

AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC306

Building a data perimeter to allow access to authorized users

Laura Reith (she/her)

Identity Solutions Architect
Amazon Web Services

Swara Gandhi (she/her)

Identity Solutions Architect
Amazon Web Services



Agenda

Data perimeters on AWS

Hands-on labs



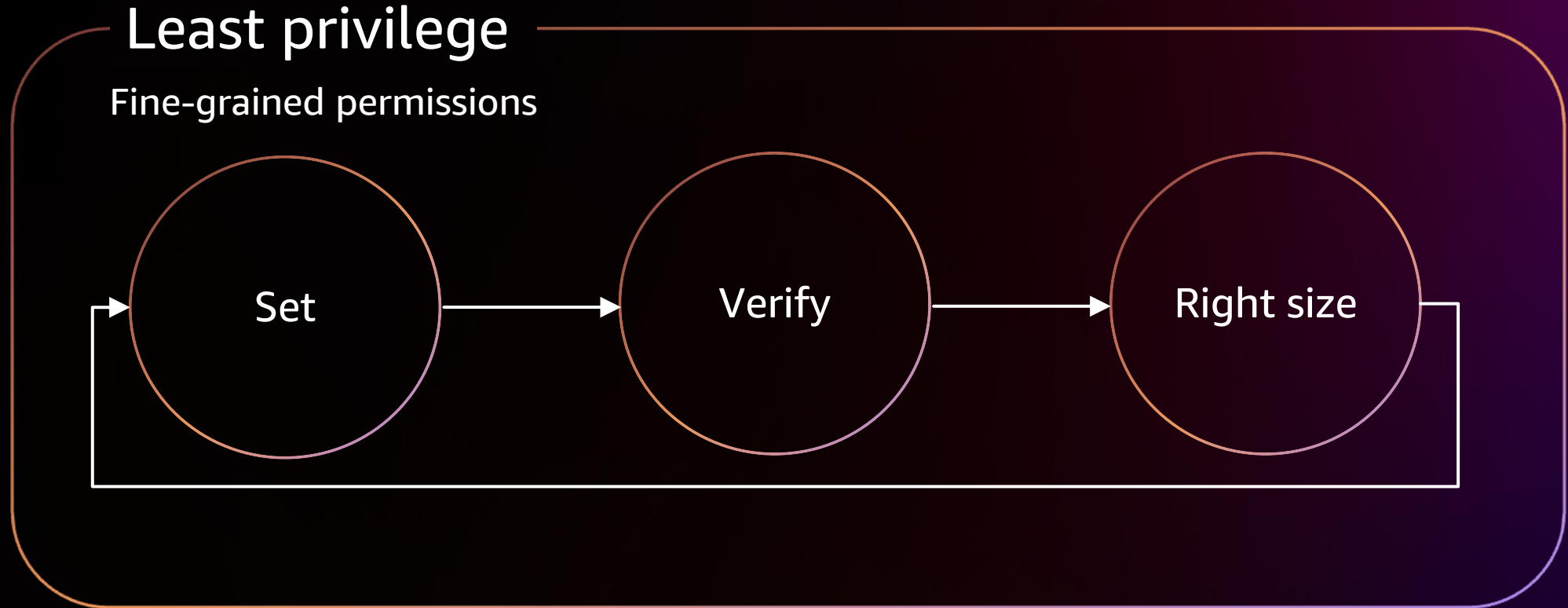
Access management

Data perimeter

Coarse-grained controls

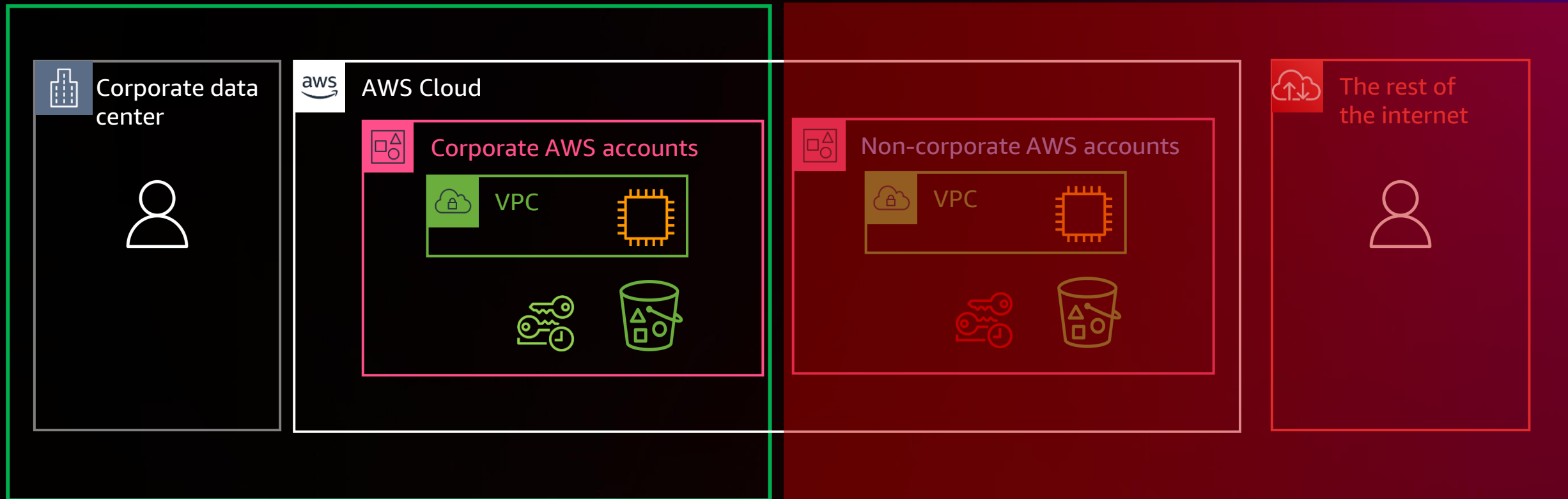
Least privilege

Fine-grained permissions



What is a data perimeter?

A set of preventive guardrails in your AWS environment to help ensure that only your **trusted identities** are accessing **trusted resources** from **expected networks**



What is a data perimeter?



