AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

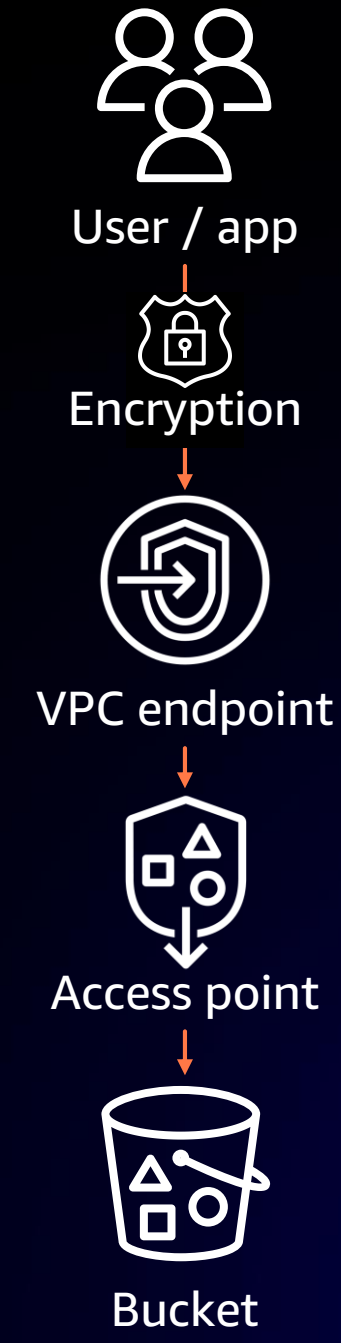
STG322-R1

Amazon S3 security patterns and anti-patterns

Vasily Pantyukhin
Principal Solutions Architect
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Let’s recall Amazon S3 security principles

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Where EPARC lives...

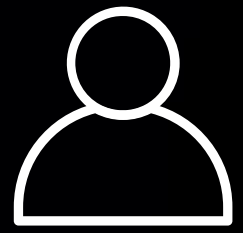
```
"Statement":[
  {
     "Effect":"Allow/Deny",
     "Principal":"arn",
     "Action":"s3:GetObject",
     "Resource":"arn",
     "Condition":{
          "condition":{"key":"value" }
      }
   }
]
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Identity-based

What can this principal do?

- Effect
- ~~Principal~~
- Action
- Resource
- Condition



Principal

- AWS accounts
- IAM users
- Roles
- AWS services
- Anonymous users

Resource-based

Who can access the S3 bucket and objects?

- Effect
- Principal
- Action
- Resource
- Condition



Resource

- Bucket
- Object

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

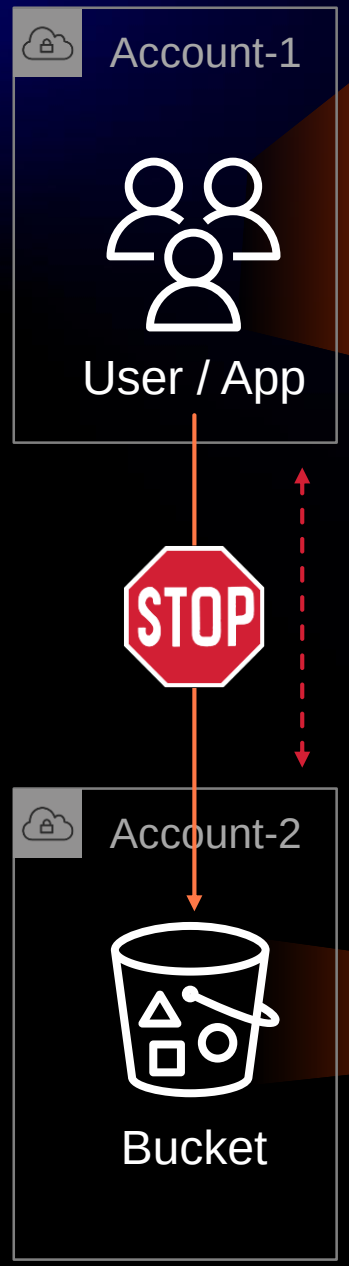



```
"Effect": "Allow",
"Action": [
    "s3:PutObject",
    "s3:GetObject"],
"Resource": "arn:aws:s3:::/reinvent21/*"
```

- Users can read and write to the bucket in the same account

Private by default

aws




```
"Effect": "Allow",
"Action": [
    "s3:PutObject",
    "s3:GetObject"],
"Resource": "arn:aws:s3:::/reinvent21/*"
```

- Users can not to read and write to the bucket in account-2

Private by default

aws



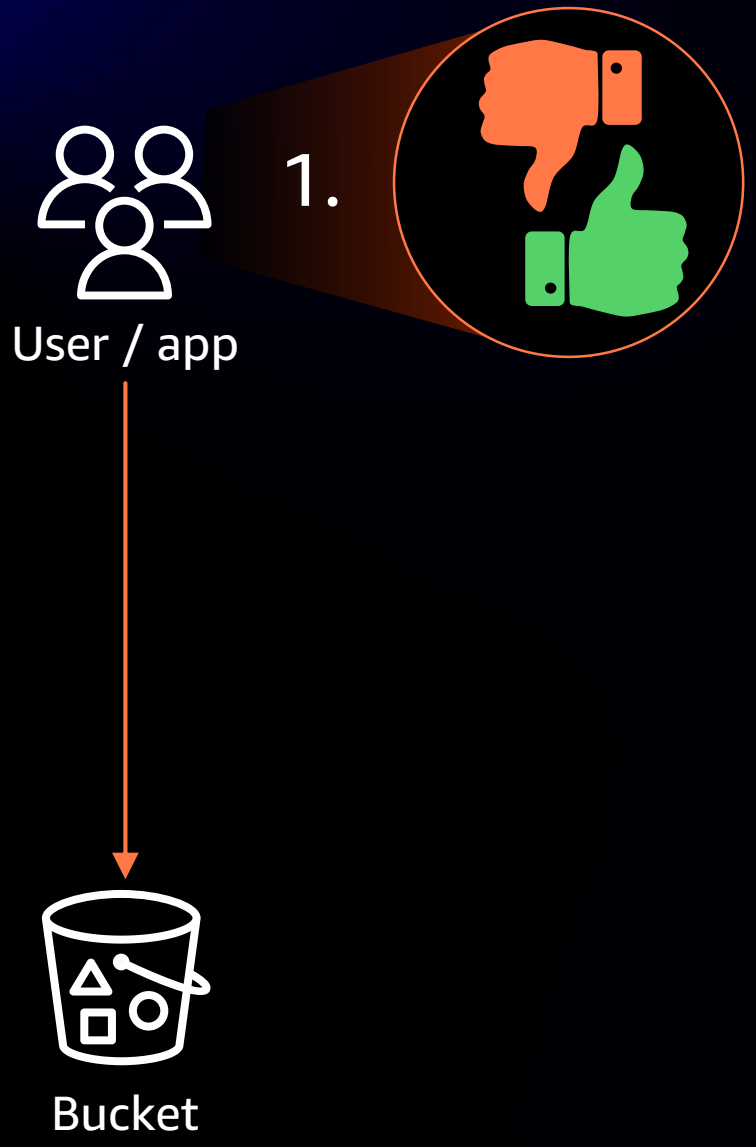

```
"Effect": "Allow",
"Action": [
    "s3:PutObject",
    "s3:GetObject"],
"Resource": "arn:aws:s3:::/reinvent21/*"
```

- Users can read and write to the bucket in account-2

