

Alibaba Cloud Application Real-time Monitoring Service

FAQ

Issue: 20200305

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, consequent

ial, 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.
<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>

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

Contents

Legal disclaimer	I
Document conventions	I
1 General FAQ	1
1.1 FAQ about usage.....	1
1.2 Access the console with a RAM user.....	2
1.3 FAQ about starting and stopping monitoring jobs.....	3
1.4 FAQ about billing.....	4
2 Application Monitoring FAQ	5
2.1 How do I uninstall the ARMS agent?.....	5
2.2 What should I do if the data of my application with the OpenFeign component is incomplete in ARMS?.....	8
2.3 FAQ about installing the ARMS agent for Java applications with one click.....	9
2.4 FAQ about installing the ARMS agent for applications on ECS instances with one click.....	9
2.5 FAQ about installing the ARMS agent for Java applications.....	11
2.6 Install ARMS Agent for applications in open-source Kubernetes environments.....	14
2.7 FAQ about updating the ARMS agent for Java applications.....	15
2.8 How can I change the name of a Java application without reinstalling the ARMS agent?.....	15
3 Browser Monitoring FAQ	20
3.1 FAQ about browser monitoring.....	20
3.2 Script error causes and solutions.....	21
4 FAQ	25
4.1 Failed to create an application for monitoring.....	25
4.2 An error occurred when a RAM user visited the Application Details page.....	25

1 General FAQ

1.1 FAQ about usage

This topic lists FAQ about Application Real-Time Monitoring Service (ARMS) usage and provides solutions.

1. How long is ARMS report data retained on a server?

By default, the data is retained for six months.

2. Does ARMS support monitoring of other data sources than logs?

Currently, ARMS supports both logs and Message Queue (MQ) data as data sources.

3. How long is the delay on reports in ARMS?

The delay on the statistical computing is within 10 seconds, as long as there is no delay on the log channel. For example, if you customize a report to count how many times a log field appears in ARMS. The data as of 12:10:00 in UTC will be collected before 12:10:10 in UTC.

4. Besides viewing reports in the ARMS console, can I retrieve the data in a report with an API operation?

Yes, you can call QueryDataset to retrieve data in a report.

5. Does ARMS modify or remove log files on my local machine?

No. The StarAgent client that ARMS uses only performs the read operation on the files on your machine according to your configurations. It does not modify the files in any way.

6. Is the real-time computing engine JStorm that is used by ARMS directly available for customers?

Currently, JStorm is not directly available for customers. This is because ARMS is significantly optimized in terms of performance and Quality of Service (QoS) for JStorm. However, we may provide the optimized JStorm interface for your direct use later.

7. Is the columnar storage of ARMS directly available for customers?

No, Currently, only RESTful APIs are supported for retrieving data. This is, again, because our storage method is optimized accordingly.

1.2 Access the console with a RAM user

Application Real-Time Monitoring Service (ARMS) supports Resource Access Management (RAM) of Alibaba Cloud. This topic explains how to authorize a RAM user to access ARMS.

Prerequisites

If you use a RAM user to access the ARMS console, the user must meet the following conditions:

- AccessKey ID and AccessKey Secret are created for this RAM user.
- The console logon function is enabled for this user, and the logon username and password are set for this user.

For the instructions, see [#unique_6](#).

Authorize a RAM user to access the ARMS console

In addition to the preceding prerequisites, the RAM user must be authorized before using the ARMS console. Currently, a RAM user can only be granted with full access to ARMS resources.



Note:

Currently, a RAM user cannot access ARMS resources by calling API operations.

The procedure is as follows:

1. Log on to the RAM console and select a RAM user to be authorized on the RAM Roles page. For instructions, see [#unique_7](#).
2. On the Policies page, select AliyunARMSFullAccess.

After the authorization is completed, you can log on to the ARMS console as the RAM user.

1.3 FAQ about starting and stopping monitoring jobs

This topic lists FAQ about starting and stopping monitoring jobs, and provides solutions.

How do I disable the Application Real-Time Monitoring Service (ARMS) agent?

If you want to stop monitoring an application, you can disable the ARMS agent for this application. If you want to resume monitoring of the application by using the ARMS agent, you can enable the ARMS agent again for this application. The procedure is as follows:

- 1. In the ARMS console, choose Applications from the left-side navigation pane.**
- 2. On the Applications page, find the application for which you want to stop billing and click its name.**
- 3. On the Application Overview page, choose Application Settings from the left-side navigation pane.**
- 4. On the Application Settings page, click the Customize Config tab. On the tab page that appears, disable the ARMS agent in the Agent Switch Settings section. Then, ARMS stops monitoring this application.**

How do I disable browser monitoring?

