
AWS
re:Invent

SEC206

Getting started with AWS identity services

Becky Weiss

Senior Principal Engineer

AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Principles of identity in Amazon Web Services

Authentication for human users

Authentication for applications in AWS

Authorization – how to read and write AWS Identity and Access Management (IAM) permission policies

➔ This session is for builders



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

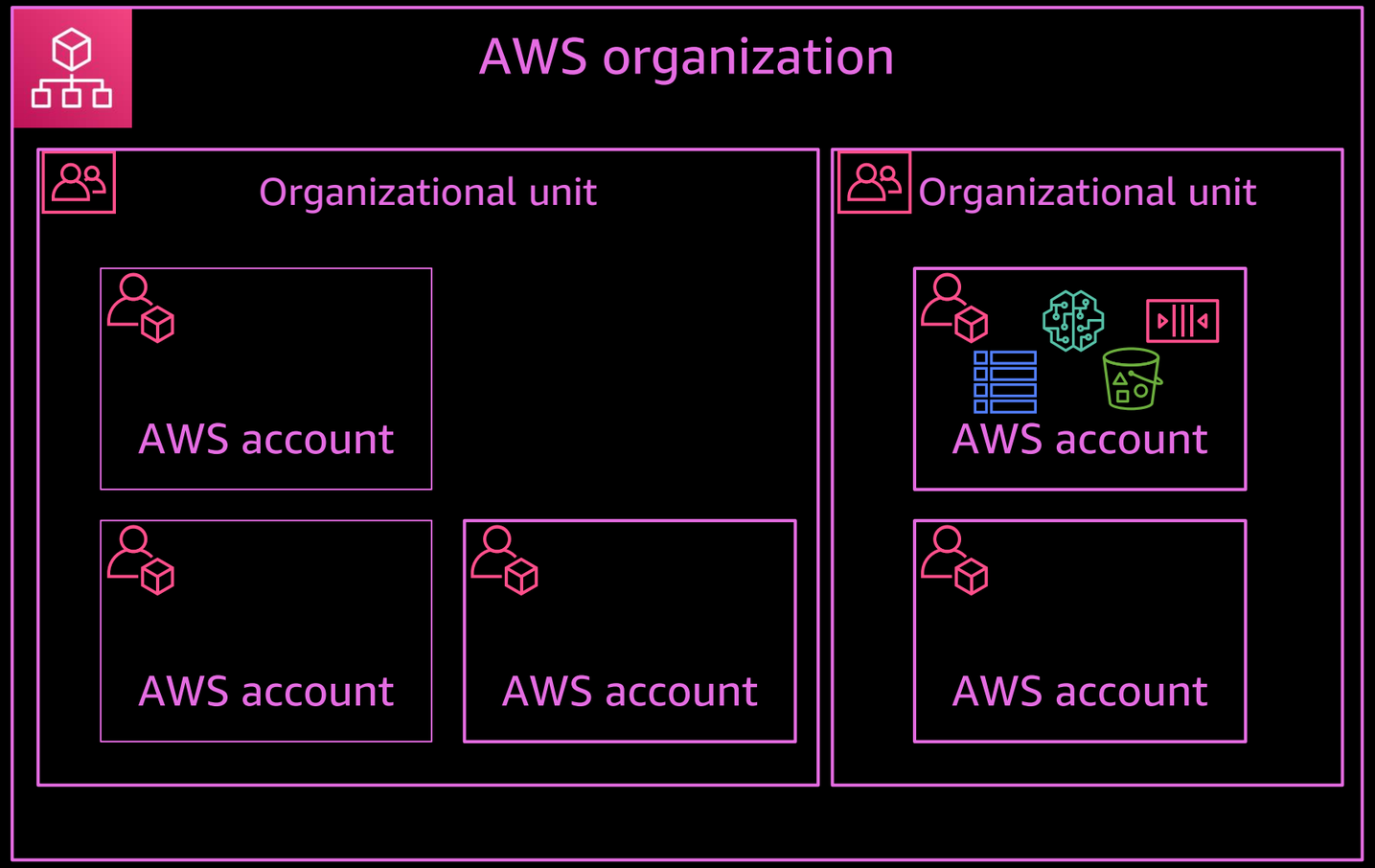
The fundamentals: Accounts, AWS Organizations, and IAM



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Terminology: Account and organization



Use AWS Organizations for

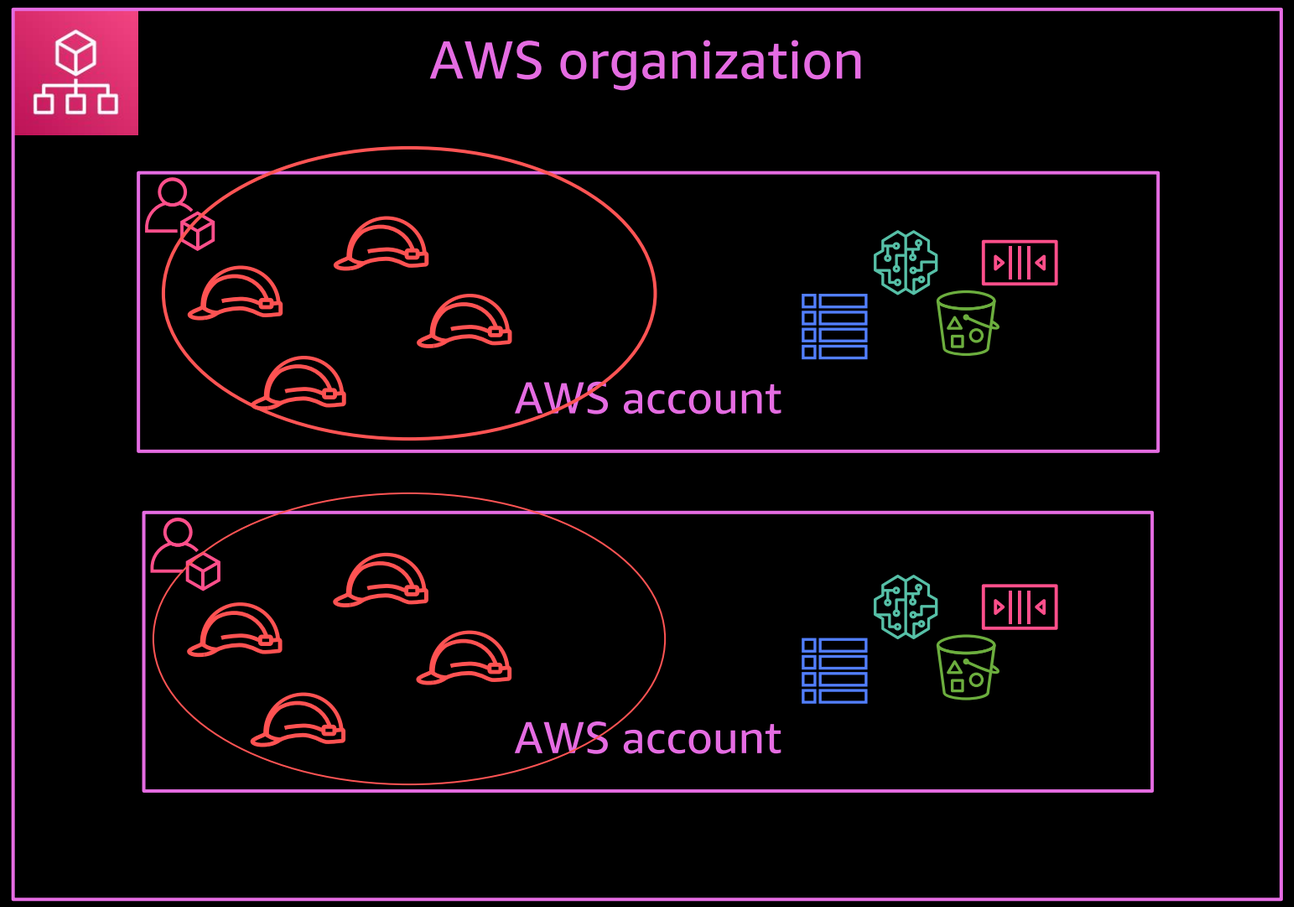
- Billing – single payer
- Management – for managing AWS services at scale
- **Security invariants – service control policies**