```
"Effect": "Allow",
”Principal”:{"AWS":"1111111111"}
"Action": [
    "s3:PutObject",
    "s3:GetObject"],
"Resource": "arn:aws:s3:::/reinvent21/*"
```

- The bucket can be read and written by account-1

aws



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



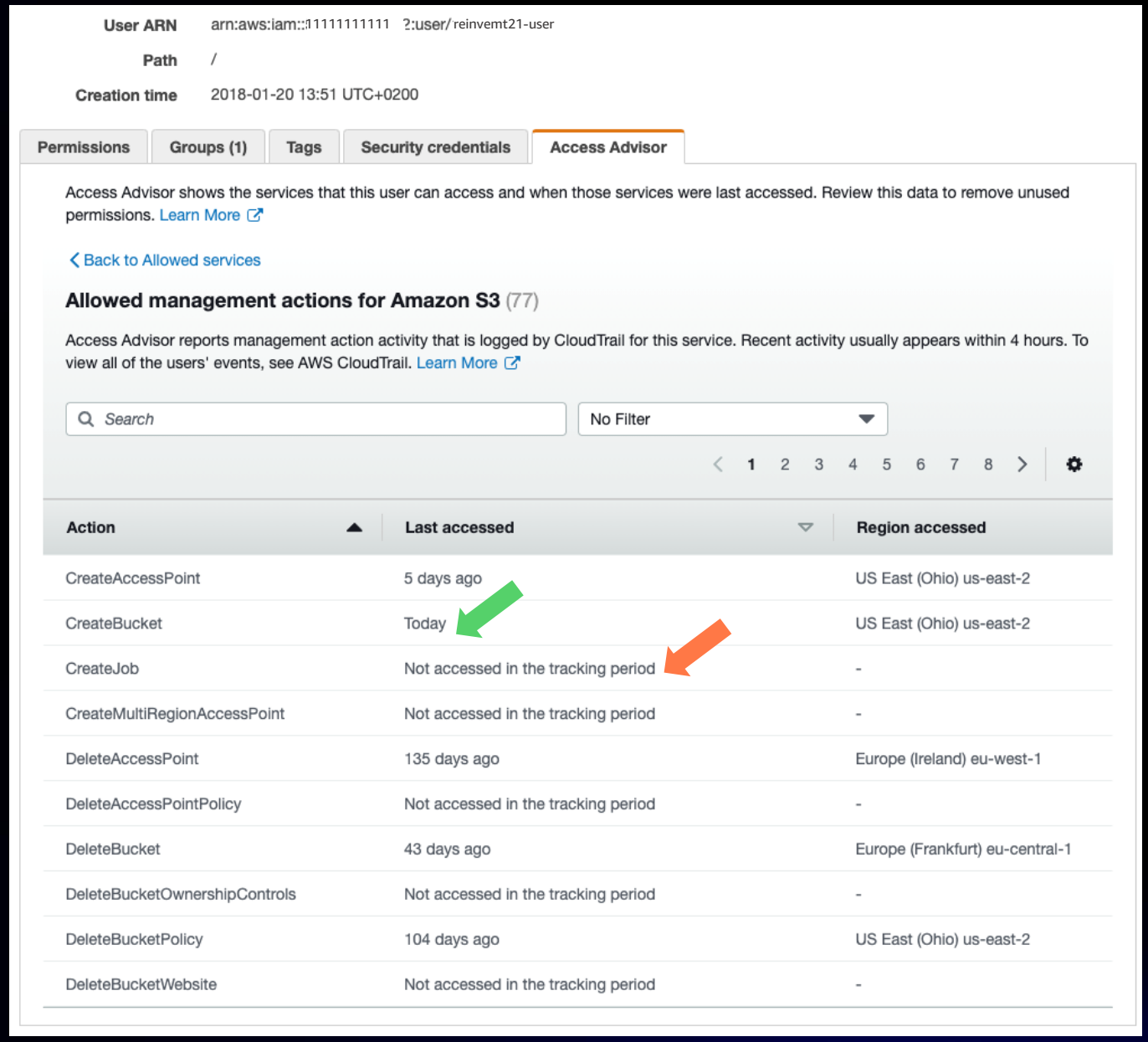
Pattern

Remove unnecessary permissions

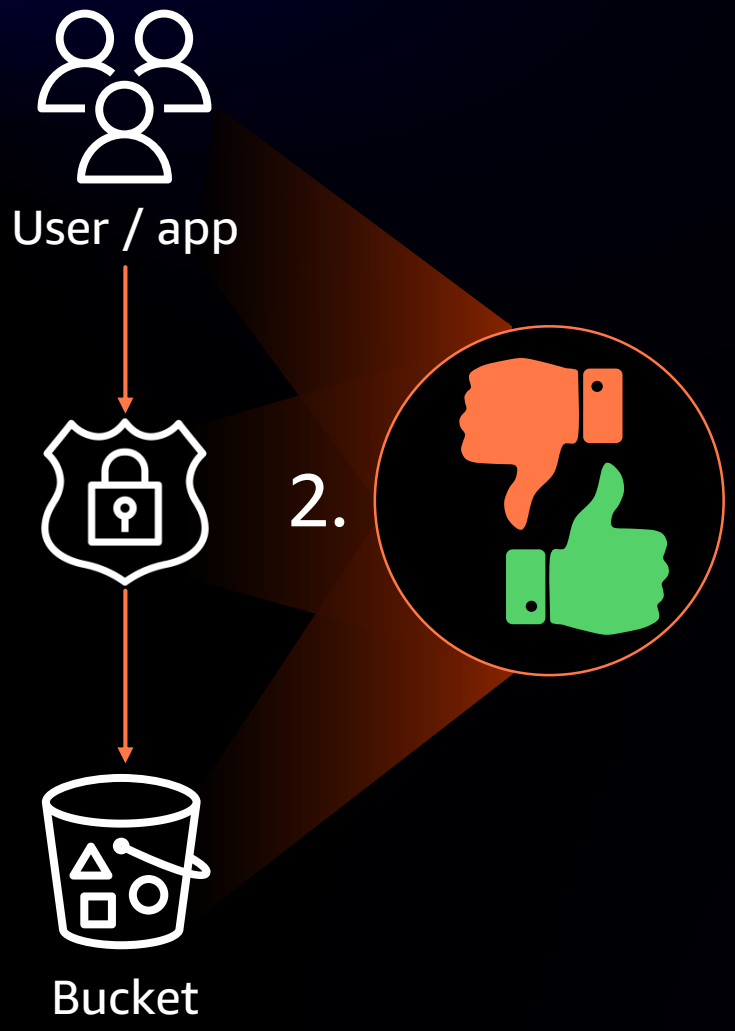
aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IAM access advisor



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Anti-pattern

Keep data unencrypted

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Client-side

- Application encrypts data before sending data to S3 and decrypts data after retrieving it from S3
- AWS never knows the encryption keys



In transit

