

AWS re:Invent

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

SEC401-R

AWS Identity and Access Management (IAM) policy evaluation in action

Roberto Migli (he/him)

Principal Solutions Architect, Financial Services
AWS

Matt Luttrell (he/him)

Principal Solutions Architect, Identity
AWS



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

Agenda

IAM policy evaluation overview

Workshop labs overview

Hands-on labs

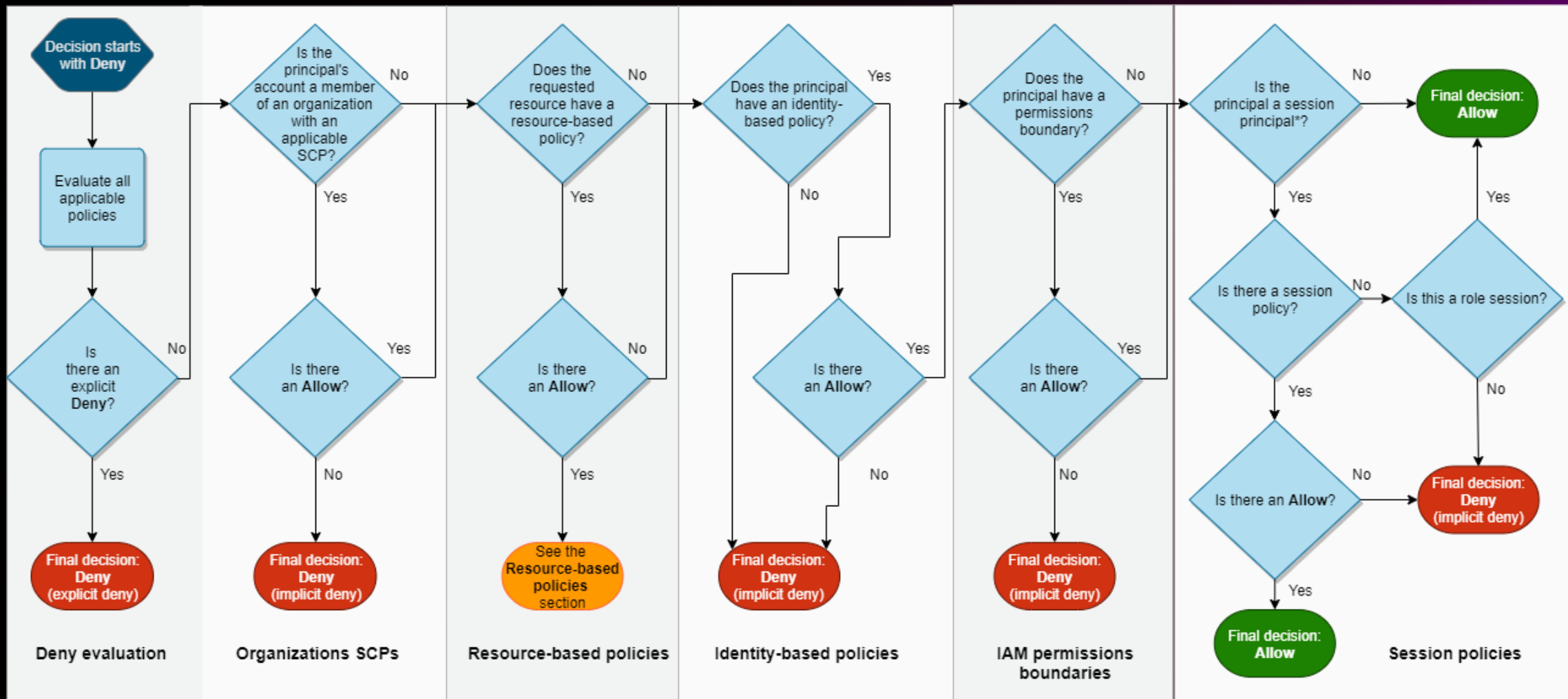
IAM policy evaluation overview



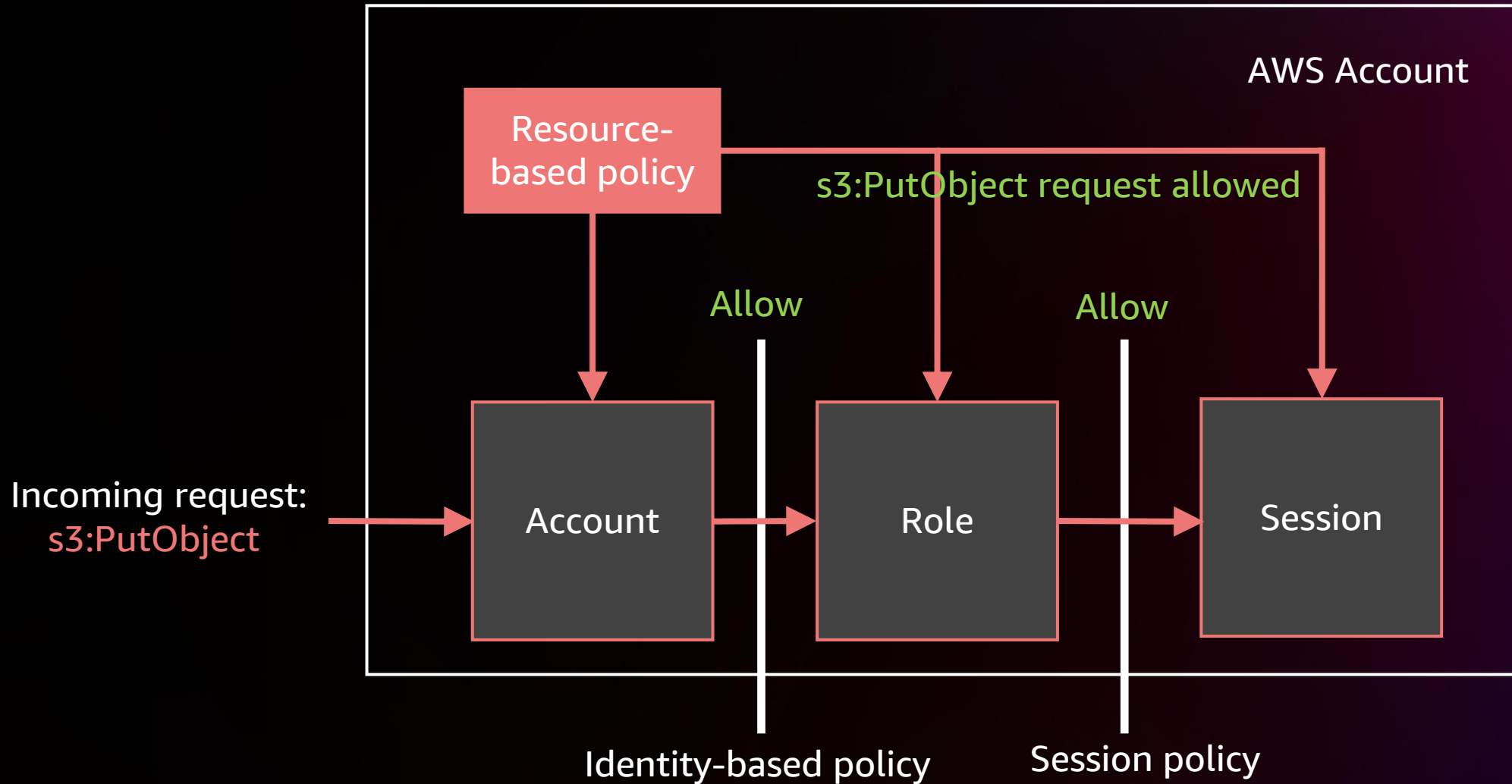
Policy evaluation definitions

- Implicit Deny
- Explicit Deny
- ~~Implicit Allow~~
- Explicit Allow

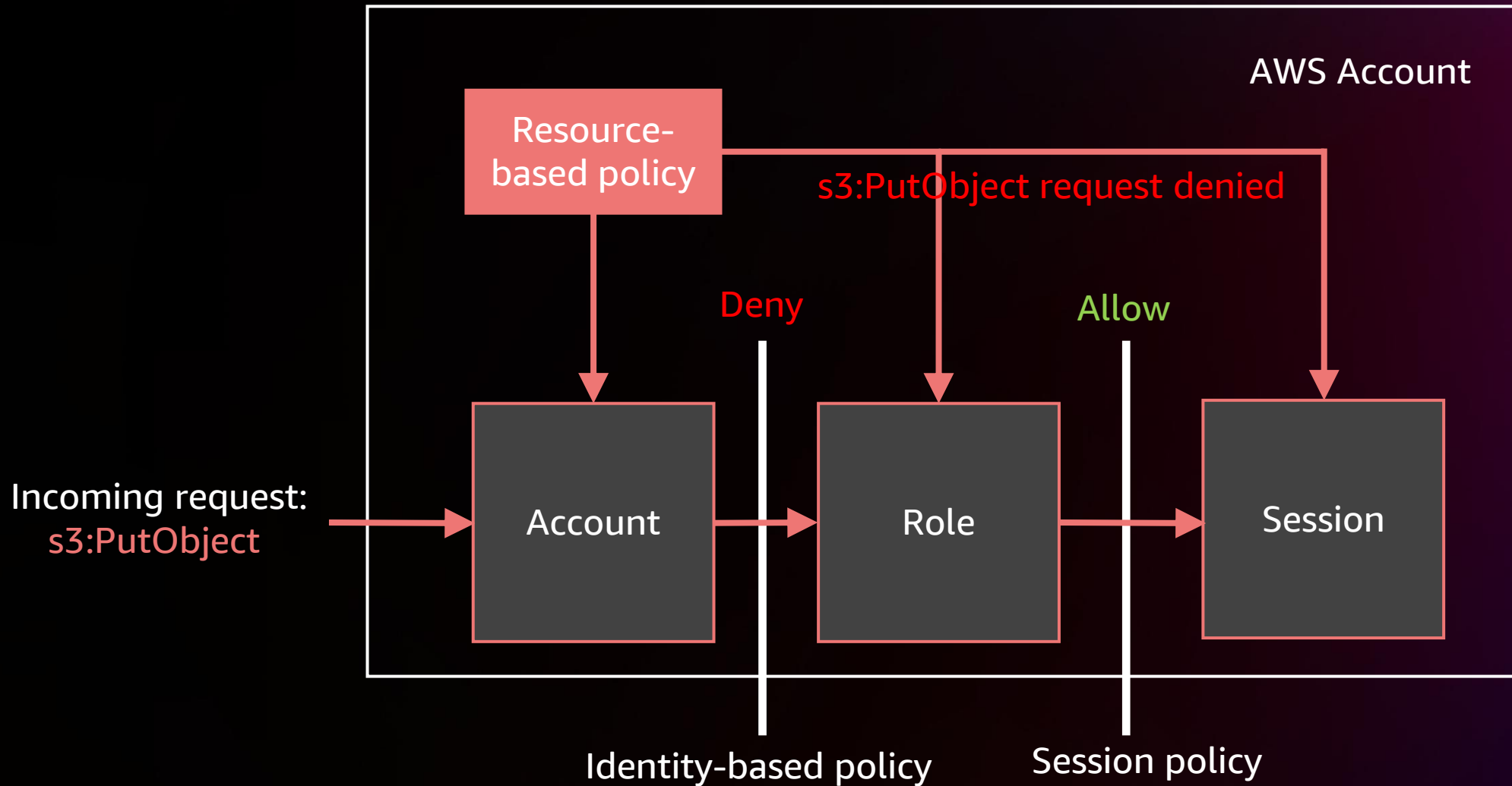
