对象存储服务

权限配置指南（巴黎区域）

文档版本	01
发布日期	2022-05-20

华为技术有限公司

商标声明


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

注意

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

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

安全声明

漏洞处理流程

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

目 录

1 OBS 权限控制概述

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

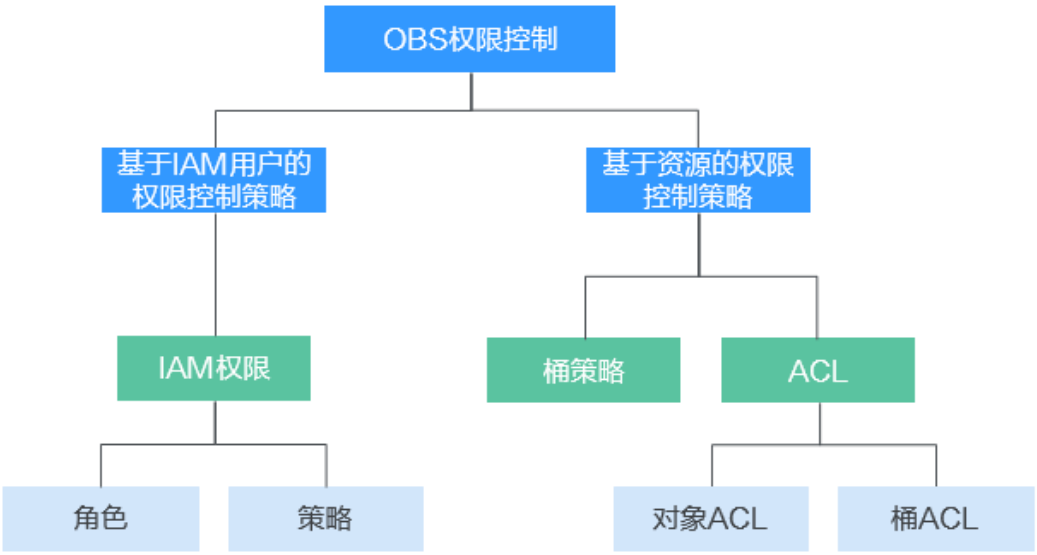


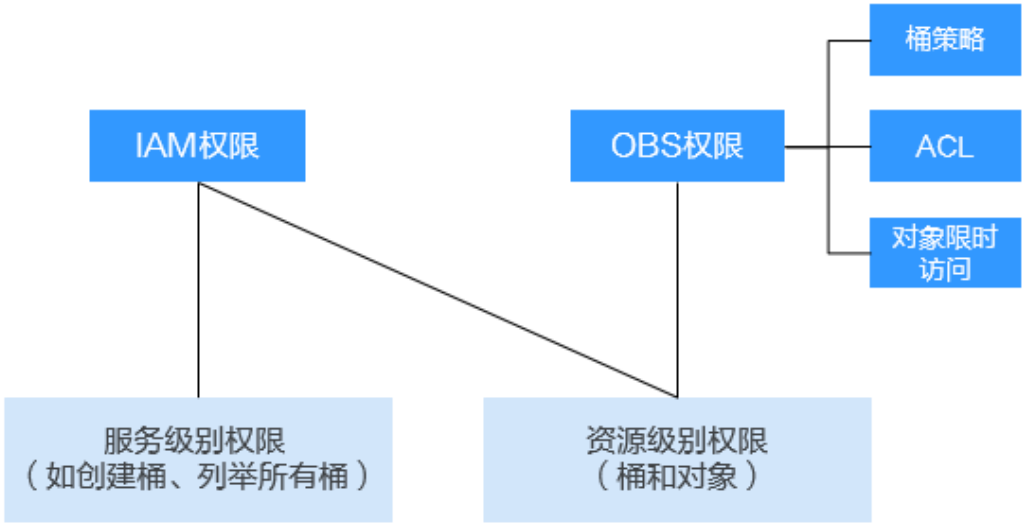
表 1-1 OBS 权限控制方式说明和应用场景

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（效果）**
- **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	支持的效果	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	支持的效果	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 • 匿名用户	• 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匿名用户授权时
  - 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。