AWS's API identity system: IAM

Each AWS account has its own pool of identities

- IAM roles
  - Authenticated with short-term credentials
  - Used in a variety of scenarios
- IAM users

  Authenticated with long-term credentials
- IAM identities are given permissions (policies)



Identities for humans



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

If you're starting today: AWS Single Sign-On



Choosing an identity strategy for humans

AWS Single Sign-On

- Create a user pool directly in AWS SSO, or
- Use a supported identity provider, such as Azure Active Directory, Okta, or OneLogin

Identity providers with SAML 2.0 support, such as Active Directory Federation Services, can be configured to provide direct federation to IAM roles

Custom federation solutions – build a federation solution using the AWS Security Token Service (AWS STS) API

IAM users

Identities for applications



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IAM roles for AWS compute environments



IAM

Temporary security credentials



Amazon EC2 instance

AWS Lambda function

Amazon SageMaker notebook

Amazon Elastic Container Service task

Amazon EMR cluster

And many more

How to write great IAM policies



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IAM authorization: The rules

```
{
  "Effect": "Allow",
  "Action": …
  "Resource": …
}
```

```
{
  "Effect": "Allow",
  "Action": …
  "Resource": …
}
```

```
{
  "Effect": "Deny",
  "Action": …
  "Resource": …
}
```

```
{
  "Effect": "Allow",
  "Action": …
  "Resource": …
}
```

Policy statements matching the request



Matching statements

- Something allows the action
- Nothing denies it

➔ ALLOWED

IAM authorization: The rules

```
{
  "Effect": "Allow",
  "Action": …
  "Resource": …
}
```

```
{
  "Effect": "Deny",
  "Action": …
  "Resource": …
}
```

```
{
  "Effect": "Allow",
  "Action": …
  "Resource": …
}
```

Policy statements matching the request

```
{
  "Effect": "Allow",
  "Action": …
  "Resource": …
}
```



Matching statements

- Something allows the action
- Nothing denies it

➔ ALLOWED

IAM authorization: The rules

```
{
  "Effect": "Allow",
  "Action": …
  "Resource": …
}
```

```
{
  "Effect": "Allow",
  "Action": …
  "Resource": …
}
```

```
{
  "Effect": "Deny",
  "Action": …
  "Resource": …
}
```

```
{
  "Effect": "Allow",
  "Action": …
  "Resource": …
}
```

Policy statements matching the request



Matching statements

- Something allows the action
- Something denies it

➔ DENIED

IAM authorization: The rules

```
{
  "Effect": "Allow",
  "Action": …
  "Resource": …
}
```

```
{
  "Effect": "Allow",
  "Action": …
  "Resource": …
}
```

Policy statements matching the request

```
{
  "Effect": "Allow",
  "Action": …
  "Resource": …
}
```



```
{
  "Effect": "Deny",
  "Action": …
  "Resource": …
}
```

Matching statements

- Something allows the action
- Something denies it

➔ DENIED

IAM authorization: The rules

```
{
  "Effect": "Allow",
  "Action": …
  "Resource": …
}
```

```
{
  "Effect": "Allow",
  "Action": …
  "Resource": …
}
```

```
{
  "Effect": "Deny",
  "Action": …
  "Resource": …
}
```

```
{
  "Effect": "Allow",
  "Action": …
  "Resource": …
}
```

