

Solution

Serverless Real-Time Log Analysis

Issue 1.0.0
Date 2023-04-25



Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

| | |
|--|-----------|
| 1 Solution Overview..... | 1 |
| 2 Resource and Cost Planning..... | 3 |
| 3 Procedure..... | 5 |
| 3.1 Preparations..... | 5 |
| 3.2 Quick Deployment..... | 12 |
| 3.3 Getting Started..... | 17 |
| 3.4 Quick Uninstallation..... | 20 |
| 4 Appendix..... | 22 |
| 5 Change History..... | 23 |

1 Solution Overview

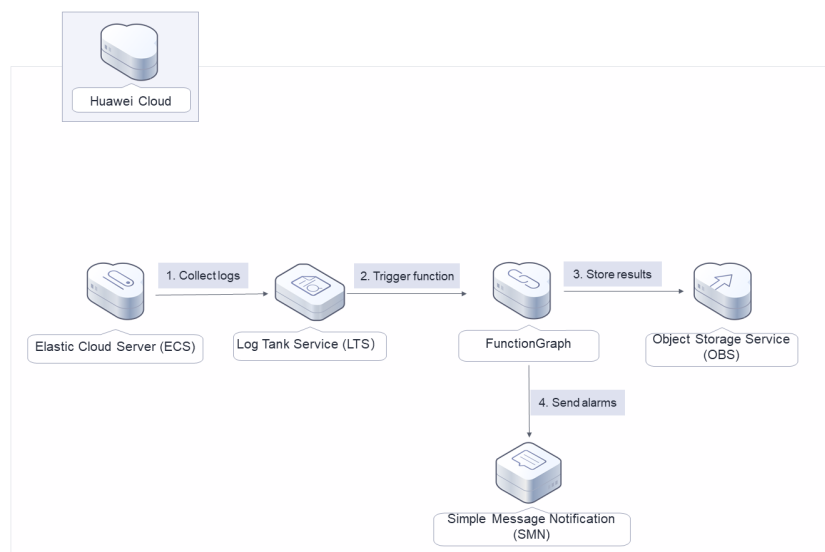
Scenarios

This solution helps you collect, analyze, and archive Elastic Cloud Server (ECS) logs with a serverless architecture. It uses Log Tank Service (LTS) to collect ECS logs, FunctionGraph LTS trigger to obtain logs and analyze alarms in logs, Simple Message Notification (SMN) to push alarms to users, and Object Storage Service (OBS) to archive alarms.

Solution Architecture

This solution uses LTS to collect ECS logs, FunctionGraph LTS trigger to obtain logs and analyze alarms in logs, SMN to push alarms, and OBS to archive alarms. This solution architecture is illustrated below.

Figure 1-1 Architecture



This solution will:

- Create an OBS bucket to store alarm logs.
- Create a FunctionGraph function.
- Create an SMN topic to push alarms in logs.
- Create an LTS log group and log stream to manage collected logs.

Advantages

- Serverless architecture
LTS collects ECS logs, FunctionGraph analyzes and dumps logs, and SMN pushes alarms.
- Customization based on open source
This solution is open-source and free for commercial use. You can also make custom development based on source code.
- Easy deployment
You can deploy a real-time log analysis system in just a few clicks.

Constraints

- Before deploying this solution, ensure that you have an account with access to the target region and sufficient balance for purchasing the resources listed in [Table 2-1](#).
- Ensure that OBS buckets are empty before deleting them.

2 Resource and Cost Planning

This solution deploys the resources listed in the following table. The costs are only estimates and may differ from the final prices. For details, see [pricing details](#).

Table 2-1 Resource and cost planning (pay-per-use)

| Huawei Cloud Service | Example Configuration | Estimated Monthly Cost (1000 Requests) |
|------------------------|--|--|
| FunctionGraph | <ul style="list-style-type: none">• Region: AP-Singapore• Pricing tier:<ul style="list-style-type: none">≤ 1 million requests: \$0 USD per 1 million requests> 1 million requests: \$0.2 USD per 1 million requests• Metering duration:<ul style="list-style-type: none">≤ 400,000 GB-seconds: \$0 USD per GB-second> 400,000 GB-seconds: \$0.00001667 USD per GB-second | \$0 USD |
| Log Tank Service (LTS) | <ul style="list-style-type: none">• Region: AP-Singapore• Log Management: log groups Free creation for log groups; billing by log volume | \$0 USD |

| Huawei Cloud Service | Example Configuration | Estimated Monthly Cost (1000 Requests) |
|-----------------------------------|--|---|
| Object Storage Service (OBS) | <ul style="list-style-type: none"> ● Region: AP-Singapore ● Billing Mode: Pay-per-use ● Product Type: Object storage ● Storage Class: Standard ● Data Redundancy Policy: Multi-AZ storage ● Pay per Use Pricing, Standard (USD): 0.0250/GB per month Traffic: Upload traffic to OBS: Free | <p>It is estimated that 1 GB data will be added every month, which will cost \$0.025 USD.</p> <p>The storage cost of this solution is low. For details, see the monthly bill.</p> |
| Simple Message Notification (SMN) | <ul style="list-style-type: none"> ● Region: AP-Singapore ● Protocol: Email ≤ 1000: \$0 USD per 1000 emails >1000: \$2 USD per 1000 emails | \$0 USD |
| Total | - | About \$0.025 USD |

3 Procedure

- [3.1 Preparations](#)
- [3.2 Quick Deployment](#)
- [3.3 Getting Started](#)
- [3.4 Quick Uninstallation](#)

3.1 Preparations

Creating the rf_admin_trust Agency

- Step 1** Log in to Huawei Cloud official website, open the [console](#), hover over the account name, and choose **Identity and Access Management**.

