AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

SEC324

A least privilege journey: AWS IAM policies and Access Analyzer

Brigid Johnson (she/her)
GM of Access Analyzer, AWS Identity
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

AWS Identity overview

Permissions in AWS – The tools and how they work Pro tip

Permissions lifecycle to get to the right permissions

- Setting permissions Demo! Pro tip
- Verifying permissions Demo! Pro tip
- Refining permissions Demo! Pro tip

Permissions challenges

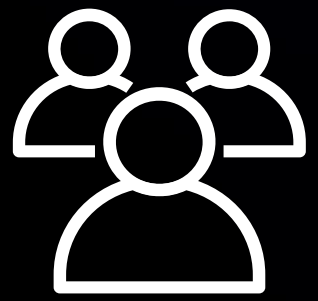
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Identity overview

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Who can access what

Who



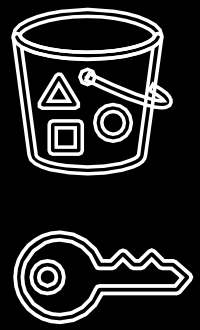
Developers and applications

Can access



Permissions

What



Resources

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What you need to know about AWS Identity

Govern your AWS environment	**with**	AWS accounts and AWS Organizations
Centralize identity management	**with**	AWS SSO
Rely on short-term credentials	**with**	federation and application roles
Organize your resources	**with**	tags and resource groups
Establish a data perimeter	**with**	policies and conditions
Journey to least privilege	**with**	AWS Identity and Access Management (IAM) policies and IAM Access Analyzer

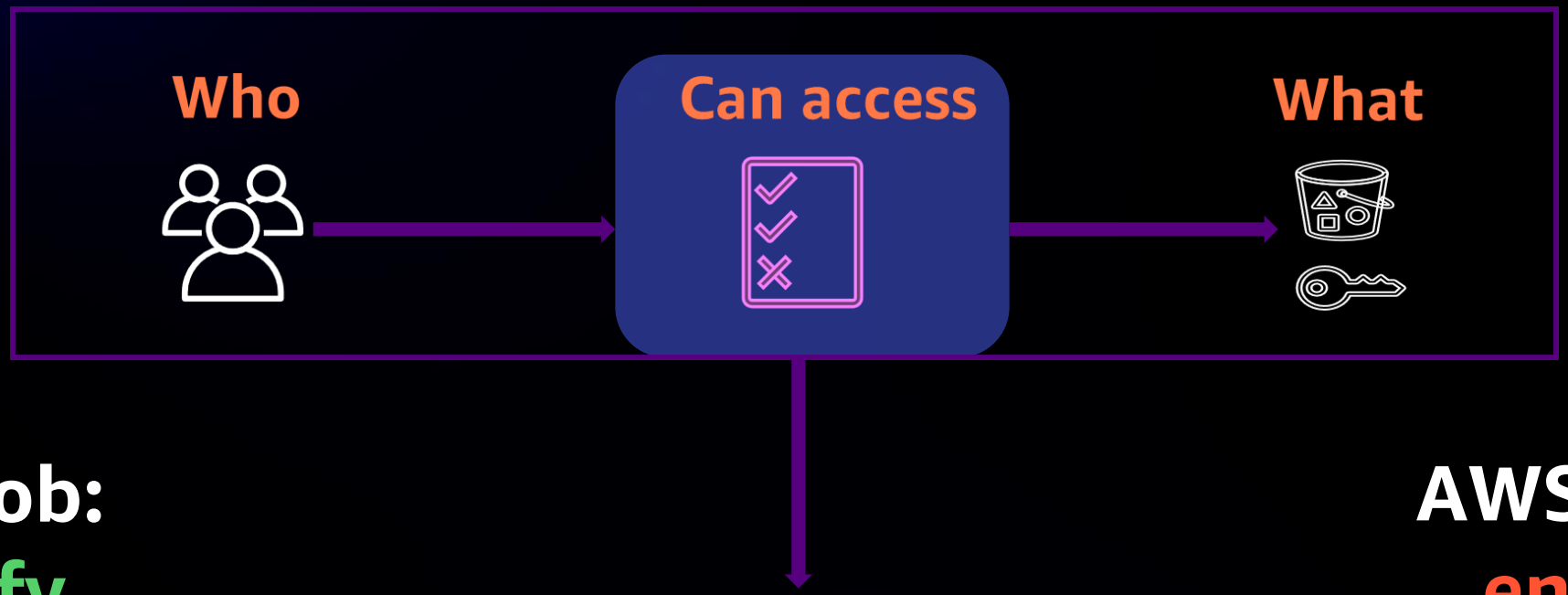
aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

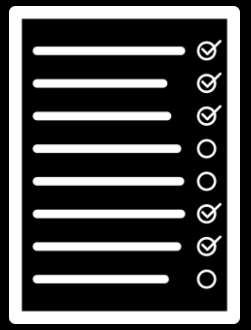
Permissions in AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Focus on access in AWS



Your job:
specify



Access control

AWS's job:
enforce



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Specify: The goal

Adhere to the principle of least privilege (POLP)

Grant users and systems the narrowest set of privileges to complete required tasks

Goals



Business to innovate

Agility to move fast

Freedom for builders



Dangerous action prevention

Accountable security posture

Cost-effective solutions

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Specify: IAM policy language



```
{
 "Statement":[{
"Effect":"effect",
"Principal":"principal",
"Action":"action",
"Resource":"arn",
"Condition":
{  "condition":{
        "key":"value" }
}
  }
 ]
}
```

Principal – the entity that is allowed or denied access

`"principal":"AWS":"arn:aws:iam::123456789012:user/username"`

Action – type of access that is allowed or denied access

`"action":"secretsmanager:getSecret"`

Resource – the Amazon resources the action will act on

`"Resource":"arn:aws:secretsmanager:us-east-2:111122223333:secret:pickles"`

Pro tip: do not use variables such as ${Account} in the ARN

Condition – the condition under which the access defined is valid

`"StringEquals": {"aws:CalledViaFirst": "lambda.amazonaws.com "}`

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Specify: Tools to grant access



