

### **COMMUNITY DAY**

# Access Denied: Understanding & Debugging AWS IAM

Peter Sankauskas | @pas256 | June 2025 he/him



## Typical AWS usage

## <u>interation</u>: Access Denied



#### You Need Permissions

billing information and (2) you have the required IAM permissions.

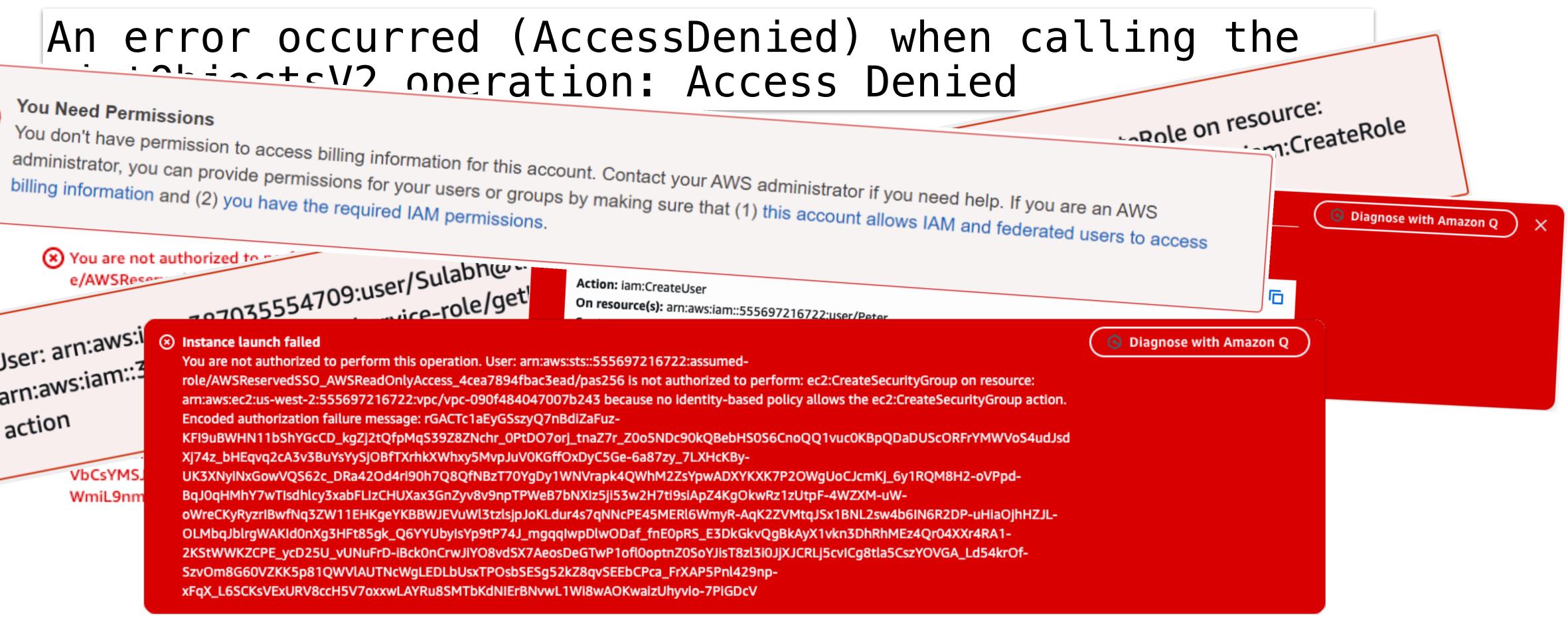
707035554709:user/Sulabn@-You are not authorized to e/AWSRese

Action: iam:CreateUser wice-role/get

🛞 User: arn:aws:i arn:aws:iam::3 action VbCsYMS. WmiL9nm

#### Instance launch failed

You are not authorized to perform this operation. User: arn:aws:sts::555697216722:assumedrole/AWSReservedSSO\_AWSReadOnlyAccess\_4cea7894fbac3ead/pas256 is not authorized to perform: ec2:CreateSecurityGroup on resource: arn:aws:ec2:us-west-2:555697216722:vpc/vpc-090f484047007b243 because no identity-based policy allows the ec2:CreateSecurityGroup action. Encoded authorization failure message: rGACTc1aEyGSszyQ7nBdiZaFuz-KFI9uBWHN11bShYGcCD\_kgZj2tQfpMqS39Z8ZNchr\_0PtDO7orj\_tnaZ7r\_Z0o5NDc90kQBebHS0S6CnoQQ1vuc0KBpQDaDUScORFrYMWVoS4udJsd Xj74z\_bHEqvq2cA3v3BuYsYySjOBfTXrhkXWhxy5MvpJuV0KGffOxDyC5Ge-6a87zy\_7LXHcKBy-UK3XNyiNxGowVQS62c\_DRa42Od4ri90h7Q8QfNBzT70YgDy1WNVrapk4QWhM2ZsYpwADXYKXK7P2OWgUoCJcmKj\_6y1RQM8H2-oVPpd-BqJ0qHMhY7wTIsdhlcy3xabFLIzCHUXax3GnZyv8v9npTPWeB7bNXIz5ji53w2H7ti9siApZ4KgOkwRz1zUtpF-4WZXM-uWoWreCKyRyzrIBwfNq3ZW11EHKgeYKBBWJEVuWl3tzlsjpJoKLdur4s7qNNcPE45MERl6WmyR-AqK2ZVMtqJSx1BNL2sw4b6IN6R2DP-uHiaOjhHZJL-OLMbqJblrgWAKId0nXg3HFt85gk\_Q6YYUbyIsYp9tP74J\_mgqqIwpDlwODaf\_fnE0pRS\_E3DkGkvQgBkAyX1vkn3DhRhMEz4Qr04XXr4RA1-2KStWWKZCPE\_ycD25U\_vUNuFrD-iBck0nCrwJiYO8vdSX7AeosDeGTwP1ofl0optnZ0SoYJisT8zl3i0JjXJCRLj5cvICg8tla5CszYOVGA\_Ld54krOf-SzvOm8G60VZKK5p81QWVlAUTNcWgLEDLbUsxTPOsbSESg52kZ8qvSEEbCPca\_FrXAP5Pnl429npxFqX\_L6SCKsVExURV8ccH5V7oxxwLAYRu8SMTbKdNIErBNvwL1Wi8wAOKwaizUhyvio-7PiGDcV



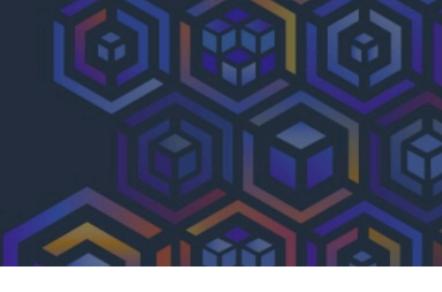




## Replace this talk with Amazon Q

You don't have sufficient permissions to Diagnose with Amazon Q. ∞ You or your AWS administrator can grant access by adding the AmazonQDeveloperAccess policy to your IAM identity. For more information, see the AWS managed policies for Amazon Q.





### Standard IAM error message format

- User: arn:aws:sts::12345678901:sux/to-be-you is not authorized to perform aws:SimpleAction on resource arn:aws:ec2:us-tirefire-1:12345678901:service/abcd1234 because
- I haven't had my coffee yet.





- How is IAM is designed?
- How does it evaluate policies?
- What are the different types of policies?
- When is each one useful?
- What is this error trying to tell me?
- What techniques can I use to debug permission errors?





## Peter Sankauskas

### **Strategic Engineering Hiring Partner** ② PAS Ventures

### A former CTO, now helping you hire great engineers!

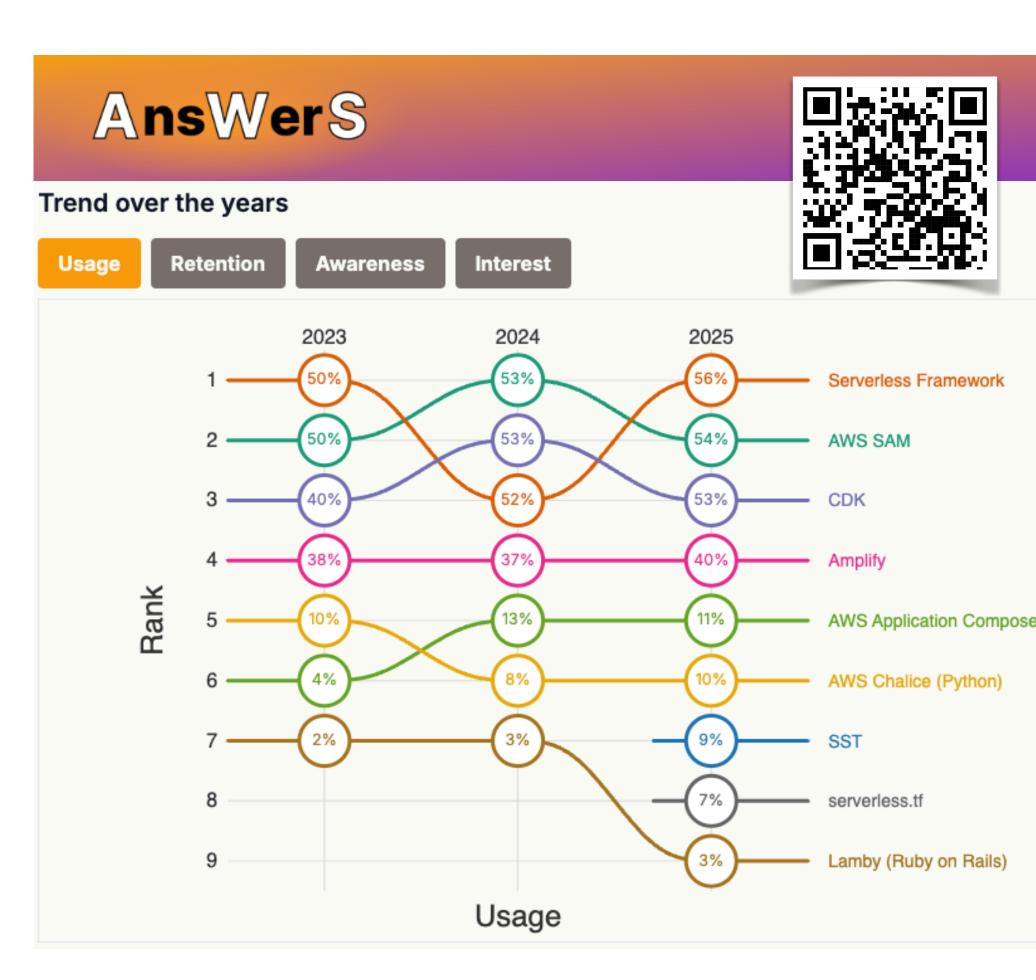
- AWS Community Hero since 2014
- Advanced AWS Meetup in SF
- Answers for AWS community survey