Policy evaluation workflow



Policy evaluation workflow – a new model



Policy evaluation workflow – a new model



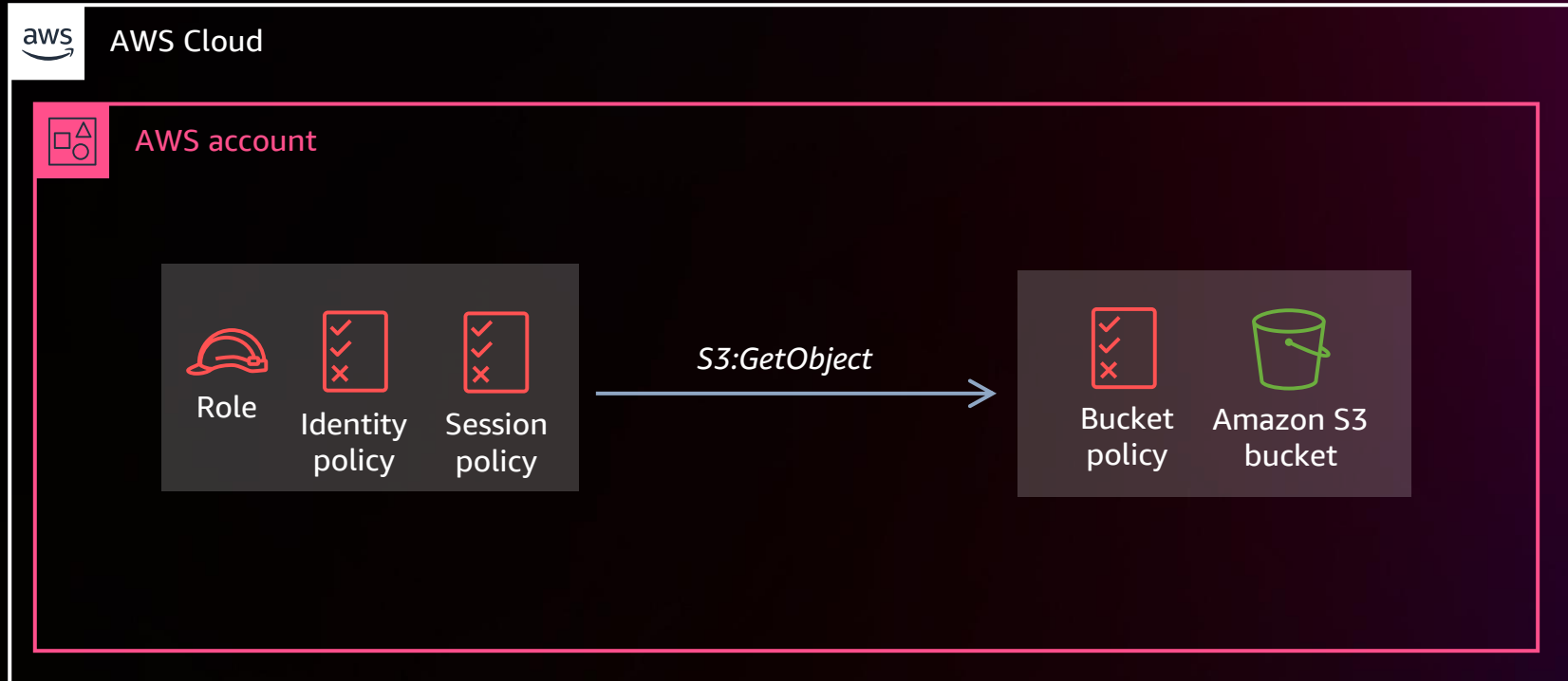
Rules of policy evaluation

- An explicit Deny always overrides an Allow
- A request must have an explicit Allow in all policies in the evaluation chain to be allowed

