组织

快速入门

文档版本	01
发布日期	2024-07-22

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 使用 Organizations 管理多账号

操作场景

组织（以下简称Organizations）云服务为企业用户提供多账号关系的管理能力。当您的企业拥有多个分公司、部门或者不同的业务应用，通过Organizations服务，企业可以在云上构建符合自身管理和工作方式的多层级资源结构，同时将多个分散的华为云账号，纳入到构建的多层级组织单元中，实现对多账号的集中和结构化管理。

本章节为您介绍创建组织、组织单元以及邀请账号加入组织的操作，指导您使用组织对多账号进行结构化管理。

操作流程

操作步骤	说明
准备工作	1. 注册华为账号并开通华为云且完成企业实名认证。 2. 开通企业中心并成为企业主账号。 3. 为账号充值，确保账号未因欠费受限冻结。
步骤一：创建组织	创建组织。
步骤二：创建组织单元	为组织创建多层级组织单元。
步骤三：邀请账号加入组织	组织管理账号邀请其他账号加入组织。
步骤四：移动账号	将成员账号移动至不同的组织单元。

准备工作

1. 注册华为账号并开通华为云且完成企业实名认证。
   a. 打开**华为云官网**，单击“注册”。
   b. 根据提示信息完成注册，详细操作请参见“**注册华为账号并开通华为云**”。
      注册成功后，系统会自动跳转至您的个人信息界面。
   c. 参考**企业账号如何完成实名认证**，完成企业账号实名认证。

2. 开通企业中心并成为企业主账号。

   如果您想创建组织，则需先开通企业中心并成为企业主账号。

   a. 进入“**企业中心**”控制台。

   b. 单击“免费开通”，进入申请开通企业中心页面。

   c. 勾选“我已阅读并同意《华为云企业管理服务使用声明》”，并单击“免费开通”。

      开通后您将自动成为企业主账号。

3. 为账号充值。

   Organizations服务为免费服务，使用Organizations服务的相关功能不收取任何费用。

   但当您的账号因欠费受限冻结后，将无法在Organizations控制台执行任何写操作，因此您需要确保账号有足够的余额，避免因账号欠费冻结而无法使用Organizations服务的相关功能，如何充值请参见**账户充值**。

步骤一：创建组织

步骤1 登录管理控制台。

步骤2 单击页面左上角的 ☰ 图标，在弹出的服务列表中，选择“管理与监管 > 组织 Organizations”。

步骤3 在服务开通页，单击“立即开通”。

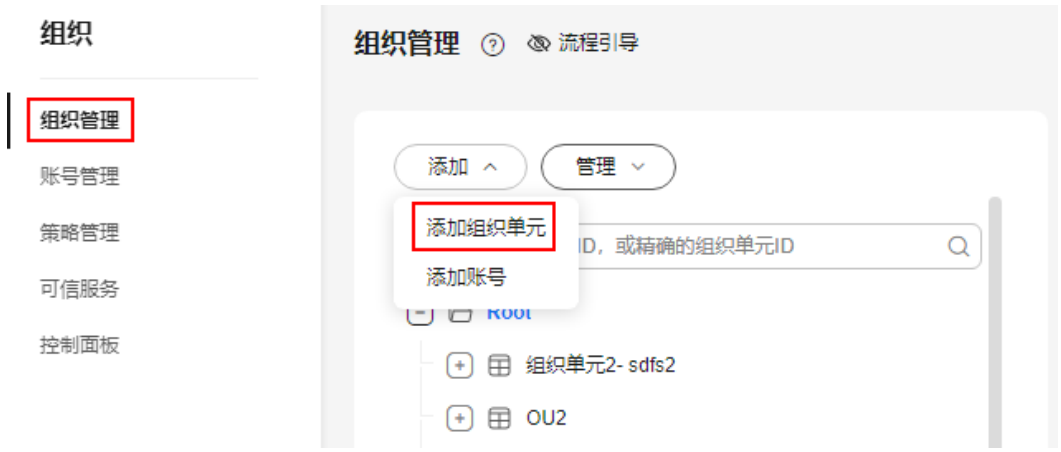
开通Organizations云服务后，系统会自动创建组织和根组织单元，并将开通服务的账号设置为管理账号。

