
aws
SUMMIT
SAN FRANCISCO | APRIL 20-21, 2022

SEC205

Data perimeter workshop

Swara Gandhi
Solutions Architect – Identity Solutions
AWS

Liam Wadman
Solutions Architect – Identity Solutions
AWS

Agenda

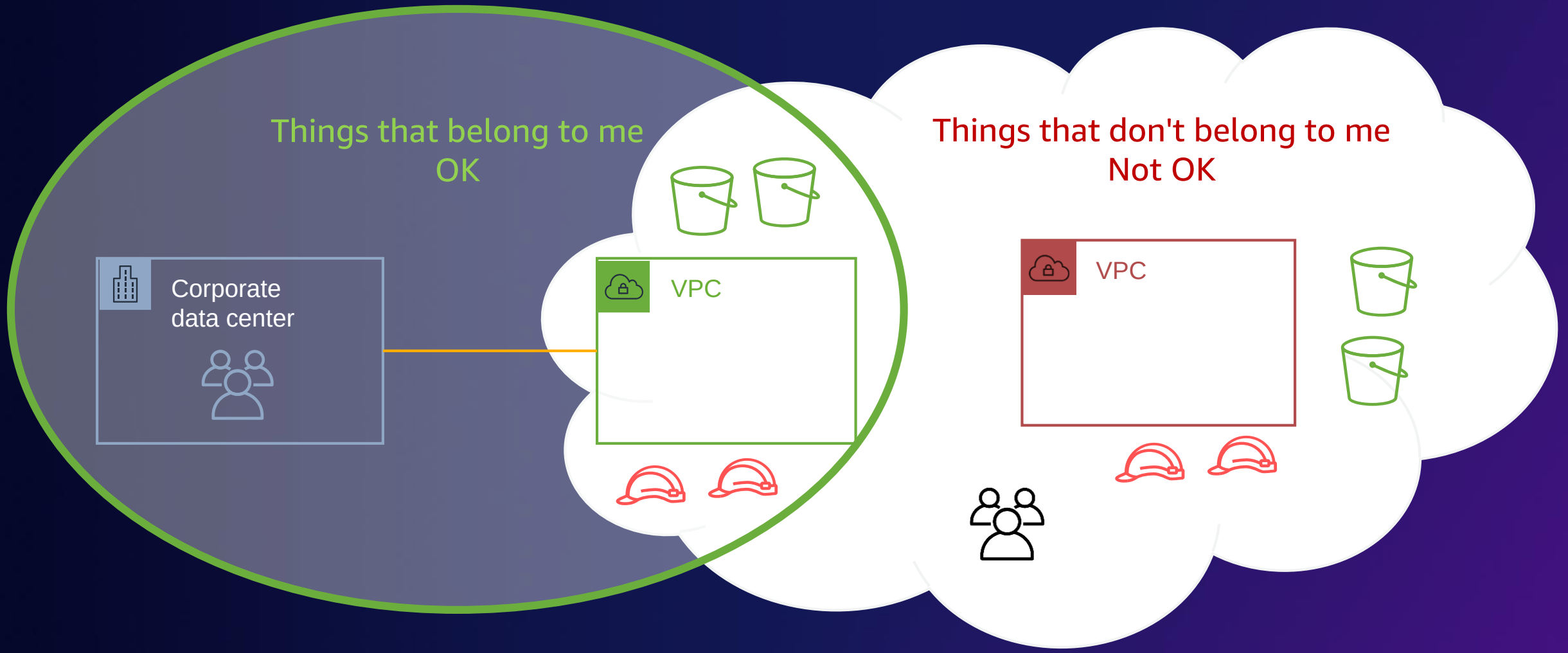
The challenge

Establishing a data perimeter

Hands-on labs

The challenge

How to establish a perimeter around things that belong to me?



Perimeter control objectives

Perimeter	Intent/control objective
Identity	Ensure my resources are only accessed by **my identities** or AWS service principals
	Ensure only **my identities** are allowed from my network
Resource	Ensure my identities only access **my resources** or AWS owned resources
	Ensure my network can only access **my resources** or AWS owned resources
Network	Ensure my identities only access from **my network** or AWS service network
	Ensure my resources are only accessed from **my network** or from AWS service network

Establishing a data perimeter

General data protection best practices

- Identify and classify sensitive data
- Encrypt, tokenize, and mask sensitive data
- Keep humans away from sensitive data
- Establish data perimeter guardrails
- Implement preventive, detective, and responsive controls

What is a data perimeter?

