Scaling Accounts & Permissions Management with AWS

Brigid Johnson, Senior Manager of Product Management
AWS Identity, Directory, and Access Management

Purpose of permissions in your organization

Goal

Business to innovate

Agility to move fast

Give developers freedom

Ensure

Prevent dangerous actions

Accountable for security posture

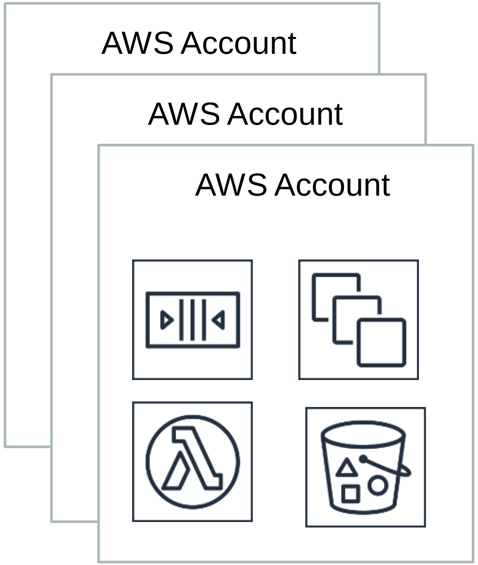
Cost effective solutions

Who Can Access What

Workforce Users

Permissions

AWS Resources



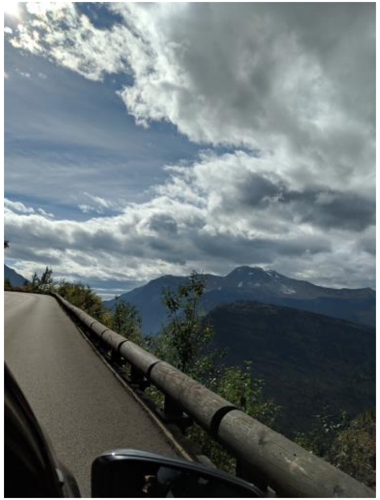
AWS Account

AWS Account

AWS Account

Model for Permissions Management at Scale

Guardrails + **General workforce permissions** + **Dial in permissions over time**



AWS permissions management services

Guardrails + **General workforce permissions** + **Dial in permissions over time**

AWS Organizations

AWS IAM roles and policies

AWS IAM access advisor

What we will cover today

- Managing Accounts with AWS Organizations
- Account Strategy with AWS Organizations
- Permission Guardrails
- Enable Developers to Create Roles Safely with Permission Boundaries
- Use Tags to Scale Permissions Management
- Automate analyzing your permissions using IAM access advisor APIs

Managing Accounts with AWS Organizations

Overview of AWS Organizations

Centrally manage and govern across AWS accounts

Central governance and management for multiple AWS accounts

Manage billing, control access, compliance, and security, across your AWS accounts

Automate account creation, create groups of accounts based on business need. Apply policies for these groups.

Multi-account capabilities with AWS Organizations

AWS Artifact – accept agreements on behalf of all accounts within your organization

AWS CloudTrail – create an organization trail that logs all events for all accounts in that organization

Amazon CloudWatch Events – enable sharing of all CloudWatch Events across all accounts in your organization

AWS Config – View an organization-wide view of your compliance status.

AWS Directory Service – seamless directory sharing across multiple accounts and any VPC in a Region

Multi-account capabilities with AWS Organizations

AWS Firewall Manager – centrally configure and manage AWS WAF rules across accounts in your organization

AWS License Manager – enable cross-account discovery of computing resources throughout your organization

AWS RAM – share resources within your organization without exchanging additional invitations.

AWS Service Catalog – share portfolios and copy products across accounts more easily, without sharing portfolio IDs

AWS Single Sign-On – enable users to sign in to the AWS SSO user portal with their corporate credentials and access resources in their assigned accounts

Account Strategy with AWS Organizations

AWS Accounts and Organizational Units (OUs)

