

解决方案实践

快速构建基于事件网格的运维审计环境

文档版本 1.0.0
发布日期 2023-11-30



版权所有 © 华为技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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	1
2 资源和成本规划	3
3 实施步骤	5
3.1 准备工作.....	5
3.2 快速部署.....	14
3.3 开始使用.....	19
3.4 快速卸载.....	25
4 附录	27
5 修订记录	28

1 方案概述

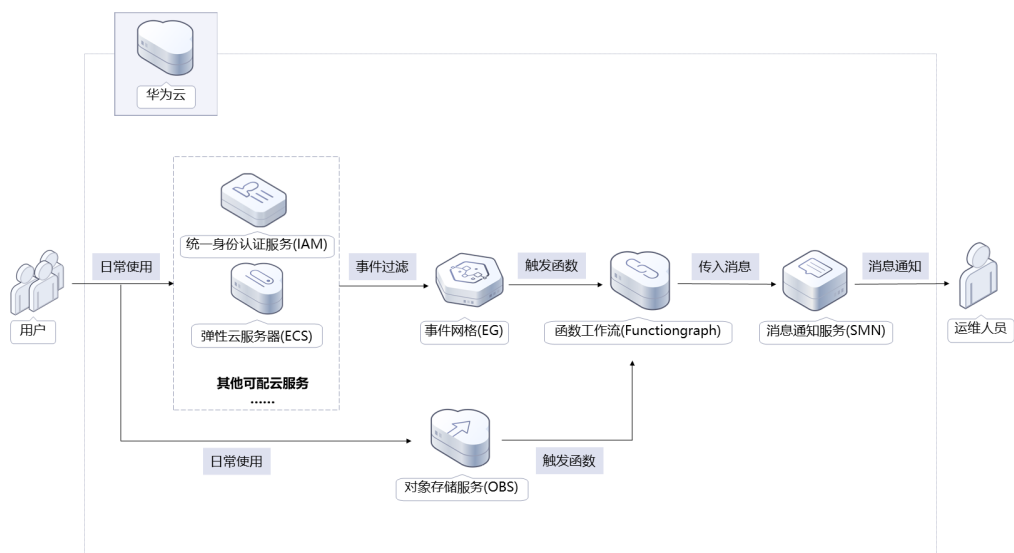
应用场景

该解决方案基于华为云函数工作流 FunctionGraph无服务器架构，将云服务（如：弹性云服务器 ECS、对象存储服务 OBS、统一身份认证服务 IAM等）产生的事件发送到事件网格 EG中，事件网格对事件进行校验、过滤、路由和转化，然后推送给已经订阅事件的函数。在函数中执行业务处理逻辑，并将关键的事件信息通过消息通知服务 SMN推送给运维人员。从而对云服务的访问和操作行为进行审计，防止恶意行为，保障云服务和数据的安全。

方案架构

该解决方案基于华为云事件网格 EG、函数工作流 FunctionGraph及消息通知服务 SMN，帮助用户快速构建运维审计环境。解决方案架构图如下：

图 1-1 方案架构图



该解决方案会部署如下资源：

- 在事件网格 EG 中创建两个事件订阅，用于将事件源（弹性云服务器 ECS、统一身份认证服务 IAM）、事件通道和事件目标绑定在一起，通过事件规则将事件源发出的事件路由到事件目标。
- 创建一个或多个对象存储服务 OBS 触发器，用于由指定的桶内对象触发函数。
- 在函数工作流 FunctionGraph 中创建两个函数，一个用于接收来自事件网格路由的特定事件，另一个用于接收来自对象存储服务产生的事件。并将消息格式化后调用消息通知服务推送给订阅终端。
- 使用消息通知服务 SMN，用于将指定的事件发送给消息订阅终端。
- 在统一身份认证服务 IAM 创建两个委托，一个用于将 SMN 的操作权限委托给函数工作流，另一个用于授权 EG 投递事件给函数工作流。

方案优势

- 实时监控
实时监控华为云上云服务状态，将高危操作及时路由给运维人员，从而发现并解决问题。
- 开源定制化
该解决方案是开源的，用户可以根据该解决方案模板，定制专属的运维审计环境。
- 一键部署
采用现成的事件网格技术，可以快速构建一个运维审计环境，节省大量的开发时间和成本。

约束与限制

- 部署该解决方案之前，您需注册华为账号并开通华为云，完成实名认证，且账号不能处于欠费或冻结状态。
- 当前登录账号拥有使用事件网格的权限。账号权限授权与绑定，请参考[创建用户并授权使用 EG](#)。如果您的账号为 IAM 用户，请先联系华为云账号拥有者为 IAM 用户授权，然后才能使用事件网格服务。
- 部署该解决方案之前，请确保您有一个可用的消息服务 SMN 主题。