----结束

步骤二：创建组织单元

您可以按各种维度（例如业务范围、账号所有者或账号使用环境）对账号进行分组，相同分组的账号可以使用组织单元（Organizational Units，以下简称OU）进行归类和结构化管理。如下步骤以一个简单的示例来说明如何创建多层级OU，OU最深可嵌套至5层。

步骤1 在Organizations控制台的“组织管理”页面中，选中根OU（Root），单击“添加”，然后单击“添加组织单元”。



步骤2 在弹窗中填写OU名称，此处填写“OU1”，单击“确定”完成OU创建。

步骤3 选中组织单元“OU1”，参考以上步骤，为“OU1”创建子组织单元“OU2”和“OU3”。最终组织结构如下图所示。

----结束

步骤三：邀请账号加入组织

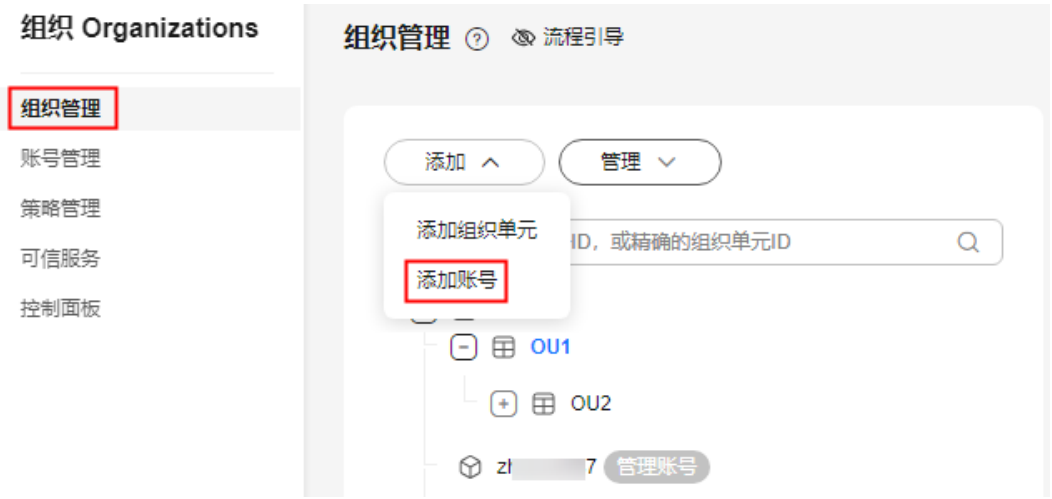
此时您已拥有一个组织，且已搭建简单的组织结构，现在可以开始向其中填充账号，本步骤以邀请账号加入组织为例进行说明。您还可以在组织中直接创建新账号加入组织，具体请参见**创建账号**。