A set of preventive guardrails that ensures that access to **trusted resources** is restricted to **trusted identities** from **expected network locations**

Trusted resources – resources belonging to your AWS organization

Trusted identities – principals belonging to your AWS organization

Expected network locations – your data centers and your VPCs

Data is stored in **trusted resources**

Data perimeter controls

Perimeter	Applied on	Using	Control objective
Identity	**Resources**	Resource-based policies	Ensure my resources are only accessed by **my trusted identities** or AWS service principals
	Network	VPC endpoint policy	Ensure only **my trusted identities** are allowed from my network
Resource	**Identities**	IAM/SCP policies	Ensure my identities only access **my resources** or AWS owned resources
	Network	VPC endpoint policy	Ensure my network can only access **my resources** or AWS owned resources
Network	**Identities**	IAM/SCP policies	Ensure my identities only access from **my network** or AWS service network
	Resources	Resource-based policies	Ensure my resources are only accessed from **my network** or from AWS service network

Tools for your data perimeter

Service control policies

Permissions guardrails
for identities

Prevent users from publishing data to Amazon SNS topics
that do not belong to my AWS organization

Tools for your data perimeter

Service control policies

Permissions guardrails for identities

VPC endpoint policies

Ensure network access only from trusted identities

Prevent users outside my organization from moving my customer data through this VPC endpoint to an S3 bucket that I don’t own

Tools for your data perimeter

Service control policies

Permissions guardrails for identities

VPC endpoint policies

Ensure network access only from trusted identities

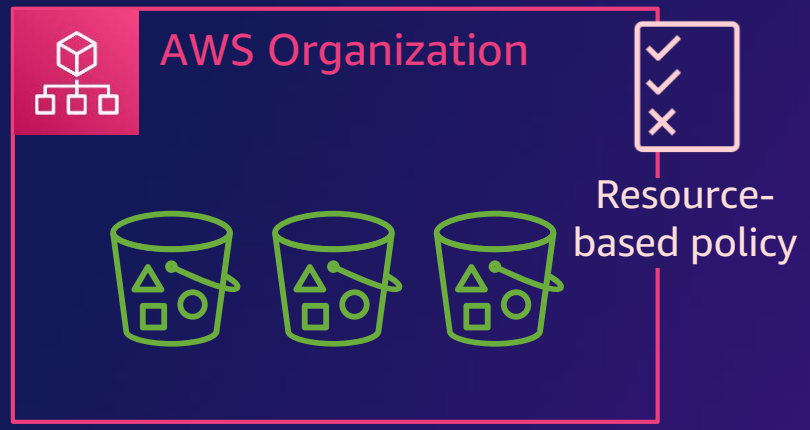
Resource-based policies

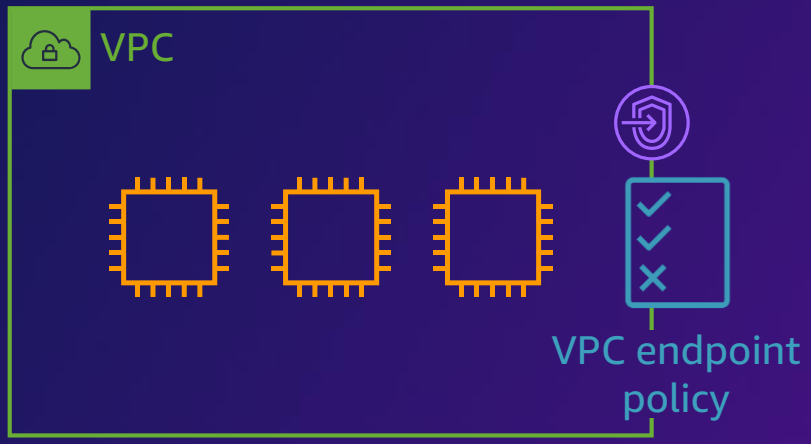
Ensure access only by your identities and AWS services

Prevent access to this Amazon SQS queue from identities outside my accounts in AWS Organizations unless they are AWS services

Identity: Telling the difference

- Trusted identities
  - aws:PrincipalOrgId (/OUPath/Account)
- AWS service acting on behalf of me
  - aws:PrincipalIsAwsService
- Implementing at scale
  - Infrastructure as code or detective controls to ensure resources are deployed with appropriate controls
  - VPC endpoints and endpoint policies

