AWS Security

Rajesh Kumar

DevOps Architect

11 November 2016

amazon web services | Webinars

AWS Shared Responsibility Model

Customers

Customer Applications & Content

Platform, Applications, Identity, and Access Management

Operating System, Network, and Firewall Configuration

Client-side Data Encryption | Server-side Data Encryption | Network Traffic Protection

Customers are responsible for security **IN** the cloud

AWS Foundation Services

Compute | **Storage** | **Database** | **Networking**

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

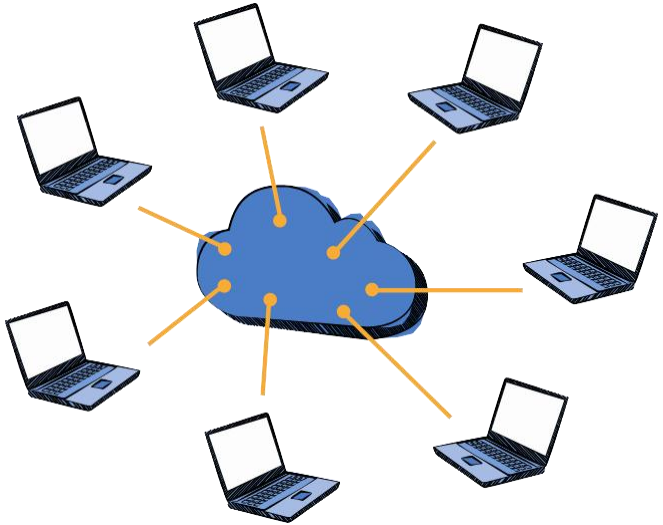
AWS is responsible for the security **OF** the cloud

Physical Security

- 24/7 trained **security staff**
- AWS data centers in **nondescript** and **undisclosed** facilities
- **Two-factor authentication** for authorized staff
- **Authorization** for data center access

Hardware, Software, and Network

- Automated **change-control** process
- Bastion servers that **record all access attempts**
- **Firewall** and other **boundary devices**
- AWS **monitoring** tools



Certifications and Accreditations

ISO 9001, ISO 27001, ISO 27017, ISO 27018, IRAP (Australia), MLPS Level 3 (China), MTCS Tier 3 Certification (Singapore) and more …

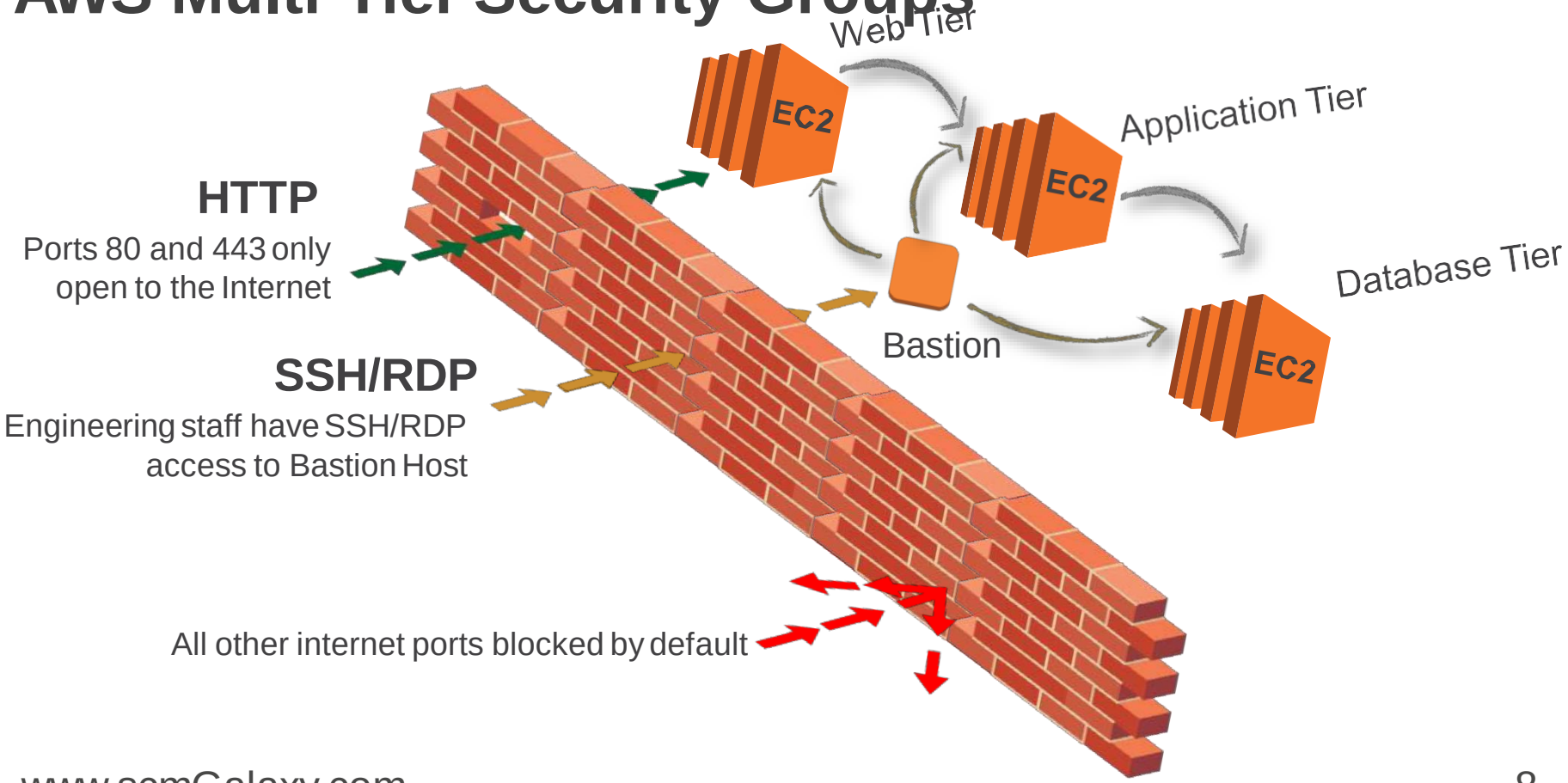
SSL Endpoints

SSL Endpoints	Security Groups	VPC
Secure Transmission Use secure endpoints to establish secure communication sessions (HTTPS).	**Instance Firewalls** Use security groups to configure firewall rules for instances.	**Network Control** Use public and private subnets, NAT, and VPN support in your virtual private cloud to create low-level networking constraints for resource access.

Security Groups

SSL Endpoints	Security Groups	VPC
Secure Transmission	**Instance Firewalls**	**Network Control**
Use secure endpoints to establish secure communication sessions (HTTPS).	Use security groups to configure firewall rules for instances.	Use public and private subnets, NAT, and VPN support in your virtual private cloud to create low-level networking constraints for resource access.

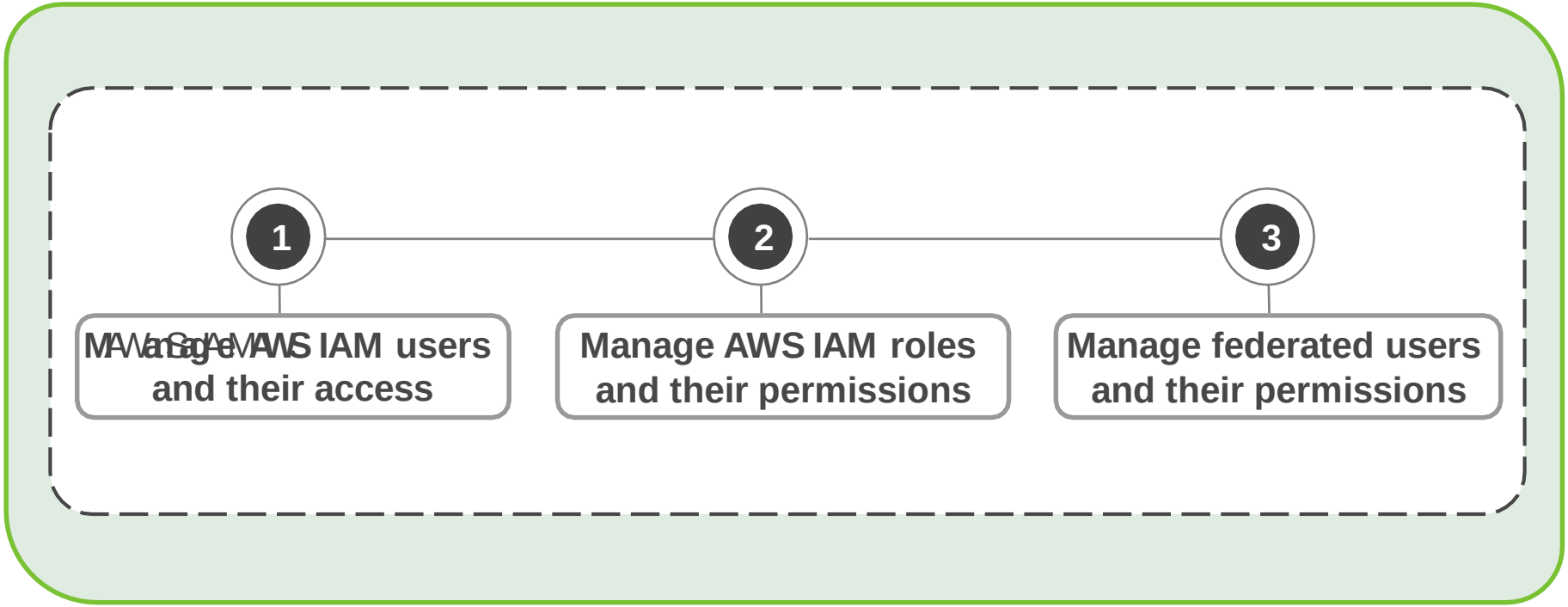
AWS Multi-Tier Security Groups



Amazon Virtual Private Cloud (VPC)

SSL Endpoints	Security Groups	VPC
Secure Transmission	**Instance Firewalls**	**Network Control**
Use secure endpoints to establish secure communication sessions (HTTPS).	Use security groups to configure firewall rules for instances.	Use public and private subnets, NAT, and VPN support in your virtual private cloud to create low-level networking constraints for resource access.