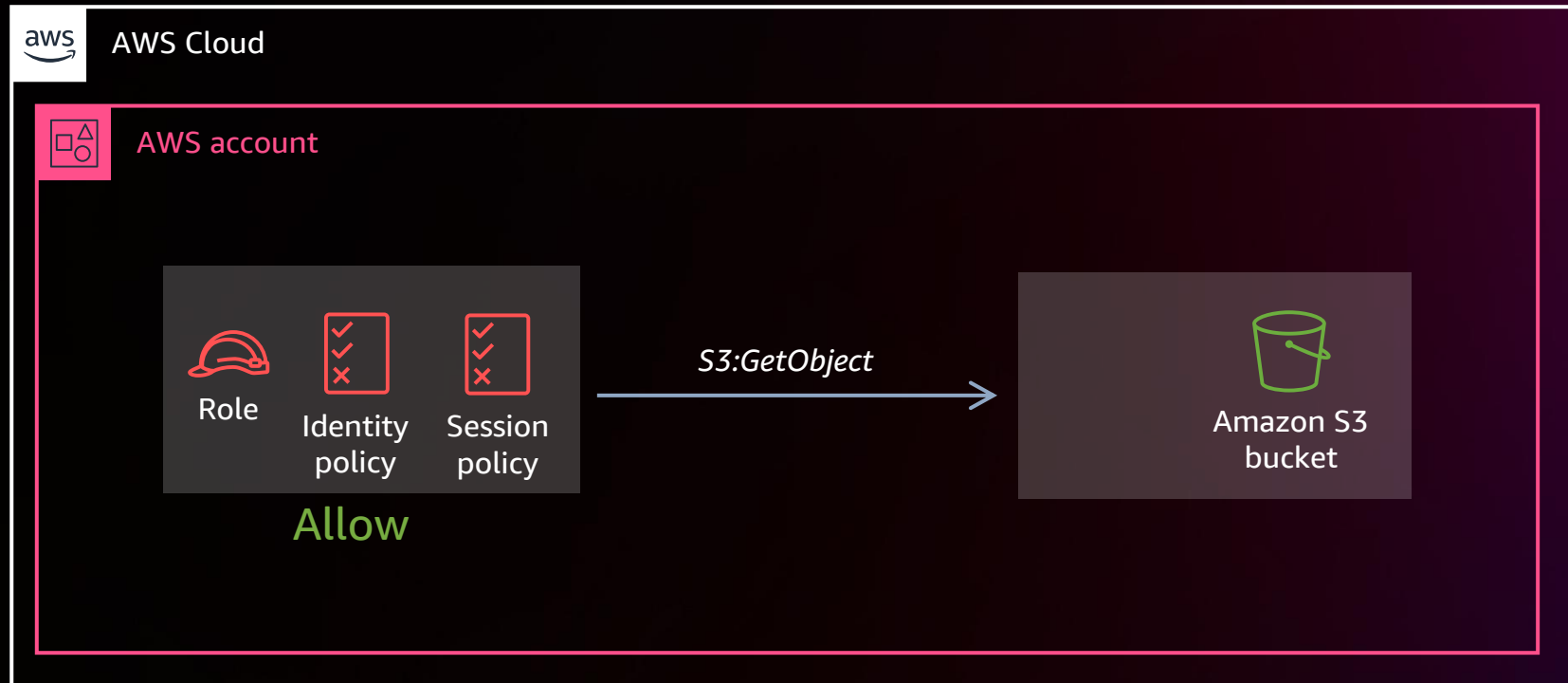
Workshop labs



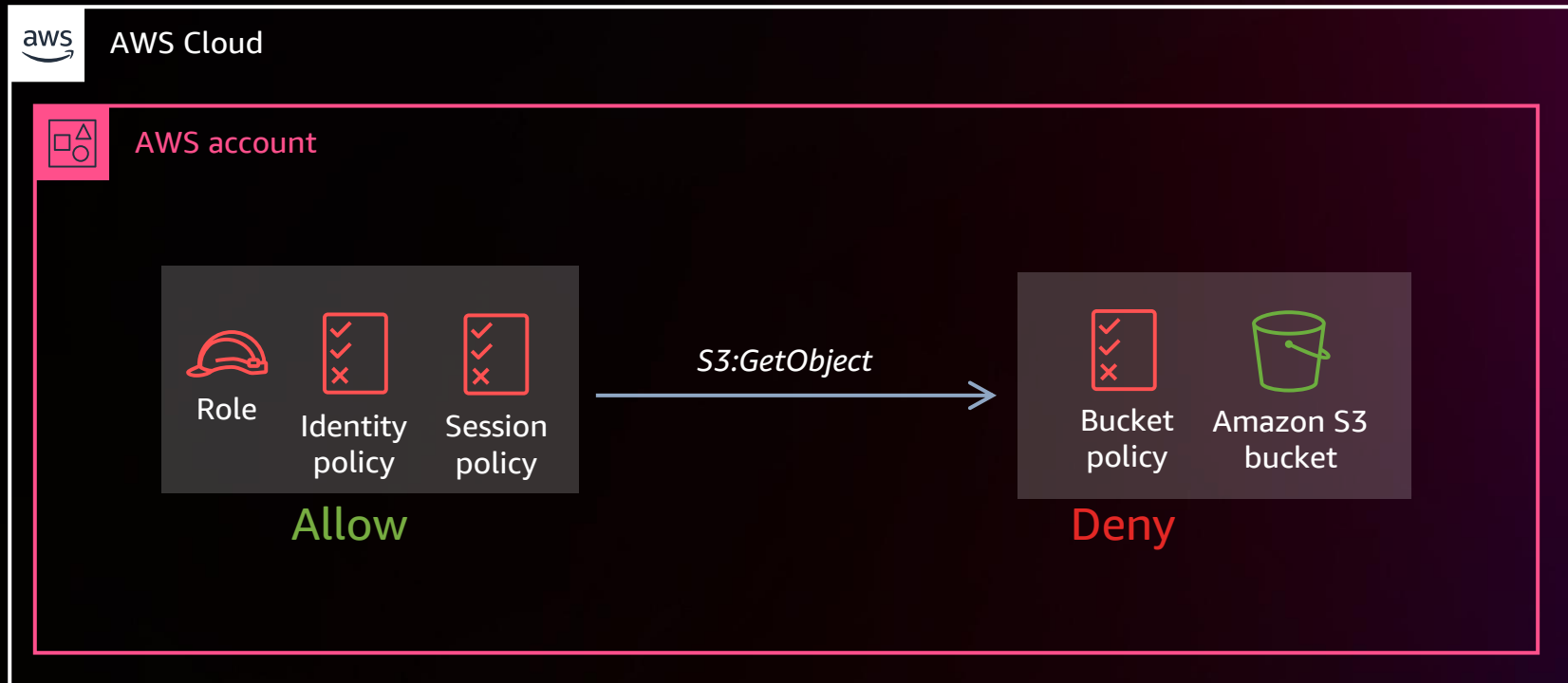
Lab 1: IAM policy evaluation logic with identities and resources