说明

邀请其他成员账号加入组织，要求成员账号需要完成企业或个人实名认证，详情参见：**实名认证**。

邀请加入组织的成员账号，原财务关系不会调整，保留原有企业主子账号之间的财务模式。

步骤1 在Organizations控制台的“组织管理”页面中，单击“添加”，然后单击“添加账号”。



步骤2 在弹窗中输入邀请账号的账号名，例如“Account-1”。单击“确定”，向该账号发出加入组织的邀请。

步骤3 登录Account-1账号，进入Organizations控制台，单击“接受”，账号Account-1成功加入组织。

步骤4 参考以上步骤邀请多个账号加入组织。

----结束

步骤四：移动账号

邀请进入组织的成员账号会默认放置到根OU（Root）中，登录到组织管理账号后，您可以将组织内的账号移动到其他的OU中，对账号进行分组管理。

步骤1 使用组织管理账号登录华为云控制台。

步骤2 进入Organizations控制台的“组织管理”页面，选中要移动的账号，单击“管理”，然后单击“移动账号”。

步骤3 在弹窗中选中要移动的目标组织单元，例如OU2，在下方文本框中输入“确认”，然后单击“确定”，完成账号移动。

步骤4 参考以上步骤将其他账号移动至目标组织单元。

----结束

相关信息

创建组织并构建组织架构完成后，您随时可以对OU和成员账号进行增、删、改、查等操作，当您不需要使用组织功能时，还可删除组织。具体请参见：

- **组织管理**
- **OU管理**
- **账号管理**

2 使用 SCP 控制成员账号的权限

操作场景

服务控制策略 (Service Control Policy，SCP) 是一种基于组织的访问控制策略。组织管理账号可以使用SCP指定组织中成员账号的权限边界，限制账号内用户的操作。SCP可以关联到组织、OU和成员账号。当SCP关联到组织或OU时，该组织或OU下所有账号均受该策略影响。

本章节以创建一个简单的SCP并将其绑定至成员账号为例，帮助您快速了解和使用SCP。

操作流程

操作步骤	说明
准备工作	1. 已创建组织并加入一个成员账号。 2. 为账号充值，确保账号未因欠费受限冻结。
步骤一：启用并创建SCP	启用并创建自定义SCP。
步骤二：绑定SCP	为成员账号绑定SCP。
步骤三：验证SCP	使用成员账号验证SCP是否生效。

准备工作

1. 已创建组织，且组织中至少已加入一个成员账号。具体操作请参见**使用Organizations管理多账号**。
2. 为账号充值。

   Organizations服务为免费服务，使用Organizations服务的相关功能不收取任何费用。

   但当您的账号因欠费受限冻结后，将无法在Organizations控制台执行任何写操作，因此您需要确保账号有足够的余额，避免因账号欠费冻结而无法使用Organizations服务的相关功能，如何充值请参见**账户充值**。

