资源访问管理

用户指南

文档版本 01

发布日期 2025-11-05

华为云计算技术有限公司

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云计算技术有限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，华为云计算技术有限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。

目 录

1 共享您的资源

1.1 共享您的资源概述

资源访问管理（Resource Access Manager，简称RAM）服务为用户提供安全的跨账号共享资源的能力。如果您有多个账号，您可以创建一次资源，并使用RAM服务将该资源共享给其他账号使用。如果您的账号由组织管理，则您可以直接与组织、OU或成员账号共享资源，还可以输入账号ID与账号共享，无论账号是否属于组织。

本章节将为您介绍如下内容：

- **创建共享**
- **更新共享**
- **查看共享**
- **删除共享**
- **查看您共享的资源**
- **查看资源使用者**

1.2 创建共享

操作场景

要共享您拥有的资源给其他账号使用时，需要创建共享。创建共享的流程分为指定共享资源、权限配置、指定使用者以及配置确认。

操作步骤

1. 登录**华为云控制台**。
2. 单击页面左上角的 ☰ ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。
3. 单击左侧的“我的共享”，选择“共享管理”。
4. 单击页面右上角的“创建共享”。

图 1-1 创建共享

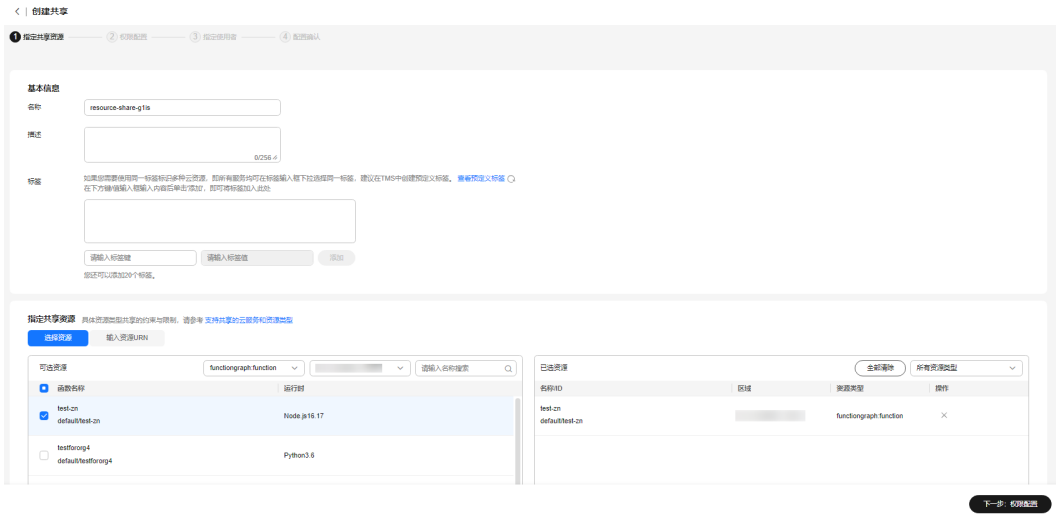
5. 进入指定共享资源页面，配置基本信息并指定共享资源，配置完成后，单击页面右下角的“下一步：权限配置”。

   您可以根据需要选择如下两种方式中的其中一种方式指定共享资源：

   - 选择资源：在列表上方选择资源类型和区域，还支持输入资源名称进行搜索，然后在列表中直接勾选共享资源。此方式仅支持选择到区域层级下的资源，如在列表中无法选到需要共享的资源，可使用直接输入资源URN的方式进行指定。
   - 输入资源URN：在输入框中直接输入资源的URN，多个资源URN之间需用“;”分隔开。

     资源URN的具体构成为“服务名:区域ID（regionID）:账号ID（domainID）:资源类型:资源ID”。例如：pca:cn-north-7:05c734152f00d4200f2bc0179ac6c5e0:ca:305fd6b0-c15f-42f8-81b4-b41de0fccd93。其中全局级资源URN中的regionID为空，例如：anc::05c734152f00d4200f2bc0179ac6c5e0:anc:3ad31999-1a97-4282-901e-63706f122b4d。

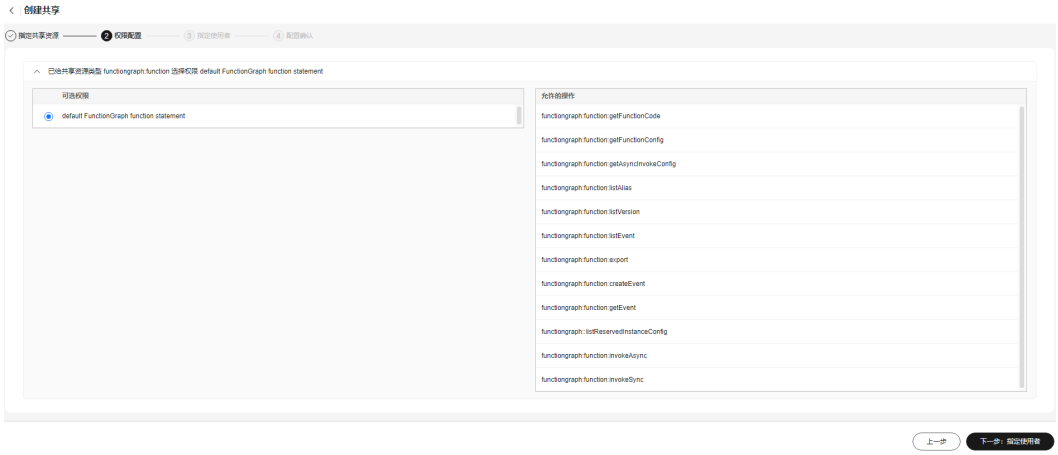
图 1-2 指定共享资源



6. 进入“权限配置”页面，选择指定资源类型支持的共享权限，配置完成后，单击页面右下角的“下一步：指定使用者”。

   此处可选的权限是RAM针对不同资源类型预置的系统权限，某些资源类型定义了多个预置的系统权限，您可以根据自身业务需求进行选择，如何查看每种权限的详细信息请参见：**查看RAM权限库**。