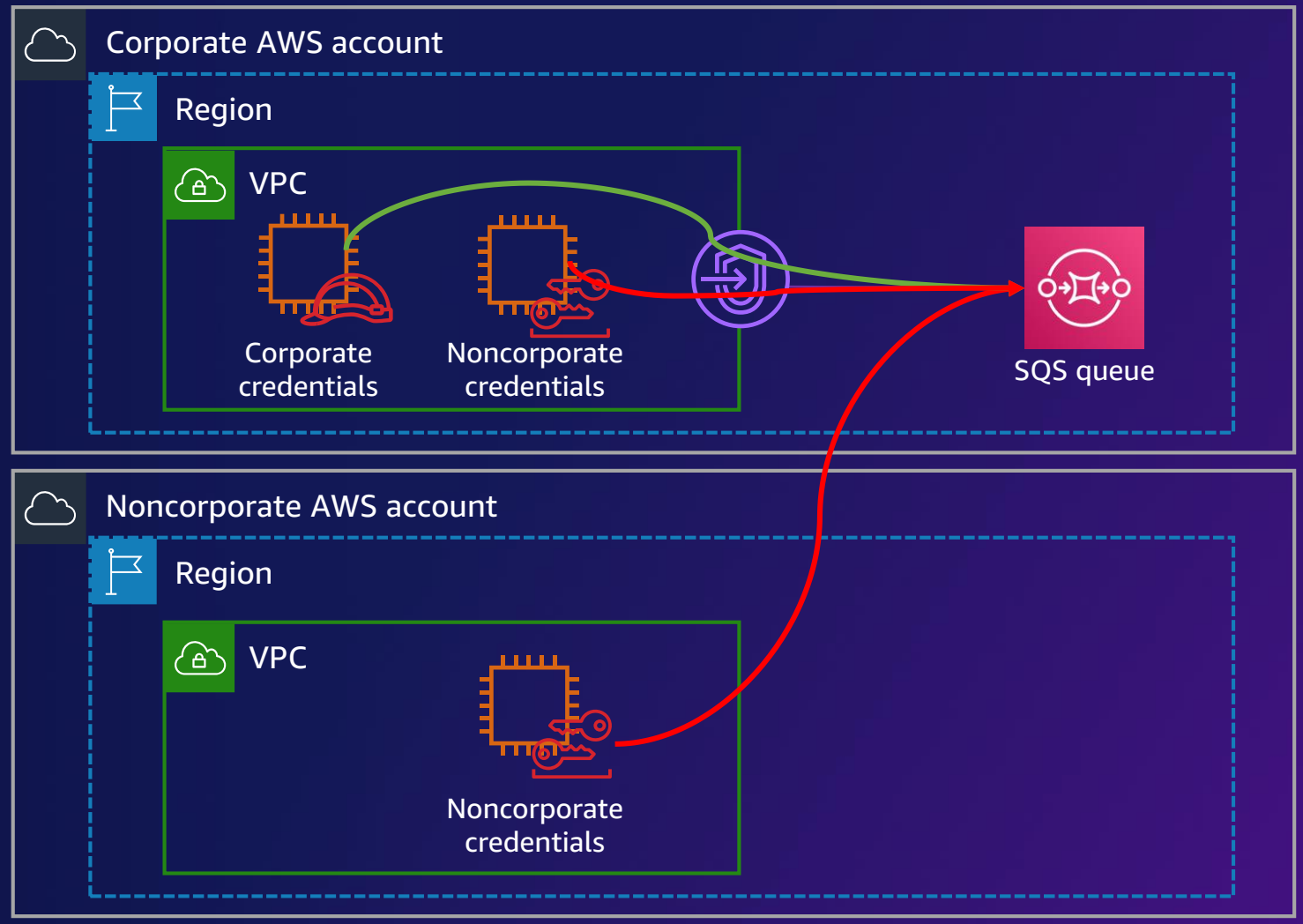




Identity: Telling the difference

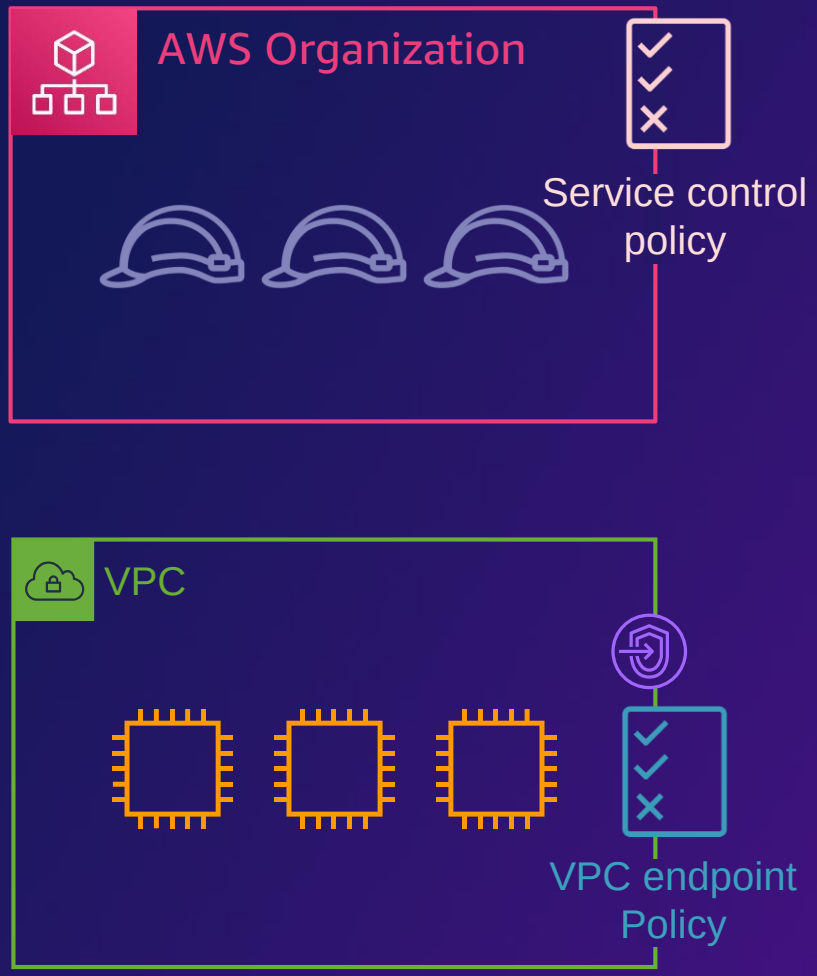
Configure an identity perimeter in the VPC endpoint policy and resource policy to accept traffic only from principals belonging to your AWS organization

```
{
   "Statement":[
      {
         "Sid":"TrustedPrincipal",
         "Effect":"Deny",
         "Principal":"*",
         "Action":"sqs:SendMessage",
"Resource":"arn:aws:sqs:*:111122223333:queue1",
         "Condition":{
            "StringNotEquals":{
               "aws:PrincipalOrgID":[
                  "o-xxxxxxxxxx"
               ]
            }
         }
      }
   ]
}
```



Resources: Telling the difference

- Trusted resources
  - Resource path
  - s3:ResourceAccount
- Implementing at scale
  - Service control policies
  - VPC endpoints and endpoint policies
  - Exceptions may be required for some AWS service-owned resources within AWS service accounts (e.g., AWS Systems Manager-owned S3 buckets)