IAM principal policies

Attach policies to IAM identities (users, groups, or roles)

- Managed policies are standalone and attached to multiple principals
- Inline policies are attached directly to a single principal

Resource policies



IAM roles (trust policies)



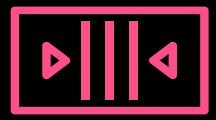
Amazon Simple Storage Service (Amazon S3) buckets



AWS Lambda functions



AWS Key Management Service (AWS KMS) keys



Amazon Simple Queue Service (Amazon SQS) queues

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Specify: Tools to restrict access



AWS Organizations service control policies (SCPs)

Permissions guardrails to restrict access for principals across accounts in your organization

IAM permissions boundaries

Developers can manage permissions and control the maximum permissions they grant

Amazon VPC endpoint policies

Require that traffic stays within your VPC

Block public access

Block existing public access and ensure that public access is not granted to newly created items



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pro tip: Use the right permissions tool





Service control policies (SCPs)



Permissions boundaries



IAM permissions policy



Scoped-down policies



Resource-based policies



Endpoint policies

Restrict powerful actions except for admins

Grant only the actions your role uses

Developers can manage roles safely

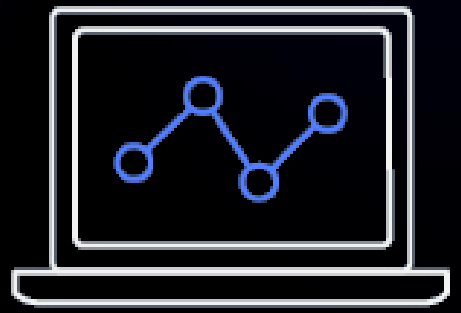
Grant direct, cross-account access

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enforce: Context and policies to evaluate

Context of AWS request



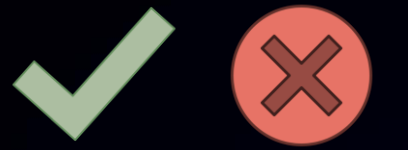
IAM



Policies evaluated



```
action : terminateInstance
resource:
    arn:aws:ec2:us-east-1:111122223333:
    instance/i-054dsfg34gdsfg38
ResourceTag/project : pickles
PrincipalTag/project : pickles
CalledViaFirst :
  cloudformation.amazonaws.com
```



Allowed Denied

```
Allow
action : ec2:terminateInstance
resource: *
ResourceTag/project : pickles
```

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enforce: How AWS evaluates policies

All access requests start with DENY

If using SCPs → SCP must allow

If using permissions boundaries → Permissions boundary must allow

---

If same account access → Identity **or** resource policy must allow

AWS KMS keys and IAM roles require resource policy

If direct, cross-account access → Both the identity **and** resource policy must allow

If using a session policy → Session and identity policy must allow

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Specify: Granting AWS services access



Pro tips

Service-linked roles (SLR)	Roles linked directly to an AWS service; permissions predefined to only those required by the service to call other AWS services on your behalf	●	IAM Access Analyzer Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling	●	Grant access to create SLRs for services you use
Service roles	A role an AWS service assumes to perform actions on your behalf; you manage permissions	●	Amazon EC2 Lambda	●	Specify the service in the trust policy
Requester permissions	AWS services use temporary credentials generated from the requester to perform actions on your behalf	●	AWS CloudFormation Encryption with AWS KMS	●	Principal needs access for all permissions AWS will use