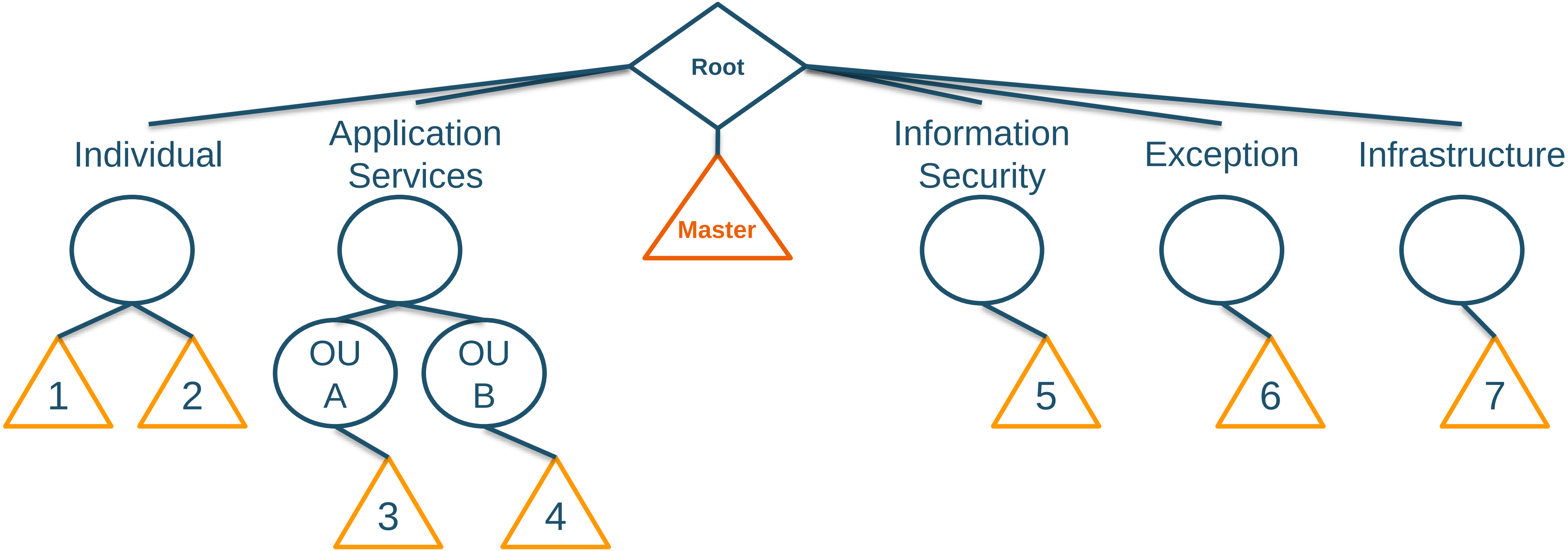
AWS accounts contain your AWS resources

Use resource permissions or roles to share across accounts

Group accounts in your organization into organizational units (OUs) to simplify management of these accounts.

Create multiple OUs within a single organization, and you can create OUs within other OUs to form a hierarchical structure

Organizing Your Accounts



Separate workloads using AWS accounts

Isolation requirements (e.g. compliance requirements)

Support for automation

Permission guardrail and application similarities

Course

Fine-grained

Less Accounts

Manual Okay

More Accounts

More Automation

Organizing Service Accounts into OUs

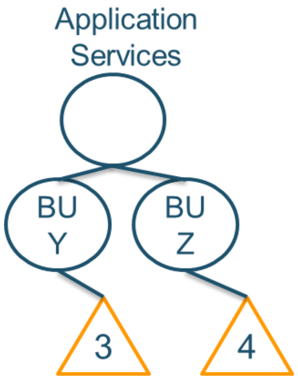
Questions to Consider:

How many business units will you grow to?

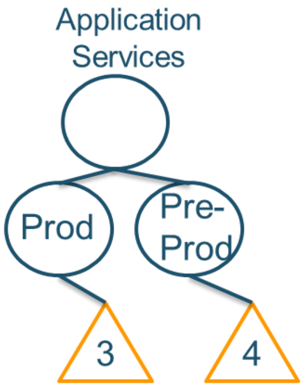
What are the commonalities among account guardrails?

How much can you automate?