2 资源和成本规划

该解决方案主要部署如下资源，以下费用仅供参考，具体请参考华为云官网[价格计算器](#)，实际收费以账单为准。

表 2-1 成本预估（仅供参考）

华为云服务	计费说明	每月花费
事件网格 EG	<ul style="list-style-type: none">区域：华北-北京四自定义（包含云服务租户侧事件产生）或三方事件流入的事件数量 根据事件流入的数量按量计费，6.75元/百万个。 <ul style="list-style-type: none">华为云服务事件源自身产生发布的事件（任意事件状态变化）免费，事件消费免费。	免费

华为云服务	计费说明	每月花费
消息通知服务 SMN	<ul style="list-style-type: none"> ● 区域：华北-北京四 ● 外网下行流量 0GB-1GB 0 元/GB ● 外网下行流量 大于1GB 0.8 元/GB ● 中国短信推送 0个数~100个数 (含) 0 元/条 ● 中国短信推送 100个数~100,000 个数 (含) 0.045 元/条 ● 中国短信推送 100,000个数 ~300,000个数 (含) 0.04 元/条 ● 中国短信推送 300,000个数 ~500,000个数 (含) 0.039 元/条 ● 中国短信推送 500,000个数 ~1,000,000个数 (含) 0.038 元/条 ● 中国短信推送 1,000,000个数 ~3,000,000个数 (含) 0.037 元/条 ● 中国短信推送 大于3,000,000个数 0.036元/条 ● 电子邮件 0个数-1,000个数 (含) 0 元/1,000封 ● 电子邮件 大于1,000个数 2 元/1,000封 ● HTTP(S) 0个-1,000,000个 (含) 0 元/百万次 ● HTTPS(S) 大于1,000,000个 2 元/百万次 <p>具体请参考价格计算器及计费说明。</p>	详情请参考收费账单
函数工作流 FunctionGraph	<ul style="list-style-type: none"> ● 区域：华北-北京四 ● 产品：函数 ● 请求次数： 0-100万次： 0元/100万次 100万次以上： 1.33元/100万次 ● 计量时间： 0-400,000 GB/秒： 0元/GB-秒 400,000 GB/秒以上： 0.00011108元/GB-秒 	详情请参考收费账单
合计	-	函数费用 + 消息通知费用

3 实施步骤

当您首次使用华为云时注册的账号，则无需执行该准备工作5-6，如果您使用的是IAM用户账户，请确认您是否在admin用户组中，如果您不在admin组中，则需要为您的账号[授予相关权限](#)，并完成以下所有准备工作。

3.1 准备工作

3.2 快速部署

3.3 开始使用

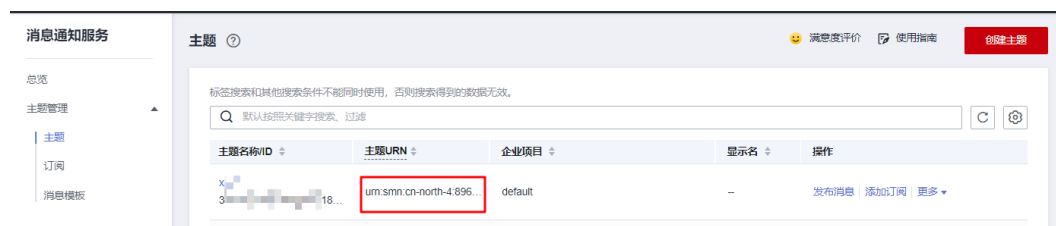
3.4 快速卸载

3.1 准备工作

1. 获取消息通知服务 SMN 主题 URN

步骤1 进入华为云官网，打开[控制台管理](#)界面，打开[消息通知服务主题列表](#)，选择一个适用于运维人员专用的主题，复制URN。

图 3-1 主题 URN



----结束

2. 获取事件网格 EG 云服务事件通道 ID

步骤1 进入华为云官网，打开[控制台管理](#)界面，打开[事件网格](#)，复制default通道ID。

图 3-2 事件通道 ID



----结束

3. 获取弹性云服务器 ECS ID

步骤1 进入华为云官网，打开**控制台管理**界面，打开**弹性云服务器 ECS**，选择与事件网格同 Region 下的云服务器，复制ID。

图 3-3 弹性云服务器 ECS ID



----结束

4. 获取对象存储服务 OBS 桶名（可选）

步骤1 进入华为云官网，打开**控制台管理**界面，打开**弹性云服务器 ECS**，选择与事件网格同 Region 下的OBS桶，复制桶名。

图 3-4 对象存储桶名



----结束

5. 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 3-5 控制台管理界面



图 3-6 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 3-7 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”，选择“RFS”，单击“下一步”。