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

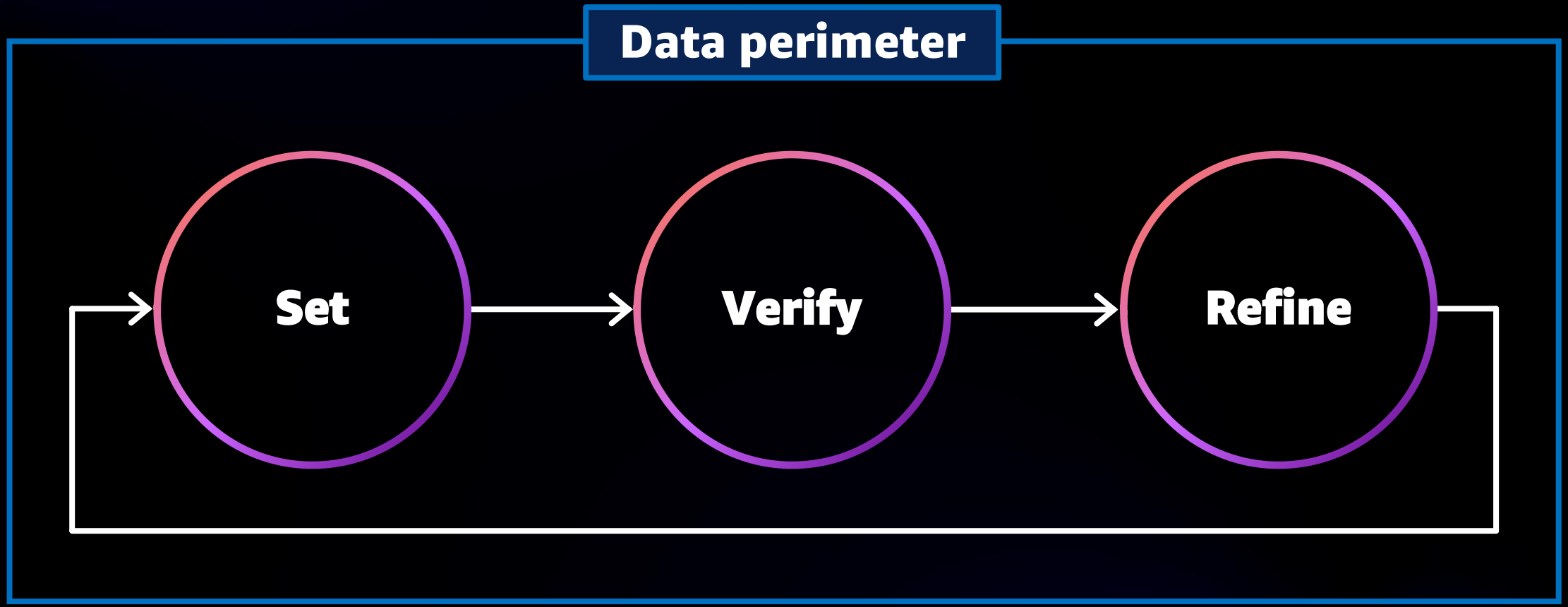
Permissions lifecycle

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



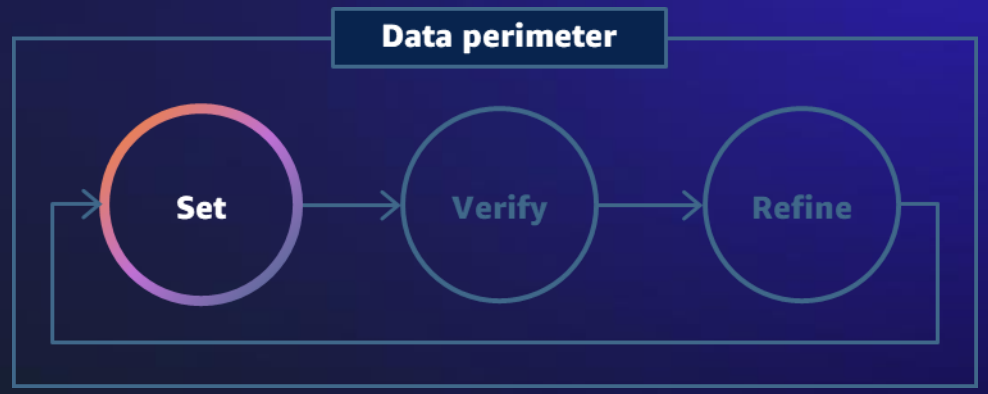
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Getting to the right permissions



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Setting permissions



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Set: Tools to define policies

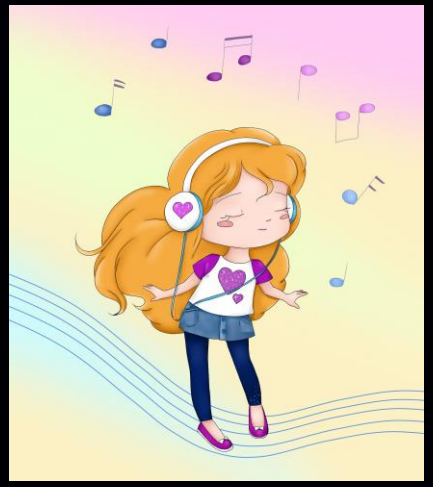


Exploring AWS



Start broader with AWS managed policies or custom templates

Right sizing



Generate and customize using policy generation with IAM Access Analyzer

Specific conditions



Author custom policies and validate by using policy validation with IAM Access Analyzer

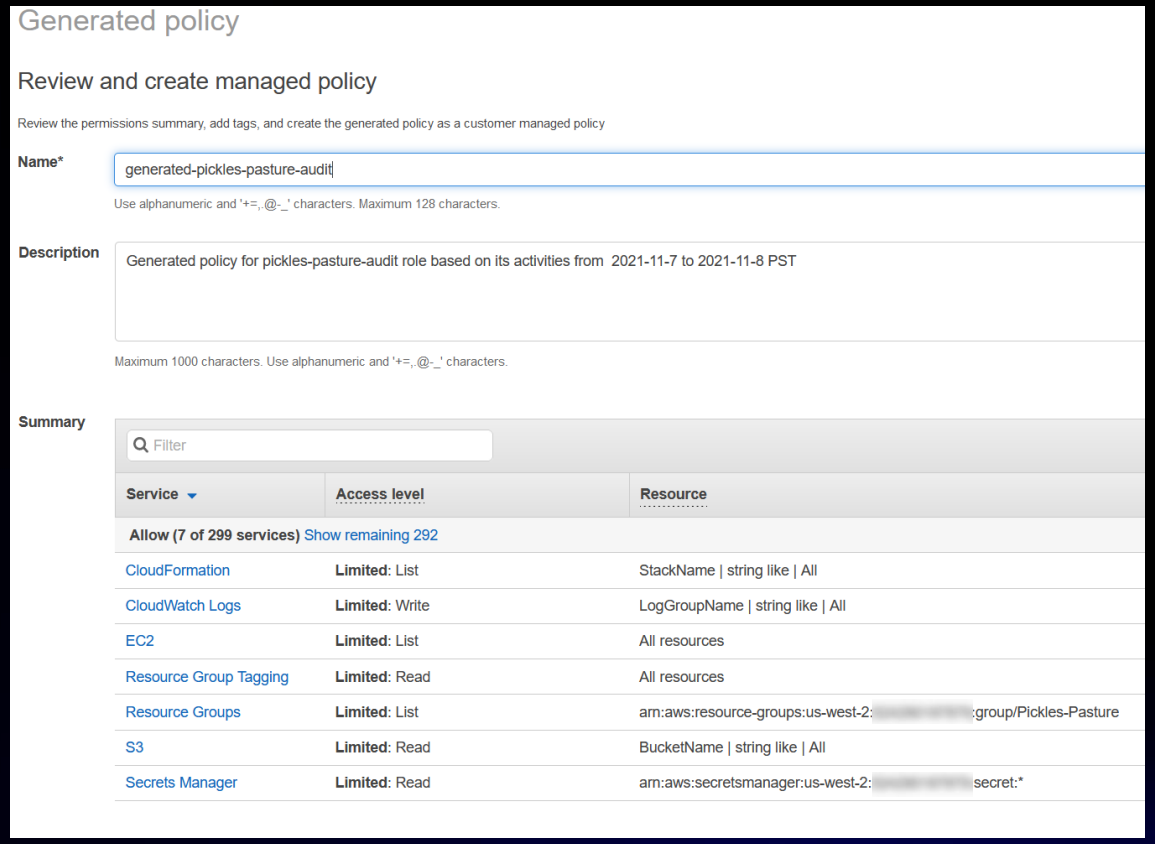
aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Set: Policy generation with IAM Access Analyzer