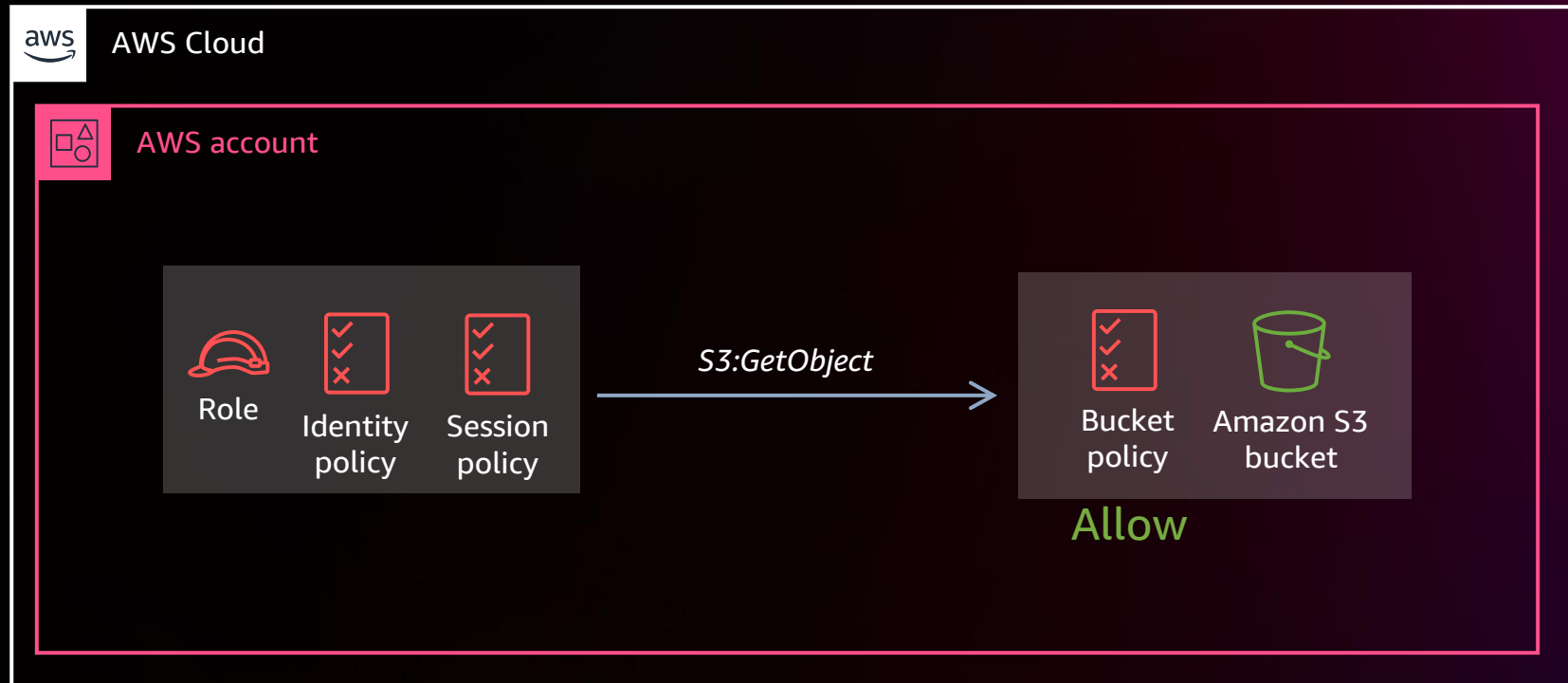
Lab 1 – Scenario 1



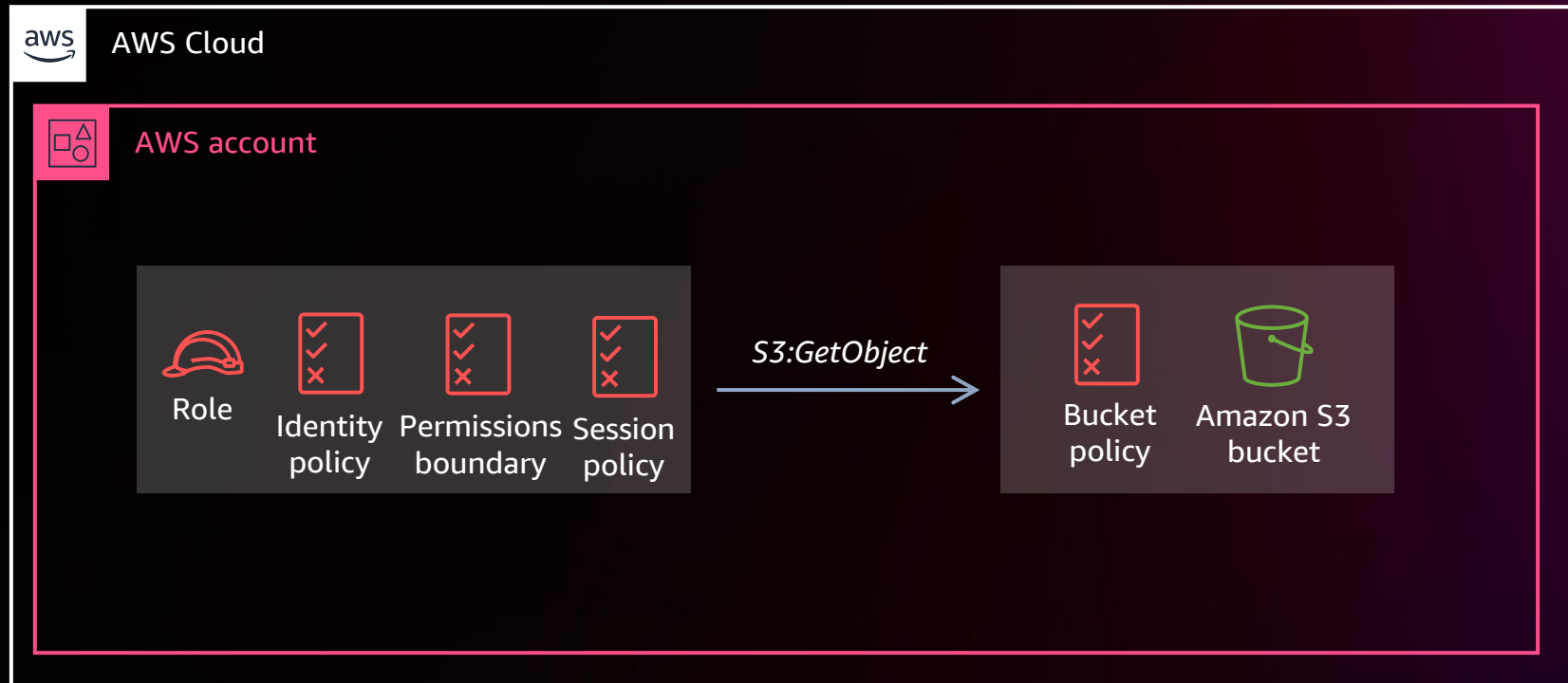