Figure 3-1 Console page

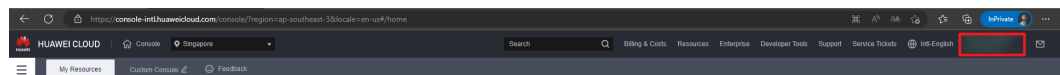
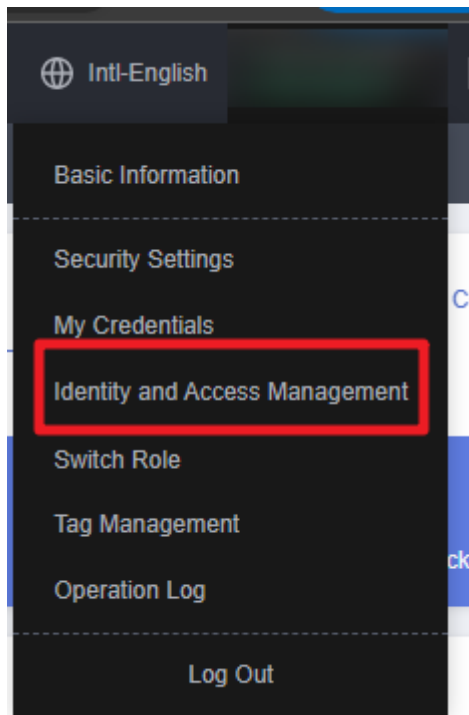
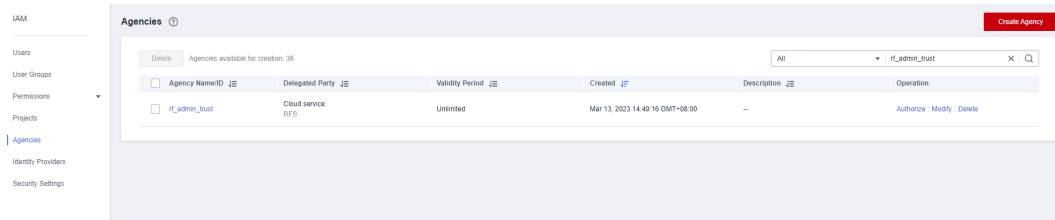


Figure 3-2 Identity and Access Management



Step 2 Choose **Agencies** in the left navigation pane and search for the **rf_admin_trust** agency.

Figure 3-3 Agency list



- If the agency is found, skip the following steps.
- If the agency is not found, perform the following steps to create it.

Step 3 Click **Create Agency** in the upper right corner of the page. On the displayed page, enter **rf_admin_trust** for **Agency Name**, select **Cloud service** for **Agency Type**, select **RFS** for **Cloud Service**, and click **Next**.

Figure 3-4 Creating an agency

Agencies / Create Agency

* Agency Name

* Agency Type Account
Delegate another HUAWEI CLOUD account to perform operations on your resources.
 Cloud service
Delegate a cloud service to access your resources in other cloud services.

* Cloud Service

* Validity Period

Description
0/255

Step 4 Search for **Tenant Administrator**, select it in the search results, and click **Next**.

Figure 3-5 Selecting a policy

Authorize Agency

1 Select Policy/Role 2 Select Scope 3 Finish

Assign selected permissions to rf_admin_trust1. Create Policy

View Selected (1) Copy Permissions from Another Project

| Policy/Role Name | Type |
|---|-----------------------|
| <input type="checkbox"/> DME AdministratorAccess Data Model Engine tenant administrator with full permissions. | System-defined policy |
| <input checked="" type="checkbox"/> Tenant Administrator Tenant Administrator (Exclude IAM) | System-defined role |
| <input type="checkbox"/> CS Tenant Admin Cloud Stream Service Tenant Administrator, can manage multiple CS users | System-defined role |

Step 5 Select **All resources** and click **OK**.

Figure 3-6 Selecting a scope

Authorize Agency

1 Select Policy/Role 2 Select Scope 3 Finish

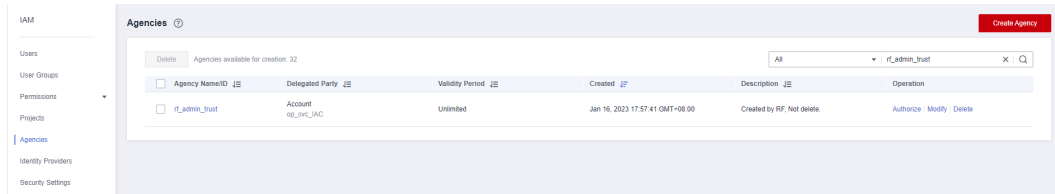
i The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization.

Scope

All resources
IAM users will be able to use all resources, including those in enterprise projects, region-specific projects, and global services under your account based on assigned permissions.
[Show More](#)

Step 6 Check that the **rf_admin_trust** agency is displayed in the agency list.

Figure 3-7 Agency list

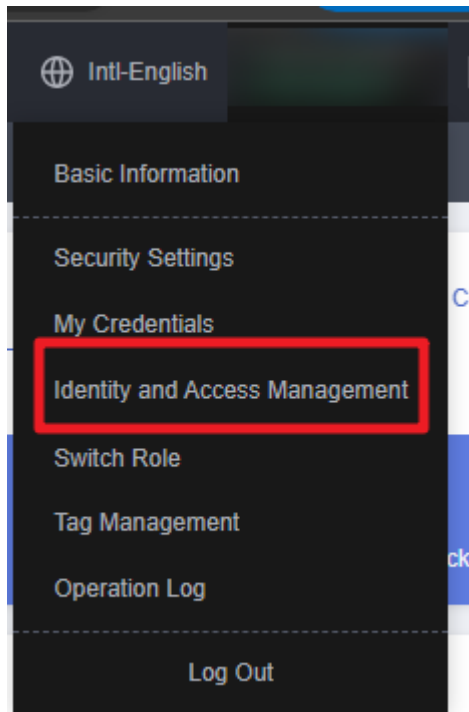


----End

Creating the IAM Agency Management FullAccess Policy

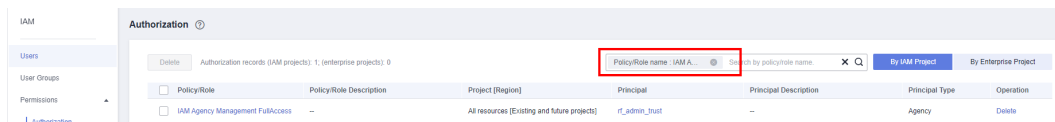
Step 1 Choose Identity and Access Management.

Figure 3-8 Identity and Access Management



Step 2 Choose Permissions > Authorization, enter IAM Agency Management FullAccess in the search box, and check whether this policy exists.

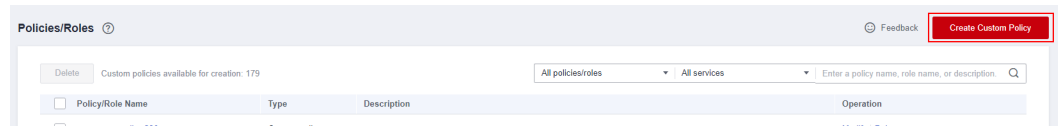
Figure 3-9 Permission list



- If the policy is found, you do not need to create it.
- If the policy is not found, create it.

Step 3 Choose Permissions > Policies/Roles, and click Create Custom Policy.

Figure 3-10 Clicking Create Custom Policy



Step 4 Enter policy name **IAM Agency Management FullAccess**, select **JSON**, enter the following JSON code in the **Policy Content** text box, and click **OK**.