```
"Effect": "Deny",
"Principal": "*",
"Action": "s3:GetObject",
"Resource": "arn:aws:s3:::reinvent21/*",
"Condition": {"Bool": { "aws:SecureTransport": "false"} }
:
"Effect": "Allow",
"Principal": "*",
"Action": "s3:GetObject",
"Resource": "arn:aws:s3:::reinvent21/*",
"Condition": { "StringEquals": {"s3:TlsVersion": "1.2"} }
```



At rest

- Data is transparently encrypted on the S3 side and decrypted back when requested
  - SSE-S3 – keys are managed by AWS
  - SSE-KMS – keys are managed by AWS Key Management Service (AWS KMS)
  - SSE-C – keys are passed to AWS to handle each encryption (write) or decryption (read) request; AWS doesn't store these keys

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

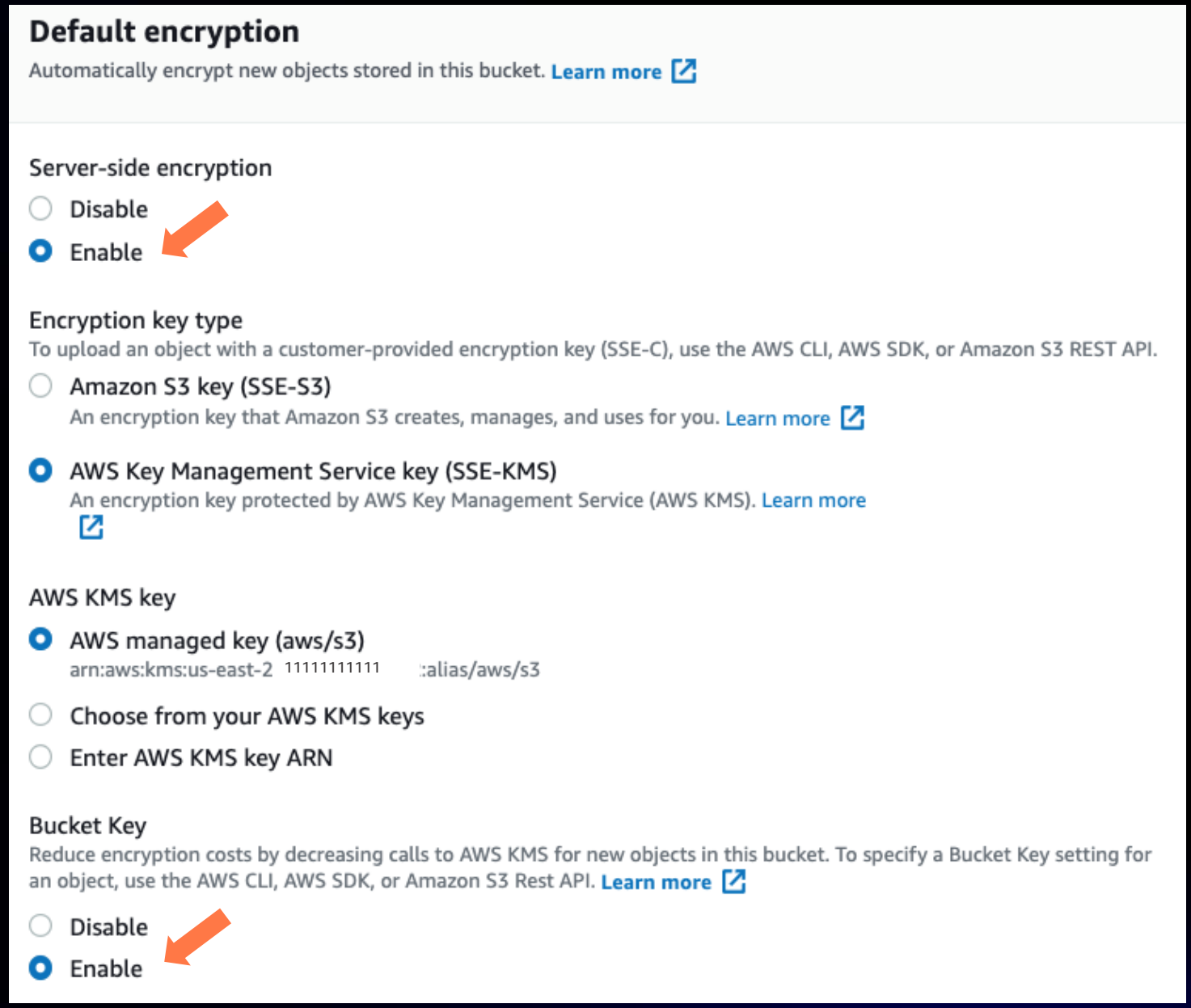


Pattern

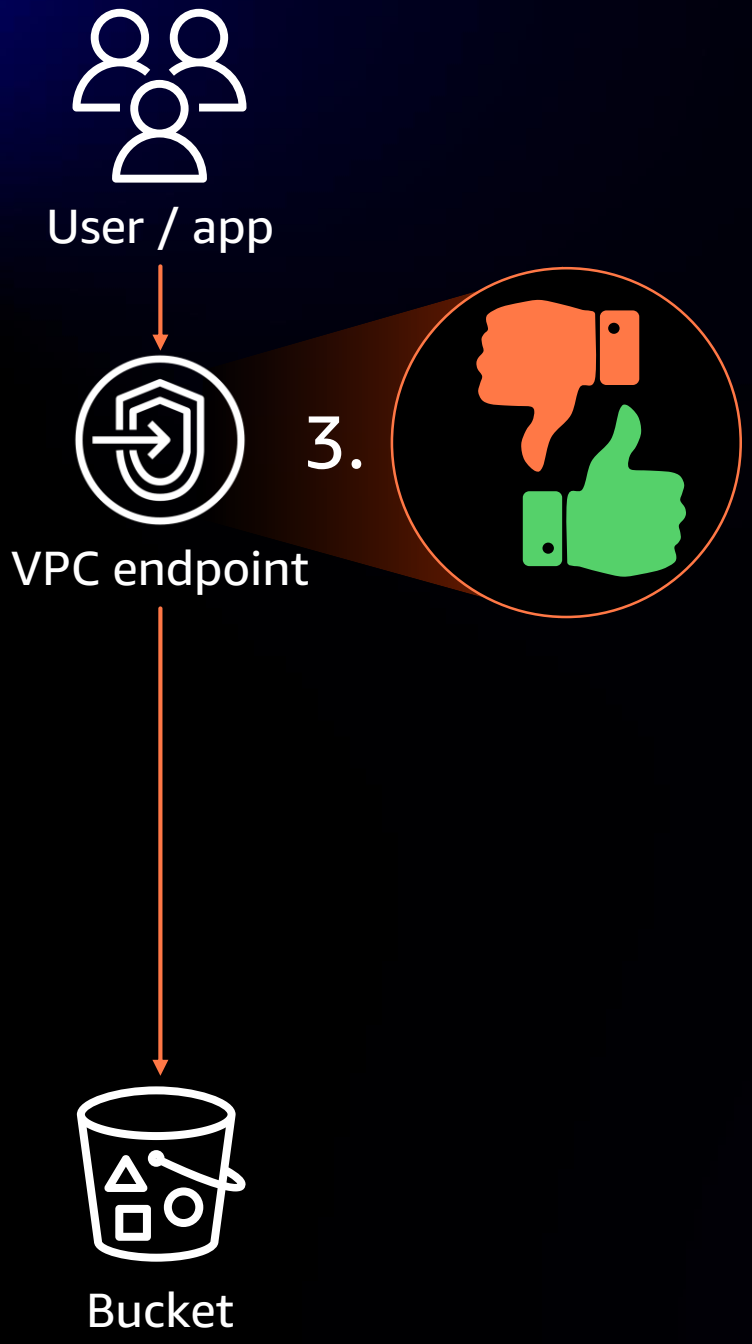
Use bucket key

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Inexpensive at-rest encryption (↓$ by 99%)



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



