# AWS S3

Amazon Simple Storage Service(Amazon S3)是一种对像存储服务，提供行业领先的可扩展性、数据可用性、安全性和性能

这意味首各种规模和行业的客户都可以使用S3来存储并保护名各种用例(如数据湖、网站、移动应用程序、备份和还原、存档、企业应用程序、IOP设备和大数据分析)的数据，容量不限，

Amazon S3提供了易于使用的管理功能，因此您可以组织数据并配置精细调整过的使用权限控制，从而调足特定的业务、组织和合规件要求。

Amazon S3可达到99.999999999%(11个9)的特久性，并为全球各地的公司存储数百万个应用程序的数据

S3是一个object storage的服务，可以存任何东西，文件，视频，图片，都会被存储在一个Bucket里，这是一个没有层级的存储方式，你可以想象一下数据之闸并没有关系，是一个扁平的结构。

每一个文件呢，在被创建的时侯都会有一个Header和0-5TB大小的存储内容。然后这每一个文件都会有一个唯一的ID与其绑定，这个ID将可以被任何wb应用对这个文件进行访问。比如在你的AWS一个VM虚拟机就可以调用存储在S3里的文件。所以它适合存储那些那些需要经常被访问的文件

S3还有个非常实用的功能，就是它能host静态网站（就是不需要后台数据库登陆和各种操作的那种纯展示型网站），可以连接cloudfront进行全球部署



##### 适用的场景

1.数据文件保存

2.日志文件保存

3.备份快照保存

4.静态网站主机

5.教据湖data lake)

6.云盘(类google drive,onedrive,,dropbox)

##### 存储分类(SAA必考)：

·S3标准：活用于频骤访问的数据的通用存储

·S3智能分层：适用于具有未知或变化的访问模式的数据

·S3标准-A：不频繁访问

·S3单区-lA：不频访问(所有数据存在一个zone里)

·S3 Glacier：长期存档（取数据稍快）

·S3 Glacier Deep Archive：长期存档(取数据很慢，但便宜)

·S3 Outposts:本地存储(在公司放AWS快件做储存)

S3智能分层重点讲解：

专为希望在数据访问模式发生变化时自动优化存储成木而不会响性能或运营开销的客户而设计。S3智能分层是第一个云对象存储类，通过在访问模式发生变化时在两个访问层（频繁访问层和不频繁访问层）之间移动数据来实现自动节省成本，非常适用于访问模式未知或不断变化的数据。S3智能分层将对象存储在两个访问层中：一个是针对频繁访问进行了优化的层，另一个是针对不频繁访问进行了优化的更低成本的层。每个对象每月只需支付少量的监控和自动化费用，S3智能分层即可监控访问模式并将连续30天未访问的对象移动到不频繁访问层。S3智能分层没有检索费用。如果日后访问了不频访问层中的对像，S3智能分层会自动将其移回频繁访问层。

### 访问控制

S3的三种访问控制如下：

1.IAM Policy,是基于用户层面的控制，attach to IAM实体（User,Role或Group）,规定了谁能对感些S3做什么操作

2.Bucket Policy,是基于Bucket层面的控制，attach to Bucket, 规定了哪些人能对我这个Bucket中的resource做什么操作。

3.S3 ACL是基于Bucket或单个对象的，规定了谁能对我这个Bucket或对象做什么操作。

#### IAM Policy

IAM Policy是实施在IAM层面的。规定了某个AWS IAM实体（User,Goup或者Rol)可以对S3所能做的操作。

IAM Policy由多个Statement组成，每个Statement都规定了谁被允许/禁止对某个aws资源(包括但不限于s3)进行哪些操作这样的一组策略。

如下是一个IAM Policy的例子。在这个Policy中，尤许对名为my\_bucket的S3的bucket做任何s3的操作。



### Bucket Policy

Bucke Policy是实施在S3 Bucker层面的，只能定义本Bucke时中简源的访问权限。无法定义对其他Bucket的访问权限。如果定义了其他Bucket的访问权限，保存Policy的时候会报错。

