解决方案实践

无服务器日志实时分析

文档版本	1.0.0
发布日期	2023-04-25

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 方案概述

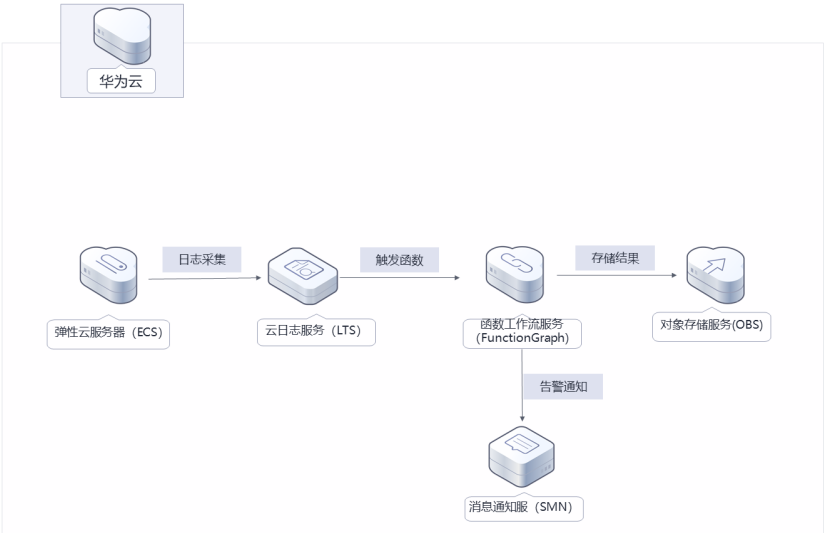
应用场景

该解决方案帮助您无服务器架构实现弹性云服务器 ECS日志的采集、分析、告警以及存档，基于云日志服务 LTS实时采集弹性云服务器 ECS的日志数据，通过函数工作流 FunctionGraph的LTS触发器自动获取日志数据，并实现对日志中告警信息的分析，通过消息通知服务 SMN将告警信息推送给用户，并存储到对象存储服务 OBS桶中进行存档。

方案架构

该解决方案基于云日志服务 LTS实时采集日志数据，函数工作流 FunctionGraph中的函数创建LTS触发器获取日志数据，对日志中的告警信息进行分析和处理，通过消息通知服务 SMN推送告警信息，并将告警日志集中存储在对象存储服务 OBS桶中。部署架构如下图所示：

图 1-1 方案架构



该解决方案会部署如下资源：

- 创建对象存储服务 OBS，用于存储告警日志。
- 函数工作流 FunctionGraph，只需编写业务函数代码并设置运行的条件，即可以弹性、免运维、高可靠的方式运行。
- 在消息通知服务 SMN创建主题，用于推送日志中的告警信息。
- 创建云日志服务 LTS日志组和日志流，用于管理采集到的日志。

方案优势

- 无服务器架构

  云日志服务 LTS实施采集弹性云服务器日志，函数工作流实现日志的分析以及转储，消息通知服务实现告警推送。

- 开源和定制化

  该解决方案是开源的，用户可以免费用于商业用途，并且还可以在源码基础上进行定制化开发。

- 一键部署

  一键轻松部署，即可完成日志实时分析系统的搭建。

约束与限制

- 在开始解决方案部署之前，请确认您已经拥有一个可以访问该区域的华为账号且已开通华为云。
- 快速卸载前请确认OBS桶中无文件，否则会导致删除失败。

2 资源和成本规划

该解决方案主要部署如下资源，不同产品的花费仅供参考，具体请参考华为云**官网价格**，实际以收费账单为准：

表 2-1 资源和成本规划（按需计费）

华为云服务	配置示例	每月预估花费（调用1000次）
函数工作流 FunctionGraph	• 区域：亚太-新加坡 • 产品：函数 • 请求次数： 0-100万次： $0 USD/0元/100万次 100万次以上： $0.2 USD/100万次 • 计量时间： 0-400,000 GB/秒： $0 USD/GB-秒 400,000 GB/秒以上： $0.00001667 USD/GB-秒	$0 USD
云日志服务 LTS	• 区域：亚太-新加坡 • 日志管理：日志组 创建日志组免费，使用阶段按照日志量收费	$0 USD