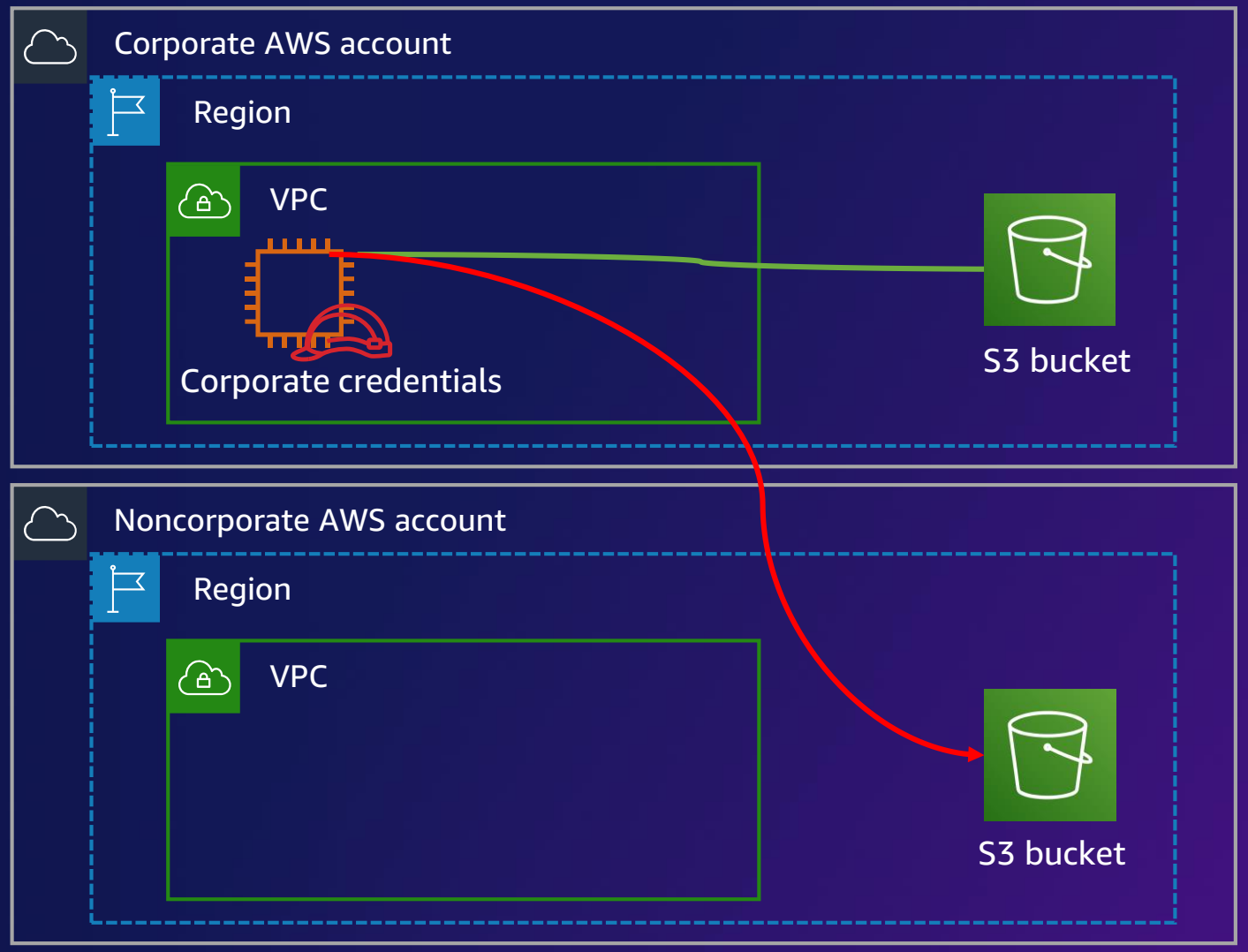


Resources: Telling the difference

Configure a resource perimeter for your identities, IAM policy, or SCP to allow access only to your resources

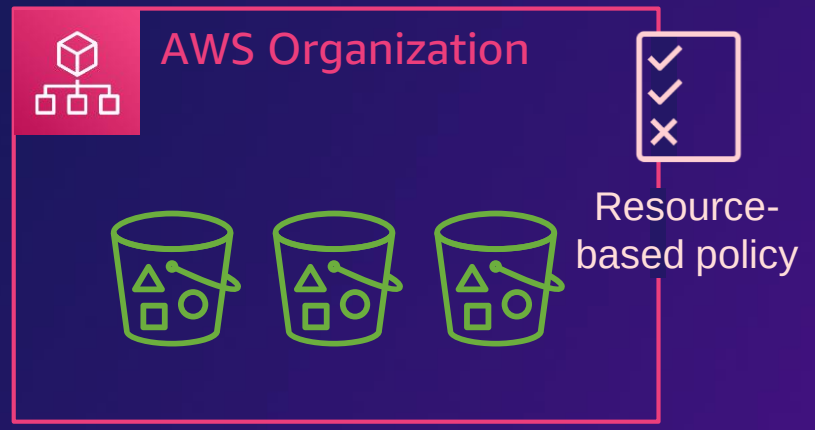
```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"TrustedS3Resources",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{

"s3:ResourceAccount":"123456789012"
            }
         }
      }
   ]
}
```