If you want to disable browser monitoring for an application, delete the target application from the monitored application list. Deletion is irreversable. Be cautious when performing this operation. Perform the following steps to disable browser monitoring:

- 1. In the ARMS console, choose Browser Monitoring from the left-side navigation pane.**
- 2. In the application list, find the target application and click Settings in the Actions column.**
- 3. On the Application Settings page, click the Other Settings tab.**
- 4. On the Other Settings tab, click Delete Site. In the Confirmation dialog box, click OK. Then, ARMS stops monitoring this application.**

If you want to stop monitoring all applications, see [Billing management](#).

1.4 FAQ about billing

This topic lists FAQ about billing and provides solutions.

How do I view my bill?

For pay-as-you-go services, you can view your bill as follows:

- 1. In the top navigation bar, choose Billing Management.**
- 2. In the left-side navigation pane, click Back to Old Version.**
- 3. On the Expenses Center page, choose Purchases Record > Purchases Details.**
- 4. On the Consumption Details page, select the filtering criteria such as Product, Payment Status, and by billCycled, and click Query. Your bill is displayed.**

How do I view the usage of my resource package?

If you have bought a resource package, you can view the usage of your resource package as follows:

- 1. View the resource package overview.**
 - a. On the Expenses Center page, choose Resource Packages > Resource Packages Overview from the left-side navigation pane.**
 - b. On the Resource Packages Overview page, select the filtering criteria such as Product, Resource Package, and Effective Period, and then click Search. An overview of your resource package is displayed.**
- 2. View the usage details of your resource package.**
 - a. On the Expenses Center page, choose Resource Packages > Usage from the left-side navigation pane.**
 - b. On the Usage page, select the filtering criteria such as Product, Resource Package, Resource Package ID, and Usage Period, and then click Search. The usage details of your resource package are displayed.**

2 Application Monitoring FAQ

2.1 How do I uninstall the ARMS agent?

When you no longer need Application Real-Time Monitoring Service (ARMS) to monitor your applications, you can uninstall the ARMS agent installed on the applications. After the ARMS agent is uninstalled from an application, ARMS stops monitoring the application. This topic describes how to uninstall the ARMS agent from Java and PHP applications.

Uninstall the ARMS agent installed in common mode

In common mode, you need to manually install the ARMS agent for a Java application. For more information, see [#unique_12](#).

1. If you no longer need ARMS to monitor your Java application, you can delete the `AppName` and `LicenseKey` parameters added in [Step 8](#) in the "Install the ARMS agent for Java applications."
2. Restart the Java application.

Uninstall the ARMS agent installed in quick mode

In quick mode, the ARMS agent is installed for the Java application by using a script with one click. For more information, see [#unique_13](#).

1. If you no longer need ARMS to monitor your Java application, you can run the `jps -l` command to view all processes and find the process ID of `com.alibaba.mw.arms.apm.supervisor.daemon.Daemon` in the command output. In this example, the process ID of `com.alibaba.mw.arms.apm.supervisor.daemon.Daemon` is 62857.

```
→ ~ jps -l
62800 org.apache.catalina.startup.Bootstrap
62857 com.alibaba.mw.arms.apm.supervisor.daemon.Daemon
5411
62799 org.jetbrains.jps.cmdline.Launcher
67809 sun.tools.jps.Jps
```

2. Run the `kill -9 <process ID>` command, for example, `kill -9 62857`.

3. Run the `rm -rf /.arms /root/.arms` command.
4. Restart your application.

Uninstall the ARMS agent from the Java application on the ECS instance

1. If you no longer need ARMS to monitor your Java application, you can run the `jps -l` command to view all processes and find the process ID of `com.alibaba.mw.arms.apm.supervisor.daemon.Daemon` in the command output. In this example, the process ID of `com.alibaba.mw.arms.apm.supervisor.daemon.Daemon` is 62857.

```
→ ~ jps -l
62800 org.apache.catalina.startup.Bootstrap
62857 com.alibaba.mw.arms.apm.supervisor.daemon.Daemon
5411
62799 org.jetbrains.jps.cmdline.Launcher
67809 sun.tools.jps.Jps
```

2. Run the `kill -9 <process ID>` command, for example, `kill -9 62857`.
3. Run the `rm -rf /.arms /root/.arms` command.
4. Restart your application.

Uninstall the ARMS agent from the Java application in a Container Service Kubernetes cluster

If you no longer need ARMS to monitor the Java application in the Container Service Kubernetes cluster, you can uninstall the ARMS agent as follows:

1. In the left-side navigation pane, choose Applications > Releases.
2. On the Releases page, click the Helm tab, and select the cluster from which the ARMS agent needs to be uninstalled in the Cluster list.
3. Select the release name `arms-pilot` of the ARMS agent, and click Delete in the Actions column.
4. In the Delete Application dialog box, click OK.
5. Restart your business pod.