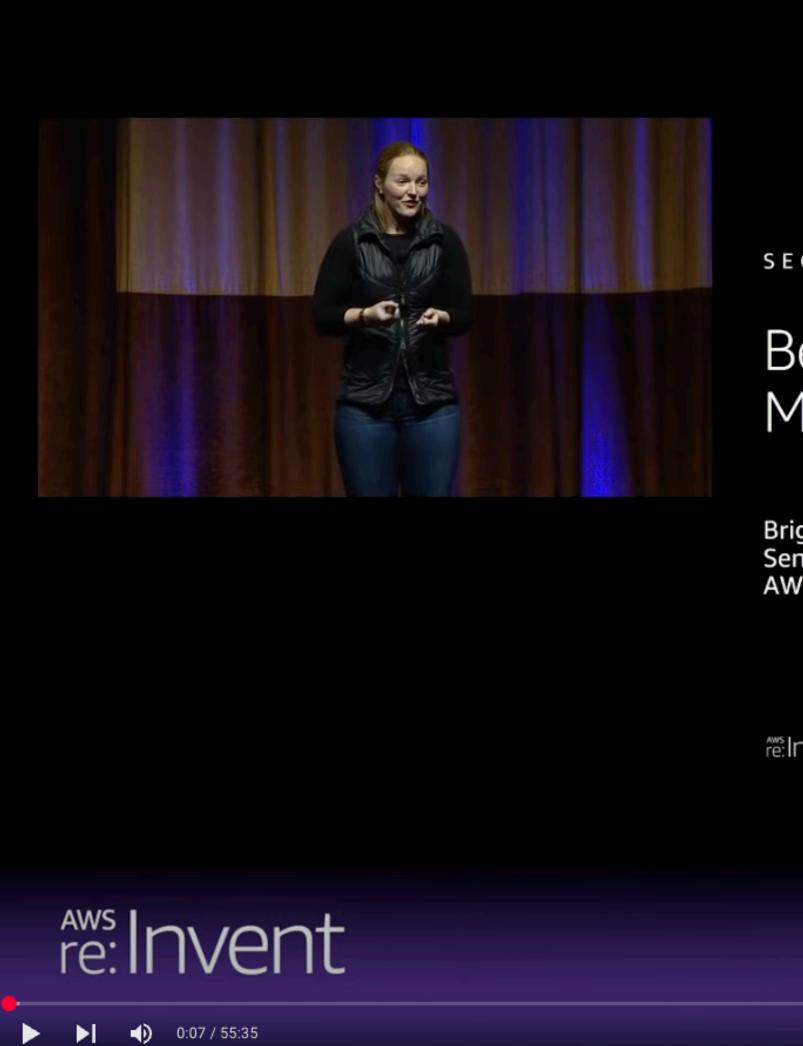






### Inspiration

a.k.a great artist steel



S E C 3 1 6

Brigid Johnson Senior Manager of Product Management AWS Identity

re: Invent

#### Become an IAM Policy Master in 60 Minutes or Less

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserve



aws

••• •• •• ••

aws



## What are IAM Policies?

### Specification

which conditions.

#### Enforcement 2)

IAM enforces this access by *evaluating* the AWS request with the policies you defined and returns either allow or deny.







## IAM Policy Language - PARC model

```
"Statement": [{
  "Sid": "unique",
  "Effect": "effect",
  "Principal": "principal",
  "Action": "action",
  "Resource": "resource",
  "Condition": {
    "operator": { "key": "value" }
  }
}]
```

**Principal** - The entity that is allowed or denied access arn:aws:iam::123456789012:user/you

**Action** - Type of access that is allowed or denied s3:Put0bject

**Resource** - The AWS resource(s) the action will act on arn:aws:s3:::my-bucket

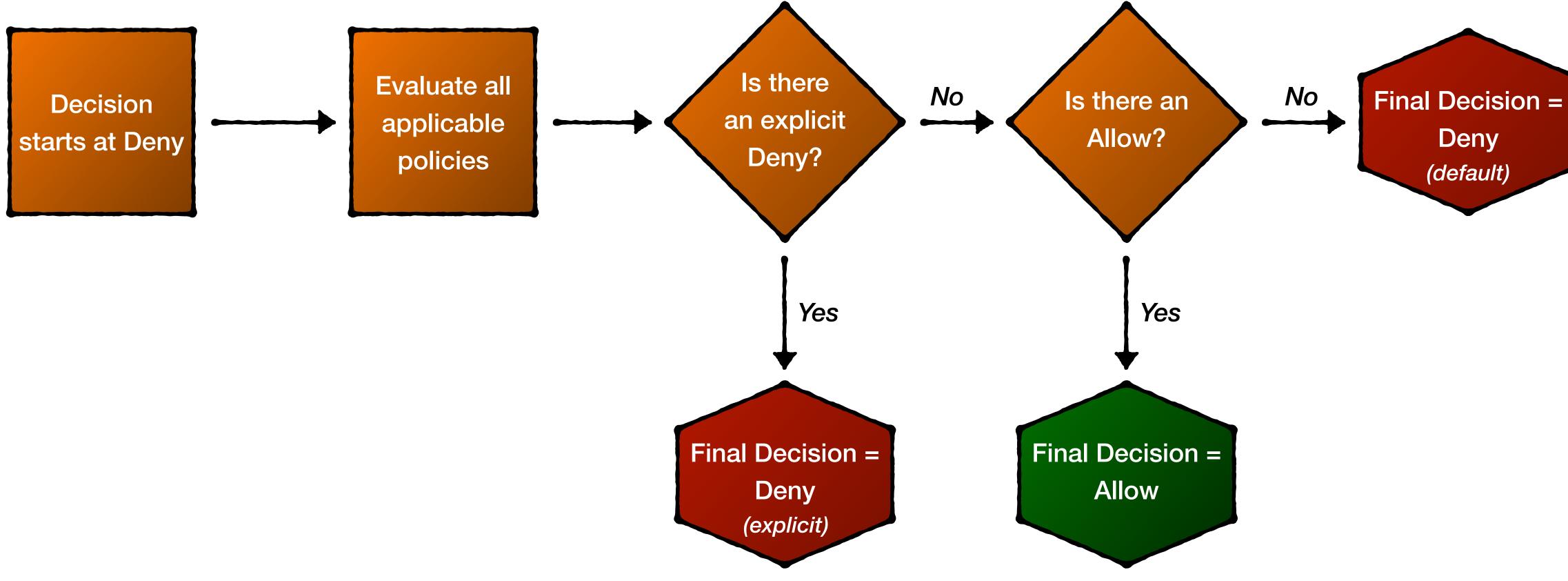
**Condition** - But only under these conditions aws:MultiFactorAuthPresent = true

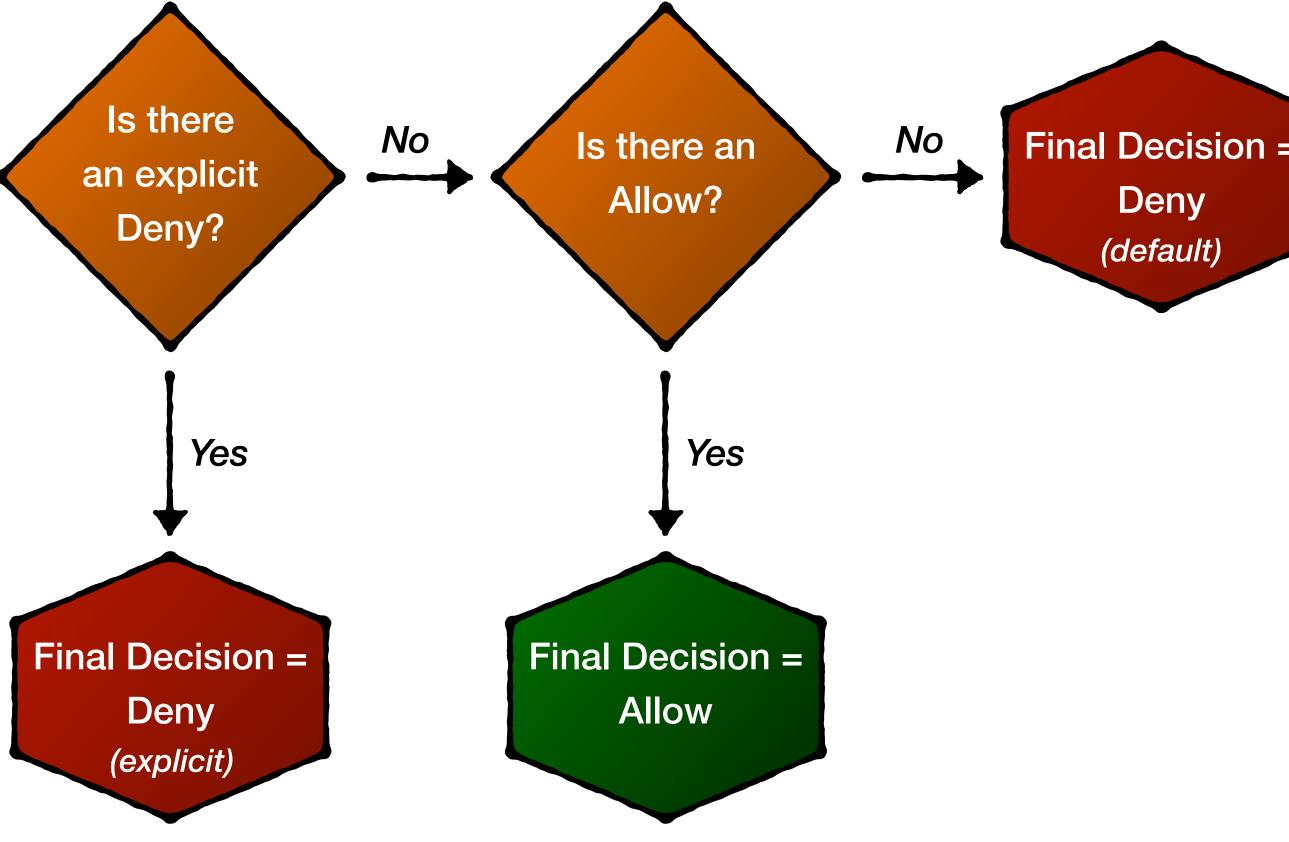






## IAM Policy Evaluation





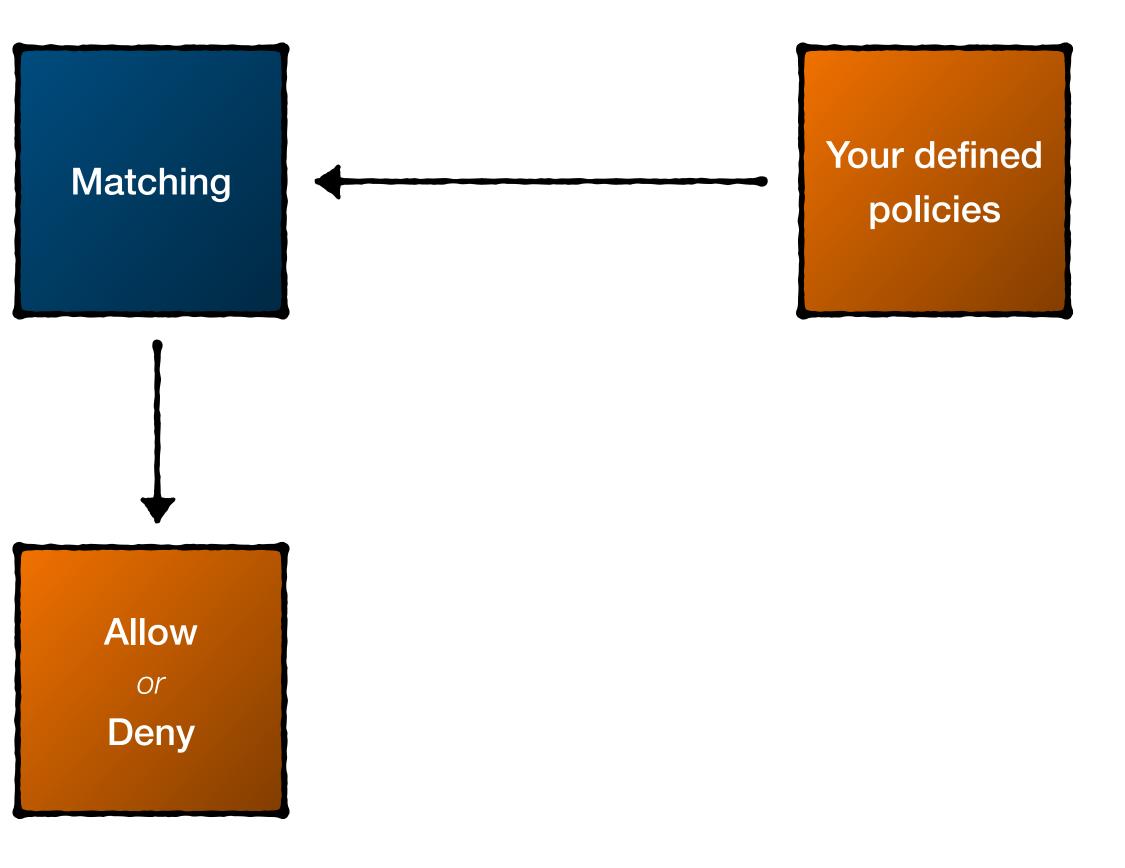






### What's not matching?

Context of your request





## Policy types

#### Identity-Based Policies

### Trust Policies

VPC Endpoint Policies

Resource Control Policies



### Service Control Policies

#### Resource-Based Policies

### Permission Boundaries

Session Policies



)