Lab 1 – Scenario 2



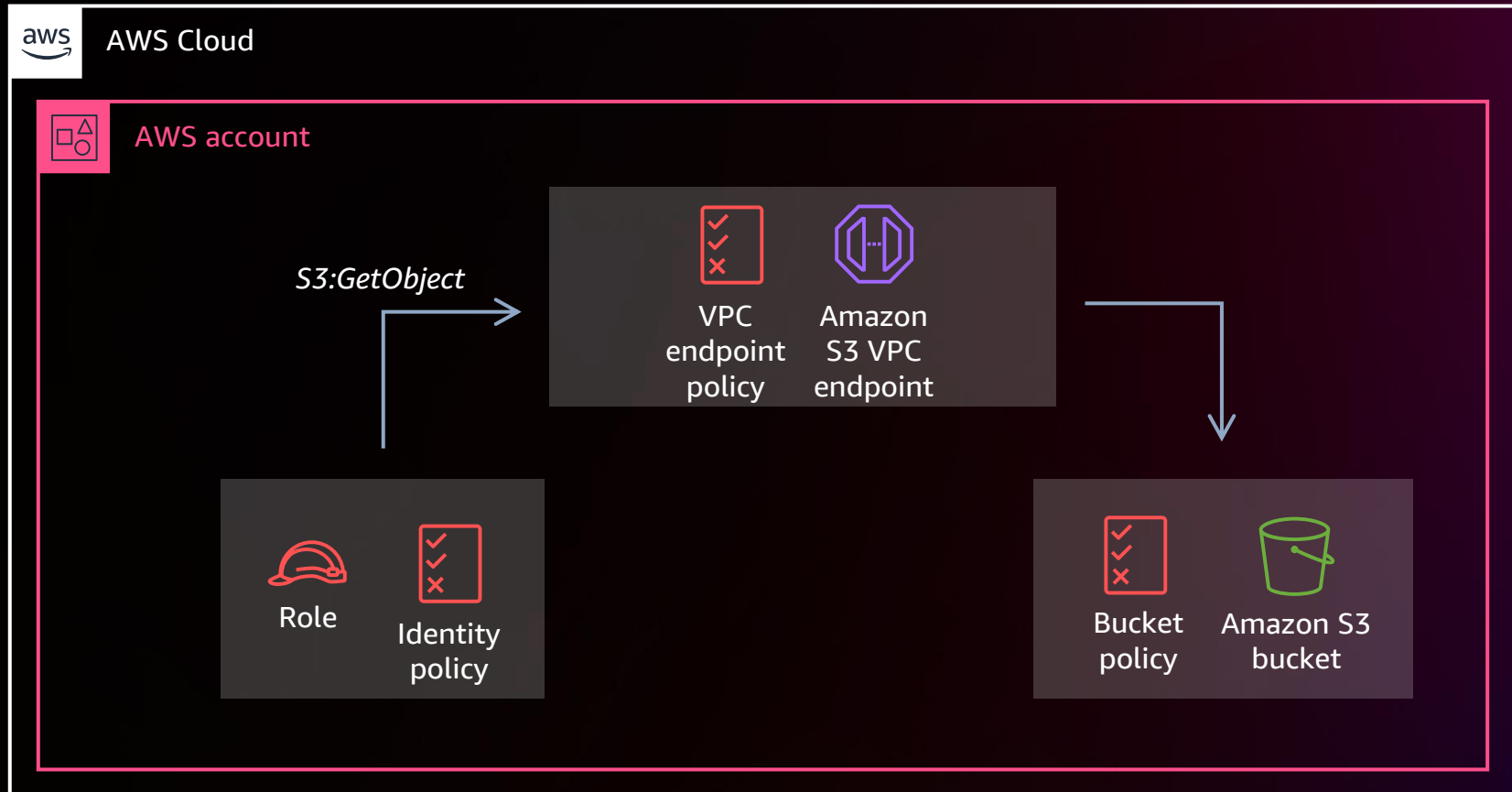
Lab 1 – Scenario 3