Figure 3-11 Creating a custom policy

★ Policy Name

Policy View Visual editor **JSON**

★ Policy Content

```

1 {
2   "Version": "1.1",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "iam:agencies:updateAgency",
8         "iam:permissions:listRolesForAgencyOnDomain",
9         "iam:permissions:revokeRoleFromAgencyOnDomain",
10        "iam:permissions:listRolesForAgency",
11        "iam:permissions:checkRoleForAgencyOnProject",
12        "iam:roles:listRoles",
13        "iam:agencies:deleteAgency",
14        "iam:permissions:checkRoleForAgency",
15        "iam:permissions:listRolesForAgencyOnProject",
16        "iam:permissions:checkRoleForAgencyOnDomain",
17        "iam:agencies:listAgencies",
18        "iam:permissions:grantRoleToAgencyOnDomain",
19        "iam:permissions:revokeRoleFromAgencyOnProject",
20        "iam:agencies:getAgency",
21        "iam:agencies:createAgency",
22        "iam:permissions:grantRoleToAgency",
23        "iam:permissions:grantRoleToAgencyOnProject",
24        "iam:permissions:revokeRoleFromAgency"
25      ]
26    }
27  ]
28 }
    
```

Description

Scope Global services

```

{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "iam:agencies:createAgency",
        "iam:agencies:listAgencies",
        "iam:agencies:getAgency",
        "iam:agencies:deleteAgency",
        "iam:agencies:updateAgency",
        "iam:permissions:revokeRoleFromAgencyOnProject",
        "iam:permissions:revokeRoleFromAgencyOnDomain",
        "iam:permissions:revokeRoleFromAgency",
        "iam:permissions:grantRoleToAgencyOnDomain",
        "iam:permissions:grantRoleToAgencyOnProject",
        "iam:permissions:grantRoleToAgency",
      ]
    }
  ]
}
    
```

```
"iam:permissions:listRolesForAgencyOnDomain",  
"iam:permissions:listRolesForAgencyOnProject",  
"iam:permissions:checkRoleForAgencyOnDomain",  
"iam:permissions:checkRoleForAgencyOnProject",  
"iam:permissions:listRolesForAgency",  
"iam:permissions:checkRoleForAgency",  
"iam:roles:listRoles"  
  ],  
  "Effect": "Allow"  
}  
]
```

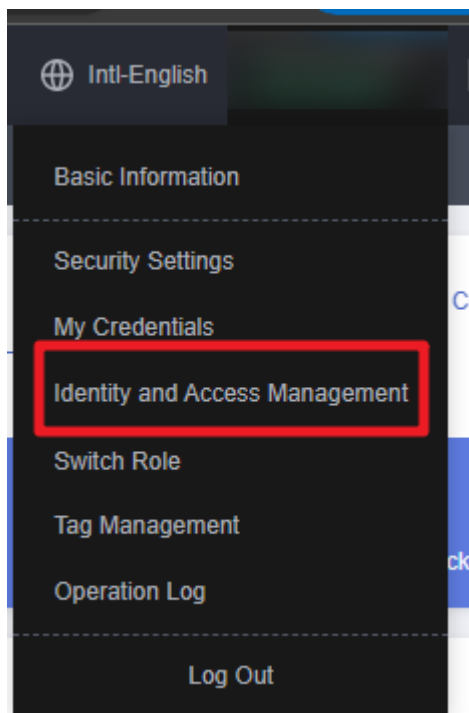
Step 5 If no error message is displayed, the **IAM Agency Management FullAccess** policy is successfully created.

----End

Assigning the IAM Agency Management FullAccess Policy to Agency `rf_admin_trust`

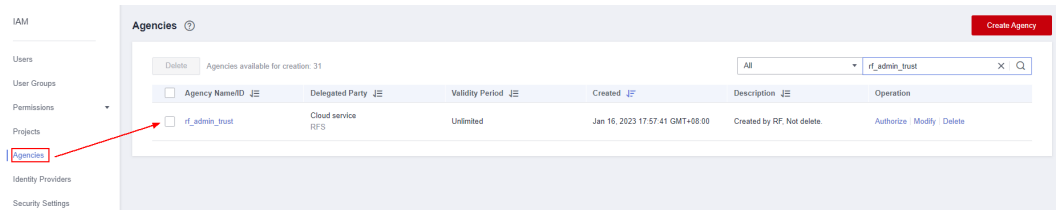
Step 1 Choose **Identity and Access Management**.

Figure 3-12 Identity and Access Management



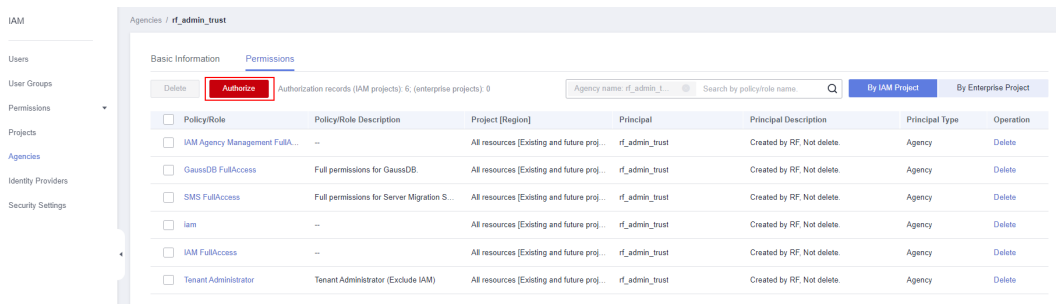
Step 2 Choose **Agencies** in the left navigation pane and select the `rf_admin_trust` agency.

Figure 3-13 Agency list



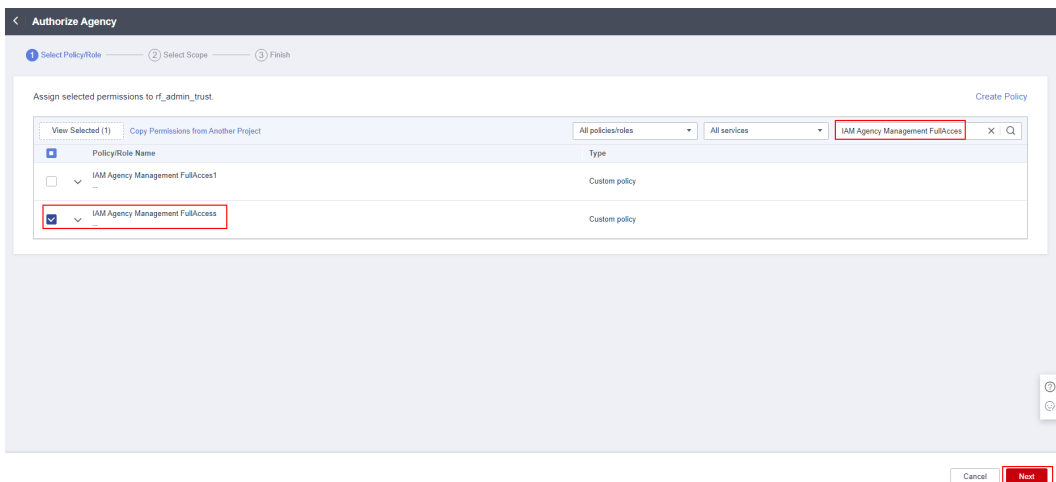
Step 3 Click the **Permissions** tab and click **Authorize**.