Expected network: Telling the difference

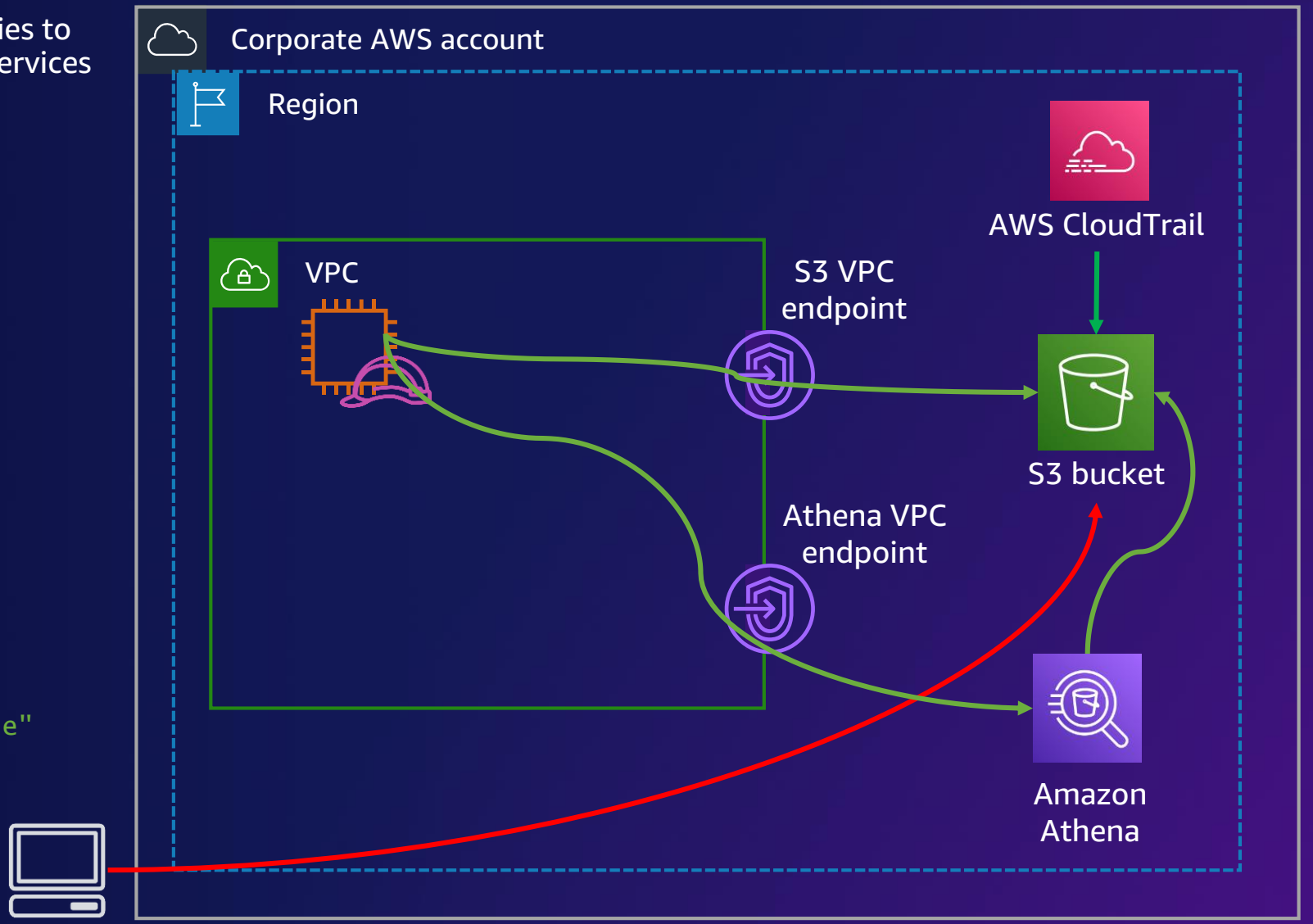
- Expected network
  - aws:SourceIp
  - aws:SourceVpc/e
- AWS service actions from service-owned network
  - aws:ViaAWSService (when caller's identity is used, such as Amazon Athena)
  - aws:PrincipalIsAwsService (when service principal is used, such as AWS CloudTrail)
- Implementing at scale
  - Service control policies



Expected network: Telling the difference

Configure network perimeter in your resource policies to allow access only from expected networks & AWS services

```
"Statement":[
   {
      "Sid":"trusted-network-ViaAWSService",
      "Effect":"Deny",
      "Principal":"*",
      "Action":[
         "s3:PutObject",
         "s3:GetObject*"
      ],
      "Resource":[
         "arn:aws:s3:::my-data-bucket",
         "arn:aws:s3:::my-data-bucket/*"
      ],
      "Condition":{
         "StringNotEqualsIfExists":{
            "aws:SourceVpc":"vpc-111bbb22"
         },
         "BoolIfExists":{
            "aws:ViaAWSService":"false",
            "aws:PrincipalIsAWSService":"false"
         }
      }
   }
]
```