HELPS YOU GET TO THE RIGHT PERMISSIONS MORE QUICKLY BY ANALYZING YOUR ACCESS ACTIVITY IN AWS CLOUDTRAIL

1. Run your application or task
2. Request a policy from IAM Access Analyzer
3. IAM Access Analyzer gets to work
4. Customize further and apply



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Set: Policy generation inputs

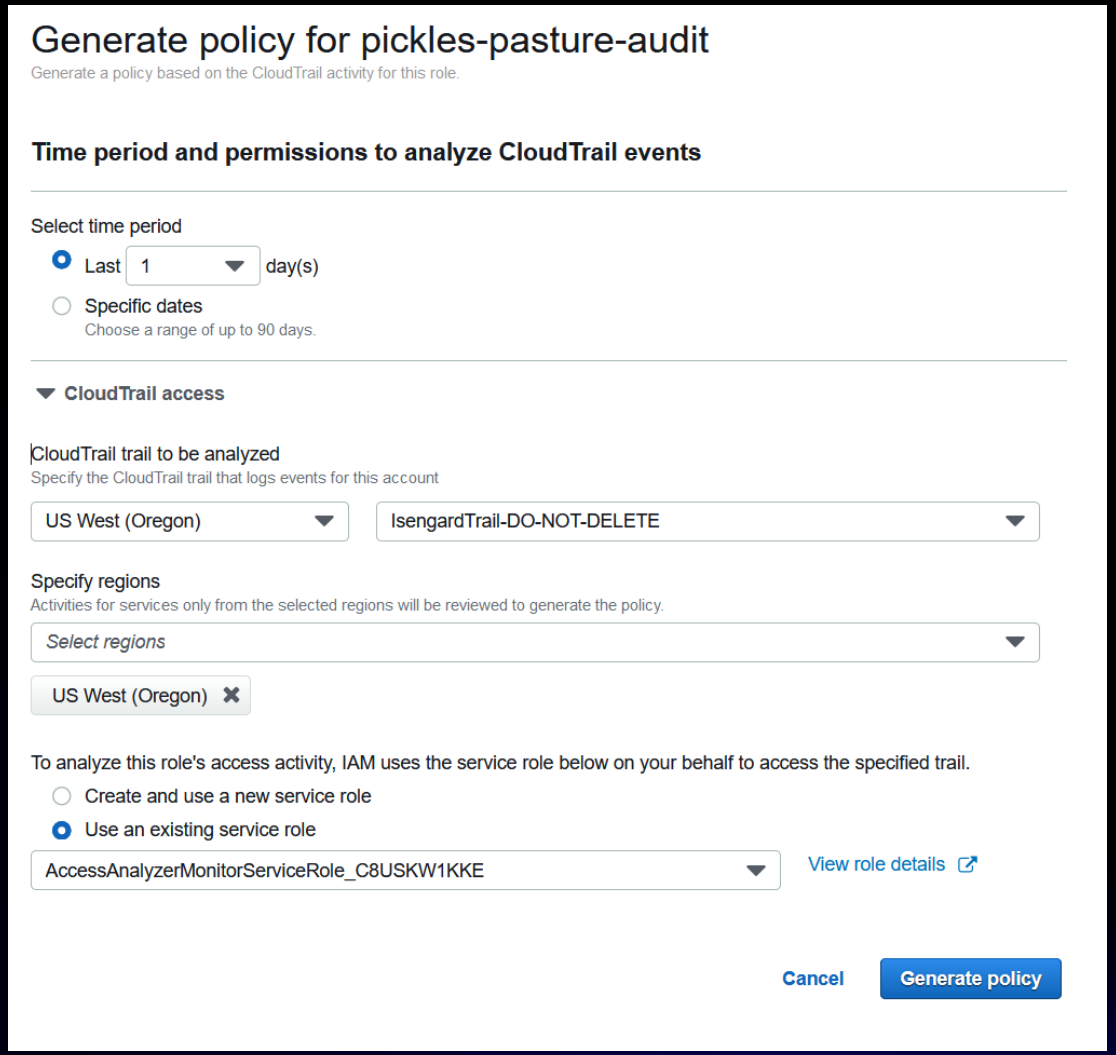


1. Run your application or task

2. Request a policy from IAM Access Analyzer

Tell us the following inputs from Step 1:

- Application role used
- Time period
- CloudTrail trail and access
- AWS Regions



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Set: Policy generation analysis



3 IAM Access Analyzer gets to work

- Looks for all unique AWS actions
- Maps CloudTrail activity to IAM actions for 50+ services
- Generates policy that adheres to IAM policy language

4 Customize and apply

- Specify additional actions
- Specify resource-level permissions with templates

Generated policy

Customize permissions

Review the following policy template. You must specify resources for actions that support resource-level permissions to continue creating the policy.

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": [
7                  "ec2:DescribeInstances",
8                  "tag:GetResources"
9              ],
10             "Resource": "*"
11         },
12         {
13             "Effect": "Allow",
14             "Action": [
15                 "cloudformation:DescribeStacks",
16                 "cloudformation:ListStackResources"
17             ],
18             "Resource": "arn:aws:cloudformation:${Region}:${Account}:stack/${StackName}/${Id}"
19         },
20         {
21             "Effect": "Allow",
22             "Action": [
23                 "logs:CreateLogGroup",
24                 "logs:CreateLogStream"
25             ],
26             "Resource": "arn:aws:logs:${Region}:${Account}:log-group:${LogGroupName}"
27         },
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Set: Policy generation in action

Demo!