Figure 3-14 Permissions



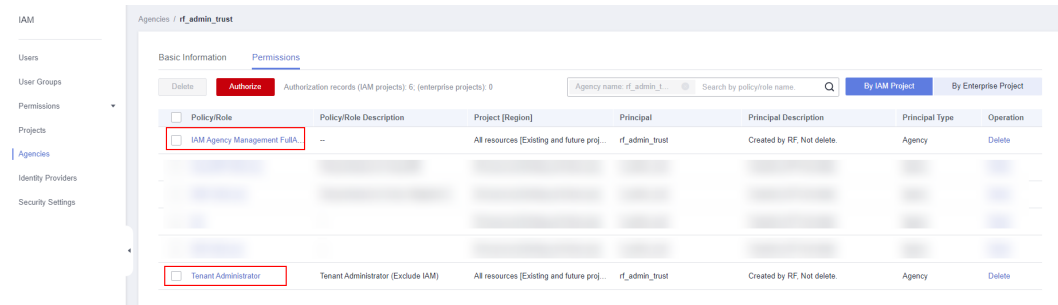
Step 4 Enter **IAM Agency Management FullAccess** in the search box, select the policy, click **Next**, and then click **OK**.

Figure 3-15 Configuring the IAM Agency Management FullAccess policy



Step 5 Check that the **rf_admin_trust** agency has the **Tenant Administrator** and **IAM Agency Management FullAccess** permissions.

Figure 3-16 Permissions



----End

3.2 Quick Deployment

This section describes how to deploy the Serverless Real-Time Log Analysis solution.

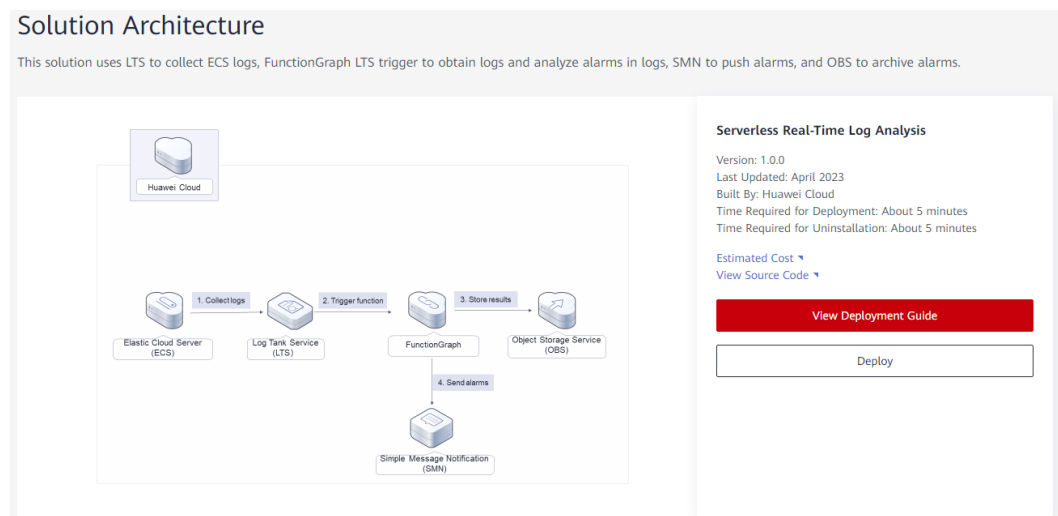
Table 3-1 Parameter description

| Parameter | Type | Mandatory | Description | Default Value |
|-----------------|--------|-----------|--|--|
| function_name | String | Yes | Function name, which identifies a function and serves as the prefix of other resource names. It must be unique and can contain 2 to 53 characters, including letters, digits, underscores (_), and hyphens (-). Start with a letter. | serverless-real-time-log-analysis-demo |
| lts_bucket_name | String | Yes | Name of an OBS bucket to upload alarm logs to. It must be unique and can contain 3 to 59 characters, including lowercase letters, digits, hyphens (-), and periods (.). | Left blank |
| lts_name | String | Yes | Log group and log stream prefix. It must be unique and can contain 1 to 57 characters, including letters, digits, hyphens (-), underscores (_), and periods (.). Do not start with a period or underscore, or end with a period. | serverless-real-time-log-analysis-demo |

| Parameter | Type | Mandatory | Description | Default Value |
|-----------|--------|-----------|--|--|
| smn_name | String | Yes | Topic name, which cannot be modified once the topic is created. The name can contain 1 to 255 characters, including letters, digits, hyphens (-), and underscores (_), and must start with a letter or digit. Modifying this parameter will create a resource. | serverless-real-time-log-analysis-demo |
| email | String | Yes | Email address for receiving alarms. | Left blank |

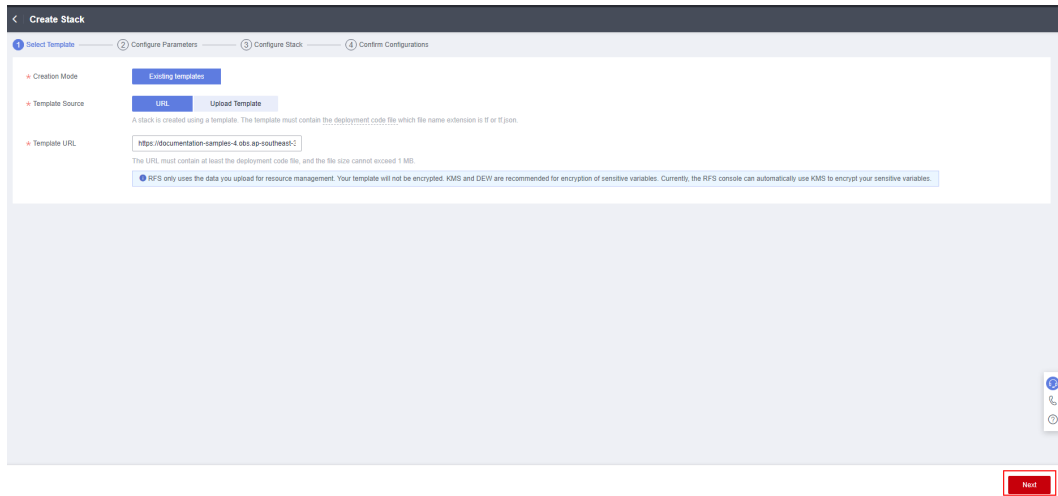
Step 1 Log in to Huawei Cloud Solution Best Practices, choose **Serverless Real-Time Log Analysis**, and click **Deploy**.