Data perimeter controls

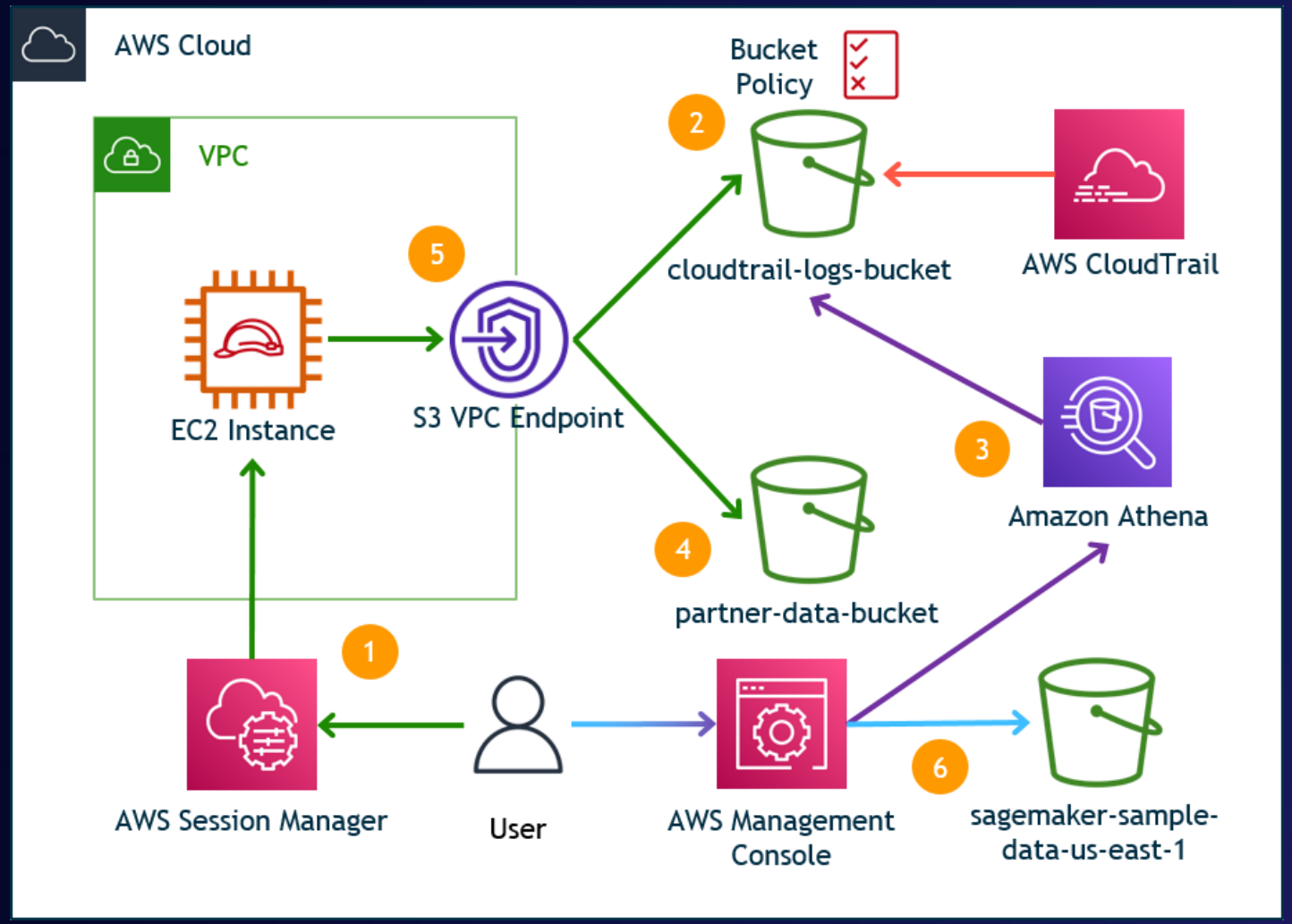
Perimeter	Applied on	Using	Primary IAM feature	Data perimeter control objective
Identity	**Resources**	Resource-based policies	PrincipalOrgID PrincipalIsAWSService	Ensure my resources are only accessed by **my trusted identities** or AWS service principals
	Network	VPC endpoint policy	PrincipalOrgID	Ensure only **my trusted identities** are allowed from my network
Resource	**Identities**	IAM/SCP policies	ResourceAccount	Ensure my identities only access **my resources** or AWS owned resources
	Network	VPC endpoint policy	ResourceAccount	Ensure my network can only access **my resources** or AWS owned resources
Network	**Identities**	IAM/SCP policies	SourceIp SourceVpc SourceVpce ViaAWSService	Ensure my identities only access from **my network** or AWS service network
	Resources	Resource-based policies	SourceIp SourceVpc SourceVpce ViaAWSService PrincipalIsAWSService	Ensure my resources are only accessed from **my network** or from AWS service network