图 1-3 权限配置



7. 进入“指定使用者”页面，指定共享资源的使用者，配置完成后，单击页面右下角的“下一步：配置确认”。

   指定使用者时您可以选择“允许共享给任何华为云账号”或“仅允许在组织内共享”，当选择“仅允许在组织内共享时”，指定的使用者必须为您组织内的成员。

   使用者类型可选择“组织”或“华为云账号ID”，如果您未打开“启用与组织共享资源”开关，使用者类型将无法选择“组织”，具体请参见**启用与组织共享资源**。

图 1-4 指定使用者-华为云账号

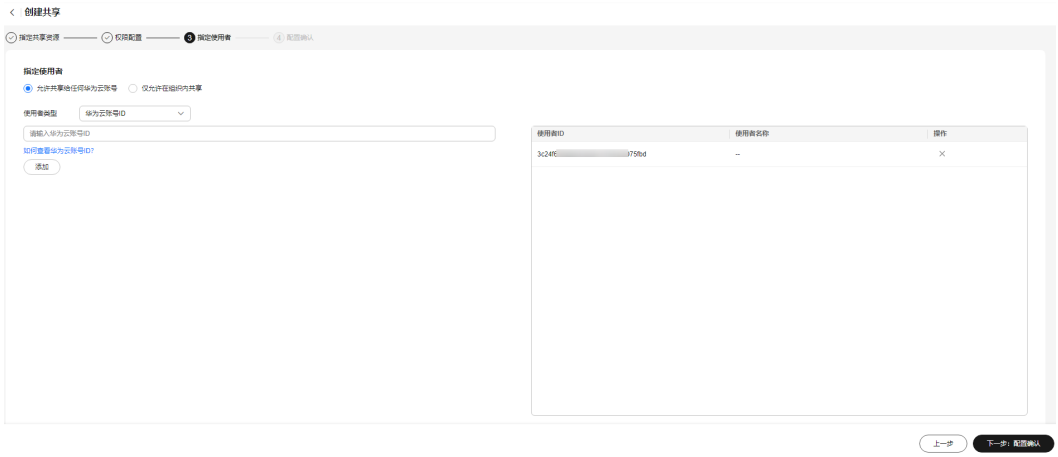
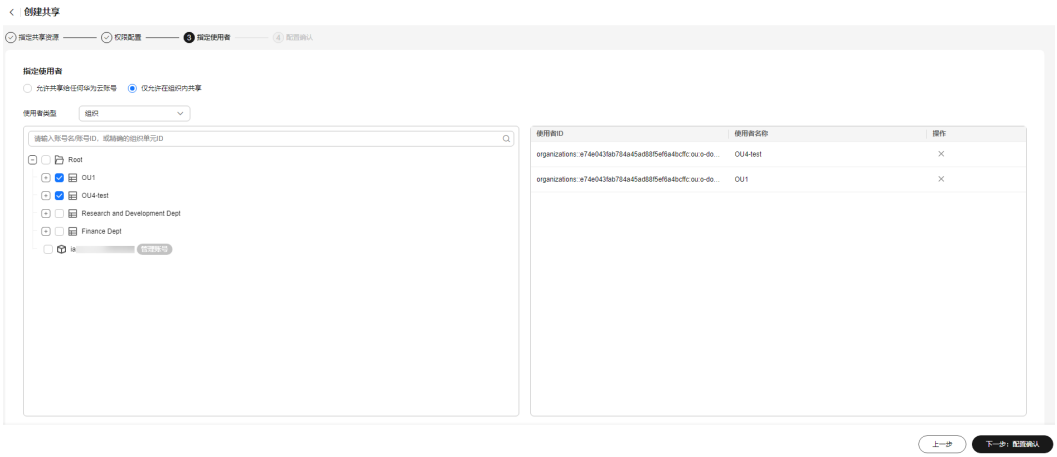
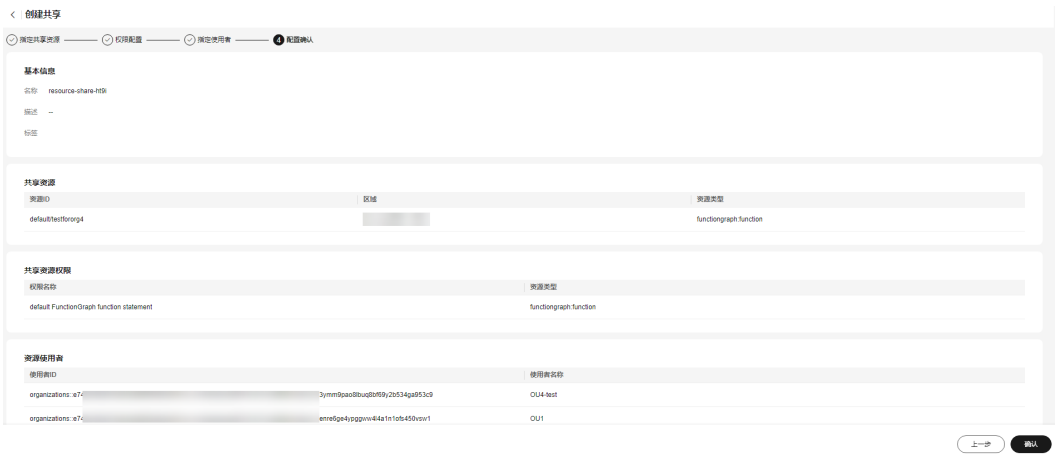


图 1-5 指定使用者-组织



8. 进入“配置确认”页面，确认配置无误后，单击页面右下角的“确认”，完成资源共享实例的创建。

图 1-6 配置确认



共享创建完成后，RAM会向指定的使用者发送共享邀请，使用者需接受共享邀请后，才可以访问和使用被共享的资源；如果指定的使用者与您属于同一组织，且启用“启用与组织共享资源”功能，则指定的使用者无需接受邀请即可访问和使用被共享的资源。

说明

每个资源使用者最多只能被共享100个VPC子网。

1.3 更新共享

操作场景

您可以随时更新资源共享实例，支持更新资源共享实例的名称、描述、标签、共享的资源、共享权限以及共享使用者。

操作步骤

1. 登录华为云控制台。
2. 单击页面左上角的 ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。
3. 单击左侧的“我的共享”，选择“共享管理”。
4. 在共享管理列表中选择需要更新的共享，单击“操作”列的“编辑”。

图 1-7 更新共享

5. 进入“指定共享资源”页面，您可更新共享的名称、描述、标签以及增加或删除共享的资源。更新完成后，单击页面右下角的“下一步：权限配置”。

   说明

   在共享的编辑页面移除共享资源时，每次最多支持移除20个原有资源，如需移除20个以上的原有资源，请分多次编辑完成，或在共享详情页操作，具体请参见进入共享详情页。

6. 进入“权限配置”页面，您可增加或删除指定资源类型支持的共享权限，更新完成后，单击页面右下角的“下一步：指定使用者”。
7. 进入“指定使用者”页面，您可更改指定使用者的范围（“允许共享给任何华为云账号”或“仅允许在组织内共享”），还可以增加或删除共享资源的使用者，配置完成后，单击页面右下角的“下一步：配置确认”。
8. 进入“配置确认”页面，确认配置无误后，单击页面右下角的“确定”，完成共享的更新。

1.4 查看共享

操作场景

您可以通过共享管理列表查看所有已创建共享的详情，并支持在列表中进行搜索、编辑和删除共享的操作，便于您管理共享。

操作步骤

1. 登录华为云控制台。
2. 单击页面左上角的 ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。
3. 单击左侧的“我的共享”，选择“共享管理”。
4. 进入“共享管理”页面，在列表中可查看所有已创建的共享。

   列表上方的搜索框支持根据共享名称、ID、状态和标签进行搜索。
5. 在列表中的“操作”列可对共享进行“编辑”和“删除”操作，在“共享名称/ID”列可直接修改共享名称和复制共享名称和ID。