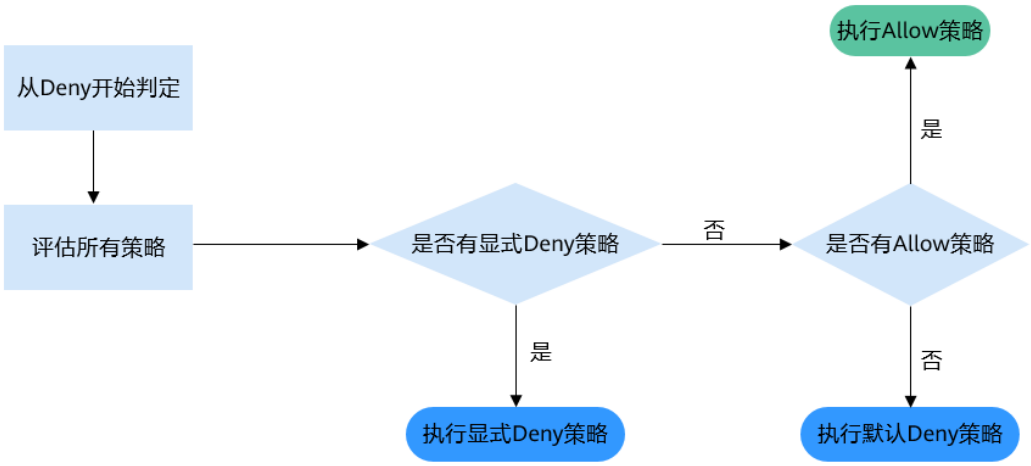
访问控制机制冲突时，如何工作？

OBS权限控制要素中，Effect（效果）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

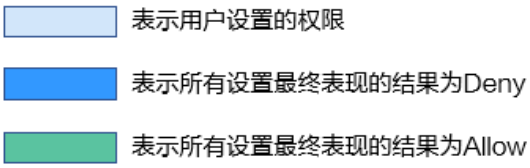
表示所有设置最终表现的结果为Deny

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



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。

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。

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 FullAccess	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	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。	系统策略	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 FullAccess	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 FullAccess	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 FullAccess	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
管理事件通知	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
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：

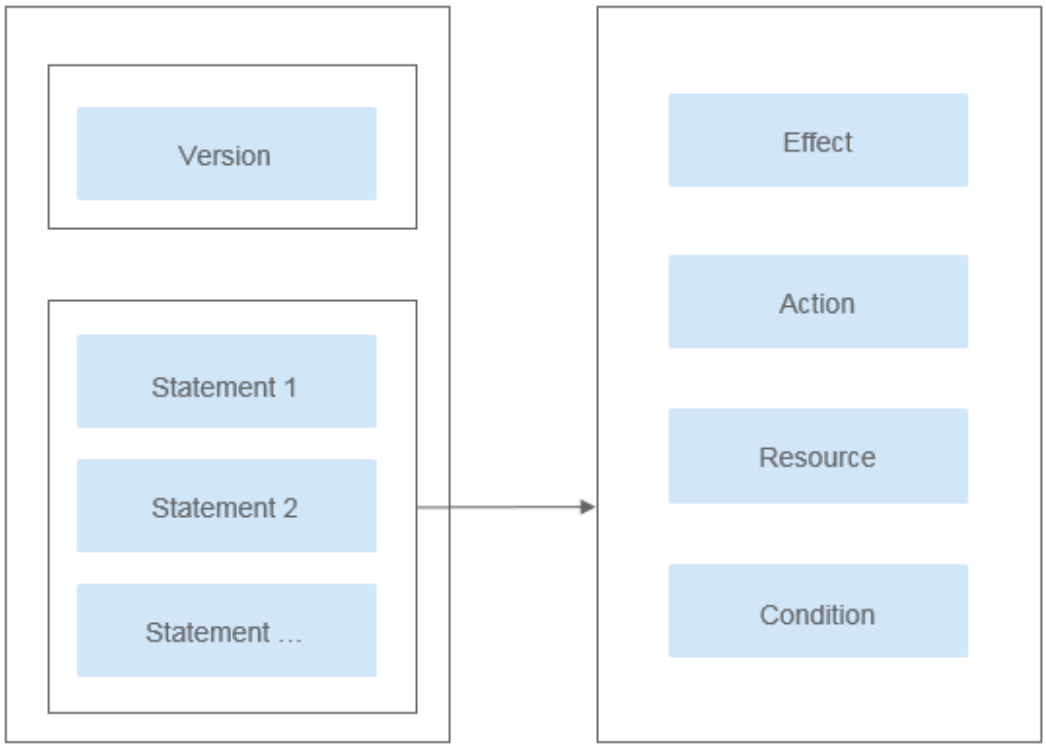
- 使用策略控制账号下整个云资源的权限时，使用IAM权限授权。
- 使用策略控制账号下OBS所有的桶和对象的权限时，使用IAM权限授权。

- 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。 • **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。

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、SMN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。

桶策略简介

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、其他账号或匿名用户授权桶及桶内对象的操作权限。OBS提供标准桶策略和高级桶策略。

标准桶策略：

标准桶策略提供三种策略供用户直接设置。

- 私有：除桶ACL授权外的其他用户无桶的访问权限。
- 公共读：任何用户都可以对桶内对象进行读操作。

- 公共读写：任何用户都可以对桶内对象进行读/写/删除操作。

桶创建成功后，默认桶策略为私有，仅桶拥有者具有完全控制权限，其他用户在未经授权的情况下均无访问权限。为确保数据安全，不推荐用户使用公共读或公共读写，建议使用私有。

表 2-4 标准桶策略描述

参数	私有	公共读	公共读写
效果	无	允许	允许
被授权用户	无	*（任何用户）	*（任何用户）
资源	无	*（桶内所有对象）	*（桶内所有对象）
动作	无	• GetObject • GetObjectVersion • HeadBucket • ListBucket	• GetObject • GetObjectVersion • PutObject • DeleteObject • DeleteObjectVersion • HeadBucket • ListBucket
条件	无	无	无

