对象存储服务

权限配置指南

文档版本 01

发布日期 2024-08-15

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 OBS 不同权限控制方式的区别

默认情况下，OBS的资源（桶和对象）都是私有的，只有资源拥有者可以访问OBS资源，其他用户在未经授权的情况下均无OBS访问权限。OBS的权限控制是指通过编写访问策略向其他账号或者IAM用户授予资源的控制权限。例如，你拥有一个桶，你可以授权一个其他的IAM用户上传对象到你的桶中；你也可以将桶开放给非公有云用户访问，即桶作为一个公共资源，能被互联网上任何人访问。OBS提供多种方式将OBS资源权限授予给他人，资源拥有者可以根据业务需求制定不同的权限控制方案，从而确保数据安全。

OBS 权限控制模型

OBS提供多种权限控制方式，包括IAM权限、桶策略、对象ACL、桶ACL。各个方式说明及应用场景如表1-1所示。

图 1-1 OBS 权限控制方式

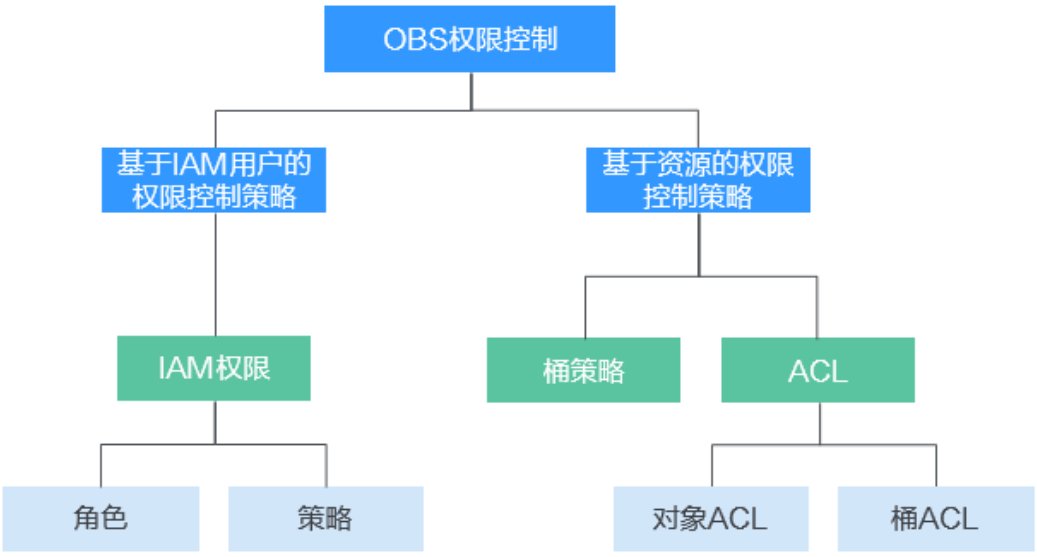


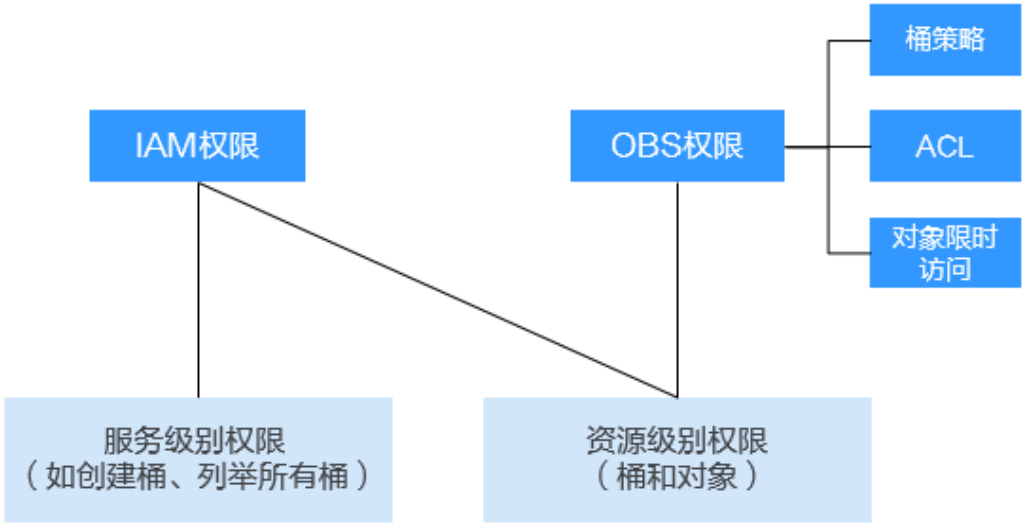
表 1-1 OBS 权限控制方式说明和应用场景

方式	说明	应用场景
IAM权限	IAM权限是作用于云资源的，IAM权限定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。管理员创建IAM用户后，需要将用户加入到一个用户组中，IAM可以对这个组授予OBS所需的权限，组内用户自动继承用户组的所有权限。	• 使用策略控制账号下整个云资源的权限时，使用IAM权限授权。 • 使用策略控制账号下OBS所有的桶和对象的权限时，使用IAM权限授权。 • 使用策略控制账号下OBS指定资源的权限时，使用IAM权限授权。
桶策略	桶策略是作用于所配置的OBS桶及桶内对象的。桶拥有者通过桶策略可为IAM用户或其他账号授权桶及桶内对象精确的操作权限，桶ACL和对象ACL是对桶策略的补充（更多场景下是替代）。	• 允许其他华为云账号访问OBS资源，可以使用桶策略的方式授权对应权限。 • 当不同的桶对于不同的IAM用户有不同的访问控制需求时，需使用桶策略分别授权IAM用户不同的权限。
对象ACL	基于账号或用户组的对象级访问控制，对象的拥有者可以通过对象ACL向指定账号或用户组授予对象基本的读、写权限。 **说明** • 默认情况下，创建对象时会同步创建ACL，授权对象拥有者拥有对象的完全控制权限。 • 对象的拥有者是上传对象的账号，而不是对象所属的桶的拥有者。例如，如果账号B被授予访问账号A的桶的权限，然后账号B上传一个文件到桶中，则账号B是对象的拥有者，而不是账号A。默认情况下，账号A没有该对象的访问权限，也无法读取和修改该对象的ACL。	• 需要对象级的访问权限控制时，桶策略可以授予对象或对象集访问权限，当授予一个对象集权限后，想对对象集中某一个对象再进行单独授权，通过配置桶策略的方法显然不太实际。此时建议使用对象ACL，使得单个对象的权限控制更加方便。 • 使用对象链接访问对象时。一般使用对象ACL，将某一个对象通过对象链接开放给匿名用户进行读取操作。
桶ACL	基于账号或用户组的桶级访问控制，桶的拥有者可以通过桶ACL向指定账号或用户组授予桶基本的读、写权限。 **说明** • 默认情况下，创建桶时会同步创建ACL，授权拥有者对桶的完全控制权限。 • 桶ACL的权限控制粒度不如IAM权限和桶策略，一般情况下，建议使用IAM权限和桶策略进行权限访问控制。	• 授予指定账号桶读取权限和桶写入权限，用以共享桶数据或挂载外部桶。比如，账号A授予账号B桶读取权限及桶写入权限后，账号B就可以通过OBS Browser+挂载外部桶、API&SDK等方式访问到该桶。 • 授予日志投递用户组桶写入权限，用以存储桶访问请求日志。

OBS 权限与 IAM 权限的关系

OBS权限控制方式中，对象限时访问、对象ACL、桶ACL和桶策略属于OBS权限。某些服务级的权限（例如创建桶、列举所有桶）无法通过OBS权限进行配置，只能在IAM权限中配置，OBS权限只能作用于资源级（桶和对象）。如果要同时授予OBS服务级权限和资源级权限，必须使用IAM权限，或者IAM权限与OBS权限结合使用。

图 1-2 OBS 权限与 IAM 权限的关系



OBS 权限控制要素

OBS的权限控制模型中，以下几个要素共同决定了授权的结果：

- **Principal（被授权用户）**
- **Effect（效力）**
- **Resource（资源）**
- **Action（动作）**
- **Condition（条件）**

各个要素的详细介绍，请参见**桶策略参数说明**。

不同权限控制方式中各个要素的支持情况如**表1-2**所示。

表 1-2 不同权限控制方式中的 OBS 权限控制要素

方式	被授权用户	支持的效力	被授权资源	被授权动作	是否支持配置条件
IAM权限	IAM用户	• 允许 • 拒绝	OBS所有资源或指定资源	OBS所有操作权限	支持

方式	被授权用户	支持的效力	被授权资源	被授权动作	是否支持配置条件
桶策略	• 账号 • IAM用户 • 所有用户	• 允许 • 拒绝	指定桶及桶内资源	OBS所有操作权限	支持
对象ACL	• 账号 • 匿名用户	允许	对象	• 获取对象内容及元数据 • 获取指定版本对象内容及元数据 • 获取对象ACL相关信息 • 获取指定版本对象ACL相关信息 • 设置对象ACL • 设置指定版本对象ACL	不支持
桶ACL	• 账号 • 匿名用户 • 日志投递用户组	允许	桶	• 判断桶是否存在 • 列举桶内对象，获取桶元数据 • 列举桶内多版本对象 • 列举多段上传任务 • PUT上传，POST上传，上传段，初始化上传段任务，合并段 • 删除对象 • 删除特定版本的对象 • 获取桶ACL的相关信息 • 设置桶ACL • 获取对象的内容 • 获取对象的元数据	不支持

IAM 权限、桶策略和 ACL 如何选择?

基于三者的优劣势对比，通常情况下推荐您优先使用IAM权限和桶策略：

- 以下情况使用IAM权限：
  - 要对同账号下的大量IAM用户授予相同权限时
  - 要给所有OBS资源或者多个桶配置相同权限时
  - 要配置OBS服务级权限时，如创建桶、列举桶
  - 临时授权访问OBS时，限制临时访问密钥的权限

- 以下情况使用桶策略：
  - 要进行跨账号授权或对所有用户授权时
  - 要对同账号下的不同IAM用户授予不同权限时
- 给同账号IAM用户授权时仍然不知道如何选择？

  可考虑您更关心哪个问题：
  - 关心用户能做什么——推荐IAM权限

    可通过查找IAM用户，并检查其所属用户组的权限来了解用户能做什么
  - 关心谁能访问这个OBS桶——推荐桶策略

    可通过查找桶，并检查桶策略来了解谁能访问

说明

无论选择哪种方式，建议尽可能保持统一。随着IAM权限和桶策略数量的增加，权限维护难度将越来越大。

何时选择ACL？

- 作为IAM权限和桶策略的补充：

  IAM权限和桶策略已授予某个对象集访问权限，还想对其中某一个对象再进行单独授权
- 需要将某个对象开放给所有互联网匿名用户访问，对象ACL操作更为便捷

  上传对象时可通过携带ACL头域指定对象的读写权限

桶策略和 ACL 的关系

桶ACL用于授予桶基本的读写权限，桶策略高级设置中支持更多在桶上可以执行的动作。桶ACL是对桶策略的补充，更多时候桶策略可以替代桶ACL管理桶的访问权限。桶ACL访问权限和桶策略动作的映射关系请参见**桶策略和ACL的关系**。

OBS 权限控制原则

- 最小权限原则

  仅授予IAM用户或账号执行任务所需的最小权限。例如，一个IAM用户仅需执行向指定目录上传、下载对象任务，则无需为其配置整个桶的读写权限。
- 责任分离原则

  同一账号下建议使用不同IAM用户分别管理OBS资源和权限。例如，IAM用户A负责权限分配，而其他IAM用户负责管理OBS资源。
- 条件限制原则

  尽可能的为权限定义更精细化的条件，约束权限生效的场景，强化桶内资源的安全性。例如，约束OBS只接受来自某特定IP地址发起的访问请求。

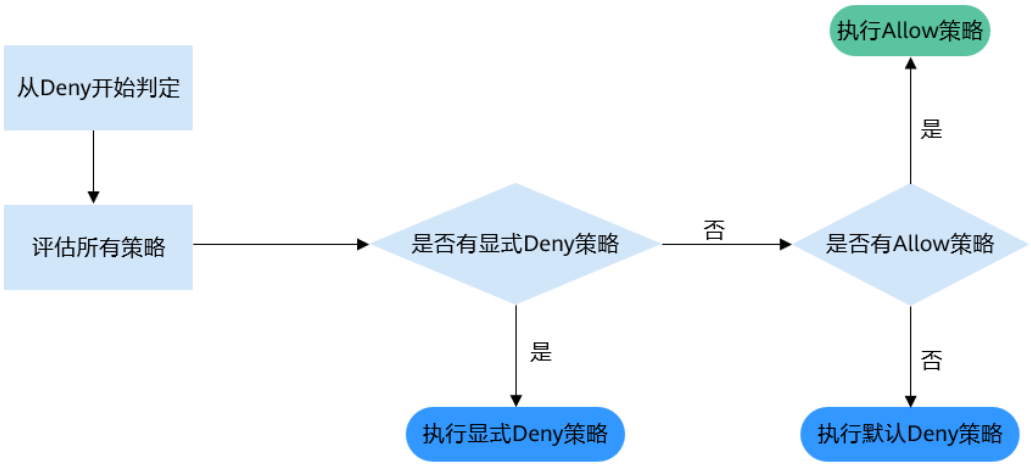
访问控制机制冲突时，如何工作？

OBS权限控制要素中，Effect（效力）包含两种：Allow（允许）和Deny（拒绝），分别表示允许或拒绝执行某操作的权限。

基于最小权限原则，权限控制策略的结果默认为Deny， 显式的Deny始终优先于Allow。例如，IAM权限授权了用户访问对象的权限，但是桶策略拒绝了该用户访问对象的权限，且没有ACL时，该用户不能访问对象。

没有策略授予Allow权限时，默认情况即为Deny权限。当有策略授权Allow权限，且没有其他策略Deny该权限时，Allow的权限才能生效。例如，某个桶已经存在多条Allow权限的桶策略，再新增Allow权限的桶策略，会在原权限的基础上进行叠加，增大用户的权限；如果新增Deny权限的桶策略，则会根据Deny优先原则调整用户的权限，即使Deny策略中定义的动作在其他桶策略中Allow。

图 1-3 访问策略授权过程



同账号场景下，为当前华为云账号下的IAM用户授予OBS桶和桶内资源的访问权限，桶策略、IAM权限和ACL的Allow和Deny作用结果如图1-4所示。ACL是基于账号级别的读写权限控制，IAM用户在访问所属账号的桶和桶内资源时，不受ACL控制。

图 1-4 同账号场景下桶策略、IAM 权限的 Allow 和 Deny 作用结果

桶策略	IAM策略		
	Deny	Allow	Default Deny
Deny	Deny	Deny	Deny
Allow	Deny	Allow	Allow
Default Deny	Deny	Allow	Deny

表示用户设置的权限
表示所有设置最终表现的结果为Deny
表示所有设置最终表现的结果为Allow

跨账号场景下，为其他华为云账号及账号下的IAM用户授予OBS桶和桶内资源的访问权限，桶策略、IAM权限和ACL的Allow和Deny作用结果如图1-5所示。

图 1-5 跨账号场景下桶策略、IAM 权限和 ACL 的 Allow 和 Deny 作用结果

桶策略	IAM策略			ACL
	Deny	Allow	Default Deny	
Deny	Deny	Deny	Deny	Allow
				Default Deny
Allow	Deny	Allow	Deny	Allow
				Default Deny
Default Deny	Deny	Allow	Deny	Allow
		Deny	Deny	Default Deny

表示用户设置的权限

表示所有设置最终表现的结果为Deny

表示所有设置最终表现的结果为Allow

说明

- 当桶策略和IAM策略均为Default Deny，ACL设置为Allow时，由于ACL权限范围限制，最终的作用结果其实为Deny。ACL可以理解为对桶策略的一种补充。

相关概念

- 账号：用户注册华为云后自动创建，该账号对其所拥有的资源和IAM用户具有完全的访问控制权限。
- IAM用户：由管理员在IAM中创建的用户，是云服务的使用者，对应员工、系统或应用程序，具有身份凭证（密码和访问密钥），可以登录管理控制台或者访问API。
- 匿名用户：未注册华为云的普通访客。
- 日志投递用户组：用于投递OBS桶及对象的访问日志。由于OBS本身不能在用户的桶中创建或上传任何文件，因此在需要为桶记录访问日志时，只能由用户授予日志投递用户组一定权限后，OBS才能将访问日志写入指定的日志存储桶中。该用户组仅用于OBS内部的日志记录。

2 权限控制方式介绍

2.1 IAM 权限

IAM 权限简介

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略和角色，才能使得用户组中的用户获得策略定义的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

对于OBS，IAM权限作用于OBS所有的桶和对象。如果要授予IAM用户操作OBS资源的权限，则需要向IAM用户所属的用户组授予一个或多个OBS权限。

OBS部署时不区分物理区域，为全局级服务。授权时，在全局级服务中设置权限，访问OBS时，不需要切换区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对OBS服务，管理员能够控制IAM用户仅能对某一个桶资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，OBS支持的API授权项请参见**权限和授权项说明**。

说明

由于缓存的存在，对用户、用户组以及企业项目授予OBS相关的角色和策略后，大概需要等待10~15分钟权限才能生效。

IAM中为各云服务预置了系统权限，方便您快速完成基础权限配置，**表2-1**为OBS的所有系统权限。

如果系统预置的OBS权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考**桶相关授权项**和**对象相关授权项**。

表 2-1 OBS 系统权限

系统角色/策略名称	描述	类别	依赖关系
Tenant Administrator	拥有该权限的用户拥有除IAM外，其他所有服务的所有执行权限。	系统角色	无
Tenant Guest	拥有该权限的用户拥有除IAM外，其他所有服务的只读权限。	系统角色	无
OBS Administrator	拥有该权限的用户为OBS管理员，可以对账号下的所有OBS资源执行任意操作。	系统角色	无
OBS Buckets Viewer	拥有该权限的用户可以执行列举桶、获取桶基本信息、获取桶元数据的操作。	系统角色	无
OBS ReadOnlyAccess	拥有该权限的用户可以执行列举桶、获取桶基本信息、获取桶元数据、列举对象（不包含多版本）的操作。 **说明** 拥有该权限的用户如果在控制台上列举对象失败，可能是因为桶中存在多版本对象。此时需要额外授予该用户列举多版本对象的权限（obs:bucket:ListBucketVersions），才能在控制台正常看到对象列表。	系统策略	无
OBS OperateAccess	拥有该权限的用户可以执行OBS ReadOnlyAccess的所有操作，在此基础上还可以执行上传对象、下载对象、删除对象、获取对象ACL等对象基本操作。 **说明** 拥有该权限的用户如果在控制台上列举对象失败，可能是因为桶中存在多版本对象。此时需要额外授予该用户列举多版本对象的权限（obs:bucket:ListBucketVersions），才能在控制台正常看到对象列表。	系统策略	无

下表列出了OBS常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 2-2 OBS 操作与资源权限关系

操作名称	Tenant Administrator	Tenant Guest	OBS Administrator	OBS Buckets Viewer	OBS ReadOnly Access	OBS Operate Access
列举桶	可以	可以	可以	可以	可以	可以
创建桶	可以	不可以	可以	不可以	不可以	不可以
删除桶	可以	不可以	可以	不可以	不可以	不可以
获取桶基本信息	可以	可以	可以	可以	可以	可以

操作名称	Tenant Administrator	Tenant Guest	OBS Administrator	OBS Buckets Viewer	OBS ReadOnly Access	OBS Operate Access
管理桶访问权限	可以	不可以	可以	不可以	不可以	不可以
管理桶策略	可以	不可以	可以	不可以	不可以	不可以
修改桶存储类别	可以	不可以	可以	不可以	不可以	不可以
列举对象	可以	可以	可以	不可以	可以	可以
列举多版本对象	可以	可以	可以	不可以	不可以	不可以
上传文件	可以	不可以	可以	不可以	不可以	可以
新建文件夹	可以	不可以	可以	不可以	不可以	可以
删除文件	可以	不可以	可以	不可以	不可以	可以
删除文件夹	可以	不可以	可以	不可以	不可以	可以
下载文件	可以	可以	可以	不可以	不可以	可以
删除多版本文件	可以	不可以	可以	不可以	不可以	可以
下载多版本文件	可以	可以	可以	不可以	不可以	可以
修改对象存储类别	可以	不可以	可以	不可以	不可以	不可以
恢复文件	可以	不可以	可以	不可以	不可以	不可以
取消删除文件	可以	不可以	可以	不可以	不可以	可以
删除碎片	可以	不可以	可以	不可以	不可以	可以
管理对象访问权限	可以	不可以	可以	不可以	不可以	不可以
设置对象元数据	可以	不可以	可以	不可以	不可以	不可以
获取对象元数据	可以	可以	可以	不可以	不可以	可以
管理多版本控制	可以	不可以	可以	不可以	不可以	不可以

操作名称	Tenant Administrator	Tenant Guest	OBS Administrator	OBS Buckets Viewer	OBS ReadOnly Access	OBS Operate Access
管理日志记录	可以	不可以	可以	不可以	不可以	不可以
管理标签	可以	不可以	可以	不可以	不可以	不可以
管理生命周期规则	可以	不可以	可以	不可以	不可以	不可以
管理静态网站托管	可以	不可以	可以	不可以	不可以	不可以
管理CORS规则	可以	不可以	可以	不可以	不可以	不可以
管理防盗链	可以	不可以	可以	不可以	不可以	不可以
域名管理	可以	不可以	可以	不可以	不可以	不可以
管理跨区域复制	可以	不可以	可以	不可以	不可以	不可以
管理图片处理	可以	不可以	可以	不可以	不可以	不可以
追加写对象	可以	不可以	可以	不可以	不可以	可以
设置对象ACL	可以	不可以	可以	不可以	不可以	不可以
设置指定版本对象ACL	可以	不可以	可以	不可以	不可以	不可以
获取对象ACL	可以	可以	可以	不可以	不可以	可以
获取指定版本对象ACL	可以	可以	可以	不可以	不可以	可以
多段上传	可以	不可以	可以	不可以	不可以	可以
列举已上传段	可以	可以	可以	不可以	不可以	可以
取消多段上传任务	可以	不可以	可以	不可以	不可以	可以

IAM 权限应用场景

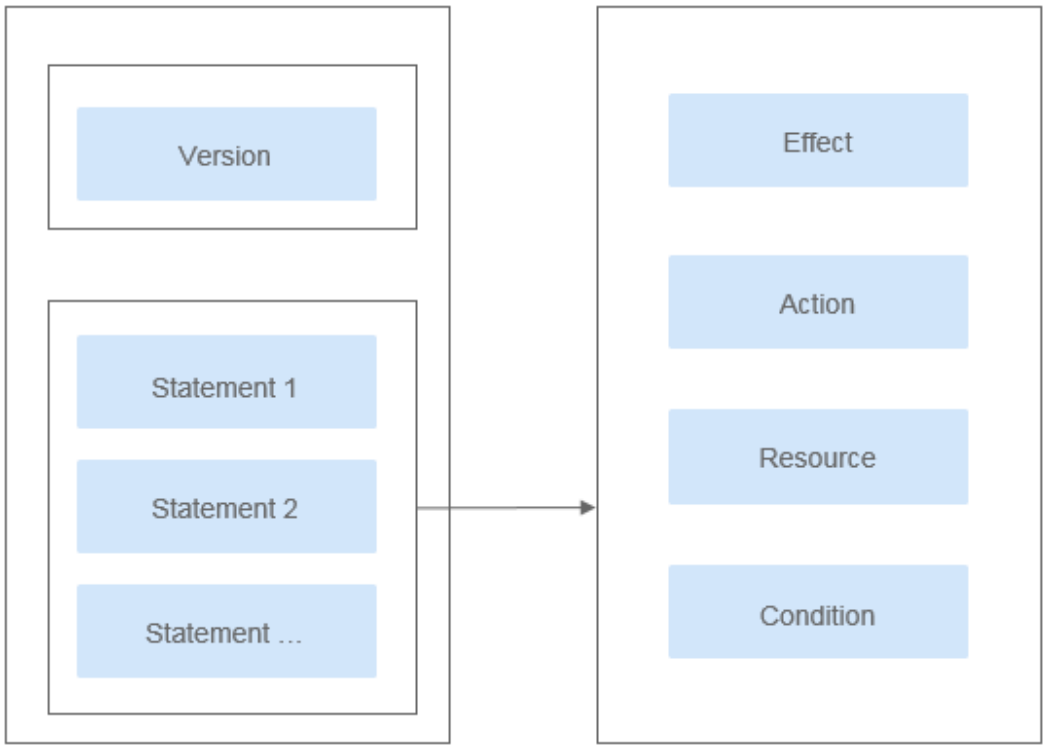
IAM权限主要面向对同账号下IAM用户授权的场景：

- 使用策略控制账号下整个云资源的权限时，使用IAM权限授权。
- 使用策略控制账号下OBS所有的桶和对象的权限时，使用IAM权限授权。
- 使用策略控制账号下OBS指定资源的权限时，使用IAM权限授权。

策略结构&语法

策略结构包括：Version（策略版本号）和Statement（策略权限语句），其中Statement可以有多个，表示不同的授权项。

图 2-1 策略结构



策略语法，示例：

```
{
   "Version": "1.1",
   "Statement": [
            {
         "Effect": "Allow",
         "Action": [
            "obs:bucket:HeadBucket",
            "obs:bucket:ListBucket",
            "obs:bucket:GetBucketLocation"
         ],
         "Resource": [
            "obs:*:*:bucket:*"
         ],
         "Condition": {
            "StringEndWithIfExsits": {
               "g:UserName": ["specialCharacter"]
            },
            "Bool": {
               "g:MFAPresent": ["true"]
            }
         }
      }
```

```
  ]
}
```