Figure 3-17 Selecting a solution



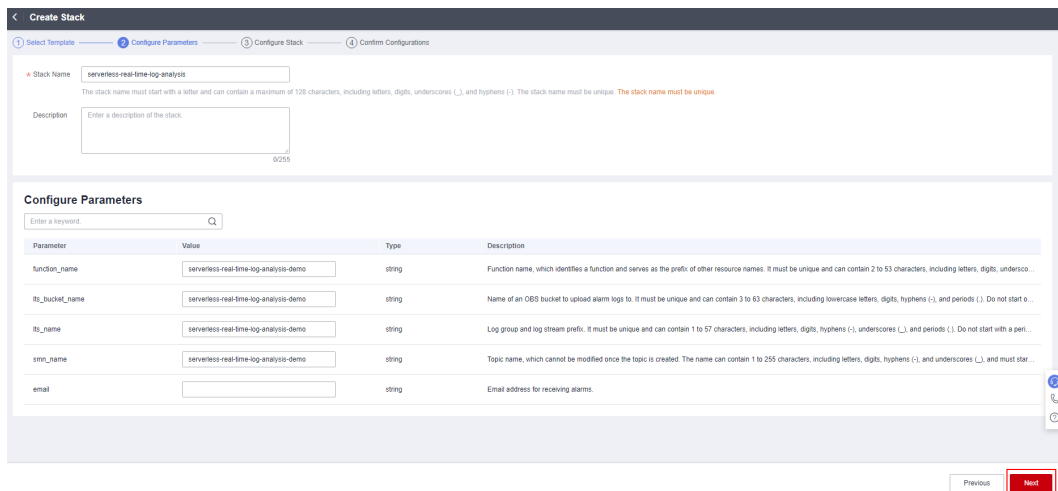
Step 2 On the **Select Template** page, click **Next**.

Figure 3-18 Selecting a template



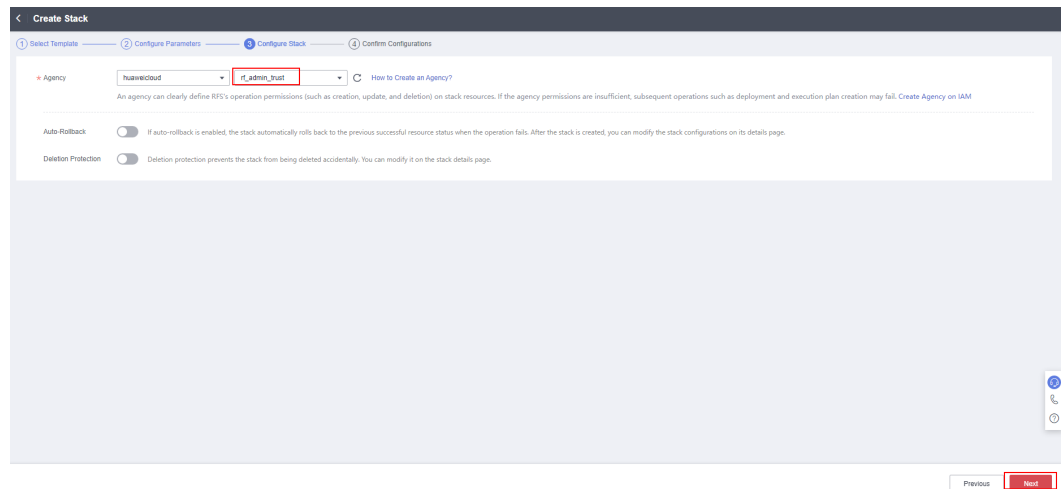
Step 3 On the **Configure Parameters** page, configure parameters by referring to [Table 3-1](#) and click **Next**.

Figure 3-19 Configuring parameters



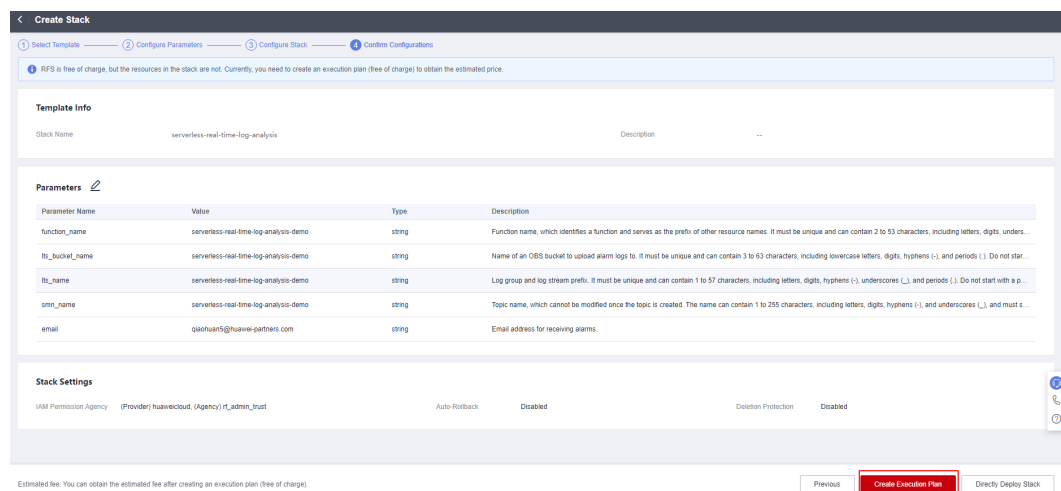
Step 4 On the **Configure Stack** page, select the **rf_admin_trust** agency and click **Next**.

Figure 3-20 Advanced settings



Step 5 On the **Confirm Configurations** page, click **Create Execution Plan**.

Figure 3-21 Confirming configurations



Step 6 In the displayed **Create Execution Plan** dialog box, enter an execution plan name and click **OK**.