Uninstall the ARMS agent from the Java application in an open-source Kubernetes environment

- 1. If you no longer need ARMS to monitor the Java application in the open-source Kubernetes environment, you can run the following command to uninstall arms-pilot:**

```
helm del --purge arms-pilot
```

- 2. Restart your business pod.**

Uninstall the ARMS agent from the Java application in Docker

- 1. If you no longer need ARMS to monitor the Java application in the Docker cluster, you can delete the *Dockerfile* content edited in [Step 1](#) in the "Install the ARMS agent for Java applications."**
- 2. Run the `docker build` command to construct an image.**
- 3. Run the `docker run` command to start the image.**

Uninstall the ARMS agent from a common PHP application

If you no longer need ARMS to monitor your PHP application, you can uninstall the ARMS agent as follows:

- 1. Delete the following four lines from the *php.ini* file:**

```
[arms]
extension=<php_extension_dir>/arms.so
arms.trace_exception=true
arms.config_full_name=/<php-agent-dir>/arms-agent.conf
```

- 2. Restart your PHP application.**

Uninstall the ARMS agent from the PHP application in a Container Service Kubernetes cluster

If you no longer need ARMS to monitor the PHP application in the Container Service Kubernetes cluster, you can uninstall the ARMS agent as follows:

- 1. In the left-side navigation pane, choose Applications > Releases.**
- 2. On the Releases page, click the Helm tab, and select the cluster from which the ARMS agent needs to be uninstalled in the Cluster list.**
- 3. Select the release name arms-pilot of the ARMS agent, and click Delete in the Actions column.**
- 4. In the Delete Application dialog box, click OK.**

5. Restart your business pod.

2.2 What should I do if the data of my application with the OpenFeign component is incomplete in ARMS?

After your application with the OpenFeign component is connected to ARMS, if the data is incomplete and the data of downstream applications cannot be viewed, a possible cause is as follows:

- Hystrix is enabled for the OpenFeign component by default. Hystrix uses an asynchronous RxJava framework, which is not supported by ARMS.
- The OpenFeign component uses the HttpURLConnection request class of JDK. Due to restrictions of the ARMS instrumentation mechanism, this class is often intercepted because the loading time is too early, and thus the request fails. To solve this problem, you should use the OkHttp request class.

You can disable Hystrix and enable the OkHttp request class to solve this problem as follows:

1. Add the following dependencies to the pom.xml file:

```
<!-- OKHttp supports Feign -->
<dependency>
  <groupId>io.github.openfeign</groupId>
  <artifactId>feign-okhttp</artifactId>
</dependency>
```

2. Add the following content to the Spring Cloud configuration file:

```
feign.okhttp.enabled: true
feign.hystrix.enabled: false
```

3. Configure OkHttp.

```
@Configuration
@ConditionalOnClass(Feign.class)
@AutoConfigureBefore(FeignAutoConfiguration.class)
public class FeignClientOkHttpConfiguration {

    @Bean
    public OkHttpClient okHttpClient() {
        return new OkHttpClient.Builder()
            // The connection times out.
            .connectTimeout(20, TimeUnit.SECONDS)
            // The response times out.
            .readTimeout(20, TimeUnit.SECONDS)
            // The write request times out.
            .writeTimeout(20, TimeUnit.SECONDS)
            // Indicates whether to enable automatic reconnection.
            .retryOnConnectionFailure(true)
    }
}
```

```
        // The connection tool.  
        .connectionPool(new ConnectionPool())  
        .build();  
    }
```

2.3 FAQ about installing the ARMS agent for Java applications with one click

This topic lists FAQ about installing the Application Real-Time Monitoring Service (ARMS) Agent for Java applications with one click, and provides solutions.

What can I do when getcwd errors are reported after I run the script to access a Java application?

If the following error message is returned after you run the script for one-click Java application access:

```
shell-init: error retrieving current directory: getcwd: cannot access  
parent directories: No such file or directory Error occurred during  
initialization of VM java.lang.Error: Properties init: Could not  
determine current working directory. at java.lang.System.initProper  
ties(Native Method) at java.lang.System.initializeSystemClass(System.  
java:1119)
```

A possible cause is that you have deleted the current directory when running the script. To solve this problem, run the `cd` command and then run the script again.

Where can I view logs after installing the ARMS agent with one click?

The logs are stored in the following directory by default: `/root/.arms/supervisor/logs/arms-supervisor.log`. If no logs are found in this directory, run the `ps -ef | grep arms` command to check the log directory.

2.4 FAQ about installing the ARMS agent for applications on ECS instances with one click

This topic lists FAQ about installing the Application Real-Time Monitoring Service (ARMS) agent for applications on Elastic Compute Service (ECS) instances with one click, and provides solutions.