Goal

Right-size the permissions for the pasture audit Lambda function that Pickles uses

Demo steps

1. Select the “pickles-pasture-audit” role used for my Lambda function
2. Request a policy from IAM Access Analyzer
3. Customize by specifying resources and additional actions
4. Apply the new right-sized policy



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pro tip: Become besties with conditions



Grant access to these actions, **but only if** these conditions are met

```
"Effect": "Allow",
"Action": [
        "ec2:StartInstances",
        "ec2:StopInstances"],
"Resource": "*",
"Condition": {
        "StringEquals": {"ec2:ResourceTag/project": "pickles"}
            }
```

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Conditions: Deep dive

"Condition" : { "{condition-operator}" : { "{condition-key}" : "{condition-value}" }}

Specify the type of operator used to compare the value from the context to the value in the policy

`StringEquals`
`StringLike`

If you don't have any wildcard characters, use stringEquals

Use predefined keys to look up the value in the context for policy comparison; you can use global condition keys or service-specific keys

`PrincipalIsAWSService`
`ResourceTag/project`

You cannot put a wildcard character in the condition key

The value you define that is based on your permissions requirements

`true`
`pickles`
`${PrincipalTag/project}`

A single-valued condition key can be used as a variable for condition values

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Conditions: Using multiple conditions

Every policy statement stands on its own; if there is a match, the effect applies

AND

All conditions met together

Same statement

OR

Any part of conditions met

Separate statements

OR

AND

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":“CreateSLRs",
         "Effect":"Allow",
         "Action":"iam:CreateServiceLinkedRole",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:PrincipalServiceName":"access-analyzer.amazonaws.com"
            }
         }
      },
      {
         "Sid":“RoleCreate-CFN",
         "Effect":"Allow",
         "Action":"iam:CreateRole",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
             "iam:PermissionsBoundary":"arn:aws:iam::524290187879:
                                        policy/pasture-audit-broad",
               "aws:CalledViaFirst":"cloudformation.amazonaws.com",
               "aws:RequestTag/project":["pickles", "bubble"]
            }
         }
      }
   ]
}
```

OR

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Conditions: Using multi-value conditions

Compare values in context to the values in the policy

ForAllValues: Is the context a subset of the policy? If there are no mismatches, the condition applies

Reminder: An empty set is a subset of all other sets

ForAnyValues: Is the context an intersection of the policy? If there is at least one match, the condition applies

aws:TagKeys project costcenter name	ForAllValues:StringEquals	"aws:TagKeys": ["project","name"]	Not subset
aws:TagKeys	ForAllValues:StringEquals	"aws:TagKeys": ["project","name"]	Subset
aws:TagKeys project bubbles	ForAnyValues:StringEquals	"aws:TagKeys": ["project","name"]	Intersection
aws:TagKeys	ForAnyValues:StringEquals	"aws:TagKeys": ["project","name"]	Not intersection

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Conditions: Noteworthy condition keys

aws:ResourceTag	Allow actions, but only if these tags exist	Attribute-based access control
aws:RequestTag	Create resources, but only with these tags	Attribute-based access control
CalledViaFirst	Allow actions, but only if requesting through this service	Access through AWS CloudFormation
CalledViaLast	Allow, but only if this is the last service acting on the resource	AWS KMS access to Amazon S3 bucket
PrincipalOrgID	Allow actions, but only if the principal is from my organization	A condition for most resource policies
PrincipalArn	Deny actions for all principals except this ARN	Use in SCPs to deny with exceptions
PrincipalIsAWSService	Restrict access to corporate IP and AWS services	Use in SCPs when restricting SourceIP

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Using Conditions with Denies

Deny access to principals if they are outside of my organization (PrincipalOrgID) and if they are not an AWS service (PrincipalIsAWSService).

If the principal is from my organization or the principal is an AWS service (such as AWS CloudTrail or AWS Billing and Cost Management), do not deny.

```
{
   "Sid":"EnforceIdentityPerimeter",
   "Effect":"Deny",
   "Principal":"*",
   "Action":"s3:*",
   "Resource":[
      "arn:aws:s3:::your-bucket-name",
      "arn:aws:s3:::your-bucket-name/*"
   ],
   "Condition":{
      "StringNotEqualsIfExists":{
         "aws:PrincipalOrgID":"o-n8ecxxxxx"
      },
      "BoolIfExists":{
         "aws:PrincipalIsAWSService":"false"
      }
   }
}
```

Deny access if the call is made outside of my network (a list of IPs and VPCs) and the API call is not made by an AWS service principal (PrincipalIsAWSService) or by an AWS service using the caller's identity (ViaAWSService).

```
{
   "Sid":"EnforceNetworkPerimeter",
   "Effect":"Deny",
   "Principal":"*",
   "Action":"s3:*",
   "Resource":[
      "arn:aws:s3:::your-bucket-name",
      "arn:aws:s3:::your-bucket-name/*"
   ],
   "Condition":{
      "StringNotEqualsIfExists":{
         "aws:SourceVpc":[
            "vpc-111bbb22",
            "vpc-222ccc33"
         ]
      },
      "NotIpAddressIfExists":{
         "aws:SourceIp":[
            "111.222.333.444/25",
            "555.666.777.888/29"
         ]
      },
      "BoolIfExists":{
         "aws:PrincipalIsAWSService":"false",
         "aws:ViaAWSService":"false"
      }}}
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Set: Policy validation with IAM Access Analyzer

MAKES IT EASIER TO AUTHOR SECURE AND FUNCTIONAL POLICIES WITH MORE THAN 100 CHECKS

Security
A policy contains access that can be overly permissive

Errors
A policy contains errors that prevent the policy from functioning



General warnings
A policy doesn't conform to best practices, but the issues are not security risks

Suggestions
A policy contains statements to be improved but doesn't impact the permissions of the policy

We are always adding new checks! Let us know if you have an idea

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Set: Policy validation (round 1)

Demo!