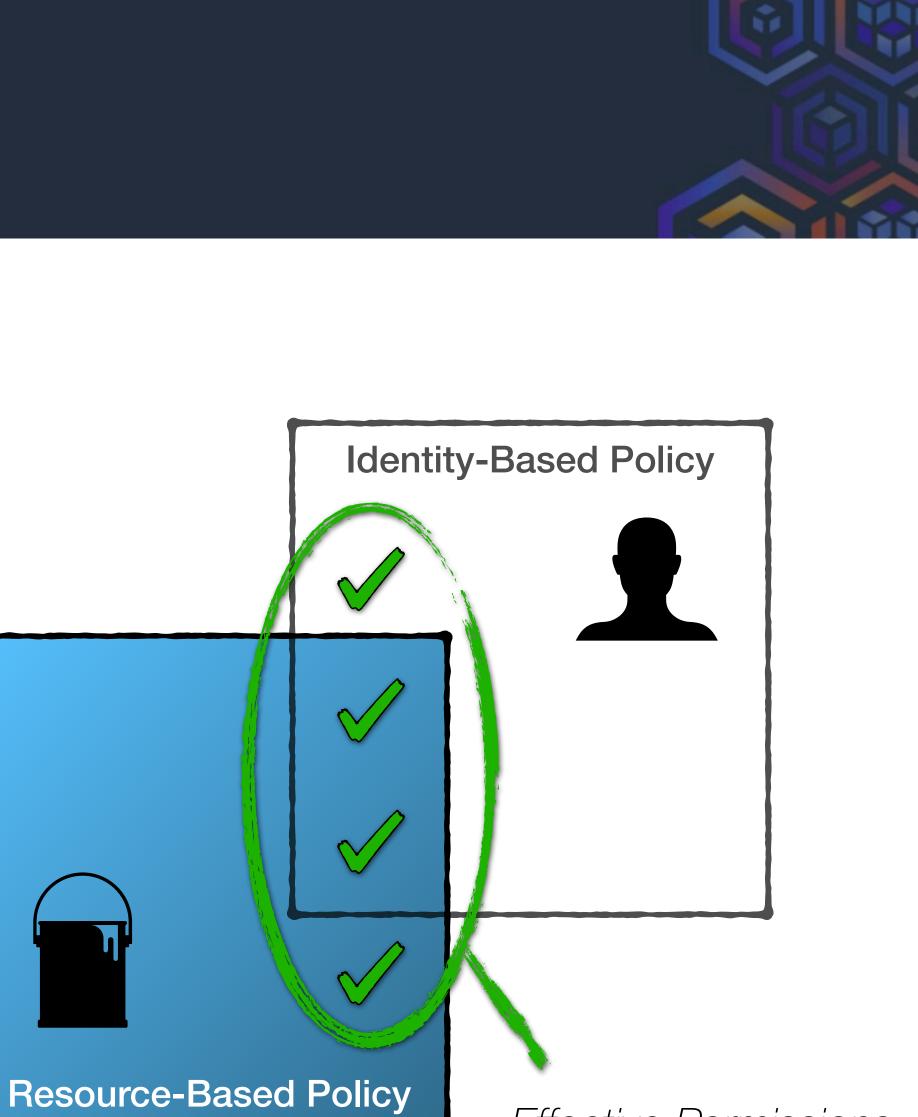
## Policy types

### **Identity-Based Policies**

Attach to a Principal e.g. User, Group, Role, Session

### **Resource-Based Policies**

Attach to a Resource e.g. S3 Bucket, VPC Endpoint



Effective Permissions = UNION

\*within an AWS Account



## Organization policy types

### Service Control Policies (SCP)

Getting more common

- Set at the Organization level
- Limit permissions granted to Identities

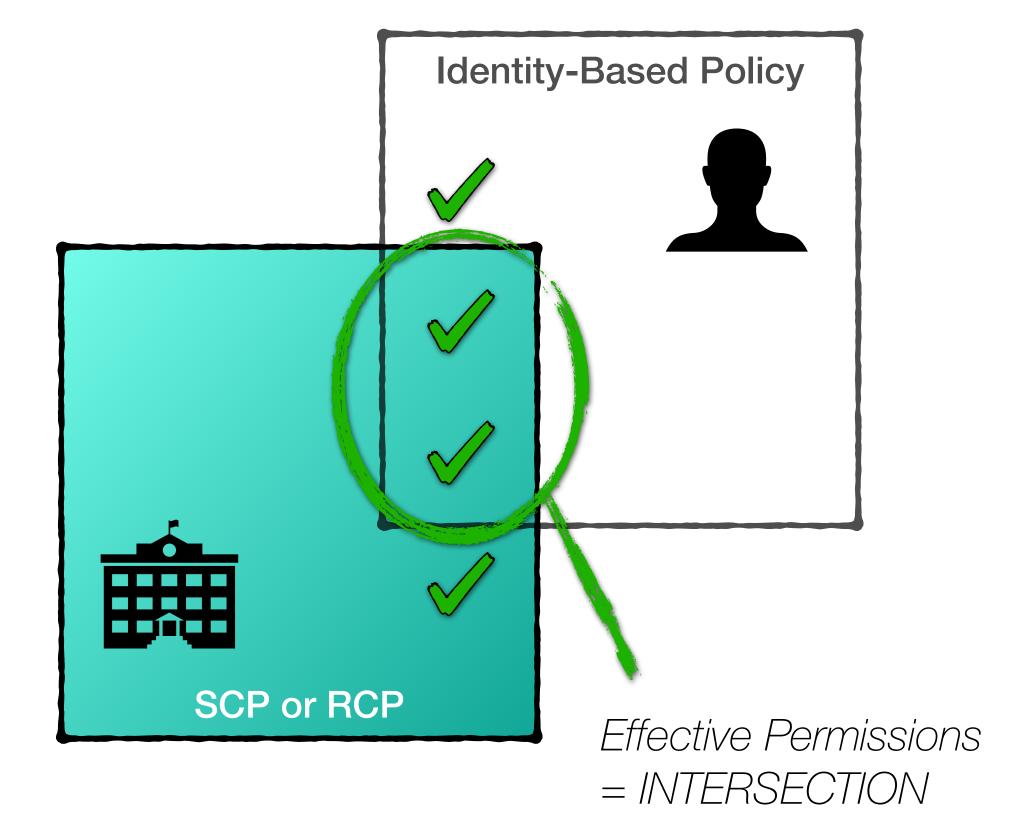
### **Resource Control Policies (RCPs)**

New - released Dec 2024

Set at the Organization level

Limit permissions granted on Resources







## Policy type matrix

Policy type	Act on	Set at	Used to	Example		
<b>Identity-based</b>	Principals	Account level	Grant permissions	Grant granular permissions for Users, Groups and Roles.		
<b>Resource-based</b>	Resources	Account level	Grant permissions	Grant cross-account access to a Resource. Control access from a Resource.		
Service Control (SCP)	Principals	Organization level	Deny permissions	Disable access to services by Users, Groups or Roles.		
Resource Control (RCP)	Resources	Organization level	Deny permissions	Disable access to Resources.		