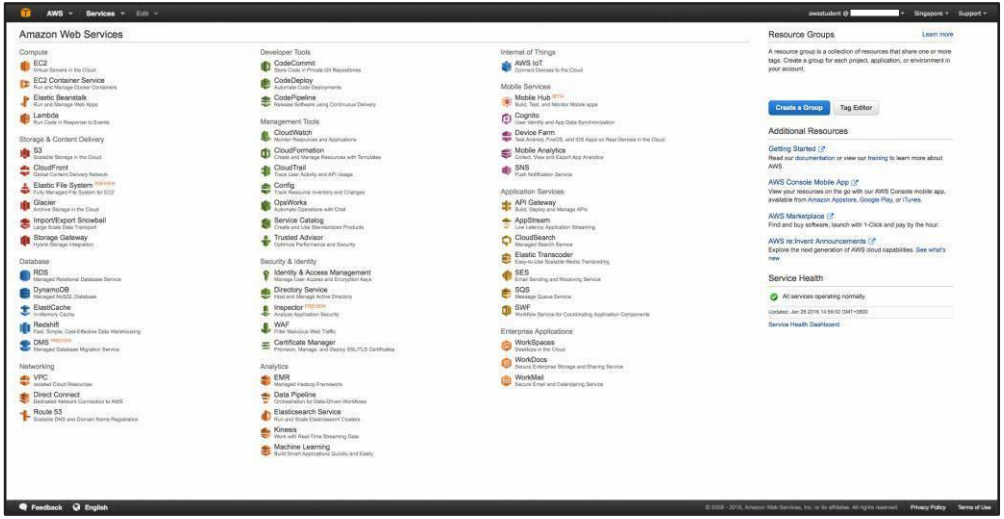
AWS Identity and Access Management (IAM)



AWS IAM Authentication

- **Authentication**
- **AWS Management Console**
  - User Name and Password

IAM User



AWS IAM Authentication

- **Authentication**
- **AWS CLI or SDK API**
  - Access Key and Secret Key

IAM User

```
Access Key ID: AKIAIOSFODNN7EXAMPLE
Secret Access Key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

AWS CLI