Figure 3-22 Creating an execution plan

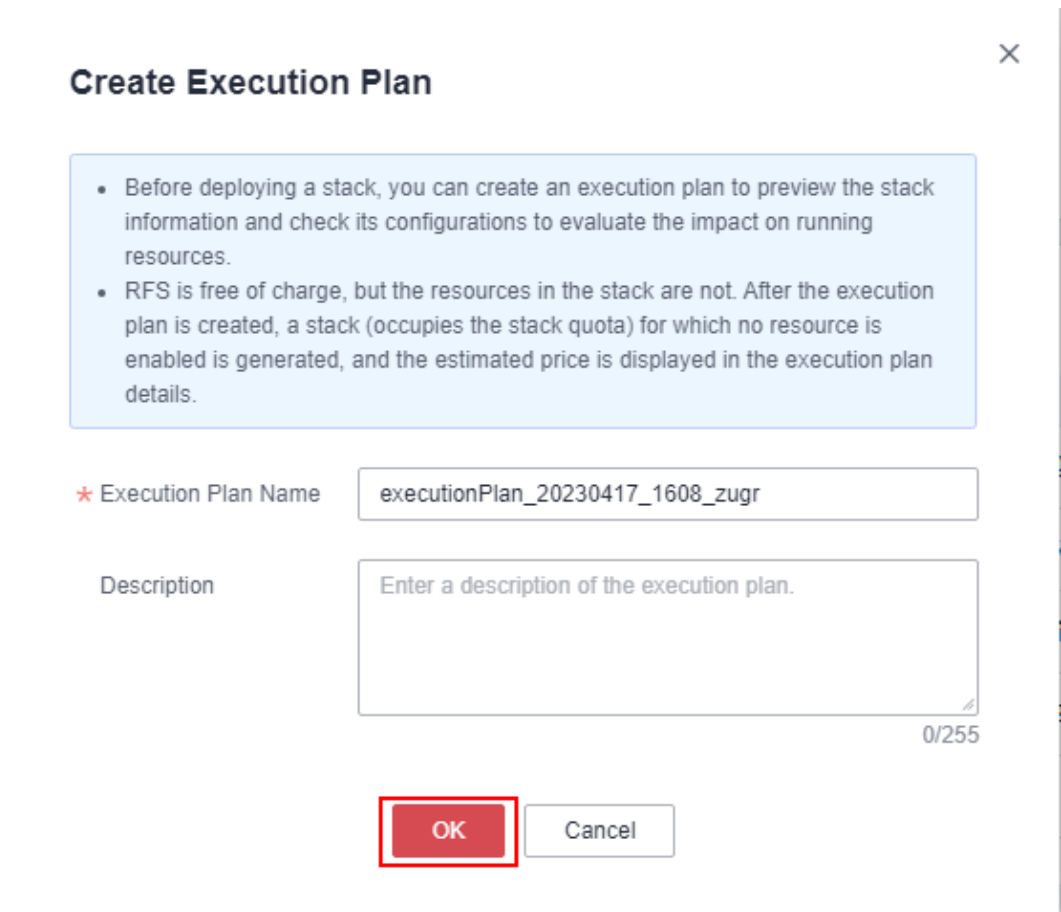
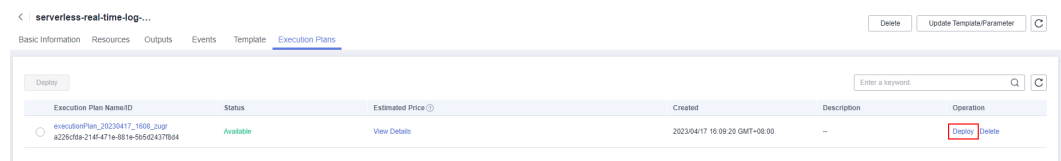
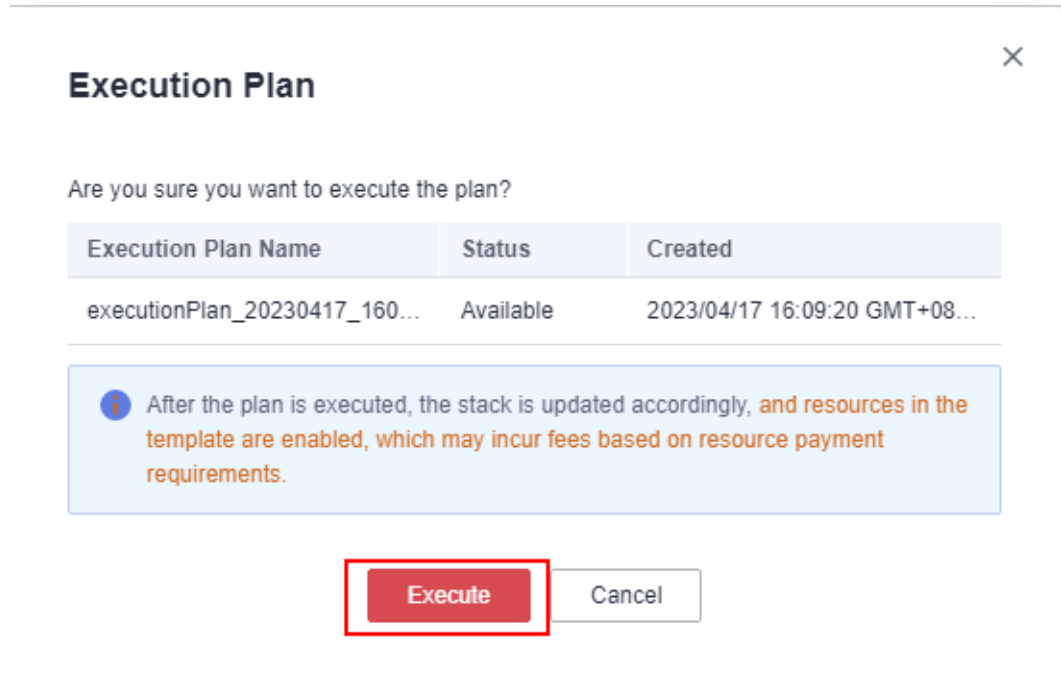


Figure 3-23 Execution plan created



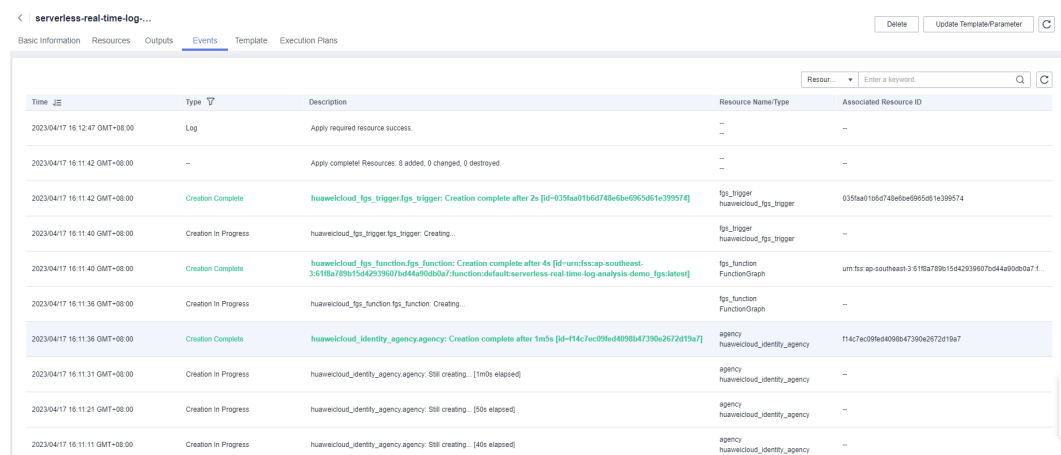
Step 7 Click **Deploy**. In the displayed dialog box, click **Execute**.