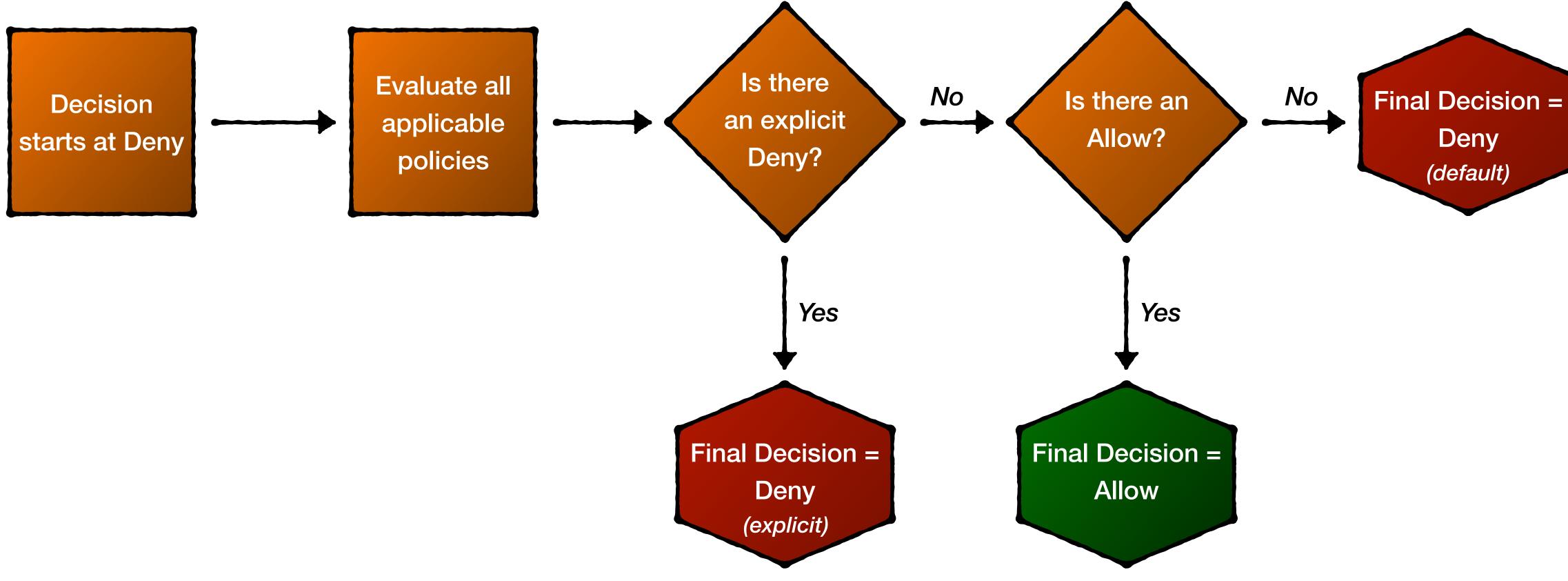


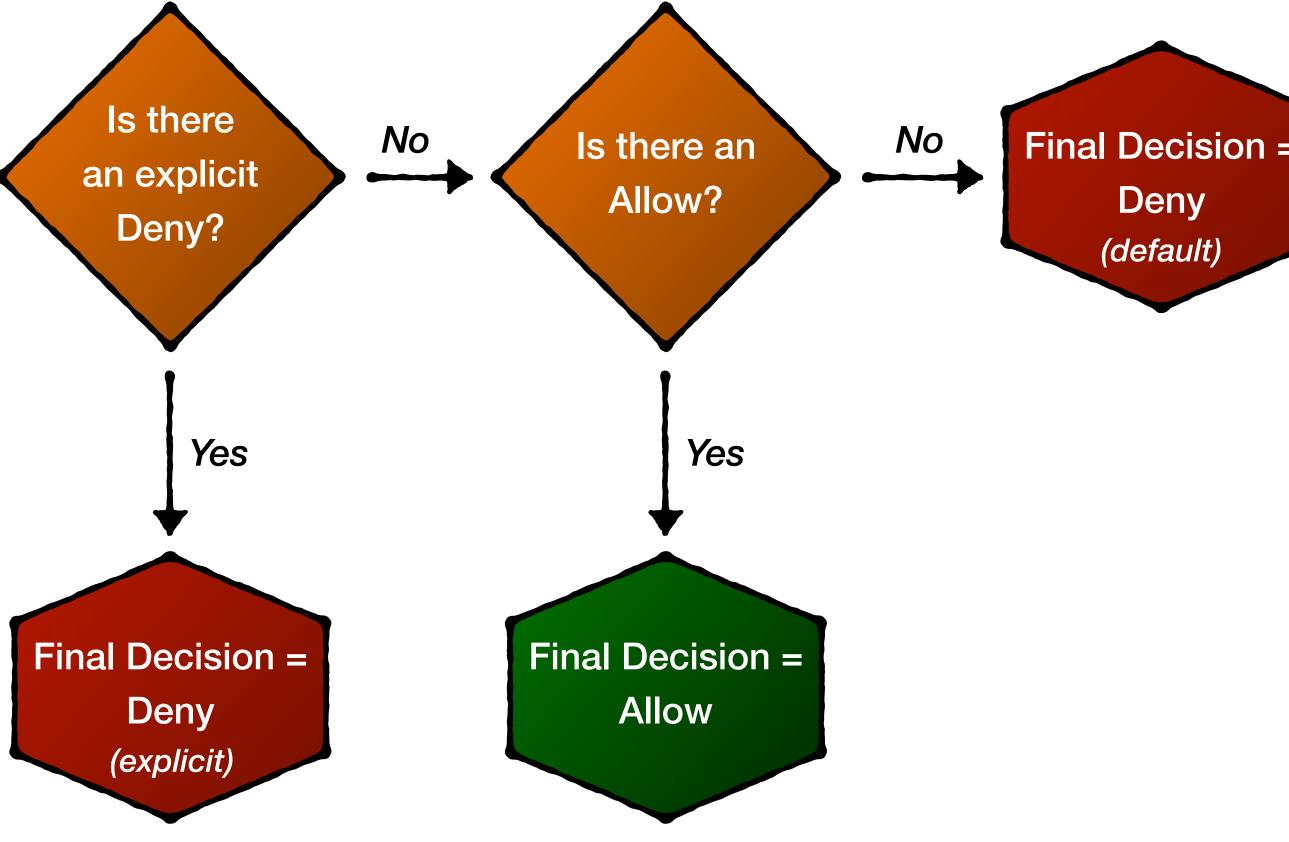
## SCP default policy

aws III Q Search	[Option	+S] D. 4 0 0	United States (Oregon)  AWSAdministratorAccess/pas256
🙆 EC2 🛛 🙆 Elastic Container Service 🛛 👼 Rout	æ 53 🔞 S3 🛛 CloudWatch 😽 Control Tower 🤱 AV	WS Organizations 🛛 👔 CloudFormation 🛛 🧟 IAM Identity 🤅	Center 🛛 🔞 Service Catalog
■ IAM > Permission Guardrails > p	p-FullAWSAccess		() <b>₽</b> (s)
IAM - Preview < New home of IAM Identity Center	FullAWSAccess Details		Manage in AWS Organizations
Organization   Home	Policy ID p-FullAWSAccess	Permission guardrail type Service control policy	Target OUs and AWS accounts 19
Directory     People     Groups	Description Allows access to every operation	Policy type AWS managed	ARN arn:aws:organizations::aws:policy/service_ control_policy/p-FullAWSAccess
<ul> <li>Multi-account access</li> <li>AWS accounts</li> <li>Permission guardrails</li> <li>Permission sets</li> </ul>	Policy content Target OUs and AWS	S accounts Service access report	Edit in AWS Organizations
Application access Applications	1 { 2 "Version": "2012-10-17",		
<ul> <li>Access findings</li> <li>Summary</li> <li>External access</li> <li>Unused access</li> </ul>	<pre>3 "Statement": [ 4 { 5 "Effect": "Allow", 6 "Action": "*", 7 "Resource": "*" 8 }</pre>		
Settings	9 ] 10 }		



## IAM Policy Evaluation











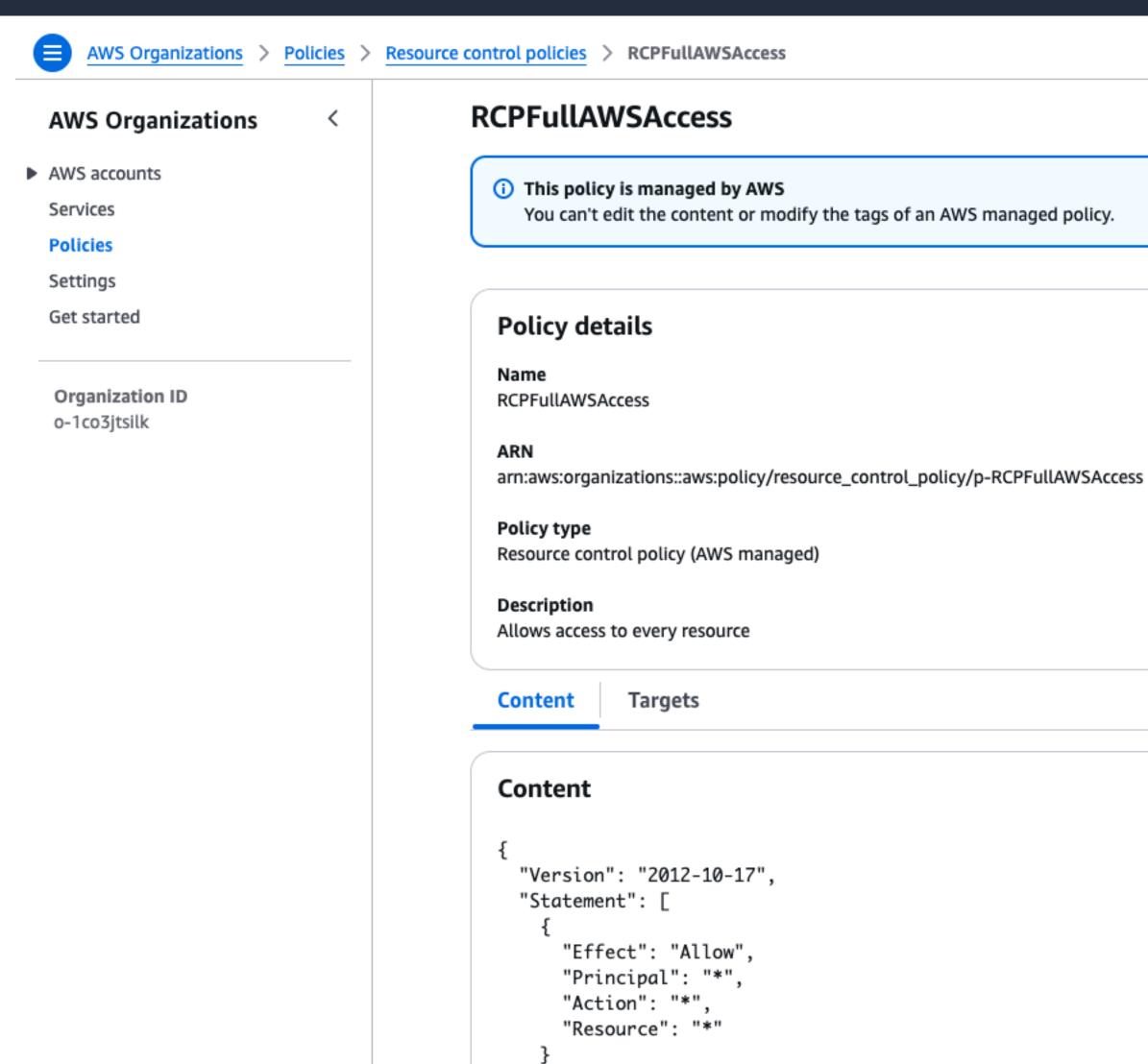
## Example SCP policy - Guardrail

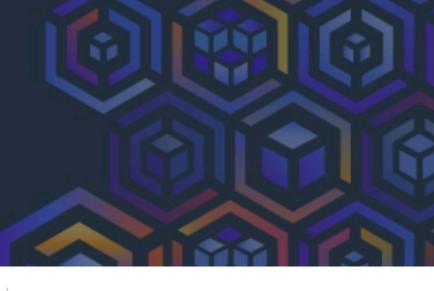
```
{
 "Statement": [{
   "Effect": "Deny",
   "Action": [
      "config:DeleteConfigRule",
      "config:DeleteConfigurationAggregator",
      "config:DeleteEvaluationResults",
      "config:PutConfigRule",
      "config:PutConfigurationAggregator"
    ],
   "Resource": "*",
   "Condition": {
  }]
```



"ArnNotLike": { "aws:PrincipalARN": "arn:aws:iam::\*:role/AWSControlTowerExecution" }

### RCP default policy





 $\odot$ 

You can't edit the content or modify the tags of an AWS managed policy.

## Organization Policies

<

#### **AWS Organizations**

AWS accounts

Services

Policies

Settings

Get started

Organization ID o-1co3jtsilk

#### Policies

Policies in AWS Organizations enable you to manage different features of the AWS accounts in your organization. Learn more [

#### Supported policy type

Policy type

AI services opt-out policies AI services opt-out policies allow yo organization. Learn more [

Backup policies Backup policies allow you to central accounts. Learn more [

Chat applications policies Amazon Q Developer in chat applica applications such as Microsoft Teams

Declarative policies for EC2

Declarative policies for EC2 allow you organization. Once attached, the con more 🖸

Resource control policies Resource control policies (RCPs) offe organization. Learn more [

Service control policies

Service control policies (SCPs) offer roles in an organization. Learn mor

Tag policies

Tag policies allow you to standardize more 🔼

25	
▲	Status
u to control data collection for AWS AI services for all the accounts in an	⊖ Disabled
ly manage and apply backup plans to the AWS resources across an organization's	⊖ Disabled
itions policies allow you to control access to an organization's accounts from chat s and Slack. Learn more	⊖ Disabled
ou to centrally declare and enforce desired configurations for EC2 at scale across an nfiguration is always maintained when EC2 adds new features or APIs. Learn	⊖ Disabled
er central control over the maximum available permissions for resources in an	⊘ Enabled
central control over the maximum available permissions for IAM users and IAM	⊘ Enabled
e the tags attached to the AWS resources in an organization's accounts. Learn	⊖ Disabled



## Some additional policy types

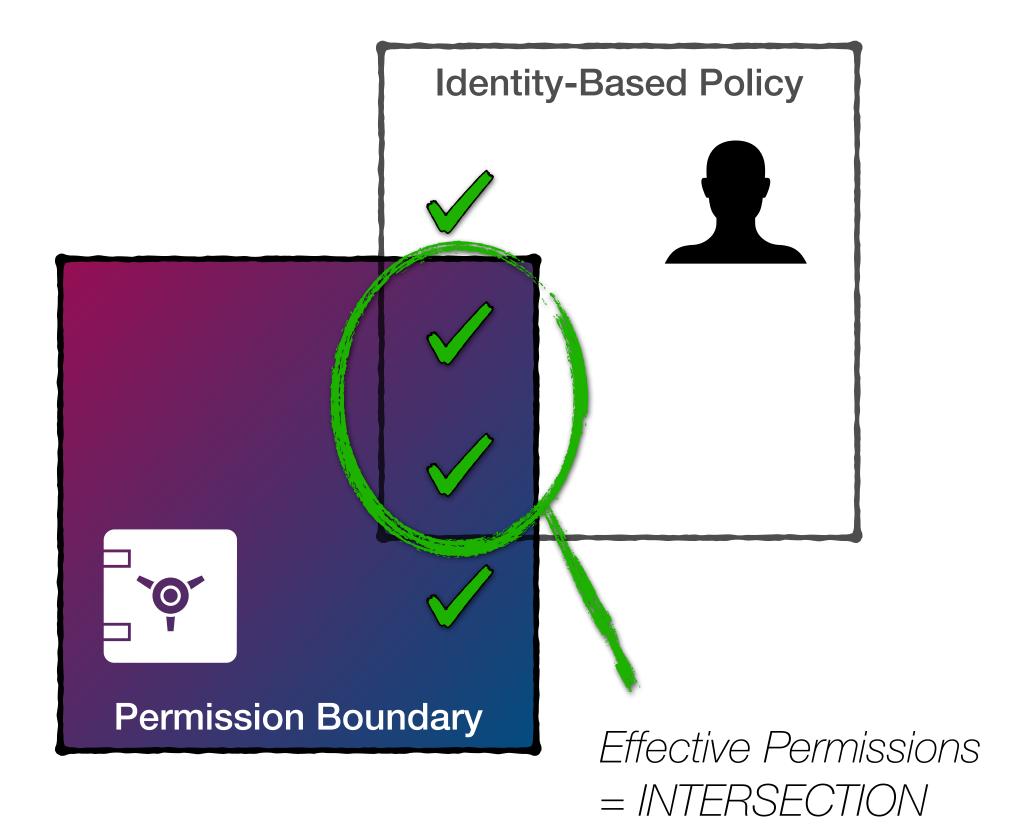
### **Permission Boundaries**

Powerful way to limit privilege escalation, but not widely adopted outside of larger enterprises

### **Scoped-down policies**

Assume a role (via STS) with a minimum set of permissions







## IAM Role Trust Policy

- Allows you to define which Principals you trust to assume a role.
- Not to be confused with what the role can do

Permissions

**Trust relationships** 

#### **Trusted entities**

Entities that can assume this IAM role under specified conditions.