步骤一：启用并创建 SCP

例如您希望组织内的某一成员账号无法删除RAM服务的资源共享实例，可以参考如下示例创建SCP。

如下步骤仅针对示例中的关键参数进行设置和介绍，其他参数保存默认，更多SCP的详细信息请参见**创建SCP**。

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入Organizations控制台。

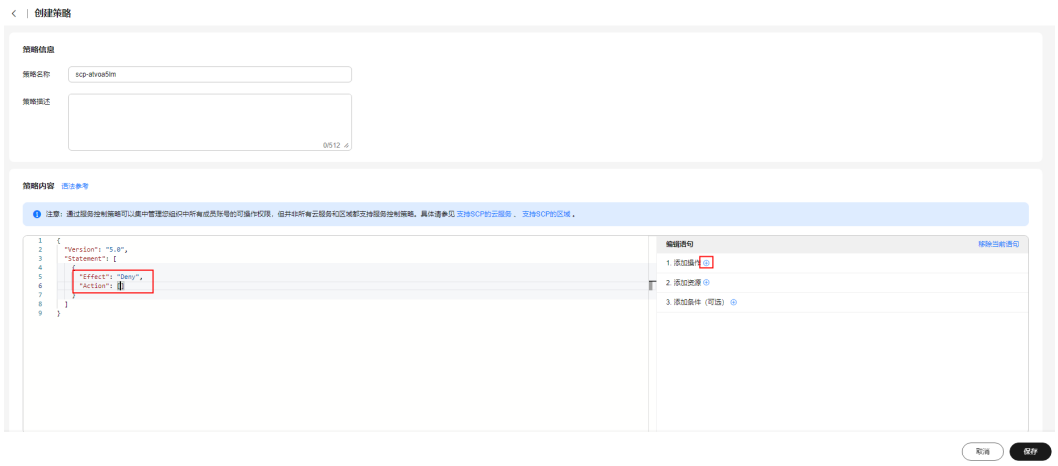
步骤2 在左侧导航中选择“策略管理”，单击“服务控制策略”操作列的“启用”。

步骤3 在弹窗中勾选确认框，然后单击“确定”，完成SCP功能启用。

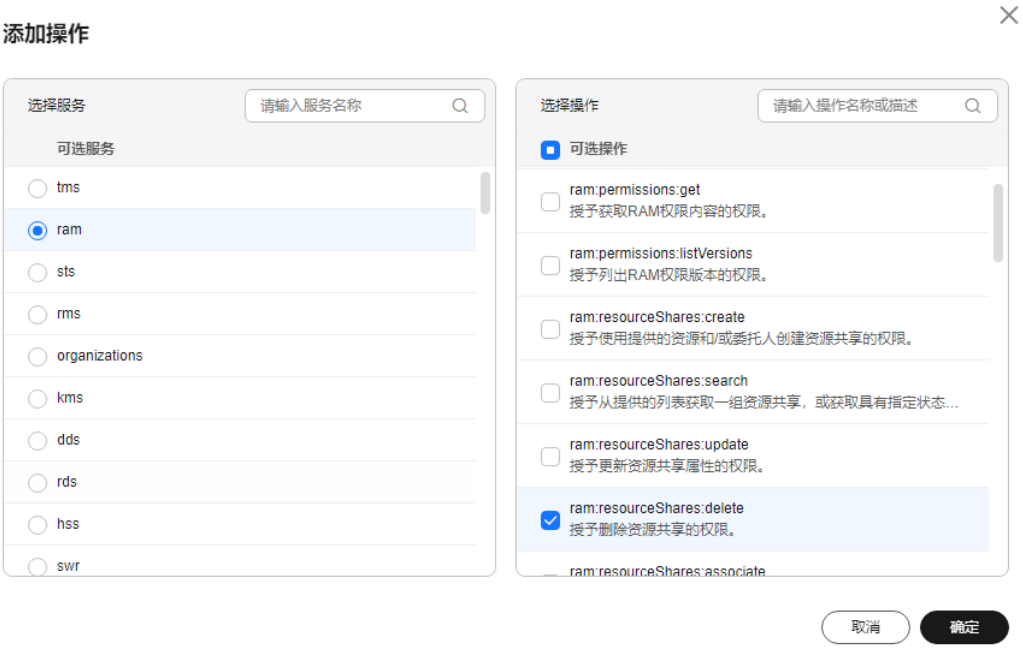
步骤4 单击“服务控制策略”，进入SCP管理页。

步骤5 单击“创建”，进入创建策略页面。

步骤6 在策略内容左侧单击策略语句中的“Effect”或“Action”，然后在右侧的策略编辑器中单击“添加操作”后的“+”号。



步骤7 在弹窗中选择RAM服务的“ram:resourceShares:delete”操作，单击“确定”。



步骤8 单击“添加资源”后的“+”号，在弹窗中选择RAM服务的“所有资源”，单击“确定”。

最终的策略内容如下，表示禁止删除RAM服务的资源共享实例：

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:delete"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

步骤9 单击页面右下角的“保存”，自定义SCP创建完成。

----结束

步骤二：绑定 SCP

将创建的SCP与某一成员账号进行绑定后，该成员账号将被禁止删除资源共享实例。

步骤1 在SCP策略列表中，单击上一步创建的SCP操作列的“绑定”。

步骤2 在弹窗中选择要绑定的成员账号，在文本框中输入“确认”，然后单击“确定”，完成SCP绑定。

须知

策略完成绑定后将在30分钟内生效。

----结束

步骤三：验证 SCP

本步骤对SCP的权限管控效果进行验证。

步骤1 以绑定该SCP的成员账号登录管理控制台，进入RAM服务控制台。

步骤2 尝试删除资源共享实例，页面报错，SCP生效。

----结束

相关信息

本章节仅使用一个简单的SCP为例进行说明，如您想使用SCP实现更为复杂的权限控制，可参考如下内容：

- SCP的详细说明请参见**SCP原理介绍**和**SCP语法介绍**，其中包括策略语句中可使用的全局级条件键以及运算符的详细说明和示例。
- 目前支持SCP的服务请参见**支持SCP的云服务**，各云服务支持的授权项、资源类型和服务级条件键的详细说明请参见**SCP授权参考**。
- 常用的SCP示例请参见**SCP示例**。