Figure 3-24 Confirming the execution plan



Step 8 Wait until deployment is completed, and click the **Events** tab to view details.

Figure 3-25 Resources created

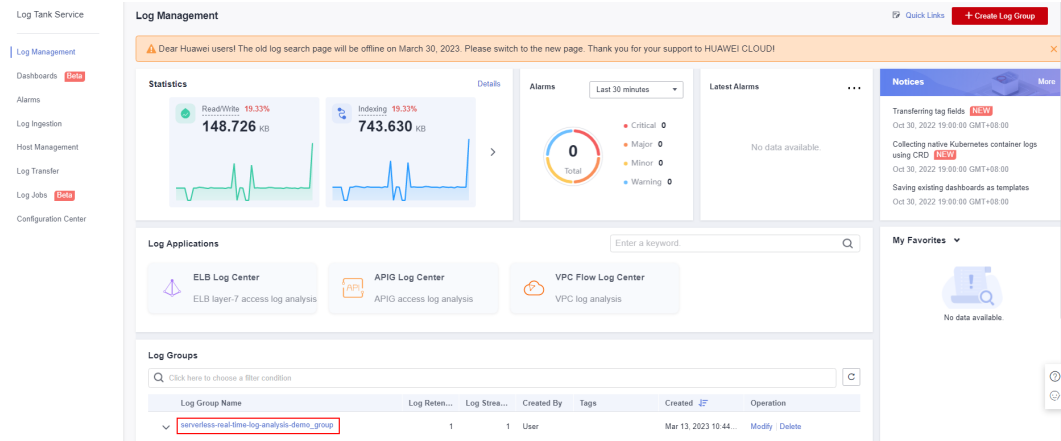


----End

3.3 Getting Started

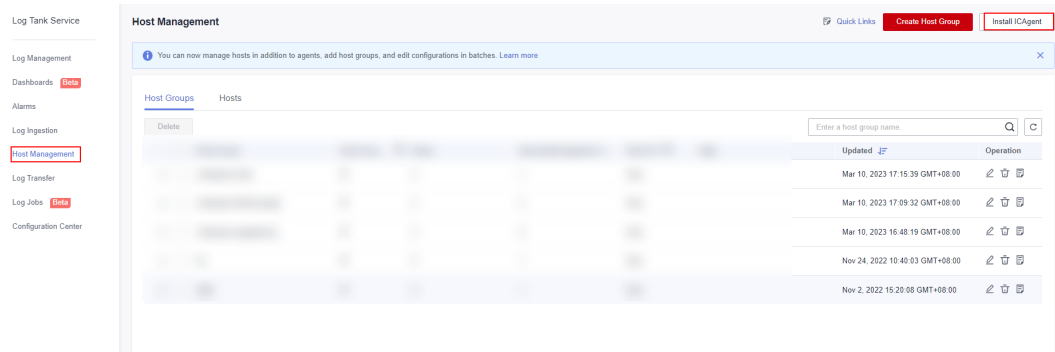
Step 1 Log in to the [LTS console](#), and view the created log group and log stream.

Figure 3-26 LTS console



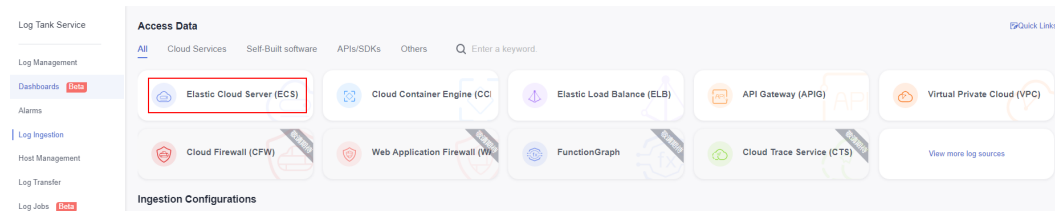
Step 2 Choose **Host Management** and click **Install ICAgent**. For details, see [Installing ICAgent](#).

Figure 3-27 Installing an ICAgent



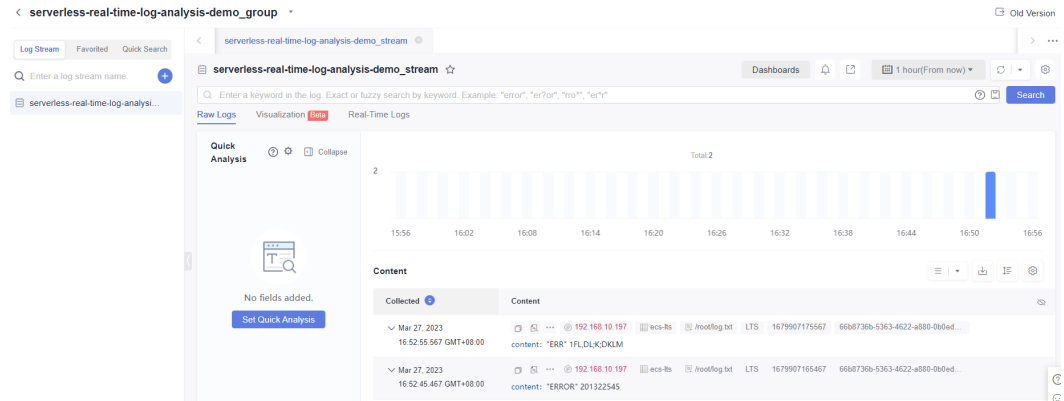
Step 3 Choose **Log Ingestion** and click **Elastic Cloud Server (ECS)**. For details, see [Ingesting Logs to Log Streams](#).

Figure 3-28 Ingesting logs



Step 4 Choose **Log Management**, click the created log group, and view the collected logs in the **Content** area.

Figure 3-29 Viewing logs



Step 5 Log in to the mailbox for receiving alarms, and click **Confirm Subscription** to receive collected alarms.

Figure 3-30 Alarms

Dear Sir or Madam,

Welcome to Simple Message Notification (SMN) service.

You are invited to subscribe to the topic:
urn:smn:ap-southeast-3:61f8a789b15d42939607bd44a90db0a7:serverless-real-time-log-analysis-demo

After confirmation, you will receive messages posted to this topic via email. Instructions on how to cancel notifications will be included in these messages.

Click the following URL to confirm your subscription: (If you don't want to subscribe to this topic, please ignore this email)
[Confirm Subscription](#)
 This URL is valid only within 48 hours.