表 2-3 策略语法参数

参数	说明
Version	标识策略的版本号： ● 1.0：RBAC策略。RBAC策略是将服务作为一个整体进行授权，授权后，用户可以拥有这个服务的所有权限。 ● 1.1：细粒度策略。相比RBAC策略，细粒度策略基于服务的API接口进行权限拆分，授权更加精细，可以精确到具体操作和具体资源。例如：您可以限制子用户只能访问某一个OBS桶中某一个目录下的对象。

参数	说明
Statement	策略授权语句，描述策略的详细信息，包含Effect（效果）、Action（动作）、Resource（资源）和Condition（条件）。其中Resource和Condition为可选。 • **Effect（效果）** 作用包含两种：Allow（允许）和Deny（拒绝），系统预置策略仅包含允许的授权语句，自定义策略中可以同时包含允许和拒绝的授权语句，当策略中既有允许又有拒绝的授权语句时，遵循Deny优先的原则。 • **Action（动作）** 对资源的具体操作权限，格式为：**服务名:资源类型:操作**，支持单个或多个操作权限，支持通配符号*，通配符号表示所有。OBS只有两种资源类型：bucket和object。 详细的Action描述请参见**桶相关授权项**和**对象相关授权项**。 • **Resource（资源）** 策略所作用的资源，格式为：**服务名:region:domainId:资源类型:资源路径**，支持通配符号*，通配符号表示所有。在JSON视图中，不带Resource表示对所有资源生效。 Resource支持以下字符：-_0-9a-zA-Z*./\，如果Resource中包含不支持的字符，请采用通配符号*。 OBS是全局级服务，**region**填“*”；domainId表示资源拥有者的账号ID，建议填写“*”简单地表示所填资源的账号ID。 示例： – "obs:*:*:bucket:*": 表示所有的OBS桶。 – "obs:*:*:object:my-bucket/my-object/*": 表示桶my-bucket中“my-object”目录下的所有对象。 • **Condition（条件）** 您可以在创建自定义策略时，通过添加Condition元素来控制策略何时生效。Condition包括条件键和运算符，条件键表示策略语句的Condition元素，分为全局级条件键和服务级条件键。**全局级条件键**（前缀为g:）适用于所有操作，服务级条件键（前缀为服务缩写，如obs:）仅适用于对应服务的操作。运算符与条件键一起使用，构成完整的条件判断语句。 OBS通过IAM预置了一组条件键，例如，您可以先使用obs:SourceIp条件键检查请求者的IP地址，然后再允许执行操作。 OBS支持的条件键和运算符与桶策略的Condition一致，在IAM配置时需要在前面加上“obs:”。详细的Condition介绍请参见**桶策略参数说明**。 Condition的条件值仅支持以下字符：-,./ a-zA-Z0-9_@#$%&，如果条件值中包含不支持的字符，请考虑使用模糊匹配的条件运算符，如：StringMatch等。 示例： – "StringEndWithIfExists":{"g:UserName":["specialCharacter"]}：表示当用户输入的用户名以"specialCharacter"结尾时该条statement生效。

参数	说明
	– "StringLike":{"obs:prefix":["private/"]}：表示在列举桶内对象时，需要指定prefix为private/或者包含private/这一子字符串。

说明

- Resource（资源）级别细粒度授权特性会逐步在各个区域上线，需要使用该特性时请确保桶所在区域已经支持。
- 使用Resource（资源）级别细粒度授权特性前，请**提交工单**到OBS，申请开通Resource（资源）级别细粒度授权特性白名单。

IAM 权限通用配置方法

- **创建IAM用户名授权使用OBS**
- **创建自定义策略**

OBS 自定义策略样例

- **示例1：给用户授予OBS的所有权限**

  此策略表示用户可以对OBS进行任何操作，使用方式包括API、SDK、控制台及工具。

  由于用户登录OBS控制台时，会访问一些其他服务的资源，如CTS审计信息，CDN加速域名，KMS密钥等。因此除了配置OBS的权限外，还需要配置其他服务的访问权限。其中CDN属于全局服务，CTS、KMS等属于区域级服务，需要根据您实际使用到的服务和区域分别在全局项目和对应区域项目中配置**Tenant Guest**权限。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:*:*"
            ]
        }
    ]
}
```

- **示例2：给用户授予桶的只读权限（不限定目录）**

  此策略表示用户可以对桶obs-example下的所有对象进行列举和下载。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:GetObject",
                "obs:bucket:ListBucket"
            ],
            "Resource": [
                "obs:*:*:object:obs-example/*",
                "obs:*:*:bucket:obs-example"
            ]
        }
```



```
    ]
}
```

- **示例3：给用户授予桶的只读权限（限定目录）**

  此策略表示用户只能下载桶obs-example中“my-project/”目录下的所有对象，其他目录下的对象虽然可以列举，但无法下载。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:GetObject",
                "obs:bucket:ListBucket"
            ],
            "Resource": [
                "obs:*:*:object:obs-example/my-project/*",
                "obs:*:*:bucket:obs-example"
            ]
        }
    ]
}
```

- **示例4：给用户授予桶的读写权限（限定目录）**

  此策略表示用户可以对桶obs-example中“my-project”目录下的所有的对象进行列举、下载、上传和删除。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:GetObject",
                "obs:object:ListMultipartUploadParts",
                "obs:bucket:ListBucket",
                "obs:object:DeleteObject",
                "obs:object:PutObject"
            ],
            "Resource": [
                "obs:*:*:object:obs-example/my-project/*",
                "obs:*:*:bucket:obs-example"
            ]
        }
    ]
}
```

- **示例5：给用户授予桶的所有权限**

  此策略表示用户可以对桶obs-example进行任何操作。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:*:*"
            ],
            "Resource": [
                "obs:*:*:bucket:obs-example",
                "obs:*:*:object:obs-example/*"
            ]
        }
    ]
}
```

- **示例6：拒绝用户上传对象**

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循**Deny优先原则**。

如果您给用户授予OBS OperateAccess的系统策略，但不希望用户拥有OBS OperateAccess中定义的上传对象的权限，您可以创建一条拒绝上传对象的自定义策略，然后同时将OBS OperateAccess和拒绝策略授予用户，根据Deny优先原则，则用户可以执行除了上传对象外OBS OperateAccess允许的所有操作。拒绝策略示例如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "obs:object:PutObject"
            ]
        }
    ]
}
```

- **示例7：给用户授予指定桶的修改桶存储类别权限以及桶内指定对象的删除权限**

  此策略表示用户可以对桶obs-example进行修改桶存储类别，以及对桶obs-example中“my-object.txt”对象进行删除。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:bucket:ListAllMyBuckets",
                "obs:bucket:ListBucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:DeleteObject",
                "obs:bucket:PutBucketStoragePolicy"
            ],
            "Resource": [
                "OBS:*:*:object:obs-example/my-object.txt",
                "OBS:*:*:bucket:obs-example"
            ]
        }
    ]
}
```

2.2 桶策略

桶策略

桶策略是作用于所配置的OBS桶及桶内对象的。OBS桶拥有者通过桶策略可为IAM用户或其他账号授权桶及桶内对象的操作权限。

说明

- 创建桶和获取桶列表这两个服务级的操作权限，需要通过**IAM权限**配置。
- 由于缓存的存在，配置桶策略后，最长需要等待5分钟策略才能生效。

桶策略模板：

OBS控制台预置了八种常用典型场景的桶策略模板，用户可以使用模板创建桶策略，快速完成桶策略配置。

选择使用模板创建时，部分模板需要指定被授权用户或资源范围，您也可以在原模板基础上修改被授权用户、资源范围、模板动作以及增加桶策略执行的条件。

表 2-4 桶策略模板

被授权用户	授权资源	模板名称	模板动作	高级设置
所有账号	整个桶（包括桶内对象）	公共读	**允许所有账号（所有互联网用户）对整个桶及桶内所有对象执行以下动作：** HeadBucket（判断桶是否存在、获取桶元数据） GetBucketLocation（获取桶位置） GetObject（获取对象内容、获取对象元数据） RestoreObject（恢复归档存储对象） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据）	不支持排除以上授权操作

被授权用户	授权资源	模板名称	模板动作	高级设置
		公共读写	**允许所有账号（所有互联网用户）对整个桶及桶内所有对象执行以下动作：** ListBucket（列举桶内对象、获取桶元数据） ListBucketVersions（列举桶内多版本对象） HeadBucket（判断桶是否存在、获取桶元数据） GetBucketLocation（获取桶位置） PutObject（PUT上传，POST上传，上传段，初始化上传段任务，合并段） GetObject（获取对象内容、获取对象元数据） ModifyObjectMetaData（修改对象元数据） ListBucketMultipartUploads（列举多段上传任务） ListMultipartUploadParts（列举已上传段） AbortMultipartUpload（取消多段上传任务） RestoreObject（恢复归档存储对象） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） PutObjectAcl（设置对象ACL） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象ACL）	不支持排除以上授权操作
当前账号/其他账号/委托账号	整个桶（包括桶内对象）	桶只读	**允许指定账号对整个桶及桶内所有对象执行以下动作：** Get*（所有获取操作） List*（所有列举操作） HeadBucket（判断桶是否存在、获取桶元数据）	不支持排除以上授权操作

被授权用户	授权资源	模板名称	模板动作	高级设置
		桶读写	**允许指定账号对整个桶及桶内所有对象执行除以下动作以外的所有动作：** DeleteBucket（删除桶） PutBucketPolicy（设置桶策略） PutBucketAcl（设置桶ACL）	排除以上授权操作
所有账号/当前账号/其他账号/委托账号	当前桶+指定对象	目录只读	**允许所有账号（所有互联网用户）或指定账号对当前桶和桶内指定资源执行以下动作：** GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象ACL） RestoreObject（恢复归档存储对象） HeadBucket（判断桶是否存在、获取桶元数据） GetBucketLocation（获取桶位置） **说明** 被授权用户选择“所有账号”时，模板动作中不包含ListBucket、ListBucketVersions。	不支持排除以上授权操作

被授权用户	授权资源	模板名称	模板动作	高级设置
		目录读写	**允许所有账号（所有互联网用户）或指定账号对当前桶和桶内指定资源执行以下动作：** PutObject（PUT上传，POST上传，上传段，初始化上传段任务，合并段） GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） ModifyObjectMetaData（修改对象元数据） ListBucketMultipartUploads（列举多段上传任务） ListMultipartUploadParts（列举已上传段） AbortMultipartUpload（取消多段上传任务） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象ACL） PutObjectAcl（设置对象ACL） RestoreObject（恢复归档存储对象） ListBucket（列举桶内对象、获取桶元数据） ListBucketVersions（列举桶内多版本对象） HeadBucket（判断桶是否存在、获取桶元数据） GetBucketLocation（获取桶位置）	不支持排除以上授权操作

被授权用户	授权资源	模板名称	模板动作	高级设置
所有账号/当前账号/其他账号/委托账号	指定对象	对象只读	**允许所有账号（所有互联网用户）或指定账号对桶内指定资源执行以下动作：** GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象ACL） RestoreObject（恢复归档存储对象）	不支持排除以上授权操作
		对象读写	**允许所有账号（所有互联网用户）或指定账号对桶内指定资源执行以下动作：** PutObject（PUT上传，POST上传，上传段，初始化上传段任务，合并段） GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） ModifyObjectMetaData（修改对象元数据） ListMultipartUploadParts（列举已上传段） AbortMultipartUpload（取消多段上传任务） GetObjectVersionAcl GetObjectAcl（获取对象ACL） PutObjectAcl（设置对象ACL） RestoreObject（恢复归档存储对象）	不支持排除以上授权操作

自定义桶策略：

你也可以根据实际业务场景的定制化需求，不使用预置桶策略模板，自定义创建桶策略。自定义桶策略由效力、被授权用户、资源、动作和条件5个桶策略基本元素共同决定。详细请参见**OBS权限控制要素**。

对象策略

对象策略即为桶策略中针对对象的策略，桶策略中针对对象的策略是通过配置资源来实现对象匹配的，资源可配置“*”（表示所有对象）或对象前缀（表示对象集）。对象策略则是直接选定对象后，配置到选定的对象资源的策略。

对象策略模板：

OBS控制台预置了两种常用典型场景的对象策略模板，用户可以使用模板创建对象策略，快速完成对象策略配置。

选择使用模板创建时，部分模板需要指定被授权用户，您也可以在原模板基础上修改被授权用户、模板动作以及增加对象策略执行的条件。资源范围即为所需配置对象策略的对象，系统自动指定，无需修改。

表 2-5 对象策略模板

被授权用户	授权资源	模板名称	模板动作	高级设置
所有账号/当前账号/其他账号/委托账号	指定对象	对象只读	**允许所有账号（所有互联网用户）或指定账号对桶内指定资源执行以下动作：** GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象ACL） RestoreObject（恢复归档存储对象）	不支持排除以上授权操作
		对象读写	**允许所有账号（所有互联网用户）或指定账号对桶内指定资源执行以下动作：** PutObject（PUT上传，POST上传，上传段，初始化上传段任务，合并段） GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） ModifyObjectMetaData（修改对象元数据） ListMultipartUploadParts（列举已上传段） AbortMultipartUpload（取消多段上传任务） GetObjectVersionAcl GetObjectAcl（获取对象ACL） PutObjectAcl（设置对象ACL） RestoreObject（恢复归档存储对象）	不支持排除以上授权操作

自定义对象策略：

你也可以根据实际业务场景的定制化需求，不使用预置对象策略模板，自定义创建对象策略。自定义对象策略由效力、被授权用户、资源、动作和条件5个桶策略基本元素共同决定，与桶策略类似，详细请参见**桶策略参数说明**。其中资源为已选择的对象，系统自动配置。

桶策略和对象策略之间的关系

对象策略即为桶策略中针对对象的策略，区别是对象策略只针对一个对象，桶策略中针对对象的策略可以配置多个对象或桶中所有对象。

桶策略应用场景

- 允许其他华为云账号访问OBS资源，可以使用桶策略的方式授权对应权限。
- 当不同的桶对于不同的IAM用户有不同的访问控制需求时，需使用桶策略分别授权IAM用户不同的权限。

桶策略通用配置方法

- **使用模板创建桶策略**
- **自定义创建桶策略（可视化视图）**
- **自定义创建桶策略（JSON视图）**

桶策略样例

- **示例1：向IAM用户授予指定桶中所有对象的指定操作权限**

  以下示例策略向账号b4bf1b36d9ca43d984fbcb9491b6fce9（账号ID）下的用户ID为71f3901173514e6988115ea2c26d1999的IAM用户授予PutObject和PutObjectAcl权限。

```
{
   "Statement":[
   {
     "Sid":"AddCannedAcl",
     "Effect":"Allow",
     "Principal": {"ID": ["domain/b4bf1b36d9ca43d984fbcb9491b6fce9:user/
71f3901173514e6988115ea2c26d1999"]},
     "Action":["PutObject","PutObjectAcl"],
     "Resource":["examplebucket/*"]
   }
  ]
}
```

- **示例2：向IAM用户授予指定桶的所有操作权限**

  以下示例策略向账号b4bf1b36d9ca43d984fbcb9491b6fce9（账号ID）下的用户ID为71f3901173514e6988115ea2c26d1999的IAM用户授予examplebucket的所有操作权限（包含桶操作与对象操作）。

```
{
   "Statement":[
   {
     "Sid":"test",
     "Effect":"Allow",
     "Principal": {"ID": ["domain/b4bf1b36d9ca43d984fbcb9491b6fce9:user/
71f3901173514e6988115ea2c26d1999"]},
     "Action":["*"],
     "Resource":[
       "examplebucket/*",
       "examplebucket"
     ]
   }
```

```
 ]
}
```

- **示例3：向OBS用户授予除删除对象外的所有对象操作权限**

  以下示例策略向账号b4bf1b36d9ca43d984fbcb9491b6fce9（账号户ID）下的用户ID为71f3901173514e6988115ea2c26d1999的IAM用户授予examplebucket除删除对象外的所有对象操作权限。

```
{
   "Statement":[
   {
     "Sid":"test1",
     "Effect":"Allow",
     "Principal": {"ID": ["domain/b4bf1b36d9ca43d984fbcb9491b6fce9:user/
71f3901173514e6988115ea2c26d1999"]},
     "Action":["*"],
     "Resource":["examplebucket/*"]
   },
   {
     "Sid":"test2",
     "Effect":"Deny",
     "Principal": {"ID": ["domain/b4bf1b36d9ca43d984fbcb9491b6fce9:user/
71f3901173514e6988115ea2c26d1999"]},
     "Action":["DeleteObject"],
     "Resource":["examplebucket/*"]
   }
 ]
}
```

- **示例4：向**所有账号**授予指定对象的只读权限**

  下面的示例策略向所有账号授予examplebucket桶中exampleobject的GetObject（下载对象）权限。此权限允许任何人读取对象exampleobject的数据。

```
{
   "Statement":[
   {
     "Sid":"AddPerm",
     "Effect":"Allow",
     "Principal": "*",
     "Action":["GetObject"],
     "Resource":["examplebucket/exampleobject"]
   }
 ]
}
```

- **示例5：限制对特定IP地址的访问权限**

  以下示例向任何用户授予对指定桶中的对象执行任何OBS操作的权限。但是，请求必须来自条件中指定的IP地址范围。此语句的条件确定允许的IP地址范围为192.168.0.*，只有一个例外：192.168.0.1。

  Condition块使用IpAddress和NotIpAddress条件以及SourceIp条件键（这是OBS范围的条件键）。另请注意SourceIp值使用RFC 4632中描述的CIDR表示法。

```
{
 "Statement": [
   {
     "Sid": "IPAllow",
     "Effect": "Allow",
     "Principal": "*",
     "Action": "*",
     "Resource": "examplebucket/*",
     "Condition": {
        "IpAddress": {"SourceIp": "192.168.0.0/24"},
        "NotIpAddress": {"SourceIp": "192.168.0.1/32"}
     }
   }
 ]
}
```


2.3 ACL

访问控制列表（Access Control List，ACL）是一个指定被授权者和所授予权限的授权列表。

OBS桶和对象的ACL是基于账号的访问控制，默认情况下，创建桶和对象时会同步创建ACL，授权拥有者对桶和对象资源的完全控制权限。

OBS的ACL为了实现用户简单实用地授权，包含以下特点：

- ACL对租户和租户下的用户都生效。
- 桶和对象的拥有者相同时，设置桶上的ACL默认对桶及桶中对象都生效。
- 桶创建时可以携带ACL，也可以创建成功后设置ACL；对象上传时可以携带ACL，也可以上传成功后再单独设置。

OBS ACL是基于账号级别的读写权限控制，权限控制细粒度不如桶策略和IAM权限。一般情况下，建议使用IAM权限和桶策略进行访问控制。

OBS支持通过ACL对**表2-6**所示用户或用户组授予桶的访问权限。

表 2-6 OBS 支持的被授权用户

被授权用户	描述
特定用户	ACL支持通过账号授予桶/对象的访问权限。授予账号权限后，账号下所有具有OBS资源权限的IAM用户都可以拥有此桶/对象的访问权限。 当需要为不同IAM用户授予不同的权限时，可以通过桶策略配置。
拥有者	桶的拥有者是指创建桶的账号。桶拥有者默认拥有所有的桶访问权限，其中桶ACL的读取和写入这两种权限永远拥有，且不支持修改。 对象的拥有者是上传对象的账号，而不是对象所属的桶的拥有者。对象拥有者默认拥有其对象的所有访问权限，其中对象ACL的读取和写入这两种权限永远拥有且不支持修改。 **须知** 不建议修改桶拥有者对桶的读取和写入权限。
匿名用户	未注册华为云的普通访客。如果匿名用户被授予了访问桶/对象的权限，则表示所有人都可以访问对应的桶/对象，并且不需要经过任何身份认证。 **须知** 开启匿名用户的桶/对象访问权限后，所有人都可以在不经过身份认证的情况下，对桶/对象进行访问。

被授权用户	描述
日志投递用户组 **说明** 仅桶ACL支持。	日志投递用户组用于投递OBS桶及对象的访问日志。由于OBS本身不能在账户的桶中创建或上传任何文件，因此在需要为桶记录访问日志时，只能由账户授予日志投递用户组一定权限后，OBS才能将访问日志写入指定的日志存储桶中。该用户组仅用于OBS内部的日志记录。 **须知** 当日志记录开启后，目标存储桶的日志投递用户组会同步开启桶的写入权限和ACL读取权限。如果手动将日志投递用户组的桶写入权限和ACL读取权限关闭，桶的日志记录会失败。

ACL 权限

桶ACL的访问权限如表2-7所示：

表 2-7 桶 ACL 访问权限

权限	选项	描述
桶访问权限	读取权限	此权限可以获取该桶内对象列表和桶的元数据。
	写入权限	此权限可以上传、覆盖和删除该桶内任何对象。
对象权限	对象读权限	此权限可以获取该桶内对象的内容和对象的元数据。 **说明** 仅支持给除匿名用户和日志投递用户组之外的用户配置该权限。
ACL访问权限	读取权限	此权限可以获取对应的桶的权限控制列表。 桶的拥有者默认永远具有ACL的读取权限。
	写入权限	此权限可以更新对应桶的权限控制列表。 桶的拥有者默认永远具有ACL的写入权限。

对象ACL的访问权限如表2-8所示：

表 2-8 对象 ACL 访问权限

权限	选项	描述
对象访问权限	读取权限	此权限可以获取该对象内容和元数据。
ACL访问权限	读取权限	此权限可以获取对应的对象的权限控制列表。 对象的拥有者默认永远具有ACL的读取权限
	写入权限	此权限可以更新对象的权限控制列表。 对象的拥有者默认永远具有ACL的写入权限。

说明

每一次对桶/对象的授权操作都将覆盖桶/对象已有的权限列表，而不会对其新增权限。

桶 ACL 应用场景

在以下场景，建议您使用桶ACL：

- 授予指定账号桶读取权限和桶写入权限，用以共享桶数据或挂载外部桶。比如，账号A授予账号B桶读取权限及桶写入权限后，账号B就可以通过OBS Browser+挂载外部桶、API&SDK等方式访问到该桶。
- 授予日志投递用户组桶写入权限，用以存储桶访问请求日志。

对象 ACL 应用场景

在以下场景，建议您使用对象ACL：

- 需要对象级的访问权限控制时。桶策略可以授予对象或对象集访问权限，当授予一个对象集权限后，想对对象集中某一个对象再进行单独授权，通过配置桶策略的方法显然不太实际。此时建议使用对象ACL，使得单个对象的权限控制更加方便。
- 使用对象链接访问对象时。一般使用对象ACL，将某一个对象通过对象链接开放给匿名用户进行读取操作。

使用头域设置 ACL

权限控制策略

OBS支持在创建桶或上传对象时通过头域设置桶或对象的权限控制策略（使用示例见**创桶请求示例**，**对象上传请求示例**），其设置的权限控制策略只能选择预定义的几种策略。其中，x-obs-acl比较特殊，可以设置六种权限，这六种权限对桶或对象的Owner不产生影响，即Owner拥有完全控制的权限。其详细情况如下图所示。

表 2-9 OBS 预定义的权限控制策略

预定义的权限控制策略	描述
private	桶或对象的所有者拥有完全控制的权限，其他任何人都没有访问权限。
public-read	设在桶上，所有人可以获取该桶内对象列表、桶内多段任务、桶的元数据。 设在对象上，所有人可以获取该对象内容和元数据。
public-read-write	设在桶上，所有人可以获取该桶内对象列表、桶内多段任务、桶的元数据、上传对象、删除对象、初始化段任务、上传段、合并段、拷贝段、取消多段上传任务。 设在对象上，所有人可以获取该对象内容和元数据。
public-read-delivered	设在桶上，所有人可以获取该桶内对象列表、桶内多段任务、桶的元数据，可以获取该桶内对象的内容和元数据。 不能应用在对象上。

预定义的权限控制策略	描述
public-read-write-delivered	设在桶上，所有人可以获取该桶内对象列表、桶内多段任务、桶的元数据、上传对象、删除对象、初始化段任务、上传段、合并段、拷贝段、取消多段上传任务，可以获取该桶内对象的内容和元数据。 不能应用在对象上。
bucket-owner-full-control	设在对象上，桶和对象的所有者拥有对象的完全控制权限，其他任何人都没有访问权限。 默认情况下，上传对象至其他用户的桶中，桶拥有者没有对象的控制权限。对象拥有者为桶拥有者添加此权限控制策略后，桶所有者可以完全控制对象。 例如，用户A上传对象x至用户B的桶中，系统默认用户B没有对象x的控制权。当用户A为对象x设置bucket-owner-full-control策略后，用户B就拥有了对象x的控制权。

说明

系统默认权限控制策略为private权限。

在创建桶或上传对象时，可以用来设置权限控制策略的其他头域如下所示：

表 2-10 通过头域设置桶或对象 ACL 的头域格式

头域	含义
x-obs-grant-read	授权给指定domain下的所有用户有READ权限。
x-obs-grant-write	授权给指定domain下的所有用户有WRITE权限。
x-obs-grant-read-acp	授权给指定domain下的所有用户有READ_ACP权限。
x-obs-grant-write-acp	授权给指定domain下的所有用户有WRITE_ACP权限。
x-obs-grant-full-control	授权给指定domain下的所有用户有FULL_CONTROL权限。
x-obs-grant-read-delivered	授权给指定domain下的所有用户有对桶和桶内对象的READ权限，且对象继承桶权限。 不能应用在对象上。
x-obs-grant-full-control-delivered	授权给指定domain下的所有用户有对桶和桶内对象的FULL_CONTROL权限，且对象继承桶权限。 不能应用在对象上。

3 请求方式介绍

3.1 通过永久访问密钥访问 OBS

OBS的REST接口既支持认证请求，也支持匿名请求。匿名请求通常仅用于需要公开访问的场景，例如静态网站托管。除此之外，绝大多数场景是需要经过认证的请求才可以访问成功。经过认证的请求总是需要包含一个签名值，该签名值以请求者的访问密钥（AK/SK）作为加密因子、结合请求体携带的特定信息计算而成。计算签名的过程已经包含在SDK中，使用者只需将访问密钥在SDK初始化阶段设置好即可，无需关心签名计算的具体实现。但是，如果客户端选择通过REST API自行开发程序对接OBS，则需要按照OBS定义的签名算法来计算签名并添加到请求中。

用户可以在“我的凭证”页面创建永久访问密钥（AK/SK）。

- Access Key Id（AK）：访问密钥ID。与私有访问密钥关联的唯一标识符；访问密钥ID和私有访问密钥一起使用，对请求进行加密签名。
- Secret Access Key（SK）：与访问密钥ID结合使用的私有访问密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。

AK可唯一标识公有云IAM用户，OBS根据AK/SK确认请求者身份，并进行权限检查。

获取永久访问密钥的方法，请参见**获取访问密钥（AK/SK）**。

3.2 通过临时访问密钥访问 OBS

临时访问密钥

OBS可以通过IAM获取临时访问密钥（临时AK，SK和securitytoken）进行临时授权访问。通过使用临时AK，SK和securitytoken，您可以为第三方应用或IAM用户颁发一个自定义时效和权限的访问凭证。

您可以通过调用IAM的**获取临时AK/SK和securitytoken接口**获取临时AK/SK和securitytoken。

临时AK/SK和securitytoken遵循权限最小化原则，可应用于临时访问OBS等。使用临时AK/SK调用API鉴权时，临时AK/SK和securitytoken必须同时使用，请求头中需要添加“x-obs-security-token”字段。

临时访问密钥相比IAM用户的永久访问密钥的优势主要有两点：

- 临时访问密钥的有效时间为15min至24h，不必暴露出IAM用户的永久密钥，降低了账号泄露带来的安全风险。
- 在获取临时访问密钥时，通过传入policy参数设置临时权限来进一步约束使用者的权限范围，方便IAM用户对使用者的权限进一步管理。

具体使用方法，参考**用户签名验证**。

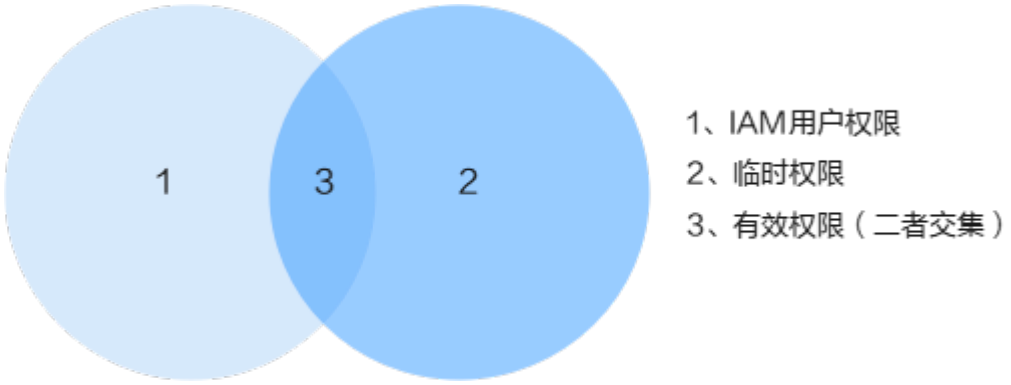
临时访问密钥的权限

IAM用户在调用IAM的**获取临时AK/SK和securitytoken接口**时，可通过设置policy参数，为临时访问密钥增加临时策略来约束使用者的权限。临时策略的格式与内容与**IAM权限**保持一致。

- 如果不设置policy参数，即不使用临时策略，则获取的临时访问密钥具有与IAM用户相同的权限。
- 如果设置了policy参数，即使用了临时策略，则获取的临时访问密钥的权限在IAM用户原有权限的基础上，进一步约束在设置的临时策略以内。

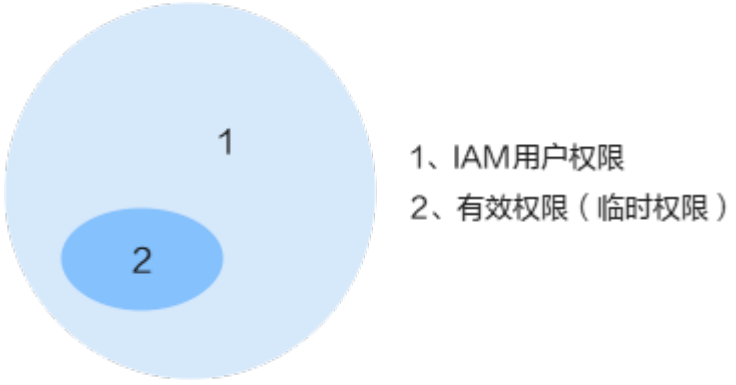
如下图，“1”代表了IAM用户的原有权限，“2”为设置的临时策略所对应的临时权限，两个权限的交集“3”即为使用者最终的有效权限。

图 3-1 IAM 用户权限和临时权限交集



临时访问密钥遵循权限最小化原则，建议在IAM用户原有权限范围内配置临时策略，以免在使用时产生配置了临时策略却没有对应权限的疑惑。如下图所示，使用者最终的有效权限即为设置的临时权限。

图 3-2 临时权限设置在 IAM 用户权限范围内



临时策略的权限判断同样遵循Deny优先的原则，对于未设置的权限则默认拒绝。

说明

设置临时策略时，因不设置的权限将默认拒绝，所以建议只设置显式的Allow权限即可。

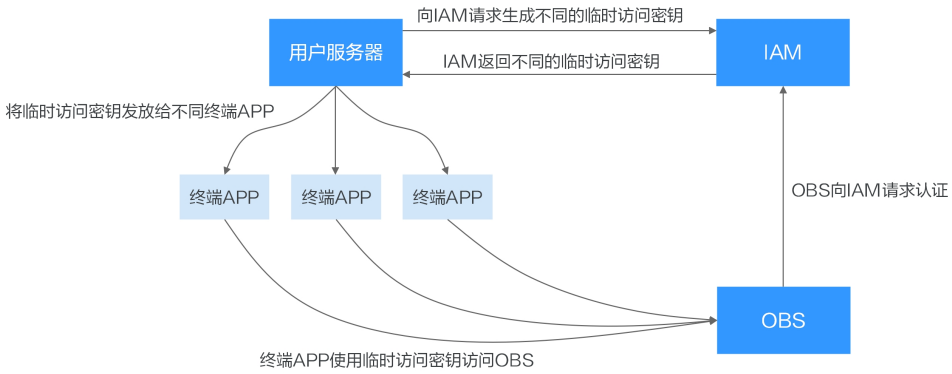
应用场景

临时访问密钥主要用于授权第三方临时访问OBS服务。例如，部分企业拥有自己的用户管理系统，用户管理系统中的用户包括终端APP用户、企业本地用户等，这部分用户并不具有IAM用户的权限，通过授予其临时访问密钥来访问OBS。

典型场景如下：

某企业拥有大量的终端APP，终端APP都需要拥有访问OBS服务的能力，不同的终端APP可能代表着不同的终端用户，不同的终端用户需要拥有不同的访问权限。该场景便可使用临时访问密钥访问OBS服务。

图 3-3 临时访问密钥使用场景



1. 用户服务器可配置IAM用户的永久访问密钥，由该用户服务器向IAM请求，为不同的终端APP生成不同的临时访问密钥。

   IAM用户调用IAM的**获取临时AK/SK和securitytoken接口**获取临时AK/SK和securitytoken。在调用该接口时，传入policy参数来设置临时策略，例如：

   ```
   {
       "auth": {
           "identity": {
               "methods": [
                   ... ...
               ],
               "policy": {
                   ... ...
               }
           }
       }
   }
   ```

   其中policy的语义与格式和**IAM权限**相同，相关授权项参考**权限及授权项说明**。
2. IAM根据传入的policy内容以及有效时间来生成拥有不同权限和不同有效期的临时访问密钥并返回给用户服务器。
3. 用户服务器将临时访问密钥分发给对应权限的终端APP。

4. 终端APP可通过临时访问密钥使用OBS SDK或API访问OBS服务，因临时凭据的有效时间较短，终端APP需及时向用户服务器请求更新临时访问密钥。

配置示例

请参见**临时授权访问OBS**。

3.3 通过临时 URL 访问 OBS

您可以通过临时URL访问OBS，对桶或对象进行创建桶、上传对象和下载对象等操作，详细示例可参考**通过临时URL访问OBS**。本章节主要详细介绍如何通过临时URL分享对象。

分享对象

OBS提供分享功能，将存放在OBS中对象（文件或文件夹）限时分享给所有用户。

文件分享

文件分享强调临时性，所有分享的URL都是临时URL，存在有效期。

临时URL是由文件的访问域名和临时鉴权信息组成。示例如下：