What can I do when the ARMS agent cannot be installed?

- 1. Make sure that you can access the ARMS agent download link in the region where your ECS instance is located.**

```
First, make sure that you can access the public network on your ECS  
instance and the ARMS agent download link in the region where your  
ECS instance is located.
```

```
# China (Hangzhou)
http://arms-apm-hangzhou.oss-cn-hangzhou.aliyuncs.com/install.sh
# China (Shanghai)
http://arms-apm-shanghai.oss-cn-shanghai.aliyuncs.com/install.sh
# China (Qingdao)
http://arms-apm-qingdao.oss-cn-qingdao.aliyuncs.com/install.sh
# China (Beijing)
http://arms-apm-beijing.oss-cn-beijing.aliyuncs.com/install.sh
# China (Shenzhen)
http://arms-apm-shenzhen.oss-cn-shenzhen.aliyuncs.com/install.sh
# Singapore
http://arms-apm-ap-southeast.oss-ap-southeast-1.aliyuncs.com/
cloud_ap-southeast-1/install.sh
```

2. Make sure that you can access the ARMS console on your ECS instance.

```
# Mainland China
https://arms.console.aliyun.com/
# Singapore
https://arms-ap-southeast-1.console.aliyun.com
```

3. Log on to the [ECS console](#) and check the following items:

- a. In the left-side navigation pane, choose Cloud Assistant.
- b. On the Cloud Assistant page, select Command in the search box, and enter the `InstallJavaAgent` command.



Note:

If no result is returned, contact Customer Services of ARMS.

- c. On the Cloud Assistant page, enter the ID of the `InstallJavaAgent` command in the search bar of the Tasks section. In the results that are returned, find the target record and click View Results in the Actions column to check whether the `InstallJavaAgent` command is executed successfully. If not, troubleshoot the problem based on the detailed execution results. For example, if the ECS disk is full or the ARMS agent is not installed, you can clean up the disk or install the ARMS agent. If the problem persists, submit the detailed execution results to Customer Services of ARMS.

Why is the ECS instance process information inaccurate after the ARMS agent is installed?

After you install the ARMS agent, if no ECS instance process information is displayed or the ECS instance process information is inaccurate, click - and then + on the left of the ECS instance. If the problem persists, contact Customer Services of ARMS.

What can I do if I cannot enable ARMS for a process on the ECS instance?

On the ECS instance, check whether the `/root/.arms/supervisor/logs/arms-supervisor.log` file contains error logs. If it does, troubleshoot the problem according to the error message. If the problem persists, contact Customer Services of ARMS.

2.5 FAQ about installing the ARMS agent for Java applications

This topic lists FAQ about installing the Application Real-Time Monitoring Service (ARMS) agent for Java applications, and provides solutions.

Is the ARMS agent compatible with agents of other Application Performance Management (APM) products, such as Pinpoint?

The ARMS agent is incompatible with agents of other APM products. Most APM technologies use the Automatic Storage Management (ASM) framework for bytecode instrumentation. If you install two agents, your code instrumentation will be implemented twice. Code instrumentation varies with manufacturers and code conflicts may cause serious performance issues. We do not recommend that you install multiple APM agents at the same time.

What can I do if `OutOfMemoryError` is reported upon startup of an application after the ARMS agent is installed?

In this case, add the corresponding JVM heap memory parameter as appropriate.

If the initial value of heap memory size (`Xms`) is 512 MB and the maximum value of heap memory size (`Xmx`) is 2 GB, the configuration items are as follows: Adjust the values according to the actual requirement. In other environments such as Tomcat, add this parameter to `JAVA_OPTS` of the configuration file.

```
-Xms512M  
-Xmx2048M
```

If the `OutOfMemoryError: PermGen space` error is reported, add the following parameters:

```
-XX:PermSize=256M
```

```
-XX:MaxPermSize=512M
```

How do I check the network connectivity?

When deploying the ARMS agent, you can run the Telnet command to check if the target host is connected to the ARMS server network.

Table 2-1: Endpoints of ARMS application monitoring servers

Region	Endpoint
China (Hangzhou)	arms-dc-hz.aliyuncs.com
China (Beijing)	arms-dc-bj.aliyuncs.com
China (Shanghai)	arms-dc-sh.aliyuncs.com
China (Qingdao)	arms-dc-qd.aliyuncs.com
China (Shenzhen)	arms-dc-sz.aliyuncs.com

If you created an application in the China (Shenzhen) region of ARMS, you need to test if the environment in China (Shenzhen) is connected to the ARMS server network. The following result indicates that the network is connected:

```
telnet arms-dc-sz.aliyuncs.com 8443Trying 119.23.169.12...Connected to
arms-dc-sz.aliyuncs.com.Escape character is '^']'.
```



Note:

You must replace the endpoint according to your region. The port number remains unchanged.