Policy statements
matching the request

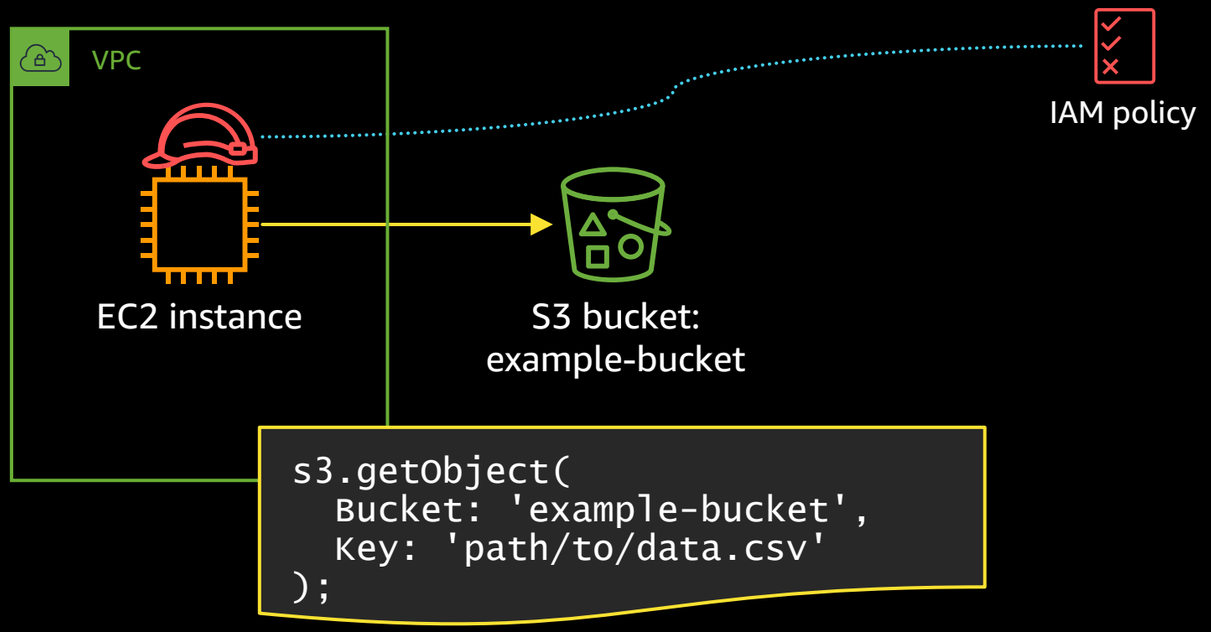


Matching statements

- Nothing allows the action
- Nothing denies it

➔ DENIED

An application that reads data from Amazon S3



Application code

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    // … something to allow
    // that call to s3.getObject()
  }]
}
```

IAM policy

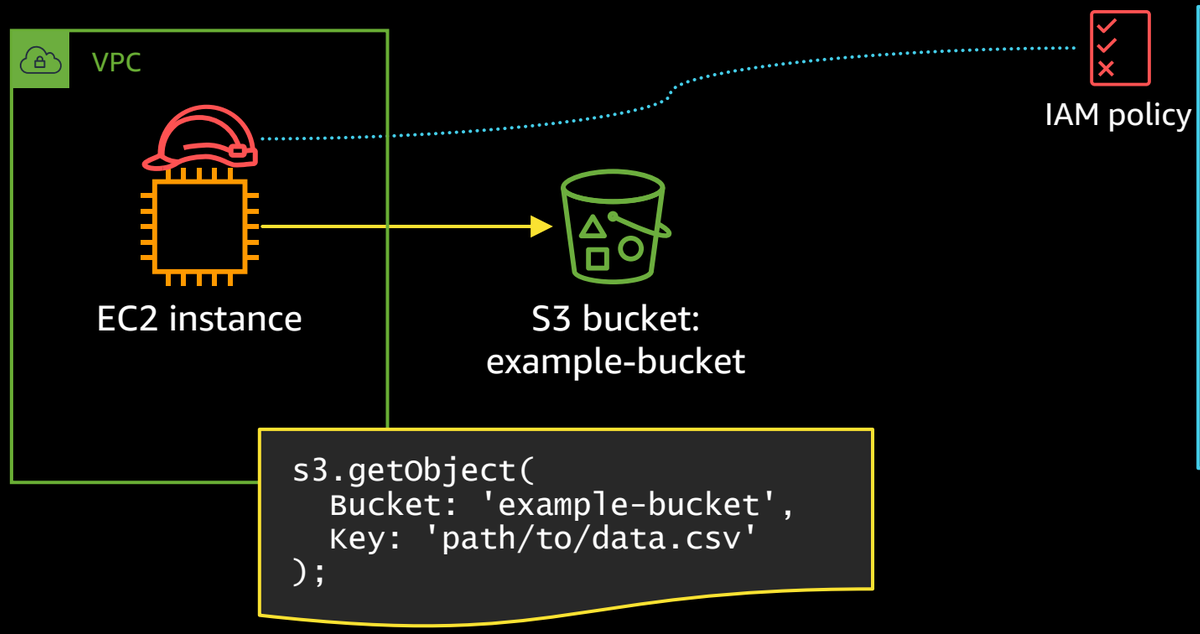
Least-privilege permission to an AWS service

Actions	Description	Access Level	Resource Types (*required)	Condition Keys
GetObject	Grants permission to retrieve objects from Amazon S3	Read	object*	s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:signatureAge s3:signatureversion s3:x-amz-content-sha256

Resource Types	ARN
accesspoint	arn:${Partition}:s3:${Region}:${Account}:accesspoint/${AccessPointName}
bucket	arn:${Partition}:s3:::${BucketName}
object	arn:${Partition}:s3:::${BucketName}/${ObjectName}

https://docs.aws.amazon.com/IAM/latest/UserGuide/list_amazons3.html

An application that reads data from Amazon S3



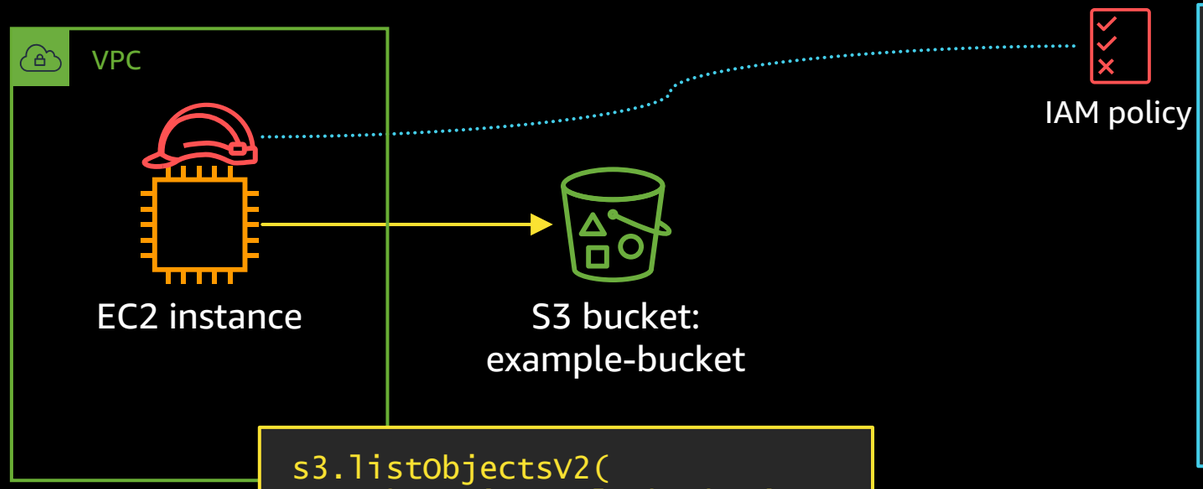
Application code

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource":
      "arn:aws:s3:::example-bucket/path/to/data.csv"
  }]
}
```

IAM policy

Resource Types	ARN
accesspoint	arn:${Partition}:s3:${Region}:${Account}:accesspoint/$
bucket	arn:${Partition}:s3:::${BucketName}
object	arn:${Partition}:s3:::${BucketName}/${ObjectName}

Is this going to work?




```
s3.listObjectsV2(
  Bucket: 'example-bucket',
  Prefix: 'path/to/'
);

// Other application code

s3.getObject(
  Bucket: 'example-bucket',
  Key: 'path/to/data.csv'
);
```

Application code

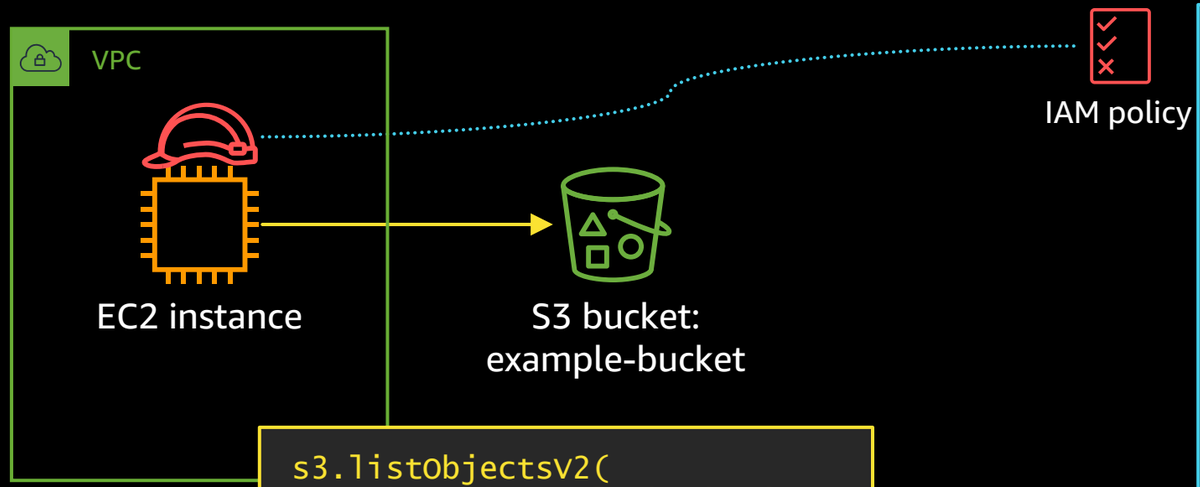
```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource":
      "arn:aws:s3:::example-bucket/path/to/data.csv"
  }]
}
```

IAM policy

Pause the recording and see if you can figure it out!