```
https://bucketname.obs.cn-north-4.myhuaweicloud.com:443/image.png?
AccessKeyId=xxx&Expires=xxx&response-content-disposition=xxx&x-obs-security-token=xxx&Signature=xxx
```

临时鉴权信息主要包含**AccessKeyId**、**Expires**、**x-obs-security-token**和**Signature**四个参数。其中**AccessKeyId**、**x-obs-security-token**和**Signature**用于鉴权，**Expires**定义鉴权的有效期。临时鉴权的方法及各参数的详细解释，请参见《对象存储服务API参考》的**URL中携带签名**章节。此外，临时URL中还包含了**response-content-disposition**，定义访问对象时是直接下载或者在浏览器中预览，取值由浏览器根据所分享对象的Content-Type解析所得。

当在OBS控制台上单击了对象后的“分享”之后，OBS就会以默认5分钟的有效期获取临时鉴权信息，并生成分享链接，此时链接就已经生效并且开始计算时间了。每调整一次URL有效期，OBS就会重新获取一次鉴权信息以生成新的分享链接，新链接的有效期从调整的时候开始计算。

文件夹分享

文件夹分享强调临时性，存在有效期。临时分享分为两种方式：提取码分享、直接分享。

- 提取码分享：分享者需要先设置一个6位数的提取码，再创建分享。创建成功后，OBS会自动将文件夹中的所有对象的下载链接汇总到一个静态网站中，并托管到一个公共的OBS桶。所有用户均可使用创建分享时生成的临时URL和提取码，访问这个静态网站，并进行文件下载。
- 直接分享：分享者输入有效期后直接分享链接给用户。用户通过一个签名即可访问文件夹下所有的对象。

约束与限制

- 通过OBS控制台分享的文件或文件夹，有效期的范围为1分钟到18小时。如果想要设置更长的有效期，建议使用客户端工具OBS Browser+，OBS Browser+最长支持1年的有效期。如果想要设置永久的权限，请**通过桶策略向所有账号授予指定对象的读权限**。

- 仅桶版本号为3.0的桶支持文件和文件夹分享功能。桶版本号可以在桶概览页的“基本信息”中查看。
- 对于文件分享，归档存储或深度归档存储对象需恢复后才能分享；对于文件夹分享，归档存储或深度归档存储对象需在原桶恢复后才能下载。

配置方法

对于文件和文件夹的分享方法，请参见**向所有账号临时分享对象**。

3.4 通过 IAM 委托访问 OBS

IAM委托为统一身份认证服务IAM的功能特性，OBS在部分使用场景中（如CDN私有桶回源、跨区域复制），需要使用IAM委托功能，授予其他用户或云服务OBS的访问权限，替委托方管理OBS资源，实现安全高效的代维工作。

关于IAM委托的相关介绍，请参考**《统一身份认证服务用户指南》**。

4 典型场景配置案例

4.1 对当前账号下单个 IAM 用户授权

4.1.1 对单个 IAM 用户授予创建桶和列举桶的权限

场景介绍

本案例介绍如何为华为云账号下的某个IAM用户授予OBS创建桶和列举桶的权限。拥有本权限的IAM用户可以创建桶，创建的桶仍然属于IAM用户对应的账号。同时该IAM用户也可以看到账号下的所有桶。

推荐配置方法

创建桶和列举桶属于OBS服务级别权限，只能通过IAM权限实现，推荐使用IAM自定义策略。

配置步骤

步骤1 使用账号登录华为云，在右上角单击“控制台”。

步骤2 在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”。

步骤3 在左侧导航窗格中，单击“权限管理”>“权限”>“创建自定义策略”。

步骤4 配置自定义策略参数。

图 4-1 配置自定义策略

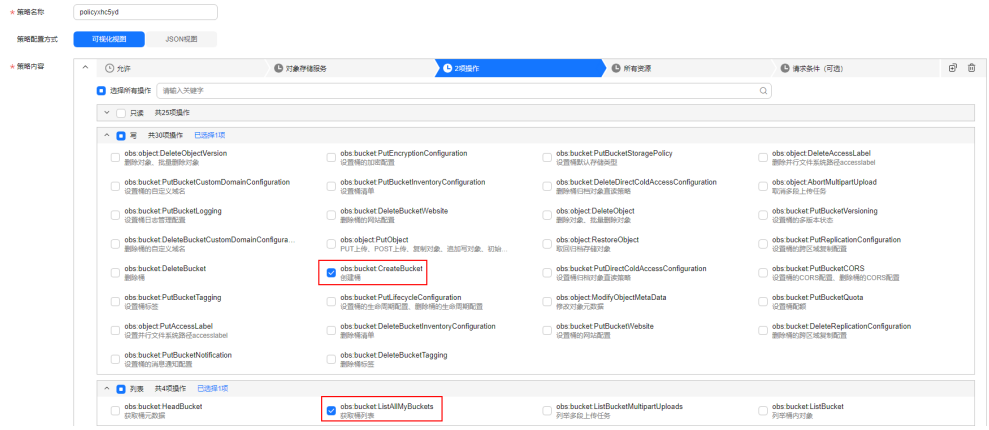


表 4-1 自定义策略参数配置说明

参数	说明
策略名称	输入自定义策略的名称
策略配置方式	根据使用习惯进行选择，此处以“可视化视图”为例
策略内容	• 选择“允许” • 选择“对象存储服务（OBS）” • 勾选“写”操作中的“obs:bucket:CreateBucket”和“列表”操作中的“obs:bucket:ListAllMyBuckets” • 选择“所有资源”
作用范围	默认为“全局级服务”

步骤5 单击“确定”，完成自定义策略创建。

步骤6 **创建用户组并授权**。

按照IAM文档指导，将前面步骤创建的自定义策略添加到用户组中。

步骤7 将需要授权的IAM用户**加入到创建的用户组中**，授权完成。

说明

由于缓存的存在，授予OBS相关的策略后，大概需要等待10~15分钟策略才能生效。

----结束

4.1.2 对单个 IAM 用户授予桶的读写权限

场景介绍

本案例介绍如何为华为云账号下的某个IAM用户授予OBS桶的读写权限。

推荐配置方法

对单个IAM用户授予资源级别权限，推荐使用桶策略。

配置须知

本案例预置的“桶读写”模板允许指定IAM用户对整个桶及桶内所有对象执行除以下权限以外的所有权限：

- DeleteBucket：删除桶
- PutBucketPolicy：设置桶策略
- PutBucketAcl：设置桶ACL

按照本案例配置后，可以正常通过API或SDK完成读写操作（上传、下载、删除桶内所有对象），但如果通过控制台或OBS Browser+登录，会出现无权限的相关提示信息。**报错原因**

如果希望IAM用户能在控制台或OBS Browser+顺利完成相关读写操作，请按照**后续操作**继续配置IAM自定义策略。

配置完成进入桶后仍然会出现无权限相关提示，属于正常现象，因为控制台还调用了其他高级配置的接口，但此时已可以正常完成读写模式中允许的操作。

配置步骤

步骤1 在OBS管理控制台左侧导航栏选择“桶列表”。

步骤2 在桶列表单击目标桶的桶名称，进入“对象”页面。

步骤3 在左侧导航栏，单击“访问权限控制>桶策略”，进入桶策略页面。

步骤4 单击“创建”。

步骤5 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。

步骤6 配置桶策略内容。

图 4-2 配置桶策略

表 4-2 桶策略配置说明

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许
	被授权用户	• 被授权用户：当前账号 • 选择子用户：选择被授权的IAM用户
	授权资源	• 资源范围：整个桶（包括桶内对象）
	授权操作	• 动作范围：模板配置 • 模板：桶读写

步骤7 核对权限配置信息，确认无误后单击“创建”，完成桶策略创建。

----结束

后续操作

如果希望在控制台或OBS Browser+顺利完成读写操作，需要能“看到”桶和桶中的对象，即需要通过IAM自定义策略配置列举桶（obs:bucket:ListAllMyBuckets）和列举桶中对象（obs:bucket:ListBucket）的权限。

说明

obs:bucket:ListAllMyBuckets面向所有资源，obs:bucket:ListBucket只面向授权的桶，所以策略要分别添加两条权限。

步骤1 使用账号登录华为云，在右上角单击“控制台”。

步骤2 在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”。

步骤3 在左侧导航窗格中，单击“权限管理”>“权限”>“创建自定义策略”。

步骤4 配置自定义策略参数。

图 4-3 配置自定义策略

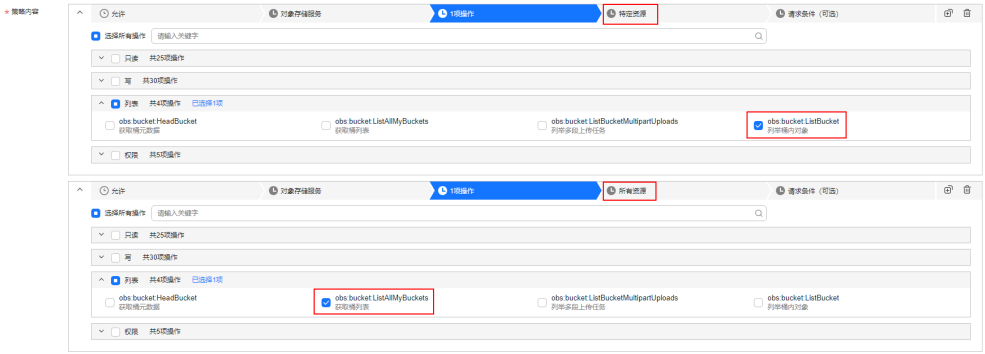


表 4-3 自定义策略参数配置说明

参数	说明
策略名称	输入自定义策略的名称
策略配置方式	根据使用习惯进行选择，此处以“可视化视图”为例
策略内容	【权限1】 • 选择“允许” • 选择“对象存储服务 (OBS)” • 勾选“列表”操作中的“obs:bucket:ListAllMyBuckets” • 选择“所有资源” 【权限2】 • 选择“允许” • 选择“对象存储服务 (OBS)” • 勾选“列表”操作中的“obs:bucket:ListBucket” • 选择“特定资源 > 通过资源路径指定 >添加资源路径”，在路径中输入授权的桶名称，表示本策略只对该桶生效

参数	说明
作用范围	默认为“全局级服务”

步骤5 单击“确定”，完成自定义策略创建。

步骤6 创建用户组并授权。

按照IAM文档指导，将前面步骤创建的自定义策略添加到用户组中。

步骤7 将需要授权的IAM用户加入到创建的用户组中，授权完成。

说明

由于缓存的存在，授予OBS相关的策略后，大概需要等待10~15分钟策略才能生效。

----结束

4.1.3 对单个 IAM 用户授予桶的指定操作权限

场景介绍

本案例介绍如何为华为云账号下的某个IAM用户授予OBS桶的指定操作权限，此处以授予删除桶的权限为例。

如果需要配置其他指定的权限，在桶策略的动作名称中选择对应动作即可。OBS支持的动作

推荐配置方法

对单个IAM用户授予资源级别权限，推荐使用桶策略。

配置须知

按照本案例配置后，可以正常通过API或SDK完成桶删除操作，但如果通过控制台或OBS Browser+登录桶列表，会出现无权限的相关提示信息。

报错原因：控制台或OBS Browser+登录后，加载桶列表会调用获取桶列表（ListAllMyBuckets）等接口，删除桶时会先调用列举多版本对象（ListBucketVersions）接口。而授予的权限中并没有包含这些操作的权限，所以会提示“拒绝访问，请检查相应权限”，或者“不允许在请求的资源上执行此操作”。

如果希望IAM用户能在控制台或OBS Browser+顺利完成桶删除操作，桶策略中要额外配置ListBucketVersions权限，同时请按照后续操作继续配置IAM自定义策略授予ListAllMyBuckets权限。

配置步骤

步骤1 在OBS管理控制台左侧导航栏选择“桶列表”。

步骤2 在桶列表单击目标桶的桶名称，进入“对象”页面。

步骤3 在左侧导航栏，单击“访问权限控制>桶策略”，进入桶策略页面。

步骤4 在“桶策略”页面，单击“创建”。

步骤5 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。

步骤6 配置桶策略内容。

图 4-4 配置桶策略

表 4-4 桶策略配置说明

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许
	被授权用户	• 被授权用户：当前账号 • 选择子用户：选择被授权的IAM用户
	授权资源	• 资源范围：当前桶

参数		说明
	授权操作	• 动作范围：自定义配置 • 选择动作： – DeleteBucket（删除桶） – ListBucketVersions（列举桶内多版本对象） **说明** 如果需要配置其他指定的权限，选择对应动作即可。 **OBS支持的动作**

步骤7 核对权限配置信息，确认无误后单击“创建”，完成桶策略创建。

----结束

后续操作

如果希望在控制台和OBS Browser+顺利完成删除桶操作，需要能在控制台或OBS Browser+“看到”桶，即需要通过IAM自定义策略配置列举桶（obs:bucket:ListAllMyBuckets）权限。

步骤1 使用账号登录华为云，在右上角单击“控制台”。

步骤2 在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”。

步骤3 在左侧导航窗格中，单击“权限管理”>“权限”>“创建自定义策略”。

步骤4 配置自定义策略参数。

图 4-5 配置自定义策略

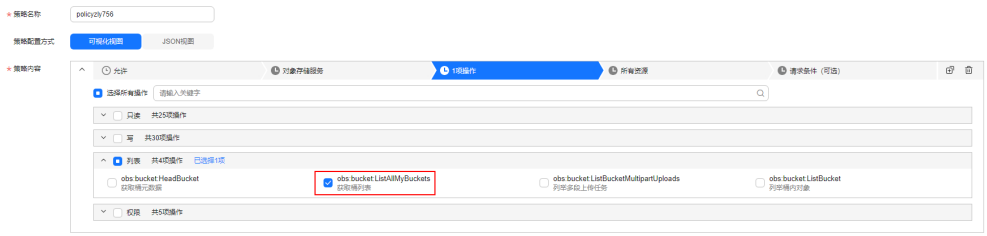


表 4-5 自定义策略参数配置说明

参数	说明
策略名称	输入自定义策略的名称。
策略配置方式	根据使用习惯进行选择，此处以“可视化视图”为例。
策略内容	• 选择“允许” • 选择“对象存储服务 (OBS)” • 勾选“列表”操作中的“obs:bucket:ListAllMyBuckets” • 选择“所有资源”
作用范围	默认为“全局级服务”。

步骤5 单击“确定”，完成自定义策略创建。

步骤6 **创建用户组并授权**。

按照IAM文档指导，将前面步骤创建的自定义策略添加到用户组中。

步骤7 将需要授权的IAM用户**加入到创建的用户组中**，授权完成。

说明

由于缓存的存在，授予OBS相关的策略后，大概需要等待10~15分钟策略才能生效。

----结束

4.1.4 对单个 IAM 用户授予指定对象的读权限

场景介绍

本案例介绍如何为华为云账号下的某个IAM用户授予OBS桶中某个对象或某类对象的读权限。

推荐配置方法

对单个IAM用户授予资源级别权限，推荐使用桶策略。

配置须知

本案例预置的“对象只读”模板允许指定IAM用户对桶内指定对象执行以下权限：

- GetObject：获取对象内容、获取对象元数据
- GetObjectVersion：获取指定版本对象内容、获取指定版本对象元数据
- GetObjectVersionAcl：获取指定版本对象ACL
- GetObjectAcl：获取对象ACL
- RestoreObject：恢复归档存储对象

按照本案例配置后，可以正常通过API或SDK完成读操作（下载指定对象），但如果通过控制台或OBS Browser+登录，会出现无权限的相关提示信息。

报错原因：通过控制台或者OBS Browser+登录后，加载桶列表时会调用获取桶列表（ListAllMyBuckets）等接口，加载对象列表时会调用列举桶内对象（ListBucket）等接口，其他页面也会调用其他的OBS接口。而授予的只读权限中并没有包含这些操作的权限，所以会提示“拒绝访问，请检查相应权限”，或者“不允许在请求的资源上执行此操作”。

如果希望IAM用户能在控制台或OBS Browser+顺利完成相关读操作，请按照**后续操作**继续配置IAM自定义策略。

配置步骤

步骤1 在OBS管理控制台左侧导航栏选择“桶列表”。

步骤2 在桶列表单击目标桶的桶名称，进入“对象”页面。

步骤3 在左侧导航栏，单击“访问权限控制>桶策略”，进入桶策略页面。

步骤4 在“桶策略”页面，单击“创建”。

步骤5 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。

步骤6 配置桶策略内容。

图 4-6 配置桶策略

表 4-6 桶策略配置说明

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许
	被授权用户	• 被授权用户：当前账号 • 选择子用户：选择被授权的IAM用户

参数		说明
	授权资源	• 资源范围：指定对象 • 资源路径：输入对象前缀 **说明** – 指定对象支持输入多个资源路径，单击“添加资源路径”按钮即可。 – 您可以指定资源路径为具体对象、对象集或目录，*表示桶内所有对象。 如果指定某个对象：对象名称。 如果指定某个对象集：“对象名称前缀”+“*”、“*”+“对象名后缀”或“*”。
	授权操作	• 动作范围：模板配置 • 模板：对象只读

步骤7 核对权限配置信息，确认无误后单击“创建”，完成桶策略创建。

----结束

后续操作

如果希望在控制台或OBS Browser+顺利完成读操作，需要能“看到”桶和桶中的对象，即需要通过IAM自定义策略配置列举桶（obs:bucket:ListAllMyBuckets）和列举桶中对象（obs:bucket:ListBucket）的权限。

说明

obs:bucket:ListAllMyBuckets面向所有资源，obs:bucket:ListBucket只面向授权的桶，所以策略要分别添加两条权限。

步骤1 使用账号登录华为云，在右上角单击“控制台”。

步骤2 在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”。

步骤3 在左侧导航窗格中，单击“权限管理”>“权限”>“创建自定义策略”。

步骤4 配置自定义策略参数。

图 4-7 配置自定义策略

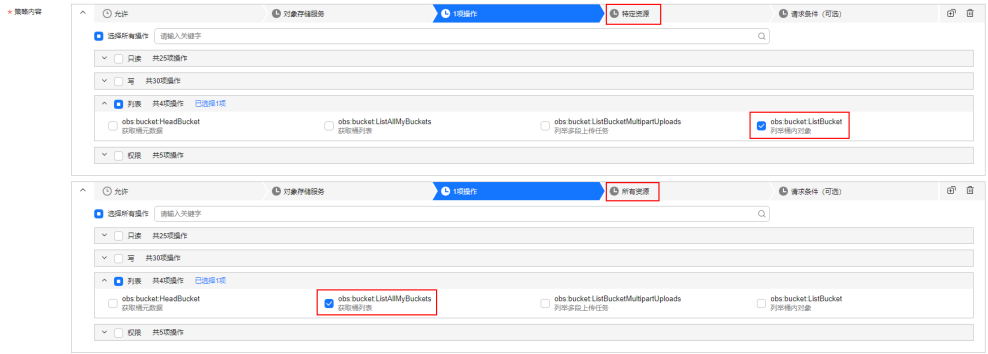


表 4-7 自定义策略参数配置说明

参数	说明
策略名称	输入自定义策略的名称
策略配置方式	根据使用习惯进行选择，此处以“可视化视图”为例
策略内容	【权限1】 • 选择“允许” • 选择“对象存储服务 (OBS)” • 勾选“列表”操作中的“obs:bucket:ListAllMyBuckets” • 选择“所有资源” 【权限2】 • 选择“允许” • 选择“对象存储服务 (OBS)” • 勾选“列表”操作中的“obs:bucket:ListBucket” • 选择“特定资源 > 通过资源路径指定 >添加资源路径”，在路径中输入授权的桶名称，表示本策略只对该桶生效
作用范围	默认为“全局级服务”

步骤5 单击“确定”，完成自定义策略创建。

步骤6 **创建用户组并授权**。

按照IAM文档指导，将前面步骤创建的自定义策略添加到用户组中。

步骤7 将需要授权的IAM用户**加入到创建的用户组中**，授权完成。

说明

由于缓存的存在，授予OBS相关的策略后，大概需要等待10~15分钟策略才能生效。

----结束

4.1.5 对单个 IAM 用户授予指定对象的指定操作权限

场景介绍

本案例介绍如何为华为云账号下的某个IAM用户授予OBS桶中指定对象的指定操作权限，此处以授予下载对象的权限为例。

如果需要配置其他指定的权限，在桶策略的动作名称中选择对应动作即可。**OBS支持的动作**

推荐配置方法

对单个IAM用户授予资源级别权限，推荐使用桶策略。

配置须知

按照本案例配置后，可以正常通过API或SDK完成对象下载操作，但如果通过控制台或OBS Browser+登录桶列表，会出现无权限的相关提示信息。

报错原因：通过控制台或者OBS Browser+登录后，加载桶列表时会调用获取桶列表（ListAllMyBuckets）等接口，加载对象列表时会调用列举桶内对象（ListBucket）等接口，其他页面也会调用其他的OBS接口。而授予的只读权限中并没有包含这些操作的权限，所以会提示“拒绝访问，请检查相应权限”，或者“不允许在请求的资源上执行此操作”。

如果希望IAM用户能在控制台或OBS Browser+顺利完成对象下载操作，请按照**后续操作**继续配置IAM自定义策略。

配置步骤

步骤1 在OBS管理控制台左侧导航栏选择“桶列表”。

步骤2 在桶列表单击目标桶的桶名称，进入“对象”页面。

步骤3 在左侧导航栏，单击“访问权限控制>桶策略”，进入桶策略页面。

步骤4 在“桶策略”页面，单击“创建”。

步骤5 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。

步骤6 配置桶策略内容。

图 4-8 配置桶策略

表 4-8 桶策略配置说明

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许
	被授权用户	• 被授权用户：当前账号 • 选择子用户：选择被授权的IAM用户

参数		说明
	授权资源	• 资源范围：指定对象 • 资源路径：输入对象前缀 **说明** – 指定对象支持输入多个资源路径，单击“添加资源路径”按钮即可。 – 您可以指定资源路径为具体对象、对象集或目录，*表示桶内所有对象。 如果指定某个对象：对象名称。 如果指定某个对象集：“对象名称前缀”+“*”、“*”+“对象名后缀”或“*”。
	授权操作	• 动作范围：自定义配置 • 动作：GetObject（获取对象内容、获取对象元数据） **说明** 如果需要配置其他指定的权限，选择对应动作即可。**OBS支持的动作**

步骤7 核对权限配置信息，确认无误后单击“创建”，完成桶策略创建。

----结束

后续操作

如果希望在控制台或OBS Browser+顺利完成指定的操作，需要能“看到”桶和桶中的对象，即需要通过IAM自定义策略配置列举桶（obs:bucket:ListAllMyBuckets）和列举桶中对象（obs:bucket:ListBucket）的权限。

说明

obs:bucket:ListAllMyBuckets面向所有资源，obs:bucket:ListBucket只面向授权的桶，所以策略要分别添加两条权限。

步骤1 使用账号登录华为云，在右上角单击“控制台”。

步骤2 在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”。

步骤3 在左侧导航窗格中，单击“权限管理”>“权限”>“创建自定义策略”。

步骤4 配置自定义策略参数。

图 4-9 配置自定义策略

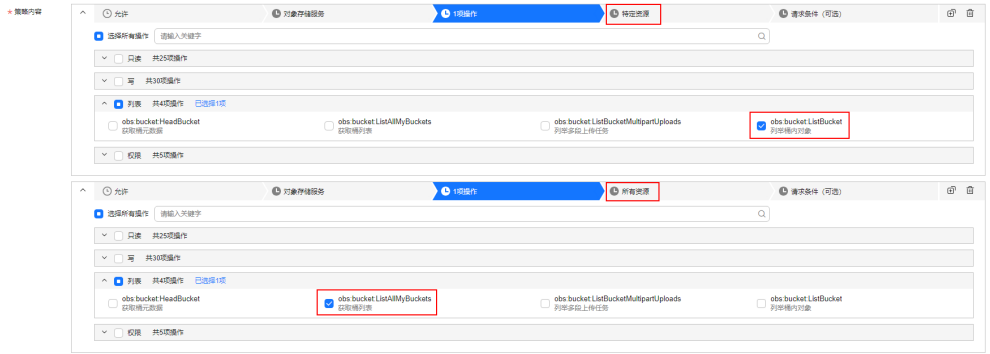


表 4-9 自定义策略参数配置说明

参数	说明
策略名称	输入自定义策略的名称
策略配置方式	根据使用习惯进行选择，此处以“可视化视图”为例
策略内容	【权限1】 • 选择“允许” • 选择“对象存储服务 (OBS)” • 勾选“列表”操作中的“obs:bucket:ListAllMyBuckets” • 选择“所有资源” 【权限2】 • 选择“允许” • 选择“对象存储服务 (OBS)” • 勾选“列表”操作中的“obs:bucket:ListBucket” • 选择“特定资源 > 通过资源路径指定 >添加资源路径”，在路径中输入授权的桶名称，表示本策略只对该桶生效
作用范围	默认为“全局级服务”

步骤5 单击“确定”，完成自定义策略创建。

步骤6 创建用户组并授权。

按照IAM文档指导，将前面步骤创建的自定义策略添加到用户组中。

步骤7 将需要授权的IAM用户加入到创建的用户组中，授权完成。

说明

由于缓存的存在，授予OBS相关的策略后，大概需要等待10~15分钟策略才能生效。

----结束

4.2 对当前账号下多个 IAM 用户或用户群组授权

4.2.1 对 IAM 用户组授予 OBS 所有资源的所有操作权限

场景介绍

本案例介绍如何为华为云账号下的多个IAM用户或用户群组授予OBS所有资源的所有操作权限。拥有本权限的IAM用户可以执行任何OBS操作。

推荐配置方法

IAM自定义策略

配置步骤

步骤1 使用账号登录华为云，在右上角单击“控制台”。

步骤2 在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”。

步骤3 在左侧导航窗格中，单击“权限管理”>“权限”>“创建自定义策略”。