How do I check if the ARMS agent is successfully loaded?

- 1. Run the following ps command to check if the ARMS agent is successfully loaded according to the command line start parameter:**

```
ps -ef | grep 'arms-bootstrap'
```

When the ARMS agent is successfully loaded, the result is as follows:

- 2. The arms.licenseKey and arms.appId attributes in the command line must be consistent with those displayed on the ARMS application setting page.**

What if no data is available after the ARMS agent is loaded?

1. If the log file of the ARMS agent contains "send Agent metrics. no metrics.", verify whether your application has continuous external access requests, including HTTP requests, HSF requests, and Dubbo requests and whether the development framework is supported by the ARMS agent. For more information about third-party components and frameworks supported by the ARMS agent, see [#unique_19](#).
2. Check whether the selected time range for query is correct. Select the past 15 minutes as the query time range and check whether monitoring data is available.
3. If you start the ARMS agent by running the `-jar` command, check the setting of the command, and make sure that the `-javaagent` parameter is before `-jar`.

```
java -javaagent:/{user.workspace}/ArmsAgent/arms-bootstrap-1.7.0-SNAPSHOT.jar -Darms.licenseKey=xxx -Darms.appId=xxx -jar demoApp.jar
```

4. If the log file in the `ArmsAgent/log/` directory contains the error "LicenseKey is invalid", check whether the region of your application is the same as the region of the ARMS agent.
5. After your application is started, if the log sub-directory is unavailable in the ARMS agent directory since `arms-bootstrap-1.7.0-SNAPSHOT.jar` fails to be loaded, check whether the permission over the ARMS agent installation directory is correct.
6. If the following error is reported when your application is started, check whether the `arms-bootstrap-1.7.0-SNAPSHOT.jar` package and the corresponding permission are correct.
7. If there is still no monitoring data, pack the log file of the ARMS agent for Java applications in the `ArmsAgent/log` directory, and contact Customer Services of ARMS at DingTalk service account [@ARMS](#) for assistance.
8. Check the JDK version. If the JDK version is 1.8.0_25 or 1.8.0_31, you may fail to install the agent. We recommend that you upgrade the JDK or contact Customer Services of ARMS at DingTalk service account [@ARMS](#).

What can I do if no IP address or an incorrect IP address is displayed after the ARMS agent is successfully loaded?

1. Run the `ifconfig -a` command to check the network configuration of the current machine. If the machine uses multiple network interface controllers

(NICs), the IP address acquired by the ARMS agent is possibly not as expected, which is related to the network configuration.

2. Solve the problem by using either of the following methods:

- Configure the `-DEAGLEEYE.LOCAL.IP=10.XX.XX.XX` JVM parameter explicitly.



Note:

Replace `10.XX.XX.XX` with the actual IP address.

- Configure the ARMS agent to obtain the `-DNETWORK.INTERFACE=eth0` JVM parameter, where `eth0` indicates the NIC name.

Troubleshoot common errors contained in the log file (`ArmsAgent/log`) of the ARMS agent

- If "LicenseKey is invalid" is reported:
 1. First, make sure that your application is successfully created in ARMS and that `AppId` and `LicenseKey` were correctly set when the ARMS agent was installed.
 2. ARMS is a multi-region environment. Therefore, you also need to check whether the download link of the ARMS agent is in the same region as your application.

2.6 Install ARMS Agent for applications in open-source Kubernetes environments

This topic lists FAQ about installing ARMS Agent for applications in open-source Kubernetes environments, and provides solutions.

Why does my application not start?

Run the following command to view the `arms-pilot-system` logs and troubleshoot the problem according to the logs:

```
kubectl logs -f {arms-pilot-arms-pilot-XXX} -n arms-pilot-system
```

How can I view the logs of ARMS Agent?

On the worker of the Kubernetes cluster, view the logs in `/home/admin/.opt/ArmsAgent/logs/xxxx.log`.

2.7 FAQ about updating the ARMS agent for Java applications

This topic describes how to update the Application Real-Time Monitoring Service (ARMS) agent for monitoring Java applications in Enterprise Distributed Application Service (EDAS) and Container Service, and on other platforms.

How do I update the ARMS agent for applications in EDAS?

To update the ARMS agent for Java applications in EDAS, re-deploy the applications.

How do I update the ARMS agent for applications in Container Service?

To update the ARMS agent for applications in Container Service, restart the pods of the applications.

How do I update the ARMS agent for applications on other platforms?

To update the ARMS agent for other applications than those in EDAS and Container Service, uninstall the ARMS agent and then install it again.

