AWS re:Invent

WPS320-R

Implement access control to data in AWS services using AWS KMS

Stephen Alexander
Senior Solutions Architect
Amazon Web Services

AWS re:Invent

aws

Agenda

Identity-based policies versus resource-based policies

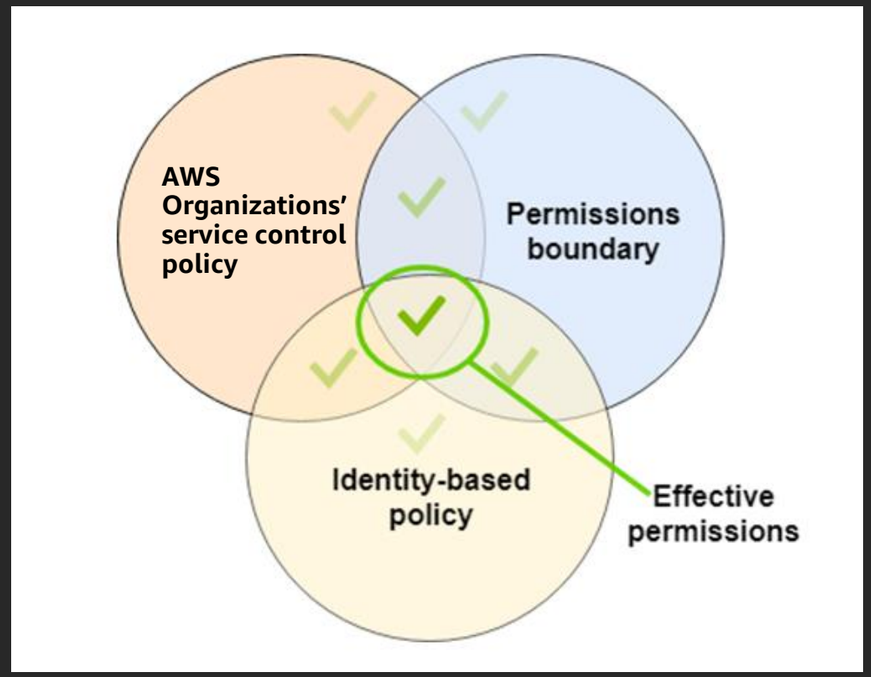
Types of AWS Key Management Service (AWS KMS) master keys

Hands-on lab

Types of policies in AWS

Identity-based policy

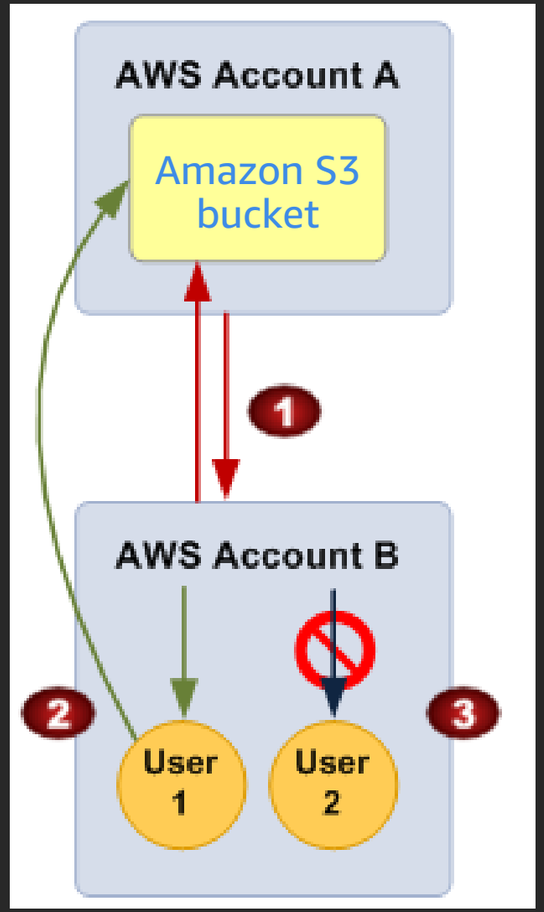
- Associated with AWS Identity and Access Management (IAM) identity or principal entity
  - User, group, or role



