Service (OSS), MaxCompute, E-MapReduce (EMR),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.