

Alibaba Cloud Elastic Container Instance

Logging and monitoring

Issue: 20200525









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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

Style	Description	Example
	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.
	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.
	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.
	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 <code>cd /d C:/window</code> command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
{ } or {a b}	This format is used for a required value, where only one item can be selected.	switch {active stand}

Contents

Legal disclaimer.....	I
Document conventions.....	I
1 Log collection.....	1
2 Use Log Service to collect container logs from an ECI.....	7

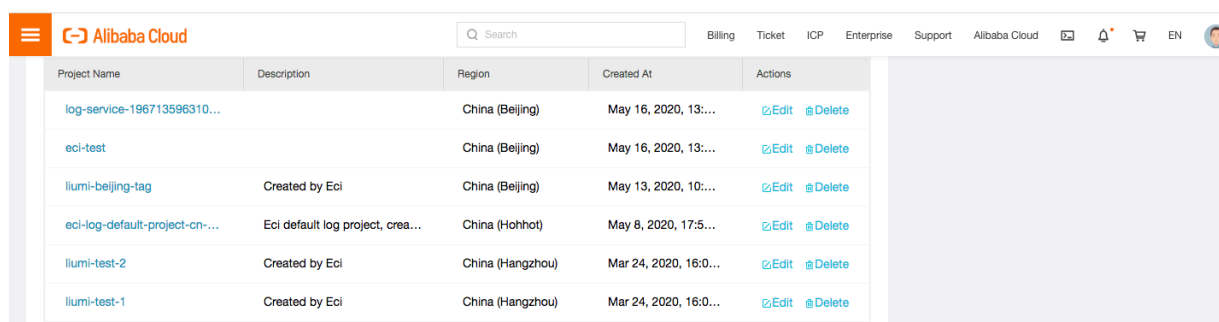
1 Log collection

Enable ECI logging

ECI supports the log collection service. When you create an ECI through OpenAPI Explorer, set `SlsEnable` to `true`, and then enable ECI log collection. By default, the standard output and error logs of your ECI containers are collected to the Logstore of Log Service under your account. You do not need to manually configure any settings. The results are as follows:

Default project

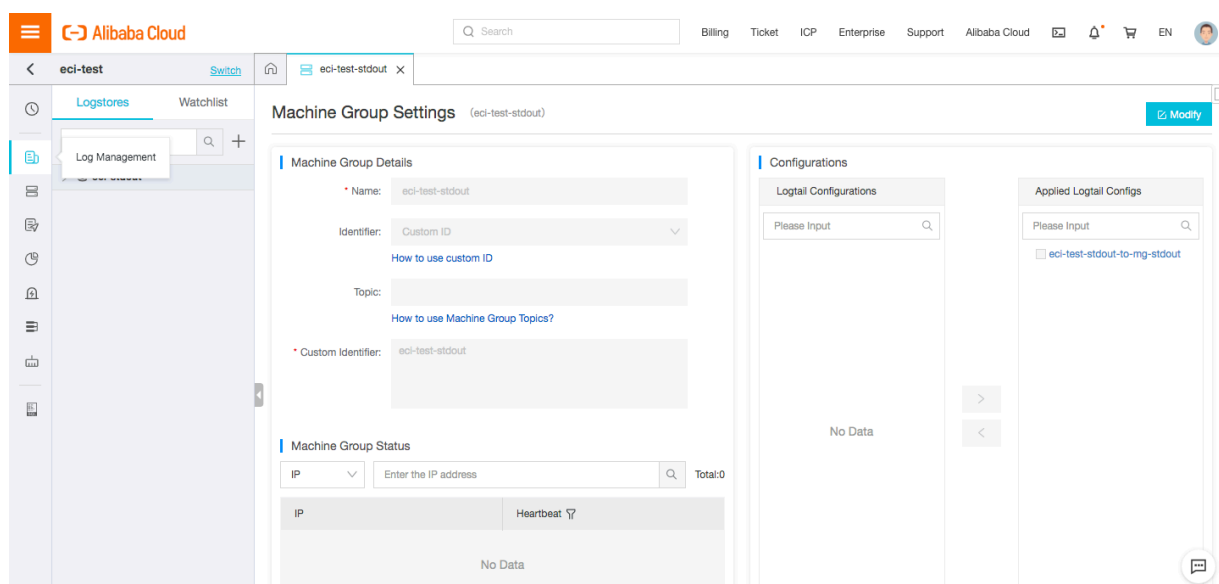
Projects starting with `eci-log-default-project-` are default projects created by the system (a default project is created for each region).