图 3-8 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，单击“下一步”。

图 3-9 选择策略



步骤5 选择“所有资源”，并单击下一步完成配置。

图 3-10 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 3-11 委托列表



----结束

6. 创建 IAM Agency Management FullAccess 策略

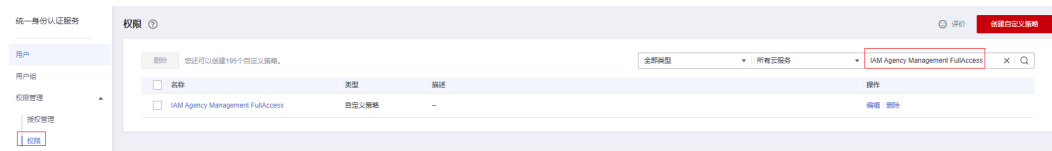
步骤1 打开“统一身份认证”菜单。

图 3-12 统一身份认证菜单



步骤2 进入“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。

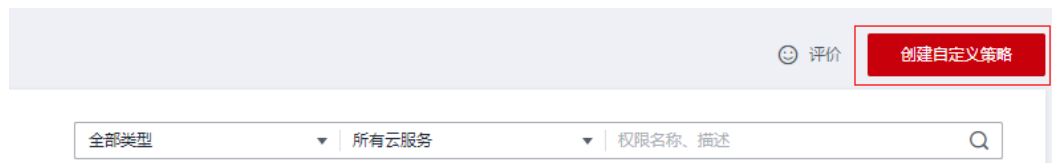
图 3-13 权限列表



- 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，检查该委托权限是否包含**步骤4**中的权限，若无则在现有“Action”中追加斜体加粗内容即可。
- 如果过搜索结果为空，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 3-14 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 3-15 创建自定义策略