Option 1: Business Unit



Option 2: Environment Type



Permission Guardrails

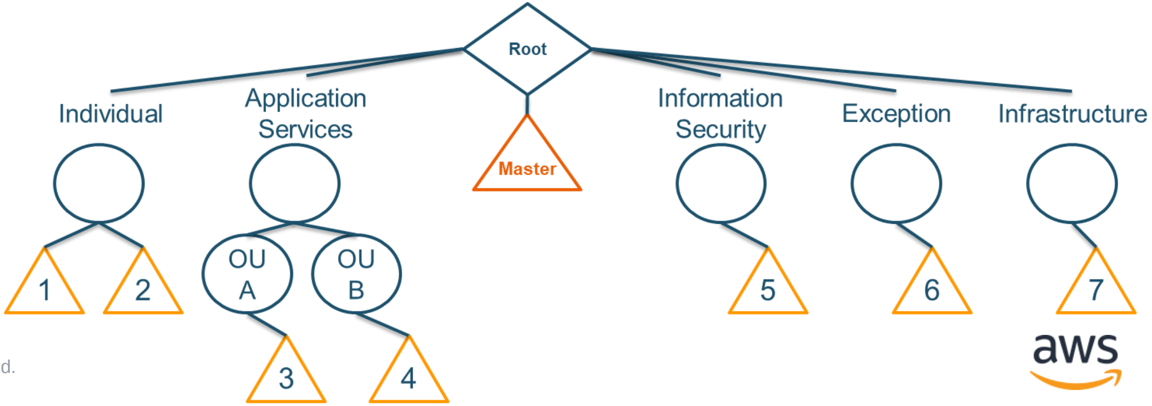
Service Control Policies with AWS Organizations

Set permission guardrails by defining the maximum available permissions for IAM entities in an account

SCPs do not grant permission

Attach SCPs to the organization root, OUs, and individual accounts

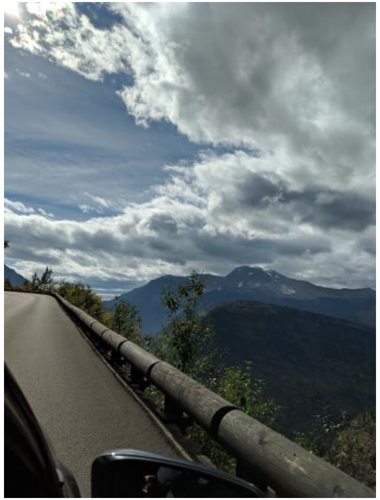
SCPs attached to the root and OUs apply to all OUs and accounts inside of them



Permission Guardrails Using SCPs

New! Specify Resources, Conditions, and NotAction in SCPs

- Restrict access from deleting common resources
- Define exceptions to your governance controls
- Centrally control access to AWS regions



Demonstration of SCPs Create and Test

New! New SCP editor to make it easier to author SCPs.

Use Case

Restrict access from deleting or modifying common IAM security audit IAM role

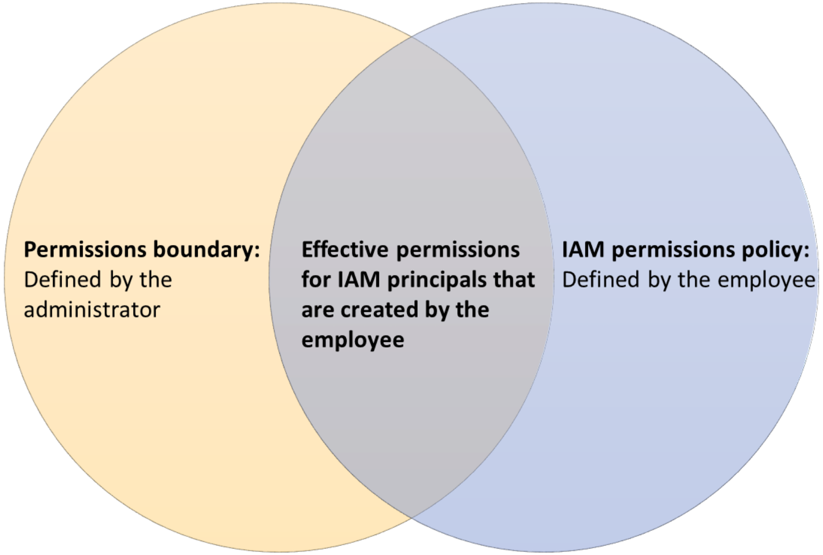
1. Create an SCP to deny access to delete and modify security audit roles
2. Attach the SCP to the root of the AWS Organization
3. Test it! Sign in to linked account and test it