https://docs.aws.amazon.com/IAM/latest/UserGuide/list_amazons3.html

Listing objects in Amazon S3




```
s3.listObjectsV2(
  Bucket: 'example-bucket',
  Prefix: 'path/to/'
);

// Other application code

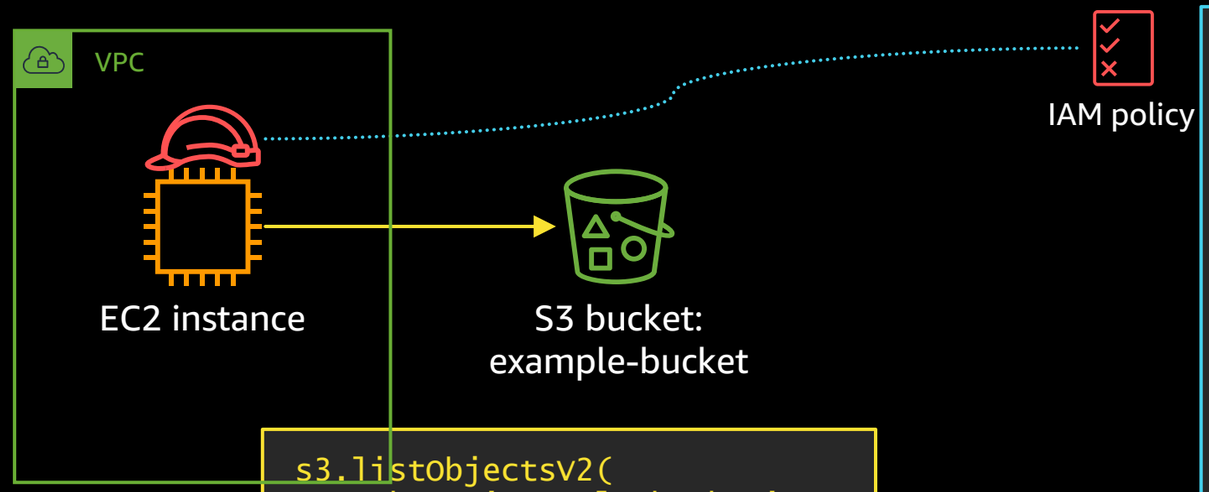
s3.getObject(
  Bucket: 'example-bucket',
  Key: 'path/to/data.csv'
);
```

Application code

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource":
      "arn:aws:s3:::example-bucket/path/to/data.csv"
  },{
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::example-bucket",
    "Condition": {
      "StringLike": {
        "s3:prefix": "path/to/*"
      }
    }
  }]
}
```

IAM policy

Listing objects in Amazon S3



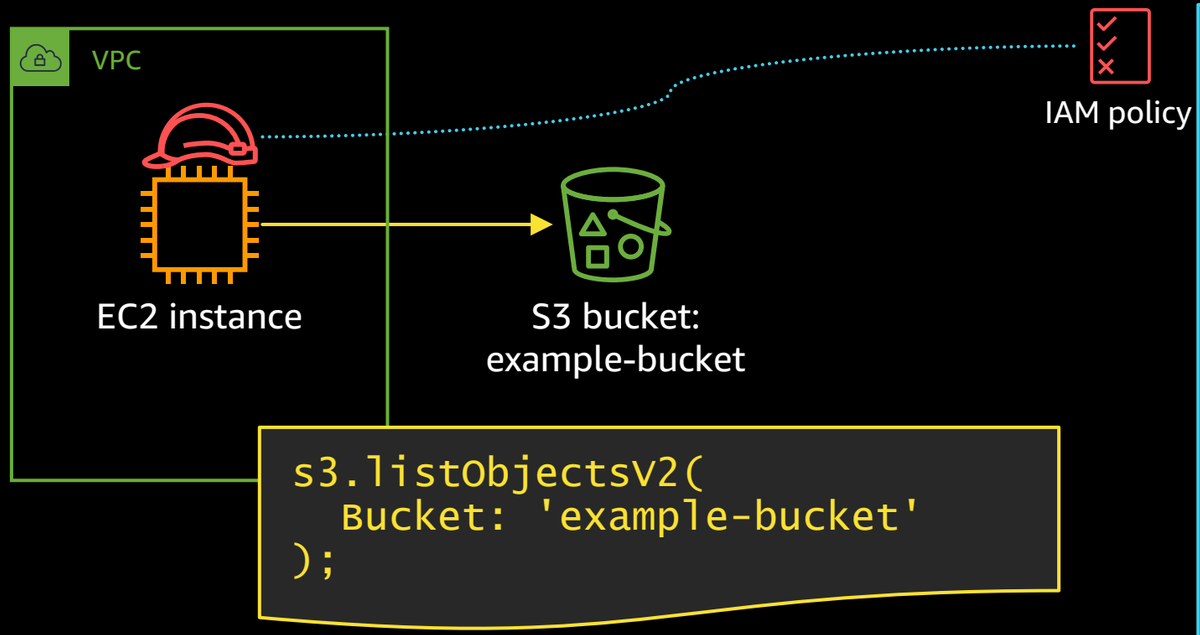

```
s3.listObjectsV2(
  Bucket: 'example-bucket',
```

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource":
      "arn:aws:s3:::example-bucket/path/to/data.csv"
  },{
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::example-bucket",
    "Condition": {
      "StringLike": {
        "s3:prefix": "path/to/*"
```

Actions	Description	Access Level	Resource Types (*required)	Condition Keys
	request			s3:x-amz-content-sha256
ListBucket	Grants permission to list some or all of	List	bucket*	
				s3:prefix

Resource Types	ARN
accesspoint	arn:${Partition}:s3:${Region}:${Account}:accesspoint/${AccessPointName}
bucket	arn:${Partition}:s3:::${BucketName}
object	arn:${Partition}:s3:::${BucketName}/${ObjectName}

Is this going to work?




```
s3.listObjectsV2(
  Bucket: 'example-bucket'
);
```

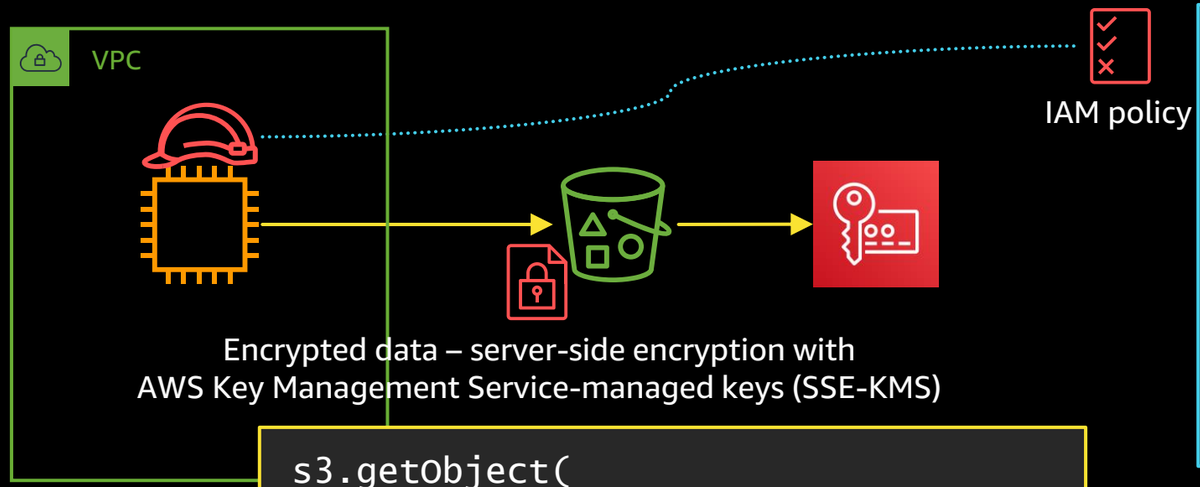
Application code

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource":
      "arn:aws:s3:::example-bucket/path/to/data.csv"
  },{
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::example-bucket",
    "Condition": {
      "StringLike": {
        "s3:prefix": "path/to/*"
      }
    }
  }]
}
```

IAM policy

Pause the recording and see if you can figure it out!

Is this going to work?




