Configuring Amazon S3 security settings and access controls

Configuring Amazon S3 security settings and access controls > S3 Security Best Practices > Lab 2 - S3 Access G...

Lab 2 - S3 Access Grants

Amazon S3 offers a variety of security features and tools. Typically, you will use one or more of these features to grant or restrict access to your Amazon S3 resources.

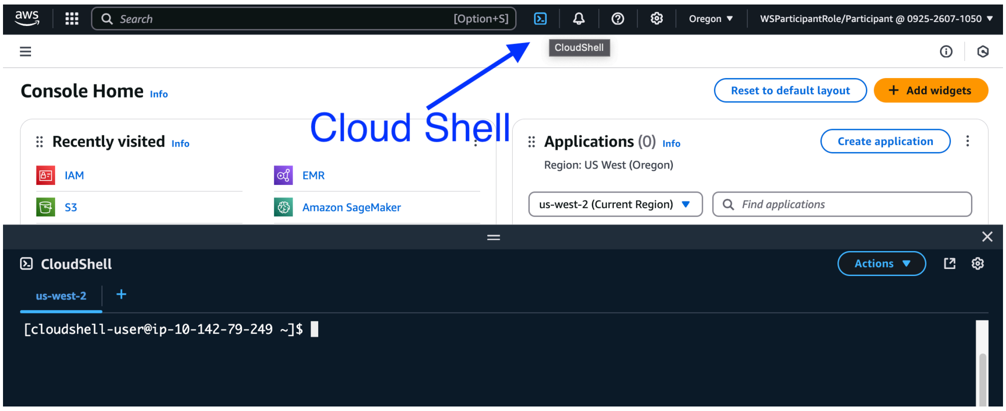
The access management tools available in Amazon S3 include:

- **Bucket Policies**: Grant other AWS accounts or AWS Identity and Access Management (IAM) identities permissions for the bucket and the objects in it.
- **Identity-based policies**: JSON-formatted policies that grant IAM identities access to your buckets or objects. You can create IAM users, groups, and roles in your account and attach access policies to them. You can then grant access to AWS resources, including Amazon S3 resources.
- **S3 Access Points**: Simplify managing data access at scale for applications that use shared datasets on S3.
- **S3 Access Grants**: Create access grants to your Amazon S3 data for both identities in corporate identity directories, such as Active Directory, and AWS Identity and Access Management (IAM) identities. S3 Access Grants helps you manage data permissions at scale.
- For completeness, while **Access control lists (ACL)** and **Object Ownership** allow defining access to your S3 objects, the majority of modern use cases in Amazon S3 no longer require the use of ACLs. Since 2011, Amazon S3 has supported IAM policies for managing access to S3 buckets. It is recommended to adopt S3 bucket policies and IAM policies and disable ACLs, which we will explore later in this security workshop.

The following exercises will show you a preview of how to configure S3 Access Grants to define granular access for personas, groups, or organizational units.

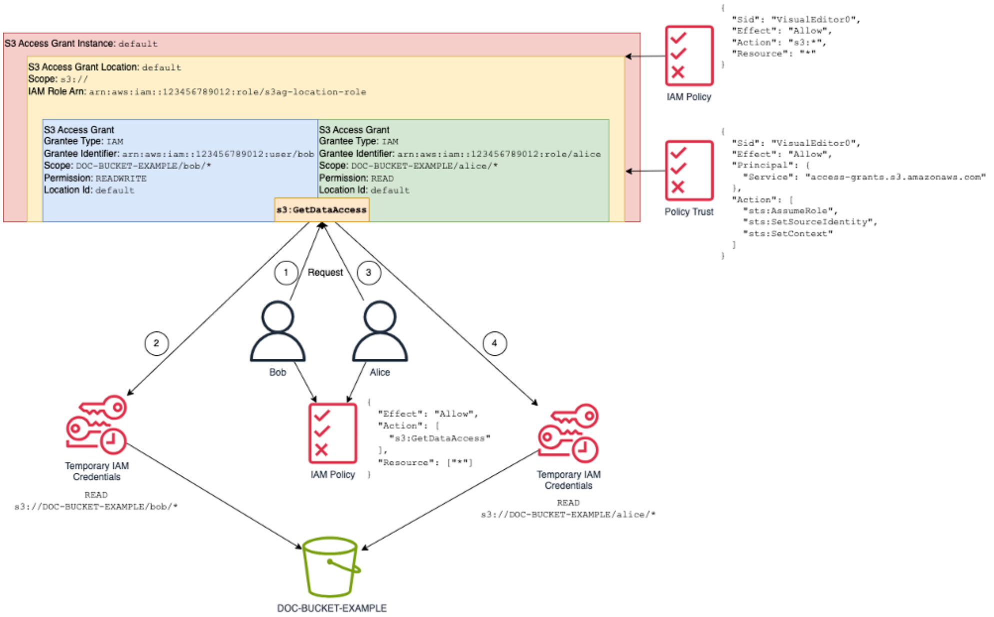
Visit S3 Access Management to deep dive on S3's security tools and features.

ⓘ For this S3 Access Grants Lab, CLI commands will be run from Cloud Shell. You can access Cloud Shell from the top middle of your AWS Console.



```
[cloudshell-user@ip-10-142-79-249 ~]$
```

You can use S3 Access Grants to manage access to your Amazon S3 data. S3 Access Grants provides a simplified model for defining access permissions to data in Amazon S3 by prefix, bucket, or object. In addition, you can use S3 Access Grants to grant access to both IAM principals and directly to users or groups from your corporate directory.



S3 Access Grant Instance: `default`

S3 Access Grant Location: `default`
Scope: `s3://`
IAM Role Arn: `arn:aws:iam::123456789012:role/s3ag-location-role`

S3 Access Grant
Grantee Type: `IAM`
Grantee Identifier: `arn:aws:iam::123456789012:user/bob`
Scope: `DOC-BUCKET-EXAMPLE/bob/*`
Permission: `READWRITE`
Location Id: `default`

S3 Access Grant
Grantee Type: `IAM`
Grantee Identifier: `arn:aws:iam::123456789012:role/alice`
Scope: `DOC-BUCKET-EXAMPLE/alice/*`
Permission: `READ`
Location Id: `default`

IAM Policy

```
{
  "Sid": "VisualEditor0",
  "Effect": "Allow",
  "Action": "s3:*",
  "Resource": "*"
}
```

Policy Trust

```
{
  "Sid": "VisualEditor0",
  "Effect": "Allow",
  "Principal": {
    "Service": "access-grants.s3.amazonaws.com"
  },
  "Action": [
    "sts:AssumeRole",
    "sts:SetSourceIdentity",
    "sts:SetContext"
  ]
}
```

IAM Policy

```
{
  "Effect": "Allow",
  "Action": [
    "s3:GetDataAccess"
  ],
  "Resource": ["*"]
}
```

s3:GetDataAccess
1
Request
3
2
4
Bob
Alice
Temporary IAM Credentials
READ
s3://DOC-BUCKET-EXAMPLE/bob/*
Temporary IAM Credentials
READ
s3://DOC-BUCKET-EXAMPLE/alice/*
DOC-BUCKET-EXAMPLE

Previous Next