Trusted identities



Trusted resources



Expected networks

Data perimeter controls

Perimeter

Intent/control objective

Identity

Only trusted identities can access my resources

Only trusted identities are allowed from my network

Resource

My identities can access only trusted resources

Only trusted resources can be accessed from my network

Network

My identities can access resources only from expected networks

My resources can only be accessed from expected networks

Establishing a data perimeter

Primary tools for your data perimeter

1

Service control policies
(SCPs)

2

VPC endpoint policies

3

Resource-based policies

Data perimeter controls

Perimeter	Intent/control objective	Applied on	Using
Identity	Only trusted identities can access my resources	Resources	Resource-based policy
	Only trusted identities are allowed from my network	Network	VPC endpoint policy
Resource	My identities can access only trusted resources	Identities	SCP
	Only trusted resources can be accessed from my network	Network	VPC endpoint policy
Network	My identities can access resources only from expected networks	Identities	SCP
	My resources can only be accessed from expected networks	Resources	Resource-based policy

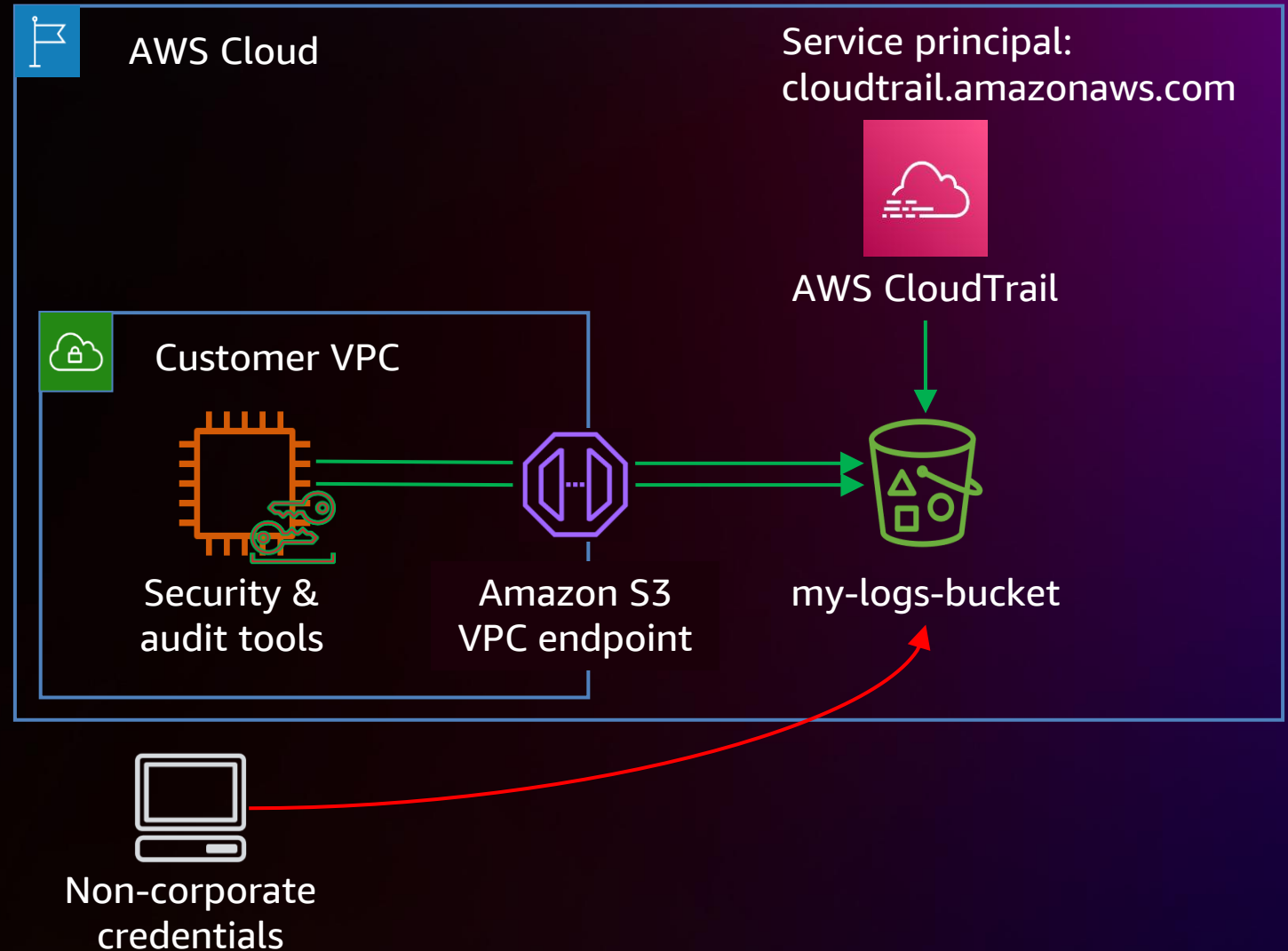
Identity perimeter on resources

ONLY TRUSTED IDENTITIES CAN ACCESS MY RESOURCES: RESOURCE-BASED POLICY

```
...
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": [
    "s3:ListBucket",
    "s3:PutObject*",
    "s3:GetObject*"
  ],
  "Resource": [
    "arn:aws:s3:::<my-logs-bucket>",
    "arn:aws:s3:::<my-logs-bucket>/*"
  ],
  "Condition": {
    "StringNotEqualsIfExists": {
      "aws:PrincipalOrgID": "<o-xxxxxxx>"
    },
    "BoolIfExists": {
      "aws:PrincipalIsAWSService": "false"
    }
  }
}
...
}
```