Project Name	Description	Region	Created At	Actions
log-service-196713596310...		China (Beijing)	May 16, 2020, 13:...	Edit Delete
eci-test		China (Beijing)	May 16, 2020, 13:...	Edit Delete
ilumi-beijing-tag	Created by Eci	China (Beijing)	May 13, 2020, 10:...	Edit Delete
eci-log-default-project-cn...	Eci default log project, crea...	China (Hohhot)	May 8, 2020, 17:5...	Edit Delete
ilumi-test-2	Created by Eci	China (Hangzhou)	Mar 24, 2020, 16:0...	Edit Delete
ilumi-test-1	Created by Eci	China (Hangzhou)	Mar 24, 2020, 16:0...	Edit Delete

Logstore

The default Logstore starts with `eci-log-default-log-store-`. It stores standard output and error logs of ECIs and can meet the needs of most scenarios.

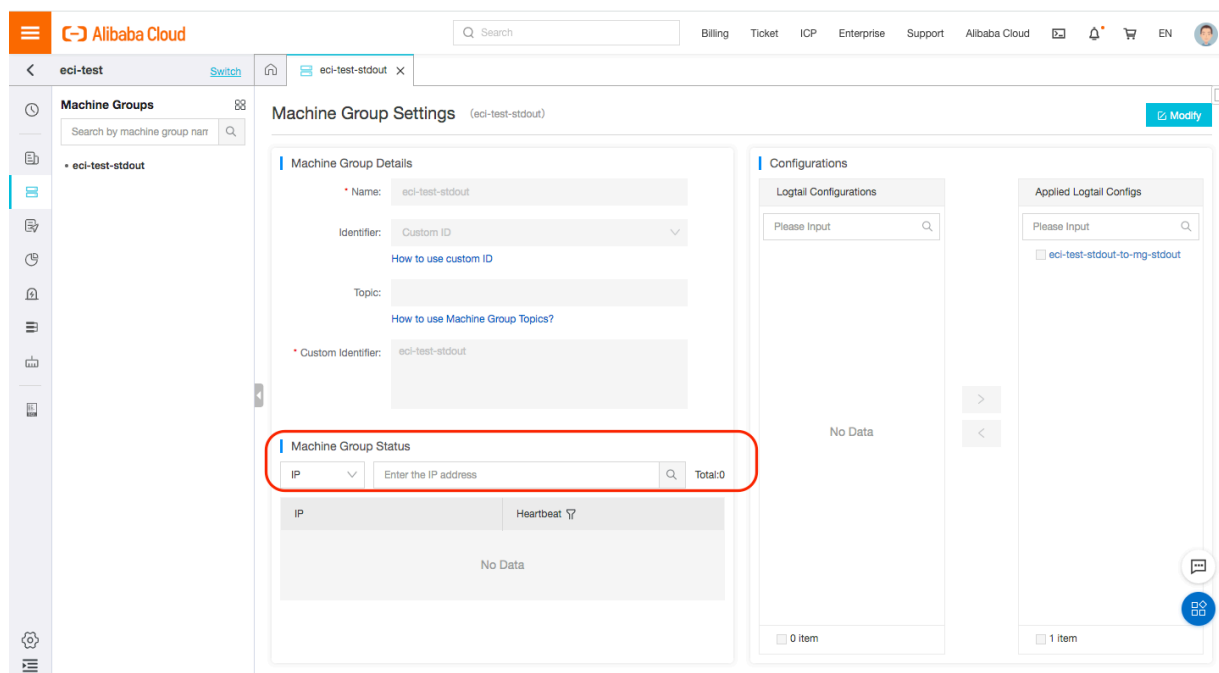


The screenshot shows the 'Machine Group Settings' page for a machine group named 'eci-test-stdout'. The page is divided into several sections:

- Machine Group Details:** Includes fields for Name (eci-test-stdout), Identifier (Custom ID), Topic, and Custom Identifier (eci-test-stdout). There are links for 'How to use custom ID' and 'How to use Machine Group Topics?'. Below this is a 'Machine Group Status' section with a search bar and a table showing IP addresses and heartbeat status. The table currently shows 'No Data'.
- Configurations:** Includes a 'Logtail Configurations' section with a search bar and a 'No Data' message. There is also an 'Applied Logtail Configs' section with a search bar and a checkbox for 'eci-test-stdout-to-mg-stdout'.

Machine group

The default machine group starts with eci-log-default-machine-group. If you enable the log collection service, ECIs are added to the default machine group. You can view the ECIs added to the machine group by checking the status of the machine group.