高级桶策略：

高级桶策略提供三种方式，方便用户快速设置桶策略。

- 只读模式：被授权用户将拥有桶内指定对象的读权限，对应可以执行获取对象内容及元数据操作。
- 读写模式：被授权用户将拥有桶内指定对象的读写权限，对应可以执行获取对象内容及元数据、上传对象、删除对象等操作。
- 自定义模式：自定义配置被授权用户可以拥有桶或对象的操作权限，由效果、被授权用户、资源、动作和条件5个桶策略基本参数共同决定。详细请参见**桶策略参数说明**。

说明

通常情况下，在控制台上通过高级桶策略给其他用户授予桶中资源的某些操作权限，需要同时授予用户桶的读权限ListBucket（配置策略时资源留空表示对桶授权），否则可能导致用户从控制台进入桶后提示没有权限。

桶策略应用场景

- 允许其他账号访问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。

桶策略结构&语法

一个桶策略由JSON描述，格式定义为：

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

实例如下所示:

```
{
   "Statement":[
      {
         "Sid": "ExampleStatementID1",
         "Principal":{
            "ID":[
               "domain/account ID",
               "domain/account ID:user/User ID"
            ]
         },
         "Effect":"Allow",
         "Action":[
            "CreateBucket",
            "DeleteBucket"
         ],
         "Resource":"000-02/key01",
         "Condition":{
            "NumericNotEquals":{
               "Referer":"sdf"
            },
            "StringNotLike":{
               "Delimiter":"ouio"
            }
         }
      }
   ]
}
```

桶策略由多条Statement组成，也可以是一条。每条Statement的结构包括下表内容：

表 2-5 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（账号）以及User（IAM用户），支持通配符“*”，表示所有用户。 ● 当对Domain（账号）下所有IAM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。	可选，Principal与NotPrincipal必选其一

元素	描述	是否必选
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必选其一
Effect	必选关键字，效果，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
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必选其一
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必选其一
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必选其一
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必选其一
Condition	可选关键字，本条statement生效的条件。	可选

各个要素的详细介绍，请参见**桶策略参数说明**。

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：向匿名用户授予指定对象的只读权限**

  下面的示例策略向匿名用户授予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。

被授权用户	描述
匿名用户	未注册的普通访客。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。
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。
	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。
	写入权限	此权限可以上传、覆盖和删除该桶内任何对象。
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

权限	选项	描述
	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、桶的多版本。 设在对象上，所有人可以获取该对象内容和元数据。

预定义的权限控制策略	描述
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、桶的多版本、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、桶的多版本，可以获取该桶内对象的内容和元数据。 不能应用在对象上。
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、桶的多版本、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。

头域	含义
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**。

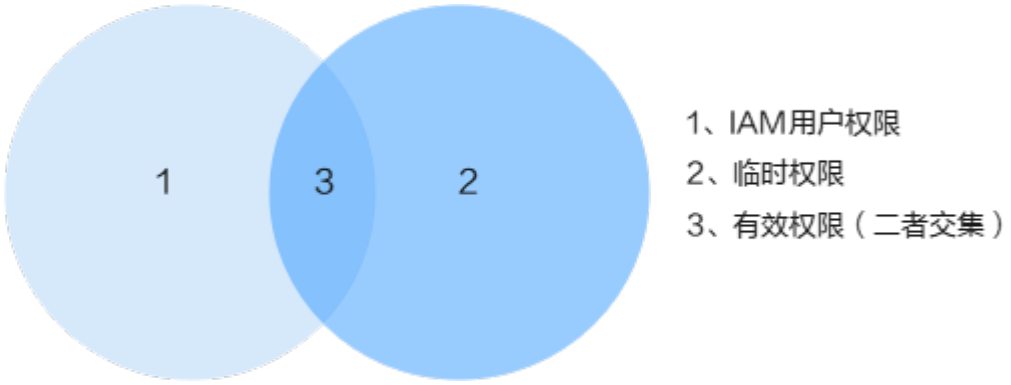
临时访问密钥的权限

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。

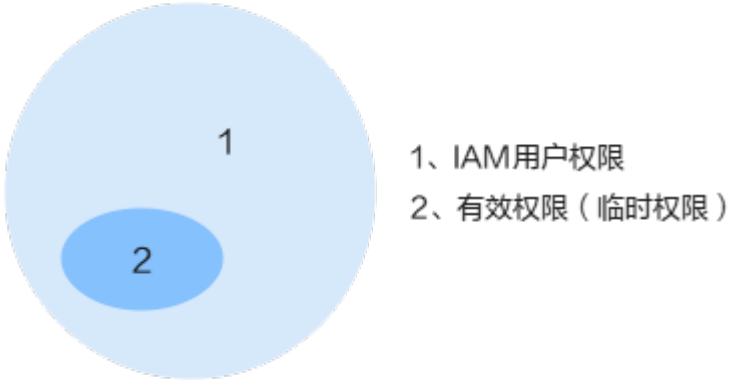
如下图，“1”代表了IAM用户的原有权限，“2”为设置的临时策略所对应的临时权限，两个权限的交集“3”即为使用者最终的有效权限。