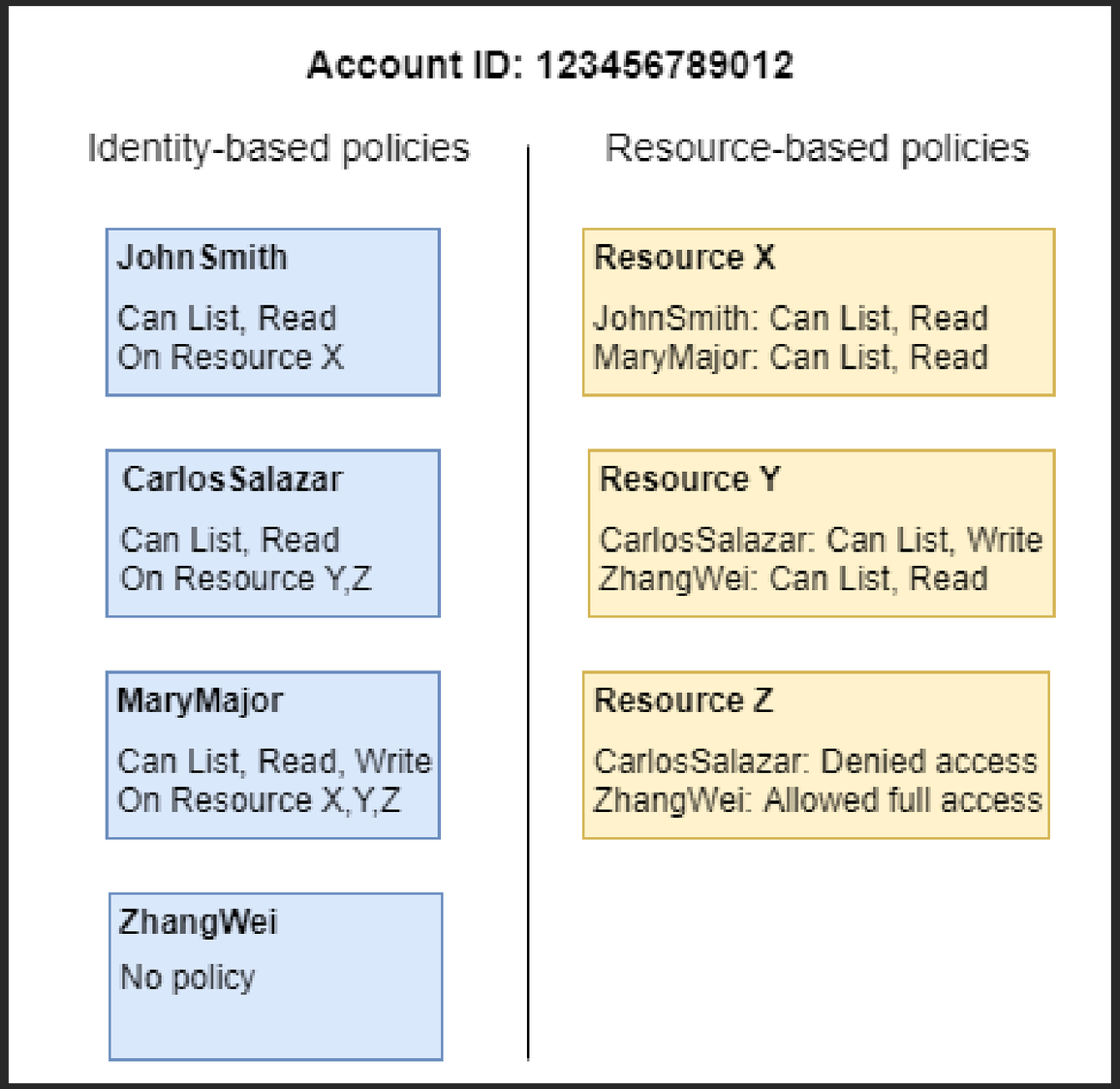
- States what the particular IAM principal can or cannot do