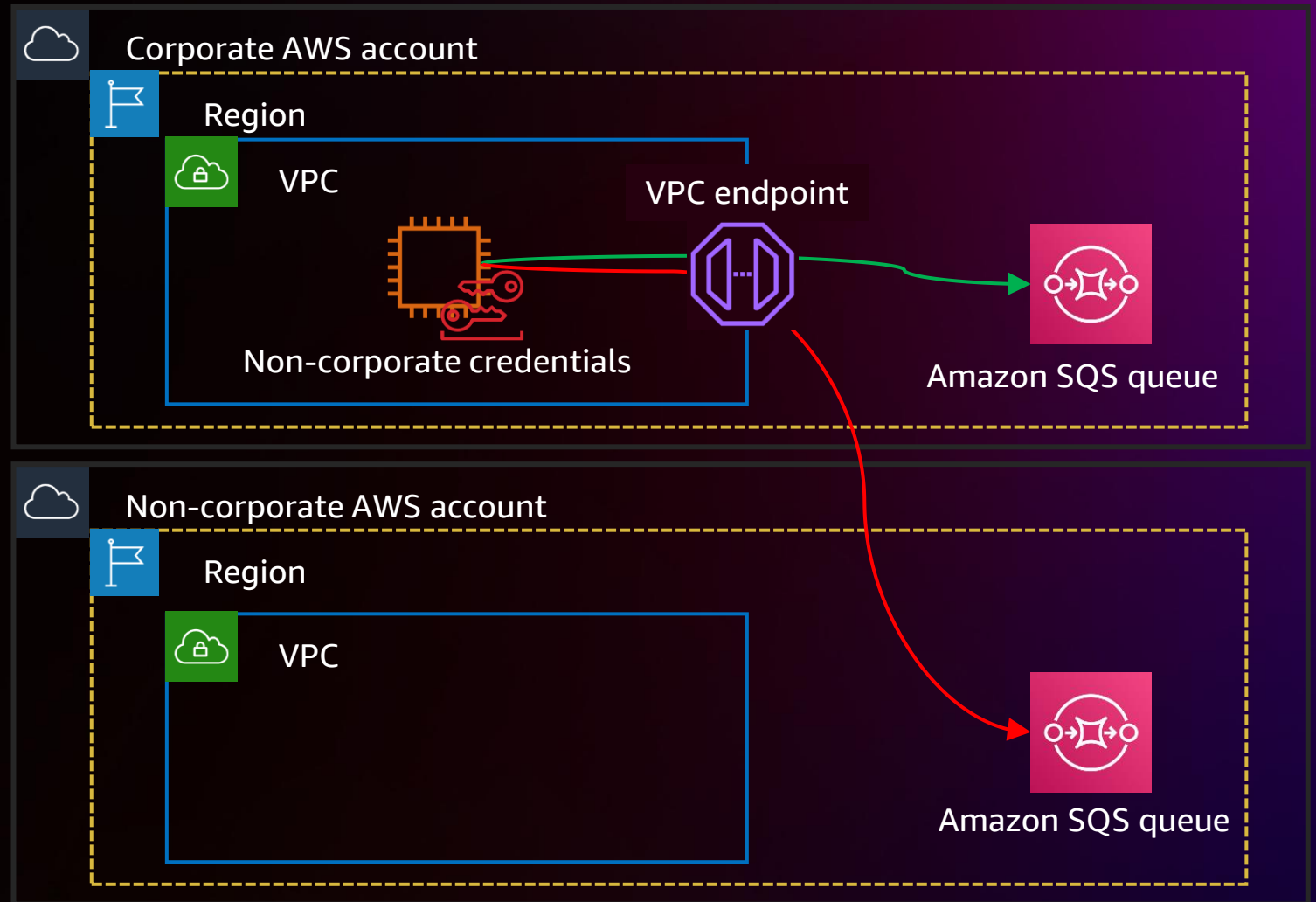
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Identity perimeter on network

ONLY TRUSTED IDENTITIES ARE ALLOWED FROM MY NETWORK: VPC ENDPOINT POLICY

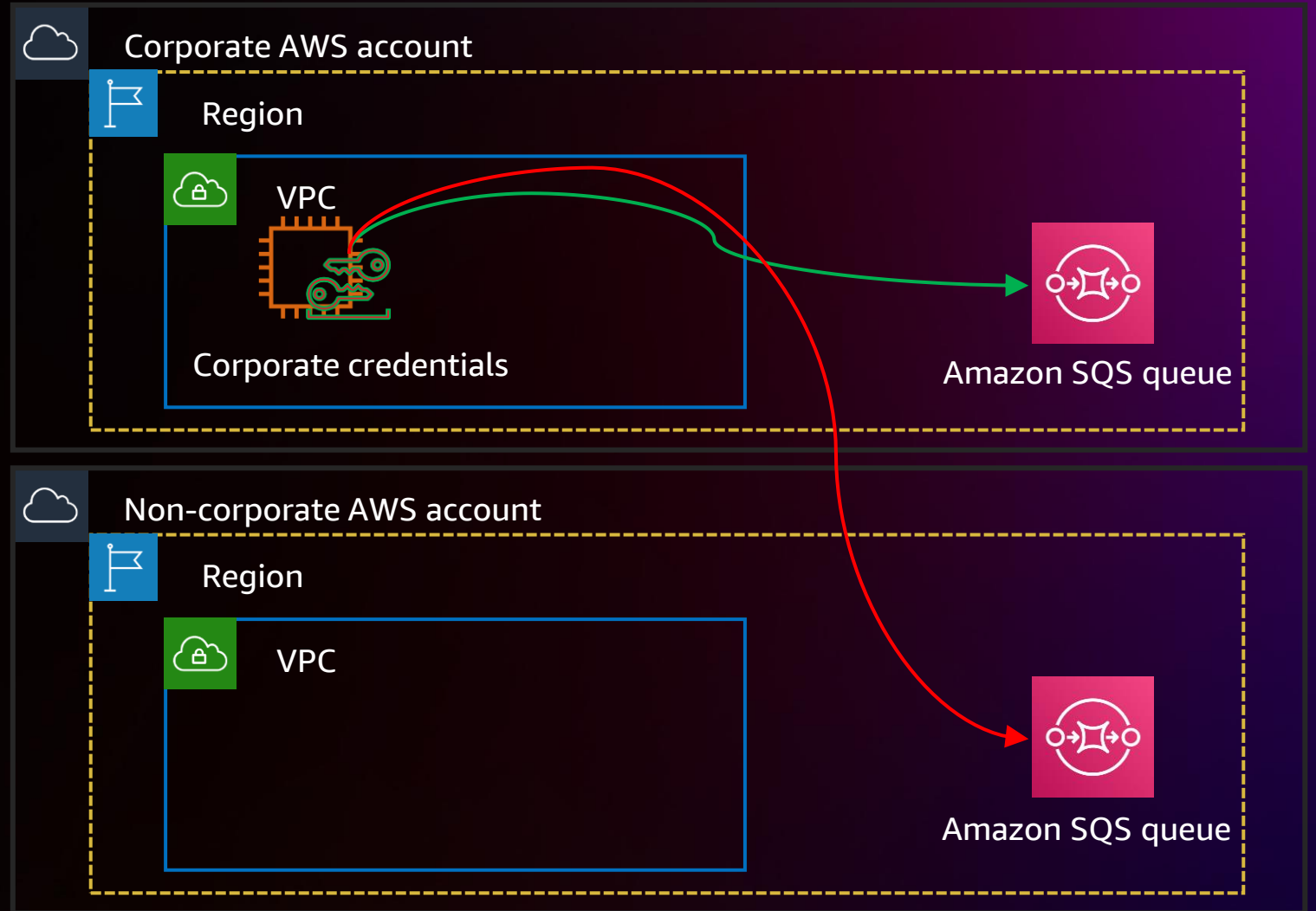
```
...
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": {
        "AWS": "*"
      },
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "o-xxxxxxx"
        }
      }
    }
  ]
}
```