Hands-on labs

Lab agenda

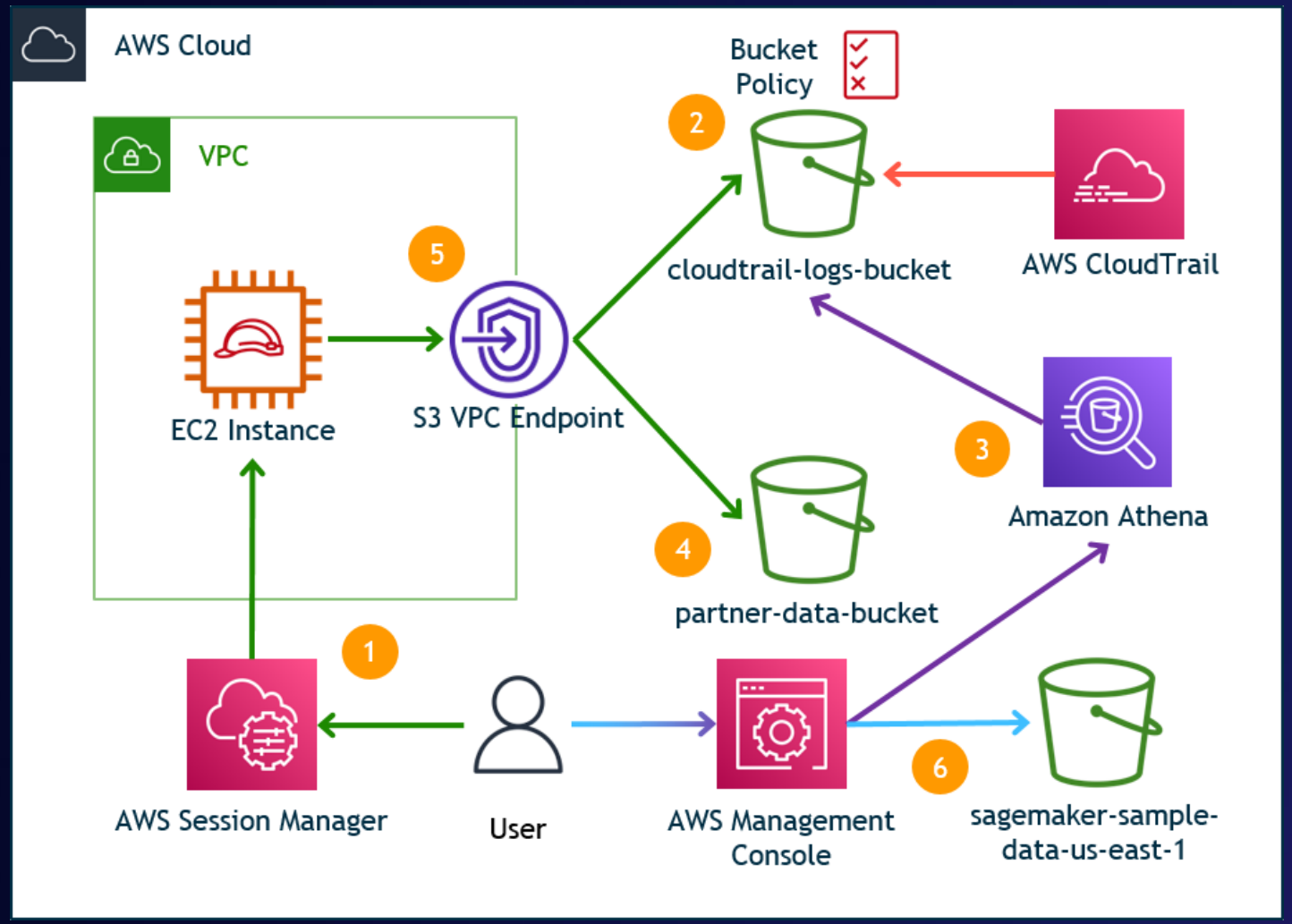
- Lab 0 – Test environment
- Lab 1 – Identity controls for resources
- Lab 2 – Network controls for resources
- Lab 3 – Identity controls for network
- Lab 4 – Resource controls for network
- Lab 5 – Resource controls for identities

Workshop setup



1. You'll use AWS Systems Manager Session Manager to access the EC2 instance in the VPC. The VPC does not have internet connectivity and will connect to all resources through VPC endpoints.
2. In Lab 1, you will access the CloudTrail bucket contents and create a bucket policy that only allows specific principals to access the content. Then in Lab 2, you'll update that bucket policy to restrict what networks can be used to access the resource.
3. In Lab 2, you will use the AWS Management Console to access Amazon Athena and run a query on the data in the CloudTrail bucket.

Workshop setup



4. In Lab 3, you will access your partner's S3 data bucket, demonstrating an access pattern you don't want to occur.
5. Continuing in Lab 3, in order to prevent the cross-account access, you'll update the S3 VPC endpoint policy to only allows principals from a specific account to access S3 resources from the network. In Lab 4, you will update that policy again to restrict what resources can be accessed from the network.
6. In Lab 5, you will use the AWS Management Console to create an IAM policy that restricts the S3 resources that can be accessed by your IAM role and test that policy on an AWS owned public S3 bucket.

Learn in-demand AWS Cloud skills

AWS Skill Builder

Access **500+ free** digital courses and Learning Plans

Explore resources with a variety of skill levels and **16+** languages to meet your learning needs

Deepen your skills with digital learning on demand

Train now

AWS Certifications

Earn an industry-recognized credential

Receive Foundational, Associate, Professional, and Specialty certifications

Join the **AWS Certified community** and get exclusive benefits

Access **new** exam guides

Thank you!

Swara Gandhi
ganswara@amazon.com

Liam Wadman
liwadman@amazon.com