Tags

Last Accessed

"Service": "cloudtrail.amazonaws.com"



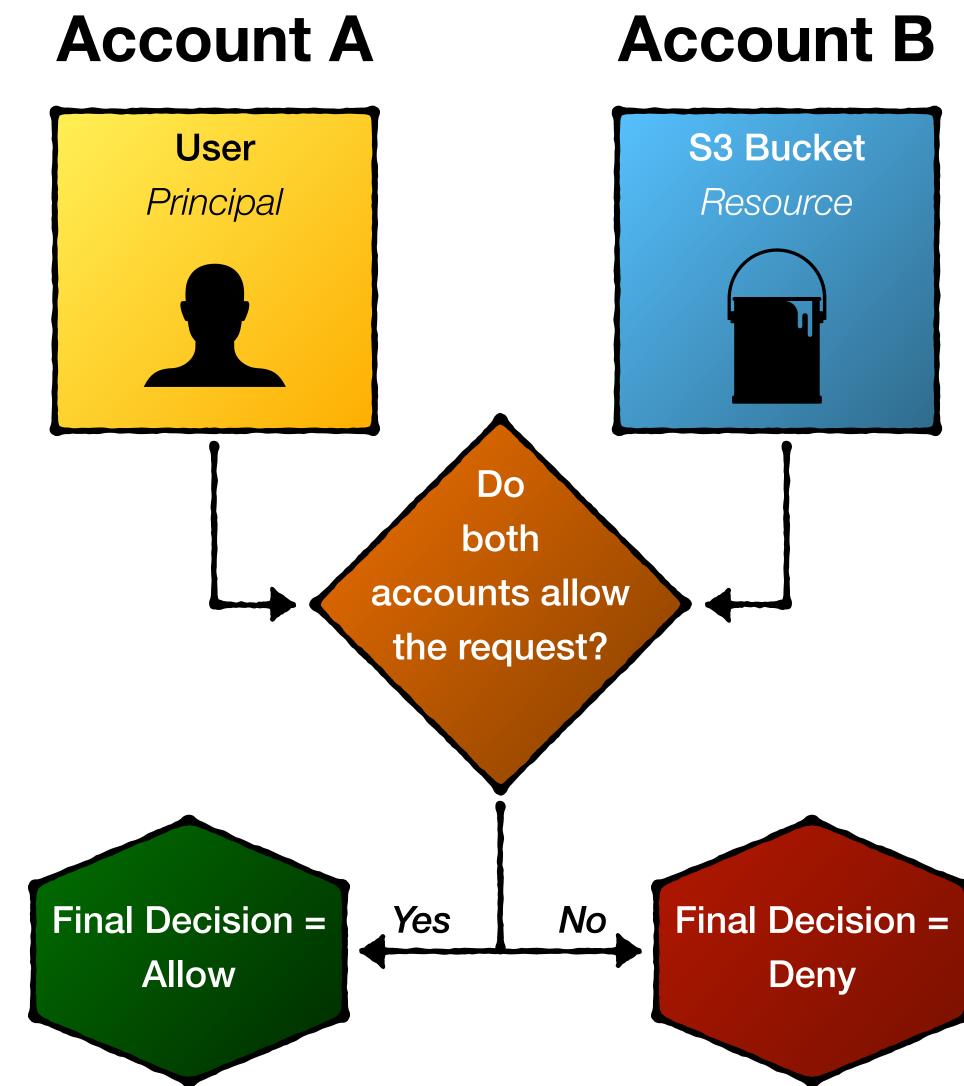
### Permission across accounts

### Within an AWS account

• Identity UNION Resource

### Across multiple AWS accounts

- Identity INTERSECT Resource
- Need explicit Allows on both sides
- Create a "trust hug"

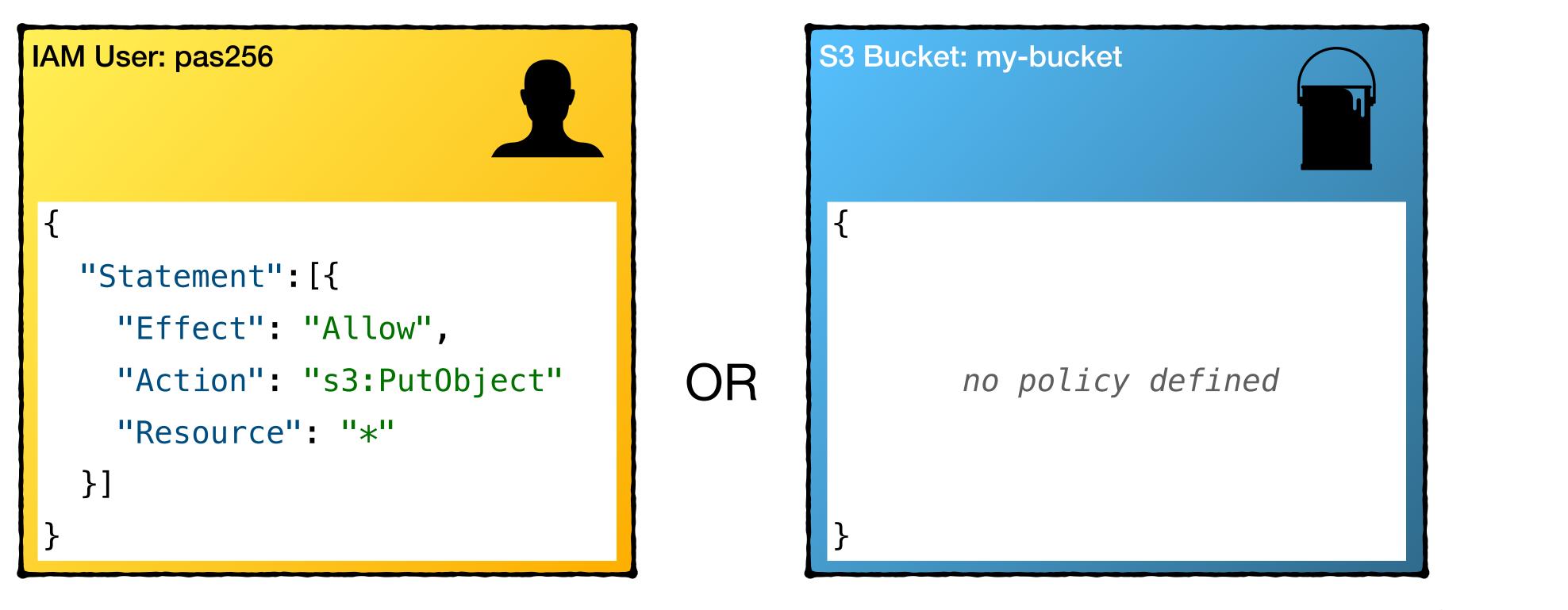








## How policies work together within an account



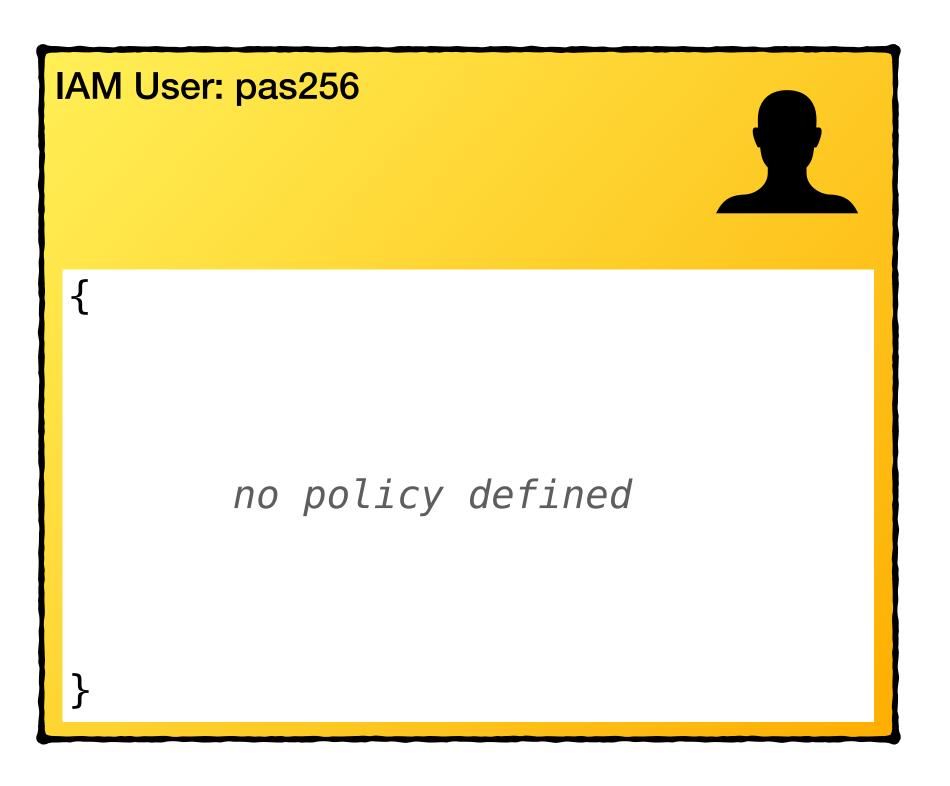
### aws s3 cp my-file.txt s3://my-bucket/