步骤4 配置自定义策略参数。

图 4-10 配置自定义策略

表 4-10 自定义策略参数配置说明

参数	说明
策略名称	输入自定义策略的名称
策略配置方式	根据使用习惯进行选择，此处以“可视化视图”为例
策略内容	• 选择“允许” • 选择“对象存储服务 (OBS)” • 勾选“选择所有操作” • 选择“所有资源”
作用范围	默认为“全局级服务”

步骤5 单击“确定”，完成自定义策略创建。

步骤6 **创建用户组并授权**。

按照IAM文档指导，将前面步骤创建的自定义策略添加到用户组中。

步骤7 将需要授权的IAM用户**加入到创建的用户组中**，授权完成。

说明

由于缓存的存在，授予OBS相关的策略后，大概需要等待10~15分钟策略才能生效。

----结束

4.2.2 对 IAM 用户组授予 OBS 所有资源的基本操作权限

场景介绍

本案例介绍如何通过IAM预置的与OBS相关的系统角色和策略，为华为云账号下的多个IAM用户或用户群组授予OBS所有资源的基本操作权限。预置的系统角色和策略所支持的权限如下表所示。

表 4-11 OBS 系统权限

系统角色/策略名称	描述	类别
Tenant Administrator	拥有该权限的用户拥有除IAM外，其他所有服务的所有执行权限。	系统角色
Tenant Guest	拥有该权限的用户拥有除IAM外，其他所有服务的只读权限。	系统角色
OBS Administrator	拥有该权限的用户为OBS管理员，可以对账号下的所有OBS资源执行任意操作。	系统策略
OBS Buckets Viewer	拥有该权限的用户可以执行列举桶、获取桶基本信息、获取桶元数据的操作。	系统角色
OBS ReadOnlyAccess	拥有该权限的用户可以执行列举桶、获取桶基本信息、获取桶元数据、列举对象（不包含多版本）的操作。 **说明** 拥有该权限的用户如果在控制台上列举对象失败，可能是因为桶中存在多版本对象。此时需要额外授予该用户列举多版本对象的权限（obs:bucket:ListBucketVersions），才能在控制台正常看到对象列表。	系统策略
OBS OperateAccess	拥有该权限的用户可以执行OBS ReadOnlyAccess的所有操作，在此基础上还可以执行上传对象、下载对象、删除对象、获取对象ACL等对象基本操作。 **说明** 拥有该权限的用户如果在控制台上列举对象失败，可能是因为桶中存在多版本对象。此时需要额外授予该用户列举多版本对象的权限（obs:bucket:ListBucketVersions），才能在控制台正常看到对象列表。	系统策略

推荐配置方法

IAM系统角色/策略

配置须知

按照本案例配置系统角色或策略后，如果通过控制台或OBS Browser+登录，可能会出现无权限的相关提示信息。

即使界面出现了权限不足的提示，也并不影响已有的权限生效。通过API或SDK可以正常调用相关接口。

对于控制台或客户端工具（OBS Browser+）而言，如果配置了OBS OperateAccess权限，是可以进行对象上传、下载等操作的。

配置步骤

步骤1 使用账号登录华为云，在右上角单击“控制台”。

步骤2 在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”。

步骤3 创建用户组并授权。

按照IAM文档指导，将符合业务场景需求的系统角色或策略添加到用户组中。

步骤4 将需要授权的IAM用户加入到创建的用户组中，授权完成。

说明

由于缓存的存在，授予OBS相关的角色和策略后，大概需要等待10~15分钟权限才能生效。

----结束

4.2.3 对 IAM 用户组授予 OBS 所有资源的指定操作权限

场景介绍

本案例介绍如何为华为云账号下的多个IAM用户或用户群组授予OBS所有资源的指定操作权限。

推荐配置方法

IAM自定义策略

配置须知

按照本案例配置后，可以正常通过API或SDK完成权限所允许的操作，但如果通过控制台或OBS Browser+登录，可能会出现无权限的相关提示信息。

报错原因：通过控制台或者OBS Browser+登录后，加载桶列表时会调用获取桶列表（ListAllMyBuckets）等接口，加载对象列表时会调用列举桶内对象（ListBucket）等接口，其他页面也会调用其他的OBS接口。如果指定的权限中没有包含如obs:bucket:ListAllMyBuckets、obs:bucket:ListBucket及一些控制台和OBS Browser+加载页面时需要调用的接口权限，会提示“拒绝访问，请检查相应权限”，或者“不允许在请求的资源上执行此操作”。

如果希望IAM用户能在控制台或OBS Browser+顺利完成桶和对象相关操作，建议至少在自定义策略中包含obs:bucket:ListAllMyBuckets和obs:bucket:ListBucket两个权限。

配置步骤

步骤1 使用账号登录华为云，在右上角单击“控制台”。

步骤2 在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”。

步骤3 在左侧导航窗格中，单击“权限管理”>“权限”>“创建自定义策略”。

步骤4 配置自定义策略参数。

图 4-11 配置自定义策略

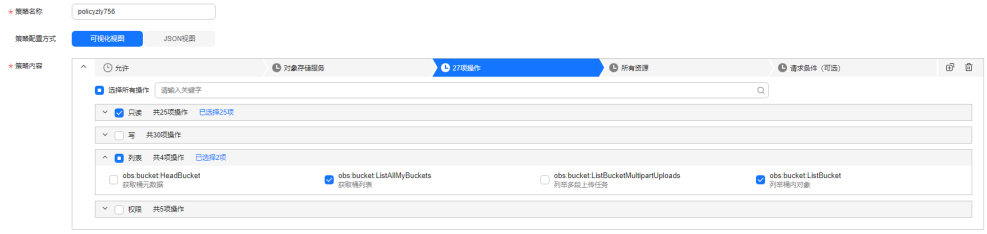


表 4-12 自定义策略参数配置说明

参数	说明
策略名称	输入自定义策略的名称
策略配置方式	根据使用习惯进行选择，此处以“可视化视图”为例
策略内容	• 选择“允许” • 选择“对象存储服务 (OBS)” • 勾选需要授权的操作 OBS支持的操作及对应权限说明请参见**桶相关授权项**和**对象相关授权项** • 选择“所有资源”
作用范围	默认为“全局级服务”

步骤5 单击“确定”，完成自定义策略创建。

步骤6 **创建用户组并授权**。

按照IAM文档指导，将前面步骤创建的自定义策略添加到用户组中。

步骤7 将需要授权的IAM用户**加入到创建的用户组中**，授权完成。

说明

由于缓存的存在，授予OBS相关的策略后，大概需要等待10~15分钟策略才能生效。

----结束

4.2.4 对 IAM 用户组授予 OBS 指定资源的指定操作权限

场景介绍

本案例介绍如何为华为云账号下的多个IAM用户或用户群组授予OBS指定资源的指定操作权限，资源可以具体到某个桶或对象。

推荐配置方法

IAM自定义策略

配置须知

按照本案例配置后，可以正常通过API或SDK完成权限所允许的操作，但如果通过控制台或OBS Browser+登录，可能会出现无权限的相关提示信息。

报错原因：通过控制台或者OBS Browser+登录后，加载桶列表时会调用获取桶列表（ListAllMyBuckets）等接口，加载对象列表时会调用列举桶内对象（ListBucket）等接口，其他页面也会调用其他的OBS接口。如果指定的权限中没有包含如obs:bucket:ListAllMyBuckets、obs:bucket:ListBucket及一些控制台和OBS Browser+加载页面时需要调用的接口权限，会提示“拒绝访问，请检查相应权限”，或者“不允许在请求的资源上执行此操作”。

如果希望IAM用户能在控制台或OBS Browser+顺利完成桶和对象相关操作，建议至少在自定义策略中包含obs:bucket:ListAllMyBuckets和obs:bucket:ListBucket两个权限。

说明

obs:bucket:ListAllMyBuckets面向所有资源，资源选择时要选择所有资源。

obs:bucket:ListBucket只面向授权的桶，资源选择时根据情况选择所有资源或者指定的桶。

配置步骤

步骤1 使用账号登录华为云，在右上角单击“控制台”。

步骤2 在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”。

步骤3 在左侧导航窗格中，单击“权限管理”>“权限”>“创建自定义策略”。

步骤4 配置自定义策略参数。

图 4-12 配置自定义策略

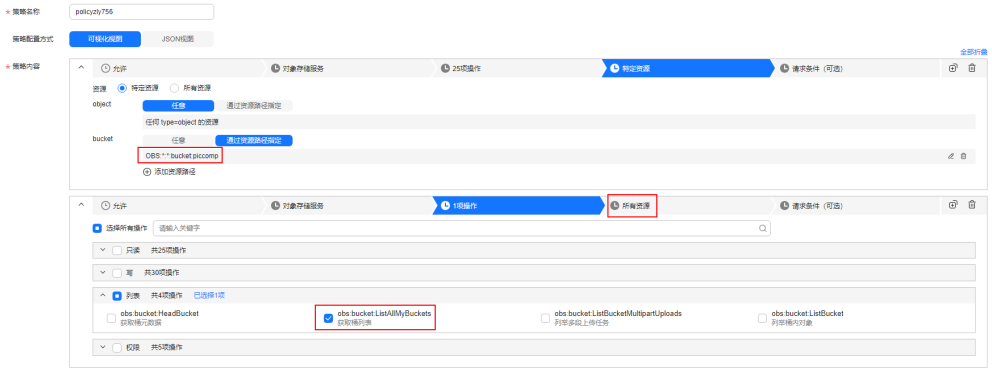


表 4-13 自定义策略参数配置说明

参数	说明
策略名称	输入自定义策略的名称
策略配置方式	根据使用习惯进行选择，此处以“可视化视图”为例

参数	说明
策略内容	【权限1】（被授权用户需要在控制台或OBS Browser+操作时必选） ● 选择“允许” ● 选择“对象存储服务 (OBS)” ● 勾选“列表”操作中的“obs:bucket:ListAllMyBuckets” ● 选择“所有资源” 【权限2】 ● 选择“允许” ● 选择“对象存储服务 (OBS)” ● 勾选需要授权的操作 OBS支持的操作及对应权限说明请参见**桶相关授权项**和**对象相关授权项** ● 选择“特定资源 > bucket”指定桶资源 【格式】 obs:*:*:bucket:*桶名称* 【说明】 对于桶资源，IAM自动生成资源路径前缀**obs:*:*:bucket:** 通过*桶名称*指定具体的资源路径，支持通配符*。例如： **obs:*:*:bucket:***表示任意OBS桶，**obs:*:*:bucket:examplebucket**表示策略作用范围为桶名为examplebucket的桶。 被授权用户需要在控制台或OBS Browser+操作时，需要给指定桶添加obs:bucket:ListBucket权限。 ● 选择“特定资源 > object”指定对象资源 【格式】 指定目录下对象：obs:*:*:object:桶名称/前缀/* 指定对象：obs:*:*:object:*桶名称/对象名称* 【说明】 对于对象资源，IAM自动生成资源路径前缀**obs:*:*:object:** 通过*桶名称/对象名称*指定具体的资源路径，支持通配符*。例如： **obs:*:*:object:my-bucket/my-object/***表示my-bucket桶下my-object目录下的任意对象。 **obs:*:*:object:my-bucket/exampleobject**表示my-bucket桶下exampleobject对象。
作用范围	默认为“全局级服务”

步骤5 单击“确定”，完成自定义策略创建。

步骤6 **创建用户组并授权**。

按照IAM文档指导，将前面步骤创建的自定义策略添加到用户组中。

步骤7 将需要授权的IAM用户**加入到创建的用户组中**，授权完成。

说明

由于缓存的存在，授予OBS相关的策略后，大概需要等待10~15分钟策略才能生效。

----结束

4.2.5 对 IAM 用户组授予 OBS 指定文件夹的指定操作权限

场景介绍

本案例介绍如何为华为云账号下的多个IAM用户或用户群组授予OBS某个桶下指定文件夹的指定操作权限。

推荐配置方法

IAM自定义策略

配置须知

按照本案例配置后，可以正常通过API或SDK完成权限所允许的操作，但如果通过控制台或OBS Browser+登录，可能会出现无权限的相关提示信息。

报错原因：通过控制台或者OBS Browser+登录后，加载桶列表时会调用获取桶列表（ListAllMyBuckets）等接口，加载对象列表时会调用列举桶内对象（ListBucket）等接口，其他页面也会调用其他的OBS接口。如果指定的权限中没有包含如obs:bucket:ListAllMyBuckets、obs:bucket:ListBucket及一些控制台和OBS Browser+加载页面时需要调用的接口权限，会提示“拒绝访问，请检查相应权限”，或者“不允许在请求的资源上执行此操作”。

如果希望IAM用户能在控制台或OBS Browser+顺利完成桶和对象相关操作，建议至少在自定义策略中包含obs:bucket:ListAllMyBuckets和obs:bucket:ListBucket两个权限。（本案例中的权限2和权限3已包含）

说明

obs:bucket:ListAllMyBuckets面向所有资源，资源选择时要选择所有资源。

obs:bucket:ListBucket只面向授权的桶，资源选择时根据情况选择所有资源或者指定的桶。

配置步骤

步骤1 使用账号登录华为云，在右上角单击“控制台”。

步骤2 在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”。

步骤3 在左侧导航窗格中，单击“权限管理”>“权限”>“创建自定义策略”。

步骤4 配置自定义策略参数。

图 4-13 配置自定义策略

表 4-14 自定义策略参数配置说明

参数	说明
策略名称	输入自定义策略的名称
策略配置方式	根据使用习惯进行选择，此处以“可视化视图”为例
策略内容	【权限1】 ● 选择“允许” ● 选择“对象存储服务 (OBS)” ● 勾选“只读”“写”和“权限”中全部Object的相关权限 ● 选择“特定资源 > 通过资源路径指定”指定文件夹 【格式】 obs:*:*:object:*桶名称/文件夹名称/* 【说明】 对于桶资源，IAM自动生成资源路径前缀**obs:*:*:object:** 通过*桶名称/文件夹名称*指定具体的资源路径，支持通配符*。例如： **OBS:*:*:object:example-002/folder-001/***表示**example-002**桶下**folder-001**文件夹下的任意对象。 【权限2】（被授权用户需要在控制台或OBS Browser+操作时必选） ● 选择“允许” ● 选择“对象存储服务 (OBS)” ● 勾选“列表”操作中的“obs:bucket:ListBucket” ● 选择“特定资源 > 通过资源路径指定”指定桶 【格式】 obs:*:*:bucket:*桶名称* ● 选择“添加条件” – 条件键：obs:prefix – 运算符：StringMatch – 值：*文件夹名称/* 【说明】 如果希望用户只有列举桶下某一个文件夹的权限，则需要针对obs:bucket:ListBucket这个动作添加请求条件。prefix为列举桶内对象携带的参数，这样用户在列举桶内对象指定参数prefix以*文件夹名称/*开头的对象时，能够列举桶内的对象。 【权限3】（被授权用户需要在控制台或OBS Browser+操作时必选） ● 选择“允许” ● 选择“对象存储服务 (OBS)” ● 勾选“列表”操作中的“obs:bucket:ListAllMyBuckets” ● 选择“所有资源”

参数	说明
作用范围	默认为“全局级服务”

步骤5 单击“确定”，完成自定义策略创建。

步骤6 **创建用户组并授权**。

按照IAM文档指导，将前面步骤创建的自定义策略添加到用户组中。

步骤7 将需要授权的IAM用户**加入到创建的用户组中**，授权完成。

说明

由于缓存的存在，授予OBS相关的策略后，大概需要等待10~15分钟策略才能生效。

----结束

验证

步骤1 使用IAM用户登录OBS控制台。

步骤2 可以在桶列表中看到所有的桶。选择目标桶example-002，进入目标桶。

图 4-14 查看桶列表

说明

配置完成进入桶后仍然会出现无权限相关提示，属于正常现象，因为控制台还调用了其他高级配置的接口，但此时已可以正常完成文件夹中允许的操作。

步骤3 单击左侧导航栏“对象”。会出现无权限相关提示，且看不到任何对象，属于正常现象。

图 4-15 进入桶 example-002

说明

无权限的原因为在控制台列举对象，是列举根文件夹下的对象，与自定义策略中配置的列举“folder-001/”文件夹下的对象不匹配，符合预期结果。

步骤4 在搜索框输入“folder-001/”，查看folder-001文件夹下的对象列表，可以看到该文件夹下有一个“222.txt”和“111.txt”。

图 4-16 查看文件

步骤5 单击”新建文件夹”，文件夹folder-002可以创建成功。

图 4-17 创建文件夹成功

步骤6 单击“上传对象”，文件333.txt上传成功。

图 4-18 上传对象成功

说明

如果需要配置其他指定的权限完成其他操作，可前往“账号名 > 统一身份认证 > 权限”页面配置的自定义策略中继续配置相关权限即可。

----结束

4.3 对其他账号授权

4.3.1 对其他账号授予桶的读写权限

场景介绍

本案例介绍如何为其他华为云账号授予OBS桶的读写权限。这里的账号指华为云账号本身，不包含账号下的IAM用户，如果要为IAM用户授权，请参见**对其他账号下的IAM用户授予桶和桶内资源的访问权限**。

推荐配置方法

对其他账号授权，推荐使用桶策略。

配置须知

本案例预置的“桶读写”模板允许其他账号对整个桶及桶内所有对象执行除以下权限以外的所有权限：

- DeleteBucket：删除桶
- PutBucketPolicy：设置桶策略
- PutBucketAcl：设置桶ACL

按照本案例配置后，被授权账号可以正常通过API或SDK完成读写操作（上传、下载、删除桶内所有对象），此外允许通过OBS Browser+挂载外部桶的方式完成读写操作。暂不支持在OBS控制台访问非本账号的OBS桶。

通过OBS Browser+访问添加的外部桶可能仍会出现无权限的相关提示信息。

报错原因：OBS Browser+桶详情页面的加载会调用一些其他的OBS接口，而授予的读写权限中并没有包含这些操作的权限，所以会提示“拒绝访问，请检查相应权限”，或者“不允许在请求的资源上执-行此操作”，但并不影响已有权限。

配置步骤

步骤1 在OBS管理控制台左侧导航栏选择“桶列表”。

步骤2 在桶列表单击目标桶的桶名称，进入“对象”页面。

步骤3 在左侧导航栏，单击“访问权限控制>桶策略”，进入桶策略页面。

步骤4 在“桶策略”页面，单击“创建”。

步骤5 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。

步骤6 配置桶策略内容。

图 4-19 配置桶策略

表 4-15 桶策略配置说明

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许
	被授权用户	• 被授权用户：其他账号 **说明** 账号ID和IAM用户ID可在“我的凭证”页面获取。 输入格式：domainId/userId，可授权给多个账号，每行一个。 domainId/*表示授权给账号下的所有用户。
	授权资源	• 资源范围：整个桶（包括桶内对象）
	授权操作	• 动作范围：模板配置 • 模板：桶读写

参数		说明
	高级设置-排除策略（可选）	• 排除以上授权操作（默认勾选）

步骤7 核对权限配置信息，确认无误后单击“创建”，完成桶策略创建。

----结束

4.3.2 对其他账号授予桶的指定操作权限

场景介绍

本案例介绍如何为其他华为云账号授予OBS桶的指定操作权限。这里的账号指华为云账号本身，不包含账号下的IAM用户，如果要为IAM用户授权，请参见**对其他账号下的IAM用户授予桶和桶内资源的访问权限**。

此处以授予设置桶ACL和获取桶ACL的权限为例。如果需要配置其他指定的权限，在桶策略的动作名称中选择对应动作即可。**OBS支持的动作**

推荐配置方法

对其他账号授权，推荐使用桶策略。

配置须知

按照本案例配置后，被授权账号可以正常通过API或SDK完成桶ACL设置和获取操作，此外允许通过OBS Browser+挂载外部桶的方式完成桶ACL设置和获取，但还需要额外配置一条ListBucket的权限才能挂载成功。暂不支持在OBS控制台访问非本账号的OBS桶。

配置步骤

步骤1 在OBS管理控制台左侧导航栏选择“桶列表”。

步骤2 在桶列表单击目标桶的桶名称，进入“对象”页面。

步骤3 在左侧导航栏，单击“访问权限控制>桶策略”，进入桶策略页面。

步骤4 在“桶策略”页面，单击“创建”。

步骤5 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。

步骤6 配置桶策略内容。

图 4-20 配置桶策略

表 4-16 桶策略配置说明

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许
	被授权用户	• 被授权用户：其他账号 **说明** 账号ID和IAM用户ID可在“我的凭证”页面获取。 输入格式：domainId/userId，可授权给多个账号，每行一个。 domainId/*表示授权给账号下的所有用户。
	授权资源	• 资源范围：当前桶

参数		说明
	授权操作	• 动作范围：自定义配置 • 选择动作： – PutBucketAcl（设置桶ACL） – GetBucketAcl（获取桶ACL的相关信息） – ListBucket（可选，列举桶内对象，获取桶元数据） **说明** 1. 选择ListBucket权限，被授权账号可以通过挂载外部桶的方式在OBS Browser+上访问此OBS桶。 2. 如果需要配置其他指定的权限，选择对应动作即可。**OBS支持的动作**

步骤7 核对权限配置信息，确认无误后单击“创建”，完成桶策略创建。

----结束

4.3.3 对其他账号下的 IAM 用户授予桶和桶内资源的访问权限

场景介绍

本案例介绍如何为其他华为云账号下的IAM用户授予OBS桶和桶内资源的访问权限。

此处以授予上传和下载桶内对象的权限为例。如果需要配置其他指定的权限，在桶策略和给IAM用户授权中配置对应的权限即可。

推荐配置方法

对其他账号下的IAM用户授予桶和桶内资源的访问权限，**需要同时配置桶策略和给IAM用户授权**。

例如要允许账号A下的IAM用户A访问账号B的桶B：

1. 首先，需要账号B配置桶策略：允许IAM用户A访问桶B。
2. 然后，需要账号A给其下的IAM用户A授权：允许IAM用户A访问桶B。

配置须知

按照本案例配置后，被授权IAM用户可以正常通过API或SDK进行对象上传下载，此外允许通过OBS Browser+挂载外部桶的方式进行上传下载，但还需要在额外配置一条ListBucket的权限才能挂载成功。暂不支持在OBS控制台访问非本账号的OBS桶。

步骤一：桶拥有者配置桶策略

由桶拥有者或者具有桶策略配置权限的用户配置一条桶策略，允许其他账号下的IAM用户对桶执行指定操作。

本示例中，由账号B（桶B的拥有者）配置一条桶策略，桶策略中允许账号A下的IAM用户A可以向账号B的桶B中上传对象和下载桶B中的对象。

步骤1 在OBS管理控制台左侧导航栏选择“桶列表”。

步骤2 在桶列表单击目标桶的桶名称，进入“对象”页面。

步骤3 在左侧导航栏，单击“访问权限控制>桶策略”，进入桶策略页面。

步骤4 在“桶策略”页面，单击“创建”。

步骤5 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。