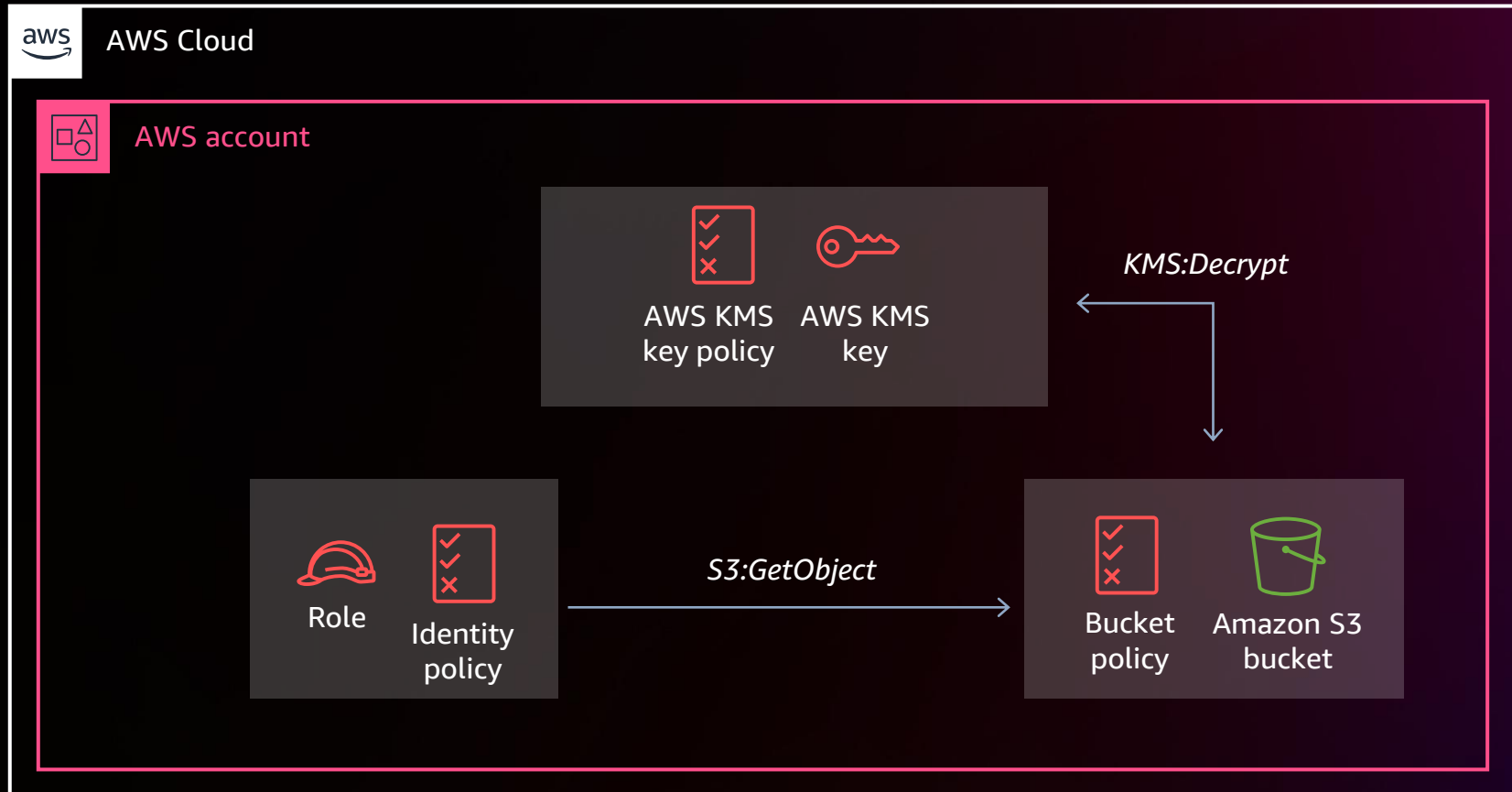
Lab 2: IAM policy evaluation logic with permissions boundaries