```
s3.getObject(
  Bucket: 'example-bucket',
  Key: 'path/to/encrypted-data.csv'
);
```

Application code

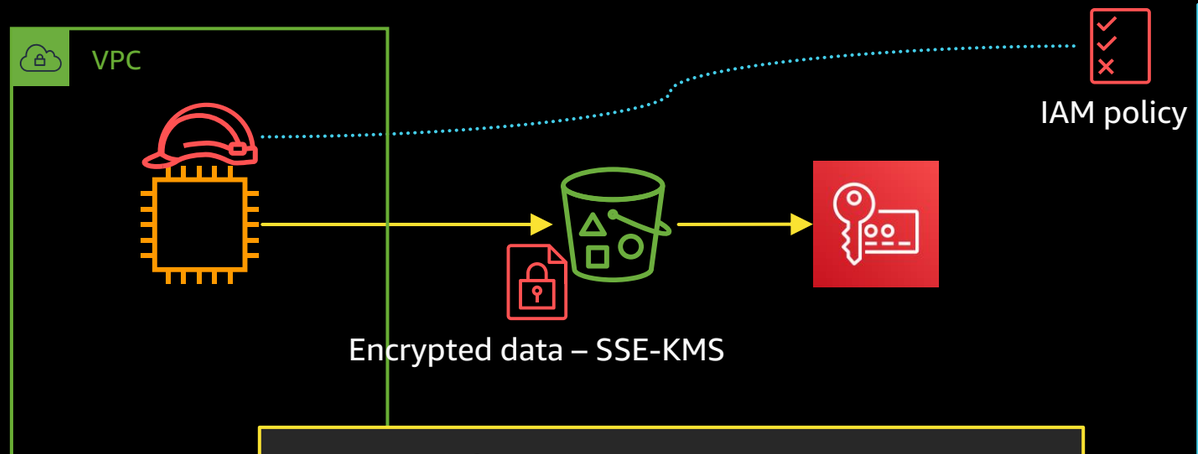
```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource":
      "arn:aws:s3:::example-bucket/path/to/*"
  }]
}
```

IAM policy

Pause – how to fix it?

Hint

Reading KMS-encrypted data from AWS service



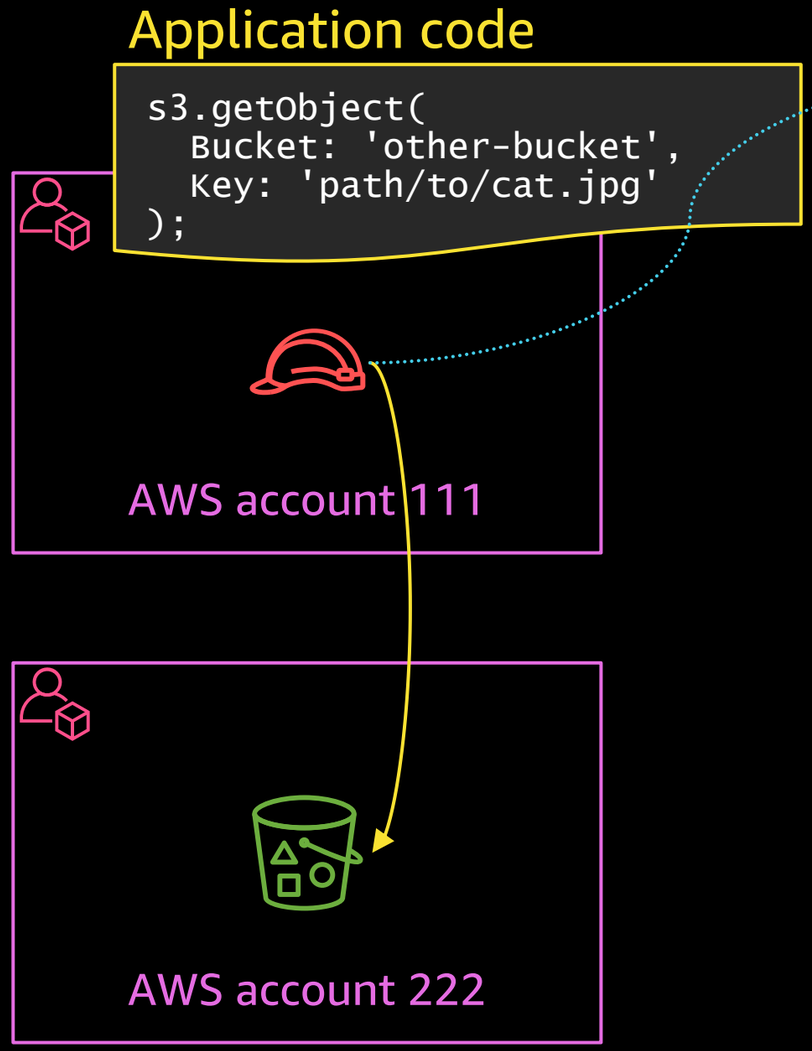

```
s3.getObject(
  Bucket: 'example-bucket',
  Key: 'path/to/encrypted-data.csv'
);
```

Application code

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource":
      "arn:aws:s3:::example-bucket/path/to/*"
  }, {
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-east-
2:111122223333:key/01234567-abcd-effe-dbca-
01234567890a"
  }]
}
```

IAM policy

Is this going to work?





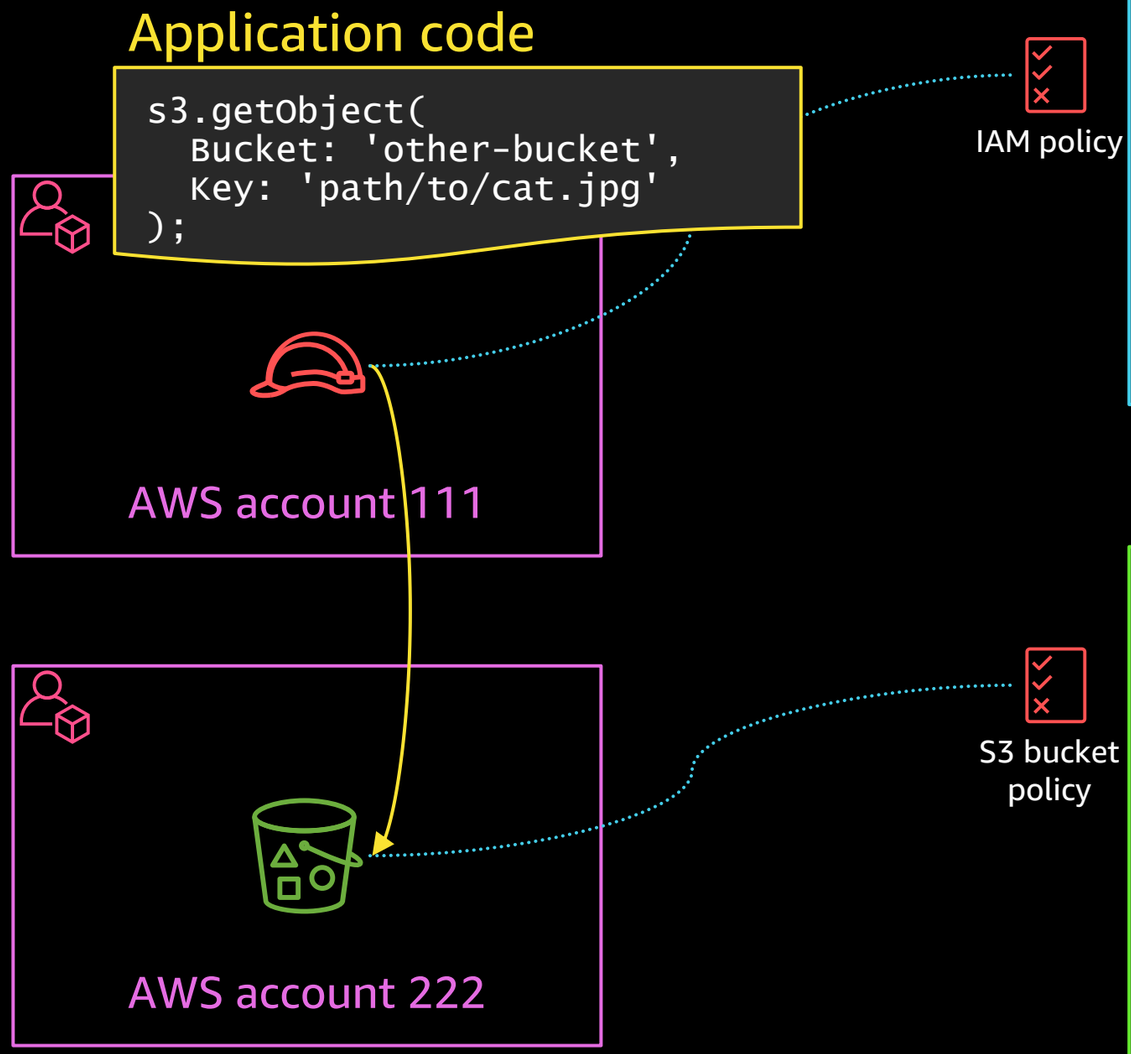

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::other-bucket/*"
  }]
}
```

IAM policy

Pause – what do you think?



Granting cross-account access to resources