Enable Developers to Create Roles Safely with Permission Boundaries

Permission boundaries

Scale and delegate permission management to developers safely

Control the maximum permissions employees can grant



Permissions boundary: Defined by the administrator

Effective permissions for IAM principals that are created by the employee

IAM permissions policy: Defined by the employee

Permission boundary workflows

1

Admin creates maximum permissions

2

Admin allows developers to create role with maximum permissions

3

Developer creates role with maximum permissions and specific permissions

4

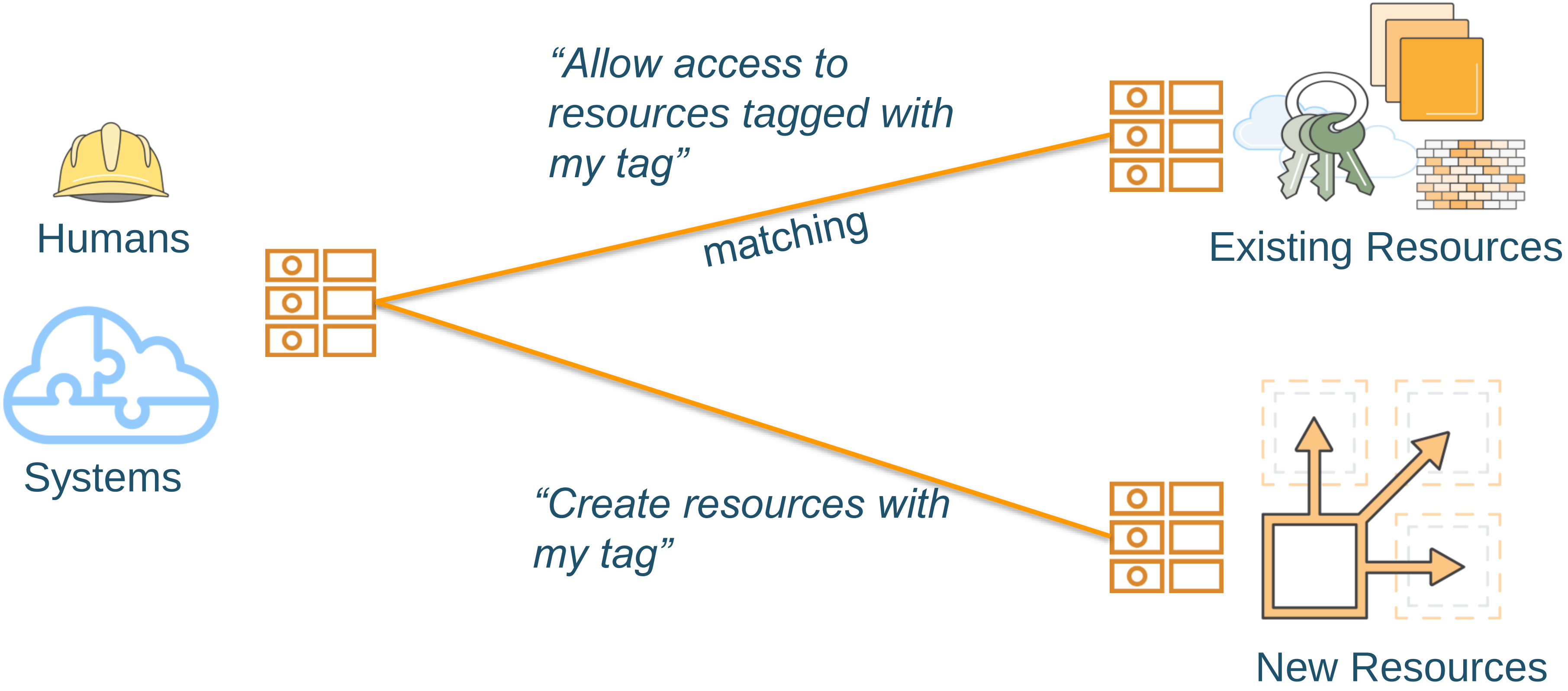
Developers passes the role to application resources

Let’s see permission boundaries in action

- Using the developer role, create a role with a permission boundary
- Use a role with a permission boundary to put data in S3 for approved regions and for unapproved regions.

Use Tags to Scale Permissions Management

Attribute-based Access Control in AWS using Tags



Humans

Systems

“Allow access to resources tagged with my tag”

matching

Existing Resources

“Create resources with my tag”

New Resources

Three parts required for tag-based access control

Allow users to create tags when creating resources, but require specific tags when users create resources

RequestTag condition to require specific tag value during create actions

Control which existing resources and values developers can tag

Use a combination of RequestTag and ResourceTag control access

Control resources users can manage based on tag values

ResourceTag to control access to resources based on a tag that exists on a resource