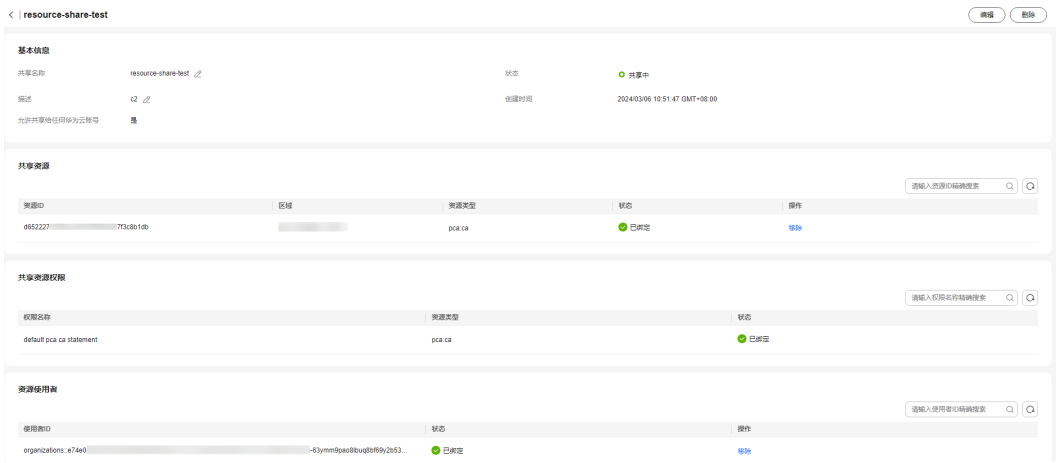
图 1-8 共享管理列表

6. 在列表中单击需要查看的共享名称，进入共享详情页，查看该共享的详细配置。

   共享详情页支持直接修改共享名称和描述以及移除共享资源和资源使用者，还支持添加、删除和修改标签的操作。

   在页面右上方单击“编辑”按钮可跳转至“编辑共享”界面进行操作，单击“删除”按钮可对共享进行删除操作。

图 1-9 共享详情



1.5 删除共享

操作场景

当您不再需要某个共享时，可以随时将其删除，共享删除后，共享资源指定的使用者将无法继续使用该共享中的资源。删除共享不会删除共享的资源。

共享删除后，已删除的共享在RAM控制台上的共享管理页面48小时内仍然可见，但其状态更改为“已删除”，系统将会在48小时后自动删除“已删除”状态的共享。

前提条件

删除共享之前需要移除此共享关联的全部资源。

在共享管理列表中单击需要操作的共享的名称，进入共享详情页移除全部共享资源。

操作步骤

1. 登录华为云控制台。
2. 单击页面左上角的 ☰ ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。

3. 单击左侧的“我的共享”，选择“共享管理”。
4. 在共享管理列表中选择需要删除的共享，单击“操作”列的“删除”。
5. 在弹出的确认框中单击“确定”，完成共享的删除。

图 1-10 删除共享

1.6 查看您共享的资源

操作场景

您可以在共享资源列表中查看您共享的所有资源。该列表可帮助您确定当前共享的资源、这些资源的共享数量以及资源使用者数量。

操作步骤

1. 登录华为云控制台。
2. 单击页面左上角的 ☰ ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。
3. 单击左侧的“我的共享”，选择“共享资源”。
4. 在共享资源列表中可查看资源ID、区域、资源类型、共享数量和资源使用者数量的信息。

   您可以在页面上方的搜索框中通过资源ID和区域快速筛选出需要查看的资源。
5. 在列表中选择需要查看的资源，单击“共享数量”列的数字，界面将跳转至“共享管理”页面并自动筛选出包含此资源的共享实例。
6. 在列表中选择需要查看的资源，单击“资源使用者数量”列的数字，界面将跳转至“资源使用者”页面并自动筛选出此资源的使用者。

图 1-11 共享的资源列表

1.7 查看资源使用者

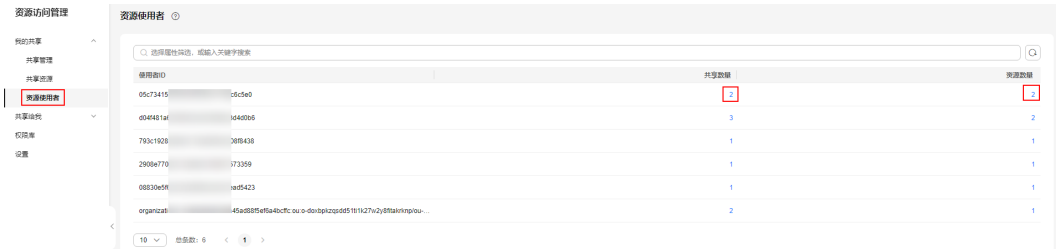
操作场景

您可以在资源使用者列表中查看您共享的资源的所有使用者。该列表可帮助您确定当前的共享资源使用者以及各使用者关联的共享和资源数量。

操作步骤

1. 登录**华为云控制台**。
2. 单击页面左上角的 ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。
3. 单击左侧的“我的共享”，选择“资源使用者”。
4. 在资源使用者列表中可查看使用者ID、共享数量和资源数量的信息。
   您可以在页面上方的搜索框中通过使用者ID快速筛选出需要查看的资源使用者。
5. 在列表中选择需要查看的使用者，单击“共享数量”列的数字，界面将跳转至“共享管理”页面并自动筛选出共享给此使用者的共享实例。
6. 在列表中选择需要查看的使用者，单击“资源数量”列的数字，界面将跳转至“共享资源”页面并自动筛选出此使用者可访问的资源。

图 1-12 资源使用者列表



2 使用共享资源

2.1 使用共享资源概述

当资源的所有者与您的账号共享资源时，接受共享邀请后您就可以访问和使用共享的资源，就像您的账号拥有它一样。资源的所有者可以依据最小权限原则和不同的使用诉求，选择不同的共享权限，提升了资源访问的安全性。

本章节将为您介绍如下内容：

- **接受/拒绝共享邀请**
- **退出共享**
- **查看共享给您的资源**
- **查看资源所有者**

2.2 接受/拒绝共享邀请

操作场景

要访问共享资源，资源所有者必须将您指定为共享资源的使用者。

- 如果资源所有者与您属于同一组织，且启用“启用与组织共享资源”功能，则您将自动获得共享资源的访问权限，无需接受邀请。
- 如果资源所有者与您不属于同一组织，或者属于同一组织但未启用“启用与组织共享资源”功能，则您将收到加入资源共享实例的邀请。
- 如果您收到加入资源共享实例的邀请，则必须接受该邀请才能访问其共享的资源。这些资源可直接在每个资源的管理控制台上使用。如果您拒绝资源共享实例的邀请，您将无法访问此共享资源。

说明

资源共享实例的邀请默认保留7天，如果您在到期前未接受邀请，系统会自动拒绝邀请，如您还需使用共享资源，请再次创建共享实例以生成新的邀请。

操作步骤

1. 登录华为云控制台。
2. 单击页面左上角的 ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。
3. 单击左侧的“共享给我”，选择“共享管理”。
4. 选择“待接受共享”页签，在列表中选择您需要接受或拒绝的共享，在“操作”列单击“接受”或“拒绝”按钮。

图 2-1 接受/拒绝共享邀请

5. 在弹出的对话框中，单击“接受”。

   接受共享邀请后，在“已接受共享”页签中可以查看所有已接受的共享，在列表中单击需要查看的共享名称，进入共享详情页，可查看该共享的详细配置。

   说明

   每个资源使用者最多只能接受100个VPC子网的共享。

2.3 退出共享

操作场景

如果您不再需要访问共享给您的资源，您可以随时退出共享。退出共享后，您将失去对共享资源的访问权限。

只有当资源所有者是作为个人账号与您共享资源，而不是在同一组织中与您共享时，您才可以退出此共享。如果资源所有者与您属于同一组织，且启用“启用与组织共享资源”功能，则您无法退出此共享，因为同组织内的资源共享是自动获得访问权限的，无需接受邀请。

操作步骤

1. 登录华为云控制台。
2. 单击页面左上角的 ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。
3. 单击左侧的“共享给我”，选择“共享管理”。
4. 选择“已接受共享”页签，在列表选择需要退出的共享，单击“操作”列的“退出”按钮。
5. 在弹出的对话框中，单击“退出”。