* 策略名称

策略配置方式

* 策略内容

```
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 }
```

策略描述

作用范围

```
{
  "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

7. 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 3-16 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 3-17 委托列表



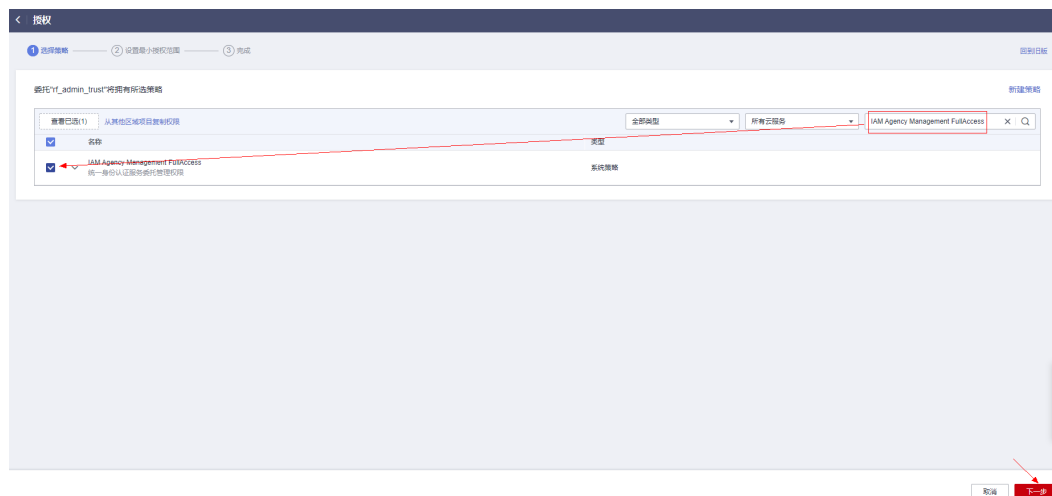
步骤3 进入“授权记录”菜单，单击“授权”按钮。

图 3-18 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 3-19 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 3-20 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

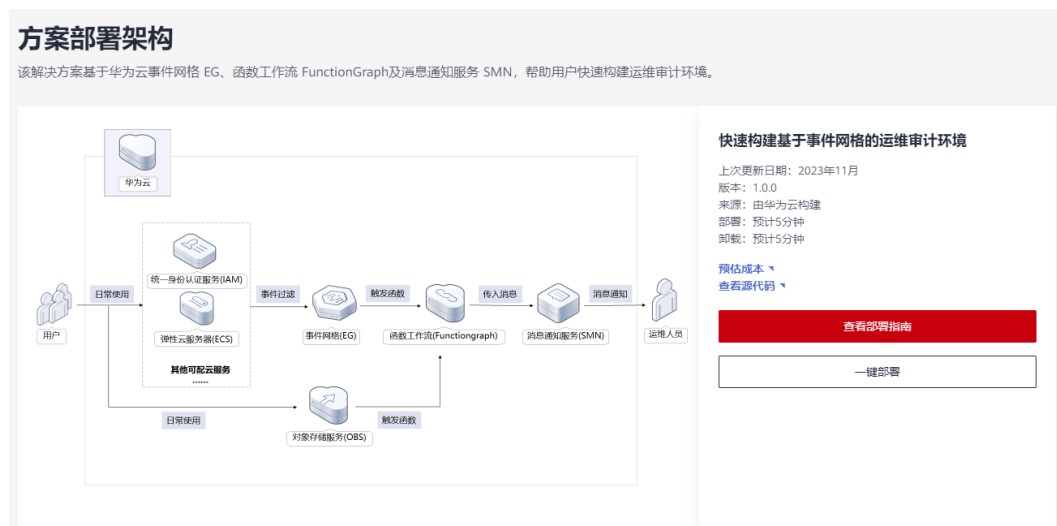
表 3-1 参数说明

参数名称	类型	是否可选	参数解释	默认值
eg_channel_id	string	必填	事件网格 EG中云服务事件通道 ID，默认default通道ID，用于接收云服务事件源产生的事件。获取请参 2. 获取事件网格 EG云服务事件通道ID 。	空
eg_subscription_name	string	必填	事件订阅名称，不允许重名，命名规则： {eg_subscription_name}-ecs (事件源是弹性云服务器 ECS)、 {eg_subscription_name}-iam (事件源是统一身份认证服务 IAM)。取值范围：长度1~124位字符，以字母或数字开头，由字母、数字、点(.)、下划线(_)和中划线(-)组成。	eventgrid-based-om-audit-environment-demo
ecs_ids	list(string)	必填	需要监控的弹性云服务器 ECS ID，长度限制1024字节。获取方式请参考 3. 获取弹性云服务器 ECS ID 。多个id之间用英文逗号隔开，格式为：["id1","id2"...]。	空
obs_names	list(string)	必填	需要监控的对象存储服务 OBS桶名，长度限制1024字节。获取方式请参考 4. 获取对象存储服务 OBS桶名(可选) 。多个名字之间用英文逗号隔开，格式为：["obs1","obs2"...]。	空
files	string	必填	需要监控的存储在上述OBS桶中的文件名，长度限制1024字节，不支持空格。多个名字之间用英文逗号隔开，格式为：file1,file2...。	空
smn_topic_urn	string	必填	消息通知服务 SMN主题URN，该模板使用已有主题，用于当特定的事件源触发后，发送消息通知运维人员。获取请参考 1. 获取消息通知服务 SMN主题URN 。	空