步骤6 配置桶策略内容。

图 4-21 配置桶策略

表 4-17 桶策略配置说明

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许

参数		说明
	被授权用户	• 被授权用户：其他账号。 本示例中，此处填写“*账号A的ID/IAM用户A的ID*”。 **说明** 1. 账号ID和IAM用户ID可在“我的凭证”页面获取。 2. 输入格式：domainId/userId，可授权给多个账号，每行一个。 3. domainId/*表示授权给账号下的所有用户。
	授权资源	• 资源范围：当前桶、指定对象 • 指定对象 - 资源路径：输入对象前缀 **说明** 1. 指定对象支持输入多个资源路径，单击“添加资源路径”按钮即可。 2. 您可以指定资源路径为具体对象、对象集或目录，*表示桶内所有对象。 如果指定某个对象：对象名称。 如果指定某个对象集：“对象名称前缀”+“*”、“*”+“对象名后缀”或“*”。
	授权操作	• 动作范围：自定义配置 • 选择动作： – GetObject（获取对象内容，获取对象元数据） – GetObjectVersion（获取指定版本对象内容，获取指定版本对象元数据） – PutObject（PUT上传，POST上传，上传段，初始化上传段任务，合并段） – ListBucket（可选，列举桶内对象，获取桶元数据） **说明** 1. 选择ListBucket权限，被授权账号可以通过挂载外部桶的方式在OBS Browser+上访问此OBS桶。 2. 如果需要配置其他指定的权限，选择对应动作即可。**OBS支持的动作**

步骤7 核对权限配置信息，确认无误后单击“创建”，完成允许上传下载的桶策略创建。

----结束

步骤二：其他账号给其下的 IAM 用户授权

需要由其他账号（非桶拥有者）给其下的IAM用户授权，允许IAM用户对桶执行指定操作（允许的操作要与桶策略中允许的操作相同）。

本示例中，需要由账号A给其下的IAM用户A授权，允许IAM用户A可以向账号B的桶B中上传对象和下载桶B中的对象。

步骤1 使用账号登录华为云，在右上角单击“控制台”。

步骤2 在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”。

步骤3 在左侧导航窗格中，单击“权限管理”>“权限”>“创建自定义策略”。

步骤4 配置自定义策略参数。

图 4-22 配置自定义策略

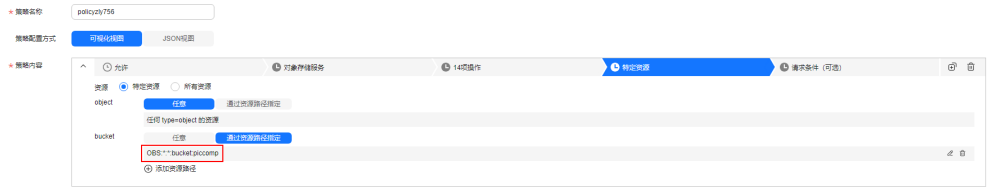


表 4-18 自定义策略参数配置说明

参数	说明
策略名称	输入自定义策略的名称
策略配置方式	根据使用习惯进行选择，此处以“可视化视图”为例
策略内容	• 选择“允许” • 选择“对象存储服务 (OBS)” • 勾选需要授权的操作 – 只读 > obs:bucket:ListBucketVersions和obs:object:GetObjectVersion – 写 > obs:object:PutObject – 列表 > obs:bucket:ListBucket（需要使用OBS Browser+挂载外部桶时勾选此操作） 如果需要配置其他指定的操作权限，勾选对应操作即可，各操作的说明请参见**桶相关授权项**和**对象相关授权项** • 选择“特定资源 > object”指定对象资源，指定的对象或对象集应与桶策略一致 – 如果桶策略设置的资源为“*”，此处选择“任意” – 如果桶策略设置的资源为指定对象或对象集，此处应通过资源路径指定与桶策略相同的对象或对象集 【格式】 obs:*:*:object:*桶名称/对象名称* 本例中桶策略设置“*”，所以此处选择“任意” • 选择“特定资源 > bucket > 通过资源路径指定”指定桶资源 单击“添加资源路径”，在“路径”中填写被授权的桶名称，如example-bucket 资源的完整路径即为：OBS:*:*:bucket:example-bucket
作用范围	默认为“全局级服务”

步骤5 单击“确定”，完成自定义策略创建。

步骤6 **创建用户组并授权**。

按照IAM文档指导，将前面步骤创建的自定义策略添加到用户组中。

步骤7 将需要授权的IAM用户**加入到创建的用户组中**，授权完成。

说明

由于缓存的存在，授予OBS相关的策略后，大概需要等待10~15分钟策略才能生效。

----结束

4.3.4 对其他账号授予指定对象的读权限

场景介绍

本案例介绍如何为其他账号授予OBS桶中某个对象或某类对象的读权限。这里的账号指华为云账号本身，不包含账号下的IAM用户，如果要为IAM用户授权，请参见**对其他账号下的IAM用户授予桶和桶内资源的访问权限**。

推荐配置方法

对其他账号授权，推荐使用桶策略。

配置须知

本案例预置的“对象只读”模板允许其他账号对桶内指定对象执行以下权限：

- GetObject：获取对象内容、获取对象元数据
- GetObjectVersion：获取指定版本对象内容、获取指定版本对象元数据
- GetObjectVersionAcl：获取指定版本对象ACL
- GetObjectAcl：获取对象ACL
- RestoreObject：恢复归档存储对象

按照本案例配置后，可以正常通过API或SDK完成读操作（下载指定对象），但如果通过控制台或OBS Browser+登录，会出现无权限的相关提示信息。

报错原因：通过控制台或者OBS Browser+登录后，加载桶列表时会调用获取桶列表（ListAllMyBuckets）等接口，加载对象列表时会调用列举桶内对象（ListBucket）等接口，其他页面也会调用其他的OBS接口。而授予的只读权限中并没有包含这些操作的权限，所以会提示“拒绝访问，请检查相应权限”，或者“不允许在请求的资源上执行此操作”。

配置步骤

步骤1 在OBS管理控制台左侧导航栏选择“桶列表”。

步骤2 在桶列表单击目标桶的桶名称，进入“对象”页面。

步骤3 在左侧导航栏，单击“访问权限控制>桶策略”，进入桶策略页面。

步骤4 在“桶策略”页面，单击“创建”。

步骤5 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。

步骤6 配置桶策略内容。

图 4-23 配置桶策略

表 4-19 桶策略配置说明

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许
	被授权用户	• 被授权用户：其他账号 **说明** 账号ID和IAM用户ID可在“我的凭证”页面获取。 输入格式：domainId/userId，可授权给多个账号，每行一个。 domainId/*表示授权给账号下的所有用户。

参数		说明
	授权资源	• 资源范围：指定对象 • 资源路径：输入对象前缀 **说明** – 指定对象支持输入多个资源路径，单击“添加资源路径”按钮即可。 – 您可以指定资源路径为具体对象、对象集或目录，*表示桶内所有对象。 如果指定某个对象：对象名称 如果指定某个对象集：“对象名称前缀”+“*”、“*”+“对象名后缀”或“*”
	授权操作	• 动作范围：模板配置 • 模板：对象只读

步骤7 核对权限配置信息，确认无误后单击“创建”，完成桶策略创建。

----结束

4.3.5 对其他账号授予指定对象的指定操作权限

场景介绍

本案例介绍如何为其他账号授予OBS桶中指定对象的指定操作权限，此处以授予下载对象的权限为例。

如果需要配置其他指定的权限，在桶策略的动作名称中选择对应动作即可。**OBS支持的动作**

这里的账号指华为云账号本身，不包含账号下的IAM用户，如果要为IAM用户授权，请参见**对其他账号下的IAM用户授予桶和桶内资源的访问权限**。

推荐配置方法

对其他账号授权，推荐使用桶策略。

配置须知

按照本案例配置后，可以正常通过API或SDK完成对象下载操作，但如果通过控制台或OBS Browser+登录桶列表，会出现无权限的相关提示信息。

报错原因：通过控制台或者OBS Browser+登录后，加载桶列表时会调用获取桶列表（ListAllMyBuckets）等接口，加载对象列表时会调用列举桶内对象（ListBucket）等接口，其他页面也会调用其他的OBS接口。而授予的只读权限中并没有包含这些操作的权限，所以会提示“拒绝访问，请检查相应权限”，或者“不允许在请求的资源上执行此操作”。

配置步骤

步骤1 在OBS管理控制台左侧导航栏选择“桶列表”。

步骤2 在桶列表单击目标桶的桶名称，进入“对象”页面。

步骤3 在左侧导航栏，单击“访问权限控制>桶策略”，进入桶策略页面。

步骤4 在“桶策略”页面，单击“创建”。

步骤5 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。

步骤6 配置桶策略内容。

图 4-24 配置桶策略

表 4-20 桶策略配置说明

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许

参数		说明
	被授权用户	• 被授权用户：其他账号 **说明** 账号ID和IAM用户ID可在“我的凭证”页面获取。 输入格式：domainId/userId，可授权给多个账号，每行一个。 domainId/*表示授权给账号下的所有用户。
	授权资源	• 资源范围：指定对象 • 资源路径：输入对象前缀 **说明** 1. 支持输入多个资源路径，单击“添加资源路径”按钮即可。 2. 您可以指定资源路径为具体对象、对象集或目录，*表示桶内所有对象。 如果指定某个对象：对象名称。 如果指定某个对象集：“对象名称前缀”+“*”、“*”+“对象名后缀”或“*”。
	授权操作	• 动作范围：自定义配置 • 选择动作：GetObject（获取对象内容，获取对象元数据） **说明** 如果需要配置其他指定的权限，选择对应动作即可。**OBS支持的动作**

步骤7 核对权限配置信息，确认无误后单击“创建”，完成桶策略创建。

----结束

4.4 对所有账号授权

4.4.1 对所有账号授予桶的公共读权限

场景介绍

当某个桶需要授权所有账号访问权限时，可以通过桶策略和桶ACL配置授予所有账号访问桶的权限。本示例以桶策略为例。

配置须知

本案例预置的“公共读”模板允许所有账号（所有互联网用户）对整个桶及桶内所有对象执行以下权限：

- HeadBucket：判断桶是否存在、获取桶元数据
- GetBucketLocation：获取桶位置
- GetObject：获取对象内容、获取对象元数据

- RestoreObject：恢复归档存储对象
- GetObjectVersion：获取指定版本对象内容、获取指定版本对象元数据

配置步骤

步骤1 在OBS管理控制台左侧导航栏选择“桶列表”。

步骤2 在桶列表单击目标桶的桶名称，进入“对象”页面。

步骤3 在左侧导航栏，单击“访问权限控制>桶策略”，进入桶策略页面。

步骤4 在“桶策略”页面，单击“创建”。

步骤5 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。

步骤6 配置桶策略内容。

图 4-25 配置桶策略

表 4-21 桶策略配置说明

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许
	被授权用户	• 被授权用户：所有账号
	授权资源	• 资源范围：整个桶（包含桶内对象）
	授权操作	• 动作范围：模板配置 • 模板：公共读

步骤7 核对权限配置信息，确认无误后单击“创建”，完成桶策略创建。

----结束

验证

步骤1 权限设置成功后，在桶“概览”页的“域名信息”找到“访问域名”。将“访问域名”的URL公布到互联网上，互联网所有用户便可以访问该桶。

步骤2 在桶“对象”页的“对象”页签下单击目标对象名称，找到对象链接。将对象链接公布到互联网上，互联网所有用户便可以访问到该对象。

----结束

4.4.2 对所有账号授予指定目录的读权限

场景介绍

当一个文件夹下的对象都需要授权所有账号访问权限时，可以通过桶策略配置授予所有账号访问文件夹内对象的权限。

配置须知

本案例预置的“目录只读”模板允许所有账号（所有互联网用户）对指定目录执行以下权限：

- GetObject：获取对象内容、获取对象元数据
- GetObjectVersion：获取指定版本对象内容、获取指定版本对象元数据
- GetObjectVersionAcl：获取指定版本对象ACL
- GetObjectAcl：获取对象ACL
- RestoreObject：恢复归档存储对象
- HeadBucket：判断桶是否存在、获取桶元数据
- GetBucketLocation：获取桶位置

说明

使用本案例授权会涉及部分桶相关权限（HeadBucket、GetBucketLocation），请谨慎使用。如果需要缩小权限范围，请参考**对所有账号授予指定对象的读权限**。

配置步骤

步骤1 在OBS管理控制台左侧导航栏选择“桶列表”。

步骤2 在桶列表单击目标桶的桶名称，进入“对象”页面。

步骤3 在左侧导航栏，单击“访问权限控制>桶策略”，进入桶策略页面。

步骤4 在“桶策略”页面，单击“创建”。

步骤5 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。

步骤6 配置桶策略内容。

图 4-26 配置桶策略

表 4-22 桶策略配置说明

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许

参数		说明
	被授权用户	● 被授权用户：所有账号
	授权资源	● 资源范围：当前桶、指定对象 ● 指定对象 - 资源路径：配置为文件夹内的所有对象，如文件夹名称为“folder-001”时，资源路径为“folder-001/*”。 **说明** 支持输入多个资源路径，单击“添加资源路径”按钮即可。
	授权操作	● 动作范围：模板配置 ● 模板：目录只读

步骤7 核对权限配置信息，确认无误后单击“创建”，完成桶策略创建。

----结束

验证

权限设置成功后，在文件夹中单击对象名称，页面上“链接”显示该对象的访问地址。将“链接”中对象对应的URL公布到互联网上，互联网所有用户便可以访问或下载该对象。

4.4.3 对所有账号授予指定对象的读权限

场景介绍

某公司A使用OBS存储了大量全球各地的地图数据，这些数据需要对外开放供所有人查阅。在这种情况下，该公司便可以为这部分数据设置所有账号的读取权限，然后将这些数据对应的URL公开在互联网上，所有人就可以使用这个URL访问或下载这些公开数据了。

配置须知

本案例预置的“对象只读”模板允许所有账号（所有互联网用户）对桶内指定对象执行以下权限：

- GetObject：获取对象内容、获取对象元数据
- GetObjectVersion：获取指定版本对象内容、获取指定版本对象元数据
- GetObjectVersionAcl：获取指定版本对象ACL
- GetObjectAcl：获取对象ACL
- RestoreObject：恢复归档存储对象

配置步骤

步骤1 在OBS管理控制台左侧导航栏选择“桶列表”。

步骤2 在桶列表单击目标桶的桶名称，进入“对象”页面。

步骤3 在左侧导航栏，单击“访问权限控制>桶策略”，进入桶策略页面。

步骤4 在“桶策略”页面，单击“创建”。

步骤5 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。

步骤6 配置桶策略内容。

图 4-27 配置桶策略

表 4-23 桶策略配置说明

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许
	被授权用户	• 被授权用户：所有账号

参数		说明
	授权资源	● 资源范围：指定对象 ● 资源路径：输入对象前缀 **说明** 1. 支持输入多个资源路径，单击“添加资源路径”按钮即可。 2. 您可以指定资源路径为具体对象、对象集，*表示桶内所有对象。 如果指定某个对象：对象名称 如果指定某个对象集：“对象名称前缀”+“*”、“*”+“对象名后缀”或“*”
	授权操作	● 动作范围：模板配置 ● 模板：对象只读

步骤7 核对权限配置信息，确认无误后单击“创建”，完成桶策略创建。

----结束

验证

权限设置成功后单击对象名称，页面上“链接”显示该对象的访问地址。将“链接”中对象对应的URL公布到互联网上，互联网所有用户便可以访问或下载该对象。

4.4.4 向所有账号临时分享对象

场景介绍

如果希望将对象限时对外开放供所有人查阅，可以通过对象的分享功能实现。

文件分享方法

步骤1 在OBS管理控制台左侧导航栏选择“对象存储”。

步骤2 在桶列表单击目标桶的桶名称，进入“对象”页面。

步骤3 选中待分享的文件，并单击右侧操作列的“分享”。

此时，链接信息中的链接就已经生效并开始计时，有效期为默认的5分钟。修改URL有效期，链接会相应变化，新链接的有效期从修改时开始计算。

图 4-28 分享文件

步骤4 URL相关操作。

- 单击“打开URL”，将在新页面打开文件进行预览或者直接下载文件到本地。
- 单击“复制链接”，您可以将该链接分享给所有用户，用户可以在浏览器中通过此链接直接访问文件。
- 单击“复制路径”，您可将该路径分享给所有拥有对象所在桶权限的用户，用户可以在对应桶中的文件搜索框中输入该路径搜索并访问文件。

说明

在“URL有效期”内，任何用户都可以访问该文件。

----结束

文件夹分享方法

步骤1 在OBS管理控制台左侧导航栏选择“对象存储”。

步骤2 在桶列表单击目标桶的桶名称，进入“对象”页面。

步骤3 选中待分享的文件夹，并单击右侧的“分享”，系统弹出“分享文件夹”对话框。

步骤4 分享文件夹有两种方式，分别是提取码分享和直接分享。

步骤5 方法一：提取码分享。

图 4-29 提取码分享

1. 分享策略选择“提取码分享”。
2. 设置相关参数。

表 4-24 提取码分享文件夹参数

参数	说明
URL有效期	单位为分钟或小时，URL有效期的取值范围为1分钟到18小时，默认值为5分钟。 在“URL有效期”内，任何用户都可以访问该文件夹。
提取码	六位数字。 用户在访问分享链接时，需要输入提取码，才能看到文件夹中的对象。

3. 单击“创建分享”，生成文件分享URL。
4. 将链接及提取码发送给所有用户，用户通过访问链接并输入提取码以访问文件夹中的对象。
5. 验证：
   a. 其他用户通过网页访问分享的文件夹。
      i. 打开网页，输入分享的URL地址，打开链接。
      ii. 在页面提示框输入“提取码”，确认即可访问分享的文件夹。
   b. 其他用户通过OBS Browser+访问分享的文件夹。
      i. 打开OBS Browser+。
      ii. 在登录页面选择“授权码登录”。
      iii. 输入“授权码”和“提取码”。

iv. 单击“登录”，即可访问分享的文件夹。

步骤6 方法二：直接分享。

图 4-30 直接分享

1. 分享策略选择“直接分享”。
2. 设置相关参数。

表 4-25 直接分享文件夹参数

参数	说明
URL有效期	单位为分钟或小时，URL有效期的取值范围为1分钟到18小时，默认值为5分钟。 在“URL有效期”内，任何用户都可以访问该文件夹。

3. 单击“复制链接”发送给用户，用户通过该链接即可访问文件夹下所有对象。该分享链接由桶域名（前缀）+签名信息（后缀）构成，对该文件夹下所有对象生效。用户可以在分享链接的前缀后面插入对象路径来访问文件夹中的对象，支持访问下载，如图4-31所示。
4. 验证：其他用户通过分享链接访问文件夹下所有对象。
   a. 打开网页，输入分享的链接（前缀+后缀）。
   b. 单击“Enter”键打开链接，列举出文件夹内所有对象。

c. 复制对象路径，然后在前缀后黏贴。

d. 单击“Enter”键打开链接，即可访问下载文件夹中的指定对象。

图 4-31 访问直接分享链接示例图

----结束

4.5 临时授权访问 OBS

场景介绍

本案例介绍如何使用临时访问密钥（临时AK/SK和securitytoken），通过临时授权的方式访问OBS。

假设您希望IAM用户（用户名：APPServer）可以访问桶hi-company的APPClient文件夹，并希望申请到两个不同的临时访问密钥分发给终端APP：APP-1和APP-2，其中APP-1仅能访问APPClient/APP-1下的文件，APP-2仅能访问APPClient/APP-2下的文件。

配置步骤

步骤1 使用账号登录华为云，在右上角单击“控制台”。

步骤2 在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”。

步骤3 创建一个IAM用户：APPServer。创建步骤请参见**创建IAM用户**。

步骤4 创建允许访问桶hi-company中APPClient文件夹的自定义策略。

1. 在左侧导航窗格中，单击“权限管理”>“权限”>“创建自定义策略”。
2. 配置自定义策略参数。

说明

在使用IAM权限之前需明确用户所需要的权限集合，IAM用户只拥有配置的策略所对应的权限。在本案例中APPServer只拥有APPClient文件夹下对象的所有操作权限。

图 4-32 配置自定义策略

表 4-26 自定义策略参数配置说明

参数	说明
策略名称	输入自定义策略的名称
策略配置方式	根据使用习惯进行选择，此处以“JSON视图”为例

策略内容	{
	"Version": "1.1",
	"Statement": [
	{
	"Action": [
	"obs:object:*"
	],
	"Resource": [
	"obs:*:*:object:hi-company/APPClient/*"
	],
	"Effect": "Allow"
	}
	]
	}

作用范围	默认为“全局级服务”

3. 单击“确定”，完成自定义策略创建。

步骤5 **创建用户组并授权**。

按照IAM文档指导，将前面步骤创建的自定义策略添加到用户组中。

步骤6 将需要授权的IAM用户（APPServer）**加入到创建的用户组中**，授权完成。

说明

由于缓存的存在，授予OBS相关的策略后，大概需要等待10~15分钟策略才能生效。

步骤7 IAM用户（APPServer）为终端APP-1和APP-2获取临时访问密钥（临时AK/SK和securitytoken）。

为获取具有不同权限的临时访问密钥，需设置临时策略，设置方式为添加请求体中的policy参数，可参考**获取临时AK/SK和securitytoken**。

下面将给出获取临时访问密钥的请求样例，其中临时策略加粗表示。

为终端APP-1获取临时访问密钥的请求示例如下：