Goal

Update a custom policy to remediate security warnings and errors

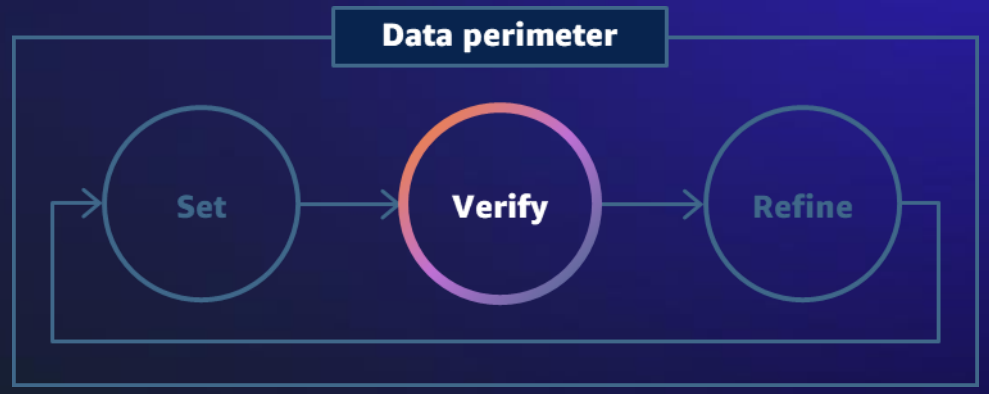
Demo steps

1. Navigate to the policy editor
2. Assess findings from IAM Access Analyzer
3. Make edits to the policy
4. Repeat steps 2 and 3 until all findings are clear

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[ "cloudtrail:GetTrail",
                    …
            "lambda:ListFunctions" ],
         "Resource":"*"
      },      {
         "Effect":"Allow",
         "Action":[ "iam:GetRole",
                    …
            "iam:ListRoleTags" ],
         "Resource":"arn:aws:iam::524290187879:role/pickles-*"
      },
      {
         "Sid":"RoleCreateCFN",
         "Effect":"Allow",
         "Action":"iam:CreateRole",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
"iam:PermissionsBoundary":"arn:aws:iam::524290187879:
policy/pasture-audit-broad",
                  "aws:RequestTag/project":["pickles", "bubble"]
}        }      }   ] }
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Verifying permissions



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Verify: Inspecting overly permissive access



Public and cross-account access



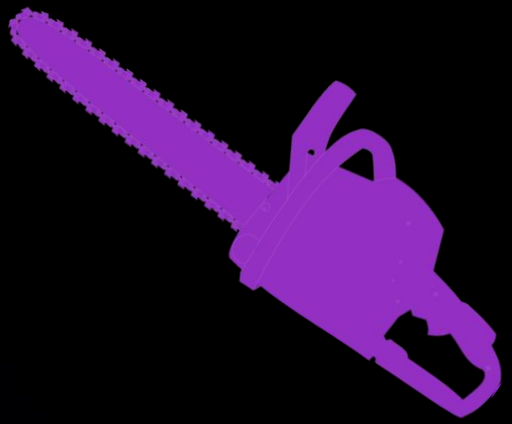
Findings using IAM Access Analyzer

PassRole access



Security warnings using policy validation with IAM Access Analyzer

Powerful permissions



Service and action last accessed

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cross-account access deep dive

Cross-account access comes from:
1. Role assumption into the account
2. Direct, cross-account access from a resource policy

Pickles's pasture (account)

horse-role

graze

hay

water

Pickles the horse



Allow horses in my barn

Verify resource policies

Treat (account)

treat-role

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pro tip: Restrict public and cross-account access



Block public access

Easy control to limit public access to Amazon S3 resources that are enforced regardless of how the resources are created

Condition: PrincipalOrgID

Require all principals accessing the resource to be from an account in the AWS organization



Condition: PrincipalArn

Restrict access to a specific principal, or deny access to all but a specific principal

Condition: PrincipalServiceName

Restrict access to specific AWS service principals, such as `cloudtrail.amazonaws.com`

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Verify: Findings with IAM Access Analyzer



IDENTIFY AND REMEDIATE PUBLIC AND CROSS-ACCOUNT ACCESS

1. **Enable** IAM Access Analyzer in your account or organization
2. Continuously **monitors and reviews** access controls across seven resources types
3. Uses **automated reasoning** to determine public or cross-account access
4. **Generates findings** for you to review and determine if they match your intent
5. **Verify** public and cross-account access by previewing access as you modify resource policies



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Verify: AWS uses automated reasoning

Reasoning is the process of **applying logic** to infer **new conclusions** from known facts about a system

Automated reasoning uses computers to unlock the ability for us to **reason about an infinite number of paths** in seconds

Proves the correctness of **universal statements** for complex systems

IAM Access Analyzer uses automated reasoning to provide you with a **comprehensive analysis of external access** to your resources

Review **public and cross-account findings** in IAM Access Analyzer to verify that existing access controls meet your intent

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Verify: Cross-account findings in action

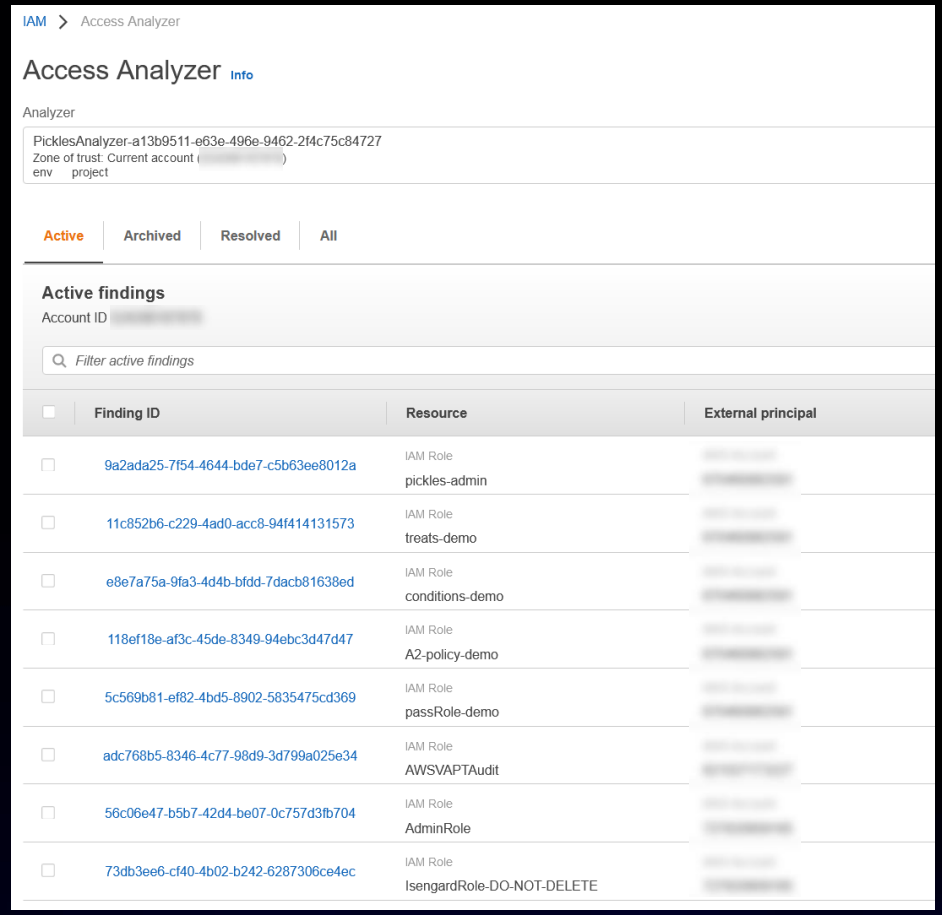
Demo!