3 使用标签策略规范资源的标签

操作场景

标签策略是策略的一种类型，可帮助您在组织账号中对资源添加的标签进行标准化管理。在标签策略中，您可以限定为资源添加的标签必须符合规范。标签策略对未添加标签的资源或未在标签策略中定义的标签不会生效。

当您需要对组织中的标签进行标准化管理时，可以通过创建标签策略来制定标签创建的规则。

本章节以创建一个简单的标签策略并将其绑定至成员账号为例，帮助您快速了解和使用标签策略。

操作流程

操作步骤	说明
准备工作	1. 已创建组织并加入一个成员账号。 2. 为账号充值，确保账号未因欠费受限冻结。
步骤一：启用并创建标签策略	启用并创建标签策略。
步骤二：绑定标签策略	为成员账号绑定标签策略。
步骤三：验证标签策略	使用成员账号测试标签策略是否生效。

准备工作

1. 已创建组织，且组织中至少已加入一个成员账号。具体操作请参见**使用Organizations管理多账号**。
2. 为账号充值。

   Organizations服务为免费服务，使用Organizations服务的相关功能不收取任何费用。

但当您的账号因欠费受限冻结后，将无法在Organizations控制台执行任何写操作，因此您需要确保账号有足够的余额，避免因账号欠费冻结而无法使用Organizations服务的相关功能，如何充值请参见**账户充值**。