华为云服务	配置示例	每月预估花费（调用1000次）
对象存储服务 OBS	● 区域：亚太-新加坡 ● 计费模式：按需计费 ● 产品类型：对象存储 ● 存储类别：标准存储 ● 数据冗余存储策略：多AZ存储 ● 存储空间：0.0250USD/GB/月 ● 流量费用：内/公网流入流量（数据上传到OBS）免费	预计每月新增1GB数据量，花费$0.025 USD。 该方案存储费用消耗较低，详细请参考每月账单。
消息通知服务 SMN	● 区域：华北-北京四 ● 订阅协议：邮件 0个数-1000个数（含）：$0 USD/1000封 大于1000个数：$2 USD/1000封	$0 USD
合计	-	约$0.025 USD

3 实施步骤

3.1 准备工作

创建 rf_admin_trust 委托

步骤1 进入华为云官网，打开**控制台管理**界面，鼠标移动至个人账号处，打开“统一身份认证”菜单。

图 3-1 控制台管理界面

图 3-2 统一身份认证菜单

步骤2 进入“委托”菜单，搜索“rf_admin_trust”委托。

图 3-3 委托列表

- 如果委托存在，则不用执行接下来的创建委托的步骤
- 如果委托不存在时执行接下来的步骤创建委托

步骤3 单击步骤2界面中右上角的“创建委托”按钮，在委托名称中输入“rf_admin_trust”，“委托类型”选择“云服务”。“委托的账号”选择“RFS”，单击“下一步”。

图 3-4 创建委托

步骤4 在搜索框中输入“Tenant Administrator”权限，并勾选搜索结果。

图 3-5 选择策略

步骤5 选择“所有资源”，并单击下一步完成配置。

图 3-6 设置授权范围

步骤6 “委托”列表中出现“rf_admin_trust”委托则创建成功。

图 3-7 委托列表

----结束

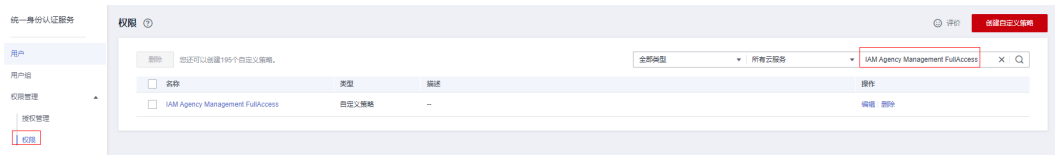
创建 IAM Agency Management FullAccess 策略

步骤1 打开“统一身份认证”菜单。

图 3-8 统一身份认证菜单

步骤2 进入“权限管理”-> “权限”菜单，在搜索框输入“IAM Agency Management FullAccess”当前账号是否存在IAM委托管理权限。

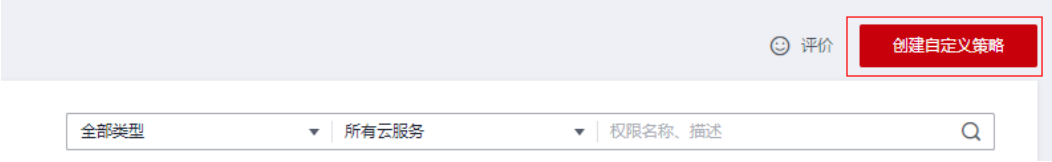
图 3-9 权限列表



- 如果搜索结果不为空，则当前账号已经存在IAM委托管理权限，不需要重复创建
- 如果搜索结果为空，则继续创建“IAM Agency Management FullAccess”权限

步骤3 单击“创建自定义策略”按钮。

图 3-10 创建自定义策略



步骤4 输入策略名称为“IAM Agency Management FullAccess”，选择“JSON视图”，在策略内容中输入如下JSON代码，单击确认按钮。

图 3-11 创建自定义策略


```
{
    "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"
    }
  ]
}
```