```
{
   "auth": {
   "identity": {
      "policy": {
      "Version": "1.1",
      "Statement": [
         {
         "Action": [
            "obs:object:*"
         ],
         "Resource": [
            "obs:*:*:object:hi-company/APPClient/APP-1/*"
         ],
         "Effect": "Allow"
         }
      ]
      },
      "token": {
      "duration-seconds": 900

      },
      "methods": [
      "token"
      ]
   }
   }
}
```

为终端APP-2获取临时访问密钥的请求示例如下：

```
{
   "auth": {
   "identity": {
      "policy": {
      "Version": "1.1",
      "Statement": [
         {
         "Action": [
            "obs:object:*"
         ],
         "Resource": [
            "obs:*:*:object:hi-company/APPClient/APP-2/*"
         ],
         "Effect": "Allow"
         }
      ]
      },
      "token": {
      "duration-seconds": 900

      },
      "methods": [
      "token"
      ]
   }
   }
}
```

----结束

验证

终端APP-1和APP-2获取对应的临时访问密钥后，可使用OBS API或SDK来访问OBS，APP-1只能访问APPClient/APP-1下的文件，APP-2只能访问APPClient/APP-2下的文件。

4.6 让 IAM 用户只能看到被授权的桶

场景介绍

本章节介绍如何通过企业项目为华为云账号下的某个IAM用户配置指定桶的权限，使其只能在控制台看到授权的桶并且拥有桶的指定权限，无法看到账号下的其他桶，实现桶资源的隔离。

本案例将指定IAM用户test-user只能在控制台看到名为example的桶，并且只拥有上传权限（obs:object:PutObject）、列举桶内权限（obs:bucket:ListBucket）和列举桶权限（obs:bucket:ListAllMyBuckets），通过这些权限test-user用户可以完成上传对象的操作。

推荐配置方法

企业项目

配置须知

- 如果同时在IAM和企业项目中针对某个动作（Action）为某IAM用户进行了授权，授权结果以IAM为准。

  举例：

  1、如果在IAM和企业项目同时配置了列举桶权限（obs:bucket:ListAllMyBuckets），最终结果会列举出所有桶，包括用户所属企业项目之外的桶。

  2、针对上传权限（obs:object:PutObject），如果在IAM中配置Allow，企业项目中配置deny，最终结果为Allow，即允许上传对象。
- 如果在IAM中为某IAM用户配置OBS Viewer权限，并且将其所在用户组加入至企业项目中，则IAM用户登录后将会出现无法列举桶的情况。
- 配置完成进入桶后仍然会出现无权限相关提示，属于正常现象，因为控制台还调用了其他高级配置的接口，但此时已可以正常完成读写模式中允许的操作。

配置步骤

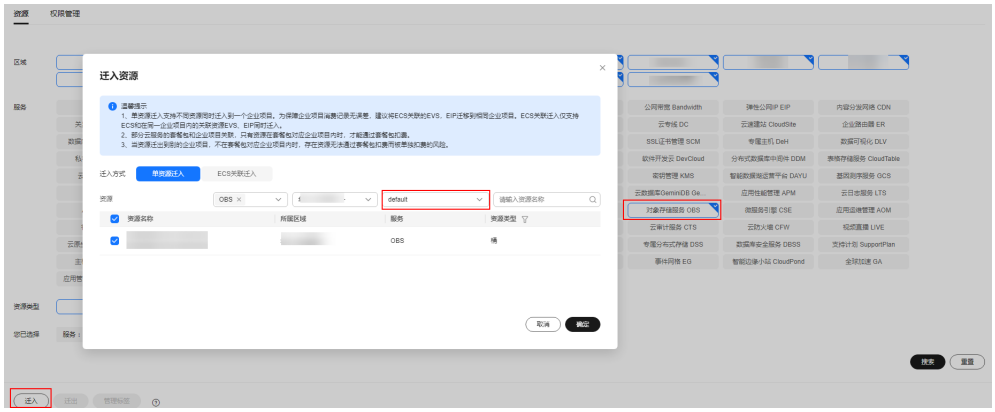
步骤1 登录控制台，单击页面右上方的“企业 > 项目管理”。参考**创建企业项目**，使用授权账号创建一个名为test-project的企业项目。

步骤2 参考**为企业项目迁入资源**，将目标桶example-001迁入**步骤1**中test-project的企业项目中。

说明

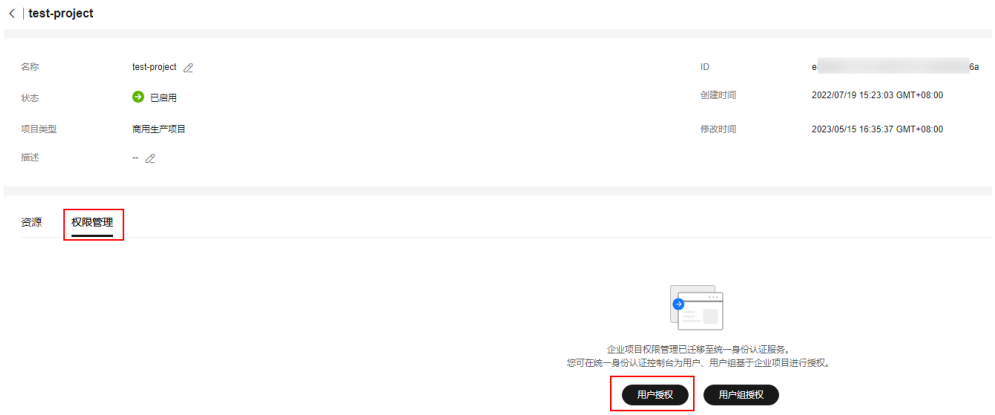
如果需要授权多个桶，则将需要的桶都迁移到企业项目中即可。

图 4-33 将目标桶迁入目标企业项目



步骤3 选择“权限管理 ”。单击“用户授权”。

图 4-34 为企业用户添加授权

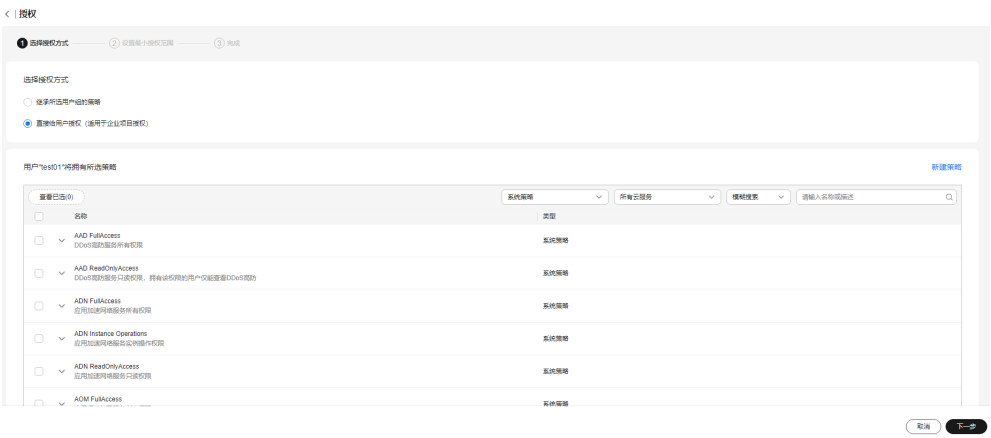


步骤4 进入IAM用户界面，找到目标用户test-user。

图 4-35 找到目标 IAM 用户

步骤5 单击“操作”列下的“授权”，进入授权页面。选择“直接给用户授权（适用于企业项目授权）”。

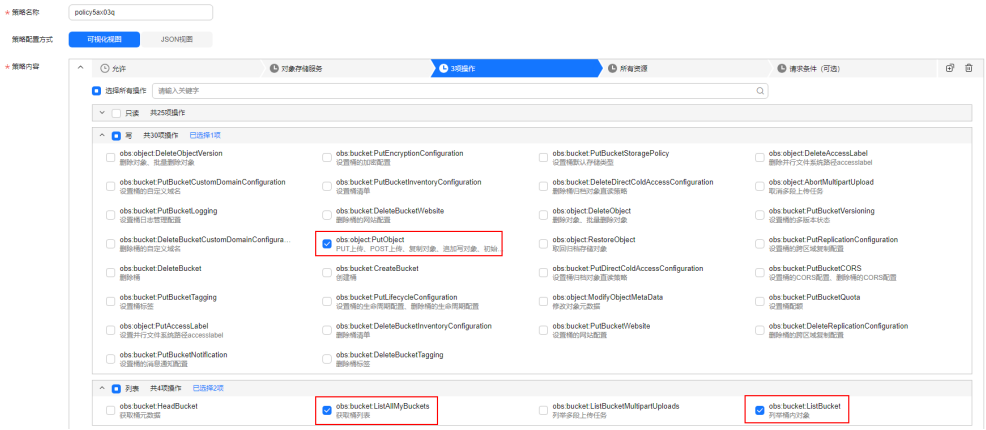
图 4-36 选择直接给用户授权



步骤6 对目标用户test-user设置策略，使该用户在test-project企业项目中拥有策略定义的权限。

1. 选择策略。您可以在所选策略的下拉框中选择“自定义策略”对已有策略进行筛选，也可以通过右侧“新建策略”创建自定义策略。
   - 创建自定义策略的具体操作请参见**创建自定义策略**。本案例配置的自定义权限内容如下图所示，其中包含上传权限（obs:object:PutObject）、列举桶内权限（obs:bucket:ListBucket）和列举桶权限（obs:bucket:ListAllMyBuckets）。
   - OBS系统权限说明请参见**表4-11**。

   图 4-37 配置自定义策略

   说明

   用户所在的用户组在IAM中需未添加此处待添加的策略，否则添加的策略将以IAM中配置的为准。

2. 勾选待添加的策略。

图 4-38 添加自定义策略

步骤7 单击“下一步”。将目标用户test-user（未加入任何用户组）添加至该企业项目中。

图 4-39 将目标用户添加至企业项目中

步骤8 单击“确定”，完成权限配置。添加成功的权限会展示在“权限管理 > 授权管理”的“企业项目视图”列表中。

图 4-40 添加完成

说明

完成企业项目权限配置后，无需再配置IAM自定义策略或系统策略。

----结束

验证

步骤1 使用目标用户test-user登录OBS控制台。

步骤2 可以看到桶列表中只有名为example-001的桶。

图 4-41 验证权限配置结果

步骤3 进入目标桶，单击左侧导航栏“对象”。可以看到桶中的其他对象。

图 4-42 进入桶 example-001

说明

配置完成进入桶后仍然会出现无权限相关提示，属于正常现象，因为控制台还调用了其他高级配置的接口，但此时已可以正常完成读写模式中允许的操作。

步骤4 上传文件111.txt至桶example-001中，可以上传成功。表示权限配置成功。

图 4-43 上传文件

说明

如果需要配置其他指定的权限完成其他操作，如下载对象或删除对象等，可前往“账号名 > 统一身份认证 > 权限”页面配置的自定义策略中继续配置相关权限即可。

----结束

4.7 限制指定的 IP 地址访问桶

场景介绍

本案例介绍如何限制访问OBS桶的源端IP地址，此处以拒绝来源IP为“114.115.1.0/24”网段的客户端访问OBS桶为例。

推荐配置方法

桶策略

配置步骤

步骤1 在OBS管理控制台左侧导航栏选择“桶列表”。

步骤2 在桶列表单击目标桶的桶名称，进入“对象”页面。

步骤3 在左侧导航栏，单击“访问权限控制>桶策略”，进入桶策略页面。

步骤4 在“桶策略”页面，单击“创建”。

步骤5 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。

步骤6 配置桶策略内容。

图 4-44 配置桶策略

表 4-27 桶策略配置说明

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	拒绝
	被授权用户	• 被授权用户：所有账号
	授权资源	• 方式一： – 资源范围：整个桶（包括桶内对象） • 方式二： – 资源范围：当前桶、指定对象 – 指定对象 - 资源路径：*（*表示桶内所有对象）

参数		说明
	授权操作	• 动作范围：自定义配置 • 选择动作：*（表示所有动作）
	（可选）授权条件	• 键：SourceIP • 条件运算符：IpAddress • 值：114.115.1.0/24 **须知** 此IP值仅用于举例，使用时请根据您的实际情况填写IP值。 **说明** – 如果需要同时配置多个IP地址（IP地址段），请以英文逗号隔开。 – 只能用于限制源IP，不能用于区分内外网。

说明

如果希望限制网段外的IP地址的客户端访问桶，需要参考**对所有账号授权**对所有账号授予允许访问的权限。

步骤7 核对权限配置信息，确认无误后单击“创建”，完成桶策略创建。

----结束

验证

使用114.115.1.0/24网段内的IP地址的客户端访问桶，访问被拒绝。使用114.115.1.0/24网段外的IP地址的客户端可以访问桶。

相关场景

- 如果想要实现只允许指定的IP地址访问OBS桶，则将上述示例中桶策略的“条件运算符”设置为“NotIpAddress”，并在“值”中指定允许的IP地址即可。
- 在内网访问OBS的场景下，如果想要限制指定私网IP地址访问桶，需要**购买网关型VPCEP终端节点**（服务类别选择“按名称查找服务”，获取服务名称请**提交工单**，技术人员将为您提供）。通过VPCEP终端节点访问桶，OBS侧感知到的源IP即为私网IP，桶策略可直接针对私网IP进行访问限制。

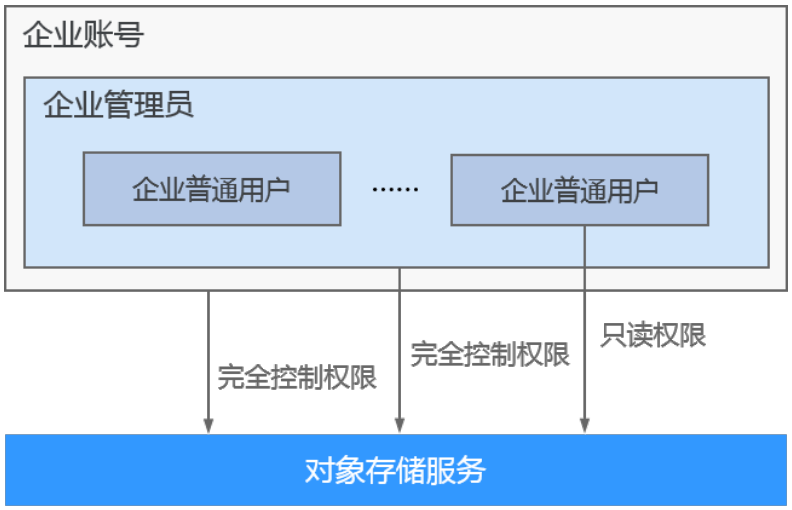
5 企业数据权限控制最佳实践

5.1 部门公共数据权限管理

企业日常有大量工作文件需要存档，但并不希望花费大量的人力、物力在存储资源上。因此该企业开通了OBS，用于存储日常工作文件，并希望为不同职能部门的员工设置不同的访问权限，以此达到不同部门人员访问公司数据的权限隔离。

对于存储在OBS中的部门公共数据，企业希望管理员用户拥有完全控制权限，普通用户仅拥有只读权限，可以在OBS执行基本的数据读取操作，其逻辑关系如图5-1所示。

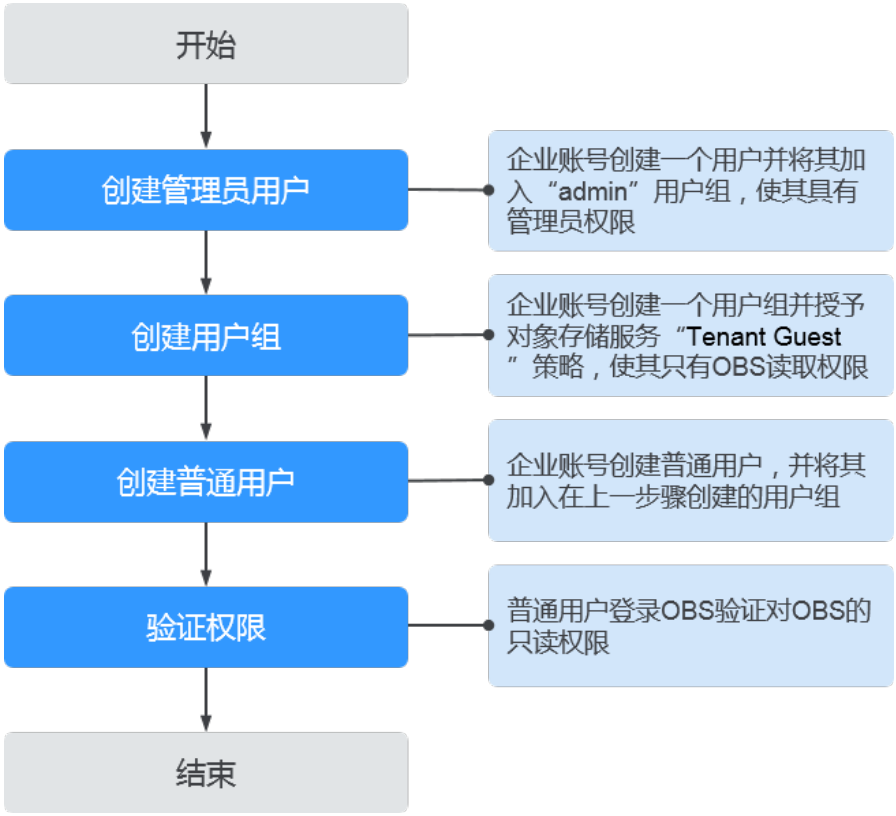
图 5-1 逻辑关系



方案及流程

在此场景下可以通过简单的IAM权限方式进行授权。将普通用户所在用户组权限设置为“Tenant Guest”，即可使普通用户以访客角色访问OBS，对OBS仅拥有只读权限。操作流程如图5-2所示。

图 5-2 部门公共数据权限管理流程



详细配置步骤

步骤1 创建管理员用户

1. 使用企业账号登录华为云控制台首页。
2. 在控制台首页选择“服务列表 > 管理与监管 > 统一身份认证服务（IAM）”，进入IAM控制台。
3. 在IAM控制台，单击左侧导航栏中的“用户”。
4. 单击“创建用户”，在“创建用户”界面，输入“用户名”并配置以下参数：
   - 凭证类型：选择“密码”。
   - 所属用户组：选择“admin”用户组。
5. 单击“下一步”，选择“密码生成方式”为“自定义”。
6. 输入“邮箱”、“手机”、“密码”和“确认密码”。
7. 单击“确定”，完成创建管理员用户。

步骤2 创建具有只读权限的用户组

1. 在IAM控制台，单击左侧导航栏中的“用户组”。
2. 单击“创建用户组”，输入“用户组名称”及“描述”。
3. 单击“确定”。

   返回用户组列表，用户组列表中将显示新创建的用户组。
4. 单击新创建用户组“操作”列的“权限配置”。
5. 单击“授权”。

6. 选择“全局服务”。在“拥有以下权限”的策略列表中，选择“Tenant Guest”策略。
7. 单击“确定”，保存用户组权限。

步骤3 创建普通用户

1. 在IAM控制台，单击左侧导航栏中的“用户”。
2. 单击“创建用户”，在“创建用户”界面，输入“用户名”并配置以下参数：
   - 凭证类型：选择“密码”。
   - 所属用户组：选择**步骤2**创建的用户组。
3. 单击“下一步”，选择“密码生成方式”为“自定义”。
4. 输入“邮箱”、“手机”、密码和“确认密码”。
5. 单击“确定”，完成创建用户。

步骤4 验证用户权限

权限授予成功后，普通用户可以通过OBS控制台、OBS Browser+以及API&SDK等多种方式验证。此处以在OBS控制台上的操作为例，介绍如何验证普通用户对部门公共数据的只读权限。

1. 使用普通用户登录OBS控制台，查看是否有权限访问OBS页面。
   - 如果显示“没有该页面的访问权限”类似提示，表示当前用户无桶内数据的读取权限，请检查用户权限配置是否正确。
   - 如果能显示桶列表，表示当前用户拥有桶列表读取权限，请执行下一步骤。
2. 单击待操作的桶，进入桶对象页面，查看对象列表。
   - 如果无法获取对象列表数据，并显示“拒绝访问，请检查相应权限。”等类似提示，表示当前用户无桶内数据的读取权限，请检查用户权限配置是否正确。
   - 如果能显示对象列表，表示当前用户拥有读取权限，请执行下一步骤。
3. 在“对象”页面，进行上传、删除对象等写删操作。
   - 如果能够进行写删，表示普通用户的只读权限配置失败，请检查用户权限配置是否正确。
   - 如果不能写删对象，表示普通用户的只读权限配置正确。

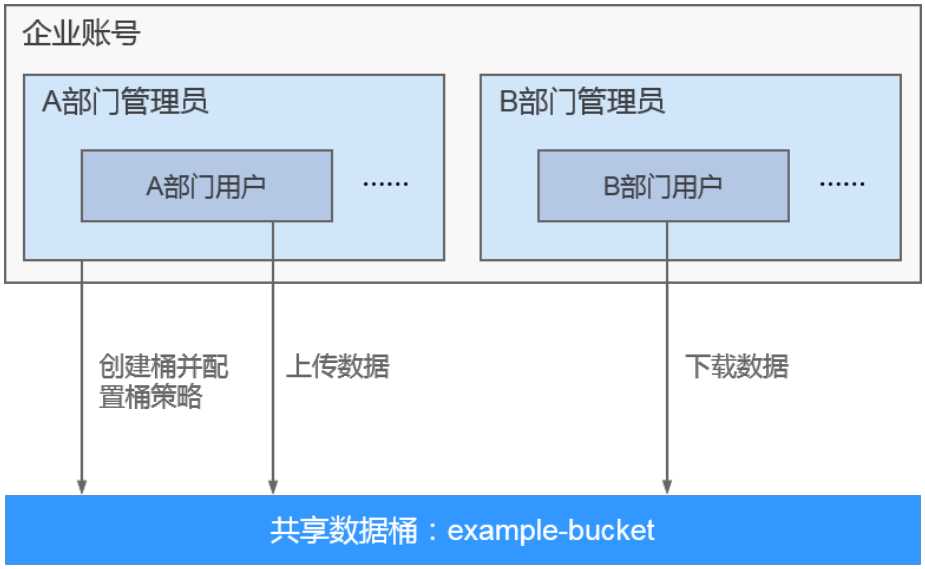
----结束

5.2 部门/项目之间数据共享

企业不同部门/项目之间需要共享的数据，本部门/项目允许其他部门/项目用户下载共享数据，禁止写删，以降低共享数据被误删、篡改的风险。

本文以部门A共享存储在example-bucket桶中的数据给部门B的用户下载为例，介绍如何以最小权限原则对共享数据进行权限控制。在本场景下两个部门的管理员、用户与共享数据桶之间的逻辑关系如**图5-3**所示。

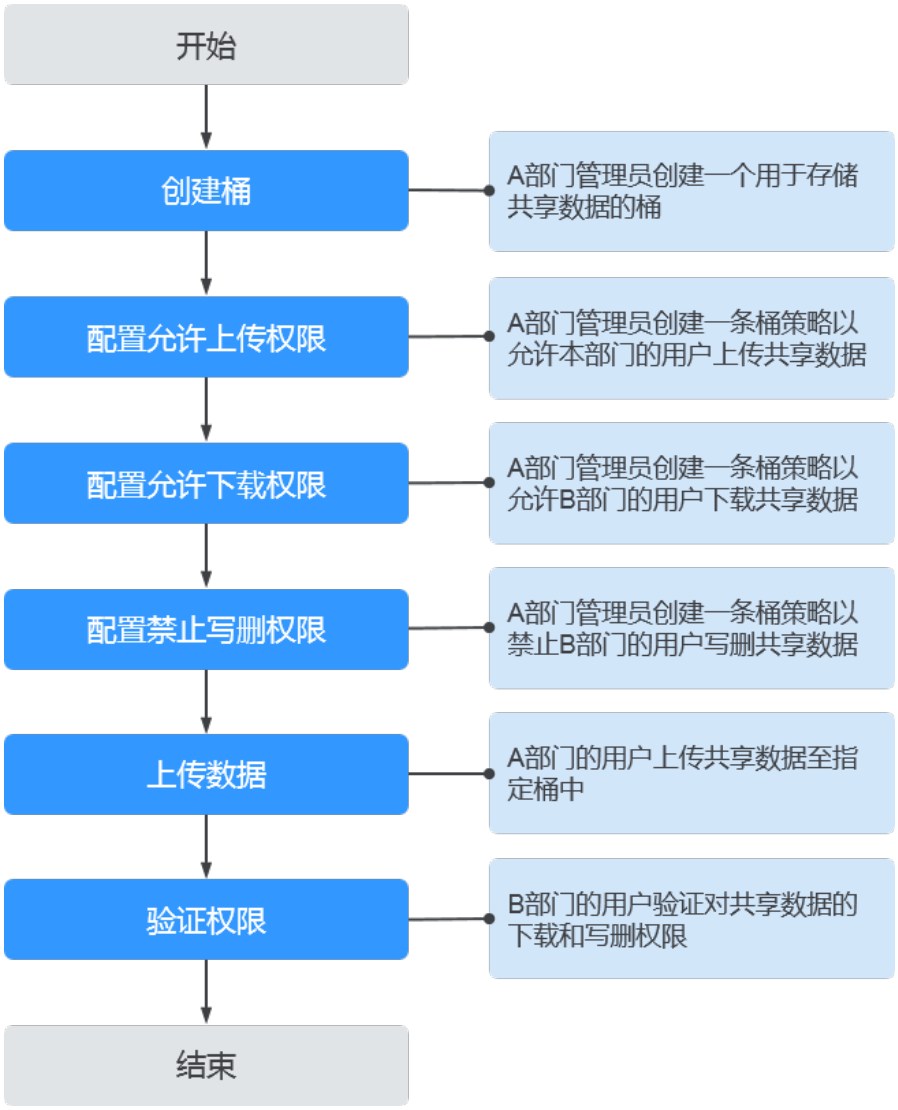
图 5-3 逻辑关系



方案及流程

在此场景下A部门的管理员可以通过桶策略配置允许下载和禁止写删共享数据的权限给B部门的用户，具体配置流程如图5-4所示。

图 5-4 共享数据权限控制流程



前提条件

A部门和B部门的管理员用户以及普通用户已由账号在IAM中创建。如何创建IAM用户请参见**创建IAM用户**。

说明

在创建管理员用户时，A部门的管理员由于要执行创建桶、配置桶策略等操作，因此需要管理员所属用户组至少拥有对象存储服务的“OBS Administrator”策略。

详细配置步骤

步骤1 创建桶

1. 使用部门A的管理员用户登录华为云控制台首页。
2. 在控制台首页选择“所有服务 > 存储 > 对象存储服务 OBS”，进入OBS控制台。
3. 在OBS控制台，单击页面右上角的“创建桶”按钮。

4. 根据页面提示，选择“区域”、“桶名称”、“存储类别”及“桶策略”等，详情请参见**创建桶**。

   说明

   为确保数据安全，“桶策略”建议选择“私有”，其他参数请根据页面提示进行配置。

5. 单击“立即创建”，完成桶创建。

步骤2 配置允许上传权限

如果部门A用户所属用户组的权限中，对象存储服务的策略为“Tenant Administrator”、“OBS Administrator”或“OBS OperateAccess”，请略过此步骤，直接执行**步骤3**。如果没有配置对象存储服务策略或策略配置为“OBS Buckets Viewer”、“Tenant Guest”或“OBS ReadOnlyAccess”，部门A的管理员则需要先执行以下步骤，为本部门的用户配置允许上传共享数据的权限。

1. 在OBS控制台，单击存放共享数据的桶名称，进入桶对象页面。
2. 在左侧导航栏单击“访问权限控制 > 桶策略”。
3. 单击“创建”。
4. 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。
5. 配置如下参数，授予部门A用户访问桶（列举对象）和上传对象的权限。

表 5-1 授予访问桶和上传对象的权限参数配置

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许
	被授权用户	– 被授权用户：当前账号 – 选择子用户：选择允许上传数据的部门A用户
	授权资源	– 方式一： ■ 资源范围：整个桶（包括桶内对象） – 方式二： ■ 资源范围：当前桶、指定对象 ■ 指定对象 - 资源路径：*（*表示桶内所有对象） **说明** 如果只允许上传到桶中的某个或多个文件夹下，桶内对象选择“指定对象”后，资源路径填写可上传的文件夹路径+通配符（例如：example-folder/*），支持配置多个资源路径。
	授权操作	– 动作范围：自定义配置 – 选择动作： ■ ListBucket（列举桶内对象，获取桶元数据） ■ PutObject（可用作于PUT上传，POST上传，上传段，初始化上传段任务，合并段）

6. 单击右下角的“创建”，完成桶策略创建。

步骤3 配置允许下载权限