参数名称	类型	是否可选	参数解释	默认值
functiongraph_name	string	必填	函数工作流 Functiongraph函数名称，不支持重名。命名规范：{functiongraph_name}-eg, {functiongraph_name}-obs, 取值范围：长度为1-56个字符，支持字母、数字、_（下划线）和-（中划线），以字母开头，以字母或数字结尾。	eventgrid-based-om-audit-environment-demo

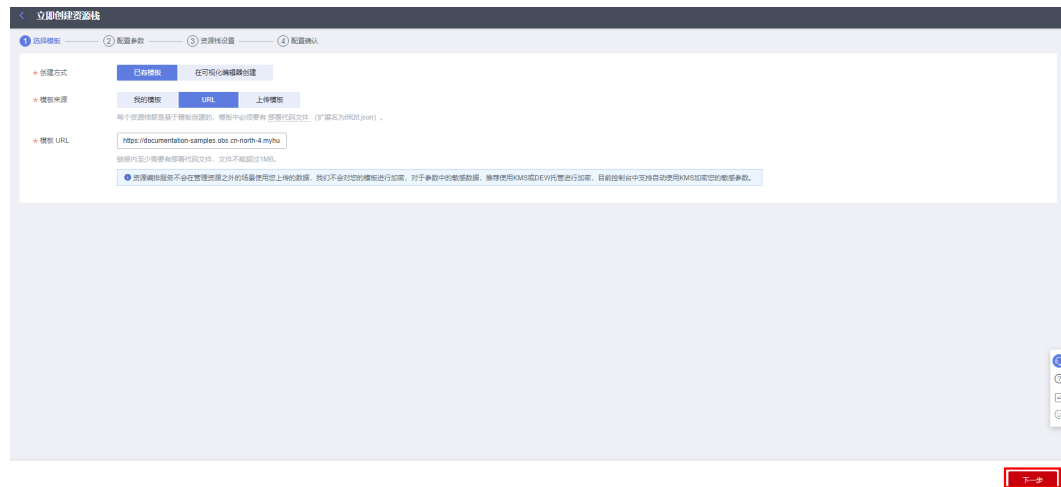
步骤1 登录[华为云解决方案实践](#)，选择“快速构建基于事件网格的运维审计环境”，单击“一键部署”，跳转至解决方案创建资源栈界面。

图 3-21 解决方案实践



步骤2 在选择模板界面中，单击“下一步”。

图 3-22 选择模板



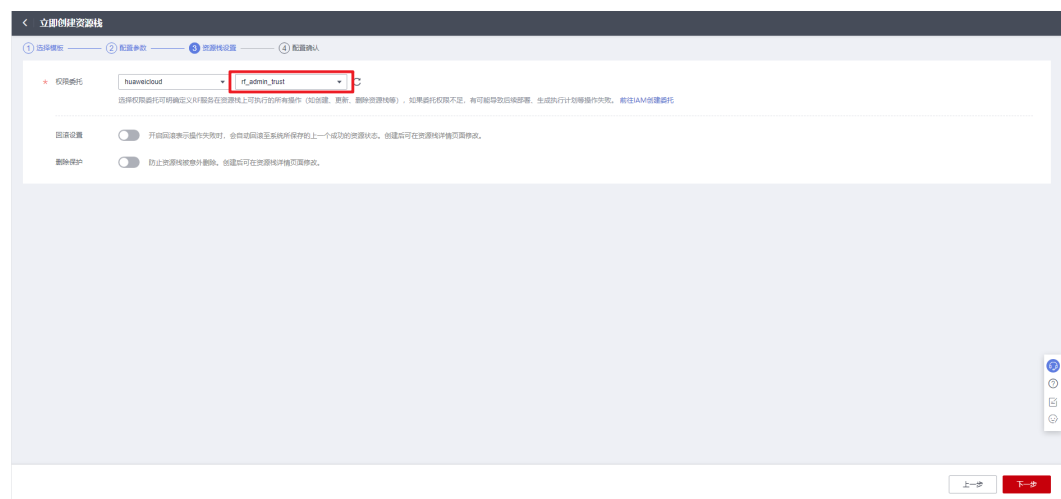
步骤3 在配置参数界面中，参考表3-1 参数填写说明完成自定义参数填写，单击“下一步”。

图 3-23 配置参数



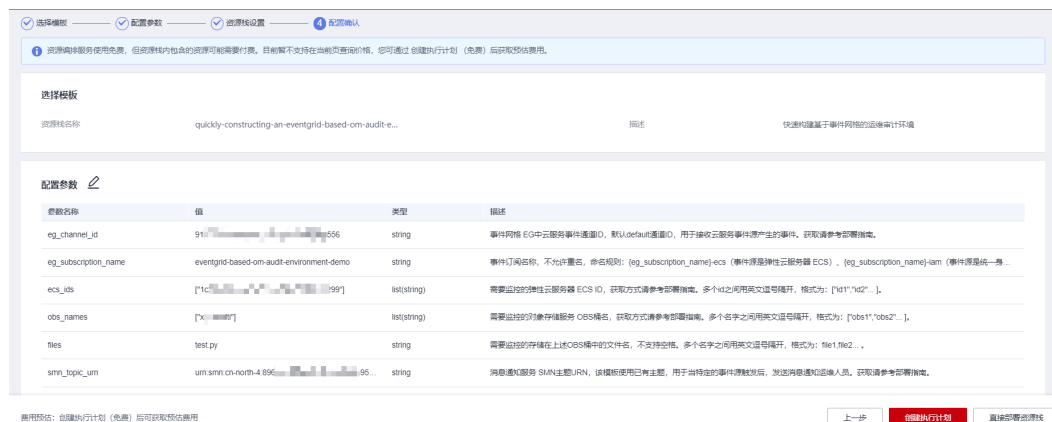
步骤4 （可选，如果使用华为主账号或admin用户组下的IAM子账户可不选委托）在资源设置界面中，在权限委托下拉框中选择“rf_admin_trust”委托，单击“下一步”。

图 3-24 资源栈设置



步骤5 在配置确认界面中，单击“创建执行计划”。

图 3-25 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 3-26 创建执行计划



步骤7 单击“部署”，并且在弹出的执行计划确认框中单击“执行”。

图 3-27 执行计划

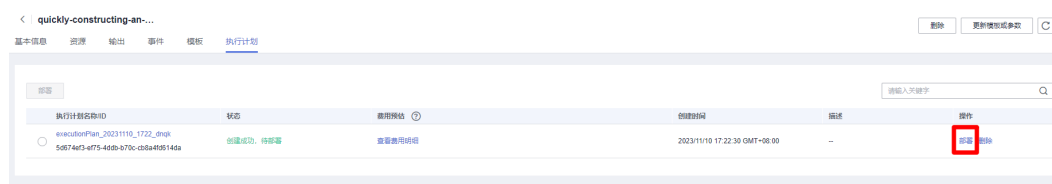
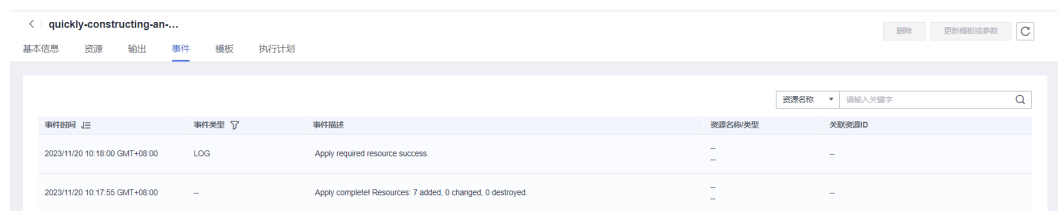


图 3-28 执行计划确认



步骤8 待“事件”中出现“Apply required resource success”，表示该解决方案已经部署完成。

图 3-29 部署完成



----结束

3.3 开始使用

该解决方案默认捕获配置示例监控事件如下（事件源过滤规则）：

- 对象存储服务 OBS：
"put": "使用Put方法上传对象"
"post": "使用Post方法上传对象"
"CompleteMultipartUpload": "表示合并分段任务"
"ObjectRemoved": "表示删除对象"
- 统一身份认证服务 IAM：
"fpwdResetSuccess": "通过忘记密码重置密码"
"createUser": "创建用户"
"deleteUser": "删除用户"
- 弹性云服务器 ECS：
弹性云服务器所提供的接口分为ECS接口与OpenStack原生接口。推荐您使用ECS接口，具体请参考[API版本选择建议](#)。在弹性云服务器控制台操作云服务器及RFS一键部署删除服务器都使用的是ECS接口，本解决方案默认监控ECS接口产生的事件。