步骤5 界面无报错，则成功创建IAM Agency Management FullAccess权限。

----结束

给 rf_admin_trust 委托添加 IAM Agency Management FullAccess 策略

步骤1 打开“统一身份认证”菜单。

图 3-12 统一身份认证菜单

步骤2 进入“委托”菜单，选择rf_admin_trust委托。

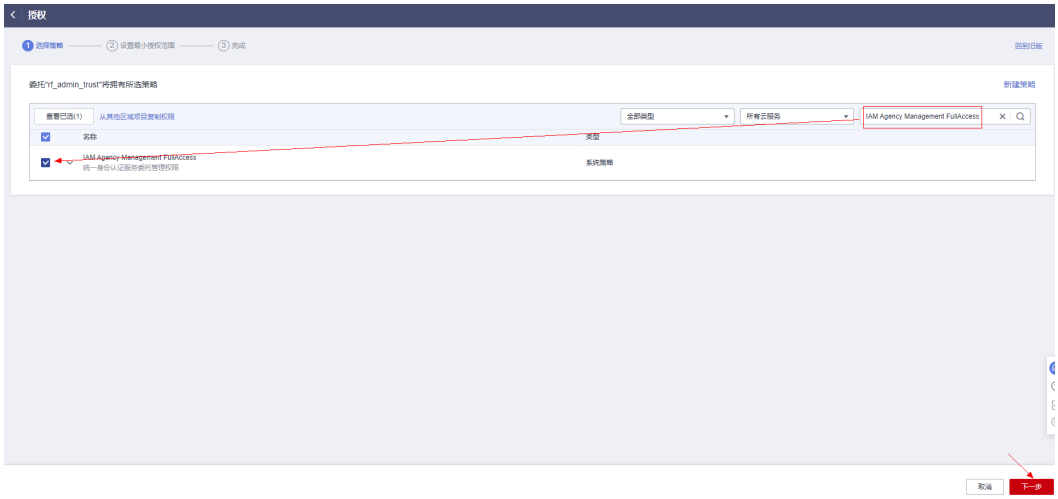
图 3-13 委托列表

步骤3 进入“授权记录”菜单，单击“授权”按钮。

图 3-14 授权记录

步骤4 在搜索框输入IAM Agency Management FullAccess，勾选过滤出来的记录，单击下一步，并确认完成权限的配置。

图 3-15 配置 IAM Agency Management FullAccess 策略



步骤5 配置好后的情况：rf_admin_trust委托拥有Tenant Administrator和IAM Agency Management FullAccess权限。

图 3-16 授权记录列表

----结束

3.2 快速部署

本章节主要帮助用户快速部署该解决方案。

表 3-1 参数填写说明

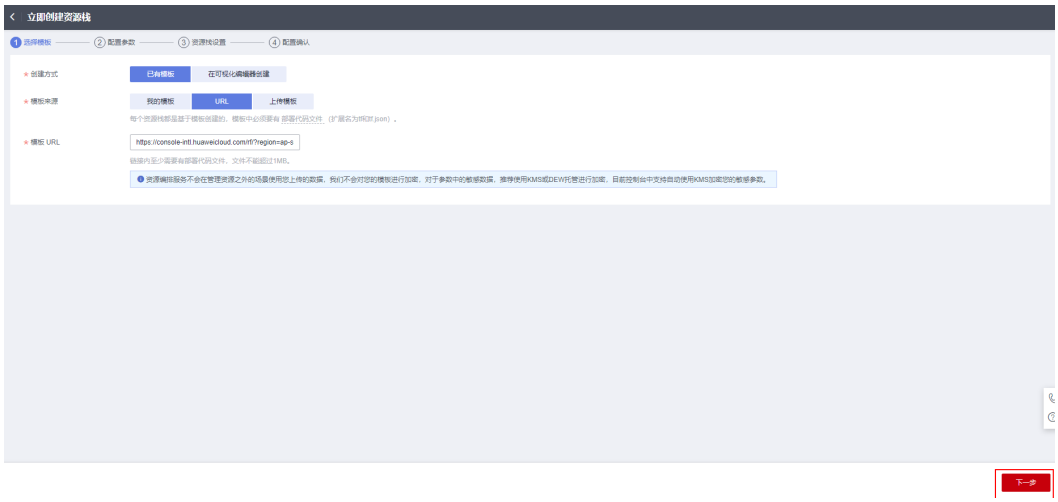
参数名称	类型	是否必填	参数解释	默认值
function_name	String	必填	函数名称，用于定义创建函数及其他资源前缀，不支持重名。取值范围：2-53个字符，可包含字母、数字、下划线和中划线，以大/小写字母开头，以字母或数字结尾。	serverless-real-time-log-analysis-demo
lts_bucket_name	String	必填	OBS桶名称，不支持重名。用于上传告警日志。取值范围：3-59个字符，支持小写字母、数字、中划线（-）、英文句号（.）。	空
lts_name	String	必填	日志组、日志流名称前缀，不支持重名。取值范围：1~57个字符，只支持输入英文、数字、中文、中划线、下划线及小数点，且不能以小数点、下划线开头或以小数点结尾。	serverless-real-time-log-analysis-demo
smn_name	String	必填	指定要创建的主题名称，创建后，不允许修改。取值范围：1~255个字符，名称只能包含大写字母、小写字母、数字、-和_，且必须由大写字母、小写字母或数字开头。更改此参数创建一个新资源	serverless-real-time-log-analysis-demo
email	String	必填	接收告警信息的邮箱地址。	空