如果部门B用户所属用户组的权限中，对象存储服务的策略为“Tenant Administrator”、“Tenant Guest”、“OBS Administrator”或“OBS OperateAccess”，请略过此步骤， 直接执行**步骤4**。如果没有配置对象存储服务策略或策略配置为“OBS Buckets Viewer”或“OBS ReadOnlyAccess”，部门A的管理员则需要先执行以下步骤，为部门B的用户配置允许下载共享数据的权限。

1. 在OBS控制台，单击存放共享数据的桶名称，进入桶对象页面。
2. 在左侧导航栏单击“访问权限控制 > 桶策略”。
3. 单击“创建”。
4. 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。
5. 配置如下参数，授予部门B用户下载对象的权限。

表 5-2 授予下载对象的权限参数配置

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许
	被授权用户	– 被授权用户：当前账号 – 选择子用户：选择允许下载数据的部门B用户
	授权资源	– 方式一： ■ 资源范围：整个桶（包括桶内对象） – 方式二： ■ 资源范围：当前桶、指定对象 ■ 指定对象 - 资源路径：*（*表示桶内所有对象） **说明** 如果只让下载桶中某一个文件夹或某一类对象，指定对象 - 资源路径输入待共享的文件夹名称（例如：example-folder/）或带有通配符的对象集（例如：*.doc，表示当前桶中所有以doc结尾的对象）。支持输入多个资源路径。
	授权操作	– 动作范围：自定义配置 – 选择动作： ■ ListBucket（列举桶内对象，获取桶元数据） ■ GetObject（可用作于获取对象内容，获取对象元数据） ■ GetObjectVersion（可用作于获取指定版本对象内容，获取指定版本对象元数据）

6. 单击右下角的“创建”，完成桶策略创建。

步骤4 配置禁止写删权限

1. 在OBS控制台，单击存放共享数据的桶名称，进入桶对象页面。
2. 在左侧导航栏单击“访问权限控制 > 桶策略”。
3. 单击“创建”。
4. 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。
5. 配置如下参数，禁止部门B用户进行写删操作。

表 5-3 禁止写删的权限参数配置

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	拒绝
	被授权用户	– 被授权用户：当前账号 – 选择子用户：选择禁止写删的部门B用户
	授权资源	– 方式一： ■ 资源范围：整个桶（包括桶内对象） – 方式二： ■ 资源范围：当前桶、指定对象 ■ 指定对象 - 资源路径：*（*表示桶内所有对象） **说明** 如果只需要禁止写删桶中某一个文件夹或某一类对象，指定对象 - 资源路径输入待共享的文件夹名称（例如：example-folder/）或带有通配符的对象集（例如：*.doc，表示当前桶中所有以doc结尾的对象）。支持输入多个资源路径。
	授权操作	– 动作范围：自定义配置 – 选择动作： ■ PutObject（可用作于PUT上传，POST上传，上传段，初始化上传段任务，合并段） ■ PutObjectAcl（设置对象ACL） ■ PutObjectVersionAcl（设置指定版本对象ACL） ■ DeleteObject（删除对象） ■ DeleteObjectVersion（删除特定版本的对象） ■ AbortMultipartUpload（取消多段上传任务）

6. 单击右下角的“创建”，完成桶策略创建。

步骤5 上传数据

A部门用户可以通过OBS控制台、OBS Browser+以及API&SDK等上传数据。此处以在OBS控制台上的操作为例，介绍如何上传数据。

1. 使用部门A的用户登录OBS控制台。
2. 在OBS桶列表页面，单击共享数据桶名称。
3. 在左侧导航栏单击“对象 > 上传对象”。
4. 在弹出的“上传对象”窗口，根据页面提示选择“上传方式”、“存储类别”及待上传数据。
5. 单击“上传”。

   上传进度及结果可以单击页面下方的“任务管理”进行查看。

步骤6 验证权限

权限授予成功后，部门B的用户可以通过OBS控制台、OBS Browser+以及API&SDK等多种方式验证。此处以在OBS控制台上的操作为例，介绍如何验证B部门用户对共享数据的只读权限。

1. 使用部门B的IAM用户登录OBS控制台。
2. 在OBS桶列表页面，单击待操作桶的桶名称。
3. 在左侧导航栏单击“对象”，进入对象列表页面。
4. 单击任一公共数据所在行的“下载”。
   - 下载失败，表示下载权限配置失败，请检查用户组权限配置是否正确。
   - 下载成功，表示下载权限配置成功，请执行下一步骤。
5. 单击“上传对象”，选择文件后单击“上传”。
   - 上传成功，表示写删权限配置失败，请检查桶策略配置是否正确。
   - 上传失败，表示写删权限配置成功，执行下一步骤。
6. 单击任一公共数据所在行的“删除”。
   - 删除成功，表示写删权限配置失败，请检查桶策略配置是否正确。
   - 删除失败，表示写删权限配置成功。

----结束

5.3 给业务部门授予独立的资源权限

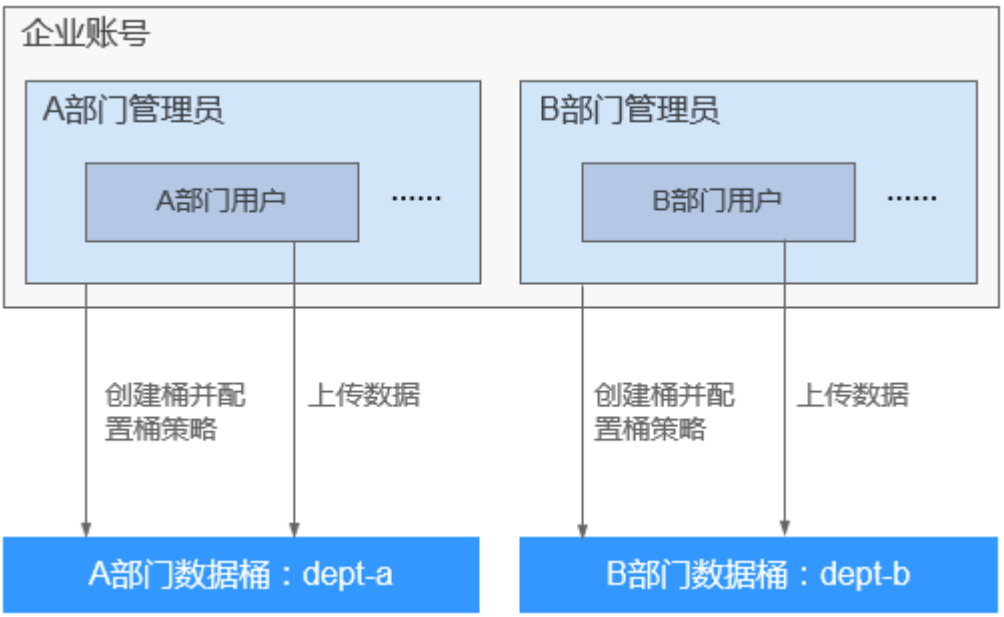
通常一个企业可能会分设多个业务部门，各业务部门之间的数据需要独立管理。在此场景下，可以考虑给各业务部门分配各自所需的IAM用户，通过桶策略给每个业务部门下的IAM用户授予独立的资源权限。

场景假设

假设某企业下有A和B两个不同的业务部门，希望各业务部门的数据存放在自己的桶中，且各业务部门的用户分别拥有本部门桶的上传权限。

在本场景下两个部门的管理员、用户与桶之间的逻辑关系如图5-5所示。

图 5-5 逻辑关系



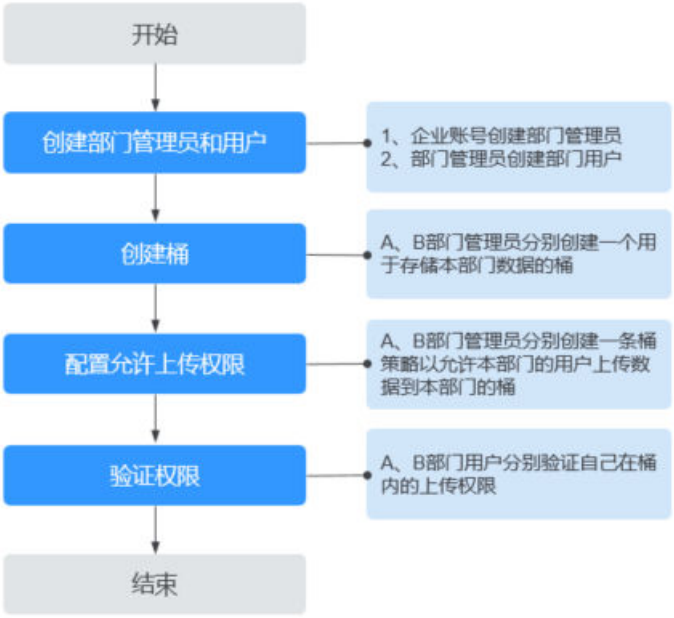
说明

本例中仅为部门用户配置上传权限，您可根据实际业务需求配置其他的权限。关于桶策略的权限说明，请参见**桶策略**。

方案及流程

A、B两部门的管理员可以通过桶策略配置仅自己部门的用户拥有部门桶的上传权限，具体配置流程如**图5-6**所示。

图 5-6 权限控制流程



前提条件

已拥有企业账号。

详细配置步骤

步骤1 创建部门管理员和用户。

部门管理员和用户都属于IAM用户，需要使用企业账号创建，部门用户也可以使用部门管理员创建。本例中需要分别为A、B部门创建一个管理员，并根据各部门的实际用户数创建用户。

由于部门管理员需要执行创建用户、创建桶、配置桶策略等操作，因此需要将部门管理员加入“admin”用户组。而部门用户不需要执行创建用户、创建桶、配置桶策略等操作，需要能够列举账号下的所有桶，因此一般将部门用户加入具有“OBS Buckets Viewer”权限的用户组。有关权限的详细介绍请参见**用户权限**。

1. 创建部门管理员和部门用户对应的IAM用户。如何创建请参见**创建IAM用户**。
2. 将部门管理员加入“admin”用户组，并将部门用户加入具有“OBS Buckets Viewer”权限的用户组。如何加入用户组并授权请参见**给IAM用户授权**。

步骤2 创建桶。

部门A、B的管理员用户分别创建属于自己部门的桶。

1. 分别使用部门A、B的管理员用户登录控制台首页。
2. 在控制台首页选择“服务列表 > 存储 > 对象存储服务 OBS”，进入OBS控制台。
3. 在OBS控制台左侧导航栏选择“对象存储”，单击页面右上角的“创建桶”按钮。
4. 根据页面提示，选择“区域”、“桶名称”、“存储类别”及“桶策略”等，详情请参见**创建桶**。

   说明

   为确保数据安全，“桶策略”建议选择“私有”，其他参数请根据页面提示进行配置。
5. 单击“立即创建”，完成桶创建。

步骤3 配置允许上传权限。

部门A、B的管理员用户分别在自己部门的桶中为本部门用户配置上传权限。

1. 分别使用部门A、B的管理员用户登录控制台首页。
2. 在控制台首页选择“服务列表 > 存储 > 对象存储服务”，进入OBS控制台。
3. 在OBS控制台左侧导航栏选择“对象存储”，在桶列表单击本部门的桶名称，进入桶对象页面。
4. 在左侧导航栏单击“访问权限控制 > 桶策略”。
5. 单击“创建”。
6. 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。
7. 配置如下参数，授予部门内用户访问桶（列举对象）和上传对象的权限。

表 5-4 授予访问桶和上传对象的权限参数配置

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许
	被授权用户	– 被授权用户：当前账号 – 选择子用户：选择部门中允许上传数据的用户
	授权资源	– 方式一： ■ 资源范围：整个桶（包括桶内对象） – 方式二： ■ 资源范围：当前桶、指定对象 ■ 指定对象 - 资源路径：*（*表示桶内所有对象） **说明** 如果只允许上传到桶中的某个或多个文件夹下，桶内对象选择“指定对象”后，资源路径填写可上传的文件夹路径+通配符（例如：example-folder/*），支持配置多个资源路径。
	授权操作	– 动作范围：自定义配置 – 选择动作： ■ ListBucket（列举桶内对象，获取桶元数据） ■ PutObject（可用作于PUT上传，POST上传，上传段，初始化上传段任务，合并段）

8. 单击右下角的“创建”，完成桶策略创建。

步骤4 验证权限。

权限授予成功后，部门A、B的用户可以通过OBS控制台、OBS Browser+以及API&SDK等多种方式验证上传权限。

验证的关键点如下（以A部门用户进行验证为例）：

1. A部门用户在A部门的桶中上传对象成功。
   如果进一步规定了用户仅拥有某个文件夹的上传权限，需同时确保：
   a. 在策略指定的文件夹中上传对象成功。
   b. 在其他文件夹或桶的根目录上传对象失败。
2. A部门用户在B部门的桶中上传对象失败。
3. A部门用户在A部门的桶中下载、删除对象失败。
4. A部门用户在B部门的桶中下载、删除对象失败。

同时满足以上几点要求，说明权限配置成功。

----结束

部门管理员权限控制说明

按照上述方法配置后，所有部门管理员会拥有其他部门桶资源的全部权限。如果要拒绝其他部门管理员访问本部门的桶资源，请按照下述步骤配置桶策略。

步骤1 使用本部门管理员用户登录控制台首页。

步骤2 在控制台首页选择“服务列表 > 存储 > 对象存储服务”，进入OBS控制台。

步骤3 在OBS控制台左侧导航栏选择“对象存储”，在桶列表单击本部门的桶名称，进入桶对象页面。

步骤4 在左侧导航栏单击“访问权限控制 > 桶策略”。

步骤5 单击“创建”。

步骤6 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。

步骤7 配置如下参数，拒绝其他部门管理员访问本部门的桶。

表 5-5 拒绝其他部门管理员访问本部门的桶

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	拒绝
	被授权用户	• 被授权用户：当前账号 • 选择子用户：选择其他部门管理员
	授权资源	• 方式一： – 资源范围：整个桶（包括桶内对象） • 方式二： – 资源范围：当前桶、指定对象 – 指定对象 - 资源路径：*（*表示桶内所有对象）
	授权操作	• 动作范围：自定义配置 • 选择动作：*（表示所有动作）

步骤8 单击右下角的“创建”，完成桶策略创建。

----结束

5.4 业务部门之间桶资源隔离

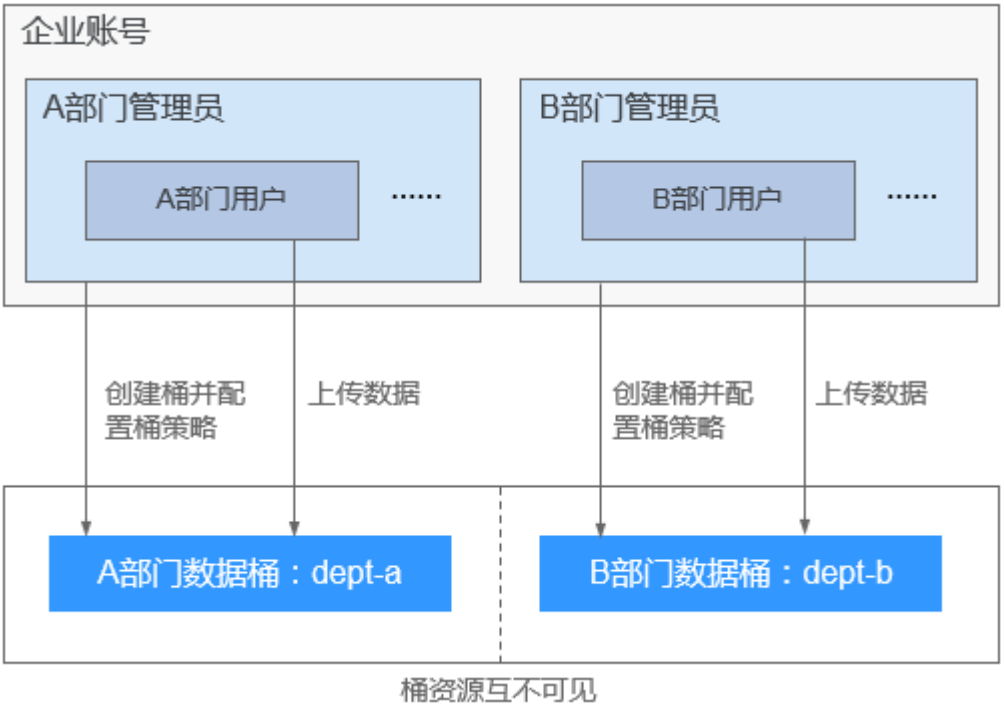
按照**给业务部门授予独立的资源权限**的场景配置，虽然可以实现不同部门用户只能访问本部门的资源，但是每个用户都可以看到企业账号下的所有桶资源，无法做到只能看到自己部门的桶。本节介绍如何通过OBS Browser+添加外部桶的方式实现业务部门之间桶资源隔离。

场景假设

假设某企业下有A和B两个不同的业务部门，希望各业务部门的数据存放在自己的桶中，各业务部门的用户只能看到本部门的桶，且拥有本部门桶的上传权限。

在本场景下两个部门的管理员、用户与桶之间的逻辑关系如图5-7所示。

图 5-7 逻辑关系



说明

本例中仅为部门用户配置上传权限，您可根据实际业务需求配置其他的权限。关于桶策略的权限说明，请参见**桶策略**。

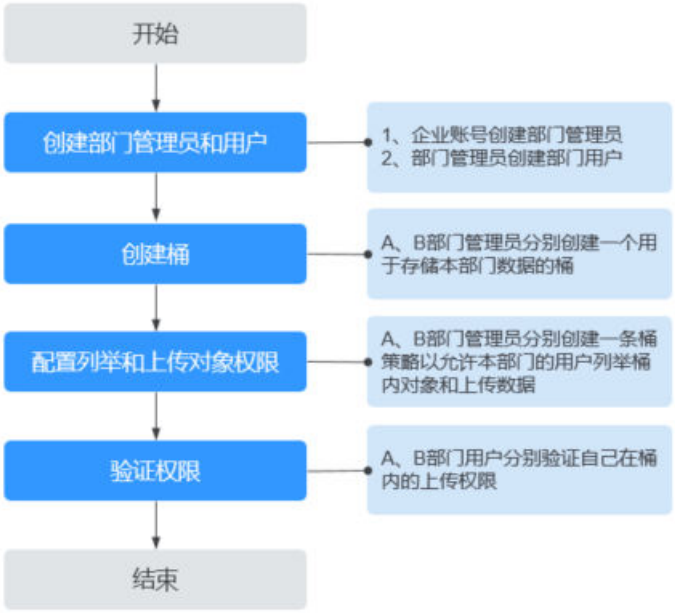
方案及流程

本场景实施方案的关键点为：

1. 部门管理员创建的部门最终用户不要在IAM中授予任何OBS访问权限。
2. 通过桶策略配置仅自己部门的用户拥有部门桶的列举对象和上传对象权限。

具体配置流程如图5-8所示。

图 5-8 权限控制流程



前提条件

已拥有企业账号。

详细配置步骤

步骤1 创建部门管理员和用户。

部门管理员和用户都属于IAM用户，需要使用企业账号创建，部门用户也可以使用部门管理员创建。本例中需要分别为A、B部门创建一个管理员，并根据各部门的实际用户数创建用户。

由于部门管理员需要执行创建用户、创建桶、配置桶策略等操作，因此需要将部门管理员加入“admin”用户组。部门用户在本例中不需要在IAM授予任何OBS访问权限。有关权限的详细介绍请参见**用户权限**。

1. 创建部门管理员和部门用户对应的IAM用户。如何创建请参见**创建IAM用户**。
2. 将部门管理员加入“admin”用户组，部门用户不要加入任何拥有OBS访问权限的用户组。如何加入用户组并授权请参见**给IAM用户授权**。

步骤2 创建桶。

部门A、B的管理员用户分别创建属于自己部门的桶。

1. 分别使用部门A、B的管理员用户登录控制台首页。
2. 在控制台首页选择“服务列表 > 存储 > 对象存储服务”，进入OBS控制台。
3. 在OBS控制台左侧导航栏选择“对象存储”，单击页面右上角的“创建桶”按钮。
4. 根据页面提示，选择“区域”、“桶名称”、“存储类别”及“桶策略”等，详情请参见**创建桶**。

说明

为确保数据安全，“桶策略”建议选择“私有”，其他参数请根据页面提示进行配置。

5. 单击“立即创建”，完成桶创建。

步骤3 配置列举桶内对象和上传对象的权限。

部门A、B的管理员用户分别在自己部门的桶中为本部门用户配置权限。

1. 分别使用部门A、B的管理员用户登录控制台首页。
2. 在控制台首页选择“服务列表 > 存储 > 对象存储服务”，进入OBS控制台。
3. 在OBS控制台左侧导航栏选择“对象存储”，在桶列表单击本部门的桶名称，进入桶对象页面。
4. 在左侧导航栏单击“访问权限控制 > 桶策略”。
5. 单击“创建”。
6. 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。
7. 配置如下参数，授予列举桶内对象和上传对象的权限。

表 5-6 授予列举桶内对象和上传对象的权限参数配置

参数		说明
策略名称		输入自定义策略的名称
策略内容	效力	允许
	被授权用户	– 被授权用户：当前账号 – 选择子用户：选择部门中允许看到该桶并上传对象的用户
	授权资源	– 方式一： ■ 资源范围：整个桶（包括桶内对象） – 方式二： ■ 资源范围：当前桶、指定对象 ■ 指定对象 - 资源路径：*（*表示桶内所有对象） **说明** 如果只允许上传到桶中的某个或多个文件夹下，桶内对象选择“指定对象”后，资源路径填写可上传的文件夹路径+通配符（例如：example-folder/*），支持配置多个资源路径。
	授权操作	– 动作范围：自定义配置 – 选择动作： ■ ListBucket（列举桶内对象，获取桶元数据） ■ PutObject（可用作于PUT上传，POST上传，上传段，初始化上传段任务，合并段）

8. 单击右下角的“创建”，完成桶策略创建。

步骤4 验证权限。

权限授予成功后，部门A、B的用户可以通过OBS Browser+验证权限。

说明

由于部门A、B的用户都只有某个指定桶的访问权限，所以使用这些用户登录OBS控制台会提示没有访问权限，属于正常现象。

需要使用OBS Browser+，通过挂载外部桶的方式将本部门的桶挂载到OBS Browser+中，进行权限验证以及后续的上传操作。

在OBS Browser+中验证权限的方法：

1. 下载OBS Browser+。
2. 使用部门用户以账号方式登录OBS Browser+。

   说明

   受上述权限配置的影响，使用部门用户登录OBS Browser+后提示访问受限属于正常现象。
3. 在左侧菜单栏，单击“外部桶”。
4. 单击“挂载”，在弹出的“挂载外部桶”对话框中，输入已授权的部门桶名称。

   图 5-9 挂载外部桶

5. 单击“确定”，挂载成功后会在桶列表中展示。
6. 在挂载成功的桶中上传文件，验证上传权限。

验证的关键点如下（以A部门用户进行验证为例）：

1. A部门用户第一次登录OBS Browser+提示访问受限，无法看到任何桶。
2. A部门用户挂载A部门桶成功。
3. A部门用户挂载B部门桶失败。
4. A部门用户在A部门的桶中上传对象成功。

   如果进一步规定了用户仅拥有某个文件夹的上传权限，需同时确保：

   a. 在策略指定的文件夹中上传对象成功。
   b. 在其他文件夹或桶的根目录上传对象失败。
5. A部门用户在A部门的桶中下载、删除对象失败。

同时满足以上几点要求，说明权限配置成功。

----结束

6 常见问题

A 附录

A.1 桶策略参数说明

一个Policy由JSON描述，格式定义为：