Configuration

The default Logtail configuration starts with eci-log-default-config. By default, the Logtail configuration is generated in simple mode. To configure advanced settings, log on to the console and customize settings.

Results

The preceding configurations are all default configurations and can meet the needs of most scenarios.

Customize settings

Although the ECI service predefines basic settings, you may still need to customize some settings. By default, all ECIs are added to the default machine group of the default project. All logs are collected to the default Logstore. You may want to customize settings when you need to collect ECI logs to a custom Logstore for other projects, and add ECIs to different machine groups for different applications and services. In this case, you can customize the settings using the following two methods.

Customize the settings in the Log Service console (API)

You can log on to the Log Service console to create projects, logstores, and machine groups. Create a custom configuration for the Logstore and apply it to a selected machine group. Logs data is then collected to the new Logstore. Different configurations cannot be applied to the same log file. When you use the new Logstore, delete the default Logstore and configuration. Otherwise, log collection fails.

If the configuration in the Log Service console is too complicated to you, you can create and configure it using the ECI service.

Customize settings by using the ECI service

The ECI service can generate all default settings for you and allows you to customize the settings. For example, you can customize the project name, Logstore name, machine group name, and log collection directory. You can use environment variables of **the first container** in ECI to pass parameters in the following format:

Project name

Optional. By default, the system automatically creates an ECI project for you. If the project name is not specified, then the default name is used. If a specific name is used, the project with the specified name is created. If the project is already created, logStore and config are created and added to this project.

```
-name: aliyun_logs_project  
-value: {project name}
```

Project name constraint

- The name can only contain lowercase letters, digits, and hyphens (-).
- The name must start and end with a lowercase letter or digit.
- The name must be 3 to 63 characters in length.



Notice:

Invalid names are ignored and the default name will be used.

Logstore

Optional. A default Logstore is automatically created to store the standard output logs of the ECI containers. If this parameter is set, the ECI service will not generate a default value. Logs are collected to the specified Logstore. The ECI service creates or modifies configurations and applies them to the corresponding machine group.

**Notice:**

If you have not set a volume log directory (see the following section), the custom log directory must be a subdirectory of `var/log/eci /`.

```
-name: aliyun_log_logstore_{Logstore name} or aliyun_logs_{Logstore name}
-value: {Logging path}
```

Logstore name constraint

- The name can contain lowercase letters, digits, hyphens (-), and underscores (_).
- The name must start and end with a lowercase letter or digit.
- The name must be 3 to 63 characters in length.

**Notice:**

Invalid names are ignored and the default name will be used.

Set the number of shards in the Logstore

For more information about shards, see [Shard](#).

Parameter settings

```
-name: aliyun_logs_{Logstore name}_shard
-value: {shard value}
```

Default value: 2. Valid values: 1 to 10.

Set the log retention period for the Logstore.

Parameter settings

```
-name: aliyun_logs_{Logstore name}_ttl
-value: {ttl value}
```

Default value: 90. Valid values: 1 to 3650.

*** Machine group name**

Optional. By default, ECIs are added to the default machine group created by the system.

One region corresponds to one ECI. You can also choose to add ECIs to other machine groups that have already been created or to be created. Machine groups are helpful if you want to configure different log collection settings for applications and services deployed on different ECIs. The collection format is set as follows:

```
-name: aliyun_logs_machinegroup
```

```
-value: {Machine group name}
```

Machine group name constraint

- The machine group name can contain only letters, digits, hyphens (-), and underscores (_).
- The name must start and end with a lowercase letter or digit.
- The name must be 3 to 63 characters in length.



Notice:

The system will ignore any invalid names and use the default name instead.

Collect user volume logs

By default, the system configures standard output and error logs for users, and collects and saves data into the default Logstore. In addition to basic logs, the system also collects user volume logs. User volume log collection is relatively flexible, and the corresponding collection directory needs to be set by users.

The standard output of ECI containers is logged in directory `var/log/eci/*/*`.log. By default, ECI automatically configures the directory for users. In most cases, a user does not need to change this directory.

The standard log collection directory of an ECI volume is a subdirectory under the directory where the volume is mounted, depending on your settings.

For example, `EmptyDirVolume` is mounted to the `/pod/data/` directory of the container. The log file of the volume can be a file in any subdirectory under `/pod/data/`. In this way, you can adjust the mounting directory and define a directory that best suits your needs.