Automate analyzing your permissions using IAM access advisor APIs

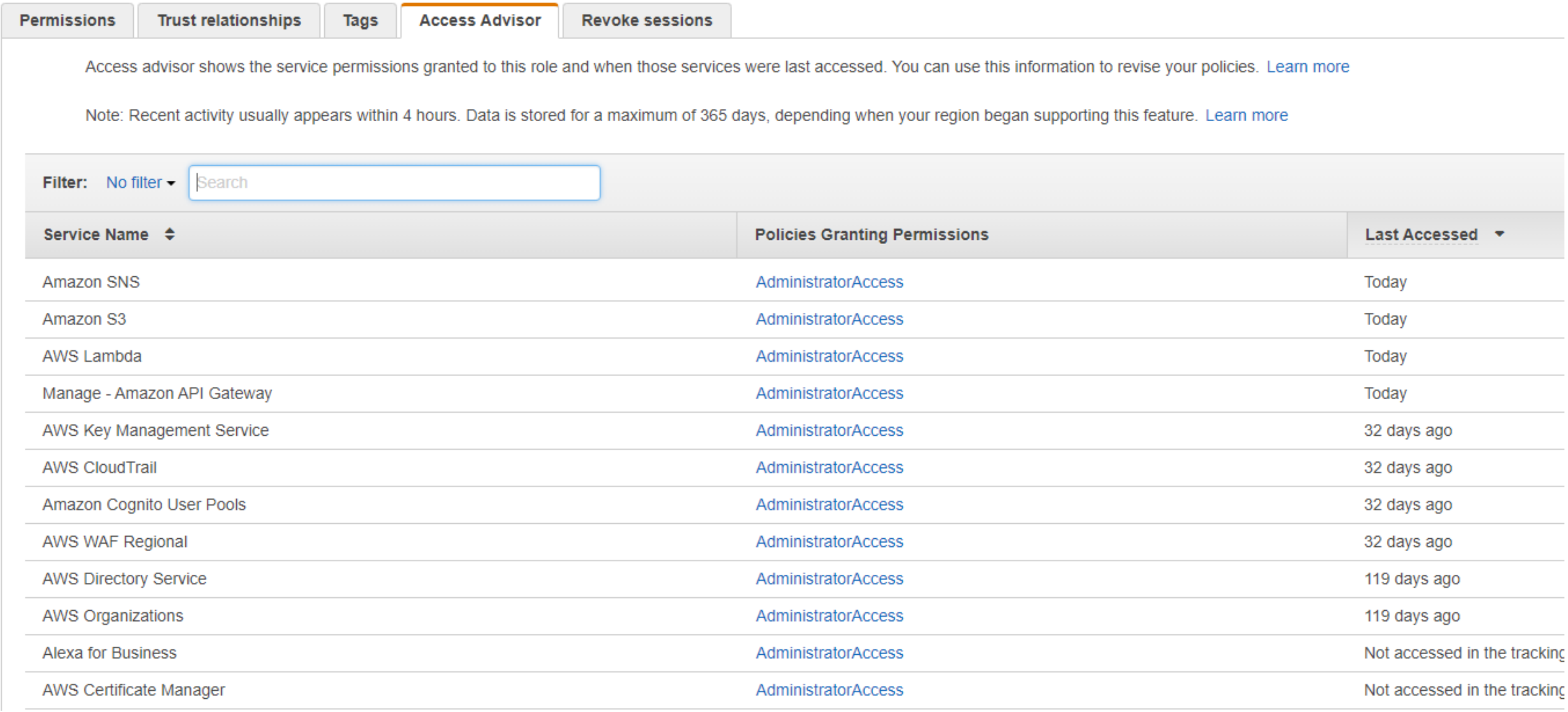
Overview of Dialing in Permissions

Step 1: Determine services last accessed

Step 2: Compare to permissions

Step 3: Remove unused permissions

Step 1: Determine services last accessed



Access advisor shows the service permissions granted to this role and when those services were last accessed. You can use this information to revise your policies. Learn more

Note: Recent activity usually appears within 4 hours. Data is stored for a maximum of 365 days, depending when your region began supporting this feature. Learn more