To uninstall the ARMS agent, perform the following steps as needed:

- **Uninstall the ARMS agent for Java applications on Elastic Compute Service (ECS) instances**
- **Uninstall the ARMS agent for Java applications on other platforms**

Delete the parameters related to `AppName` and `LicenseKey` in the configuration file or startup script. For more information, see [#unique_12/unique_12_Connect_42_uninstall](#) .

2.8 How can I change the name of a Java application without reinstalling the ARMS agent?

When using Application Real-Time Monitoring Service (ARMS) to monitor a Java application, you may want to change the application name for some reason, for example, you may forget to change the example application name Java-Demo to a custom name. This topic describes how to change the name of a Java application without restarting the application and reinstalling the ARMS agent.

Prerequisites

The version of the ARMS agent is 2.5.8.1 or later. You can check the version in the `Version` file under the ARMS agent directory. For example, `2.5.8_cf020486_20190816150025` indicates that the ARMS agent is in version 2.5.8 and was

published on August 16, 2019. The location of the ARMS agent directory varies with the installation method. For more information, see the description below.

If the version of your ARMS agent is earlier than 2.5.8.1, reinstall it by following the uninstallation procedure. You need to rename the application in this procedure.

The ARMS agent that is downloaded later than August 20, 2019 supports this function by default.

- For more information about manual installation and uninstallation, see [#unique_12](#).
- For more information about automatic installation on an Elastic Compute Service (ECS) instance, see [#unique_23](#).
- For more information about one-click installation, see [#unique_13](#).

For common Java applications (when the ARMS agent is installed in common mode)

Common Java applications are Java applications other than those deployed on ECS instances of Alibaba Cloud. If you installed the ARMS agent in common mode, the ARMS agent directory is at the location you customized.

Change your application name as follows:

1. Run the commands for either the public network or Virtual Private Cloud (VPC) to download and decompress Supervisor.



Note:

Replace the region in the download URL with the region where your application is located.

- **Public network:**

```
wget http://arms-apm-hangzhou.oss-cn-hangzhou.aliyuncs.com/ArmsSupervisor.zip -O ArmsSupervisor.zip
unzip ArmsSupervisor.zip
```

- **VPC (applicable when the public network command fails):**

```
wget http://arms-apm-hangzhou.oss-cn-hangzhou-internal.aliyuncs.com/ArmsSupervisor.zip -O ArmsSupervisor.zip
unzip ArmsSupervisor.zip
```

2. Run the following command to change the application name:

```
cd ArmsSupervisor
```

```
./attach.sh </path/to/ArmsAgent/arms-bootstrap-1.7.0-SNAPSHOT.jar> <PID> <NewAppName> <LicenseKey>
```

- `</path/to/ArmsAgent/arms-bootstrap-1.7.0-SNAPSHOT.jar>`: **the path that points to a file with the same name of the ARMS agent.**
- `<PID>`: **the target process ID, which can be obtained with the `jps/ps` command.**
- `<NewAppName>`: **new application name.**
- `<LicenseKey>`: **LicenseKey of the application monitored by ARMS, which can be obtained from the ARMS console.**

If the standard output log of the application displays the following information, the application name is successfully changed:

For common Java applications (when the ARMS agent is installed with one click)

If you installed the ARMS Agent with one click, the ARMS agent directory is `~/.arms/supervisor/agent`. Note that the account you use must be the same as the application account.

Change your application name as follows:

1. Log on to the machine where the application is located and run the following command:

```
cd ~/.arms/supervisor
./cli.sh <LicenseKey> <NewAppName>
```

- `<LicenseKey>`: **LicenseKey of the application monitored by ARMS, which can be obtained from the ARMS console.**
- `<NewAppName>`: **new application name.**

2. Select the proper process from all Java processes.



Note:

If only one process is available, this process is selected by default.

3. Open the `~/.arms/attach.info` file, change the application name to the new name, and save the file.



Warning:

Do not add content such as redundant spaces when modifying the file.

If the standard output log of the application displays the following information, the application name is successfully changed:

For Java applications deployed on ECS instances (when the ARMS agent is installed with one click)

If your Java application is deployed on an ECS instance, the ARMS agent directory is `/.arms/agent`.

Change your application name as follows:

1. Log on to the ECS instance where your application is located and run the following command with the root account:

```
su <USER> -c "./attach.sh /.arms/agent/arms-bootstrap-1.7.0-SNAPSHOT.jar <PID> <NewAppName> <LicenseKey>"
```

- **<PID>: target process ID, which can be obtained with the `jps/ps` command.**
- **<NewAppName>: new application name.**
- **<LicenseKey>: LicenseKey of the application monitored by ARMS, which can be obtained from the ARMS console.**

2. Open the `~/.arms/attach.info` file, change the application name to the new name, and save the file.



Warning:

Do not add content such as redundant spaces when modifying the file.