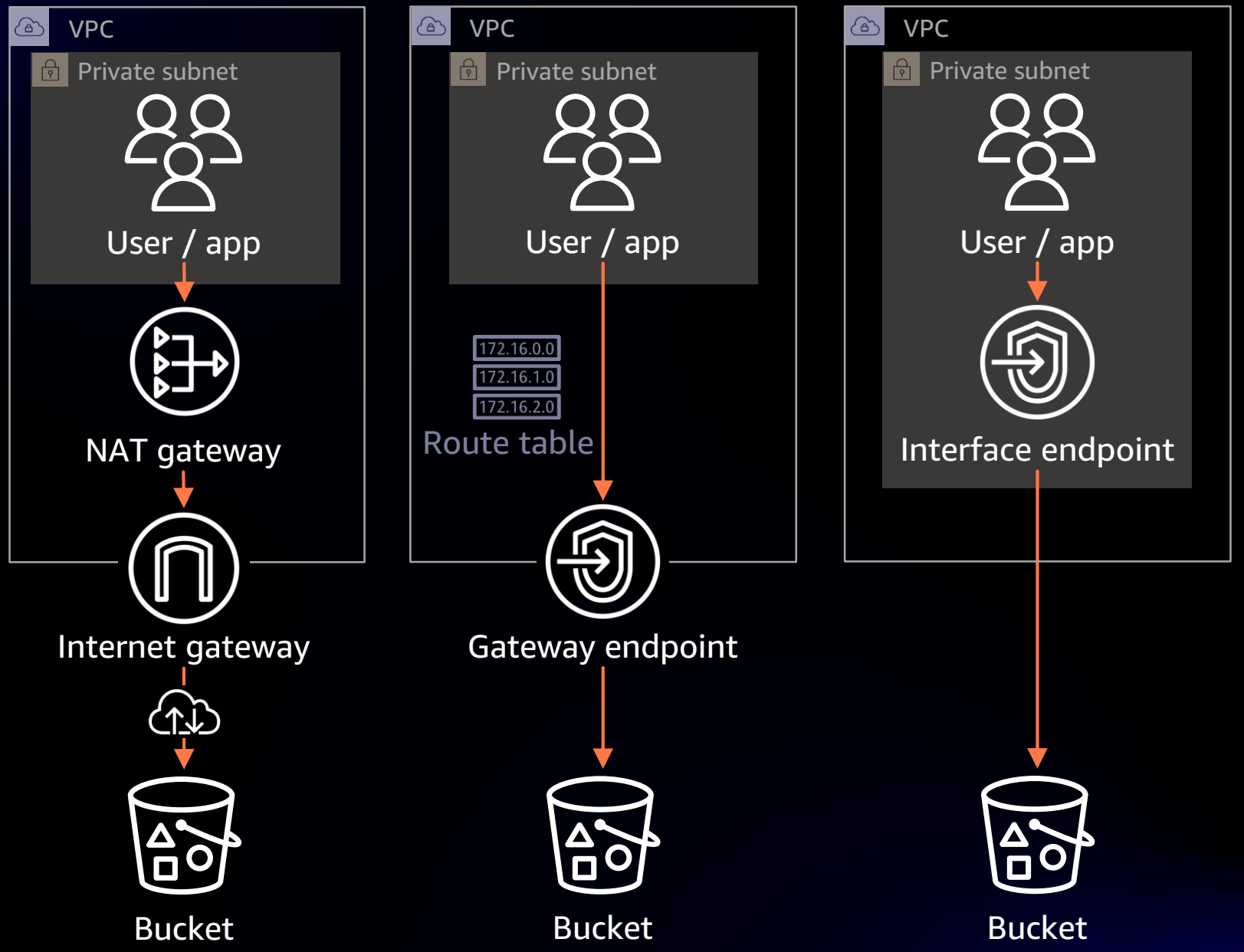
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Anti-pattern

Default access to S3 within VPC

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



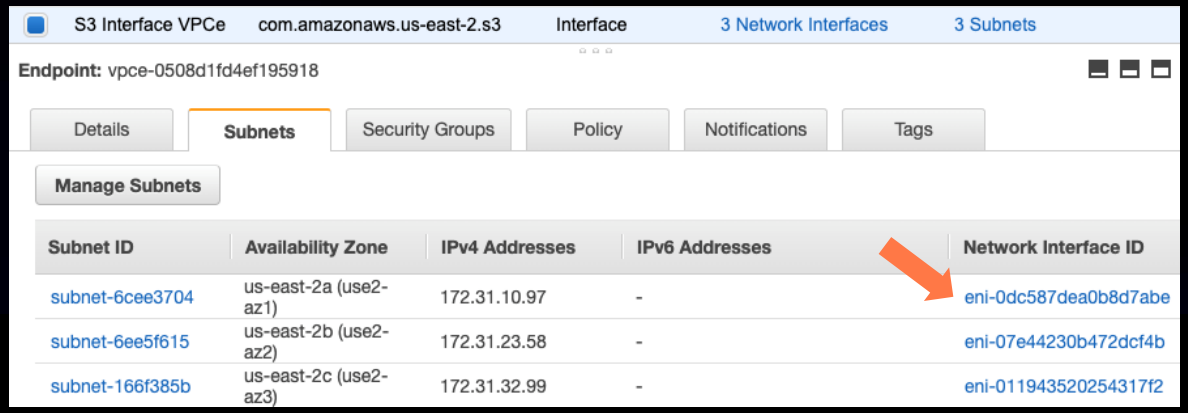
Gateway endpoint



Interface endpoint

Clients use public S3 IPs	Clients use IPs from your VPC
The route table for your VPC is updated so that all S3 requests go through the endpoint	DNS records in your VPC are updated so that all S3 requests go through the endpoint
No support for cross-Region requests or on-premises applications	Support for cross-Region requests or on-premises applications via VPN or AWS Direct Connect private VIF
Free	Paid



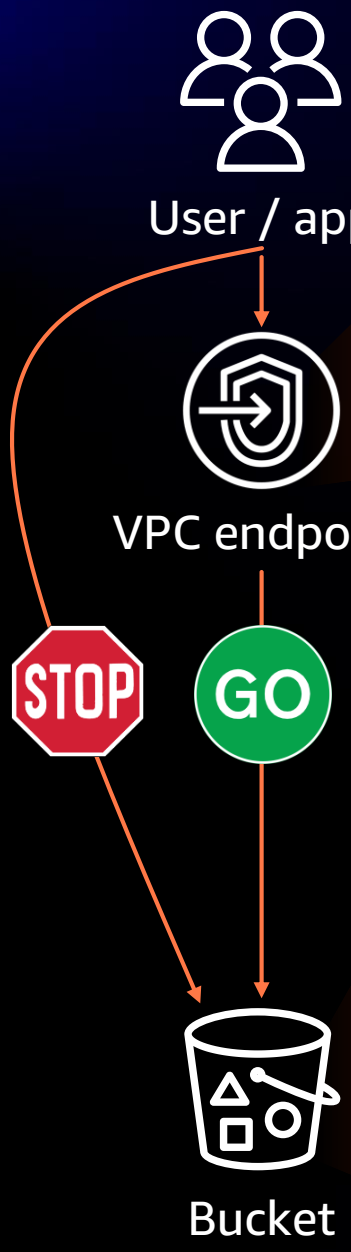




Pattern

Allow access via VPCe only

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



- Who can connect to the S3 bucket using this VPCe?"
- Does not provide access to the bucket by itself