```
{
"Statement" : [{
    statement1
 },
 {
    statement2
 },
 ......
 ]
}
```

实例如下所示:

```
{
"Statement" : [{
    "Sid": "ExampleStatementID1",
    "Principal": "*",
    "Effect": "Allow",
    "Action": ["ListBucket"],
    "Resource": "examplebucket",
    "Condition": "some conditions"
 },
 {
    "Sid": "ExampleStatementID2",
    "Principal": "*",
    "Effect": "Allow",
    "Action": ["PutObject"],
    "Resource": "examplebucket",
    "Condition": "some conditions"
 },
......
]
}
```

Policy由多条statement组成，也可以是一条。每条statement的结构包括下表内容：

表 A-1 statement 结构

元素	描述	是否必选
Sid	statement Id，可选关键字，描述statement的字符串。	可选
Principal	可选关键字，被授权人，指定本条statement权限针对的Domain以及User，支持通配符“*”，表示所有用户。当对Domain下所有用户授权时，Principal格式为domain/domainid:user/*。当对某个User进行授权时，Principal格式为domain/domainid:user/userId或者domain/domainid:user/userName。 如果通过控制台进行桶清单配置，控制台会自动生成目标桶的桶策略。目标桶的桶策略中Principal取值则固定为{"Service": "obs"}。关于桶清单的详细介绍请参见**桶清单说明**。	可选，Principal与NotPrincipal选其一
NotPrincipal	可选关键字，不被授权人，statement匹配除此之外的其他人。取值同Principal。	可选，NotPrincipal与Principal选其一
Action	可选关键字，指定本条statement作用的操作，Action字段为OBS支持的所有操作集合，以字符串形式表示，不区分大小写。支持通配符“*”，表示该资源能进行的所有操作。例如：“Action":["List*", "Get*"]。	可选，Action与NotAction选其一
NotAction	可选关键字，指定一组操作，statement匹配除该组操作之外的其他操作。 取值同Action。	可选，NotAction与Action选其一
Effect	必选关键字，效力，指定本条statement的权限是允许还是拒绝，Effect的值必须为Allow或者Deny。	必选
Resource	可选关键字，指定statement起作用的一组资源，支持通配符“*”，表示所有资源。	可选，Resource与NotResource选其一
NotResource	可选关键字，指定一组资源，statement匹配除该组资源之外的其他资源。 取值同Resource。	可选，NotResource与Resource选其一
Condition	可选关键字，本条statement生效的条件。	可选

说明

在单条statement中，Action与NotAction必须二选一，Resource与NotResource必须二选一，Principal与NotPrincipal必须二选一。

Principal / NotPrincipal

OBS支持的Principal或NotPrincipal有所有账号、特定租户、特定用户、联合身份用户，委托用户。

- 所有人（所有账号）

  ```
  "Principal": {"ID": "*"}
  ```

  在示例中，使用星号 (*) 作为Everyone/Anonymous的占位符。我们还强烈建议您不要在角色的信任策略中的Principal元素里使用通配符，除非您在该策略中通过Condition元素对访问进行了限制。

- 特定租户

  当在策略中使用租户标识符作为授权人时，可将策略语句中的权限授给该租户中包含的所有身份。这包括该租户下所有用户。以下示例演示了将租户指定为授权人的不同方法。

  ```
  "Principal": { "ID": " domain/domainIdxxxx:user/*" }
  ```

  您可以授权给多个租户，如以下示例所示：

  ```
  "Principal": {
    "ID": [
      "domain/domainIDxx1:user/useridxxxx",
      "domain/domainIDxx2:user/*"
    ]
  }
  ```

- 特定用户

  在 Principal 元素中，用户名区分大小写。

  ```
  "Principal": {"ID": "domain/domainIDxxx:user/user-name" }
  "Principal": {
    "ID": [
      "domain/domainIDxxx:user/UserID1",
      "domain/domainIDxxx:user/UserID2"
    ]
  }
  ```

- 联合身份用户（使用SAML身份提供商）

  ```
  "Principal": { "Federated": "domain/domainIDxxx:identity-provider/provider-name" }
  "Principal": { "Federated": "domain/domainIDxxx:group/groupname" }
  ```

- 委托用户

  *表示对应租户下的所有委托

  ```
  "Principal": { "ID": "domain/domainIDxxx:agency/agencyname" }
  "Principal": { "ID": "domain/domainIDxxx:agency/*" }
  ```

如果通过控制台进行桶清单配置，控制台会自动生成目标桶的桶策略。目标桶的桶策略中Principal为：

```
"Principal":{"Service": "obs"}
```

关于桶清单的详细介绍请参见**桶清单说明**。

OBS控制台支持的被授权用户指桶策略作用的用户，这里的用户可以是账号，也可以是IAM用户。被授权用户可以通过排除策略来指定：

（可选项）排除以上被授权用户：桶策略对除指定用户外的其他用户生效。

说明

- 不勾选：表示桶策略对指定的用户生效。
- 勾选：表示桶策略对除指定用户外的其他用户生效。

指定当前账号的子用户

当桶策略的“被授权用户”选择“子用户”时，可以选择配置当前账号下的子用户（即IAM用户），即为当前账号的IAM用户授权桶策略（可多选）。

指定其他账号

当桶策略的“被授权用户”类型设置“其他账号”时，可以设置一个或多个其他账号。如果只想为其他账号下的IAM用户授权，则需再配置IAM用户ID，可以指定多个IAM用户。

说明

账号ID和IAM用户ID需要由被授权用户使用IAM用户登录至控制台，前往“我的凭证”页面获取。

指定委托账号

当桶策略的“被授权用户”类型设置“委托账号”时，可以设置一个或多个委托账号。创建成功后可以将账号中的资源操作权限委托给其他账号，被委托的账号可以根据权限代替您进行资源运维工作。

说明

当勾选“其他账号”后才可添加委托账号。

指定任何人（所有账号）

要将桶访问权限授予给任何人，桶策略的“被授权用户”类型设置“所有账号”。

须知

为所有账号设置桶访问权限需谨慎使用。如果您授予所有账号桶访问权限，则意味着世界上任何人都可以访问您的桶。在一定要使用的情况下，我们建议您在条件中对访问请求进行限制，比如限制只能某一个IP地址的用户可以访问。

Action / NotAction

桶策略动作与资源相关，当资源为当前整个桶时，桶策略动作需配置为桶相关的动作；当资源为桶内对象时，桶策略动作需配置为对象相关的动作。

桶策略动作可以通过排除策略来指定：

（可选项）排除以上授权操作：桶策略对除指定动作外的其他动作生效。

说明

- 不勾选：表示桶策略对指定的动作生效。
- 勾选：表示桶策略对除指定动作外的其他动作生效。
- 对于桶策略模板，“桶读写”模板默认勾选，其他模板默认不勾选。桶策略模板中的动作排除策略不支持修改。

与桶相关的动作

表 A-2 桶相关动作含义

类型	值	描述
通用（General）	*	通配符，表示该资源能进行的所有操作。
	Get*	表示该资源能进行的所有的获取操作。
	Put*	表示该资源能进行的所有的设置操作。
	List*	表示该资源能进行的所有的列举操作。
桶（Bucket）	HeadBucket	判断桶是否存在，获取桶元数据。
	CreateBucket	创建桶。
	DeleteBucket	删除桶。
	ListBucket	列举桶内对象，获取桶元数据。
	ListBucketVersions	列举桶内多版本对象。
	ListBucketMultipartUploads	列举多段上传任务。
	GetBucketAcl	获取桶ACL的相关信息。
	PutBucketAcl	设置桶ACL。
	GetBucketCORS	获取桶CORS配置的相关信息。
	PutBucketCORS	设置桶CORS。
	GetBucketVersioning	获取桶多版本的相关信息。
	PutBucketVersioning	设置多版本。
	GetBucketLocation	获取桶位置。
	GetBucketLogging	获取桶日志记录的相关信息。
	PutBucketLogging	设置桶日志记录。
	GetBucketWebsite	获取桶的静态网站配置的相关信息。
	PutBucketWebsite	设置桶的静态网站托管。
	DeleteBucketWebsite	删除桶的静态网站托管配置。
	GetLifecycleConfiguration	获取桶生命周期规则。
	PutLifecycleConfiguration	设置桶生命周期规则。
	GetBucketInventoryConfiguration	获取桶清单配置。
	PutBucketInventoryConfiguration	设置桶清单配置。

类型	值	描述
	DeleteBucketInventoryConfiguration	删除桶清单配置。
	PutBucketPolicy	设置桶策略。 **说明** 风险操作，请谨慎授权。 拥有此权限的用户可以任意更改桶策略，并可以通过此权限获取其他权限，包括删除桶策略等。
	GetBucketPolicy	获取桶策略。
	DeleteBucketPolicy	删除桶策略。
	PutBucketStoragePolicy	设置桶默认存储类别。
	GetBucketStoragePolicy	获取桶默认存储类别。
	PutReplicationConfiguration	设置桶跨区域复制配置。
	GetReplicationConfiguration	获取桶跨区域复制配置。
	DeleteReplicationConfiguration	删除桶跨区域复制配置。
	PutBucketTagging	设置桶标签。
	GetBucketTagging	获取桶标签。
	DeleteBucketTagging	删除桶标签。
	PutBucketQuota	设置桶配额。
	GetBucketQuota	获取桶配额。
	PutBucketCustomDomainConfiguration	设置桶自定义域名。
	GetBucketCustomDomainConfiguration	获取桶自定义域名。
	DeleteBucketCustomDomainConfiguration	删除桶自定义域名。
	PutDirectColdAccessConfiguration	设置桶归档数据直读配置。
	GetDirectColdAccessConfiguration	获取桶归档数据直读配置。
	DeleteDirectColdAccessConfiguration	删除桶归档数据直读配置。

类型	值	描述
	GetEncryptionConfiguration	获取桶默认加密配置。
	PutEncryptionConfiguration	设置桶默认加密。
	PutBucketObjectLockConfiguration	配置桶级默认保留策略。
	GetBucketObjectLockConfiguration	获取桶级默认保留策略。

与对象相关的动作

表 A-3 对象相关动作含义

类型	值	描述
通用（General）	*	通配符，表示该资源能进行的所有操作。
	Get*	表示该资源能进行的所有的获取操作。
	Put*	表示该资源能进行的所有的设置操作。
	List*	表示该资源能进行的所有的列举操作。
对象（Object）	GetObject	可用作于获取对象内容，获取对象元数据。可作用于GET Object, HEAD Object。
	GetObjectVersion	可用作于获取指定版本对象内容，获取指定版本对象元数据。
	PutObject	可用作于PUT上传，POST上传，上传段，初始化上传段任务，合并段。可作用于PUT Object, POST Object, Initiate Multipart Upload,Upload Part, Complete Multipart Upload。
	GetObjectAcl	获取对象ACL的相关信息。
	GetObjectVersionAcl	获取指定版本对象ACL。
	PutObjectAcl	设置对象ACL。
	PutObjectVersionAcl	设置指定版本对象ACL。
	DeleteObject	删除对象。
	DeleteObjectVersion	删除对象（针对特定版本的对象）。
	ListMultipartUploadParts	列举已上传段。
	AbortMultipartUpload	取消多段上传任务。

类型	值	描述
	ModifyObjectMetadata	修改对象元数据。
	RestoreObject	恢复归档存储对象。
	PutObjectRetention	配置对象保留策略。
	PutObjectTagging	设置对象标签。
	GetObjectTagging	获取对象标签。
	DeleteObjectTagging	删除对象标签。

Resource / NotResource

OBS支持的Resource表示在相应的资源上操作：

- bucketname（桶操作）：在上面Action中有“支持的桶Action”列表，如果要对桶执行列表中的操作，则Resource中只填写桶名。
- bucketname/objectname（对象操作）：在上面Action中有“支持的对象Action”列表，如果要对桶中对象执行相应的操作，则Resource需要填写“bucketname/objectname”。objectname支持通配符，比如对桶下directory目录对象有权限，则Resource填写为“bucketname/directory/*”；如果对桶下所有对象都有权限，则Resource填写为“bucketname/*”；如果同时需要对桶和桶下对象都有权限，则Resource填写为["examplebucket/*","examplebucket"]。

以下示例策略向租户b4bf1b36d9ca43d984fbcb9491b6fce9（域ID）下的用户ID为71f3901173514e6988115ea2c26d1999的user1用户授予examplebucket的所有操作权限（包含桶操作与对象操作）。

```
{
   "Statement":[
   {
     "Sid":"test",
     "Effect":"Allow",
     "Principal": {"ID": ["domain/b4bf1b36d9ca43d984fbcb9491b6fce9:user/
71f3901173514e6988115ea2c26d1999"]},
     "Action":["*"],
     "Resource":["examplebucket/*","examplebucket"]
   }
  ]
}
```

OBS控制台在指定资源时，资源可以是整个桶（包含桶内对象）、当前整个桶，也可以是指定对象。

授权资源可以通过排除策略来指定：

（可选项）排除以上授权资源：桶策略对除指定资源外的其他资源生效。

说明

- 不勾选：表示桶策略对指定的OBS资源生效。
- 勾选：表示桶策略对除设置外的其他OBS资源生效。

指定资源为整个桶（包含桶内对象）

指定资源为整个桶（包含桶内对象）时，桶策略动作需配置为桶和对象相关的动作，配置方法为“资源范围”选择“整个桶（包含桶内对象）”。

指定资源为桶

指定资源为当前整个桶时，桶策略动作需配置为桶相关的动作，配置方法为“资源范围”选择“当前桶”。

指定资源为对象

指定资源为桶内对象时，桶策略动作需配置为对象相关的动作，配置方法为“资源范围”选择“指定对象”，配置格式如下：

- 对象：直接输入对象名称（包括文件夹名称）。例如，指定的资源是桶中imgs-folder文件夹下的example.jpg文件，则在资源输入框中输入以下内容。

  imgs-folder/example.jpg
- 对象集：当指定给对象集时，使用通配符“*”。通配符“*”表示0个或多个字符的任意组合。其输入格式为：
  - 仅使用一个通配符“*”，表示桶中所有对象。
  - 使用*“对象名称前缀”*+“*”，表示桶中所有以此前缀开头的对象。示例：

    imgs*
  - 使用“*”+“对象名后缀”，表示桶中所有以此后缀结尾的对象。示例：

    *.jpg

Condition

除了指定效力、被授权用户、资源、动作外，桶策略还可以指定生效条件。只有当条件设置的表达式与访问请求中的值匹配时，桶策略才生效。条件是可选参数，用户可以根据业务需要选择是否使用。

例如，账号A拥有example桶，账号B会向账号A的example桶中上传对象，账号A想要拥有账号B向example桶中上传对象的完全控制权限（因为默认情况下对象由上传该对象的账号B拥有），则可以指定上传请求中必须包含x-obs-acl键，以及显式授予完全控制权限，完整的条件表达式如下：

条件运算符	键	值
StringEquals	x-obs-acl	bucket-owner-full-control

条件由条件运算符、条件键、条件值三部分组成，最终组成一个条件表达式，决定桶策略生效的条件。同一个条件运算符中，如果存在多个相同的键，则只会保留最后一个键。条件运算符、键两者之间存在互相限制的关联关系，例如：条件运算符选择了一个String类型的，比如StringEquals，键就只能选择String类型的，比如UserAgent。键选择了一个Date类型，比如CurrentTime，条件运算符就只能选择Date类型的，比如DateEquals。

- **条件运算符**

  运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，策略才能生效。Statement中可选的条件运算符参见**表A-4**，String型运算符如未增加说明，不区分大小写。

表 A-4 各条件运算符含义

类型	关键字	说明
String	StringEquals	字符串匹配，简化为：streq
	StringNotEquals	字符串不匹配，简化为：strneq
	StringEqualsIgnoreCase	忽略大小写的字符串匹配，简化为：streqi
	StringNotEqualsIgnoreCase	忽略大小写的字符串不匹配，简化为：strneqi
	StringLike	宽松的区分大小写的匹配。这些值可以在字符串中的任何地方包括一个多字符匹配的通配符(*)和单字符匹配通配符(?)。简化为：strl
	StringNotLike	非宽松区分大小写的匹配。这些值可以在字符串中的任何地方包括一个多字符匹配的通配符(*)和单字符匹配通配符(?)。简化为：strnl
Numeric	NumericEquals	相等，简化为：numeq Numeric表示数值类型
	NumericNotEquals	不相等，简化为：numneq
	NumericLessThan	小于，简化为：numlt
	NumericLessThanEquals	小于等于，简化为：numlteq
	NumericGreaterThan	大于，简化为：numgt
	NumericGreaterThanEquals	大于等于，简化为：numgteq
Date	DateEquals	日期时间相等，简化为：dateeq
	DateNotEquals	日期时间不相等，简化为：dateneq
	DateLessThan	日期时间小于，简化为：datelt
	DateLessThanEquals	日期时间小于等于，简化为：datelteq
	DateGreaterThan	日期时间大于，简化为：dategt
	DateGreaterThanEquals	日期时间大于等于，简化为：dategteq
Boolean	Bool	严格布尔值相等
IP address	IpAddress	指定的IP或IP范围
	NotIpAddress	除指定的IP或IP范围外所有IP

说明

条件的关键字区分大小写。Date格式符合ISO 8601规范，例如：2015-07-01T12:00:00Z

每个条件可以包含多个key-value的组合。如下图的条件组合表示的判断条件为请求时间从2015-07-01T12:00:00Z到2018-04-16T15:00:00Z，请求的IP地址范围是192.168.176.0/24"或"192.168.143.0/24"网段的请求。

```
"Condition" : {
  "DateGreaterThan" : {
  "CurrentTime" : "2015-07-01T12:00:00Z"
  },
  "DateLessThan": {
  "CurrentTime" : "2018-04-16T15:00:00Z"
  },
  "IpAddress" : {
  "SourceIp" : ["192.168.176.0/24","192.168.143.0/24"]
  }
}
```

- **条件键**

条件中可选的键包括以下三种：动作无关的通用键、与桶动作有关的键和与对象动作有关的键。

动作无关的通用键包括：

表 A-5 通用键

键	类型	描述
CurrentTime	Date	服务器接收请求的时间，格式满足ISO 8601标准。
EpochTime	Numeric	服务器接收请求的时间，格式为1970.01.01 00:00:00 UTC开始所经过的秒数，不考虑闰秒。
SecureTransport	Bool	请求是否使用SSL加密。 **说明** 值为非“true”时，服务端会默认修正为“false”。
SourceIp	IP address	请求发起的源IP，即客户端IP。
UserAgent	String	请求的客户端软件代理程序。
Referer	String	请求从哪个链接发起。
SourceVpce	String	请求发起的VPC终端节点ID。 **说明** 仅华南-广州、华东-上海一区域支持。
SourceVpc	String	请求发起的VPC ID。 **说明** 仅华南-广州、华东-上海一区域支持。

条件中的键需要在一定的Action才能使用，Action和条件中的键配对使用关系如下表所示：

表 A-6 与桶动作有关的键

Action	可选键	描述	说明
ListBucket	prefix	String类型，列举以指定的字符串prefix开头的对象。	配置prefix、delimiter、max-keys后，执行List操作时需要带上符合条件的键值对信息，桶策略才生效。 例如，某桶配置了所有账号可读的桶策略，且条件运算符=NumericEquals，键=max-keys，值=100。则所有账号列举对象时需要在桶访问域名末尾加上?max-keys=100，才能完成对象列举，且列举的对象将是按照字典顺序的前100个对象。
	delimiter	String类型，用来分组桶内对象的字符串。	
	max-keys	Numeric类型，指定返回的最大数，返回的对象列表将是按照字典顺序的最多前max-keys个对象。	
ListBucketVersions	prefix	String类型，列举以指定的字符串prefix开头的多版本对象。	
	delimiter	String类型，用来分组桶内多版本对象的字符串。	
	max-keys	Numeric类型，指定返回的最大数，返回的对象列表将是按照字典顺序的最多前max-keys个对象。	
PutBucketAcl	x-obs-acl	String类型，设置桶ACL。修改桶ACL时在头域中可以包含的Canned ACL，取值范围为private|public-read|public-read-write|bucketowner-read|log-delivery-write。	无

表 A-7 与对象动作相关的键

Action	可选键	描述
PutObject	x-obs-acl	String类型，设置对象ACL。上传对象时在头域中可以包含的Canned ACL，取值范围为private|public-read|public-read-write|bucketowner-read|bucket-owner-full-control|log-delivery-write。
	x-obs-copy-source	String类型，用来指定复制对象时对象操作的源桶名以及源对象名。格式如/bucketname/keyname。

Action	可选键	描述
	x-obs-metadata-directive	String类型，用来指定新对象的元数据是从元对象中复制，还是用请求中的元数据替换，取值范围为COPY|REPLACE。
	x-obs-server-side-encryption	String类型，用来指定桶中对象以SSE-KMS方式加密存储，取值为kms。
PutObjectAcl	x-obs-acl	String类型，设置对象ACL。上传对象时在头域中可以包含的Canned ACL，取值范围为private|public-read|public-read-write|bucketowner-read|bucket-owner-full-control|log-delivery-write。
GetObjectVersion	versionId	String类型，获取versionId为xxx版本的对象。
GetObjectVersionAcl	versionId	String类型，获取versionId为xxx版本的对象ACL。
PutObjectVersionAcl	versionId	String类型，设置versionId。
	x-obs-acl	String类型，设置versionId为xxx版本的对象ACL。上传对象时在头域中可以包含的Canned ACL，取值范围为private|public-read|public-read-write|bucketowner-read|bucket-owner-full-control|log-delivery-write。
DeleteObjectVersion	versionId	String类型，删除versionId为xxx版本的对象。

Policy 权限判断逻辑

Policy在做权限判断时，每条statement会有3种结果，Explicit Deny、Allow和Default Deny。Bucket Policy对于Policy中的多条statement采用以下规则进行判定：Bucket Policy对Policy中包含的每条statement都要进行Explicit Deny、Allow和Default Deny的判断，最终的判决结果遵循Explicit Deny>Allow>Default Deny的规则；

1.如果没有显式的Deny和Allow，则请求权限判别为Default Deny

2.显式的Deny覆盖Allow；

3.Allow覆盖默认的Default Deny；

4.statement的顺序没有影响。

表 A-8 Statement Result

名称	说明
explicit deny	显式拒绝访问，资源匹配的statement中effect="deny"，表明Request无法进行访问，此时直接返回无权限失败。
allow	允许访问，资源匹配的statement中effect="allow"，表明Request可以进行访问，继续下一条statement判断。
default deny	默认拒绝访问，在没有任何一条statement与Request匹配上，默认本次Request无法进行访问。

如果ACL和Bucket Policy同时使用， 则ACL对某个租户的授权结果allow，可以被Bucket Policy的显式Deny覆盖。

如果Bucket Policy和IAM Policy同时使用，同样遵循explicit deny>allow>default deny的规则。

SSE-KMS服务端加密对象，不支持Bucket ACL/Policy进行跨租户授权访问。

A.2 桶策略和 ACL 的关系

桶 ACL 和桶策略的映射关系

桶ACL用于授予桶基本的读写权限，桶策略高级设置中支持更多在桶上可以执行的动作。桶ACL是对桶策略的补充，除了限定的只能由桶ACL授予日志投递用户组权限外，更多时候桶策略可以替代桶ACL管理桶的访问权限。桶ACL访问权限和桶策略动作的映射关系如**表A-9**所示。

表 A-9 桶 ACL 和桶策略的映射关系

ACL权限	选项	对应桶策略高级设置中的动作
桶访问权限	读取权限	• HeadBucket • ListBucket • ListBucketVersions • ListBucketMultipartUploads
	写入权限	• PutObject • DeleteObject • DeleteObjectVersion
对象权限	对象读权限	• GetObject
ACL访问权限	读取权限	• GetBucketAcl
	写入权限	• PutBucketAcl

对象 ACL 和桶策略的映射关系

对象ACL用于授予对象基本的读写权限。桶策略高级设置中支持更多在对象上可以执行的动作。对象ACL访问权限和桶策略动作的映射关系如表A-10所示。

表 A-10 对象 ACL 和桶策略的映射关系

对象ACL权限	选项	对应桶策略高级设置中的动作
对象访问权限	读取权限	• GetObject • GetObjectVersion
ACL访问权限	读取权限	• GetObjectAcl • GetObjectVersionAcl
	写入权限	• PutObjectAcl • PutObjectVersionAcl