```
"deleteServer": "删除云服务器"  
"stopServer": "关闭云服务器"  
"rebootServer": "重启云服务器"
```

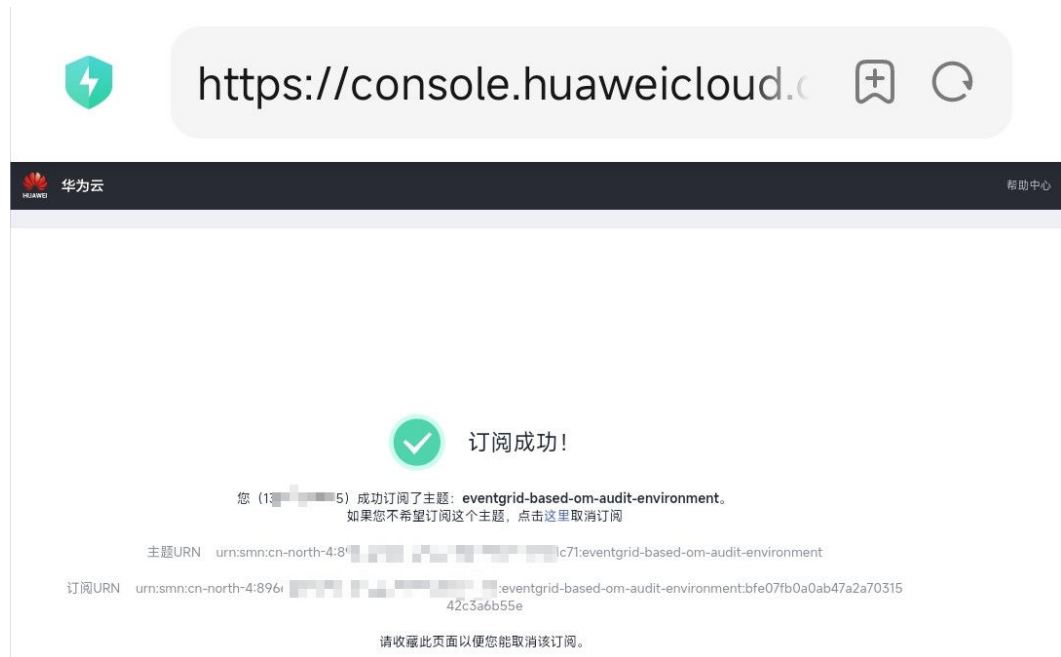
方案验证（以短信示例）

步骤1 解决方案部署成功后，用户会收到来自华为云消息通知服务 SMN发送的订阅邀请，请仔细阅读并确认订阅。

图 3-30 订阅邀请短信



图 3-31 订阅成功



步骤2 登录华为云控制台，选择以上三种任一云服务，对其进行受监控的操作，触发特殊事件行为捕获。

步骤3 手机终端会收到短信通知，记录上述行为。同时函数工作流也会打印相关日志。

图 3-32 事件订阅



步骤4 （可选）进入[函数 workflow](#)选择方案创建的函数，单击函数名称进入。单击“[监控>日志](#)”按下图所示，可以查看日志信息。

图 3-33 进入函数管理界面



图 3-34 查看日志信息



----结束

自定义配置

用户可以参考本指南，自行配置个性化的运维监控环境，详细使用轻参考[事件网格 EG](#)。

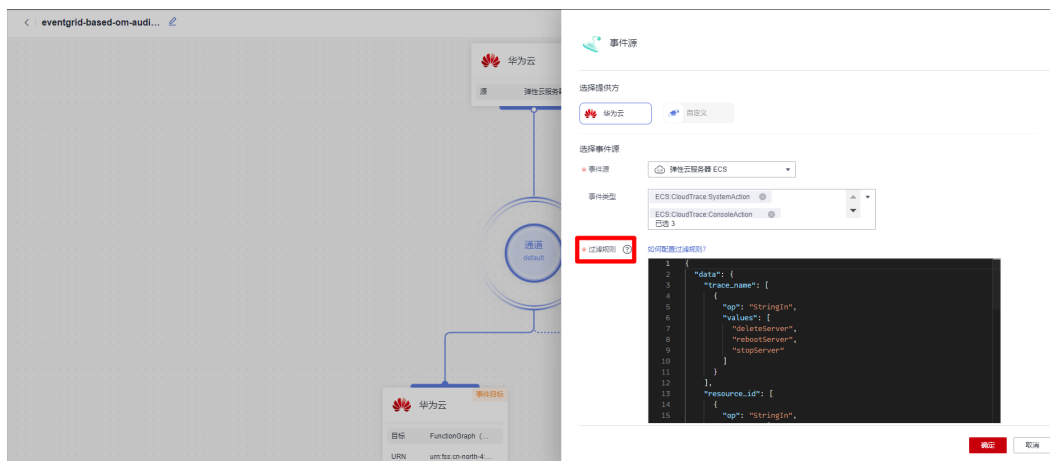
步骤1 登录华为云控制台，打开事件网格EG，进入[事件订阅](#)，查看该解决方案创建的示例事件订阅或[新建事件订阅](#)（对于事件源提供方是非华为云服务的“自定义”，需要先创建自定义[事件通道](#)，如有则忽略）。

图 3-35 事件订阅



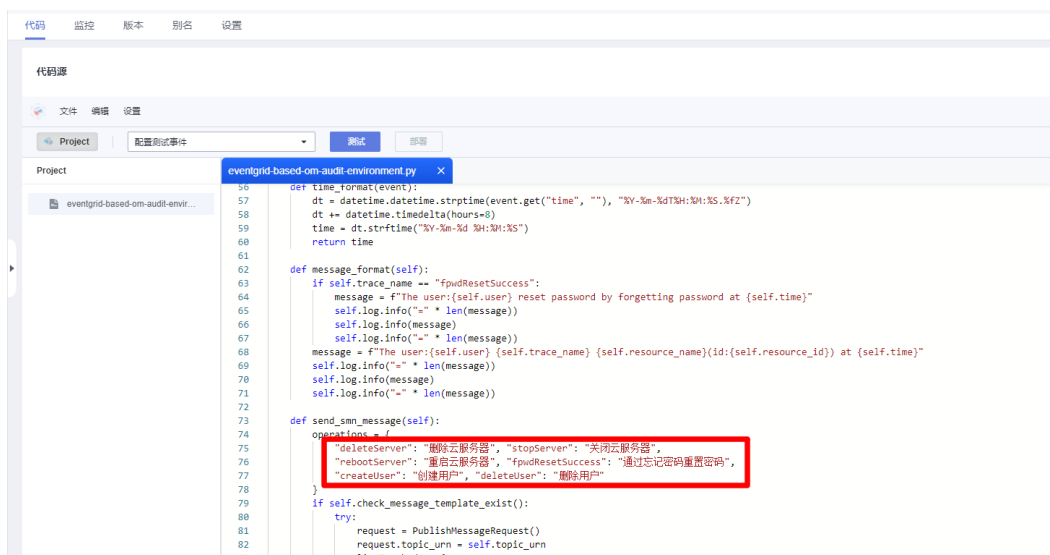
步骤2 选择一个订阅，进入详情页，查看事件订阅的配置详情，如需修改过滤规则请参考[过滤规则说明](#)及[过滤规则示例](#)。

图 3-36 事件订阅详情



步骤3 请登录[函数工作流](#)控制台选择方案创建的函数（后缀为“-eg”），单击函数名称进入，单击“代码”，同步修改过滤规则相关代码后单击“部署”以保存代码（需要一定的代码能力）。

图 3-37 修改源码



步骤4 模拟对云服务的日常使用，事件网格会捕获到特定事件源，用户可以在事件通道中查看事件轨迹。

图 3-38 事件通道



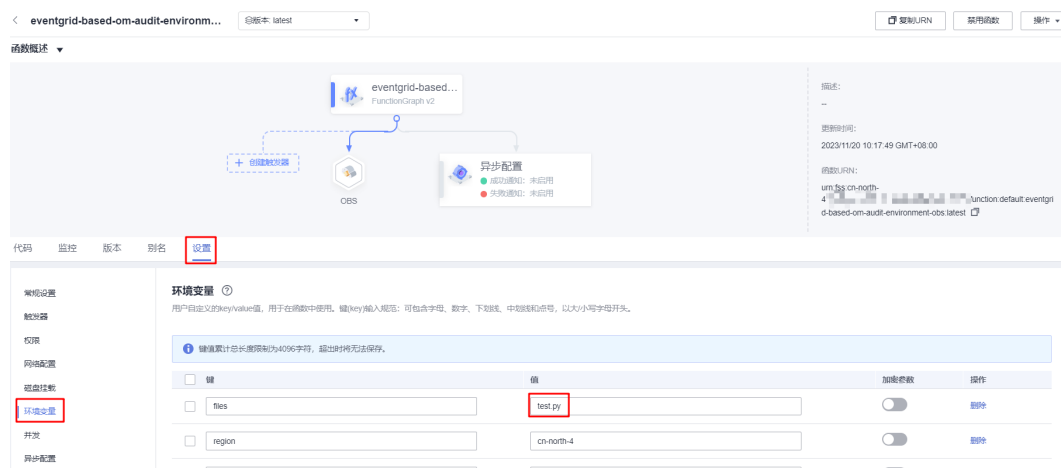
图 3-39 事件轨迹