Resource perimeter on identity

MY IDENTITIES CAN ACCESS ONLY TRUSTED RESOURCES: SCP

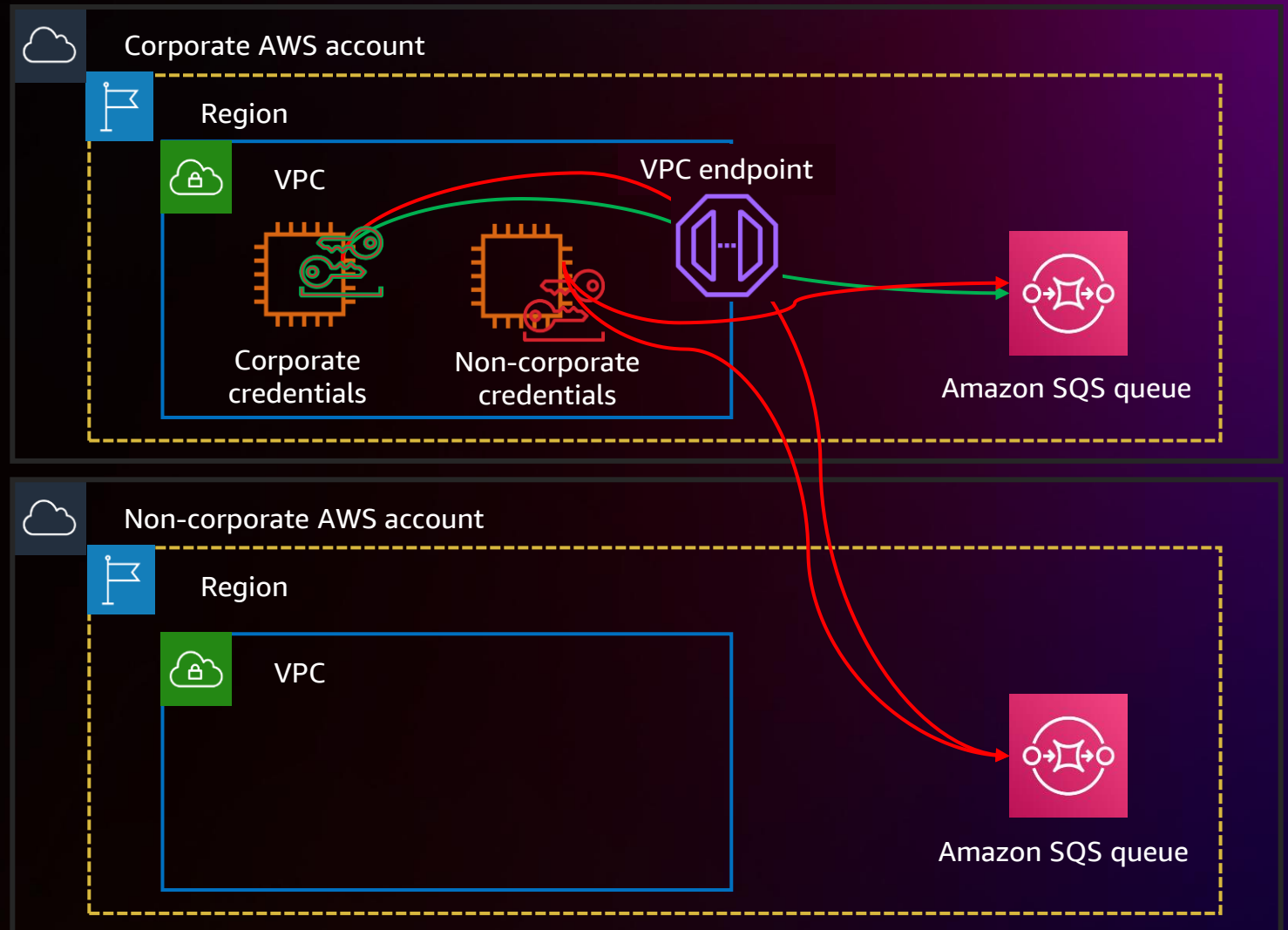
```
...
{
  "Effect": "Deny",
  "Action": [
    "sqs:SendMessage"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEqualsIfExists": {
      "aws:ResourceOrgID": "o-xxxxxxx"
    }
  }
}
```