```
[redacted]:~ [redacted]$ aws configure
AWS Access Key ID [****************O22A]:
AWS Secret Access Key [****************4m8i]:
Default region name [ap-southeast-1]:
Default output format [json]:
```

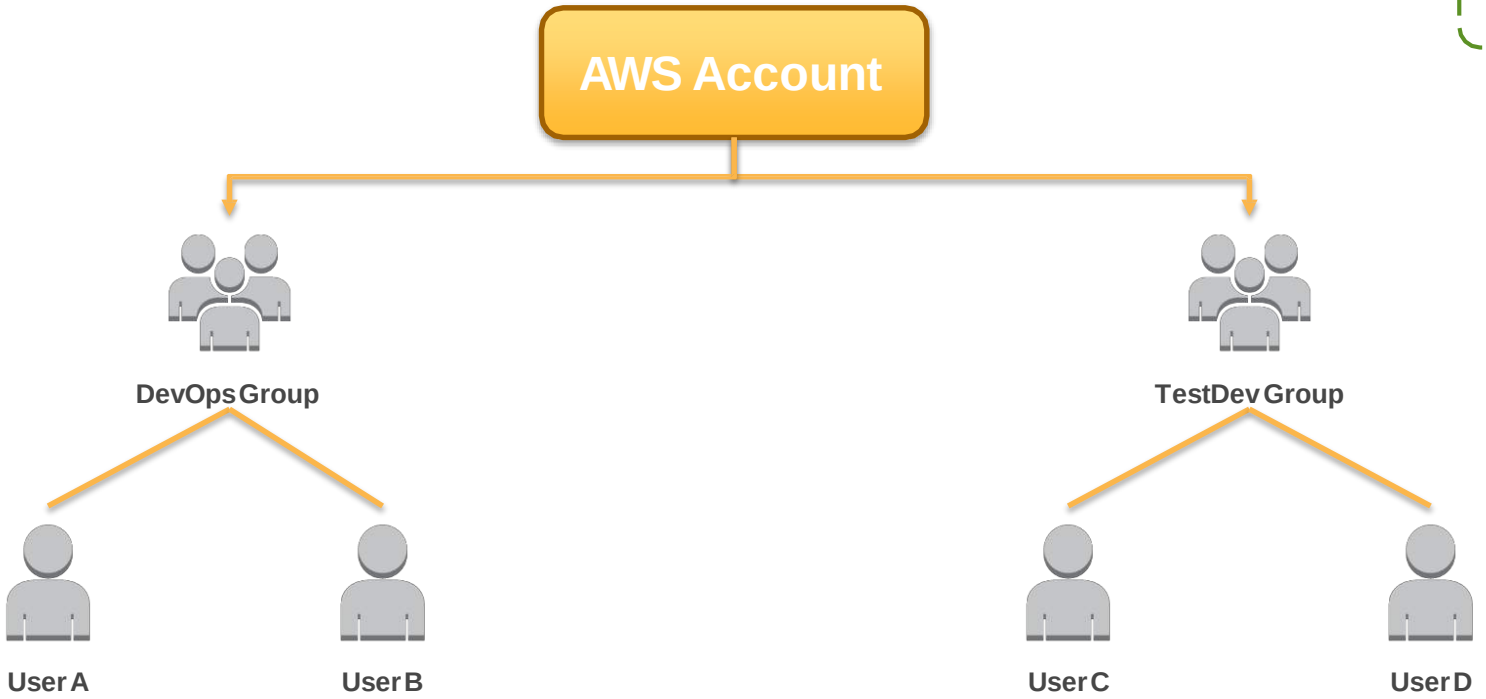
AWS SDK & API

Java

Python

.NET

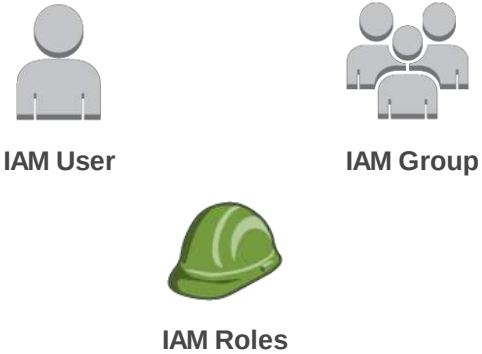
AWS IAM User Management - Groups



AWS IAM Authorization

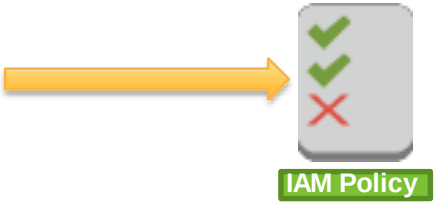
Authorization

- Policies:
  - Are JSON documents to describe permissions.
  - Are assigned to users, groups or roles.

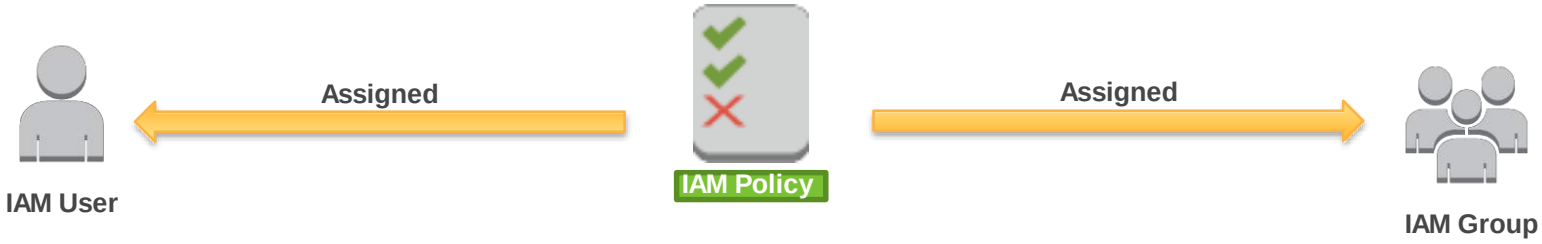


AWS IAM Policy Elements

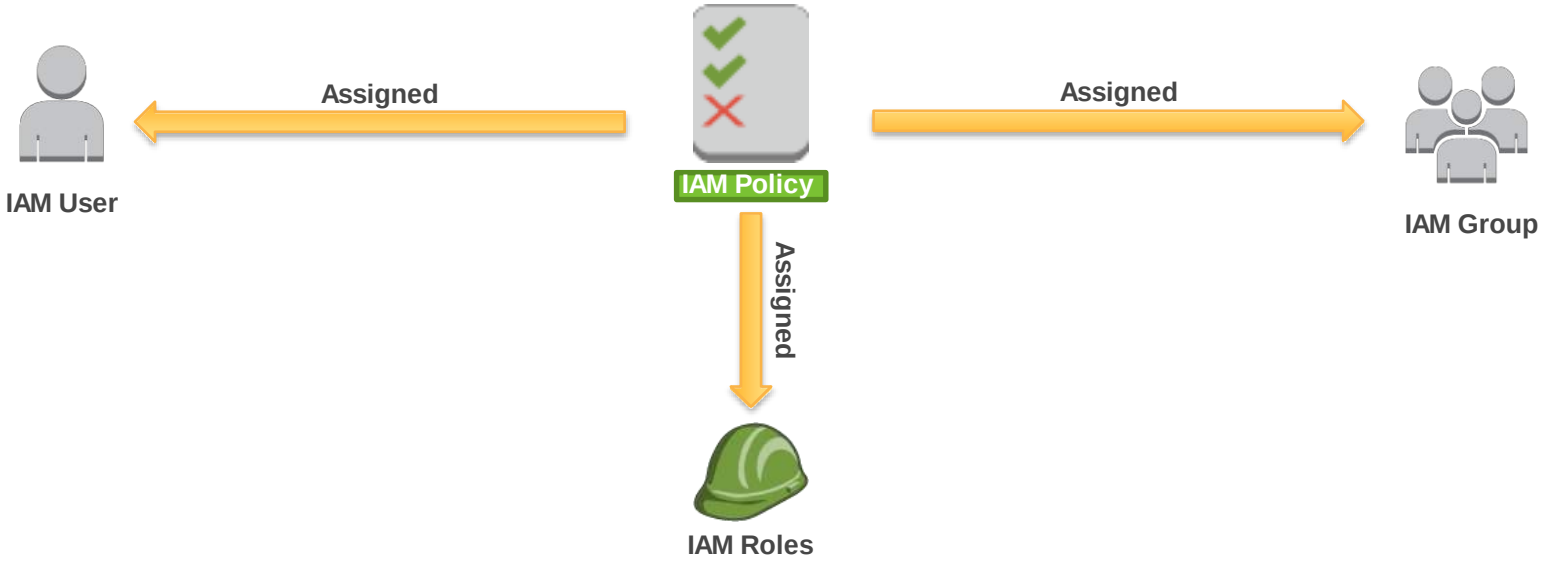
```
{
   "Version": "2012-10-17",
   "Statement": [
     {
       "Sid": "Stmt1453690971587",
         "Action": [
          "ec2:Describe*",
          "ec2:StartInstances",
          "ec2:StopInstances”
          ],
          "Effect": "Allow",
          "Resource": "*",
          "Condition": {
            "IpAddress": {
               "aws:SourceIp": "54.64.34.65/32”
            }
          }
      },
      {
          "Sid": "Stmt1453690998327",
          "Action": [
          "s3:GetObject*”
         ],
          "Effect": "Allow",
          "Resource": "arn:aws:s3:::example_bucket/*”
       }
         ]
}
```



AWS IAM Policy Assignment



AWS IAM Policy Assignment

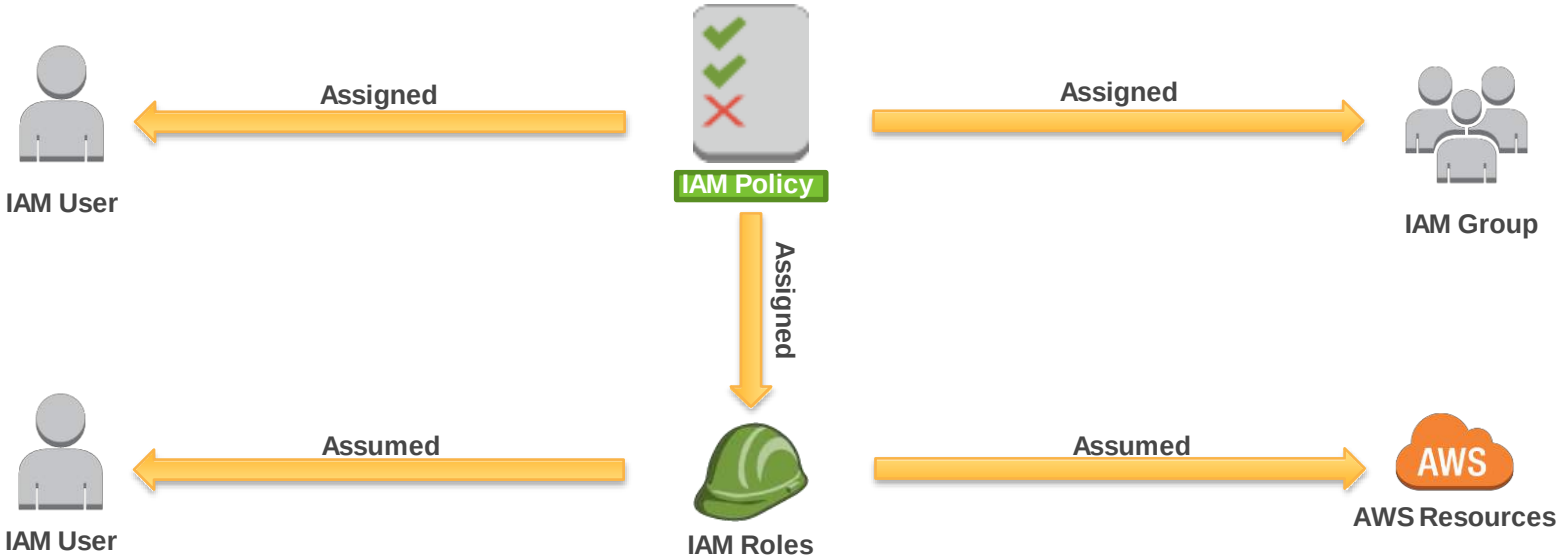


AWS IAM Roles

- An IAM role uses a policy.
- An IAM role has no associated credentials.
- IAM users, applications, and services may assume IAM roles.

IAM Roles

AWS IAM Policy Assignment



Example: Application Access to AWS Resources

- Python application hosted on an Amazon EC2 Instance needs to interact with Amazon S3.
- AWS credentials are required:
  - ~~Option 1: Store AWS Credentials on the Amazon EC2 instance.~~
  - Option 2: Securely distribute AWS credentials to AWS Services and Applications.

IAM Roles

AWS IAM Roles - Instance Profiles

Amazon EC2

1

Create Instance

Amazon S3

AWS Services Edit

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: Request Spot instances

Network: vpc-5((172.31.0.0/16) (default) — Create new VPC

Subnet: No preference (default subnet in any Availability Z — Create new subnet

Auto-assign Public IP: Use subnet setting (Enable)

Domain join directory: None — Create new directory

IAM role: None — Create new IAM role

None
aws-elasticbeanstalk-ec2-role
EMR_EC2_DefaultRole