```
"Effect": "Allow",
"Principal": {"AWS": "*"},
"Action": "s3:*",
"Resource": ["arn:aws:s3::: reinvent21 ", "arn:aws:s3::: reinvent21/*"],
"Condition": {"StringEquals":
        {"s3:ResourceAccount": "11111111111"} }
```

- Which VPC endpoint must be used to access these S3 buckets?
- Deny all actions not coming through specific VPC endpoint

```
"Effect": "Deny",
"Principal": "*",
"Action": "s3:*",
"Resource": ["arn:aws:s3:::reinvent21", "arn:aws:s3:::reinvent21/*"],
"Condition": {"StringNotEquals":
        { "aws:sourceVpce":"vpce-1a2b"} }
:
"Effect": "Allow",
"Principal": "*",
"Action": "s3:*",
"Resource": ["arn:aws:s3:::reinvent21", "arn:aws:s3:::reinvent21/*"],
"Condition": {"StringEquals": { "aws:sourceVpce":"vpce-1a2b"} }
```

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



But…

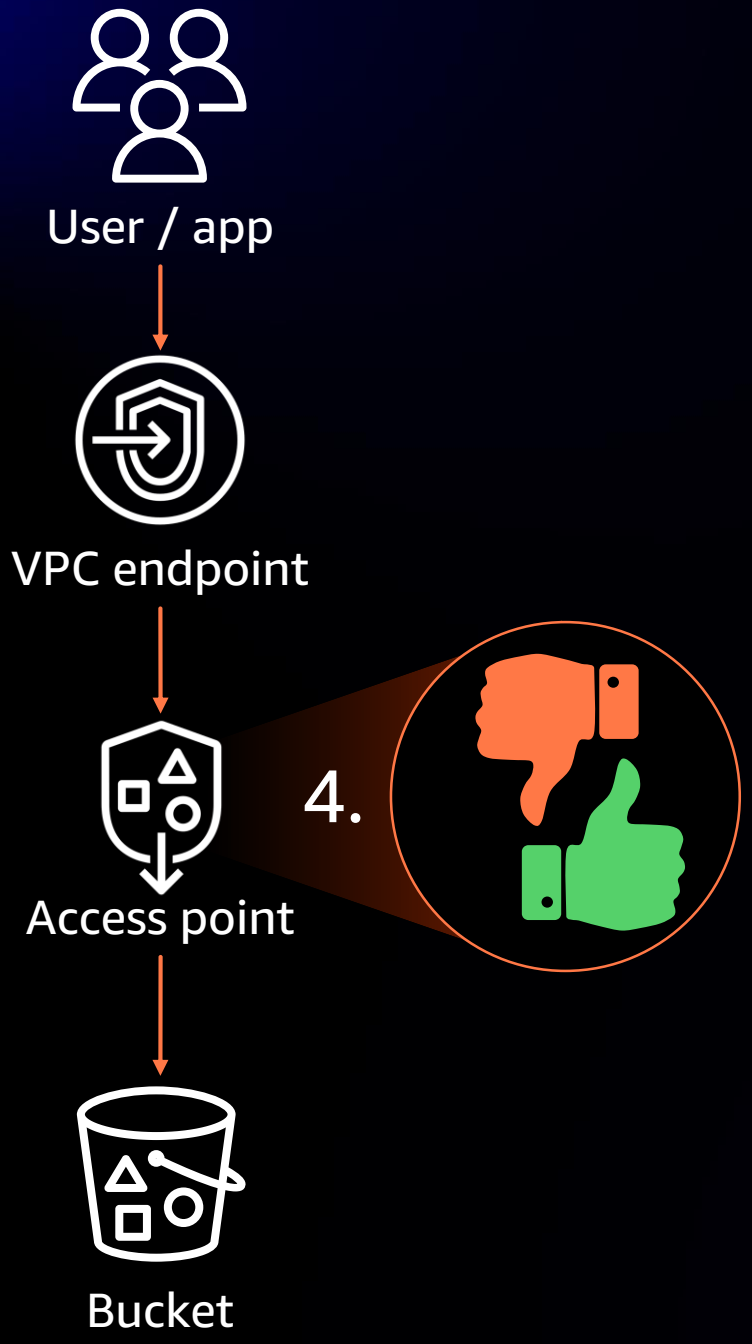
Be careful with conditional denies

```
"Effect": "Deny",
"Principal": "*",
"Action": "s3:*",
"Resource": ["arn:aws:s3:::reinvent21",
"arn:aws:s3:::reinvent21/*"],
"Condition": {"StringNotEquals":
                {"aws:sourceVpce":"vpce-1a2b"}
}
```

- Double-check VPCe ID; otherwise, you'll lose access to the bucket
- Console requests are not from specific VPCe; you'll lose console access to the bucket
- Also, you'll break Cross-Region Replication

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



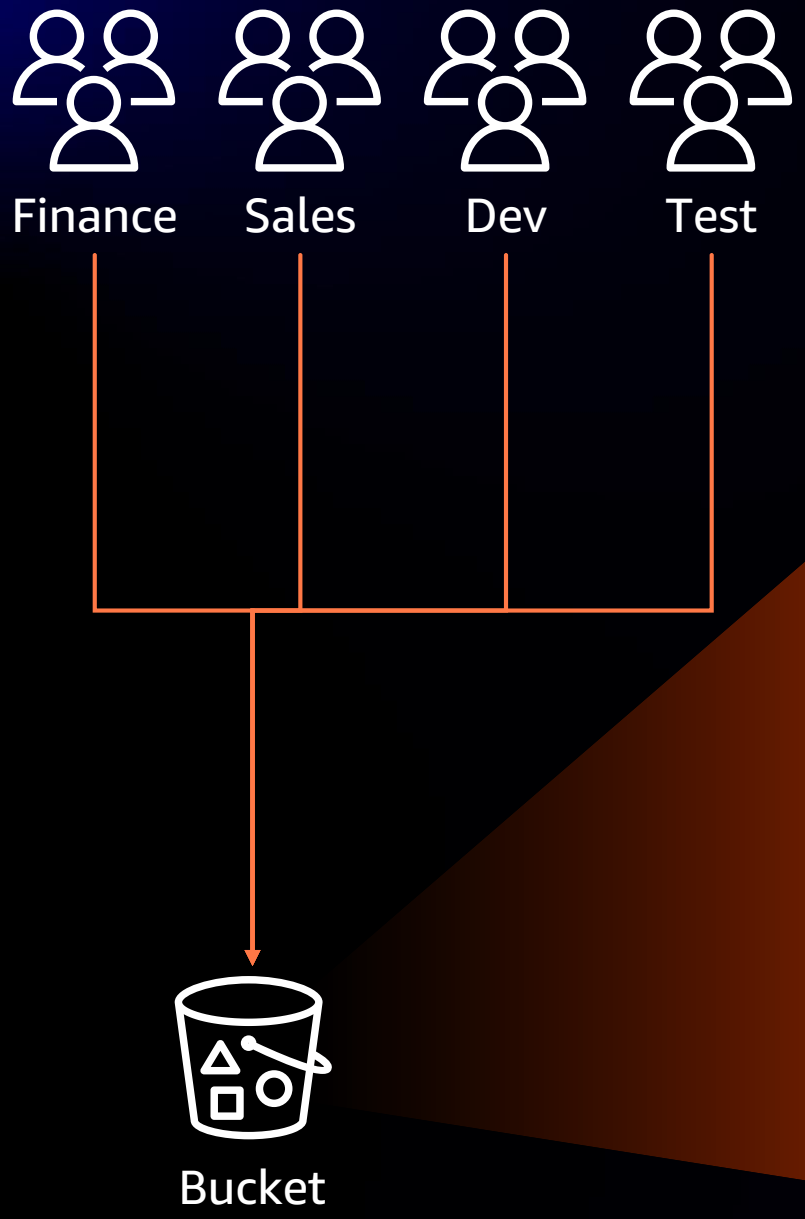
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Anti-pattern

Use single bucket policy with shared datasets

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



- More effort to maintain
- More sensitive to mistakes