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。

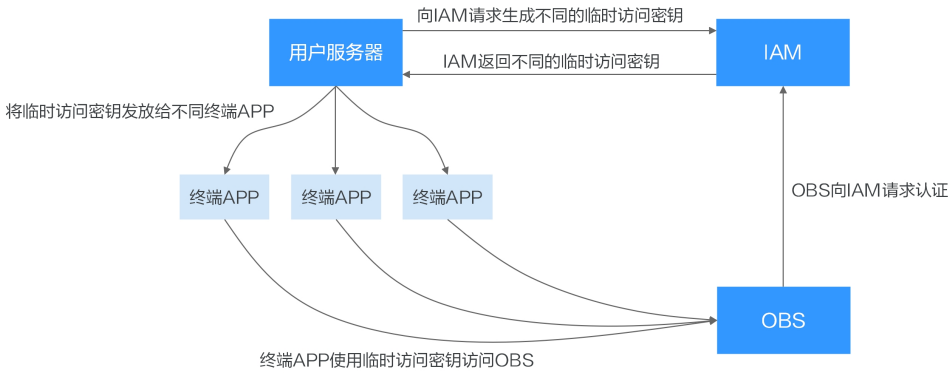
应用场景

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。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

分享文件所生成的URL都是临时URL，存在有效期。

临时URL采用V4临时授权请求鉴权方法，URL的格式示例如下：

```
https://oss.regionid.prod-cloud-ocb.orange-business.com/bucketname/objectname?X-Amz-Algorithm=xxx&X-Amz-Credential=xxx&X-Amz-Date=xxx&X-Amz-Expires=900&X-Amz-Signature=xxx&X-Amz-SignedHeaders=xxx&response-content-disposition=xxx
```

当在OBS控制台上单击了对象后的“更多 > 复制对象URL”之后，OBS就会以固定900s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。每单击一次“复制对象URL”，OBS就会重新获取一次鉴权信息以生成新的分享链接，新链接的有效期会重新开始计算。

文件夹分享

文件夹分享强调临时性，存在有效期。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。

约束与限制

- 通过OBS控制台分享的文件，有效期固定为900s。如果想要设置永久的权限，请**通过桶策略向匿名用户授予对象的公共读权限**。
- 通过OBS控制台分享的文件夹，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**通过桶策略向匿名用户授予对象的公共读权限**。
- 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。
- 冷存储对象需恢复后才能分享。

配置方法

对于文件的分享方法，请参见**向匿名用户临时分享对象**。

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 权限典型场景一览

我们提供了如下典型的权限场景，帮助您顺利完成OBS权限配置。

场景分类的总体思路为：

1. **对谁授权：**主要分为单个IAM用户、多个IAM用户或用户群组、其他账号、匿名用户
2. **对什么资源授权：**主要分为所有OBS资源（服务级权限）、指定桶、指定对象等
3. **授予什么权限：**案例中聚焦一些基础的权限，如读权限、读写权限等，您可以根据实际业务情况扩展

您可以根据上述思路，明确您的业务场景，并在场景树中找到适合您的权限配置案例，对于不同的场景，OBS都有不同的推荐配置方式。

图 4-1 典型权限场景树

下表为各个典型场景的权限配置案例，您可以选择适合您的案例查看。

表 4-1 典型权限场景配置案例

权限场景	场景配置案例
对当前账号下单个IAM用户授权	**对单个IAM用户授予创建桶和列举桶的权限**
	对单个IAM用户授予桶的读写权限
	对单个IAM用户授予桶的指定操作权限
	对单个IAM用户授予指定对象的读权限
	对单个IAM用户授予指定对象的指定操作权限
对当前账号下多个IAM用户或用户群组授权	**对IAM用户组授予OBS所有资源的所有操作权限**
	对IAM用户组授予OBS所有资源的基本操作权限
	对IAM用户组授予OBS所有资源的指定操作权限
	对IAM用户组授予OBS指定资源的指定操作权限
对其他账号授权	**对其他账号授予桶的读写权限**
	对其他账号授予桶的指定操作权限

权限场景	场景配置案例
	对其他账号下的IAM用户授予桶和桶内资源的访问权限
	对其他账号授予指定对象的读权限
	对其他账号授予指定对象的指定操作权限
对匿名用户授权	对匿名用户授予桶的公共读权限
	对匿名用户授予指定目录的读权限
	对匿名用户授予指定对象的读权限
	向匿名用户临时分享对象
临时权限	临时授权访问OBS
限制IP	限制指定的IP地址访问桶

5 典型场景配置案例

5.1 对当前账号下单个 IAM 用户授权

5.1.1 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 使用云服务账号登录管理控制台。

步骤2 在顶部导航栏选择“服务列表>管理与部署>统一身份认证服务”，进入“统一身份认证服务”管理控制台。

步骤3 在左侧导航栏单击“策略”，进入“策略”界面。

步骤4 单击右上角“创建自定义策略”。

步骤5 配置自定义策略参数。

表 5-1 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

参数	说明
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6 单击“确定”，完成自定义策略创建。

步骤7 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8 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

5.1.2 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

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。

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“对象存储”。

步骤2 在桶列表单击目标桶的桶名称，进入“概览”页面。

步骤3 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤4 在“桶策略”页面“高级桶策略”下，单击“创建桶策略”。