PythoninEC2AccessS3

Shutdown behavior

Enable termination protection

Monitoring: Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

Advanced Details

Select IAM Role

2

4

Application interacts with S3

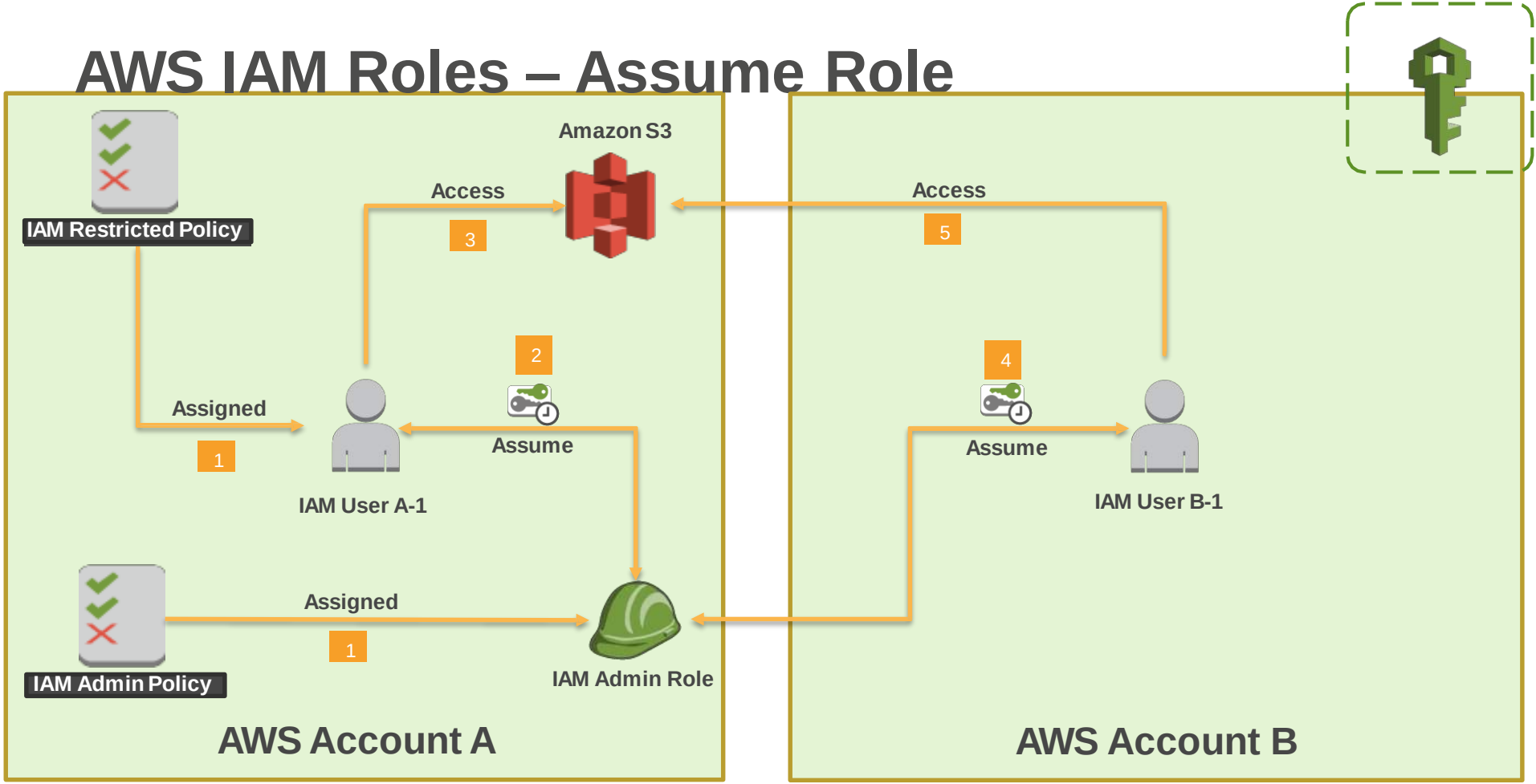
python App &

3

EC2 MetaData Service

http://169.254.169.254/latest/meta-data/iam/security-credentials/rolename

AWS IAM Roles – Assume Role



Temporary Security Credentials (AWS STS)

Session
Access Key ID
Secret Access Key
Session Token
Expiration

Temporary Security Credentials

15 minutes to 36 hours

Use Cases

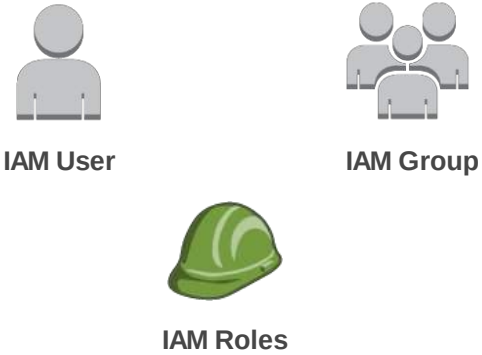
- Cross account access
- Federation
- Mobile Users
- Key rotation for Amazon EC2-based apps

Application Authentication

AWS IAM Authentication and Authorization

Authentication

- **AWS Management Console**
  - User Name and Password
- **AWS CLI or SDK API**
  - Access Key and Secret Key



Authorization

- Policies

AWS IAM Best Practices

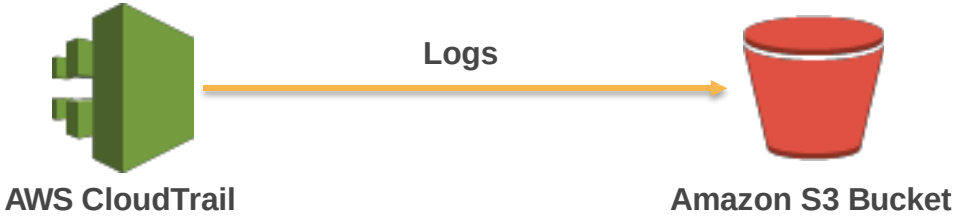
- **Delete** AWS account (root) access keys.
- Create **individual** IAM users.
- **Use groups** to assign permissions to IAM users.
- Grant **least privilege**.
- Configure a **strong password policy**.
- Enable **MFA** for privileged users.

AWS IAM Best Practices (cont.)

- Use **roles for applications** that run on Amazon EC2 instances.
- Delegate by **using roles** instead of by sharing credentials.
- **Rotate credentials** regularly.
- **Remove unnecessary** users and credentials.
- Use **policy conditions** for extra security.
- **Monitor activity** in your AWS account.

AWS CloudTrail

- Records AWS API calls for accounts.
- Delivers log files with information to an Amazon S3 bucket.
- Makes calls using the AWS Management Console, AWS SDKs, AWS CLI and higher-level AWS services.



Security Groups

A *security group* acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance.

You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.

VPS

A virtual private cloud (VPC) is a virtual network that closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of Amazon Web Services (AWS).

AWS Direct

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

VPN

You can connect your VPC to remote networks by using a VPN connection. The following are some of the connectivity options available to you.

AWS hardware VPN

AWS Direct Connect

AWS VPN CloudHub

Identity and Access Management (IAM)