Resource perimeter on network

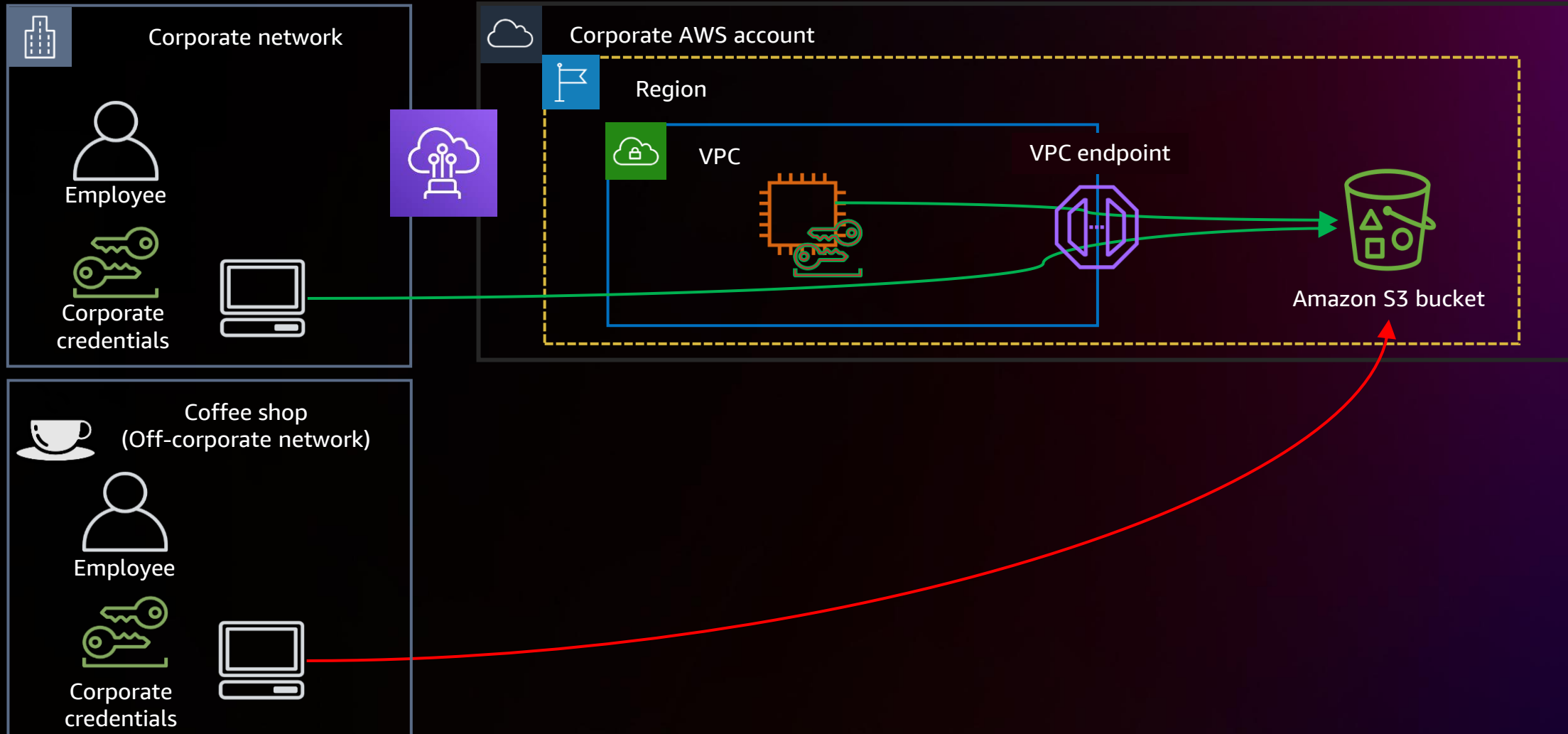
ONLY TRUSTED RESOURCES CAN BE ACCESSED FROM MY NETWORK: VPC ENDPOINT POLICY

```
...
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": {
        "AWS": "*"
      },
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "o-xxxxxxxxxx",
          "aws:ResourceOrgID": "o-xxxxxxxxxx"
        }
      }
    }
  ]
}
```