步骤5 配置桶策略参数。

表 5-2 桶策略参数配置说明

参数	说明
策略模式	选择“读写模式”
被授权用户	● 选择包含 > 当前账号 ● 用户名：选择被授权的IAM用户
资源	● 包含 ● 资源名称：填写“*”

步骤6 单击“确定”，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 使用云服务账号登录管理控制台。

步骤2 在顶部导航栏选择“服务列表>管理与部署>统一身份认证服务”，进入“统一身份认证服务”管理控制台。

步骤3 在左侧导航栏单击“策略”，进入“策略”界面。

步骤4 单击右上角“创建自定义策略”。

步骤5 配置自定义策略参数。

表 5-3 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

参数	说明
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6 单击“确定”，完成自定义策略创建。

步骤7 **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8 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

5.1.3 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“对象存储”。

步骤2 在桶列表单击目标桶的桶名称，进入“概览”页面。

步骤3 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤4 在“桶策略”页面“高级桶策略”下，单击“创建桶策略”。

步骤5 配置桶策略参数。

表 5-4 桶策略参数配置说明

参数	说明
策略模式	选择“自定义模式”
效果	选择“Allow”
被授权用户	• 选择包含 > 当前账号 • 用户名：选择被授权的IAM用户
资源	选择“包含 > 配置到整个桶”
动作	• 包含 • 动作名称： – DeleteBucket – ListBucketVersions（被授权用户需要在控制台或OBS Browser+上访问时需要） 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6 单击“确定”，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 使用云服务账号登录管理控制台。

步骤2 在顶部导航栏选择“服务列表>管理与部署>统一身份认证服务”，进入“统一身份认证服务”管理控制台。

步骤3 在左侧导航栏单击“策略”，进入“策略”界面。

步骤4 单击右上角“创建自定义策略”。

步骤5 配置自定义策略参数。

表 5-5 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6 单击“确定”，完成自定义策略创建。

步骤7 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8 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

5.1.4 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

按照本案例配置后，可以正常通过API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，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“对象存储”。

步骤2 在桶列表单击目标桶的桶名称，进入“概览”页面。

步骤3 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤4 在“桶策略”页面“高级桶策略”下，单击“创建桶策略”。

步骤5 配置桶策略参数。

表 5-6 桶策略参数配置说明

参数	说明
策略模式	选择“只读模式”
被授权用户	• 选择包含 > 当前账号 • 用户名：选择被授权的IAM用户
资源	• 包含 • 资源名称填写需要访问的桶内对象或对象集 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“*”

步骤6 单击“确定”，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 使用云服务账号登录管理控制台。

步骤2 在顶部导航栏选择“服务列表>管理与部署>统一身份认证服务”，进入“统一身份认证服务”管理控制台。

步骤3 在左侧导航栏单击“策略”，进入“策略”界面。

步骤4 单击右上角“创建自定义策略”。

步骤5 配置自定义策略参数。

表 5-7 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6 单击“确定”，完成自定义策略创建。

步骤7 **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8 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

5.1.5 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“对象存储”。

步骤2 在桶列表单击目标桶的桶名称，进入“概览”页面。

步骤3 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤4 在“桶策略”页面“高级桶策略”下，单击“创建桶策略”。

步骤5 配置桶策略参数。

表 5-8 桶策略参数配置说明

参数	说明
策略模式	选择“自定义模式”
效果	选择“Allow”
被授权用户	• 选择包含 > 当前账号 • 用户名：选择被授权的IAM用户
资源	• 选择“包含 > 指定资源” • 资源名称填写需要访问的桶内对象或对象集 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“*”
动作	• 包含 • 动作名称：选择“GetObject” 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6 单击“确定”，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 使用云服务账号登录管理控制台。

步骤2 在顶部导航栏选择“服务列表>管理与部署>统一身份认证服务”，进入“统一身份认证服务”管理控制台。

步骤3 在左侧导航栏单击“策略”，进入“策略”界面。

步骤4 单击右上角“创建自定义策略”。

步骤5 配置自定义策略参数。

表 5-9 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6 单击“确定”，完成自定义策略创建。

步骤7 **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8 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

5.2 对当前账号下多个 IAM 用户或用户群组授权

5.2.1 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 使用云服务账号登录管理控制台。

步骤2 在顶部导航栏选择“服务列表>管理与部署>统一身份认证服务”，进入“统一身份认证服务”管理控制台。

步骤3 在左侧导航栏单击“策略”，进入“策略”界面。

步骤4 单击右上角“创建自定义策略”。

步骤5 配置自定义策略参数。

表 5-10 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6 单击“确定”，完成自定义策略创建。

步骤7 **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8 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

5.2.2 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 5-11 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 FullAccess	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。	系统策略
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 使用云服务账号登录管理控制台。

步骤2 在顶部导航栏选择“服务列表>管理与部署>统一身份认证服务”，进入“统一身份认证服务”管理控制台。

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

5.2.3 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 使用云服务账号登录管理控制台。

步骤2 在顶部导航栏选择“服务列表>管理与部署>统一身份认证服务”，进入“统一身份认证服务”管理控制台。

步骤3 在左侧导航栏单击“策略”，进入“策略”界面。

步骤4 单击右上角“创建自定义策略”。

步骤5 配置自定义策略参数。

表 5-12 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 • 选择“所有资源”
作用范围	默认为“全局级服务”