User and service management

Controls access to AWS resources

Multi-factor authentication

API access

AWS IAM:
http://aws.amazon.com/iam/

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console.

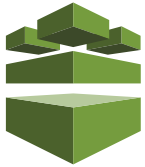
To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

- + Password
- + Multi-Factor Authentication (MFA)
- + Access Keys (Access Key ID and Secret Access Key)
- + CloudFront Key Pairs
- + X.509 Certificates
- + Account Identifiers

3 Services to Secure AWS

AWS Identity and Access Management (IAM)

AWS Config Rules

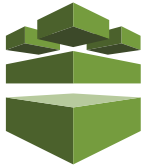


AWS CloudTrail

Services for todays Webinar

AWS Identity and Access Management (IAM)

AWS Config Rules



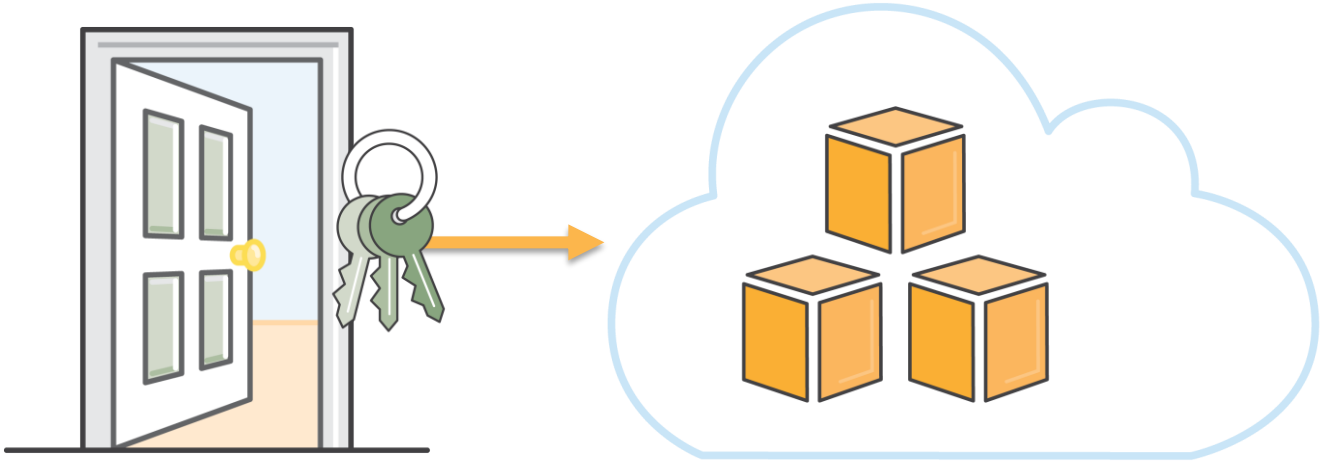
AWS CloudTrail

AWS IAM

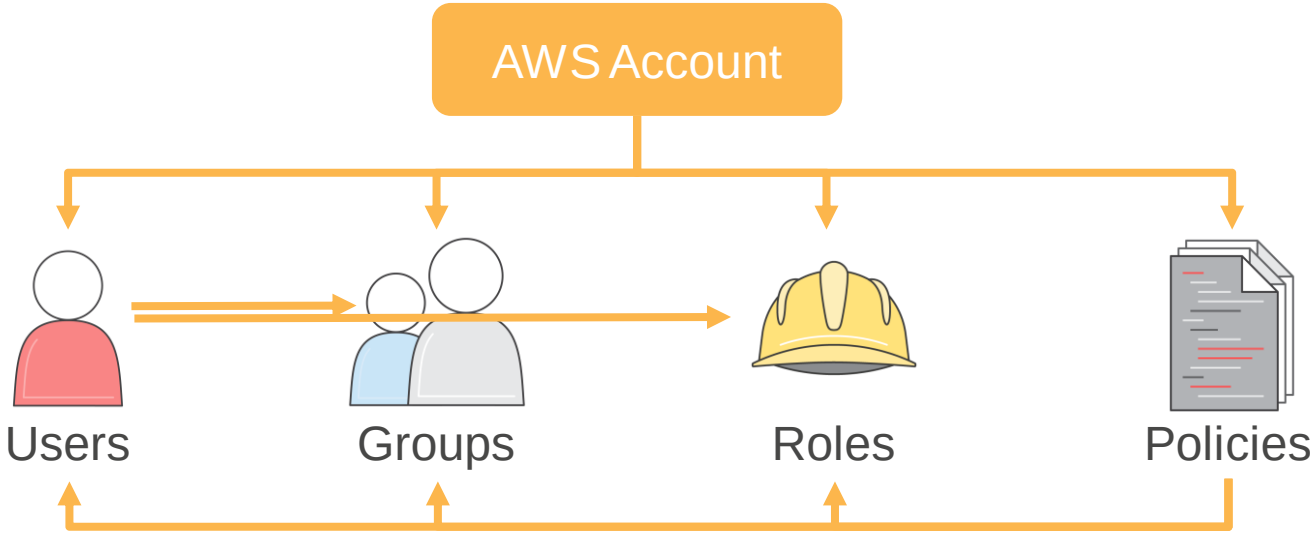
AWS IAM

IAM is a web service that enables Amazon Web Services customers to manage users and user permissions in AWS. The service is targeted for use with AWS products. With IAM, you can centrally manage users, and permissions that control which AWS resources users can access.

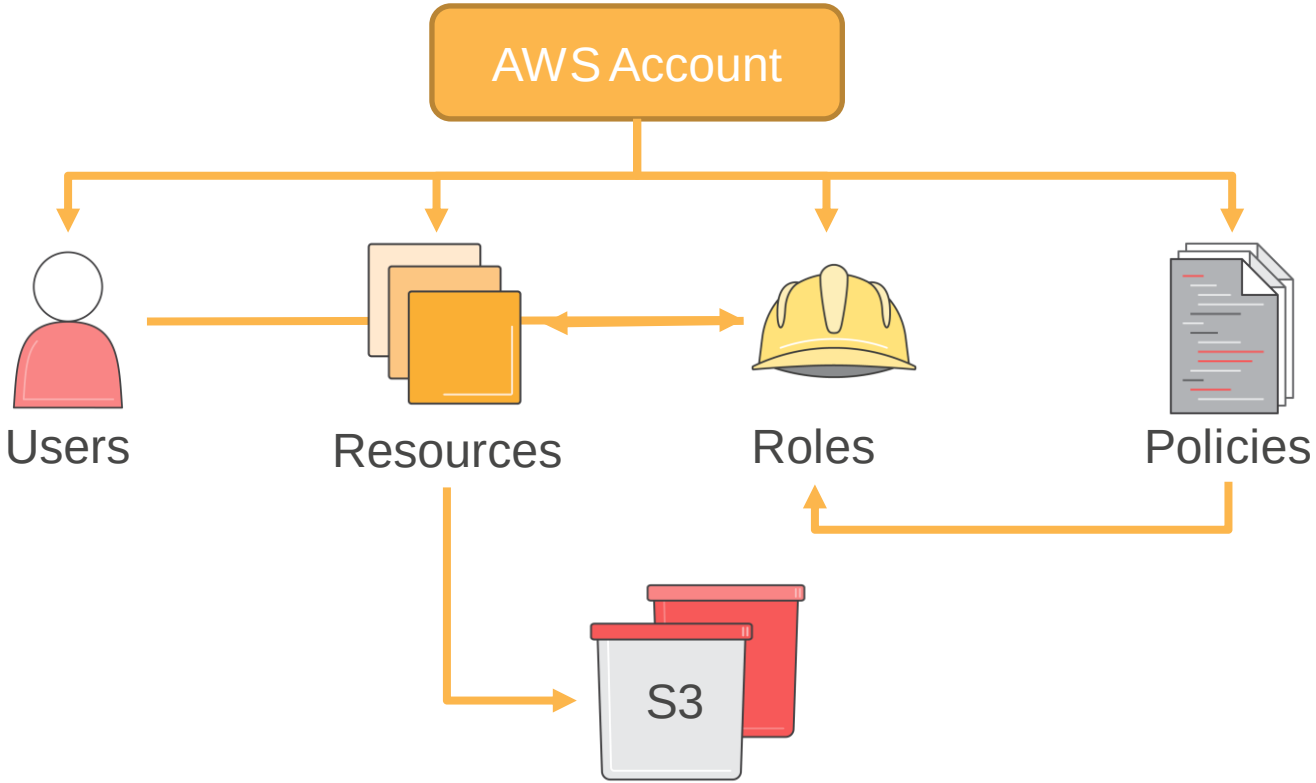
AWS IAM - Front Door



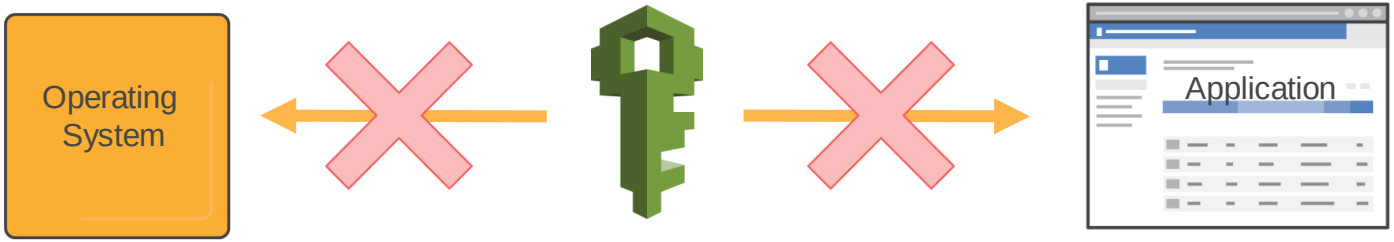
AWS IAM - Overview



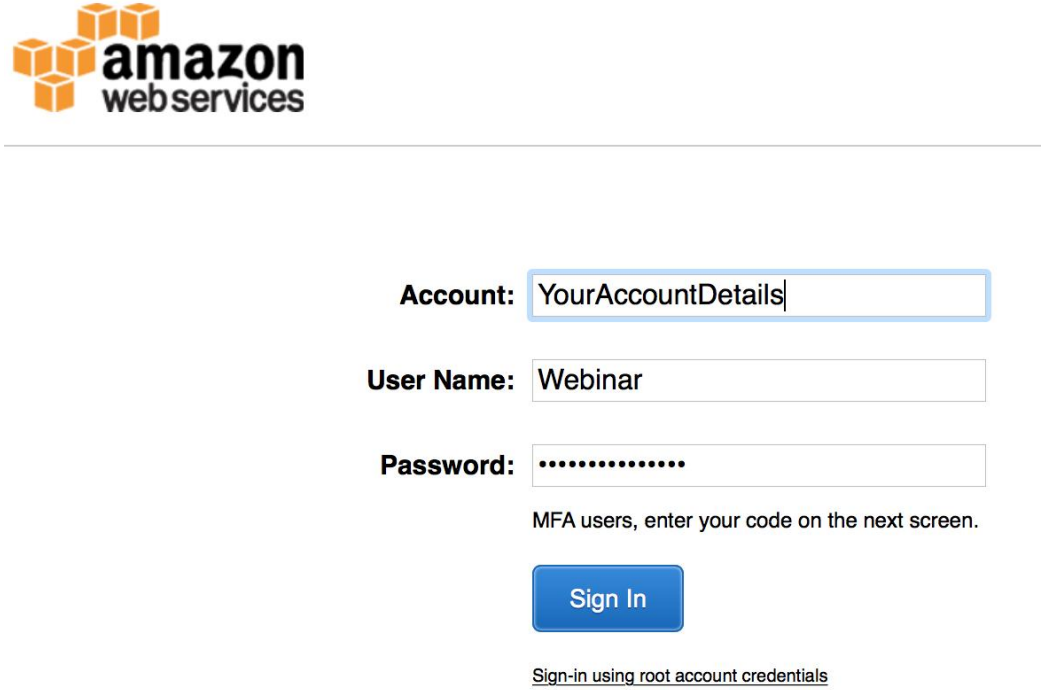
AWS IAM - Resource Access



AWS IAM – Application Authentication



AWS IAM - Logging In



AWS IAM - Inside the Console

Amazon Web Services

Compute
- **EC2** — Virtual Servers in the Cloud
- **EC2 Container Service** — Run and Manage Docker Containers
- **Elastic Beanstalk** — Run and Manage Web Apps
- **Lambda** — Run Code without Thinking about Servers
- **Server Migration** — Migrate on-premises servers to AWS

Storage & Content Delivery
- **S3** — Scalable Storage in the Cloud
- **CloudFront** — Global Content Delivery Network
- **Elastic File System** — Fully Managed File System for EC2
- **Glacier** — Archive Storage in the Cloud
- **Snowball** — Large Scale Data Transport
- **Storage Gateway** — Hybrid Storage Integration

Database
- **RDS** — Managed Relational Database Service
- **DynamoDB** — Managed NoSQL Database
- **ElastiCache** — In-Memory Cache
- **Redshift** — Fast, Simple, Cost-Effective Data Warehousing
- **DMS** — Managed Database Migration Service

Networking
- **VPC** — Isolated Cloud Resources
- **Direct Connect** — Dedicated Network Connection to AWS