步骤1 登录华为云解决方案实践，选择“无服务器日志实时分析”解决方案，单击“一键部署”，跳转至解决方案创建堆栈界面。

图 3-17 解决方案实施库

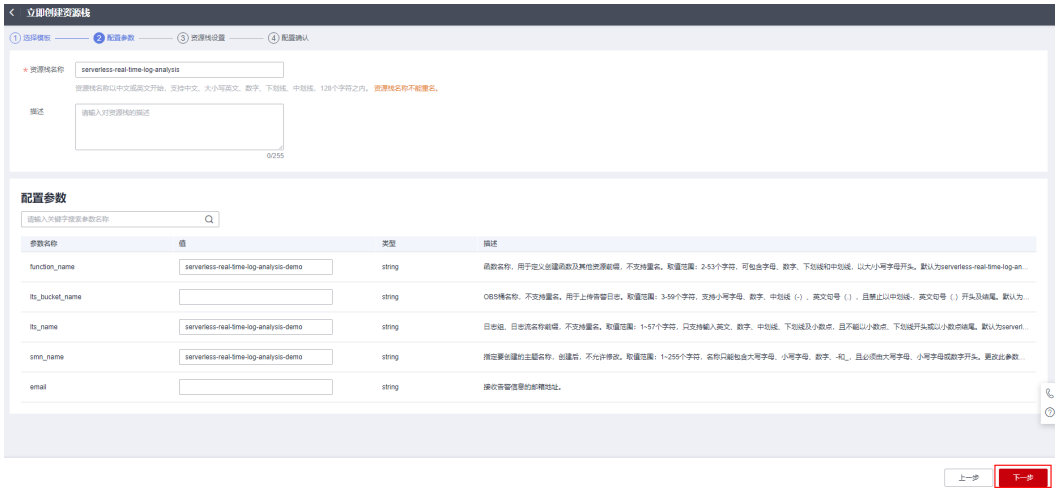
步骤2 在选择模板界面中，单击“下一步”。

图 3-18 选择模板



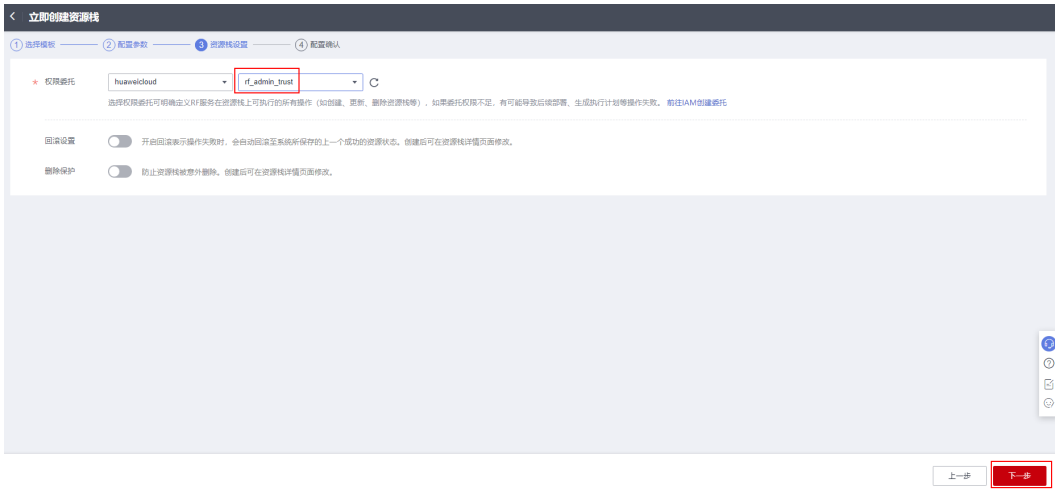
步骤3 在配置参数界面中，参考**表3-1**完成自定义参数填写，单击“下一步”。