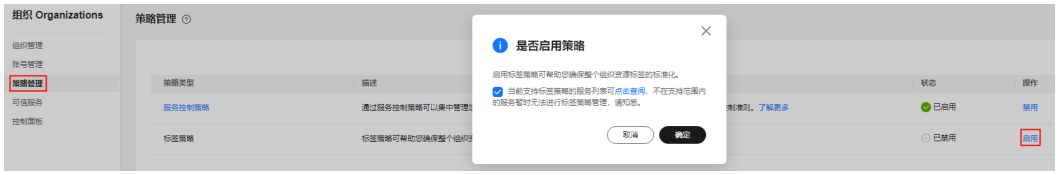
步骤一：启用并创建标签策略

如下步骤仅针对示例中的关键参数进行设置和介绍，其他参数保存默认，更多创建标签策略的详细信息请参见**创建标签策略**。

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入Organizations控制台。

步骤2 进入策略管理页，单击标签策略操作列的“启用”。

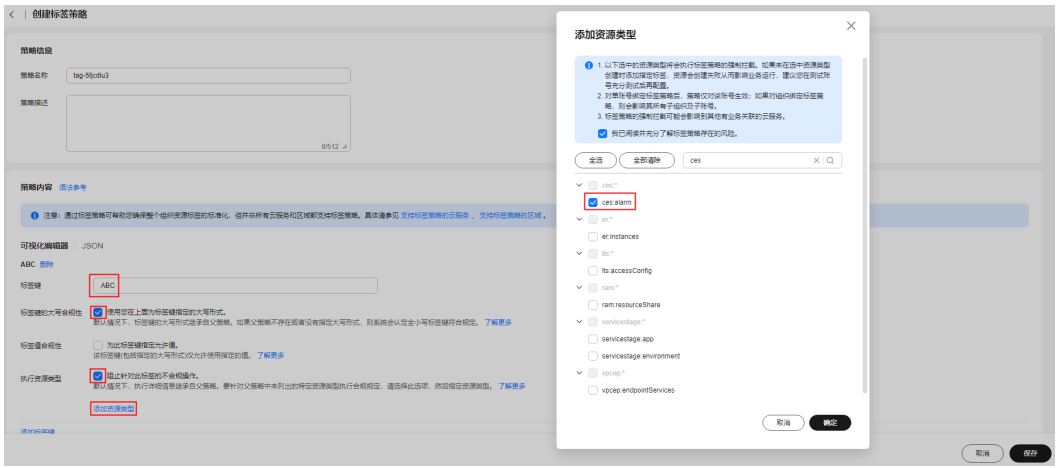
步骤3 在弹窗中勾选确认框，然后单击“确定”，完成标签策略功能启用。



步骤4 单击“标签策略”，进入标签策略管理页。

步骤5 单击“创建”，进入创建标签策略页面。

步骤6 参考如下说明设置标签策略内容，其他参数均可保持默认配置。



参数	示例	说明
标签键	**ABC**	设置标签策略定义的标签的键。 标签策略仅会对此处设置的标签生效。

参数	示例	说明
标签键的大写合规性	**勾选此项**	指定标签键的大小写形式来定义合规性。 勾选此项则表示使用标签键的大小写形式进行校验，也就是说为资源添加的标签的键为“ABC”则符合规范，添加“abc”、“Abc”等其他大小写形式的标签则为不合规，标签策略将阻止不合规标签的添加操作。
执行资源类型	**ces:alarm**	指定执行标签策略检查的资源类型。 勾选此项后单击“添加资源类型”，在弹窗中阅读并勾选确认标签策略存在的风险说明，然后选择资源类型，单击“确定”。

步骤7 单击右下角的“保存”，标签策略创建成功。

----结束

步骤二：绑定标签策略

将创建的标签策略与某一成员账号进行绑定后，该成员账号为相关资源添加标签时，需要遵循此标签策略定义的标签规范。

步骤1 在标签策略列表中，单击上一步创建的标签策略操作列的“绑定”。

步骤2 在弹窗中选择要绑定的成员账号，单击“确定”，完成标签策略绑定。

须知

策略完成绑定后将在30分钟内生效。

----结束

步骤三：验证标签策略

本步骤对标签策略的标签规范管理效果进行验证。

步骤1 以绑定该标签策略的成员账号登录管理控制台，进入云监控服务控制台，**创建告警规则**并为其添加标签，验证标签策略是否生效。

1. 为告警规则添加标签“ABC”，标签添加成功。
2. 为告警规则添加标签“abc”，界面提示此标签校验不合规，需修改后再次提交，表示标签策略已生效且验证无误。

⚠ 注意

当您在创建资源时添加不合规的标签，标签策略将阻止标签添加操作，同时资源也无法创建成功；

当您为已创建的资源添加不合规标签时，标签策略仅会阻止标签添加操作，不会对资源产生影响。

----结束

相关信息

关于标签策略更多的其他操作请参见**标签策略管理**。

4 基于可信服务提供组织级能力

操作场景

可信服务是指可与Organizations服务集成，提供组织级相关能力的华为云服务。管理账号可以在组织中开启某个云服务为可信服务。成为可信服务后，云服务可以获取组织中的组织单元及成员账号信息，并基于此信息提供组织级的管理能力。

本章节以启用Config为可信服务并创建组织合规规则“**IAM用户在指定时间内有登录行为**”为例，为您展示可信服务功能的具体使用场景。

操作流程

操作步骤	说明
准备工作	1. 已创建组织并加入一个成员账号。 2. 在Config服务开启资源记录器。 3. 为账号充值，确保账号未因欠费受限冻结。
步骤一：启用可信服务	启用Config为可信服务。
步骤二：创建组织合规规则	在Config服务使用组织级能力创建组织合规规则。

准备工作

1. 已创建组织，且组织中已加入多个成员账号。具体操作请参见**使用Organizations管理多账号**。
2. 本示例需在Config服务创建组织合规规则，由于仅被资源记录器收集的资源可参与资源评估，因此创建组织合规规则之前您需要**开启资源记录器**。
3. 为账号充值。