```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::other-bucket/*"
  }]
}
```

IAM policy

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Principal": {
      "AWS": "111"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::other-bucket/*"
  }]
}
```

S3 bucket policy

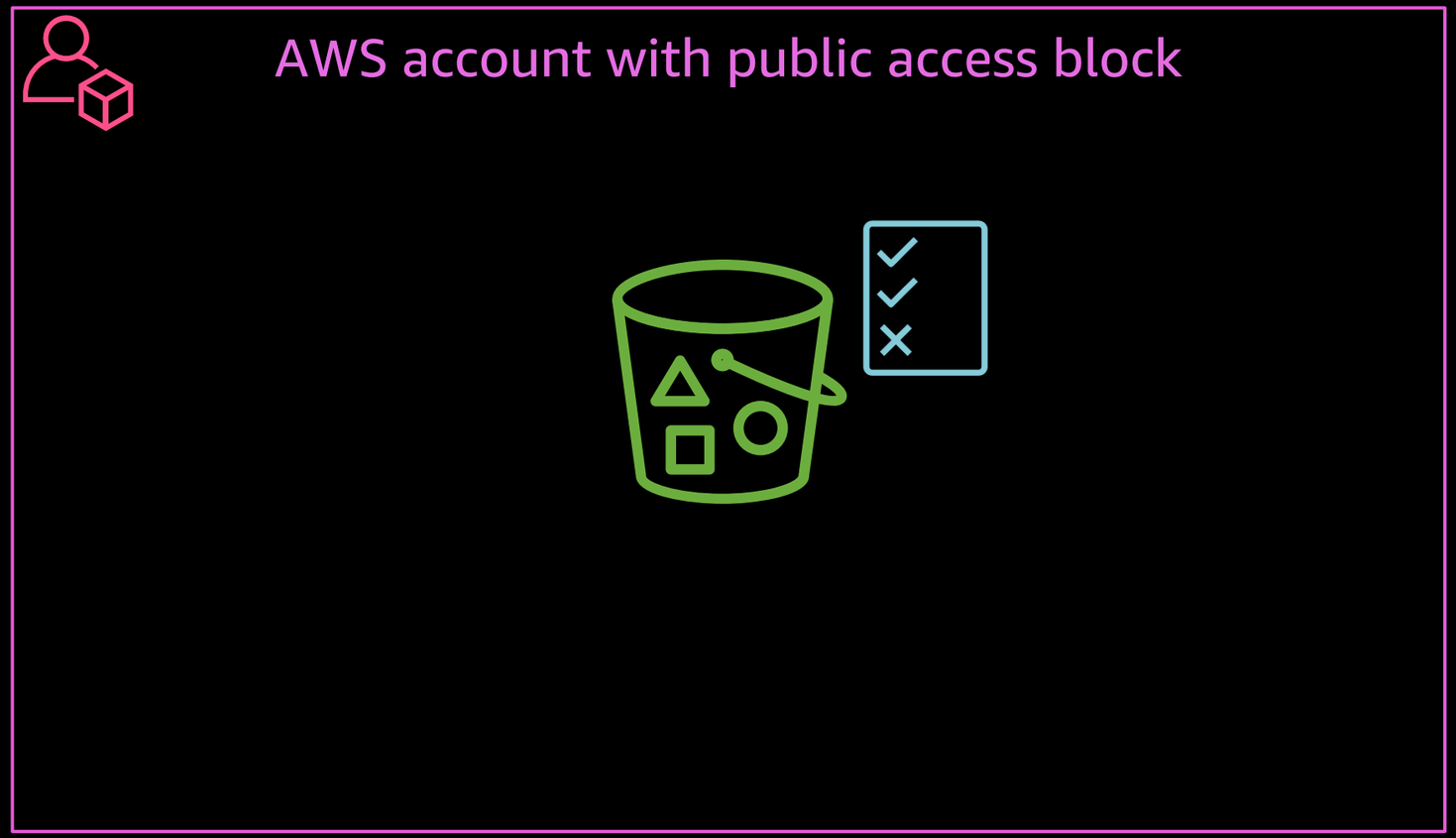
Block Public Access in Amazon S3: Do it now



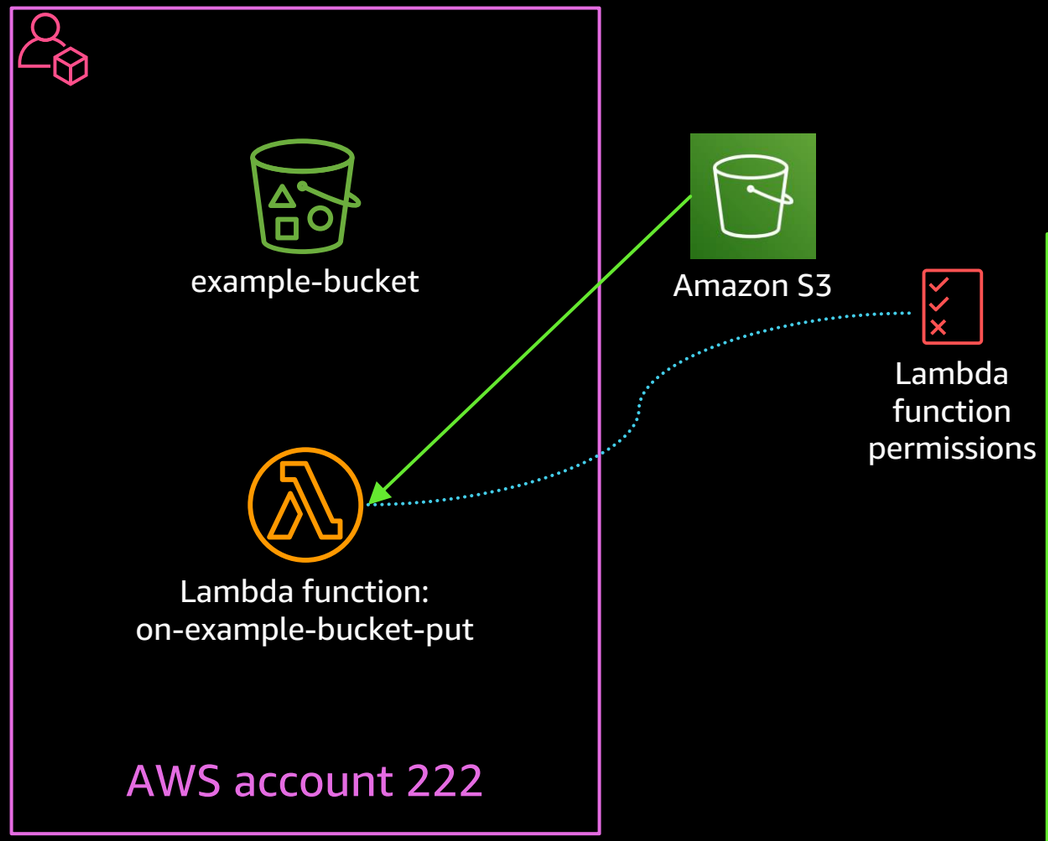
Block Public Access in Amazon S3: Do it now