图 3-19 配置参数



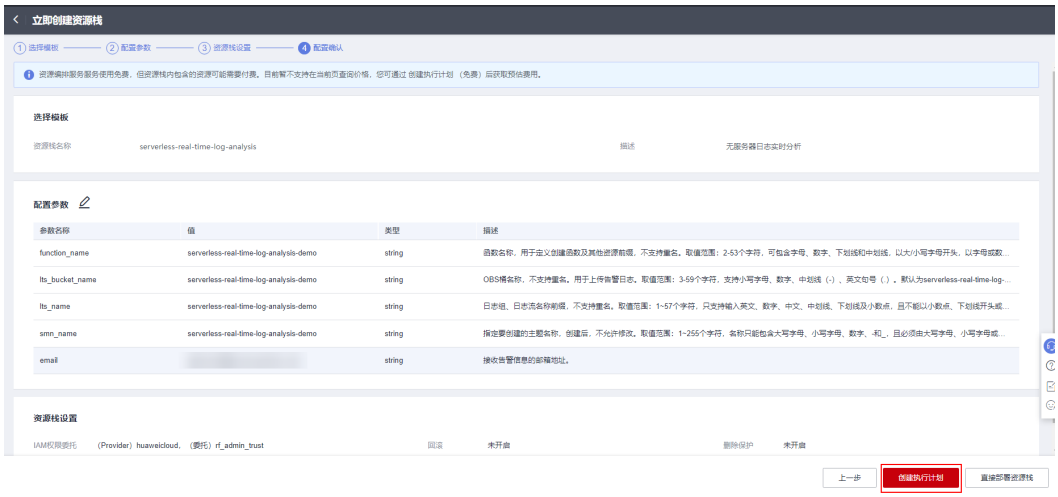
步骤4 在资源栈设置页面中，权限委托选择“rf_admin_trust”,单击“下一步”。

图 3-20 高级配置



步骤5 在配置确认页面中，单击“创建执行计划”。

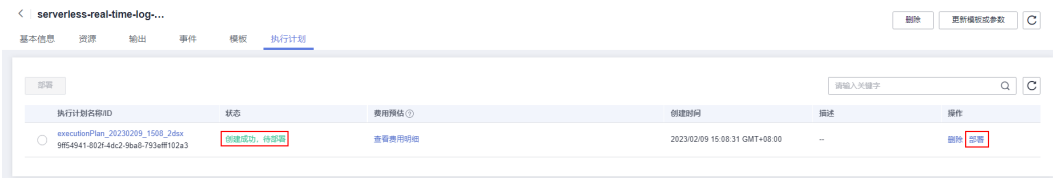
图 3-21 配置确认



步骤6 在弹出的创建执行计划框中，自定义填写执行计划名称，单击“确定”。

图 3-22 创建执行计划

图 3-23 执行计划创建成功

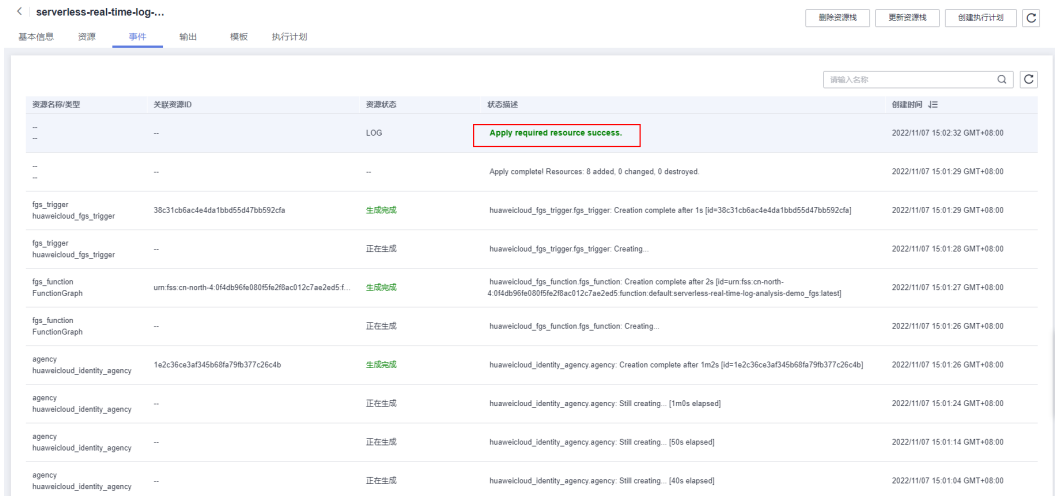


步骤7 单击“部署”，弹出执行计划提示信息，单击“执行”确认执行。

图 3-24 执行计划确认

步骤8 等待解决方案自动部署。部署成功后，单击“事件”，回显结果如下:

图 3-25 资源创建成功



----结束

3.3 开始使用

步骤1 登录**云日志服务LTS控制台**，查看创建的日志组、日志流。

图 3-26 云日志服务 LTS 控制台

步骤2 选择主机管理，单击“安装ICAgent”。详细步骤参考**安装ICAgent**。

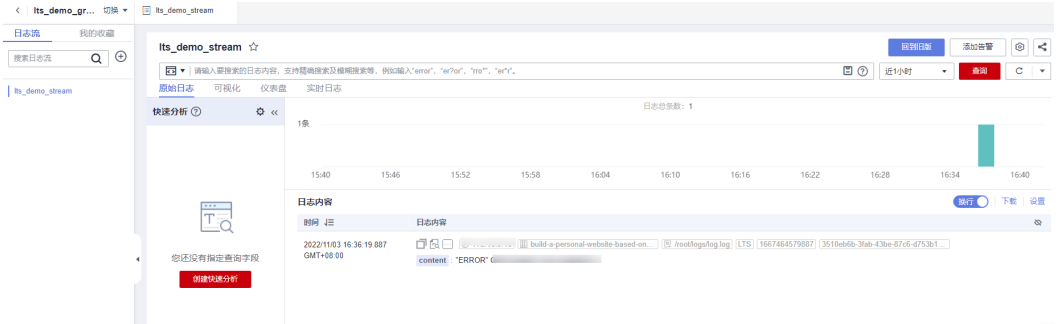
图 3-27 安装 ICAgent

步骤3 选择日志接入，单击“云主机ECS-文本日志”。详细步骤参考**接入日志**。

图 3-28 接入日志

步骤4 选择日志管理，单击创建的日志组的名称，在日志内容即可查询采集到的日志。

图 3-29 查看日志



步骤5 登录接收告警信息邮箱，单击订阅确认，即接收采集到的告警信息。

图 3-30 告警信息

尊敬的用户：

欢迎使用华为云的消息通知服务（SMN）。

您受邀订阅主题：
urn:smn:ap-southeast-3:61f8a789b15d42939607bd44a90db0a7:serverless-real-time-log-analysis-qh