Network perimeter on resource

MY RESOURCES CAN ONLY BE ACCESSED FROM EXPECTED NETWORKS: RESOURCE-BASED POLICY



Network perimeter on resource

MY RESOURCES CAN ONLY BE ACCESSED FROM EXPECTED NETWORKS: RESOURCE-BASED POLICY

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "s3:*",
  "Resource": [
    "arn:aws:s3::my-data-bucket",
    "arn:aws:s3::my-data-bucket/*"
  ],
  "Condition": {
    "NotIpAddressIfExists": {
      "aws:SourceIp": "<cidr>"
    },
    "StringNotEqualsIfExists": {
      "aws:SourceVpc": "<vpc-xxxxxxx>"
    },
    "BoolIfExists": {
      "aws:PrincipalIsAWSService": "false",
      "aws:ViaAWSService": "false"
    },
    "ArnNotLikeIfExists": {
      "aws:PrincipalArn": "arn:aws:iam::<AccountNumber>:role/aws-service-role/*"
    }
  }
}
```

My corporate IP space

My AWS network

AWS service principal

AWS service using caller identity

Service-linked role



Data perimeter controls

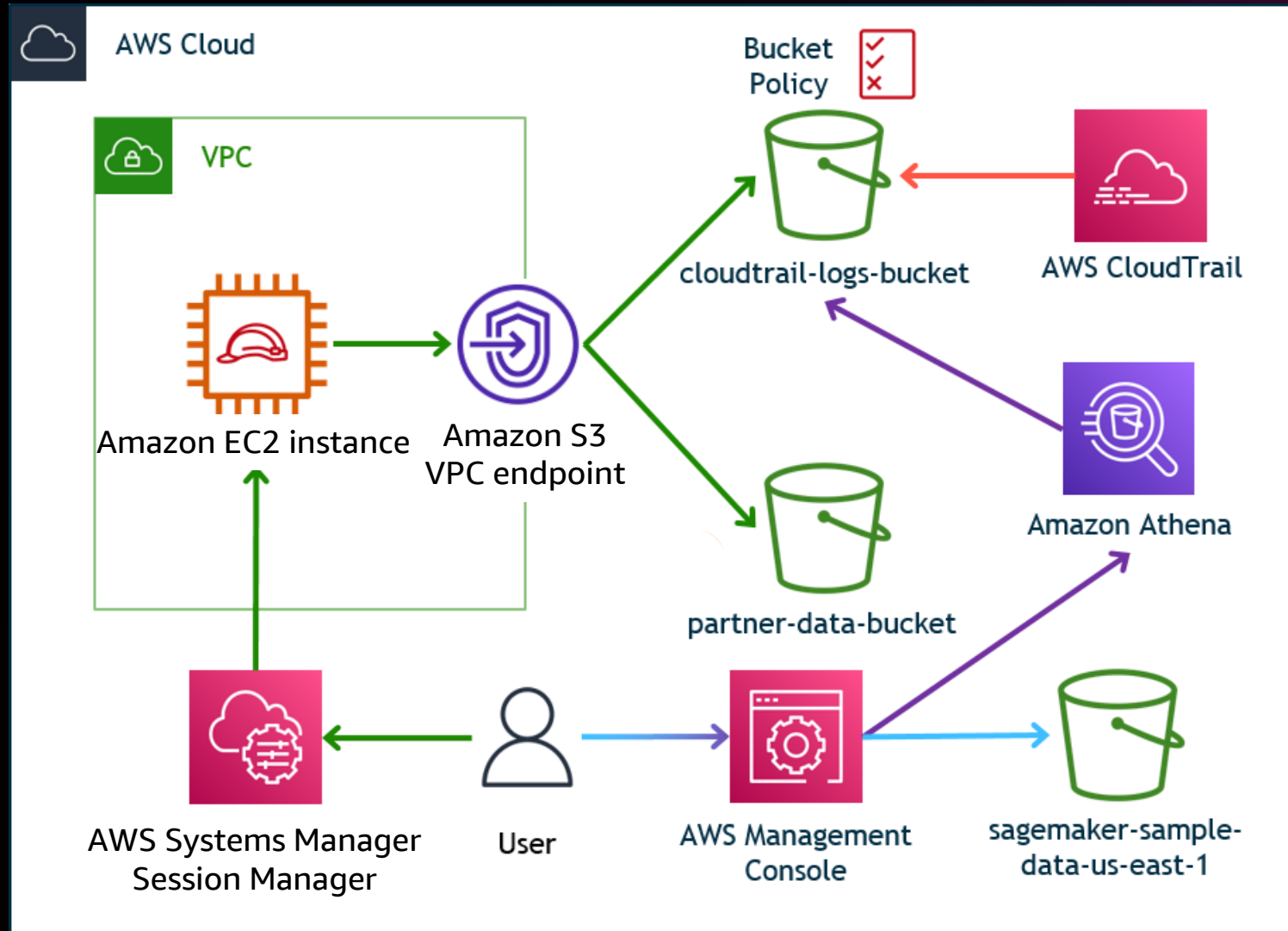
Perimeter	Intent/control objective	Applied on	Using	Primary IAM feature
Identity	Only trusted identities can access my resources	Resources	Resource-based policy	aws:PrincipalOrgID aws:PrincipalIsAWSService
	Only trusted identities are allowed from my network	Network	VPC endpoint policy	aws:PrincipalOrgID aws:PrincipalIsAWSService
Resource	My identities can access only trusted resources	Identities	SCP	aws:ResourceOrgID
	Only trusted resources can be accessed from my network	Network	VPC endpoint policy	aws:ResourceOrgID
Network	My identities can access resources only from expected networks	Identities	SCP	aws:SourceIp aws:SourceVpc/SourceVpce aws:ViaAWSService
	My resources can only be accessed from expected networks	Resources	Resource-based policy	aws:SourceIp aws:SourceVpc/SourceVpce aws:ViaAWSService aws:PrincipalIsAWSService



Hands-on



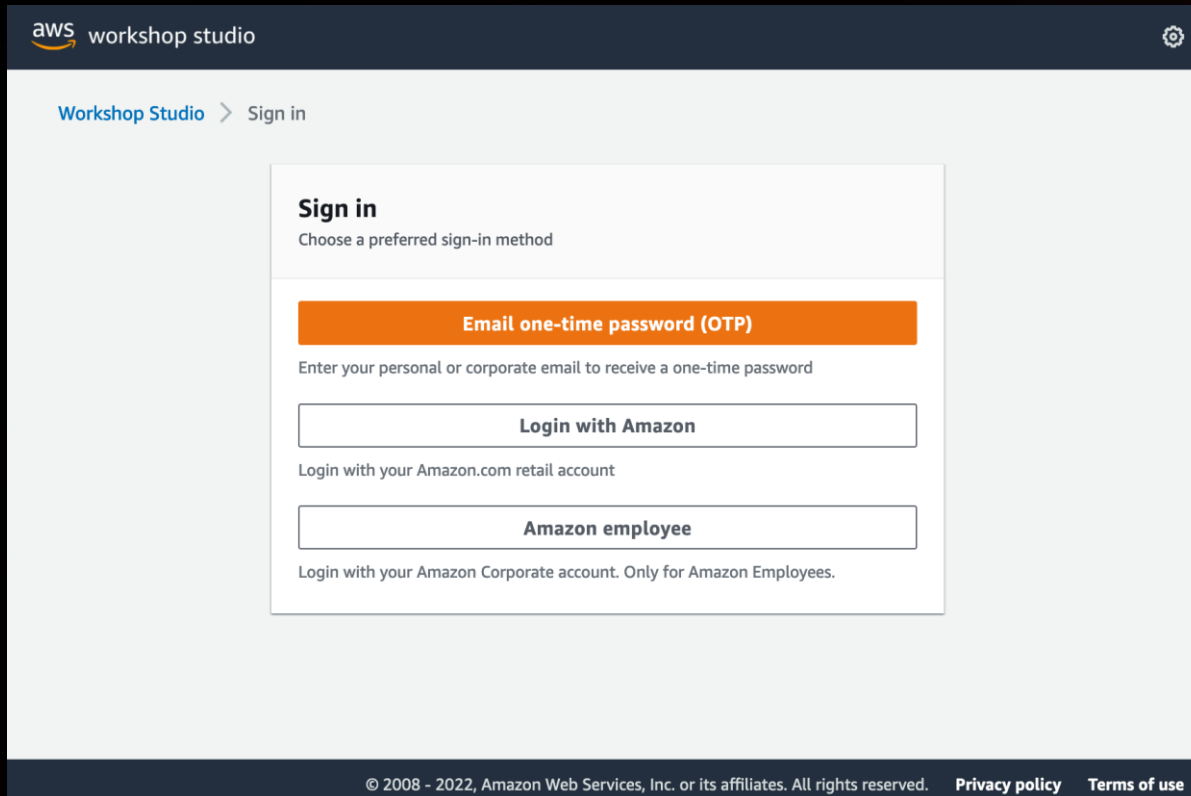
Workshop setup



Sign in using the access code

Link: <https://catalog.us-east-1.prod.workshops.aws/join>

Access code: 39af-08c656-fc