Block Public Access in Amazon S3: Do it now



Granting AWS access to resources

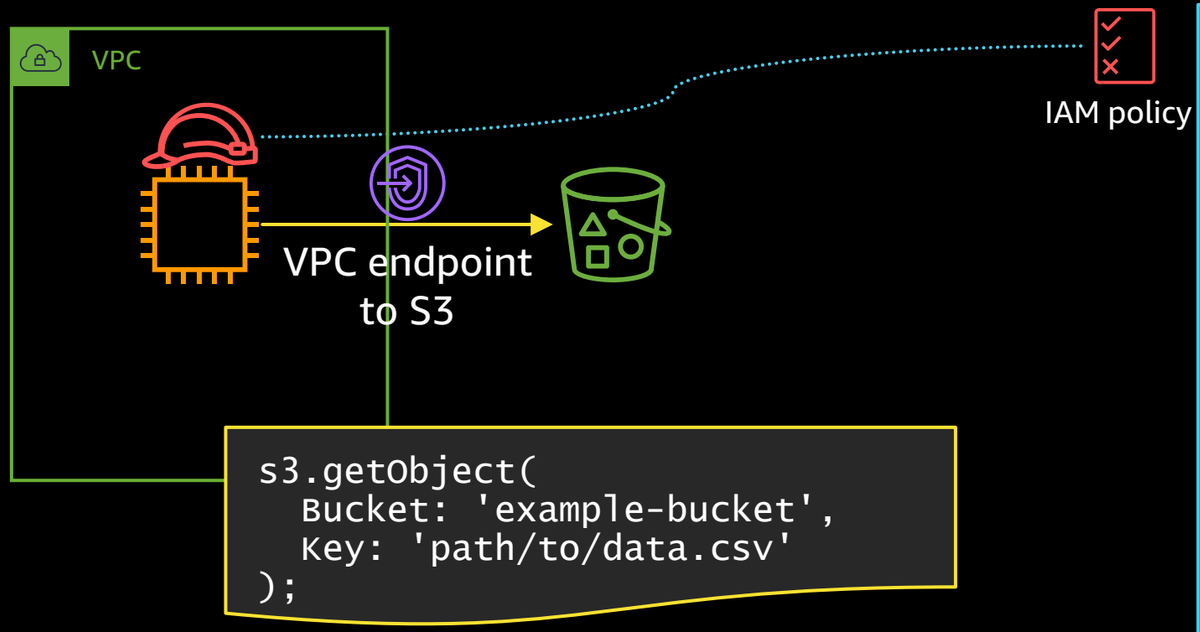


"Allow S3 to invoke this Lambda function about changes to this example-bucket owned account 222."