Bucket Policy定义了谁可以被允许/禁止对本bucket进行哪些操作，

如下是一个经典的Bucket时Policy.意思是允许任何人对Bucket Cart-test-at-seoul中的任意Object执行s3： GetObject的操作，也就是将Bucket中的Object设置为Public Read



### Access Control List (ACL)

S3 ACL可以实施在Bucket层面，也可以实施在Object层面。

AWS为ACL设置了一些预定义的组

·AWS account Access-代表的是帐户极别的设置，可以设置本帐户和授权某个帐户来访问S3的资源

·Authenticated Users group-代表的是AWS中任意验证过的帐户，对这个组授权后，是世界上任何经过身份验证的AWS用户都可以访问你的Bucket

·All Users group-代表世界上的任何人

·Log Delivery group-针对服务器访问日志记录用来允许AWS将某个S3的访问请求写入本Bucket针对每个组在Bucket或者Object层面上,有如下四种访问权限可以设置

·List objects

·Write objects

·Read bucket permissions

·Write bucket permissions

### S3生命周期

使用S3生命周期，管理您的对象以使其在整个生命周期内经济高效地存储。

S3生命周期配置是一组规则。用于定义Amazon S3对一相对象应用的操作。有两种类型的操作：

·转换操作-定义对象转换为另一个使用Amaz0S3存储类的时间。例如。意可以选择在对象

创建30天后将其转换为S3 Standard-lA存储失，或在对象创建1年后得其存档到S3 Glacier

存储类。

存在与生命周期转换请求关联的成本。有关定价信息，请参阅Amaz0S3定价。

·过期操作-定义对象的过期时间。Amaz0nS3得代表您除过期的对象。

生命周期过期成本取决于您选择过期对象的时间。

#### 转换操作

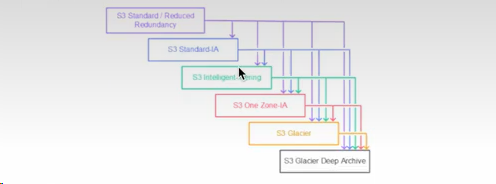
1.受支特的转换和相关限制

在S3生命周期配置中，您可以定义用于得对象从一个存储类转换为另一个存储类的规则，以节省存

储成本。如果您不了解对象的访问模式或访问模式不断变化，则可将对象转换为S3 Intelligent-

Tiering存储失，以自动实现成本节省。有关存储类别的信息，请参阅使用Amazon S3存储失。

Amazon S3支持用于在存储奥之间进行转换的瀑布模型。如下图所示。



2支持的生命周期转换

Amaz0nS3支持在使用S3生命周期配置的存储类之间进行以下生命周期转换。

您可以进行以下转换：

·从S3 Standard存储类转换为任何其他存储类。

·从任何存储类转换为S3 Glacier或S3 Glacier Deep Archive存储类。

·从S3 Standard-lA存储类转快为S3 Intelligent-Tiering或S3 One Zone-lA存储类。

·从S3 intelligent--Tiering存储类转换为S3 One Zone-lA存储类。

·从S3 Glacier存储类转换为S3 Glacier Deep Archive存储受。

在将对象从S3 Standard或S3 Standard-HA存储类转换为S3 Standard-A或S3 One Zone-lA之前，必须将它们存储在S3 Standard存储类中至少达30天。

S3 Standard-A和S3 One Zone-lA存储等级至少收取30天的存储费用。

当您得对象从S3 Standard或S3 Standard-LA存储类转换为S3 ntelligent-Tiering、S3

Standard-lA或S3 One Zone-lA时。将应用以下对象大小的束：

较大的对象一对于以下转换，转换较大对象具有成本效益：

从S3 Standard或S3 Standard-lA存储类转换为S3 Intelligent-Tiering.

从S3 Standard存储类转换为S3 Standard-lA或S30 ne Zone-lA.

小于128K对象：不支特上面转换方式



### 跨区域复制S3