Goal

Verify bucket and role access matches my intent

Demo steps

1. Prep: Enable IAM Access Analyzer
2. Review findings for IAM roles
3. Identify buckets and roles with external access
4. Refine access by removing access



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pro tip: Restrict PassRole permissions





Admin

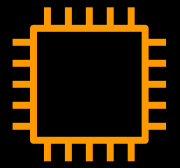


Monitoring



pickles





EC2 instance



Lambda function



Amazon RDS monitoring

Define a specific set of roles

```
"Effect": "Allow",
"Action": "iam:PassRole",
"Resource":
"arn:aws:iam::account:role/pickles-*",
"Condition": {
        "aws:PassedToService": {
        “lambda.aws”}   }
```

Define the services to pass to

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Verify: Policy validation in action (2)

Demo!

Goal

Verify my developer policy adheres to security best practices

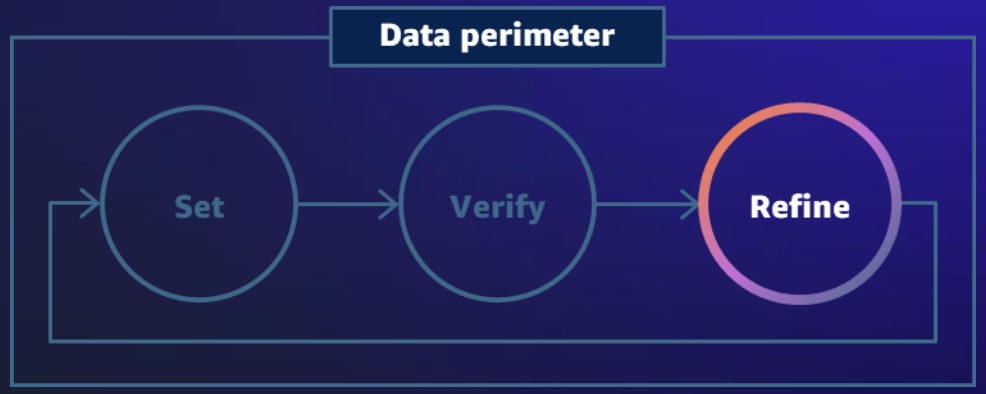
Demo steps

1. Navigate to the policy editor
2. Assess findings from IAM Access Analyzer
3. Analyze the security warnings for `PassRole`
4. Update the policy to restrict access further

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "iam:ListRoles",
                "lambda:GetAccountSettings",
                "lambda:ListEventSourceMappings",
                "lambda:ListFunctions" ],
            "Resource": "*"
        },{
            "Effect": "Allow",
            "Action": ["lambda:CreateFunction",
                "lambda:GetFunction",
                        …
                "lambda:UpdateFunctionCode",
                "lambda:invokeFunction" ],
            "Resource": "arn:aws:lambda:us-west-2:524290187879:
                                    function:pasture-*"
        },{
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::524290187879:role/pickles-*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedtoService": "lambda.aws"
                }
            }       }    ]}
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Refining permissions

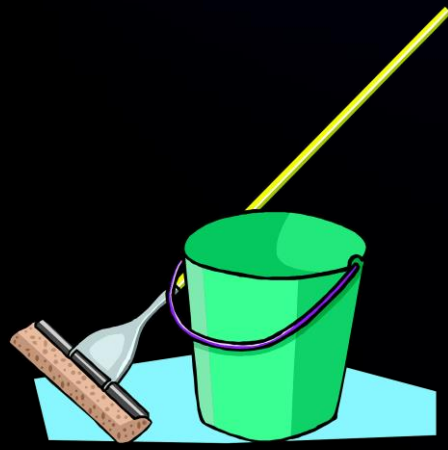


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Refine: Tools to identify unused access

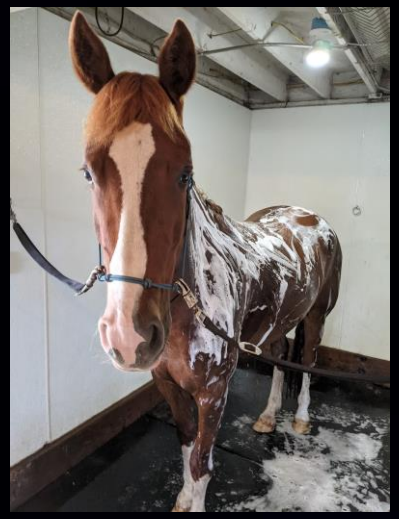


Roles and IAM users



Role last used and access key last used

Unused permissions



Service and action last accessed

Multi-account restrictions



Service last accessed for SCPs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Refine: Last accessed in action