步骤6 单击“确定”，完成自定义策略创建。

步骤7 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8 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

5.2.4 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 使用云服务账号登录管理控制台。

步骤2 在顶部导航栏选择“服务列表>管理与部署>统一身份认证服务”，进入“统一身份认证服务”管理控制台。

步骤3 在左侧导航栏单击“策略”，进入“策略”界面。

步骤4 单击右上角“创建自定义策略”。

步骤5 配置自定义策略参数。

表 5-13 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 • 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6 单击“确定”，完成自定义策略创建。

步骤7 **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8 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

5.2.5 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 使用云服务账号登录管理控制台。

步骤2 在顶部导航栏选择“服务列表>管理与部署>统一身份认证服务”，进入“统一身份认证服务”管理控制台。

步骤3 在左侧导航栏单击“策略”，进入“策略”界面。

步骤4 单击右上角“创建自定义策略”。

步骤5 配置自定义策略参数。

表 5-14 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6 单击“确定”，完成自定义策略创建。

步骤7 **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8 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。

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。

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”。

步骤5 单击”新建文件夹”，文件夹folder-002可以创建成功。

步骤6 单击“上传对象”，文件333.txt上传成功。

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

5.3 对其他账号授权

5.3.1 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账号授予OBS桶的读写权限。这里的账号指账号本身，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，被授权账号可以正常通过API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“对象存储”。

步骤2 在桶列表单击目标桶的桶名称，进入“概览”页面。

步骤3 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤4 在“桶策略”页面“高级桶策略”下，单击“创建桶策略”。

步骤5 配置桶策略参数。

表 5-15 桶策略参数配置说明

参数	说明
策略模式	选择“读写模式”
被授权用户	• 选择包含 > 其他账号 • 账号ID：填写被授权账号的账号ID，可在对应账号“我的凭证”页面获取 • 用户ID：同账号ID，填写被授权账号的账号ID，可在对应账号“我的凭证”页面获取 **说明** 因为本案例是针对账号本身授权，不包含账号下的IAM用户，所以用户ID与账号ID相同。
资源	• 包含 • 资源名称：填写“*”

步骤6 单击“确定”，完成桶策略创建。

步骤7 （可选）再次单击“创建桶策略”。

如果被授权账号希望通过挂载外部桶的方式在OBS Browser+上访问此OBS桶，需要再添加一条ListBucket权限。

步骤8 （可选）配置ListBucket权限。

表 5-16 桶策略参数配置说明

参数	说明
策略模式	选择“自定义模式”
效果	选择“Allow”
被授权用户	• 选择包含 > 其他账号 • 账号ID：填写被授权账号的账号ID，可在对应账号“我的凭证”页面获取 • 用户ID：同账号ID，填写被授权账号的账号ID，可在对应账号“我的凭证”页面获取 **说明** 因为本案例是针对账号本身授权，不包含账号下的IAM用户，所以用户ID与账号ID相同。
资源	选择“包含 > 配置到整个桶”
动作	• 包含 • 动作名称：ListBucket

步骤9 （可选）单击“确定”，完成桶策略创建。

----结束

5.3.2 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账号授予OBS桶的指定操作权限。这里的账号指账号本身，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“对象存储”。

步骤2 在桶列表单击目标桶的桶名称，进入“概览”页面。

步骤3 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤4 在“桶策略”页面“高级桶策略”下，单击“创建桶策略”。

步骤5 配置桶策略参数。

表 5-17 桶策略参数配置说明

参数	说明
策略模式	选择“自定义模式”
效果	选择“Allow”
被授权用户	• 选择包含 > 其他账号 • 账号ID：填写被授权账号的账号ID，可在对应账号“我的凭证”页面获取 • 用户ID：同账号ID，填写被授权账号的账号ID，可在对应账号“我的凭证”页面获取 **说明** 因为本案例是针对账号本身授权，不包含账号下的IAM用户，所以用户ID与账号ID相同。
资源	选择“包含 > 配置到整个桶”
动作	• 包含 • 动作名称： – PutBucketAcl – GetBucketAcl – ListBucket（被授权账号希望通过挂载外部桶的方式在OBS Browser+上访问此OBS桶时需要） 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6 单击“确定”，完成桶策略创建。

----结束

5.3.3 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IAM权限中配置对应的权限即可。

推荐配置方法

对其他账号下的IAM用户授权，**需要同时配置桶策略和IAM权限**。

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. 同时需要账号A配置IAM权限：允许IAM用户A访问桶B。

桶策略和IAM权限中同时允许的权限才能生效。

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。

配置步骤一：配置允许指定操作的桶策略

首先需要由桶拥有者或者具有桶策略配置权限的用户，配置一条允许执行指定操作的桶策略。

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“概览”页面。

步骤3 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤4 在“桶策略”页面“高级桶策略”下，单击“创建桶策略”。