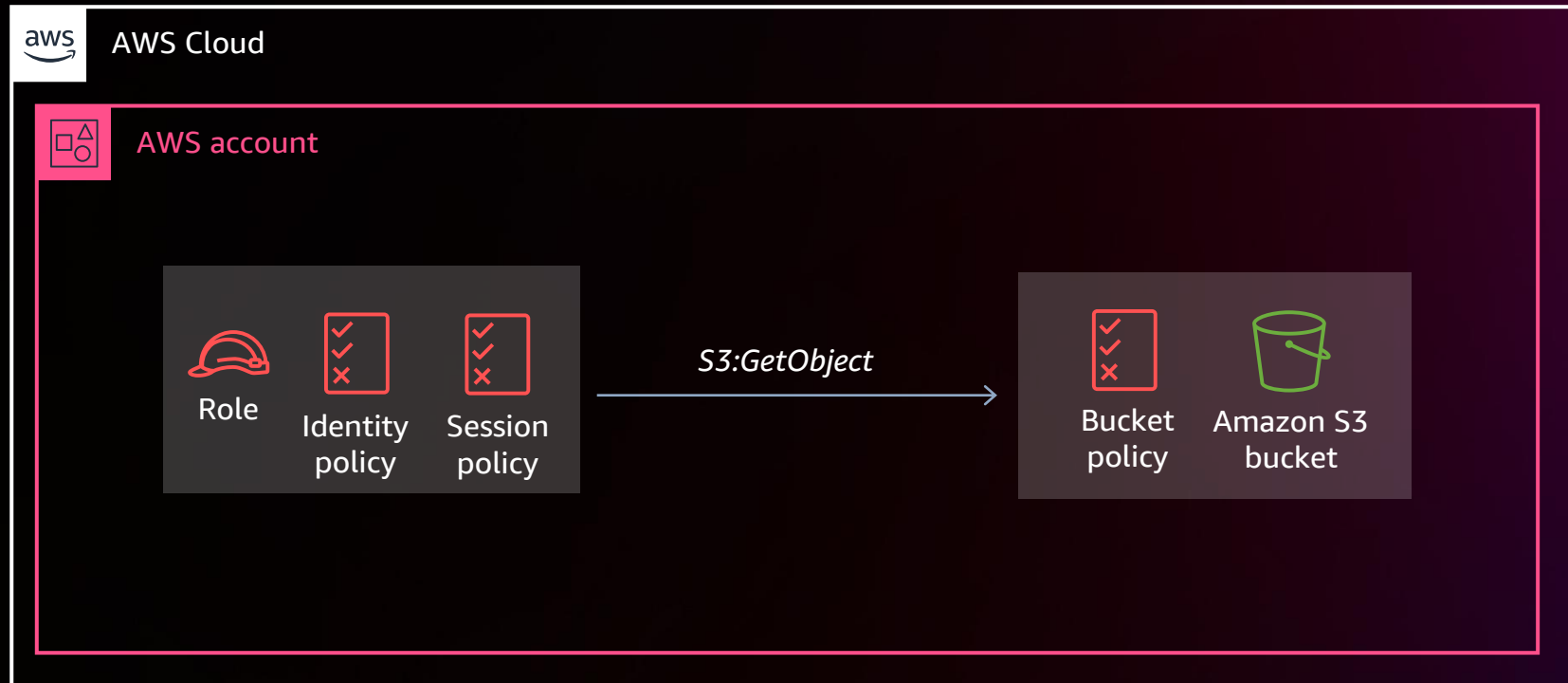
Lab 3: IAM policy evaluation logic with VPC endpoints



Lab 4: Working with AWS KMS key policies



Lab 5: Working with IAM policy conditions



The lab experience

- Run the labs at your own pace
- Lab 1 is a prerequisite to other labs
- We provide an AWS account for you
- No need to deploy AWS CloudFormation template
- Make sure to complete the “Prerequisites” steps (configure AWS Cloud9 IDE)
- Ask questions – raise your hands!

Step 1: Sign in via your preferred method

<https://catalog.workshops.aws/join?access-code=596d-01a83e-39>



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](#)

Step 2: Review terms and join event

aws workshop studio



Workshop Studio > Join event

Step 1

[Enter event access code](#)

Step 2

Review and join

Review and join

Event details

Name	Start time	Duration	Level
AWS General Immersion Day	9/23/2022 01:13 AM	12 hours	-

Description

AWS General Immersion Day

Terms and Conditions

Read and accept before joining the event

1. By using AWS Workshop Studio for the relevant event, you agree to the AWS Event Terms and Conditions and the AWS Acceptable Use Policy. You acknowledge and agree that are using an AWS-owned account that you can only access for the duration of the relevant event. If you find residual resources or materials in the AWS-owned account, you will make us aware and cease use of the account. AWS reserves the right to terminate the account and delete the contents at any time.

2. You will not: (a) process or run any operation on any data other than test data sets or lab-approved materials by AWS, and (b) copy, import, export or otherwise create derivate works of materials provided by AWS, including but not limited to, data sets.

3. AWS is under no obligation to enable the transmission of your materials through Event Engine and may, in its discretion, edit, block, refuse to post, or remove your materials at any time.

4. Your use of AWS Workshop Studio will comply with these terms and all applicable laws, and your access to AWS Workshop Studio will immediately and automatically terminate if you do not comply with any of these terms or conditions.

☒ I agree with the Terms and Conditions

Cancel

Previous

Join event

© 2008 - 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

[Privacy policy](#)

[Terms of use](#)



Thank you!



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