- **Route 53** — Scalable DNS and Domain Name Registration

Developer Tools
- **CodeCommit** — Store Code in Private Git Repositories
- **CodeDeploy** — Automate Code Deployments
- **CodePipeline** — Release Software using Continuous Delivery

Management Tools
- **CloudWatch** — Monitor Resources and Applications
- **CloudFormation** — Create and Manage Resources with Templates
- **CloudTrail** — Track User Activity and API Usage
- **Config** — Track Resource Inventory and Changes
- **OpsWorks** — Automate Operations with Chef
- **Service Catalog** — Create and Use Standardized Products
- **Trusted Advisor** — Optimize Performance and Security

Security & Identity
- **Identity & Access Management** — Manage User Access and Encryption Keys
- **Directory Service** — Host and Manage Active Directory
- **Inspector** — Analyze Application Security
- **WAF** — Filter Malicious Web Traffic
- **Certificate Manager** — Provision, Manage, and Deploy SSL/TLS Certificates

Analytics
- **EMR** — Managed Hadoop Framework
- **Data Pipeline** — Orchestration for Data-Driven Workflows
- **Elasticsearch Service** — Run and Scale Elasticsearch Clusters
- **Kinesis** — Work with Real-Time Streaming Data
- **Machine Learning** — Build Smart Applications Quickly and Easily

Internet of Things
- **AWS IoT** — Connect Devices to the Cloud

Game Development
- **GameLift** — Deploy and Scale Session-based Multiplayer Games

Mobile Services
- **Mobile Hub** — Build, Test, and Monitor Mobile Apps
- **Cognito** — User Identity and App Data Synchronization
- **Device Farm** — Test Android, iOS, and Web Apps on Real Devices in the Cloud
- **Mobile Analytics** — Collect, View and Export App Analytics
- **SNS** — Push Notification Service

Application Services
- **API Gateway** — Build, Deploy and Manage APIs
- **AppStream** — Low Latency Application Streaming
- **CloudSearch** — Managed Search Service
- **Elastic Transcoder** — Easy-to-Use Scalable Media Transcoding
- **SES** — Email Sending and Receiving Service
- **SQS** — Message Queue Service
- **SWF** — Workflow Service for Coordinating Application Components

Enterprise Applications
- **WorkSpaces** — Desktops in the Cloud
- **WorkDocs** — Secure Enterprise Storage and Sharing Service
- **WorkMail** — Secure Email and Calendaring Service

AWS IAM - Policy Generator

amazon web services

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy and an SQS Queue Policy.