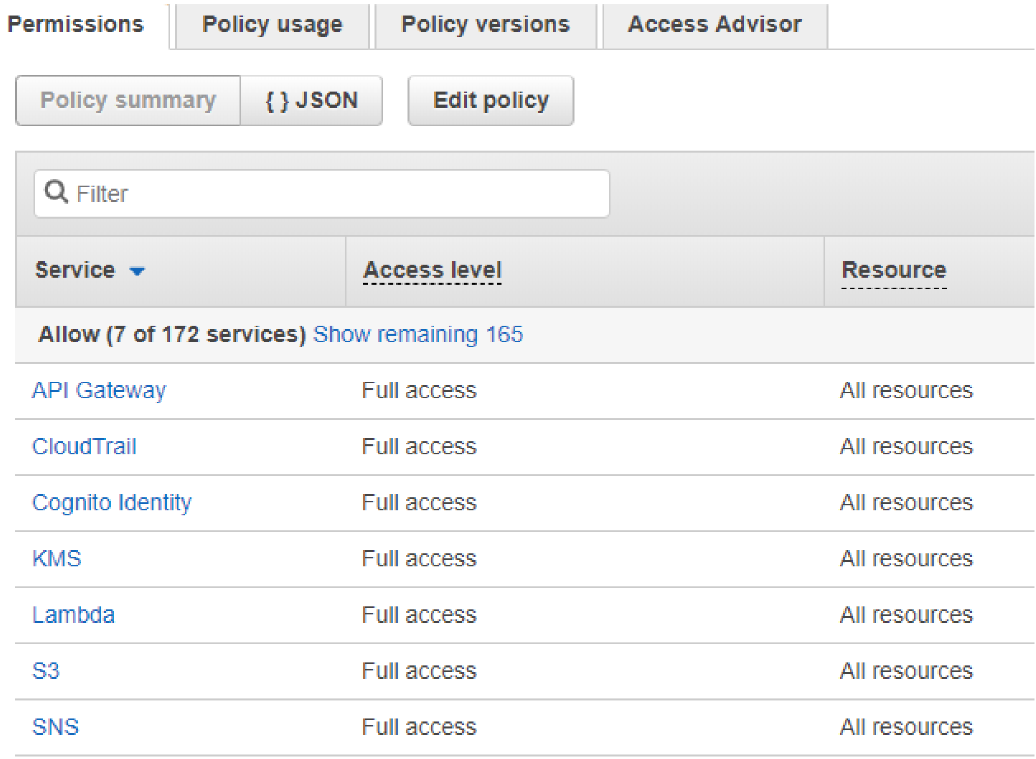
Filter: No filter ▾ Search

Service Name ⇕	Policies Granting Permissions	Last Accessed ▾
Amazon SNS	AdministratorAccess	Today
Amazon S3	AdministratorAccess	Today
AWS Lambda	AdministratorAccess	Today
Manage - Amazon API Gateway	AdministratorAccess	Today
AWS Key Management Service	AdministratorAccess	32 days ago
AWS CloudTrail	AdministratorAccess	32 days ago
Amazon Cognito User Pools	AdministratorAccess	32 days ago
AWS WAF Regional	AdministratorAccess	32 days ago
AWS Directory Service	AdministratorAccess	119 days ago
AWS Organizations	AdministratorAccess	119 days ago
Alexa for Business	AdministratorAccess	Not accessed in the tracking
AWS Certificate Manager	AdministratorAccess	Not accessed in the tracking

Step 2: Compare to permissions

Has Access To	Service Last Accessed in 60 days
Amazon SNS	Amazon SNS
Amazon S3	Amazon S3
AWS Lambda	AWS Lambda
Amazon API Gateway	Amazon API Gateway
AWS KMS	AWS KMS
AWS CloudTrail	AWS CloudTrail
AWS Cognito User Pools	AWS Cognito User Pools
AWS Organization	AWS Organization
AWS Directory Service	AWS Directory Service
AWS Certificate Manager	AWS Certificate Manager

Step 3: Remove unused permissions



Service	Access level	Resource
Allow (7 of 172 services) Show remaining 165		
API Gateway	Full access	All resources
CloudTrail	Full access	All resources
Cognito Identity	Full access	All resources
KMS	Full access	All resources
Lambda	Full access	All resources
S3	Full access	All resources
SNS	Full access	All resources

Recap

Guardrails +

AWS Organizations

Multi-account management

Organize your accounts

General workforce permissions +

AWS IAM roles and policies

Permission Boundaries

Attribute-based Access Control

Dial in permissions over time

AWS IAM access advisor

Access Advisor APIs

Learn More

Videos

Become an IAM Policy Master in 60 Minutes or Less (SEC316-R1)

Architecting Security and Governance Across a Multi-Account Stra (SID331)

Blogs

Automate analyzing your permissions using IAM access advisor APIs

Simplify granting access to your AWS resources by using tags on AWS IAM users and roles

Thank you!