The screenshot shows the AWS Workshop Studio sign-in page. The header includes the AWS logo and 'workshop studio' text. The breadcrumb trail shows 'Workshop Studio > Sign in'. The main content area is titled 'Sign in' with the instruction 'Choose a preferred sign-in method'. There are three sign-in options: 'Email one-time password (OTP)' (highlighted in orange), 'Login with Amazon', and 'Amazon employee'. The footer contains copyright information and links to 'Privacy policy' and 'Terms of use'.

aws workshop studio

Workshop Studio > Sign in

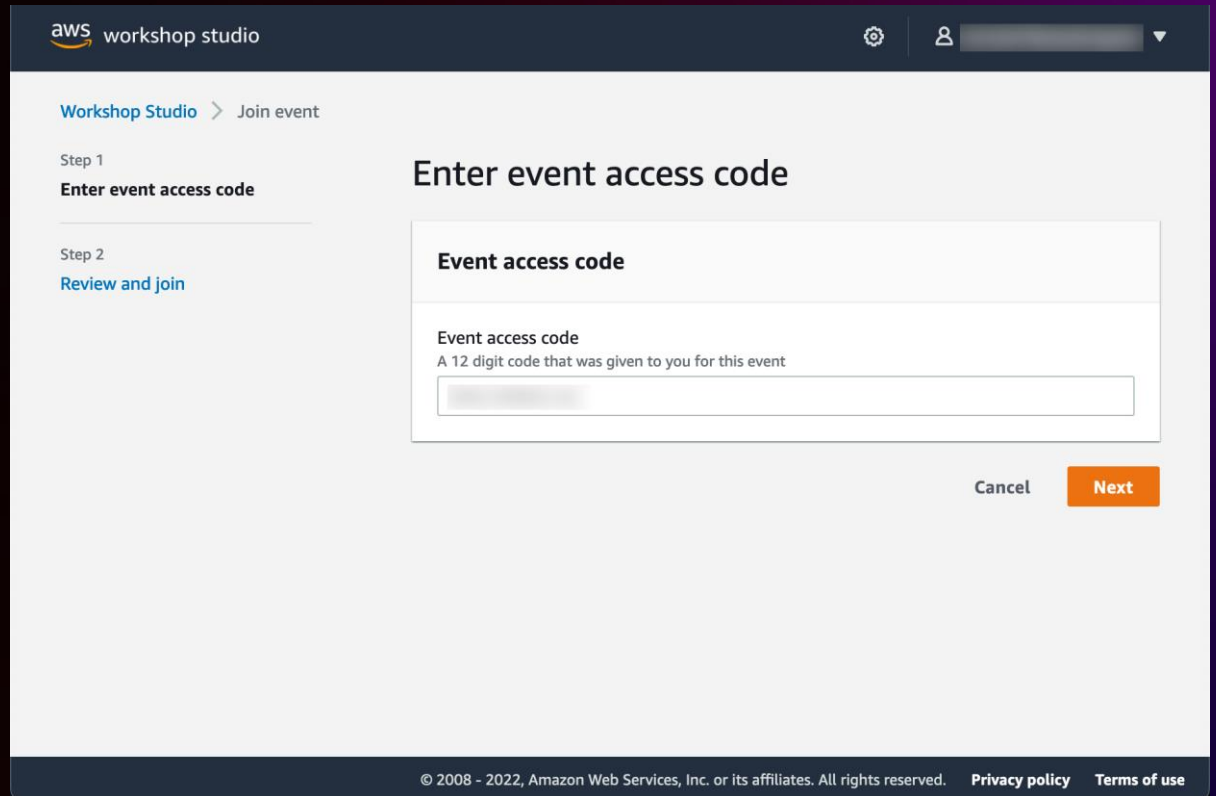
Sign in
Choose a preferred sign-in method

Email one-time password (OTP)
Enter your personal or corporate email to receive a one-time password

Login with Amazon
Login with your Amazon.com retail account

Amazon employee
Login with your Amazon Corporate account. Only for Amazon Employees.

© 2008 - 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy policy](#) [Terms of use](#)



The screenshot shows the AWS Workshop Studio 'Enter event access code' page. The header includes the AWS logo and 'workshop studio' text. The breadcrumb trail shows 'Workshop Studio > Join event'. The page is divided into two steps: 'Step 1: Enter event access code' (active) and 'Step 2: Review and join'. The main content area is titled 'Enter event access code' and contains a form for the 'Event access code' with a description: 'A 12 digit code that was given to you for this event'. There are 'Cancel' and 'Next' buttons at the bottom right. The footer contains copyright information and links to 'Privacy policy' and 'Terms of use'.

aws workshop studio

Workshop Studio > Join event

Step 1
Enter event access code

Step 2
[Review and join](#)

Enter event access code

Event access code
A 12 digit code that was given to you for this event

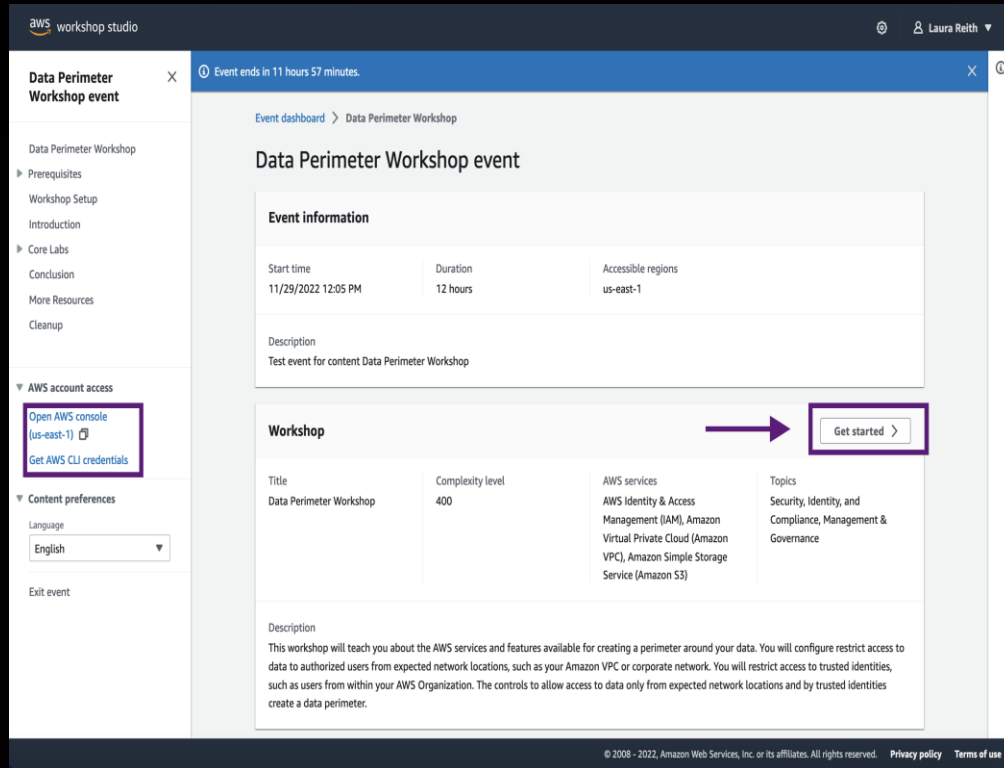
[Cancel](#) [Next](#)

© 2008 - 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy policy](#) [Terms of use](#)



Access AWS account and get started

Access the AWS Management Console



aws workshop studio

Event ends in 11 hours 57 minutes.

Data Perimeter Workshop event

Event dashboard > Data Perimeter Workshop

Event information

Start time	Duration	Accessible regions