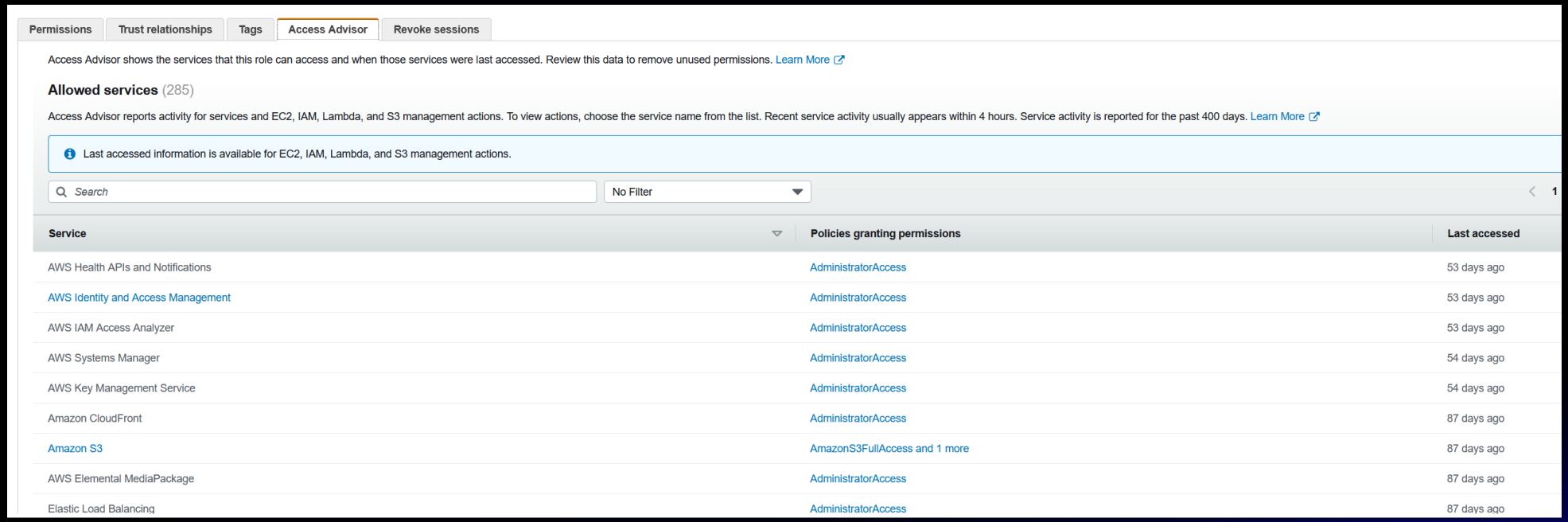
Demo!

Goal

Identify permissions the role did not use in the last 90 days and tighten permissions

Demo steps

1. Navigate to my application role
2. Analyze last accessed information
3. Update policy to remove unused access



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

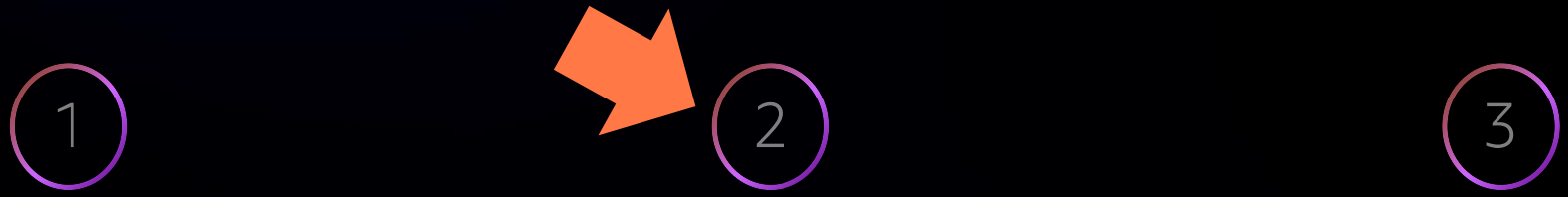
Permissions challenges

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Challenge: Pick the right tool

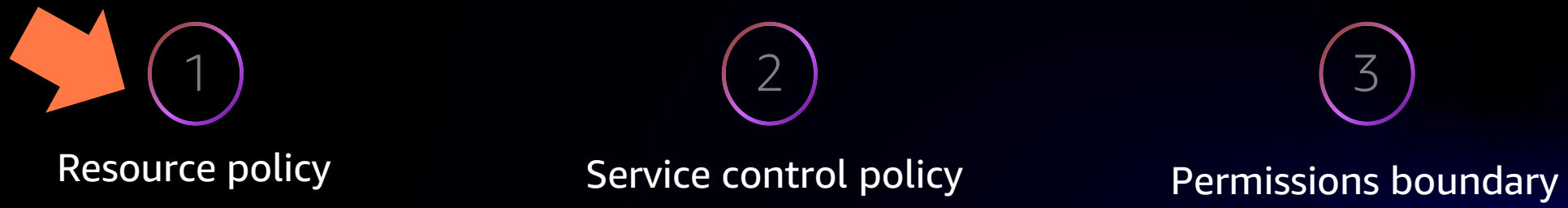
Task 1

Require a specific tag key and value when creating a secret in AWS Secrets Manager



Task 2

Implement a guardrail so that no one outside your organization can access data in a bucket



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Challenge: Pick the condition key

Task 3

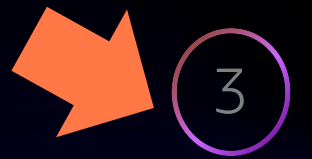
Prevent everyone but your network admin from creating and attaching internet gateways



1. aws:PrincipalARN
2. aws:CalledVia
3. aws:PrincipalOrgID

Task 4

Allow the creation of infrastructure, but only when using CloudFormation



1. aws:PrincipalIsAWSService
2. aws:PrincipalServiceName
3. aws:CalledViaFirst

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Challenge: True or false?

1. If you need to evaluate more than one type of condition together, you keep them in the same statement

   TRUE

2. You can always use any condition key anywhere in an IAM policy

   FALSE

3. If you have a list of condition values, you always need to use `forAllValues` or `forAnyValues`

   FALSE

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pro tips: Recap

- 📣 Use the right permissions tool
- 📣 Become besties with conditions
- 📣 Restrict public and cross-account access
- 📣 Restrict PassRole permissions
- 📣 Enable IAM Access Analyzer
- 📣 Validate your policies
- 📣 Use policy generation with IAM Access Analyzer

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.