事件ID	订购名称	事件源	事件类型	投递状态	接收时间	操作
ce4ba29...	eg_...	弹性云服务器 ECS	ECS.CloudTrace.ConsoleAction	投递成功	2023/11/08 15:45:37 GMT+08:00	事件轨迹
2b8f4de1...	eg_...	弹性云服务器 ECS	ECS.CloudTrace.ConsoleAction	投递成功	2023/11/08 16:02:33 GMT+08:00	事件轨迹
5de6429...	eg_...	弹性云服务器 ECS	ECS.CloudTrace.ConsoleAction	投递成功	2023/11/08 16:03:57 GMT+08:00	事件轨迹
330653q...	eg_...	统一身份认证 IAM	IAM.CloudTrace.ConsoleAction	投递成功	2023/11/08 16:09:56 GMT+08:00	事件轨迹
441f1act...	eg_...	统一身份认证 IAM	IAM.CloudTrace.ConsoleAction	投递成功	2023/11/08 16:10:23 GMT+08:00	事件轨迹
c381092...	eg_...	统一身份认证 IAM	IAM.CloudTrace.ConsoleAction	投递成功	2023/11/08 16:21:07 GMT+08:00	事件轨迹
e165e88...	eg_...	统一身份认证 IAM	IAM.CloudTrace.ConsoleAction	投递成功	2023/11/08 16:36:16 GMT+08:00	事件轨迹
ef8d579...	eg_...	弹性云服务器 ECS	ECS.CloudTrace.ConsoleAction	投递成功	2023/11/08 16:50:58 GMT+08:00	事件轨迹

步骤5 事件网格会将事件捕获路由至事件目标，如函数工作流 FunctionGraph。

步骤6 如需修改对象存储桶内文件，请登录[函数工作流](#)控制台选择方案创建的函数（后缀为“-obs”），单击函数名称进入。单击“设置>环境变量”，修改“files”变量值。

图 3-40 修改监控文件



步骤7 如需修改短信通知内容，请修改两个函数的代码。

图 3-41 修改消息模板