If the standard output log of the application displays the following information, the application name is successfully changed:

For Java applications deployed in Kubernetes clusters of Container Service

If your Java application is deployed in a Kubernetes cluster of Container Service, change the value of `armsPilotCreateAppName` in the Deployment application and then restart the pod.

For Java applications deployed in Enterprise Distributed Application Service (EDAS)

At present, you cannot change the name of a Java application deployed in EDAS.

Result

Wait a moment after your application name is changed. No monitoring data will be reported using the old application name, and monitoring data will be reported using the new application name.

3 Browser Monitoring FAQ

3.1 FAQ about browser monitoring

This topic lists the FAQ about browser monitoring.

1. Why are asterisks (*) displayed in the name of some monitored pages or APIs?

The multi-dimensional page statistics of Application Real-Time Monitoring Service (ARMS) browser monitoring is based on the exact URL of the page opened. The asterisks (*) contained in the name of the monitored pages or APIs are not a part of a page URL. They indicate the result of URL generalization. In other words, a name that contains asterisks is not a specific URL, but a group of similar URLs.

How the URL generalization works

- **Problem: "Variables" make it difficult to monitor or analyze similar URLs with slight differences.**
- **Objective: Group similar URLs by replacing "variables" with asterisks (*).**
- **Solution: With our own URL generalization algorithm, we group similar URLs to decrease the number of URLs, while keeping as much semantic information as possible. This is done in two steps:**
 - **Aggregation: Aggregate similar URLs into one group.**
 - **"Variable" identification: Extract the "variables" from the URLs in the same group, and replace them with asterisks (*).**

The following figure show the process:

2. Why is the page view list different from the page speed list?

This is because your application is a single-page application (SPA), and the SPA auto-resolution is enabled. In the SPA application scenario, the page view and page speed are measured as follows:

- **Page view: When a hashchange event is triggered, the page view is automatically reported to record the page view of the page corresponding to the hash value.**

Therefore, when checking the page view list of an SPA application, you can see the exact page view of the hash pages.

- **Page speed:** When the hash value changes for an SPA application, the page speed doesn't change. Therefore, the page speed is not recorded on the basis of hash values, which avoids unnecessary reports while clearly reflects the page performance.

3.2 Script error causes and solutions

Script errors are common errors. However, no complete error message (error stack) is available for errors of this type. Therefore, it is difficult to troubleshoot the errors. This topic analyzes causes for script errors, provides solutions, and describes how to ignore these errors in Application Real-Time Monitoring Service (ARMS).

Causes of script errors

Script errors are also called cross-origin errors. When a website requests and executes a script hosted under a third-party domain name, a script error may occur. In most cases, a Content Delivery Network (CDN) is used to host JavaScript resources.

For an easy description, assume that the following HTML page is deployed in the `http://test.com` domain:

```
<!doctype html>
<html>
<head>
  <title>Test page in http://test.com</title>
</head>
<body>
  <script src="http://another-domain.com/app.js"></script>
  <script>
    window.onerror = function (message, url, line, column, error) {
      console.log(message, url, line, column, error);
    }
    foo(); // Call the foo method defined in app.js
  </script>
</body>
</html>
```

Assume that the `foo` method calls an undefined `bar` method:

```
// another-domain.com/app.js
function foo() {
  bar(); // ReferenceError: bar is not a function
```

```
}
```

After the page is run, the captured exception information is as follows:

```
"Script error.", "", 0, 0, undefined
```

In fact, this is not a JavaScript bug. For security purposes, the browser deliberately hides specific error messages thrown by JavaScript files of other domains to prevent sensitive information from being captured accidentally by uncontrolled third-party scripts. Therefore, only scripts in the same domain can capture specific error messages, while scripts in other domains can detect errors but cannot capture specific error messages.

For more information, see [Webkit source code](#):

```
bool ScriptExecutionContext::sanitizeScriptError(String& errorMessage
, int& lineNumber, String& sourceURL)
{
    KURL targetURL = completeURL(sourceURL);
    if (securityOrigin()->canRequest(targetURL))
        return false;
    errorMessage = "Script error.";
    sourceURL = String();
    lineNumber = 0;
    return true;
}
```

The following describes how to resolve script errors.

Solution 1: Enable Cross Origin Resource Sharing (CORS)

To capture JavaScript errors across origins, take the following steps:

1. Add the `crossorigin="anonymous"` attribute.

```
<script src="http://another-domain.com/app.js" crossorigin="
anonymous"></script>
```

This step tells the browser to obtain target scripts anonymously. This means that the browser does not send potential user identity information (for example, cookies and HTTP certificates) to the server when requesting scripts.