图 2-2 退出共享

2.4 查看共享给您的资源

操作场景

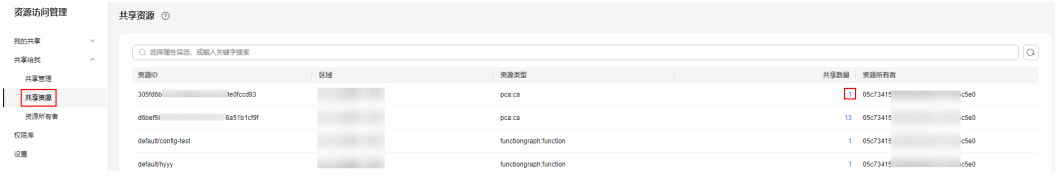
您可以在共享资源列表中查看共享给您的所有资源，以及各资源的所有者和包含这些资源的共享实例。

操作步骤

1. 登录华为云控制台。
2. 单击页面左上角的 ☰ ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。
3. 单击左侧的“共享给我”，选择“共享资源”。
4. 在共享资源列表中可查看资源ID、区域、资源类型、共享数量和资源所有者的信息。

   您可以在页面上方的搜索框中通过资源ID和区域快速筛选出需要查看的资源。
5. 在列表中选择需要查看的资源，单击“共享数量”列的数字，界面将跳转至“共享管理”页面并自动筛选出包含此资源的共享实例。

图 2-3 共享给我的资源列表



2.5 查看资源所有者

操作场景

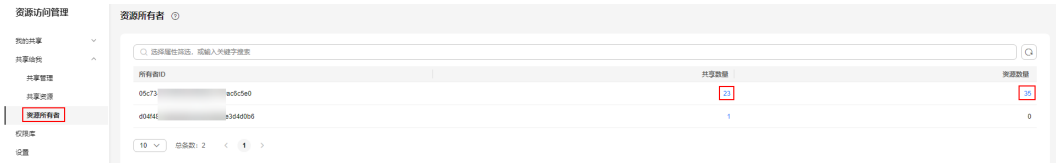
您可以在资源所有者列表中查看所有给您共享资源的资源所有者。该列表可帮助您确定各资源所有者共享给您的共享数量和资源数量。

操作步骤

1. 登录华为云控制台。
2. 单击页面左上角的 ☰ ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。

3. 单击左侧的“共享给我”，选择“资源所有者”。
4. 在资源所有者列表中可查看所有者ID、共享数量和资源数量的信息。
   您可以在页面上方的搜索框中通过所有者ID快速筛选出需要查看的资源所有者。
5. 在列表中选择需要查看的所有者，单击“共享数量”列的数字，界面将跳转至“共享管理”页面并自动筛选出此所有者共享给您的共享实例。
6. 在列表中选择需要查看的所有者，单击“资源数量”列的数字，界面将跳转至“共享资源”页面并自动筛选出此所有者共享给您的资源。

图 2-4 资源所有者列表



3 查看 RAM 权限库

操作场景

您可以在权限库列表中查看RAM针对不同资源类型预置的所有系统权限。

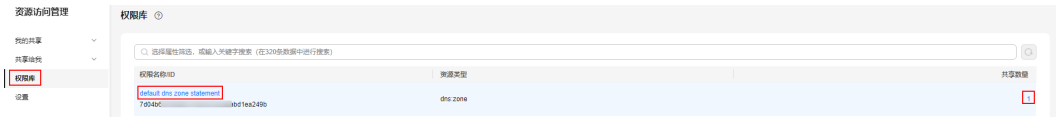
对于每种可共享的资源类型，至少有一个RAM预置的系统权限，该权限定义资源使用者对共享资源可执行的操作。某些资源类型定义了多个预置的系统权限，您在创建共享时可以依据最小权限原则和不同的使用诉求，选择不同的系统权限，提升了资源访问的安全性。

操作步骤

1. 登录华为云控制台。
2. 单击页面左上角的 ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。
3. 单击左侧的“权限库”，进入权限库列表。
4. 权限库列表中可查看权限名称/ID、资源类型和共享数量的信息。

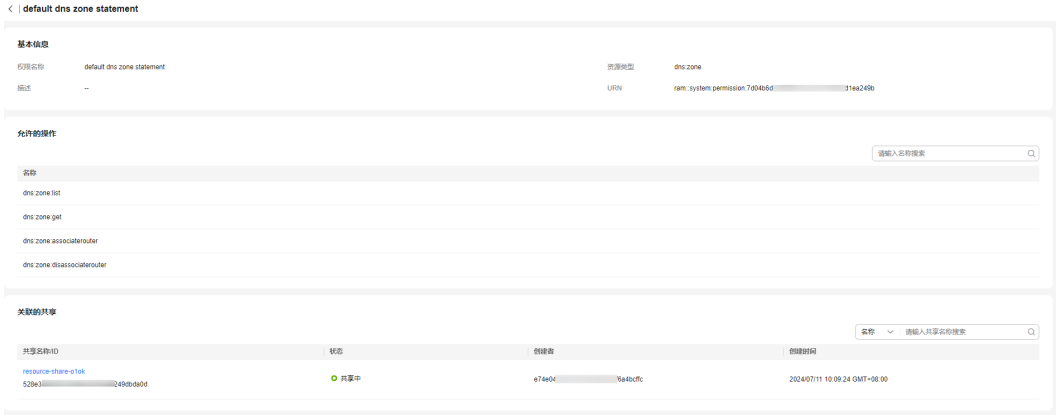
   您可以在页面上方的搜索框中通过权限名称、ID、资源类型和共享数量快速筛选出需要查看的权限。
5. 在列表中选择需要查看的权限，单击“共享数量”列的数字，界面将跳转至“共享管理”页面并自动筛选出使用此权限的所有共享实例。

   图 3-1 权限库列表



6. 在列表中选择需要查看的权限，单击权限名称，可查看此权限的详细信息，包括基本信息、允许的操作和关联的共享。

图 3-2 权限详情



4 启用或禁用与组织共享资源

操作场景

当您的账号由华为云Organizations管理时，您可以利用此优势更轻松地共享资源。如果您的账号在组织中，则您可以与单个账号共享，也可以与整个组织或OU中的所有账号共享，而不必枚举每个账号。

要在组织内共享资源，您还需先使用RAM控制台来启用与组织共享资源。当您在组织中共享资源时，您组织中的账号无需接受邀请即可访问和使用共享资源。

如果您不再需要与整个组织或OU共享资源，您可以禁用与组织共享资源，该功能禁用后，创建共享时指定的使用者将无法选择组织。

仅组织管理员才可启用或禁用与组织共享功能，其他角色无权操作。

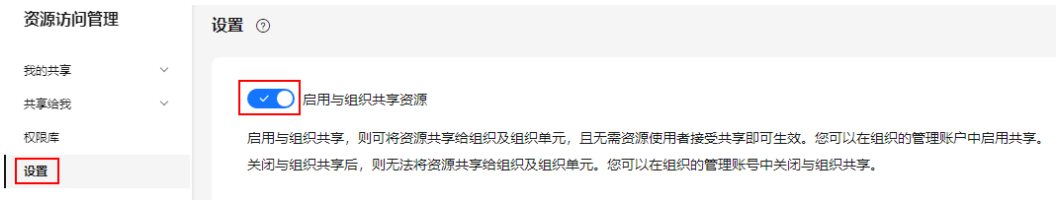
说明

- 在启用与组织共享资源期间，如果组织的成员账号主动退出组织或被管理员移出组织，该成员账号创建的资源共享实例中将解绑同组织的资源使用者；组织中共享给此成员账号的资源共享实例中将解绑此成员账号。
- 在启用与组织共享资源期间，如果组织管理员删除某个OU，则共享给此OU的资源共享实例中将解绑此OU。
- 在启用与组织共享资源期间，如果删除整个组织，则与组织共享的资源共享实例中将解绑组织内的全部账号。