Create EmptyDirVolume

```
'Volume.1.Name': 'default-volume',  
'Volume.1.Type': 'EmptyDirVolume',
```

Mount the volume to the container directory

```
'Container.1.VolumeMount.1.Name': 'default-volume',  
'Container.1.VolumeMount.1.MountPath': '/pod/data/',  
'Container.1.VolumeMount.1.ReadOnly': False,
```

Configure a Logstore

'aliyun_log_logstore_Store' is the directory used to store standard output of an ECI container, and 'aliyun_log_logstore_Store2' is a directory used to store volume logs. It can match any file under the /pod/data/ directory.

```
'Container.1.EnvironmentVar.1.Key': 'aliyun_log_logstore_Store',  
'Container.1.EnvironmentVar.1.Value': '/var/log/eci/*/*.log',  
# 'Container.1.EnvironmentVar.1.Key': 'aliyun_log_logstore_Store',  
# 'Container.1.EnvironmentVar.1.Value': 'stdout',  
'Container.1.EnvironmentVar.2.Key': 'aliyun_log_logstore_Store2',  
'Container.1.EnvironmentVar.2.Value': '/pod/data/*/*. *',
```

**Notice:**

When you set environment variables, note that stdout is equivalent to /var/log/eci/*/*.log.

Effect

As shown in the following figure, create a file under the mount directory of the volume, and then enter content.

Open the corresponding Logstore. The content has been automatically collected by the Logstore.

**Notice:**

- The log project must be in the same region as the ECI. Otherwise, the default ECI project is used.
- If you do not define a Logstore by using ECI environment variables, the system configures the ECI standard output and error log collection settings for you. If you defined your own Logstore by using ECI environment variables, the system will not configure the ECI standard output and error log collection settings.
- The number of log collection directories is unlimited. However, a file in a machine group cannot be referenced in the Logtail configuration of multiple Logstores (it is not allowed no matter the file is explicitly specified or fuzzy matched). Otherwise, the collection fails. If the log collection fails, you must modify the configuration in the Log Service console.
- Currently, only EmptyDirVolume logs can be collected.

2 Use Log Service to collect container logs from an ECI

Prerequisites:

- The virtual-kubelet node is deployed in the target Kubernetes cluster. Note that a serverless Kubernetes cluster is embedded with the virtual-kubelet node.
- Log Service is enabled for the Kubernetes cluster.

Collect container logs from an ECI

You can use environment variables to specify collection configurations and custom tags for a container. Then, you can use the volumes and volumeMounts fields to configure a volume and the directory to which the volume is mounted based on the log collection configuration. The following configuration file of a simple pod shows how to use environment variables to specify collection configurations and custom tags for a container:

```
apiVersion: v1
kind: Pod
metadata:
  name: say-hello
spec:
  containers:
    - image: registry.cn-beijing.aliyuncs.com/dzf/busybox:1.28.3
      imagePullPolicy: IfNotPresent
      name: busybox
      command: ["/bin/sh","-c","while true; do echo $(date) hello logfile. >> /var/log/sayhi.log echo $(date) hello,stdout.>>1 ; sleep 10; done"]
      env:
        - name: aliyun_logs_log-stdout
          value: stdout
        - name: aliyun_logs_log-varlog
          value: /var/log/*.log
        - name: aliyun_logs_appname_tags
          value: appname=say-hello
        - name: aliyun_logs_version_tags
          value: version=1.28.3
      volumeMounts:
        - name: volumn-sls-sayhi
          mountPath: /var/log
  volumes:
    - name: volumn-sls-sayhi
      emptyDir: {}
```

Note: A Logstore name cannot contain underscores (_). You can use hyphens (-) instead.

Use environment variables to specify **collection configurations** and **custom tags**. All environment variables related to log collection must be prefixed with `aliyun_logs_`.

Specify the following configurations in order based on your needs:

1. Logstore

```
- name: aliyun_logs_{Logstore name}  
  value: {Log path}
```

In the preceding example, two environment variables are used to specify collection configurations. The `aliyun_logs_log-stdout` environment variable instructs the system to create a Logstore named `log-stdout`, which collects the standard output of the container.

2. Custom tags

```
- name: aliyun_logs_{Tag name without underscores (_) }_tags  
  value: {Tag name}={Tag value}
```

After a custom tag is specified, it is automatically appended to certain log fields when logs from the specified container are collected.

3. Path for collecting log files other than the standard output

If you specify a path for collecting log files other than the standard output, you need to add the `volumeMounts` field. In the preceding example, the `.log` files in the `/var/log` directory are to be collected. Therefore, the `volumeMounts` field is added, where `mountPath` is set to `/var/log`.

For more information about the advanced configurations of environment variables, see the [Advanced configurations](#) section in [Use Log Service to collect Kubernetes logs](#).