   Organizations服务为免费服务，使用Organizations服务的相关功能不收取任何费用。

   但当您的账号因欠费受限冻结后，将无法在Organizations控制台执行任何写操作，因此您需要确保账号有足够的余额，避免因账号欠费冻结而无法使用Organizations服务的相关功能，如何充值请参见**账户充值**。

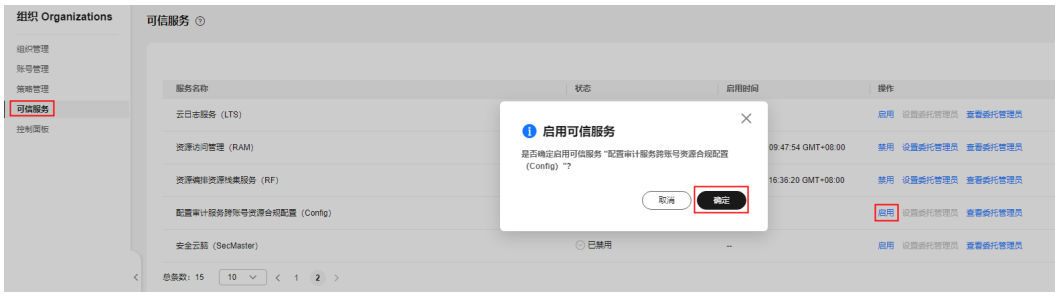
步骤一：启用可信服务

步骤1 以组织管理员或管理账号的身份登录管理控制台，进入Organizations控制台。

步骤2 在左侧导航中选择“可信服务”，进入可信服务页面。

步骤3 在可信服务列表中单击Config服务操作列的“启用”。

步骤4 在弹窗中单击“确定”，完成可信服务启用。



----结束

步骤二：创建组织合规规则

在组织中启用Config为可信服务后，您将可以在Config服务中使用组织级的相关功能，本步骤以创建Config服务的组织预定义合规规则为例进行说明。

如下步骤仅针对示例中的关键参数进行设置和介绍，其他参数保存默认，更多关于Config服务组织合规规则的详细信息请参见**组织合规规则**。

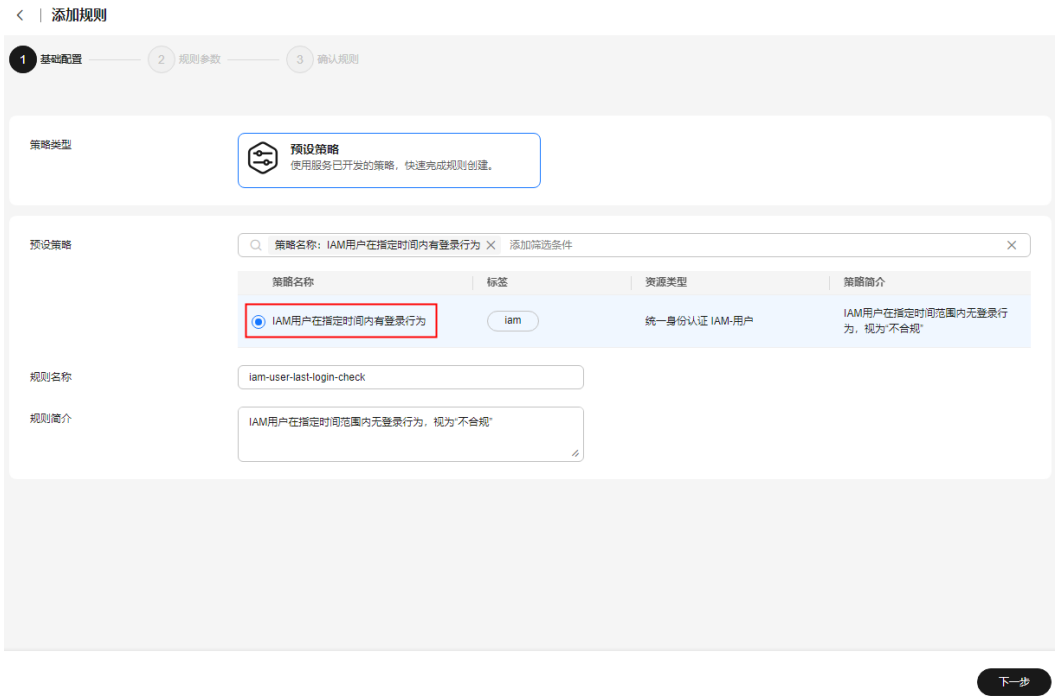
步骤1 以组织管理员账号或者Config服务的委托管理员账号登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”。