11/29/2022 12:05 PM	12 hours	us-east-1

Description
Test event for content Data Perimeter Workshop

Workshop

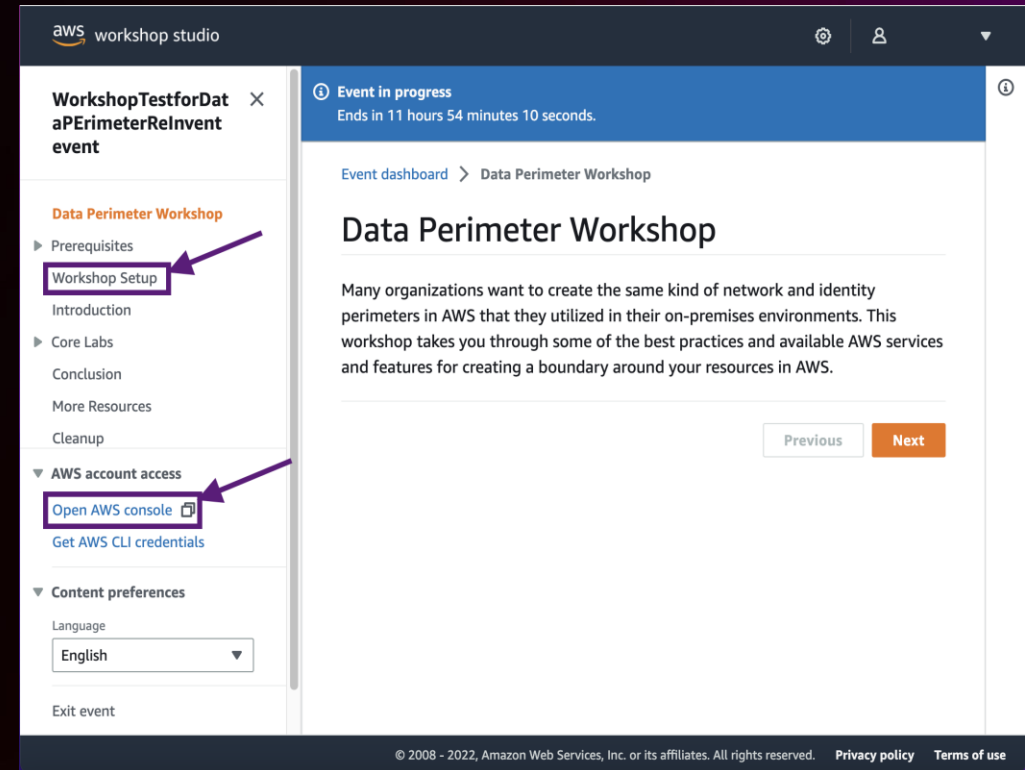
Title	Complexity level	AWS services	Topics
Data Perimeter Workshop	400	AWS Identity & Access Management (IAM), Amazon Virtual Private Cloud (Amazon VPC), Amazon Simple Storage Service (Amazon S3)	Security, Identity, and Compliance, Management & Governance

Description
This workshop will teach you about the AWS services and features available for creating a perimeter around your data. You will configure restrict access to data to authorized users from expected network locations, such as your Amazon VPC or corporate network. You will restrict access to trusted identities, such as users from within your AWS Organization. The controls to allow access to data only from expected network locations and by trusted identities create a data perimeter.

[Open AWS console \(us-east-1\)](#)
[Get AWS CLI credentials](#)

[Get started >](#)

© 2008 - 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy policy](#) [Terms of use](#)



aws workshop studio

Event in progress
Ends in 11 hours 54 minutes 10 seconds.

Event dashboard > Data Perimeter Workshop

Data Perimeter Workshop

Many organizations want to create the same kind of network and identity perimeters in AWS that they utilized in their on-premises environments. This workshop takes you through some of the best practices and available AWS services and features for creating a boundary around your resources in AWS.

[Previous](#) [Next](#)

WorkshopTestforDataPerimeterReinvent event

Data Perimeter Workshop

Prerequisites
Workshop Setup
Introduction
Core Labs
Conclusion
More Resources
Cleanup

AWS account access
[Open AWS console](#)
[Get AWS CLI credentials](#)

Content preferences
Language
English

Exit event

© 2008 - 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy policy](#) [Terms of use](#)

Thank you!

Laura Reith

reitlaur@amazon.com

Swara Gandhi

ganswara@amazon.com



Please complete the session survey in the **mobile app**



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.