启用与组织共享资源

1. 登录RAM管理控制台。
2. 单击左侧的“设置”，打开“启用与组织共享资源”开关。

图 4-1 启用与组织共享资源



说明

- RAM的“启用与组织共享资源”功能开关与组织的可信服务开关存在联动关系，即在组织服务中开启RAM为可信服务，RAM的组织共享功能将自动开启，反之亦然，如何启用组织可信服务请参见：**启用、禁用可信服务**。
- 如果您在组织中将RAM可信服务禁用，则在可信服务启用期间给组织、OU或成员账号共享的资源将自动解绑。

禁用与组织共享资源

1. 登录**RAM管理控制台**。
2. 单击左侧的“设置”，关闭“启用与组织共享资源”开关，在弹出的窗口中，单击“确定”按钮。

图 4-2 禁用与组织共享资源

5 标签管理

5.1 标签概述

标签简介

标签用于标识云资源，当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类。

RAM支持为资源共享实例添加标签，您可以根据标签快速搜索和筛选特定的资源共享实例，使您可以更轻松高效地识别和管理拥有的资源共享实例。

您可以在创建资源共享实例时添加标签，也可以在资源共享实例创建完成后，在共享的详情页添加、修改、查看、删除标签，您最多可以给每个资源共享实例添加20个标签。

标签的使用约束

- 每个云资源最多可以添加20个标签。
- 对于每个云资源，每个“标签键”都必须是唯一的，每个“标签键”只能有一个“标签值”。

5.2 添加标签

操作场景

RAM支持为资源共享实例添加标签。

您可以在创建资源共享实例时添加标签，也可以在资源共享实例创建完成后，在共享的详情页添加标签。

预定义标签的使用方法请参考**预定义标签的使用方法**。

在创建共享时添加标签

1. 登录**华为云控制台**。

2. 单击页面左上角的 ☰ ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。
3. 单击左侧的“我的共享”，选择“共享管理”。
4. 单击页面右上角的“创建共享”，进入指定共享资源页面，在基本信息区域的标签列，输入标签键和标签值，单击“添加”。

图 5-1 创建共享

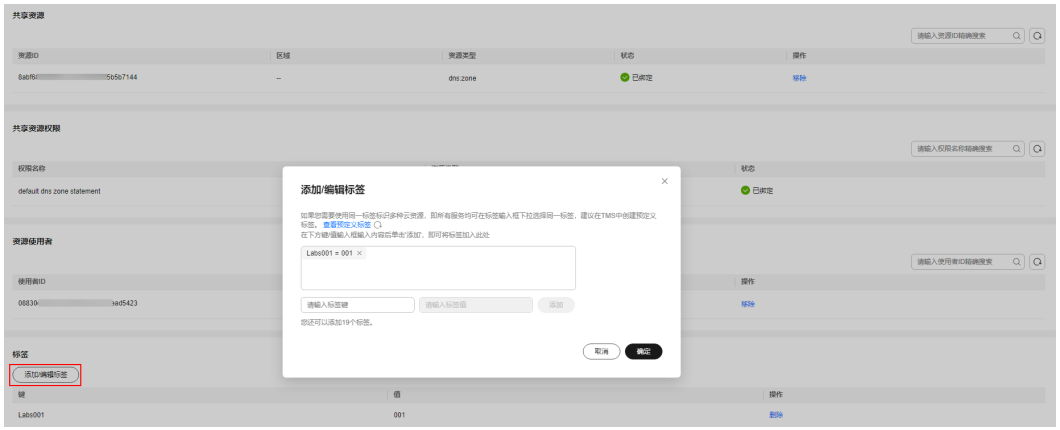
图 5-2 添加标签

5. 完成资源共享实例的其他配置，具体请参见**创建共享**。

在共享详情页添加标签

1. 登录**华为云控制台**。
2. 单击页面左上角的 ☰ ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。
3. 单击左侧的“我的共享”，选择“共享管理”。
4. 在共享管理列表中单击需要查看的共享名称，进入共享详情页。
5. 在标签列表中单击“添加/编辑标签”。
6. 在弹窗中，输入标签键和标签值，单击“添加”，然后单击“确定”，完成标签添加。

图 5-3 共享详情页添加标签



预定义标签的使用方法

通过预定义标签功能，您可以从业务角度提前规划并创建标签，也可以批量导入或导出标签。在使用服务资源时，可以快速将预定义标签与云资源进行关联。具体请参见**预定义标签**。

如果有多个资源共享实例或其他云资源需要添加同一标签，为了避免重复输入标签键和值，您可以在标签管理服务中预定义标签，然后在添加标签时直接选择键和值。具体步骤如下：

1. 登录**华为云控制台**。
2. 单击页面左上角的 ☰ ，选择“管理与监管 > 标签管理服务”，进入标签管理服务界面。
3. 在左侧导航中选择“预定义标签”，单击“创建标签”，输入标签键和值，单击“确定”。预定义标签创建成功。
4. 单击页面左上角的 ☰ ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。
5. 使用上述两种方式为资源共享实例添加标签时，直接在标签键和标签值输入框中下拉选择预定义标签即可。

5.3 使用标签检索资源

操作场景

为资源共享实例添加标签后，您可以根据标签快速筛选特定的资源共享实例。

操作步骤

1. 登录**华为云控制台**。
2. 单击页面左上角的 ☰ ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。
3. 单击左侧的“我的共享”，选择“共享管理”。

4. 在列表上方的搜索框中选择待查询的标签键和标签值。
   系统将自动根据标签键或标签值搜索目标资源共享实例。

图 5-4 使用标签检索共享

5.4 删除标签

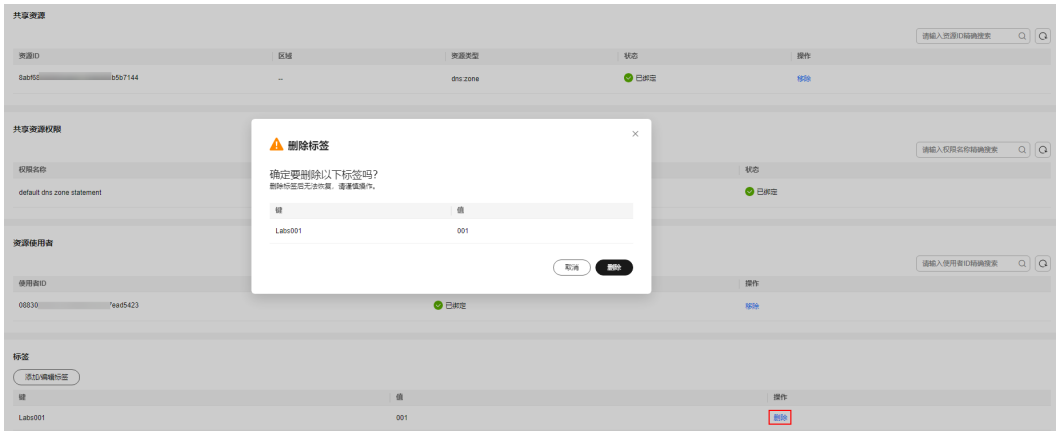
操作场景

本章节指导您删除资源共享实例的标签。

操作步骤

1. 登录华为云控制台。
2. 单击页面左上角的 ☰，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。
3. 单击左侧的“我的共享”，选择“共享管理”。
4. 在共享管理列表中单击需要查看的共享名称，进入共享详情页。
5. 在标签列表中，单击需删除标签操作列的“删除”。
6. 在弹出的确认框中，单击“删除”，标签删除完成。