Select Type of Policy IAM Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect Allow Deny

AWS Service AWS CloudTrail ☐ All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions -- Select Actions -- ☐ All Actions ('*')

Amazon Resource Name (ARN) *

This service does not have ARNs, so "*" will be used.
Use a comma to separate multiple values.

Add Conditions (Optional)

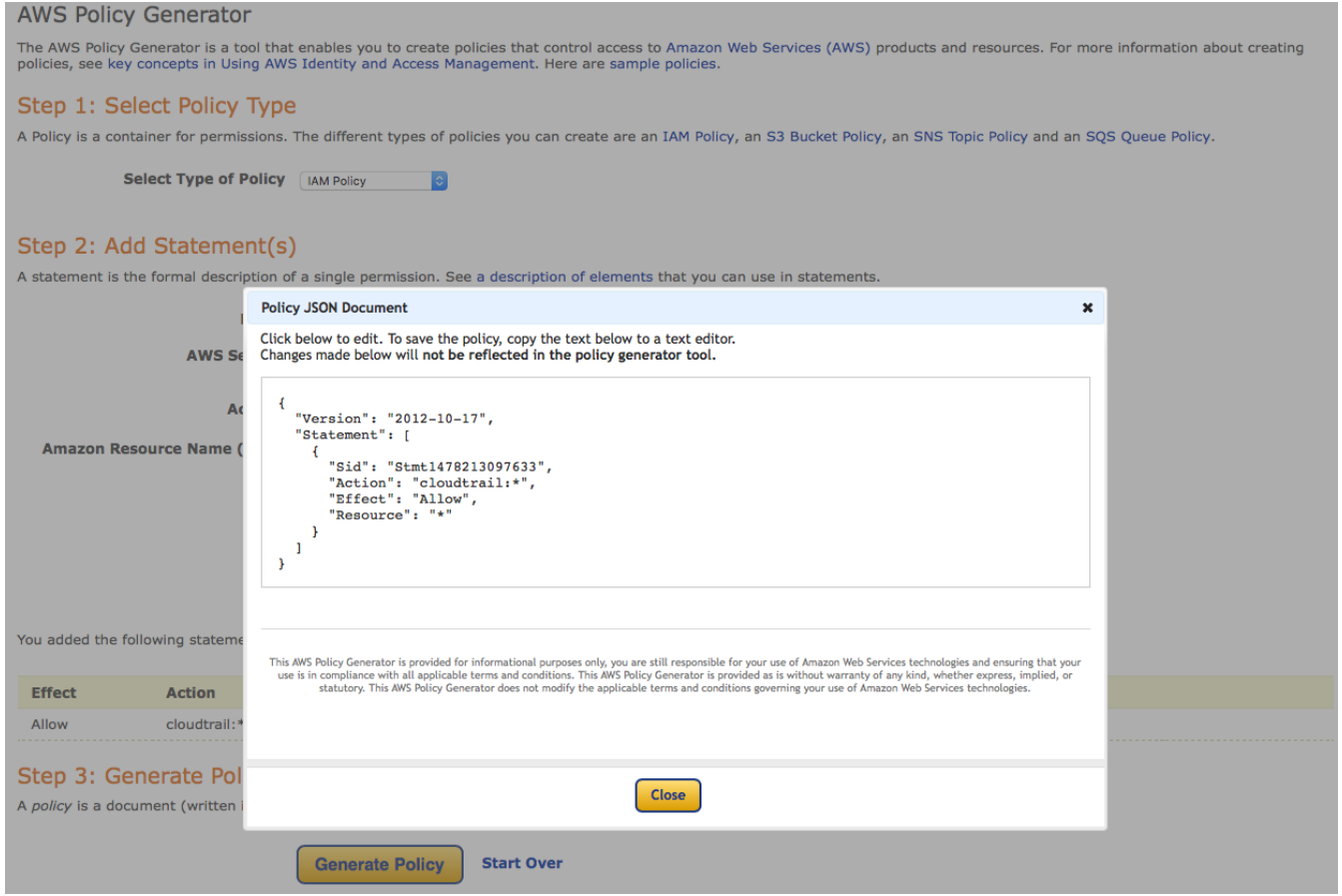
Add Statement

Step 3: Generate Policy

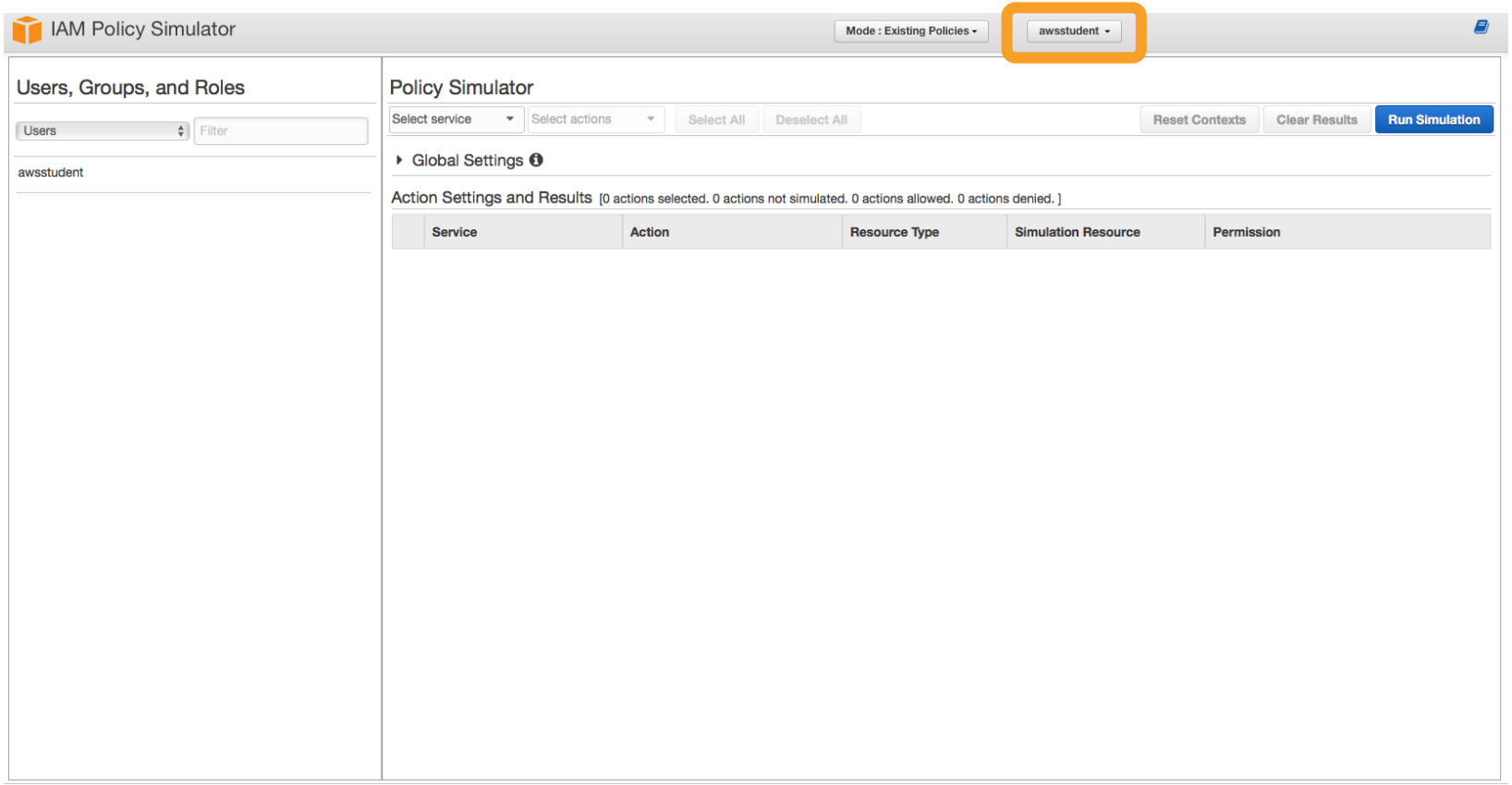
A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.

Add one or more statements above to generate a policy.

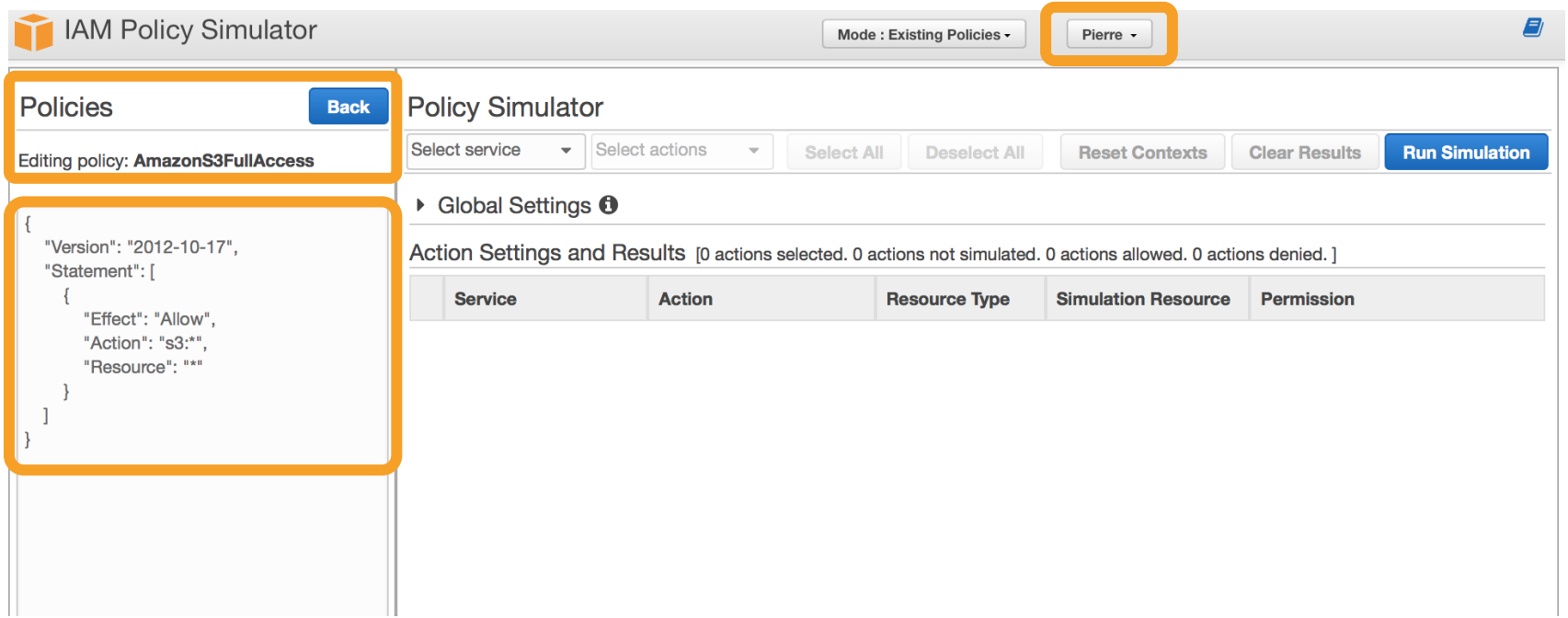
AWS IAM - Policy Generator



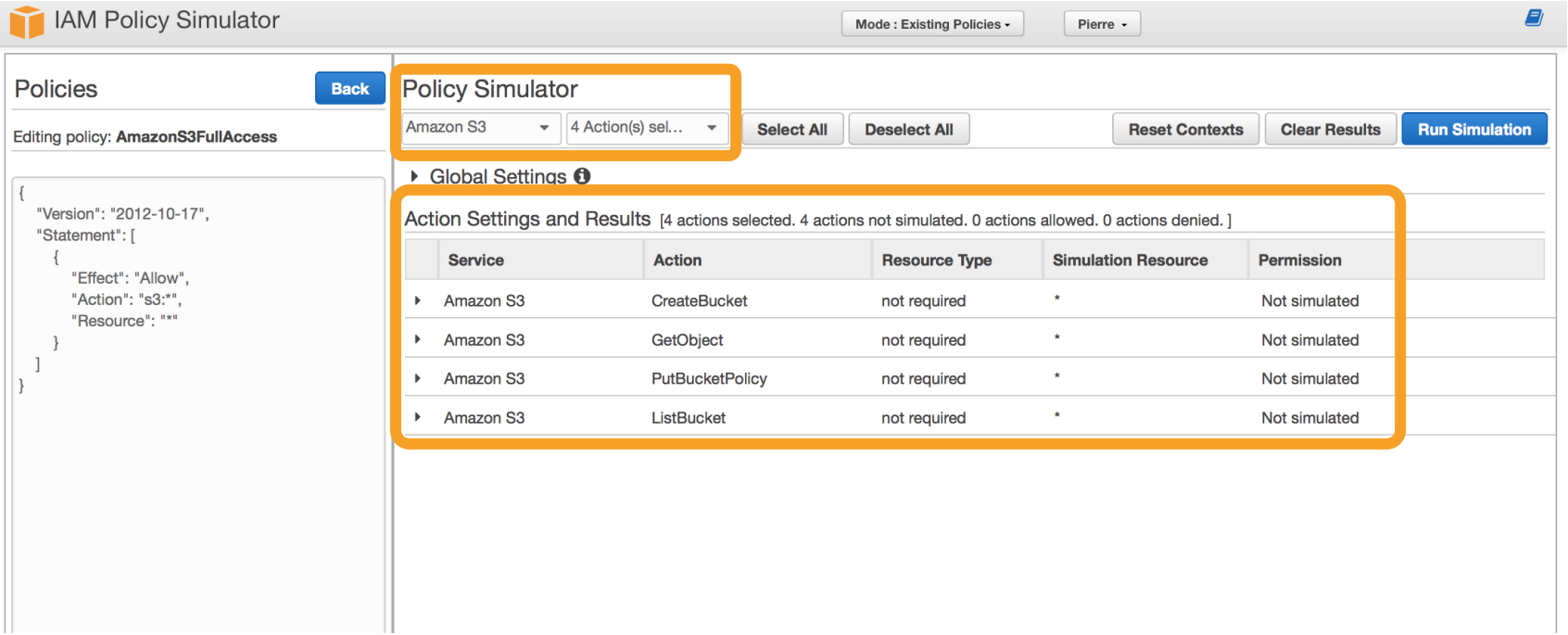
AWS IAM - Policy Simulator



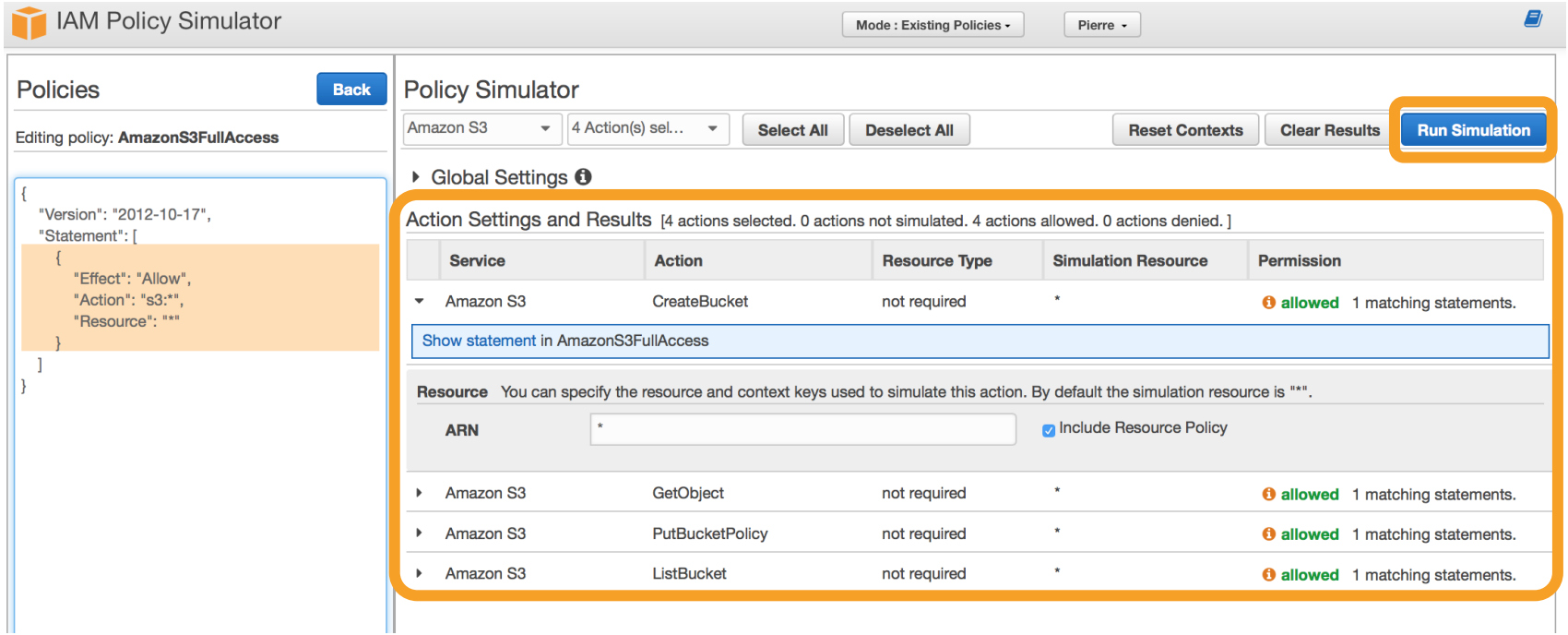
AWS IAM - Policy Simulator



AWS IAM - Policy Simulator



AWS IAM - Policy Simulator



AWS IAM - Best Practices

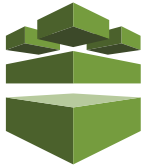
- Reduce or remove use of root
- Create Individual IAM Users
- Configure a strong password policy
- Enable MFA for privileged users
- Grant least privilege
- Manage permissions with groups
- Restrict privileged access further with conditions
- Rotate security credentials regularly
- Use IAM roles to share access
- Use IAM roles for Amazon EC2 instances
- Monitor activity

DEMO

Services for todays Webinar

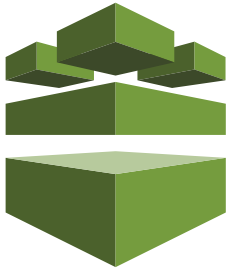
AWS Identity and Access Management (IAM)

AWS Config Rules



AWS CloudTrail

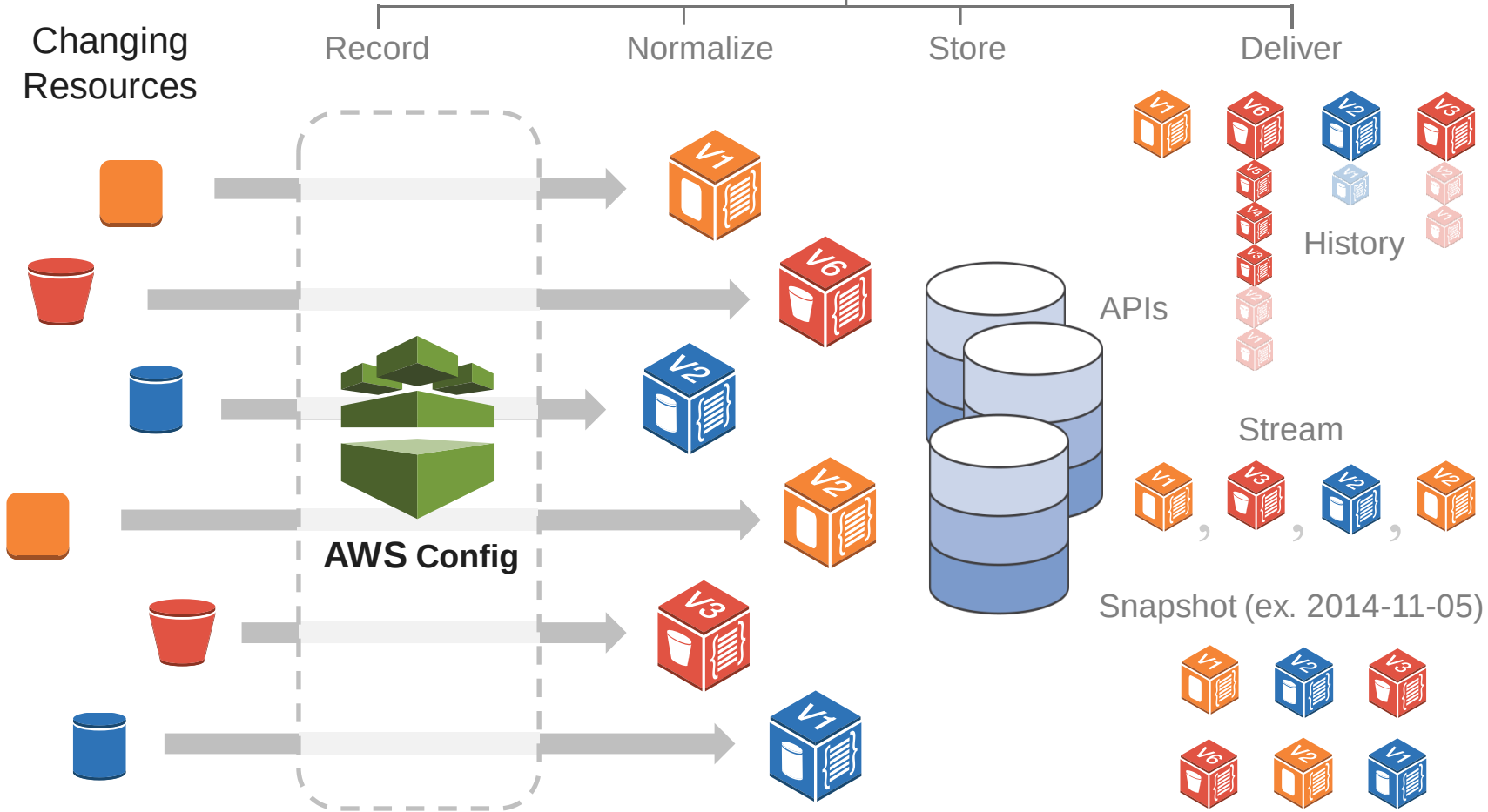
AWS Config Rules



AWS Config

AWS Config is a fully managed service that provides you with an inventory of your AWS resources, lets you audit the resource configuration history and notifies you of resource configuration changes.

AWS Config - Overview



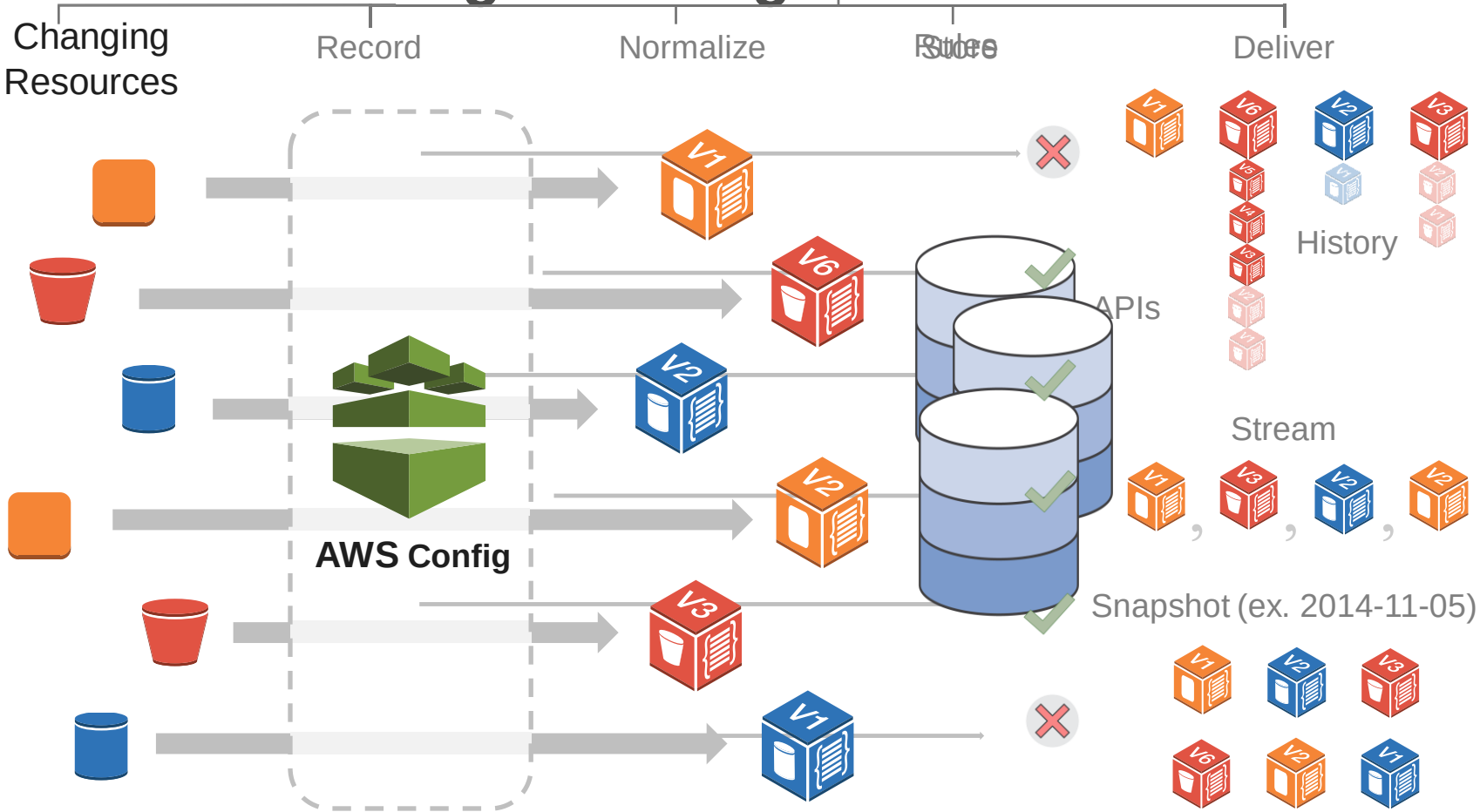
AWS Config Rules

- Set up rules to check configuration changes recorded
- Use pre-built rules provided by AWS
- Author custom rules using AWS Lambda
- Invoked automatically for continuous assessment
- Use dashboard for visualizing compliance and identifying offending changes

AWS Config Rules - Samples

Compliance guideline	Action if noncompliance
All EBS volumes should be encrypted	Encrypt volumes
Instances must be within a VPC	Terminate instance
Instances must be tagged with environment type	Notify developer (email, page, Amazon SNS)

AWS Config & Config Rules - Overview