订阅确认以后，您将收到向该主题发布的邮件消息，消息内容中包含了取消订阅的链接。

点击下面的链接，确认本次订阅（如果无需订阅本主题，请忽略此邮件）：
订阅确认
链接48小时内有效。

本邮件由系统自动发送，请勿直接回复！
官方网站: https://www.huaweicloud.com
客服电话: 4000-955-988

步骤6 登录**对象存储服务控制台**，单击创建的OBS桶名称，即可查看保存的告警日志。

图 3-31 对象存储服务控制台

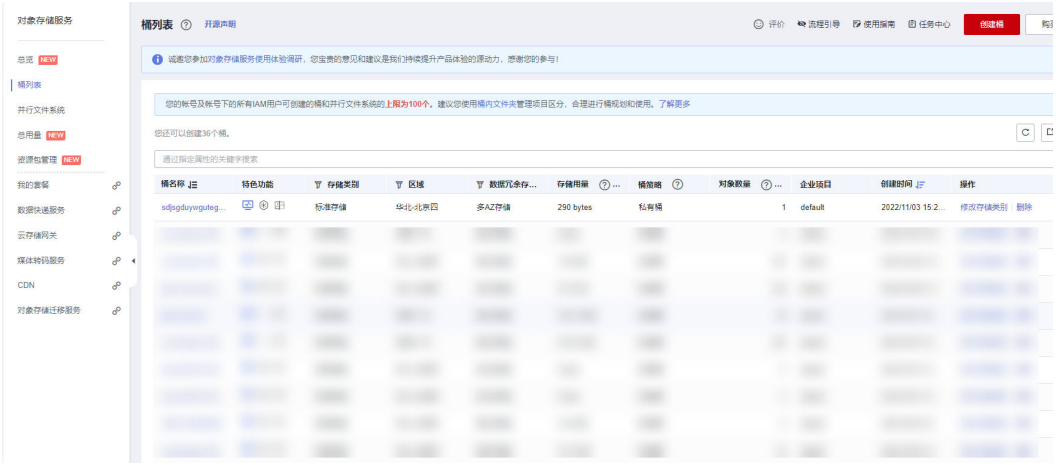


图 3-32 查看告警日志

----结束

3.4 快速卸载

须知

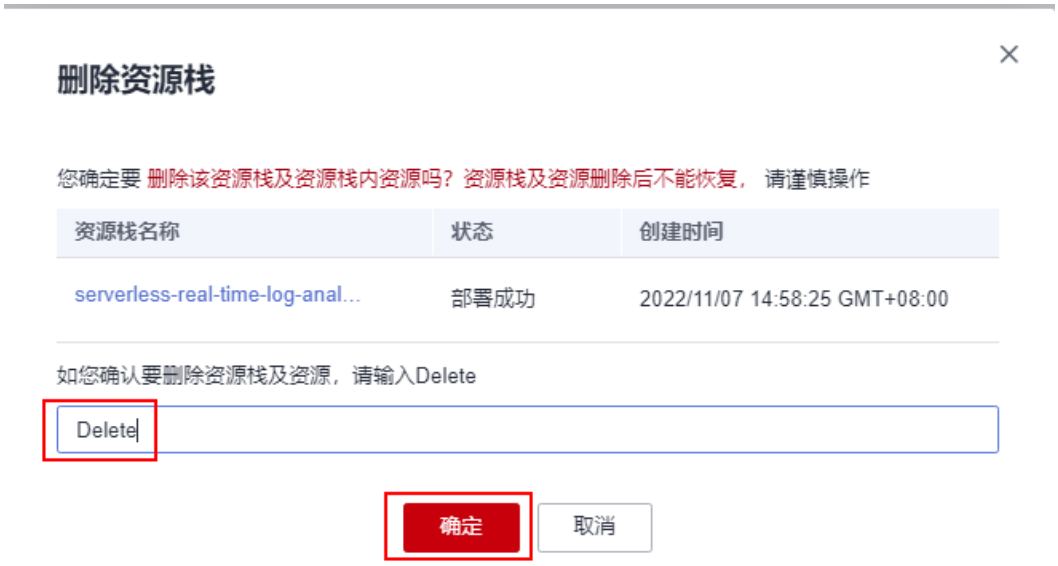
快速卸载前请确认OBS桶中无文件，否则会导致删除失败。

步骤1 解决方案部署成功后，单击该方案堆栈后的“删除”。

图 3-33 一键卸载

步骤2 在弹出的删除堆栈确认框中，输入“Delete”，单击“确定”，即可卸载解决方案。

图 3-34 删除堆栈确认



----结束

4 附录

名词解释

基本概念、云服务简介、专有名词解释

- 云日志服务(LTS)：提供一站式日志采集、秒级搜索、海量存储、结构化处理、转储和可视化图表等功能，满足应用运维、网络日志可视化分析、等保合规和运营分析等应用场。
- 对象存储服务(OBS)：一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力。
- 函数工作流(FunctionGraph)：是一项基于事件驱动的函数托管计算服务。使用FunctionGraph函数，只需编写业务函数代码并设置运行的条件，无需配置和管理服务器等基础设施，函数以弹性、免运维、高可靠的方式运行。此外，按函数实际执行资源计费，不执行不产生费用。
- 统一身份认证服务(IAM)：是华为云提供权限管理、访问控制和身份认证的基础服务，您可以使用IAM创建和管理用户、用户组，通过授权来允许或拒绝对云服务和资源的访问，通过设置安全策略提高账号和资源的安全性，同时IAM为您提供多种安全的访问凭证。
- 消息通知服务(SMN)：为用户提供快速简便、稳定可靠、简化运维、高可扩展、安全可信的消息通知能力。最终用户可以通过HTTP、HTTPS、邮件、短信、触发函数执行、即时通讯工具等方式接收通知信息。华为云用户也可以在应用之间通过消息通知服务实现应用的功能集成，降低系统的复杂性。

5 修订记录

发布日期	修订记录
2022-10-30	第一次正式发布。
2023-02-28	修订实施步骤。