This is an automatically generated email. Please do not reply.
 Official Website: <https://www.huaweicloud.com/intl/en-us>

Step 6 Log in to the **OBS console** and click the created OBS bucket to view alarm logs.

Figure 3-31 OBS console

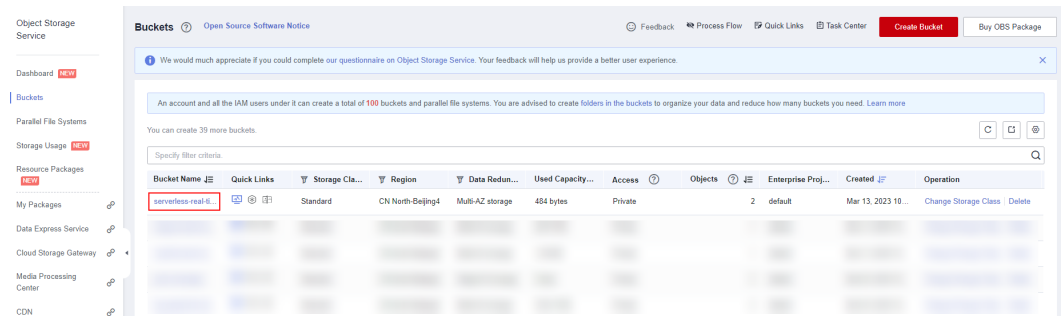
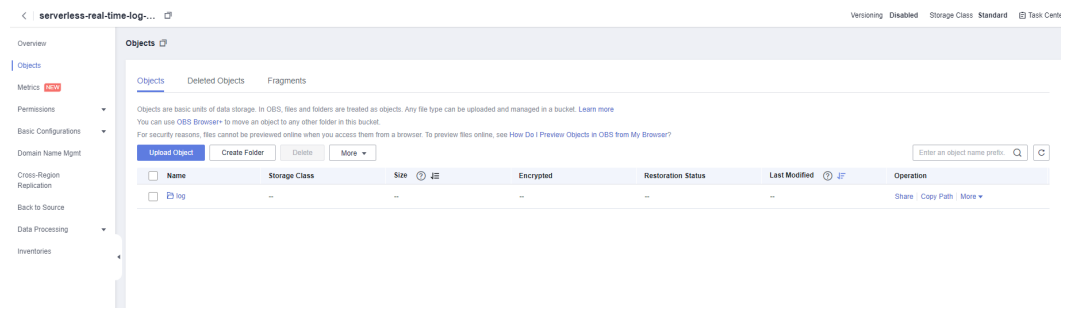


Figure 3-32 Viewing alarm logs



----End

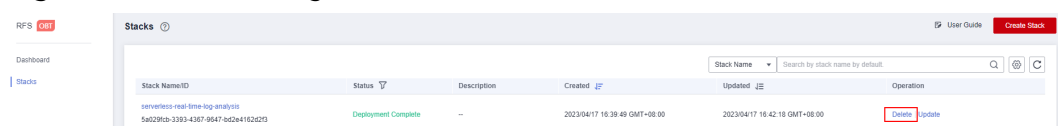
3.4 Quick Uninstallation

NOTICE

Ensure that OBS buckets are empty before deleting them.

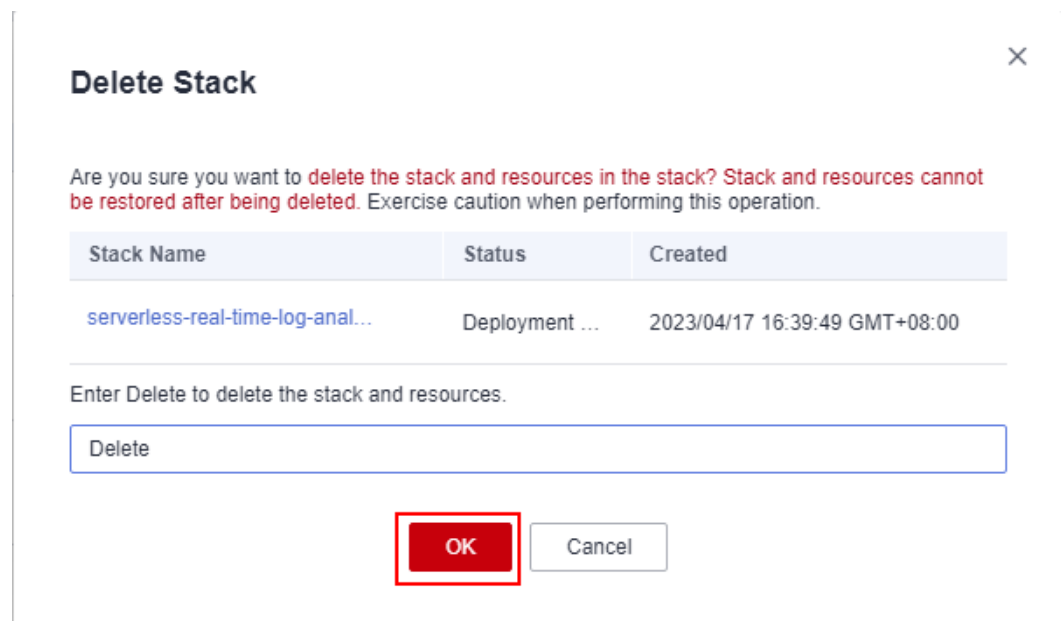
Step 1 Click **Delete** in the row where the solution stack is.

Figure 3-33 Uninstalling the solution



Step 2 Enter **Delete** and click **OK**.

Figure 3-34 Confirming the uninstallation



----End

4 Appendix

Terms

- **Log Tank Service (LTS):** Aggregate, structure, visualize, and analyze log data for actionable insights into O&M. Query logs with instant results. You can also transfer logs to OBS for long-term storage or to Distributed Message Service (DMS) for data retrieval.
- **Object Storage Service (OBS):** OBS provides stable, secure, efficient, and easy-to-use cloud storage that lets you store virtually any volume of unstructured data in any format and access it from anywhere using REST APIs.
- **FunctionGraph:** FunctionGraph allows you to run your code without provisioning or managing servers, while ensuring high availability and scalability. All you need to do is upload your code and set execution conditions, and FunctionGraph will take care of the rest. You pay only for what you use and you are not charged when your code is not running.
- **Identity and Access Management (IAM):** IAM enables you to easily manage users and control their access to Huawei Cloud services and resources.
- **Simple Message Notification (SMN):** SMN lets you send messages at scale to various endpoints, such as HTTP/HTTPS servers, email addresses, phone numbers, functions, and instant messaging tools. You can use SMN to connect cloud services, reducing system complexity.

5 Change History

| Released On | Description |
|-------------|---|
| 2023-04-30 | This issue is the first official release. |