### Account A





## How policies work together within an account



### aws s3 cp my-file.txt s3://my-bucket/

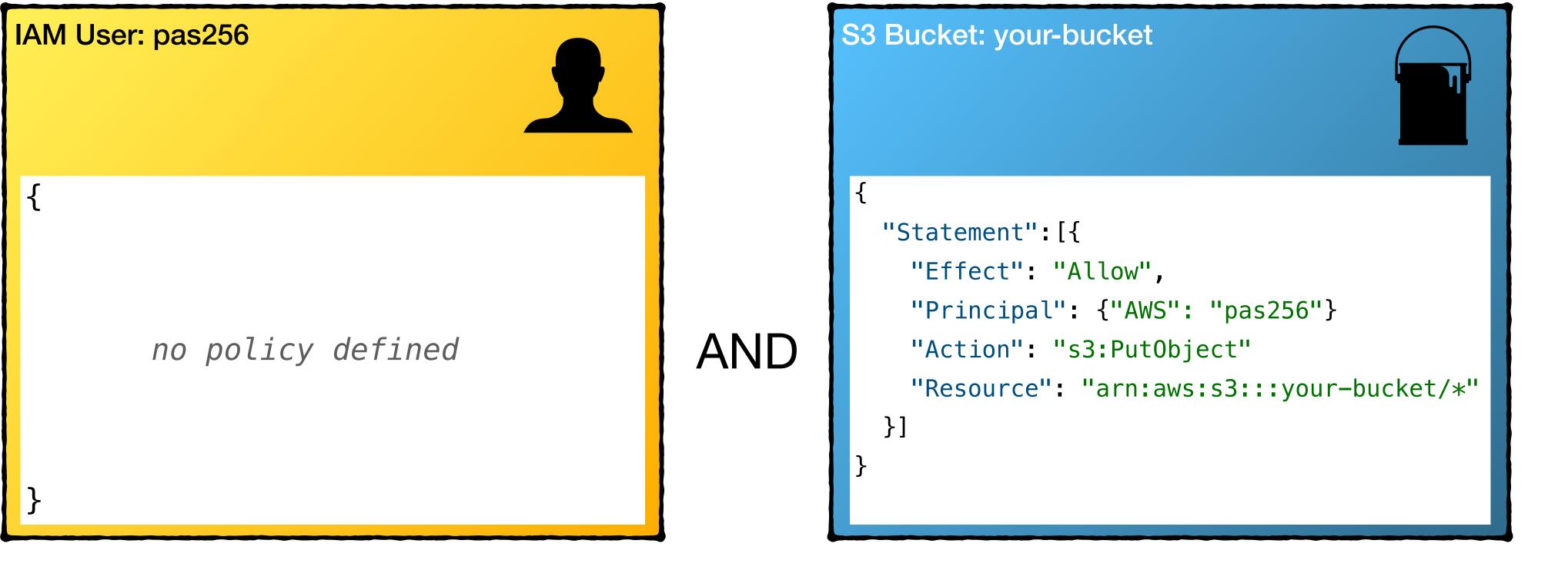
### Account A







### Account A

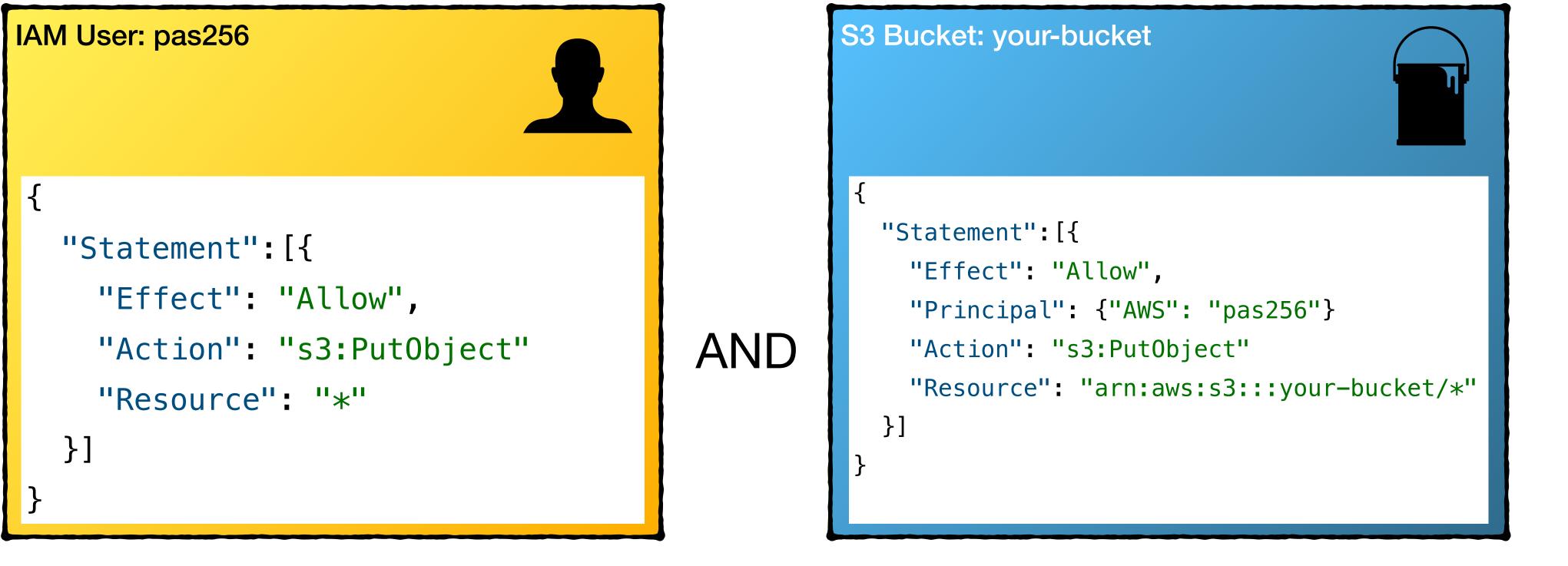


### aws s3 cp my-file.txt s3://your-bucket/





### Account A



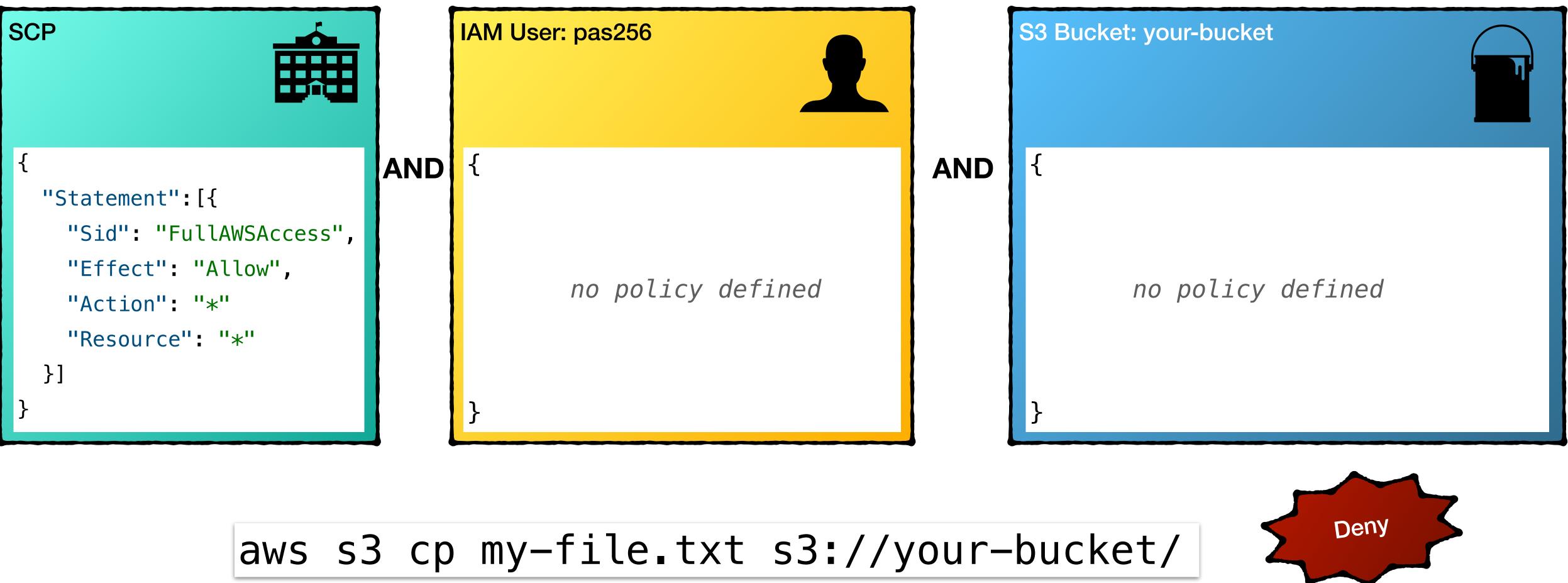
### aws s3 cp my-file.txt s3://your-bucket/

### Account **B**





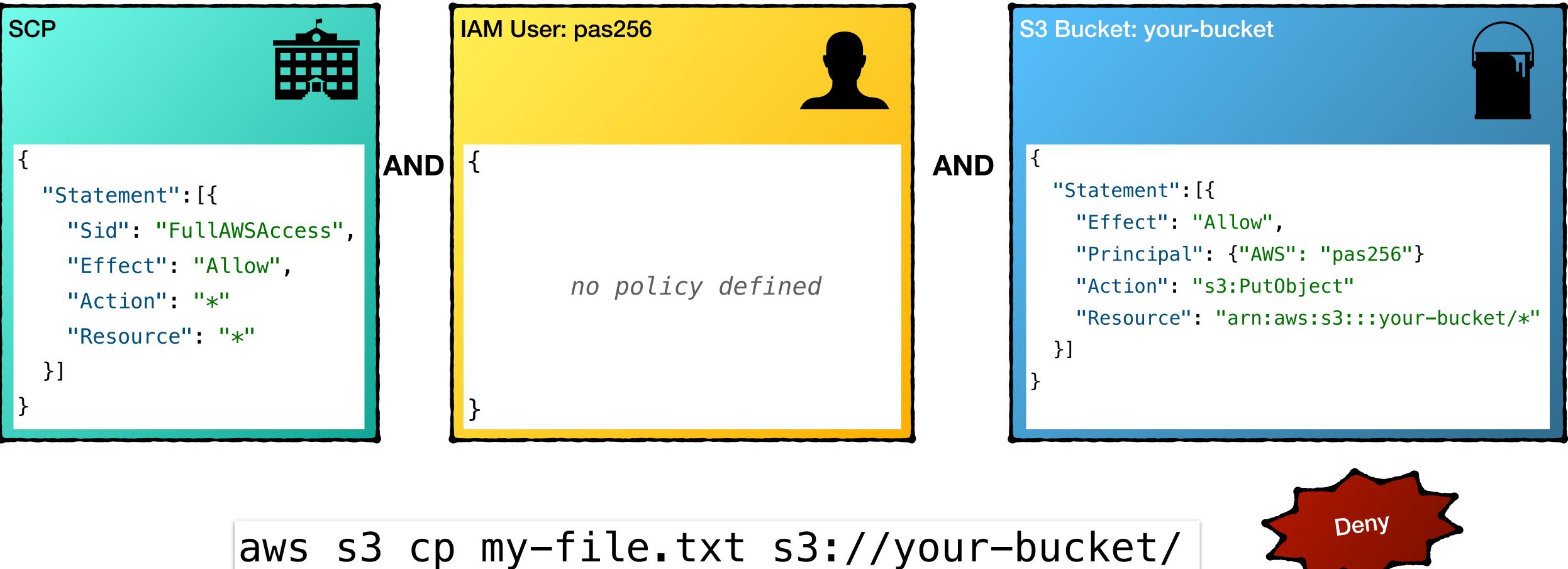
### Account A







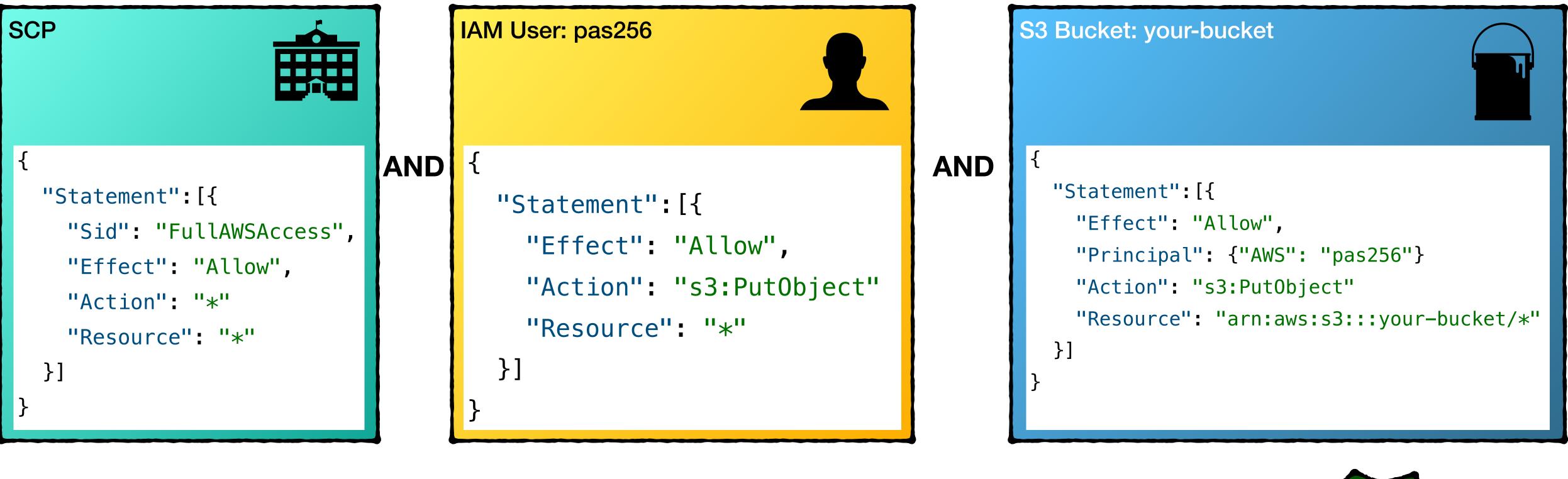
### Account A







### Account A



### aws s3 cp my-file.txt s3://your-bucket/







# Troubleshooting



## Verify Last Accessed

First, make sure the Principal you think you're using is indeed being used!