```

92
93
94 try:
95     request = PublishMessageRequest()
96     request.topic_urn = self.topic_urn
97     request.body = PublishMessageRequestBody(
98         message=f"【高危操作通知】系统监测到在{time}，桶：{self.bucket_name}中
99         f"文件夹：/{self.directory}下的文件：{self.file} "
100         f"被{operations.get(self.event_name.split(':')[0])}了，请您及时处理。",
101         subject="【华为云】【高危操作通知}"
102     )
103     self.client.publish_message(request)
104 except exceptions.ClientRequestException as e:
105     self.log.error(e.status_code)
106     self.log.error(e.request_id)
107     self.log.error(e.error_code)
108     self.log.error(e.error_msg)

```

----结束

3.4 快速卸载

一键卸载

步骤1 解决方案部署成功后，单击该方案资源栈后的“删除”。

图 3-42 一键卸载



步骤2 在弹出的删除资源栈确定框中，输入Delete，单击“确定”，即可卸载解决方案。

图 3-43 删除资源栈确认



----结束

4 附录

名词解释

- **对象存储服务 OBS**：是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。
- **事件网格 EG**：事件网格（EventGrid，简称EG）是华为云提供的一款Serverless事件总线服务，支持华为云服务、自定义应用、SaaS应用以标准化、中心化的方式接入，通过标准化的CloudEvents协议在这些应用之间以灵活方式路由事件，帮助您轻松构建松耦合、分布式的事件驱动架构。
- **消息通知服务 SMN**：提供云上应用和服务消息传送到多种终端的消息发布订阅服务。

5 修订记录

表 5-1 修订记录

发布日期	修订记录
2023-11-30	第一次正式发布。