Resource-based policy

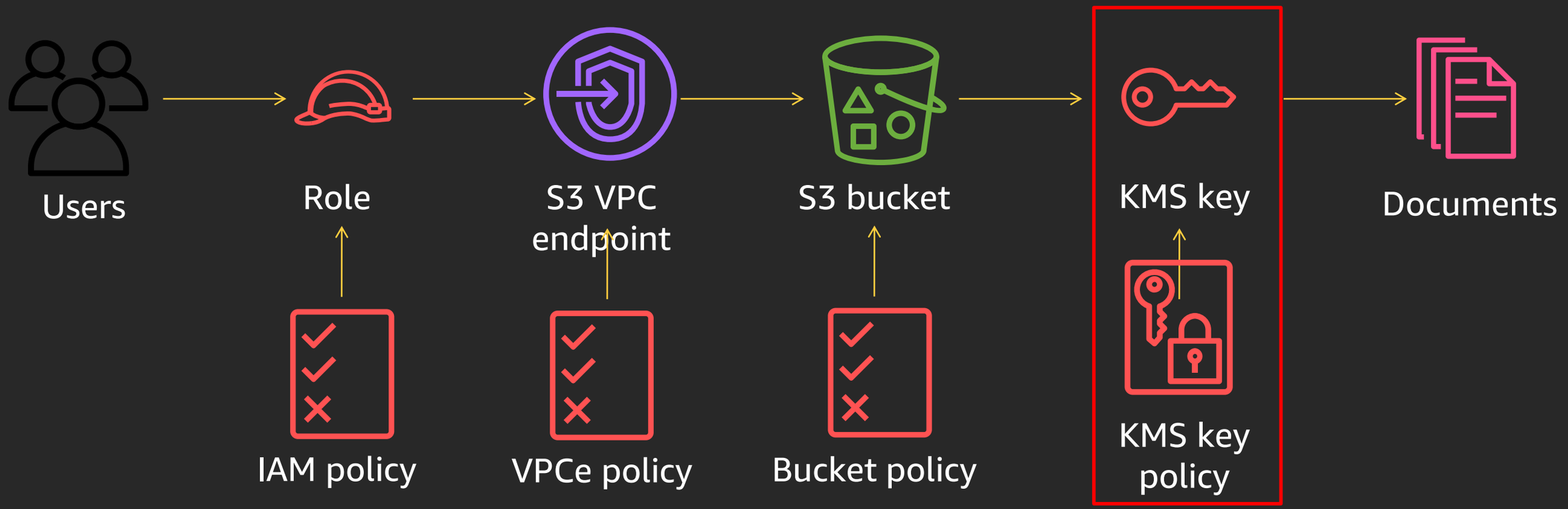
- Associated with the AWS resource
- Such as
  - Amazon Simple Storage Service (Amazon S3) bucket
  - Amazon Simple Queue Service (Amazon SQS) queue
  - Amazon CloudWatch Logs log group
  - AWS KMS keys
- Allows for cross-account access



Comparison


Account ID: 123456789012
Identity-based policies
Resource-based policies
John Smith
Can List, Read
On Resource X
Carlos Salazar
Can List, Read
On Resource Y,Z
MaryMajor
Can List, Read, Write
On Resource X,Y,Z
ZhangWei
No policy
Resource X
JohnSmith: Can List, Read
MaryMajor: Can List, Read
Resource Y
CarlosSalazar: Can List, Write
ZhangWei: Can List, Read
Resource Z
CarlosSalazar: Denied access
ZhangWei: Allowed full access

Defense in depth



Types of customer master keys (CMKs) in AWS KMS

Types of AWS KMS CMKs

	Can view CMK metadata	Can manage CMK	Used only for my AWS account
Customer managed CMK	Yes	**Yes**	Yes
AWS managed CMK	Yes	No	Yes
AWS owned CMK	No	No	No

Quiz

- Which CMK allows for cross-account access?
- Which CMK allows you to control specific actions?
- Which CMK creates data encryption keys?
- Which CMK can you audit the use of?
- Which CMK costs $1 a month?

Hands-on lab

- Log in to AWS account

- Follow instructions from print out

Thank you!

AWS re:Invent

aws

Please complete the session survey in the mobile app.