```
"Effect":"Allow",
"Principal":{"AWS":"arn:aws:iam::12345:role/Finance"},
"Action":["s3:GetObject"],
"Resource":"arn:aws:s3:::reinvent21/Fin/*”
:
"Principal":{"AWS":"arn:aws:iam::12345:role/Sales"},
"Resource":"arn:aws:s3:::reinvent21/Sale/*”
:
"Principal":{"AWS":"arn:aws:iam::12345:role/Dev"},
"Resource":"arn:aws:s3:::reinvent21/Dev/*”
:
"Principal":{"AWS":"arn:aws:iam::12345:role/Test"},
"Resource":"arn:aws:s3:::reinvent21/Test/*”
:
```

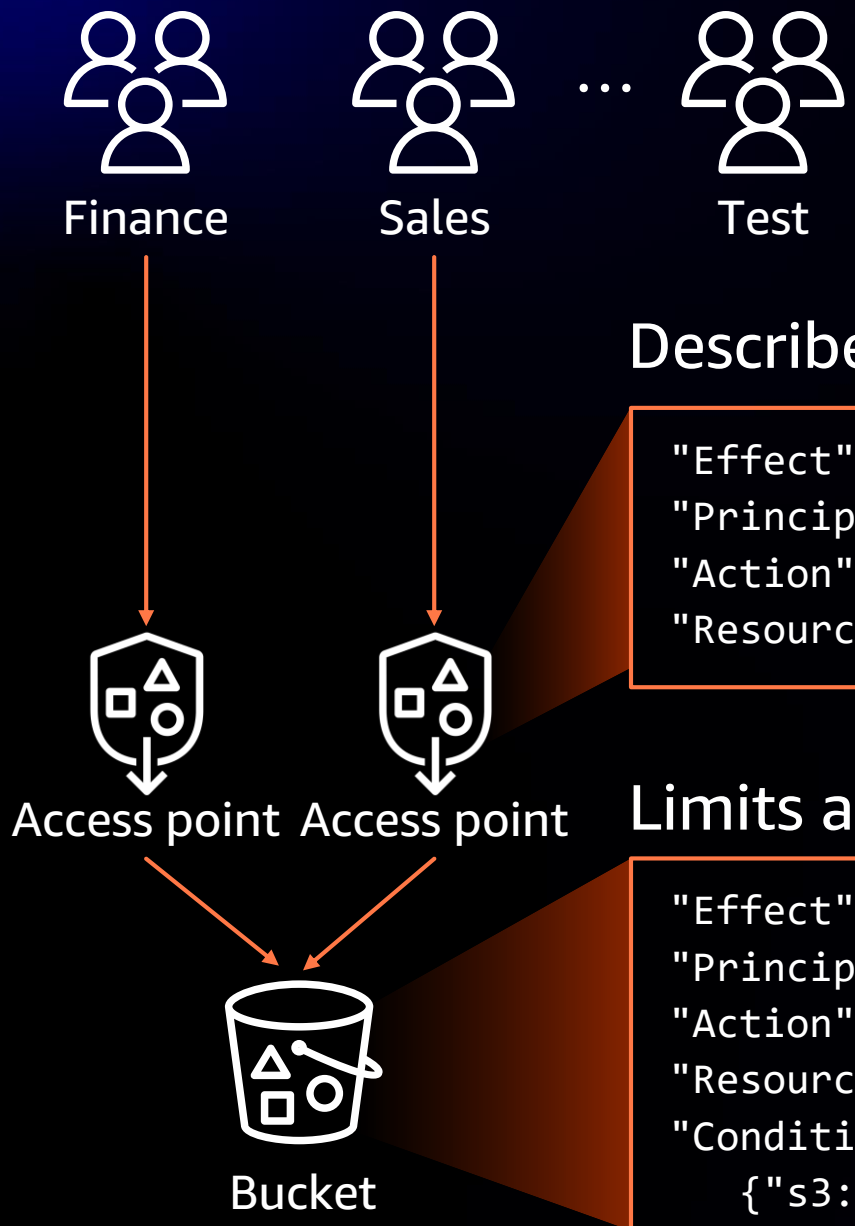
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Pattern

Use access point policies for granular control

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Describe access rules to different roles individually

```
"Effect": "Allow",
"Principal": {"AWS":"arn:aws:iam::12345:role/Sales"},
"Action": ["s3:GetObject", "s3:PutObject"],
"Resource": "arn:aws:s3:us-west-2:123:accesspoint/reinvent21-ap/object/*”
```

Limits access via access points only

```
"Effect": ”Allow",
"Principal": "*",
"Action": "s3:*",
"Resource": ["arn:aws:s3:::reinvent21","arn:aws:s3:::reinvent21/*"],
"Condition":{"ArnLike":
   {"s3:DataAccessPointArn": "arn:aws:s3:us-west-2:123:accesspoint/*”} }
```

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



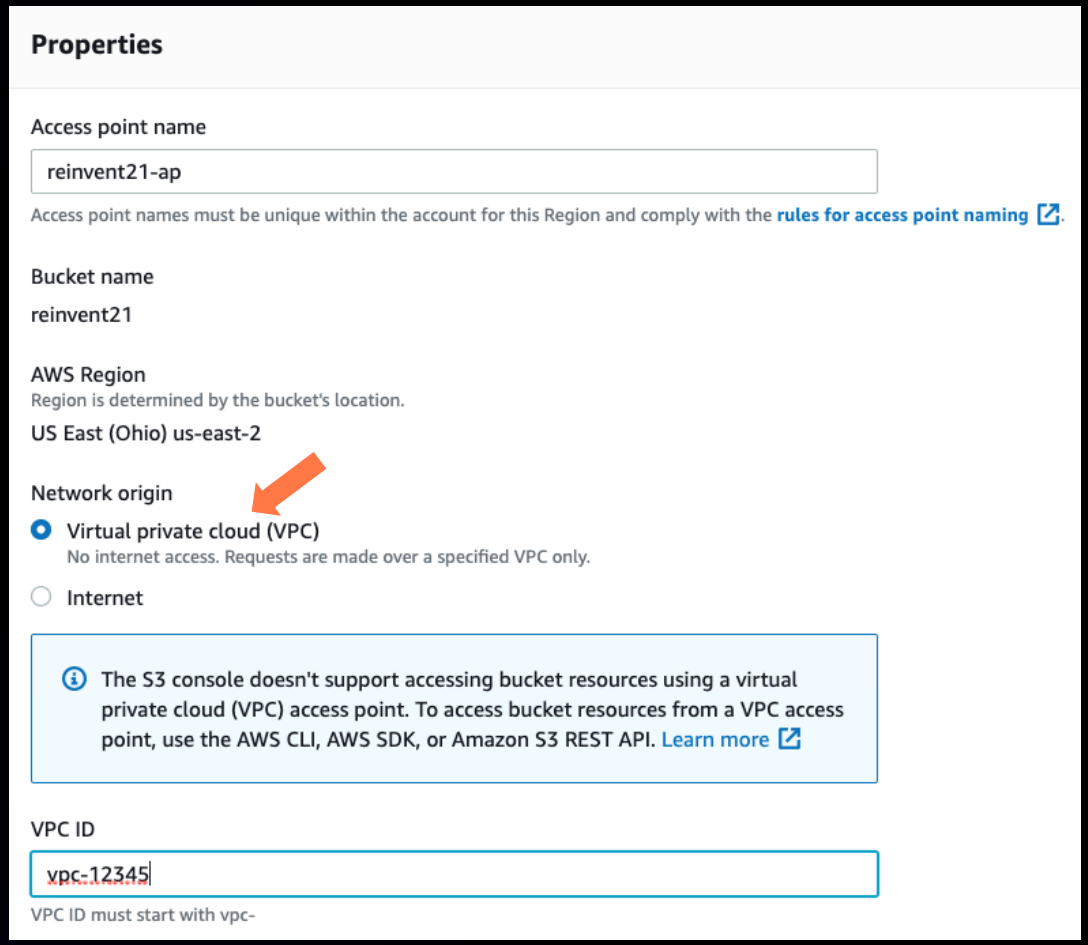
Pattern

Do not expose a bucket outside of VPC

without real need

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Limit S3 storage access by VPC subnets only

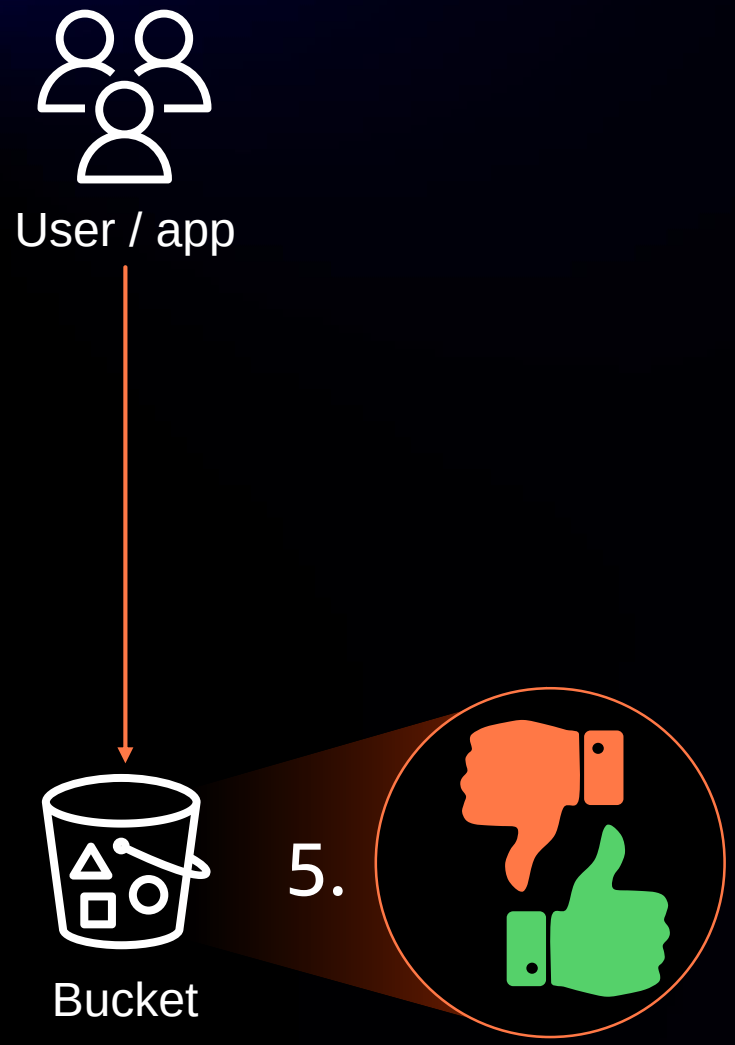


Use service control policies (SCPs) to ensure all access points are VPC-restricted