图 5-5 删除标签



6 权限管理

6.1 创建用户并授权使用 RAM

如果您需要对您所拥有的RAM进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用RAM服务。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将RAM资源委托给更专业、高效的其他账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用RAM服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如**图6-1**所示。

前提条件

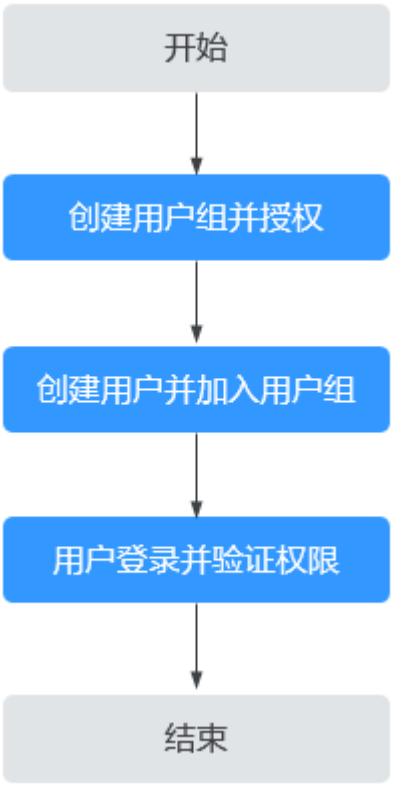
给用户组授权之前，请您了解用户组可以添加的RAM权限，并结合实际需求进行选择，RAM支持的系统权限如**表6-1**所示。若您需要对除RAM之外的其他服务授权，IAM支持服务的所有权限请参见**系统权限**。

表 6-1 RAM 系统权限

权限名称	描述
RAM FullAccess	资源访问管理服务所有权限。
RAM ReadOnlyAccess	资源访问管理服务只读权限。
RAM ResourceShareParticipantAccess	资源访问管理服务资源共享邀请的处理权限。

示例流程

图 6-1 给用户授权 RAM 权限流程



1. **创建用户组并授权**
   在IAM控制台创建用户组，授予RAM所有执行权限“RAM FullAccess”。
2. **创建用户并加入用户组**
   在IAM控制台创建用户，将其加入**步骤1**中创建的用户组。
3. **用户登录**并验证权限
   新创建的用户登录控制台，验证RAM服务的“RAM FullAccess”权限。

6.2 RAM 自定义策略

如果系统预置的RAM权限，不满足您的授权要求，可以通过IAM创建自定义策略。自定义策略中可以添加的授权项（Action）请参考**权限及授权项说明**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的RAM自定义策略样例。

RAM 自定义策略样例

- 示例1：授权用户可以接受共享邀请

```
{
   "Version": "1.0",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ram:resourceShareInvitations:accept",
         ],
         "Resource": "*"
      }
   ]
}
```

- 示例2：授权用户可查看权限列表和内容

```
{
   "Version": "1.0",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ram:permissions:list",
            "ram:permissions:get",
         ],
         "Resource": "*"
      }
   ]
}
```

7 使用 CTS 审计 RAM 操作事件

7.1 支持审计的关键操作

操作场景

平台提供了云审计服务。通过云审计服务，您可以记录与RAM相关的操作事件，便于后续的查询、审计和回溯。

前提条件

已开通云审计服务。如何开通云审计服务请参见**开通云审计服务**。

支持审计的关键操作列表

表 7-1 云审计服务支持的 RAM 操作列表

操作名称	资源类型	事件名称
创建资源共享实例	resourceShare	createResourceShare
检索资源共享实例	resourceShare	searchResourceShares
删除资源共享实例	resourceShare	deleteResourceShare
更新资源共享实例	resourceShare	updateResourceShare
为资源共享实例中包含的资源类型添加或替换RAM权限	resourceShare	associateResourceSharePermission
取消资源共享实例关联的RAM权限	resourceShare	disassociateResourceSharePermission
向资源共享实例增加角色和资源	resourceShare	associateResourceShare

操作名称	资源类型	事件名称
取消角色和资源与资源共享实例的关联	resourceShare	disassociateResourceShare
检索绑定的资源使用者和共享资源	resourceShare	searchResourceShareAssociations
接受资源共享实例的邀请	resourceShare	acceptResourceShareInvitation
拒绝资源共享实例的邀请	resourceShare	rejectResourceShareInvitation
检索共享邀请	resourceShare	searchResourceShareInvitation
检索是否启用与组织共享	resourceShare	showOrganizationShare
开启与组织的共享	resourceShare	enableShareWithOrganization
关闭与组织的共享	resourceShare	disableShareWithOrganization
检索共享资源权限列表	permission	listPermissions
检索资源共享权限内容	permission	showPermission
查询已使用的标签列表	resourceShare	listResourceShareTags
根据标签信息查询实例列表	resourceShare	listResourceSharesByTags
根据标签信息查询实例数量	resourceShareCount	searchResourceShareCountByTags
资源共享实例增加标签	resourceShare	batchCreateResourceShareTags
删除资源共享实例的标签	resourceShare	batchDeleteResourceShareTags
检索绑定的共享资源权限	resourceSharePermission	listResourceSharePermissions
检索共享的资源	sharedResource	searchSharedResources
检索去重的共享的资源	sharedResource	searchDistinctSharedResources
检索资源使用者	sharedPrincipal	searchSharedPrincipals
检索去重的共享的角色	sharedPrincipal	searchDistinctPrincipals
查询资源共享的配额	quota	listQuota
检索云服务资源类型	resourceType	listResourceTypes

操作名称	资源类型	事件名称
获取权限的所有版本	permissionVersion	listPermissionVersions

7.2 在 CTS 事件列表查看云审计事件

场景描述

云审计服务能够为您提供云服务资源的操作记录，记录的信息包括发起操作的用户身份、IP地址、具体的操作内容的信息，以及操作返回的响应信息。根据这些操作记录，您可以很方便地实现安全审计、问题跟踪、资源定位，帮助您更好地规划和利用已有资源、甄别违规或高危操作。

什么是事件

事件即云审计服务追踪并保存的云服务资源的操作日志，操作包括用户对云服务资源新增、修改、删除等操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。

什么是管理类追踪器和数据类追踪器

管理追踪器会自动识别并关联当前用户所使用的所有云服务，并将当前用户的所有操作记录在该追踪器中。管理追踪器记录的是管理类事件，即用户对云服务资源新建、修改、删除等操作事件。

数据追踪器会记录用户对OBS桶中的数据操作的详细信息。数据类追踪器记录的是数据类事件，即OBS服务上报的用户对OBS桶中数据的操作事件，例如上传数据、下载数据等。