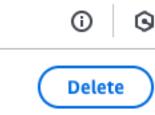
- Activity appears within 4 hours
- Tracks 400 days of history
- Tracks attempts, not just success
- Tracks Users and Roles

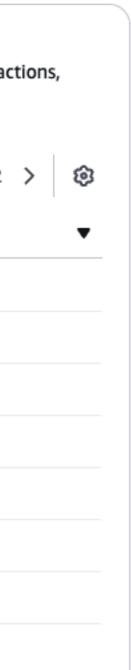
#### Documentation



IAM > Roles > AWSCont	rolTowerEx										
AWSControlTowerEx	kecutio	<b>N</b> Info									
Permissions Trust relati	onships	Tags	Last Acce	essed		Revo	ce se	ssion	S		
Allowed services (419) IAM reports activity for services ar choose the appropriate service name F	me from the			bout ac	tion l	ast ac	essec	l infor	matio	n. To	see act
Q Search	No Filter	vices access	<b>•</b>	<	1	2 3	4	5	6 7	,	42
Service	▽	Policies gr	anting permis	sions		L	ast ac	cesse	d		
AWS Config		Administra	atorAccess			3	days	ago			
AWS Lambda		Administra	atorAccess			6	days	ago			
AWS CloudFormation		Administra	atorAccess			3	15 day	ys ago	)		
Amazon SNS		Administra	atorAccess			3	15 day	ys ago	)		
Amazon EventBridge		Administra	atorAccess			3	15 day	ys ago	)		
Amazon CloudWatch Logs		Administra	atorAccess			3	15 day	ys ago	)		
AWS Key Management Service		Administra	atorAccess			3	15 day	ys ago	)		
AWS Identity and Access Manage	ement	Administra	atorAccess			3	15 day	ys ago	)		







## Inspect using CloudTrail

<b>CloudTrail</b> > Event hist	ory						
CloudTrail < Dashboard	Event history (50+) Info Event history shows you the last 90 days of management events. Lookup attributes						
Event history Insights	Read-only	<ul> <li>Q false</li> </ul>					
▼ Lake	Event name	Event time					
Dashboards Query	ConsoleLogin	March 18, 2025, 11:37:02 (UTC					
Event data stores	GetSigninToken	March 18, 2025, 11:37:02 (UTC					
Integrations	PutBucketPolicy	March 18, 2025, 11:30:56 (UTC					
Trails	PutBucketPolicy	March 18, 2025, 11:27:18 (UTC					
Settings	PutBucketPolicy	March 18, 2025, 11:27:06 (UTC					
	GetBucketMetadataT	March 18, 2025, 11:26:11 (UTC					
Pricing 🖸	PutBucketPolicy	March 18, 2025, 11:25:15 (UTC					
Documentation 🖸 Forums 🖸	PutBucketEncryption	March 18, 2025, 11:22:02 (UTC					
FAQs 🖸	CreateBucket	March 18, 2025, 11:22:02 (UTC					
	CreateBucket	March 18, 2025, 11:21:50 (UTC					

				• · · ·
		C Download	events  Creat	e Athena table
 User name	Event source	► Filter by date	and time < 1 Resource name	2 > 😥
			Resource name	
pas256	signin.amazonaws.com	-	-	
pas256	signin.amazonaws.com	-	-	
pas256	s3.amazonaws.com	AWS::S3::Bucket	my-bucket-00256	
pas256	s3.amazonaws.com	AWS::S3::Bucket	my-bucket-00256	
pas256	s3.amazonaws.com	AWS::S3::Bucket	my-bucket-00256	
pas256	s3.amazonaws.com	-	-	
pas256	s3.amazonaws.com	AWS::S3::Bucket	my-bucket-00256	
pas256	s3.amazonaws.com	AWS::S3::Bucket	my-bucket-00256	
pas256	s3.amazonaws.com	AWS::S3::Bucket	my-bucket-00256	
pas256	s3.amazonaws.com	AWS::S3::Bucket	my-bucket-1256	







## Inspect using CloudTrail

#### PutBucketPolicy Info

#### Details Info

Event time March 18, 2025, 11:30:56 (UTC-07:00)

User name pas256

Event name PutBucketPolicy

Event source s3.amazonaws.com AWS access key ASIA2UC3D7TR55K2

Source IP address 76.247.189.86

Event ID d4333450-dd1c-4a1

Request ID 92P16KM607SKHFJI

#### Resources referenced (1) Info Resource type Resource name my-bucket-00256 AWS::S3::Bucket

#### Event record Info

#### JSON view

1	{
2	"eventVersion": "1.11",
3	"userIdentity": {
4	"type": "AssumedRole",
5	"principalId": "AROA2UC3D7TR23CMOBIDD:pas256",
6	"arn": "arn:aws:sts::730335542499:assumed-role/AWSReser
7	"accountId": "730335542499",



	AWS region
ZPS6	us-west-2 Error code
	MalformedPolicy
2-894d-91c10754267c	Read-only false
0	
	AWS Config resource timeline
2	View AWS Config resource timeline [2]
	Г сору



## Inspect using CloudTrail

- View last 90 days in AWS Web Console
- Must be enabled
  - Create one, and **ONLY ONE**, trail (*otherwise* \$\$\$?!!)
- Not 100% coverage by default
  - e.g. No s3:Put0bject coverage
  - Can enable logging data events to get s3:Put0bject
    - Careful. This can cost \$\$\$ with high volume projects





### Decode the error

#### Instance launch failed

You are not authorized to perform this operation. User: arn:aws:sts::555697216722:assumedrole/AWSReservedSSO\_AWSReadOnlyAccess\_4cea7894fbac3ead/pas256 is not authorized to perform: ec2:CreateSecurityGroup on resource: arn:aws:ec2:us-west-2:555697216722:vpc/vpc-090f484047007b243 because no identity-based policy allows the ec2:CreateSecurityGroup action. Encoded authorization failure message: rGACTc1aEyGSszyQ7nBdiZaFuz-KFI9uBWHN11bShYGcCD\_kgZj2tQfpMqS39Z8ZNchr\_0PtDO7orj\_tnaZ7r\_Z0o5NDc90kQBebHS0S6CnoQQ1vuc0KBpQDaDUScORFrYMWVoS4udJsd Xj74z\_bHEqvq2cA3v3BuYsYySjOBfTXrhkXWhxy5MvpJuV0KGffOxDyC5Ge-6a87zy\_7LXHcKBy-UK3XNyiNxGowVQS62c\_DRa42Od4ri90h7Q8QfNBzT70YgDy1WNVrapk4QWhM2ZsYpwADXYKXK7P2OWgUoCJcmKj\_6y1RQM8H2-oVPpd-BqJ0qHMhY7wTIsdhlcy3xabFLIzCHUXax3GnZyv8v9npTPWeB7bNXIz5ji53w2H7ti9siApZ4KgOkwRz1zUtpF-4WZXM-uWoWreCKyRyzrIBwfNq3ZW11EHKgeYKBBWJEVuWl3tzlsjpJoKLdur4s7qNNcPE45MERl6WmyR-AqK2ZVMtqJSx1BNL2sw4b6IN6R2DP-uHiaOjhHZJL-OLMbqJblrgWAKId0nXg3HFt85gk\_Q6YYUbyIsYp9tP74J\_mgqqIwpDlwODaf\_fnE0pRS\_E3DkGkvQgBkAyX1vkn3DhRhMEz4Qr04XXr4RA1-2KStWWKZCPE\_ycD25U\_vUNuFrD-iBck0nCrwJiYO8vdSX7AeosDeGTwP1ofl0optnZ0SoYJisT8zl3i0JjXJCRLj5cvICg8tla5CszYOVGA\_Ld54krOf-SzvOm8G60VZKK5p81QWVlAUTNcWgLEDLbUsxTPOsbSESg52kZ8qvSEEbCPca\_FrXAP5Pnl429npxFqX\_L6SCKsVExURV8ccH5V7oxxwLAYRu8SMTbKdNIErBNvwL1Wi8wAOKwaizUhyvio-7PiGDcV

# aws sts decode-authorization-message jq -r '.DecodedMessage'

#### 🕒 Diagnose with Amazon Q

--encoded-message 'rGACT...GDcV'



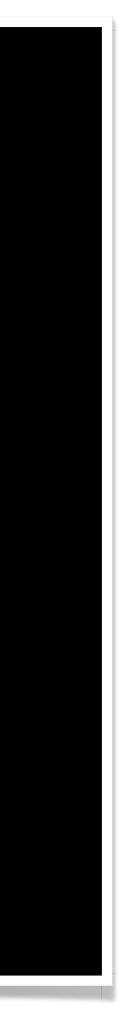


### Decode the error

```
"allowed": false,
"explicitDeny": false,
"matchedStatements": {
 "items": []
},
"failures": {
 "items": []
},
"context": {
 "principal": {
   "id": "AROA2UC3D7TR6HATBG7I0:pas256",
   "arn": "arn:aws:sts::730335542499:assumed-role/SSO/pas256"
  },
  "action": "CreateSecurityGroup",
 "resource": "arn:aws:ec2:us-west-2:730335542499:vpc/vpc-079df256ef81d3c40",
 "conditions": {
   "items":
        "key": "ec2:ResourceTag/ManagedBy",
        "values": {
         "items":
             "value": "Terraform"
```









## IAM Policy Simulator

IAM Policy Simulator			Mode :	Existing Policies -	assumed-role/SSO/pas	s256 <del>-</del>	2	
Policies Back Create New Policy	Policy Simulator							
Selected user: pas256	Amazon EC2 👻	1 Action(s) sele	Select All	Deselect All	Reset Contexts	Clear Results	Run Simulation	
AWS Organizations SCPs	Global Settings	9						
Service control policies (SCPs) applied to your account can impact your access to AWS	Action Settings and	Action Settings and Results [1 actions selected. 0 actions not simulated. 0 actions allowed. 1 actions denied. ]						
services. Learn more.	Service	Action	1	Resource Type	Simulation Resource	Permission		
	<ul> <li>Amazon EC2</li> </ul>	CreateKeyPair	1	key-pair	*	denied Implic	citly denied (no match	
IAM Policies       Filter								
S3-Write								
Custom IAM Policies								
There are no policies to display!								
Permissions Boundary Policy								
You can simulate a maximum of one permissions boundary policy per user or role.		httne <sup>.</sup> /	/nolic	nveim	<u>aws.ama</u>		nm/	
There are no policies to display!		πιρολ		<u>y y y y y y y y y y y y y y y y y y y </u>	<u>uvvJ.uma</u>		<u>////</u>	