```
"Effect": "Deny",
"Action": ”s3:CreateAccessPoint",
"Resource": "*",
"Condition":
  {"StringNotEqualsIfExists":
    {”s3:AccessPointNetworkOrigin":”vpc”} }
```

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



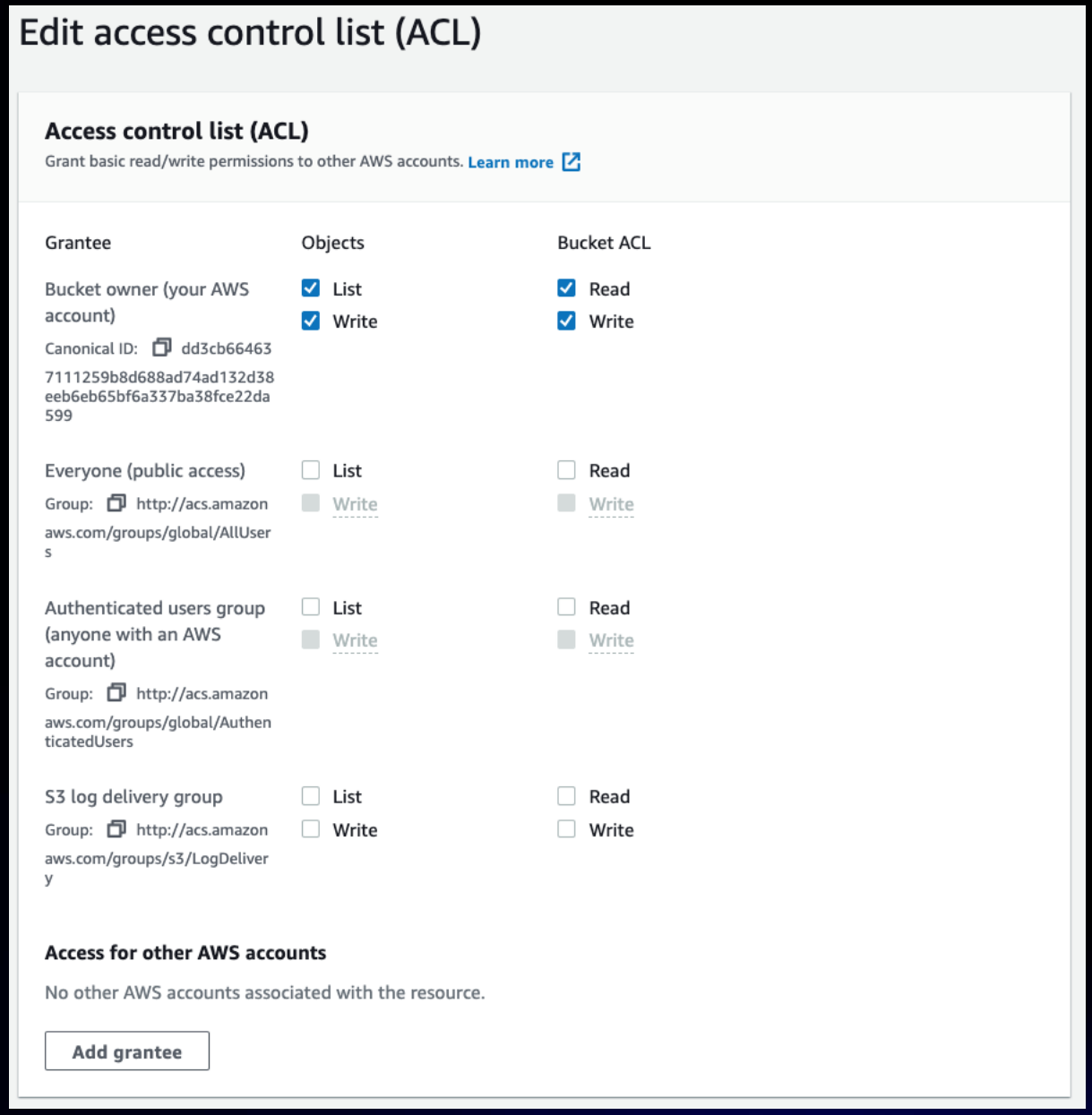
Anti-pattern

Using ACLs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Access control lists (ACLs)

- ACLs only grant access (cannot explicitly deny)
- Finite set of permissions compared to policies



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Pattern

Using bucket policy

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Easy to configure appropriate policies

ACL permission	Bucket access policy	Object access policy
READ	s3:ListBucket, s3:ListBucketVersions, s3:ListBucketMultipartUploads	s3:GetObject, s3:GetObjectVersion
WRITE	s3:PutObject, s3:DeleteObjectVersion	NA
READ_ACP	s3:GetBucketAcl	s3:GetObjectAcl, s3:GetObjectVersionAcl
WRITE_ACP	s3:PutBucketAcl	s3:PutObjectAcl, s3:PutObjectVersionAcl
FULL_CONTROL	READ + WRITE + READ_ACP + WRITE_ACP ACLs	READ + READ_ACP + WRITE_ACP ACLs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



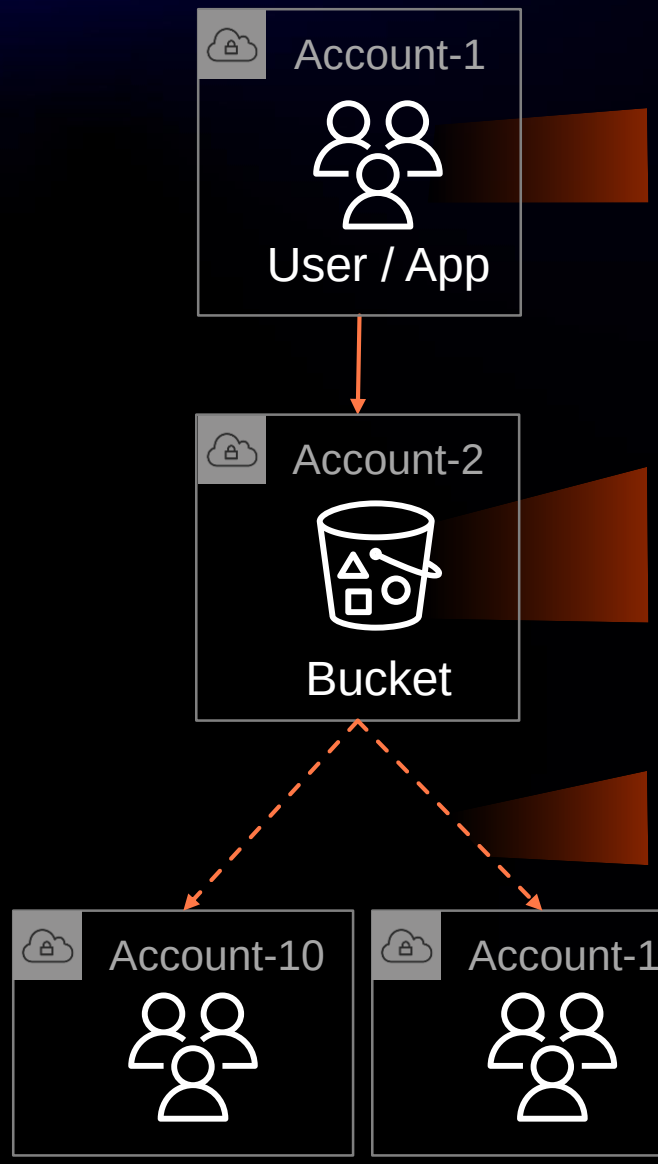
Pattern

Enforcing object ownership
for cross-account

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How cross-account write works today

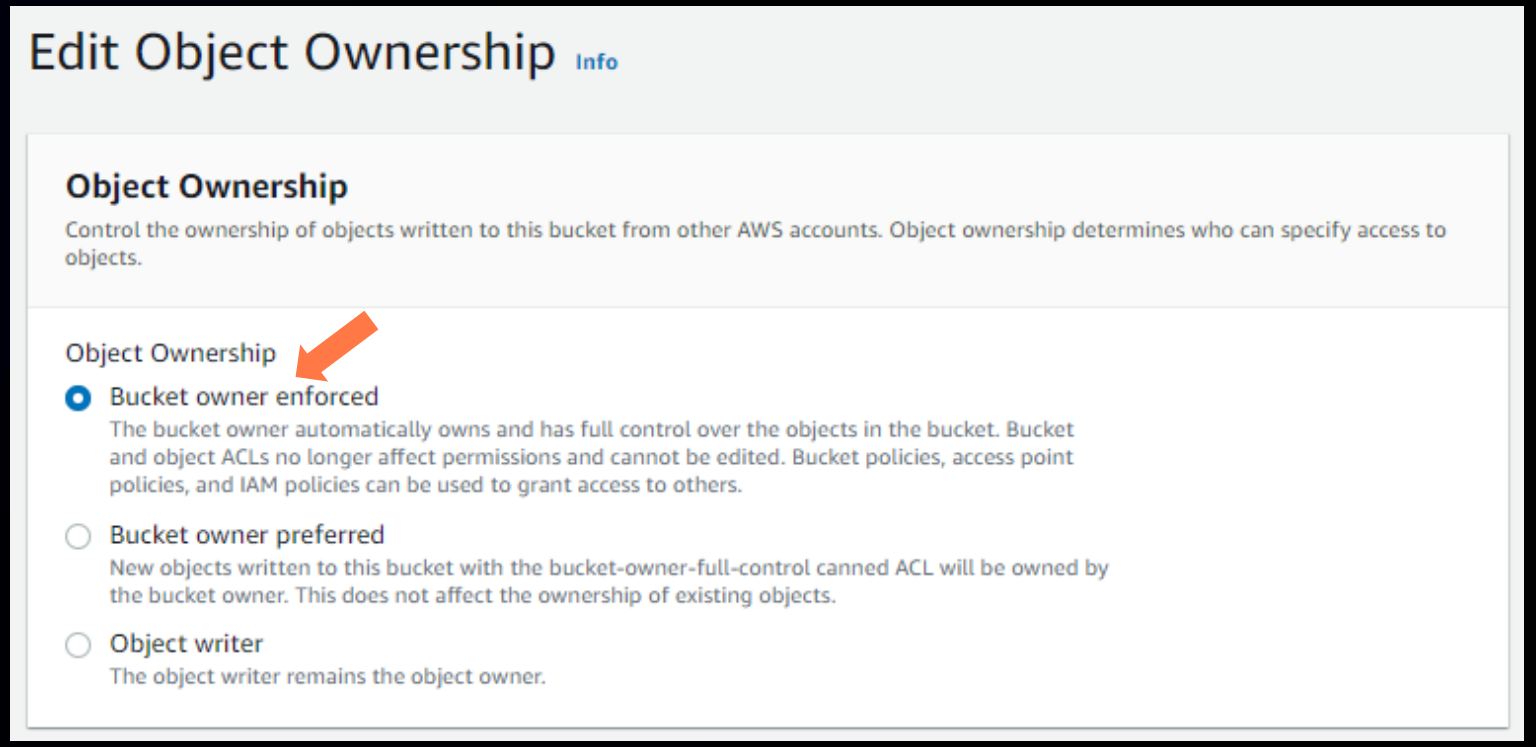


1. Give permission via ACL

2. Objects are are owned by Account-1
Account-2 cannot use bucket policy to give other accounts access

3. Give permission via ACL

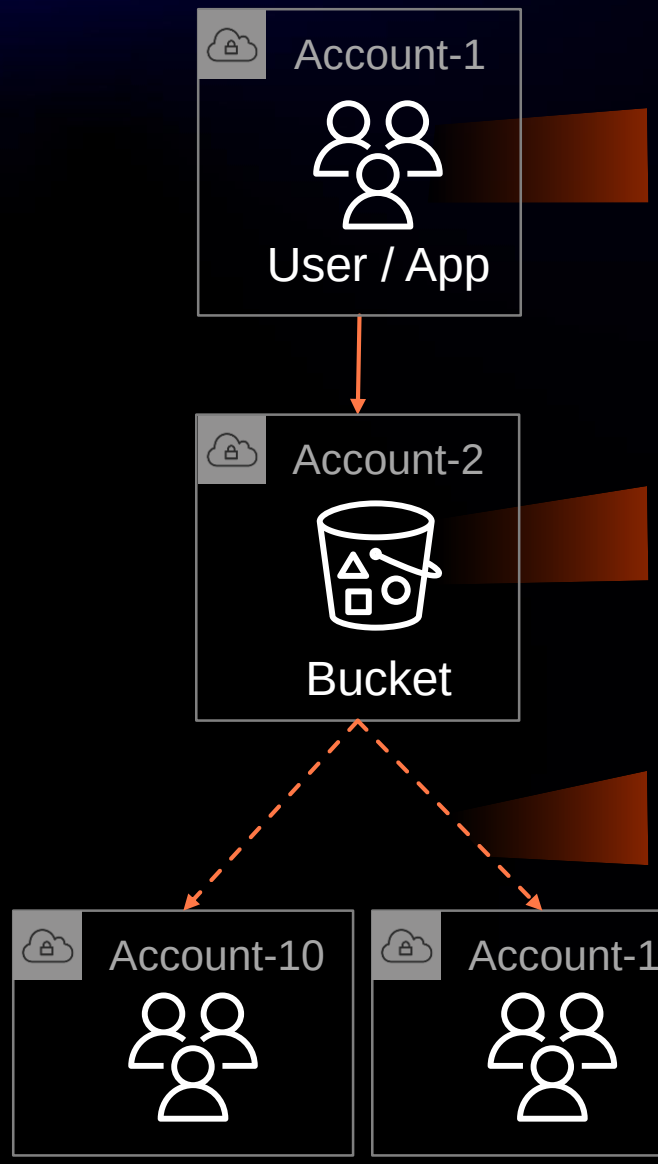
Every object in your bucket is owned by you



- ACLs are disabled and no longer used to grant permission
- Can be applied to a new or existing bucket
- Can be turned off at any time – previous ACLs will be restored

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How cross-account write works today



1. No need to specify ACL for cross-account write
2. All objects are owned by you
3. Use bucket policy to control access for all objects



Anti-pattern

Allow public access
without real need

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Public = NOT Not-public

Not-public are:

- ACLs with grantees NOT All Users or Any Authenticated User
- Any NOT-wildcarded Principal, SourceIp, SourceArn, SourceVpc, SourceVpce, SourceOwner, aws:userid, SourceAccount, DataAccessPointArn, or KMS-encrypted

Public