约束与限制

- 管理类追踪器未开启组织功能之前，单账号跟踪的事件可以通过云审计控制台查询。管理类追踪器开启组织功能之后，多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。组织追踪器的详细介绍请参见**组织追踪器概述**。
- 用户通过云审计控制台只能查询最近7天的操作记录，过期自动删除，不支持人工删除。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务（OBS）或云日志服务（LTS），才可在OBS桶或LTS日志组里面查看历史事件信息。否则，您将无法追溯7天以前的操作记录。
- 用户对云服务资源做出创建、修改、删除等操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。
- CTS新版事件列表不显示数据类审计事件，您需要在旧版事件列表查看数据类审计事件。

前提条件

1. **注册华为云并实名认证。**

如果您已有一个华为账户，请跳到下一个任务。如果您还没有华为账户，请参考以下步骤创建。

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**如何注册华为云管理控制台的用户?** 。

注册成功后，系统会自动跳转至您的个人信息界面。

c. 参考**实名认证**完成个人或企业账号实名认证。

2. **为用户添加操作权限**。

如果您是以主账号登录华为云，请跳到下一个任务。

如果您是以IAM用户登录华为云，需要联系CTS管理员（主账号或admin用户组中的用户）对IAM用户授予CTS FullAccess权限。授权方法请参见**给IAM用户授权**。

查看审计事件

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录。

在 CTS 新版事件列表查看审计事件

步骤1 登录**CTS控制台**。

步骤2 单击左侧导航栏的“事件列表”，进入事件列表信息页面。

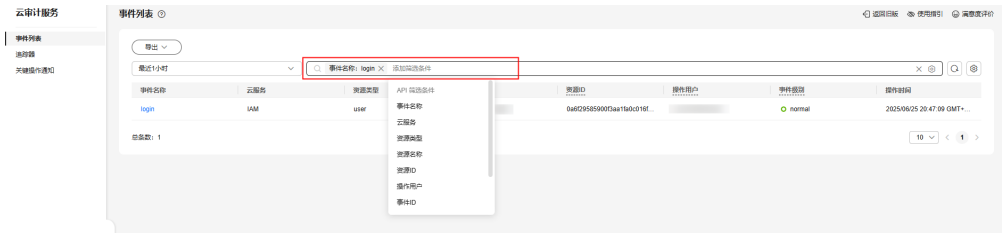
步骤3 在列表上方，可以通过筛选时间范围，查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

步骤4 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件。

表 7-2 事件筛选参数说明

参数名称	说明
事件名称	操作事件的名称。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 各个云服务支持审计的操作事件的名称请参见**支持审计的服务及详细操作列表**。 示例：updateAlarm
云服务	云服务的名称缩写。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 示例：IAM

参数名称	说明
资源名称	操作事件涉及的云资源名称。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。 示例：ecs-name
资源ID	操作事件涉及的云资源ID。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 当该资源类型无资源ID或资源创建失败时，该字段为空。 示例：*{虚拟机ID}*
事件ID	操作事件日志上报到CTS后，查看事件中的trace_id参数值。 输入的值需全字符匹配，不支持模糊匹配模式。 示例：01d18a1b-56ee-11f0-ac81-******1e229
资源类型	操作事件涉及的资源类型。 输入的值区分大小写，需全字符匹配，不支持模糊匹配模式。 各个云服务的资源类型请参见**支持审计的服务及详细操作列表**。 示例：user
操作用户	触发事件的操作用户。 下拉选项中选择一个或多个操作用户。 查看事件中的trace_type的值为“SystemAction”时，表示本次操作由服务内部触发，该条事件对应的操作用户可能为空。 IAM身份与操作用户对应关系，以及操作用户名称的格式说明，请参见**IAM身份与操作用户对应关系**。
事件级别	下拉选项包含“normal”、“warning”、“incident”，只可选择其中一项。 • normal代表操作成功。 • warning代表操作失败。 • incident代表比操作失败更严重的情况，如引起其他故障等。
企业项目ID	资源所在的企业项目ID。 查看企业项目ID的方式：在EPS服务控制台的“项目管理”页面，可以查看企业项目ID。 示例：b305ea24-c930-4922-b4b9-******1eb2
访问密钥ID	访问密钥ID，包含临时访问凭证和永久访问密钥。 查看访问密钥ID的方式：在控制台右上方，用户名下拉选项中，选择“我的凭证 > 访问密钥”，可以查看访问密钥ID。 示例：HSTAB47V9V*******TLN9



步骤5 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。

- 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
- 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
- 单击按钮，可以获取到事件操作记录的最新信息。
- 单击按钮，可以自定义事件列表的展示信息。启用表格内容折行开关，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。

步骤6 （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

----结束

在 CTS 旧版事件列表查看审计事件

步骤1 登录CTS控制台。

步骤2 单击左侧导航栏的“事件列表”，进入事件列表信息页面。

步骤3 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。

步骤4 在页面右上方，可以通过筛选时间范围，查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

步骤5 事件列表支持通过筛选来查询对应的操作事件。

表 7-3 事件筛选参数说明

参数名称	说明
事件类型	事件类型分为“管理事件”和“数据事件”。 • 管理类事件，即用户对云服务资源新建、修改、删除等操作事件。 • 数据类事件，即OBS服务上报的OBS桶中的数据的操作事件，例如上传数据、下载数据等。
云服务	在下拉选项中，选择触发操作事件的云服务名称。
资源类型	在下拉选项中，选择操作事件涉及的资源类型。 各个云服务的资源类型请参见支持审计的服务及详细操作列表。

参数名称	说明
操作用户	触发事件的操作用户。 下拉选项中选择一个或多个操作用户。 查看事件中的trace_type的值为“SystemAction”时，表示本次操作由服务内部触发，该条事件对应的操作用户可能为空。 IAM身份与操作用户对应关系，以及操作用户名称的格式说明，请参见**IAM身份与操作用户对应关系**。
事件级别	可选项包含“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。 • Normal代表操作成功。 • Warning代表操作失败。 • Incident代表比操作失败更严重的情况，如引起其他故障等。

步骤6 选择完查询条件后，单击“查询”。

步骤7 在事件列表页面，您还可以导出操作记录文件和刷新列表。

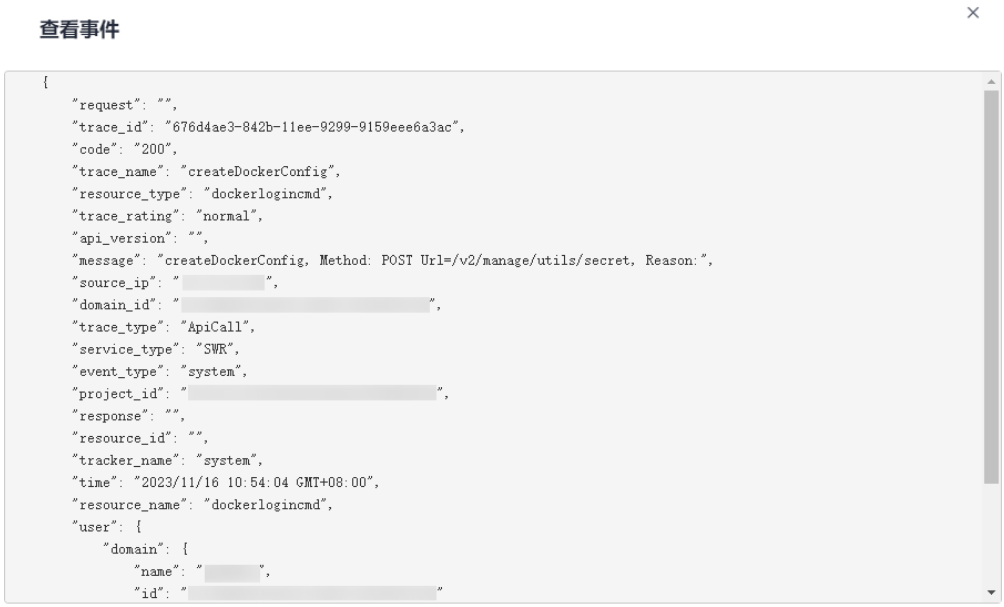
- 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
- 单击按钮，可以获取到事件操作记录的最新信息。