步骤5 配置允许上传下载的桶策略。

表 5-18 桶策略参数配置说明

参数	说明
策略模式	选择“自定义模式”
效果	选择“Allow”
被授权用户	● 选择包含 > 其他账号 ● 账号ID：填写被授权账号的账号ID，可在对应账号或账号下IAM用户的“我的凭证”页面获取 ● 用户ID：填写被授权账号下的IAM用户的IAM用户ID，可在对应IAM用户“我的凭证”页面获取，同时支持通配符（*）表示对账号下所有IAM用户生效

参数	说明
资源	• 选择“包含 > 指定资源” • 资源名称填写需要访问的桶内对象或对象集 – 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“*” 此处需要下载所有对象，则填写“*”
动作	• 包含 • 动作名称： – GetObject – GetObjectVersion – PutObject – 可选：ListBucket（需要使用OBS Browser+挂载外部桶时执行此步骤） 如果需要配置其他指定的对象操作权限，选择对应动作即可。**OBS支持的动作**

步骤6 单击“确定”，完成允许上传下载的桶策略创建。

步骤7 可选：再次单击“创建桶策略”，配置允许列举桶内对象的桶策略（需要使用OBS Browser+挂载外部桶时执行此步骤）。

表 5-19 桶策略参数配置说明

参数	说明
策略模式	选择“自定义模式”
效果	选择“Allow”
被授权用户	• 选择包含 > 其他账号 • 账号ID：与上一条桶策略一致，填写被授权账号的账号ID，可在对应账号或账号下IAM用户的“我的凭证”页面获取 • 用户ID：与上一条桶策略一致，填写被授权账号下的IAM用户的IAM用户ID，可在对应IAM用户“我的凭证”页面获取，同时支持通配符（*）表示对账号下所有IAM用户生效
资源	选择“包含 > 配置到整个桶”
动作	• 包含 • 动作名称：ListBucket 如果需要配置其他指定的桶操作权限，选择对应动作即可。**OBS支持的动作**

步骤8 单击“确定”，完成允许列举桶内对象的桶策略创建。

----结束

配置步骤二：配置允许指定操作的 IAM 权限

同时，还需要由被授权IAM用户所属账号，为IAM用户配置允许对指定桶执行指定操作的IAM权限，允许的操作要与桶策略相同。

步骤1 使用云服务账号登录管理控制台。

步骤2 在顶部导航栏选择“服务列表>管理与部署>统一身份认证服务”，进入“统一身份认证服务”管理控制台。

步骤3 在左侧导航栏单击“策略”，进入“策略”界面。

步骤4 单击右上角“创建自定义策略”。

步骤5 配置自定义策略参数。

表 5-20 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） ● 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6 单击“确定”，完成自定义策略创建。

步骤7 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8 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

5.3.4 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，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“对象存储”。

步骤2 在桶列表单击目标桶的桶名称，进入“概览”页面。

步骤3 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤4 在“桶策略”页面“高级桶策略”下，单击“创建桶策略”。

步骤5 配置桶策略参数。

表 5-21 桶策略参数配置说明

参数	说明
策略模式	选择“只读模式”

参数	说明
被授权用户	• 选择包含 > 其他账号 • 账号ID：填写被授权账号的账号ID，可在对应账号“我的凭证”页面获取 • 用户ID：同账号ID，填写被授权账号的账号ID，可在对应账号“我的凭证”页面获取 **说明** 因为本案例是针对账号本身授权，不包含账号下的IAM用户，所以用户ID与账号ID相同。
资源	• 包含 • 资源名称填写需要访问的桶内对象或对象集 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“*”

步骤6 单击“确定”，完成桶策略创建。

----结束

5.3.5 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“对象存储”。

步骤2 在桶列表单击目标桶的桶名称，进入“概览”页面。

步骤3 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤4 在“桶策略”页面“高级桶策略”下，单击“创建桶策略”。

步骤5 配置桶策略参数。

表 5-22 桶策略参数配置说明

参数	说明
策略模式	选择“自定义模式”
效果	选择“Allow”
被授权用户	• 选择包含 > 其他账号 • 账号ID：填写被授权账号的账号ID，可在对应账号“我的凭证”页面获取 • 用户ID：同账号ID，填写被授权账号的账号ID，可在对应账号“我的凭证”页面获取 **说明** 因为本案例是针对账号本身授权，不包含账号下的IAM用户，所以用户ID与账号ID相同。
资源	• 选择“包含 > 指定资源” • 资源名称填写需要访问的桶内对象或对象集 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“*”
动作	• 包含 • 动作名称：选择“GetObject” 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6 单击“确定”，完成桶策略创建。

----结束

5.4 对匿名用户授权

5.4.1 对匿名用户授予桶的公共读权限

场景介绍

当某个桶需要授权匿名用户访问权限时，可以通过桶策略和桶ACL配置授予匿名用户访问桶的权限。本示例以桶策略为例。

配置步骤

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“概览”页面。

步骤3 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤4 在“桶策略”页面“高级桶策略”下，单击“创建桶策略”。

步骤5 在“桶策略”页签下，将“标准桶策略”修改为“公共读”，完成配置。

----结束

验证

步骤1 权限设置成功后，在桶“概览”页的“基本信息”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

5.4.2 对匿名用户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匿名用户访问权限时，可以通过桶策略配置授予匿名用户访问文件夹内对象的权限。