## AWS IAM Policy Visualizer

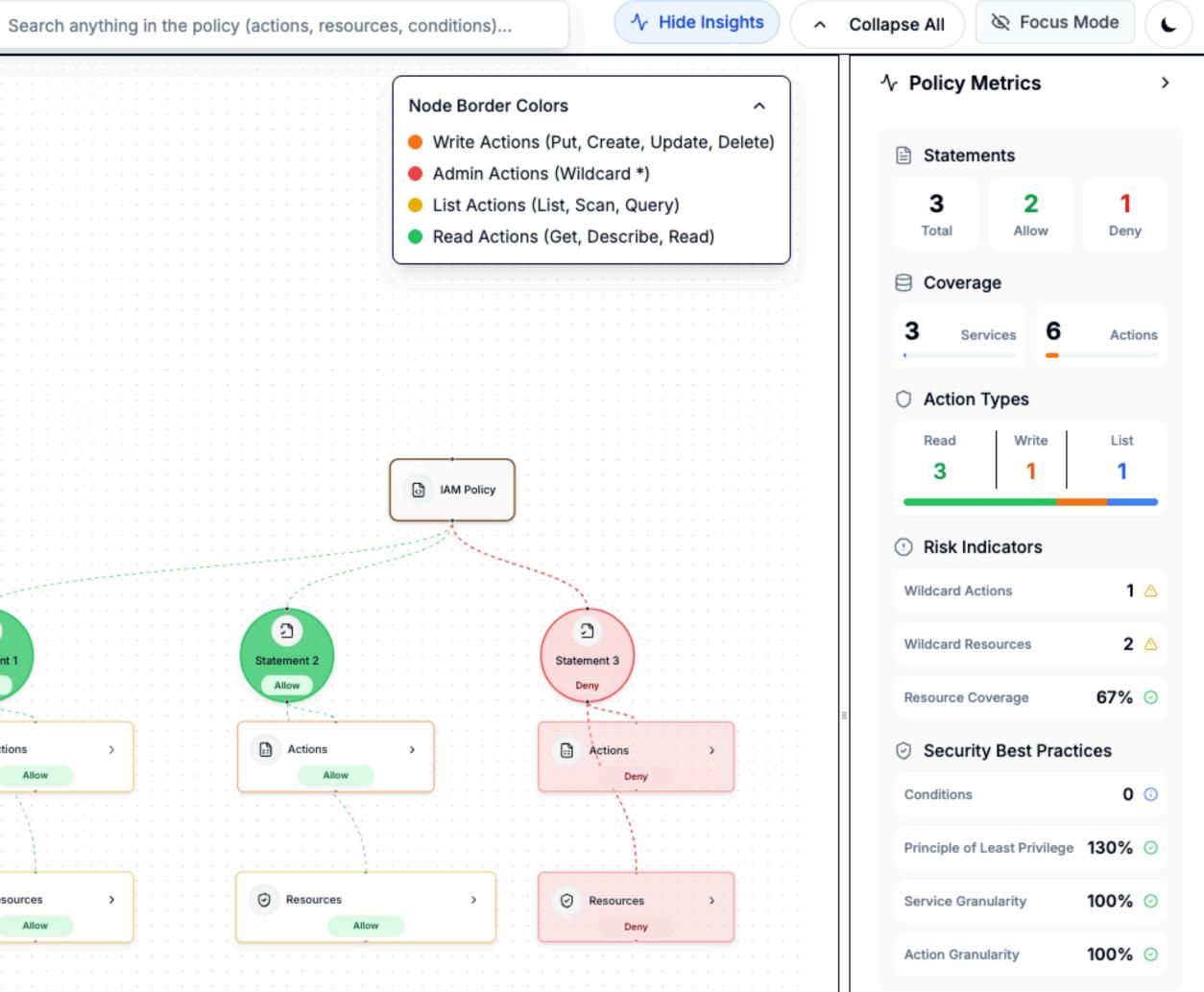
#### AWS IAM Policy Visualizer

Visualize your AWS IAM policies to better understand permissions and access patterns.

	olicy Input <	
1		
2	"Version": "2012-10-17",	
3	"Statement": [	
4	{	
5	"Effect": "Allow",	
6	"Action": [	
7	"s3:GetObject",	
8	"s3:ListBucket"	
9	1,	
10	"Resource": [	
11	"arn:aws:s3:::example-bucke	
	t",	
12	"arn:aws:s3:::example-bucke	
	t/*"	
13	]	
14	},	
15	{	
16	"Effect": "Allow",	
17	"Action": [	· · · · · · · · · · · · · · · · · · ·
18	"dynamodb:GetItem",	
19	"dynamodb:Query",	
20	"dynamodb:PutItem"	Statement 1
21	1.	Allow
22	"Resource":	
	"arn:aws:dynamodb:us-east-1:1	
	23456789012:table/Users"	Actions
23	}.	Allow
24	{	
25	"Effect": "Deny",	
26	"Action": "ec2:*",	
27	"Resource": "*"	
28		Resources
29	1	Allow
	1	







### https://iam-liart.vercel.app/

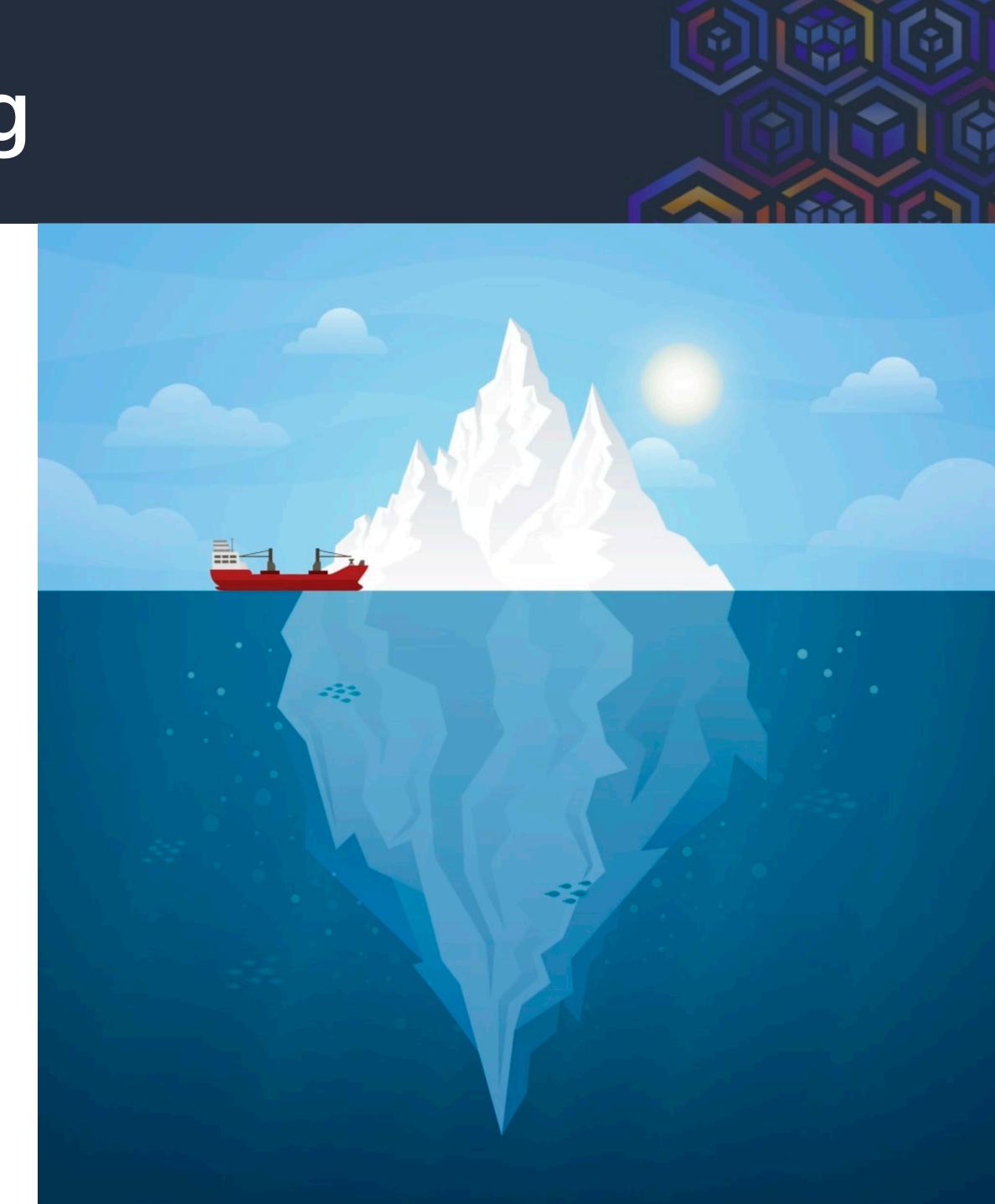


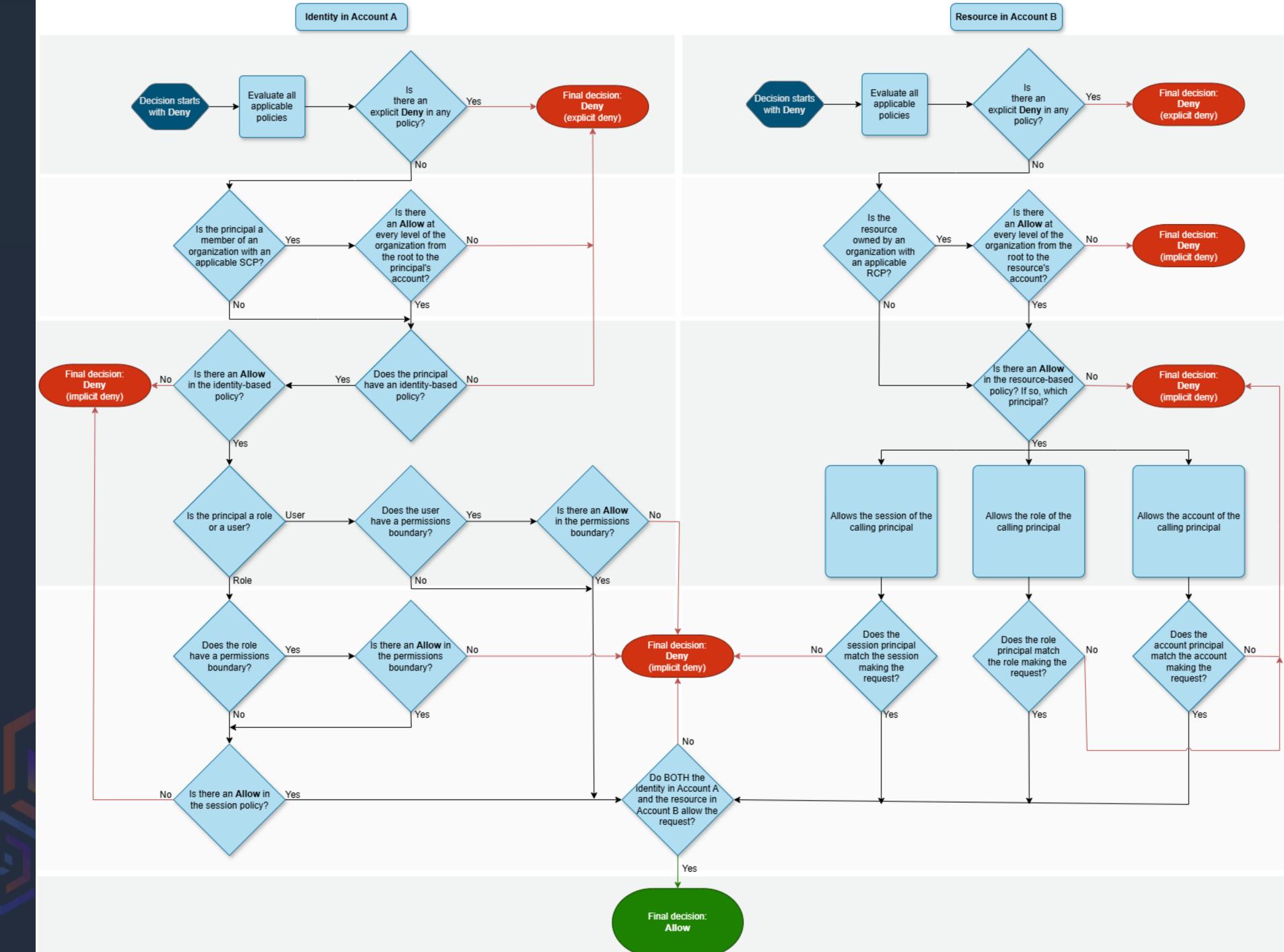
## This is the tip of the iceberg

- Experiment
  - Get hands-on
- The IAM docs are actually really good
- Watch Brigid's talk
  - https://www.youtube.com/watch?  $\bullet$ v=YQsK4MtsELU















# Thank you