2. Add the cross-origin HTTP response header

```
Access-Control-Allow-Origin: *
```

or

```
Access-Control-Allow-Origin: http://test.com
```



Note:

By default, most mainstream CDNs have the `Access-Control-Allow-Origin` attribute. The following shows an example of Alibaba Cloud CDN:

```
$ curl --head https://retcode.alicdn.com/retcode/bl.js | grep -i "
access-control-allow-origin"
=> access-control-allow-origin: *
```

After completing the preceding steps, you can use `window.onerror` to capture cross-origin script error messages. In the preceding example, after the page is run again, the captured result is as follows:

```
=> "ReferenceError: bar is not defined", "http://another-domain.com/
app.js", 2, 1, [Object Error]
```

Solution 2 (optional): Use `try catch`

When it is difficult to add a cross-origin attribute to the HTTP request or response header, use `try catch`.

Add `try catch` to the preceding HTML page:

```
<!doctype html>
<html>
<head>
  <title>Test page in http://test.com</title>
</head>
<body>
  <script src="http://another-domain.com/app.js"></script>
  <script>
    window.onerror = function (message, url, line, column, error) {
      console.log(message, url, line, column, error);
    }
    try {
      foo(); // Call the foo method defined in app.js
    } catch (e) {
      console.log(e);
      throw e;
    }
  </script>
</body>
```

```
</html>
```

Run the page again. The output results are as follows:

```
=> ReferenceError: bar is not defined
    at foo (http://another-domain.com/app.js:2:3)
    at http://test.com/:15:3
=> "Script error.", "", 0, 0, undefined
```

Complete information is displayed through the console statement of `try catch`, but from `window.onerror`, only "Script error" can be captured. Using this feature, you can manually report captured exceptions in the CATCH statement.

```
// See "Browser monitoring operations" at the end of this topic.
__bl.error(error, pos);
```



Note:

Although `try catch` can be used to capture some exceptions, we recommend that you use solution 1.

How do I ignore script errors in ARMS?

Script errors are often caused by scripts in third-party domains. If the errors do not affect the running of your application, you can ignore the errors by using the `ignore` SDK parameter of ARMS browser monitoring.

The `ignore` parameter is used to ignore JavaScript errors that are reported.

The parameter value is an object that comprises three attributes: `ignoreUrls`, `ignoreApis`, and `ignoreErrors`. The default value is as follows:

```
ignore: {
  ignoreUrls: [],
  ignoreApis: [],
  ignoreErrors: []
},
```

You can only use the `ignoreErrors` attribute for script errors. The `ignoreErrors` attribute is used to ignore certain JavaScript errors that comply with a specified rule. The value can be `String`, `RegExp`, `Function` or an array composed of the three types. Example:

```
__bl.setConfig({
  ignore: {
    ignoreErrors: /^Script error\.? $/
  }
});
```

4 FAQ

4.1 Failed to create an application for monitoring

This topic lists FAQ about creating an application for monitoring and provides solutions.

In this case, a possible cause is that the number of applications that are monitored exceeds the limit. Contact us at our DingTalk account [arms160804](#).

4.2 An error occurred when a RAM user visited the Application Details page

This topic provides solutions for the error "Sorry, you do not have access to this page." that occurs when a Resource Access Management (RAM) user visits the Application Details page.

Background

The app resources that a user created belong to this user. By default, the user has full access permissions on its resources. However, in the RAM console, a new RAM user does not have access permissions to resources of an Alibaba Cloud account. The RAM user must be authorized with access permissions to resources of the Alibaba cloud account.

Procedure

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the **Policies** page, click **Create Policy**.
4. On the **Create Custom Policy** page, enter **Policy Name** and **Note**, set **Configuration Mode** to **Script**, enter **Policy Document**, and click **OK**.

- **Policy content: read-only permission**

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "emasha: View *",
      "Resource": "*"
    }
  ]
}
```

```
    ],  
    "Version": "1"  
  }
```

- **Policy content: management permission**

```
{  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "emasha:*",  
      "Resource": "*"   
    }  
  ],  
  "Version": "1"  
}
```

5. In the left-side navigation pane, choose **Identities > Users** to go to the **Users** page. Enter the user name for which permissions need to be added in the **User Logon Name** search box, and click the search icon to search for the user. After finding the user, click **Add Permissions** in the **Actions** column.
6. In the **Add Permissions** window, select **Custom Policy** under **Select Policy**, enter the name of the policy that you added in the policy text box, and then click the search icon. Select the policy you found in the **Policy Name** list on the left. Then, the policy name is displayed in the **Selected** list on the right. Click **OK**. The policy is successfully added.