```
"Effect": "Allow",
"Principal": "*",
"Action": "s3:PutObject",
"Resource":"arn:aws:s3:::reinvent21/*"
"Condition":
  { "StringLike":
    {"aws:SourceVpc": "vpc-*"}
  }
```

Not-public

```
"Effect": "Allow",
"Principal": "*",
"Action": "s3:PutObject",
"Resource":"arn:aws:s3:::reinvent21/*"
"Condition":
  { "StringLike":
    {"aws:SourceVpc": "vpc-12345"}
  }
```

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



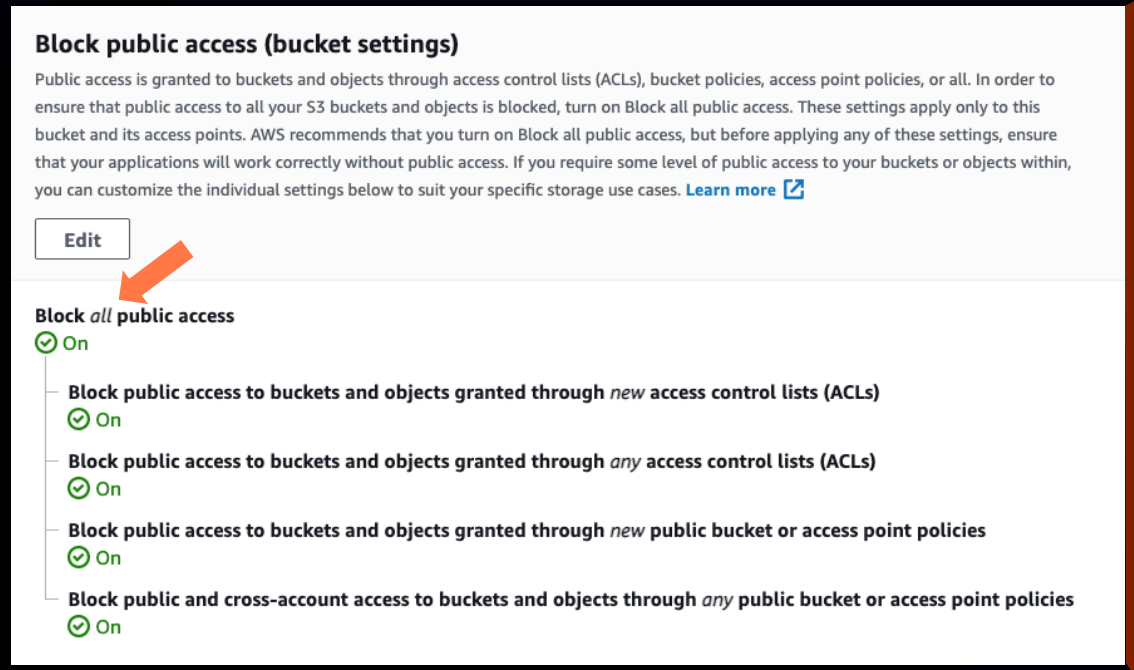
Pattern

Block public access

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Block public access

BUCKET, ACCESS POINT, ACCOUNT



- BlockPublicAcls
  - Block assigning new public ACLs for bucket and objects
  - Block creating new buckets and objects with public ACLs
  - Doesn't affect existing policies or ACLs
- IgnorePublicAcls
  - Block existing public ACLs on bucket and objects
  - Doesn't prevent new public ACLs
- BlockPublicPolicy
  - Block assigning new public bucket policies
  - Doesn't affect existing bucket policies
- RestrictPublicBuckets
  - Block whole existing public bucket policy, including non-public delegation
  - Restrict access to only AWS service principals and authorized users within account

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Anti-pattern

Mix public and private data in the same bucket

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

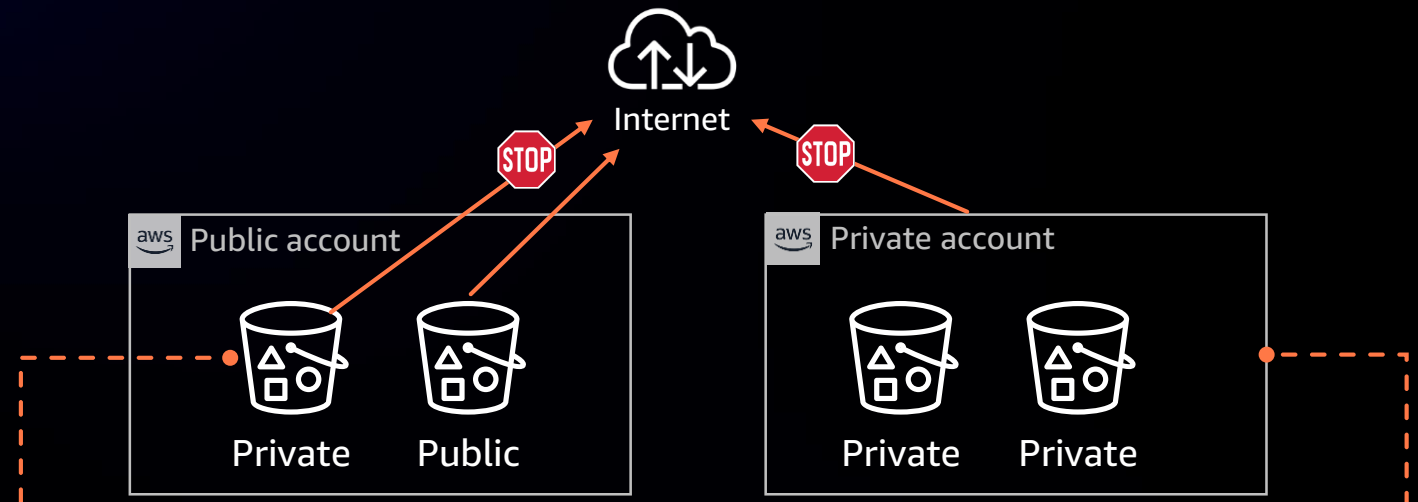


Pattern

Separate public and private data in different accounts

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Block public access to buckets and accounts



Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

Edit

Block *all* public access
On

- **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  On
- **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  On
- **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  On
- **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
  On

Block Public Access settings for this account

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply account-wide for all current and future buckets and access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects, you can customize the individual settings below to suit your specific storage use cases. Learn more

- **Block *all* public access**
  Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
  - **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
    S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
  - **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
    S3 will ignore all ACLs that grant public access to buckets and objects.
  - **Block public access to buckets and objects granted through *new* public bucket or access point policies**
    S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
  - **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
    S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

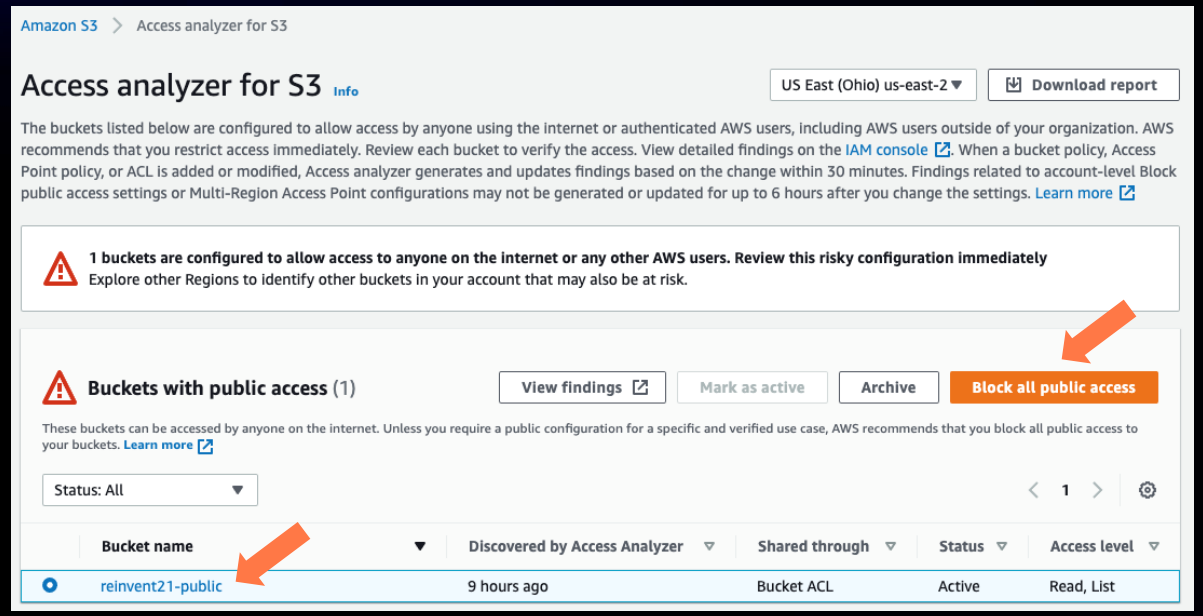


Anti-pattern

Trust yourself

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Access Analyzer for S3



Are your buckets public or do they provide cross-account access?

- It is free
- Everyone should run this at least once

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Summary

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



User / app

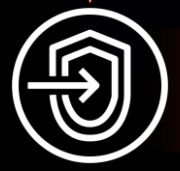
1.

- Check unnecessary permissions with IAM access advisor



2.

- Encrypt data in transit



VPC endpoint

3.

- Manage private data flow with gateway and interface VPC endpoints
- Allow access via VPC endpoints only *(when reasonable)*



Access point

4.

- With shared datasets, use access points
- Do not expose buckets outside of VPC *(when reasonable)*



Bucket

5.

- Check public access with Access Analyzer for S3
- Block public access
- Separate public and private data in different buckets
- Use bucket policy instead of ACLs *(when reasonable)*
- Minimize cost of at-rest encryption using bucket key
- Enforcing object ownership

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Vasily Pantyukhin

vspan@amazon.lu

https://bit.ly/awsgalaxy



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.