步骤8 在事件的“是否篡改”列中，您可以查看该事件是否被篡改：

- 上报的审计日志没有被篡改，显示“否”；
- 上报的审计日志被篡改，显示“是”。

步骤9 在需要查看的事件左侧，单击 展开该记录的详细信息。

步骤10 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。



步骤11 （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

----结束

相关文档

- 关于事件结构的关键字段详解，请参见**事件结构**和**事件样例**。
- 您可以通过以下示例，来学习如何查询具体的事件：
  - 使用云审计服务，审计最近两周内云硬盘服务的创建和删除操作。具体操作，请参见**安全审计**。
  - 使用云审计服务，定位现网某个弹性云服务器在某日上午发生的故障，以及定位现网创建弹性云服务器操作失败的问题。具体操作，请参见**问题定位**。
  - 使用云审计服务，查看某个弹性云服务器的所有的操作记录。具体操作，请参见**资源跟踪**。

8 调整配额

什么是配额?

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少个资源共享实例等。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

怎样查看我的配额?

1. 登录管理控制台。
2. 在页面右上角，选择“资源 > 我的配额”。
   系统进入“服务配额”页面。

   图 8-1 我的配额

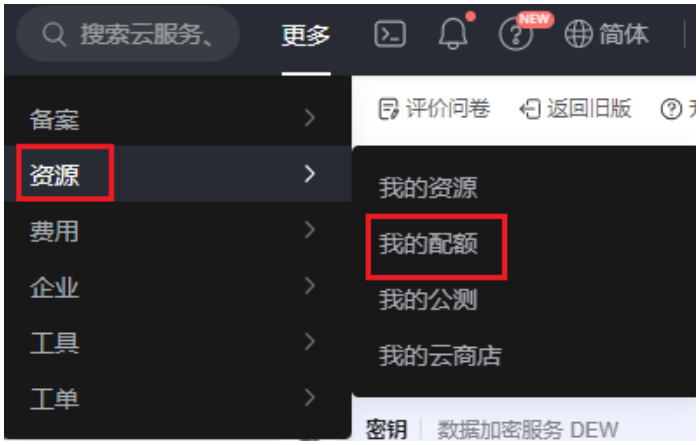
   

3. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
   如果当前配额不能满足业务要求，请参考后续操作，申请扩大配额。

如何申请扩大配额?

1. 登录管理控制台。
2. 在页面右上角，选择“资源 > 我的配额”。
   系统进入“服务配额”页面。

图 8-2 我的配额



3. 单击“申请扩大配额”。
4. 在“新建工单”页面，根据您的需求，填写相关参数。
   其中，“问题描述”项请填写需要调整的内容和申请原因。
5. 填写完毕后，勾选协议并单击“提交”。

9 附录

9.1 支持共享的资源

表 9-1 支持共享的云服务和资源类型

云服务	资源类型	是否支持主动退出共享	应用场景
虚拟私有云 VPC	vpc:subnet（子网）	是	共享VPC功能支持多个账号在一个集中管理、共享的VPC内创建云资源，比如ECS、ELB、RDS等。VPC的所有者可以将VPC内的子网共享给一个或者多个账号使用。通过共享VPC功能，可以简化网络配置，帮助您统一配置和运维多个账号下的资源，有助于提升资源的管控效率，降低运维成本。 更多信息请参见**共享VPC**。
云解析服务 DNS	dns:zone（内网域名）	是	基于资源访问管理（Resource Access Manager，简称RAM）服务，云解析服务可以实现跨账号共享内网域名，资源所有者将内网域名同时共享给多个其他账号使用，资源使用者接受共享邀请后就可以访问和使用共享的内网域名。 更多信息请参见**共享内网域名**。
	dns:resolverRule（解析器规则）	是	基于资源访问管理（Resource Access Manager，简称RAM）服务，云解析服务可以实现跨账号共享转发规则，资源所有者将转发规则同时共享给多个其他账号使用，资源使用者接受共享邀请后就可以访问和使用共享的转发规则。 更多信息请参见**共享转发规则**。

云服务	资源类型	是否支持主动退出共享	应用场景
SSL证书管理 SCM	scm:cert（证书）	是	云证书与管理服务提供共享功能，用户可以将SSL证书同时共享给同一组织单元内的所有成员账号，这些账号可以将共享证书部署到ELB、WAF和CDN等服务，以启用HTTPS协议。 更多信息请参见**共享证书**。
私有证书管理 PCA	pca:ca（私有CA）	是	云证书与管理服务私有证书管理提供共享功能，用户可以将私有CA同时共享给同一组织单元内的所有成员账号，这些账号可以使用共享CA来签发证书。 更多信息请参见**共享私有CA**。
企业路由器 ER	er:instances（实例）	是	基于资源访问管理（Resource Access Manager，简称RAM）服务，可以实现跨账号共享企业路由器，您可以将账号A所属的企业路由器同时共享给多个其他账号，比如账号B、账号C以及账号D等。通过共享功能，可以在同一个企业路由器中接入不同账号下的虚拟私有云，构建云上同区域组网。 更多信息请参见**共享概述**。
函数工作流 Function Graph	functiongraph:function（函数）	是	基于资源访问管理（Resource Access Manager，简称RAM）服务，函数工作流服务可以实现跨账号共享函数，资源所有者将函数同时共享给多个其他账号使用，资源使用者接受共享邀请后就可以访问和使用共享的函数。 更多信息请参见**共享函数**。
云原生应用网络 ANC	anc:service（服务）	是	基于资源访问管理（Resource Access Manager，简称RAM），可以实现跨账号共享ANC的服务，您可以将账号A所属的ANC的服务同时共享给多个其他账号，比如账号B、账号C等。通过共享功能，共享ANC的服务可以接收不同账号下VPC内客户端的访问请求，有助于管理多账号下的资源，提升资源的管控效率。
	anc:anc（云原生应用网络）	是	基于资源访问管理（Resource Access Manager，简称RAM），可以实现跨账号共享云原生应用网络，您可以将账号A所属的云原生应用网络同时共享给多个其他账号，比如账号B、账号C等。通过共享功能，VPC内客户端可以访问不同账号下ANC的服务，实现统一管理多账号下的资源。

云服务	资源类型	是否支持主动退出共享	应用场景
NAT网关 NAT	nat:transitSubnet	是	基于资源访问管理（Resource Access Manager，简称RAM）服务，可以实现跨账号共享中转子网，资源所有者将中转子网同时共享给多个其他账号使用，资源使用者接受共享邀请后就可以在中转子网下创建中转IP用于打通跨租户VPC网络。
密码安全中心 DEW	kms:KeyId（密钥）	是	要共享您拥有的KMS资源给其他账号使用时，请创建共享。创建共享的流程分为指定共享资源、权限配置、指定使用者以及配置确认。 共享KMS可以用于DEW服务的凭据实例加密、密钥对加密等，也可以用于创建RDS、DDS、OBS实例加密。 更多信息请参见**共享概述**。