配置步骤

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“概览”页面。

步骤3 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤4 在“桶策略”页面“高级桶策略”下，单击“创建桶策略”。

步骤5 配置如下参数，授予匿名用户访问文件夹内对象的权限。

表 5-23 授予访问指定目录权限的参数配置

参数	取值
策略模式	选择“只读模式”

参数	取值
被授权用户	• 包含 • 其他账号，账号ID输入“*”，表示所有匿名用户。
资源	• 包含 • 选择“指定资源” • 配置为文件夹内的所有对象，如文件夹名称为“folder-001”时，资源值为“folder-001/*”。

步骤6 单击“确定”完成配置。

----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。

5.4.3 对匿名用户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匿名用户的读取权限，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。

配置步骤

步骤1 在OBS管理控制台左侧导航栏选择“对象存储”。

步骤2 在桶列表单击待操作的桶，进入“概览”页面。

步骤3 在左侧导航栏，单击“对象”。

步骤4 找到待操作的对象，单击对象名称。

步骤5 在“对象ACL”页签下，单击待操作的对象并单击“对象ACL”。

步骤6 在“公共访问权限>匿名用户”中，单击“编辑”为匿名用户设置对象的读取权限。

步骤7 单击“保存”保存权限设置。

----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。

5.4.4 向匿名用户临时分享对象

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“概览”页面。

步骤3 在左侧导航栏，单击“对象”。

步骤4 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。

步骤5 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“概览”页面。

步骤3 在左侧导航栏，单击“对象”。

步骤4 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5 设置相关参数。

表 5-24 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。

步骤6 单击“创建分享”，生成文件分享URL。

步骤7 您可以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。

----结束

验证方法

其他用户通过网页访问分享的文件夹。

步骤1 打开网页，输入分享的URL地址，打开链接。

步骤2 在页面提示框输入“提取码”，确认即可访问分享的文件夹。

----结束

其他用户通过OBS Browser+访问分享的文件夹。

步骤1 打开OBS Browser+。

步骤2 在登录页面选择“授权码登录”。

步骤3 输入“授权码”和“提取码”。

步骤4 单击“登录”，即可访问分享的文件夹。

----结束

5.5 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 使用云服务账号登录管理控制台。

步骤2 在顶部导航栏选择“服务列表>管理与部署>统一身份认证服务”，进入“统一身份认证服务”管理控制台。

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. 在左侧导航栏单击“策略”，进入“策略”界面。
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。

表 5-25 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。

5.6 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“对象存储”。

步骤2 在桶列表单击目标桶的桶名称，进入“概览”页面。

步骤3 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤4 在“桶策略”页面“高级桶策略”下，单击“创建桶策略”。

步骤5 配置桶策略参数。

表 5-26 桶策略参数配置说明

参数	说明
策略模式	选择“自定义模式”
效果	选择“Deny”
被授权用户	• 选择“包含 > 其他账号” • 账号ID：输入“*”，表示对所有注册用户和匿名用户生效 • 用户ID：不填
资源	选择“包含 > 配置到整个桶”
动作	• 包含 • 动作名称：选择“*”，表示所有权限
条件	• 条件运算符：IpAddress • 键：SourceIP • 值：114.115.1.0/24 **说明** 多个IP值需要使用英文逗号隔开。

说明

如果希望限制网段外的IP地址的客户端可以访问桶，需要参考**对匿名用户授权**对匿名用户授予允许访问的权限。

步骤6 单击“确定”，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。

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。	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，效果，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有匿名用户、特定租户、特定用户、联合身份用户，委托用户。

- 所有人（匿名用户）

```
"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/*" }
  ```

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包含和排除两种方式来指定：

- 包含：桶策略对指定的用户生效。
- 排除：桶策略对除指定用户外的其他用户生效。

指定当前账号的IAM用户

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

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，可以为设置一个其他账号。如果只想为其他账号下的IAM用户授权，则需再配置用户ID，可以指定多个IAM用户，用户ID使用（,）分隔。

说明

账号ID和用户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。

指定任何人（匿名用户）

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“其他账号”，账号ID输入“*”通配符。

须知

为匿名用户设置桶访问权限需谨慎使用。如果您授予匿名用户桶访问权限，则意味着世界上任何人都可以访问您的桶，而由此产生的流量、存储费用，都将由桶拥有者（云服务账号）自己承担。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包含和排除两种方式来指定：

- 包含：桶策略对指定的动作生效。
- 排除：桶策略对除指定动作外的其他动作生效。

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）	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。

类型	值	描述
	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。

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。
	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。
	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。

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，资源可以是当前整个桶，也可以是桶内对象。

资源可以通过包含和排除两种方式来指定：

- 包含：桶策略对指定的OBS资源生效。
- 排除：桶策略对除设置外的其他OBS资源生效。

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，配置方法为在资源输入框中不输入任何内容。

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

说明

多个对象或对象集使用英文逗号“,”分隔。

Condition

除了指定效果、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

类型	关键字	说明
	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。

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，某桶配置了匿名用户可读的桶策略，且条件运算符=NumericEquals，键=max-keys，值=100。则匿名用户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
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

B 修订记录

发布日期	修订记录
2022-05-20	第一次正式发布。