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Principal": {
      "Service": "s3.amazonaws.com"
    },
    "Action": "lambda:InvokeFunction",
    "Resource": "arn:aws:lambda:us-east-
2:222:function:on-example-bucket-put",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "222",
        "aws:SourceArn": "arn:aws:s3:::example-
bucket"
```

Lambda function permission

Aside: Network path as authorization condition



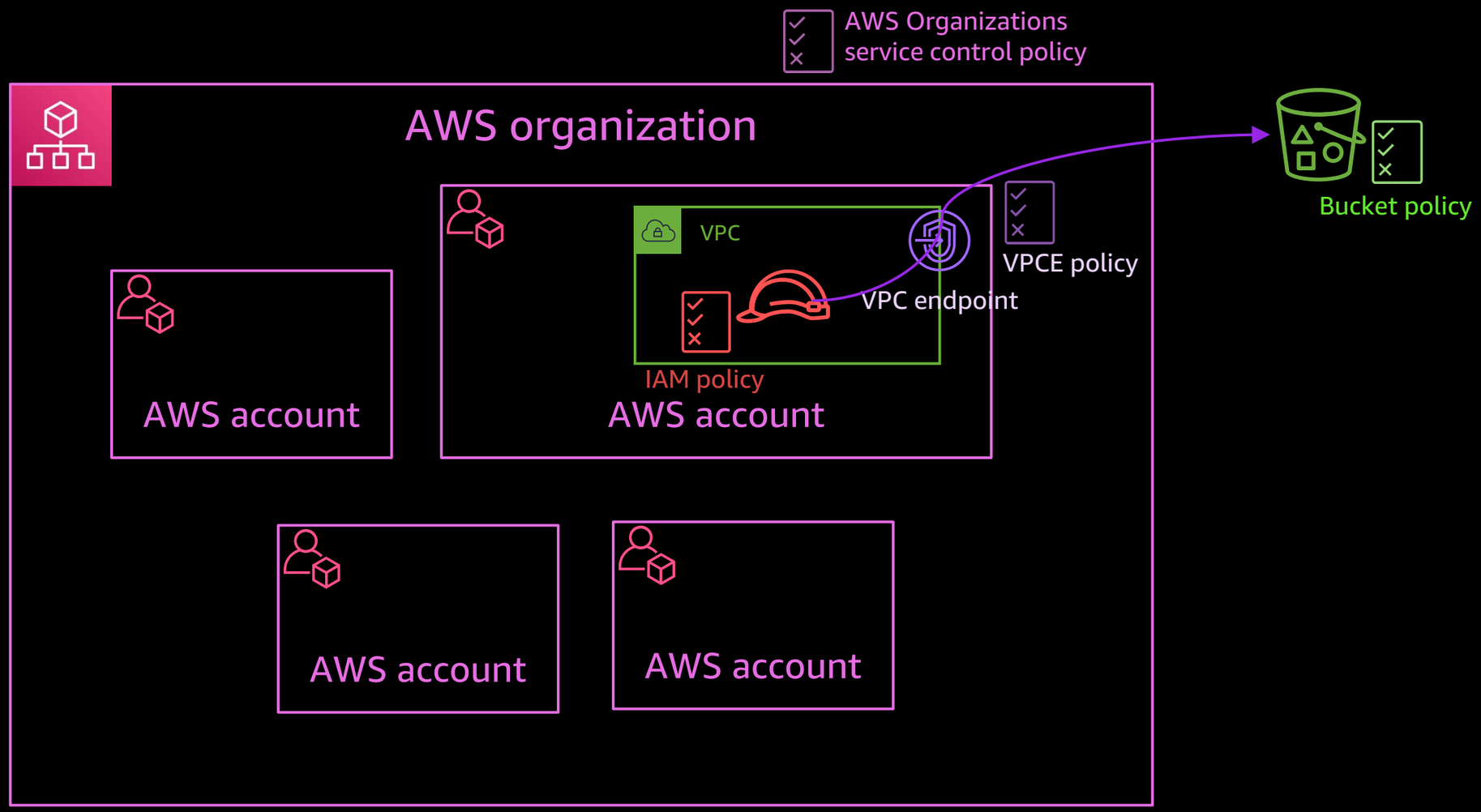
Application code

Pause – what's going on here?

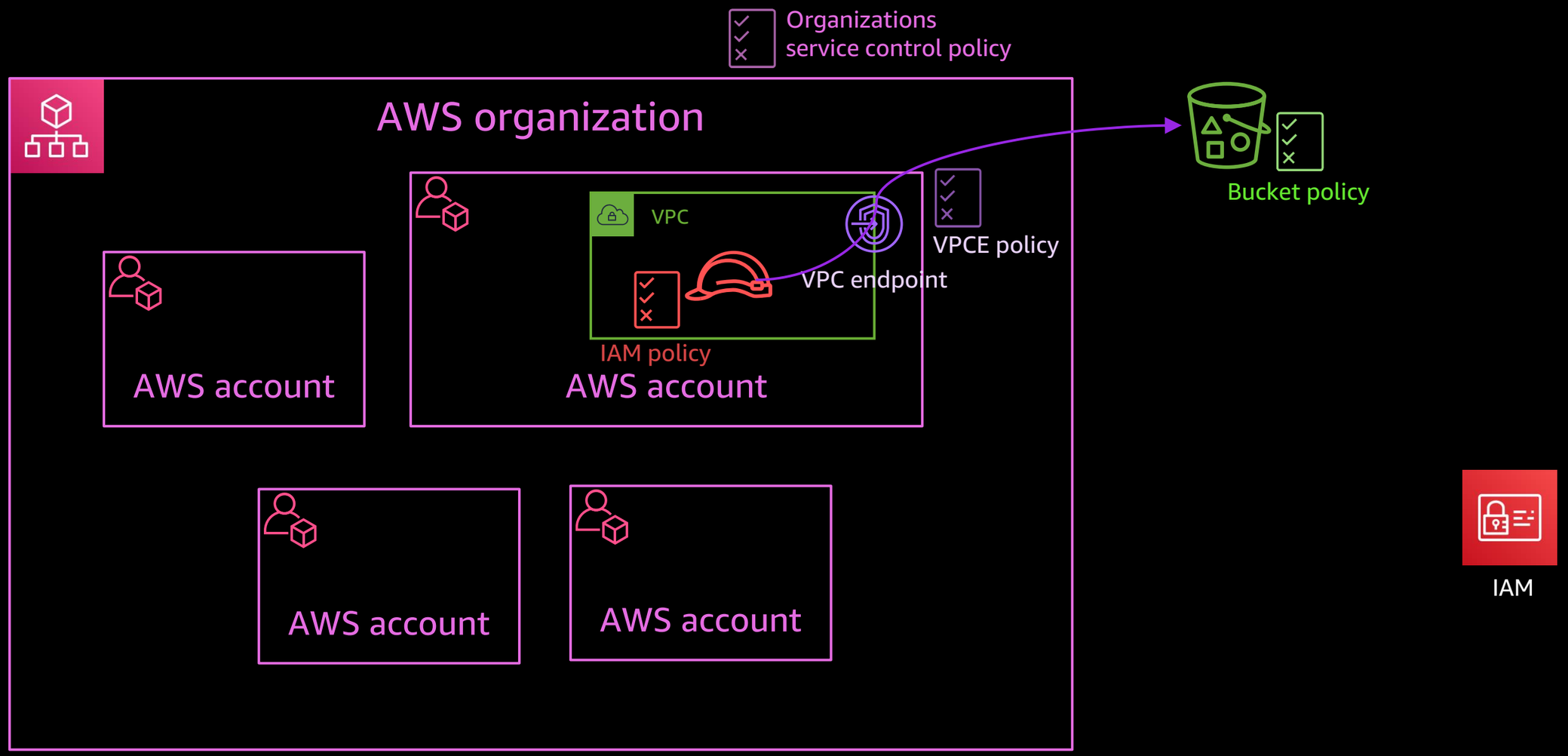
```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource":
      "arn:aws:s3:::example-bucket/path/to/data.csv"
  }, {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "StringNotEqualsIfExists": {
        "aws:SourceVpc": "vpc-1234abcd"
      },
      "Bool": {
        "aws:ViaAWSService": "false"
      }
    }
  }]
}
```

IAM policy

Zooming out: IAM at scale



Zooming out: IAM at scale



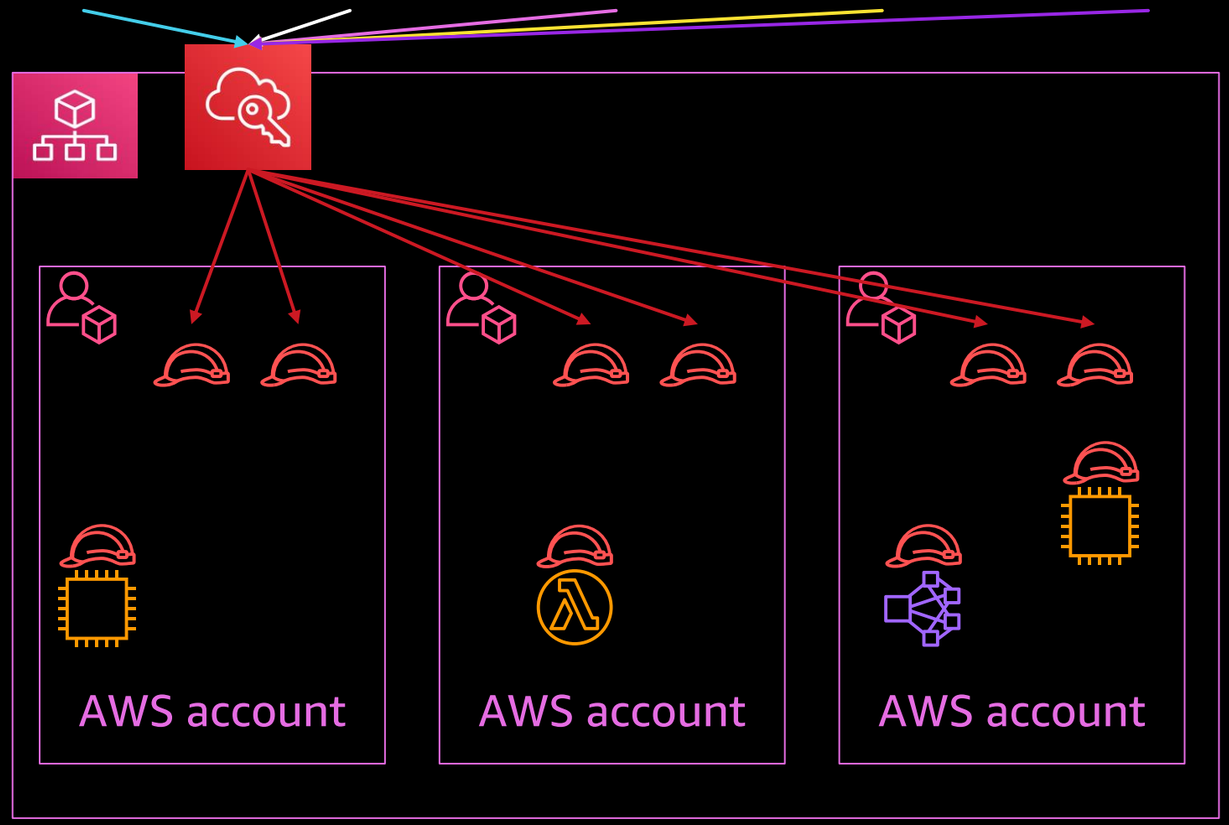
Wrapping up



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Identity and the broader security landscape in AWS



We just learned how to **authenticate** and **authorize** in AWS

Continuing your journey as a secure builder

- Amazon Virtual Private Cloud / network security features
- Encryption features
- Detective controls – AWS CloudTrail, AWS IAM Access Analyzer, and many more

Continuing your learning journey

- re:Invent 2020 session

  “Choosing the right combination of IAM policies at scale”

- IAM tutorials

  https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorials.html

- AWS Well-Architected – security pillar

  https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/identity-and-access-management.html

- Get hands-on – AWS security workshops

  https://awssecworkshops.com/workshops/#identity



Thank you!

Becky Weiss

becky@amazon.com

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.