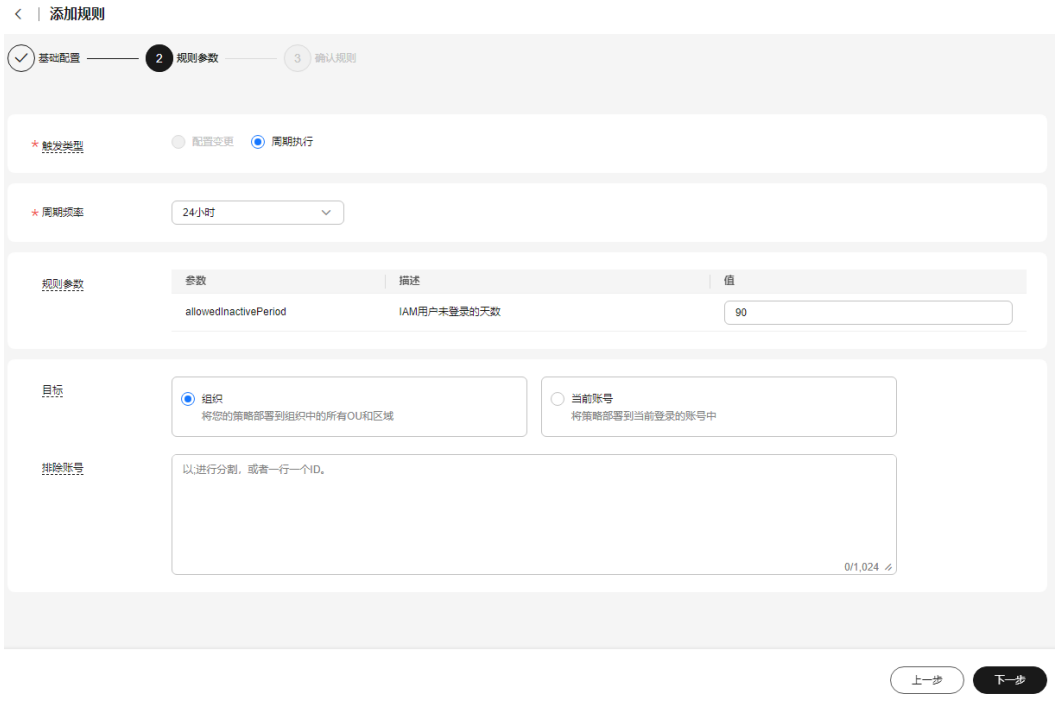
步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 选择“组织规则”页签，单击“添加规则”。

步骤5 进入“基础配置”页面，在预设策略列表中选择“IAM用户在指定时间内有登录行为”，单击“下一步”。



步骤6 进入“规则参数”页面，规则部署目标默认为“组织”无需修改，单击“下一步”。



步骤7 进入“确认规则”页面，确认规则信息无误后，单击“提交”按钮，完成预定义组织合规规则的创建。

说明

当组织合规规则部署成功后，会在组织内成员账号的规则列表中显示此组织合规规则，系统将自动在此规则名称前添加“Org-”字段用于标识。

组织内的成员账号只能触发此规则的评估和查看规则评估结果以及详情，该组织合规规则的修改和删除操作只能由创建规则的组织账号进行。

----结束

相关信息

本章节仅举例说明可信服务功能如何使用，关于已对接组织的可信服务和设置委托管理员等其他更多内容请参见**可信服务管理**。