Relationships

Bi-directional map of dependencies automatically assigned

Change to a resource propagates to create Configuration Items for related resources

Example: Elastic IP 10.12.12.120 and EC2 instance i-123a3d9 are "associated with" each other

AWS Config Rules

A rule that checks the validity of configurations recorded

- AWS managed rules
  - Defined by AWS
  - Require minimal (or no) configuration
  - Rules are managed by AWS
- Customer managed rules
  - Authored by you using AWS Lambda
  - Rules execute in your account
  - You maintain the rule

AWS Config Rules - Managed Rules

« ‹ **Viewing 9 of 19 AWS managed rules** › »

s3-bucket-logging-enabled

Checks whether logging is enabled for your S3 buckets.

s3-bucket-versioning-enabled

Checks whether versioning is enabled for your S3 buckets.

approved-amis-by-id

Checks whether running instances are using specified AMIs. Specify a list of approved AMI IDs. Running instances with AMIs that are not on this list are noncompliant.

approved-amis-by-tag

Checks whether running instances are using specified AMIs. Specify the tags that identify the AMIs. Running instances with AMIs that don't have at least one of the specified tags are noncompliant.

db-instance-backup-enabled

Checks whether RDS DB instances have backups enabled. Optionally, the rule checks the backup retention period and the backup window.

desired-instance-type

Checks whether your EC2 instances are of the specified instance types.

ebs-optimized-instance

Checks whether EBS optimization is enabled for your EC2 instances that can be EBS-optimized.

iam-password-policy

Checks whether the account password policy for IAM users meets the specified requirements.

rds-multi-az-support

Checks whether high availability is enabled for your RDS DB instances.

AWS Config Rules - Triggers

- Triggered by changes: Rules invoked when relevant resources change

  Scoped by changes to:

  - Tag key/value
  - Resource types
  - Specific resource ID

  e.g. EBS volumes tagged “Production” should be attached to EC2 instances

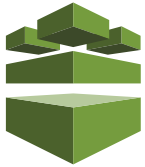
- Triggered periodically: Rules invoked at specified frequency

  e.g. Account should have no more than 3 “PCI v3” EC2 instances; every 3 hrs

Services for todays Webinar

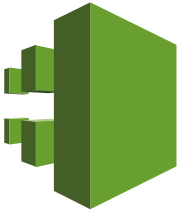
AWS Identity and Access Management (IAM)

AWS Config Rules



AWS CloudTrail

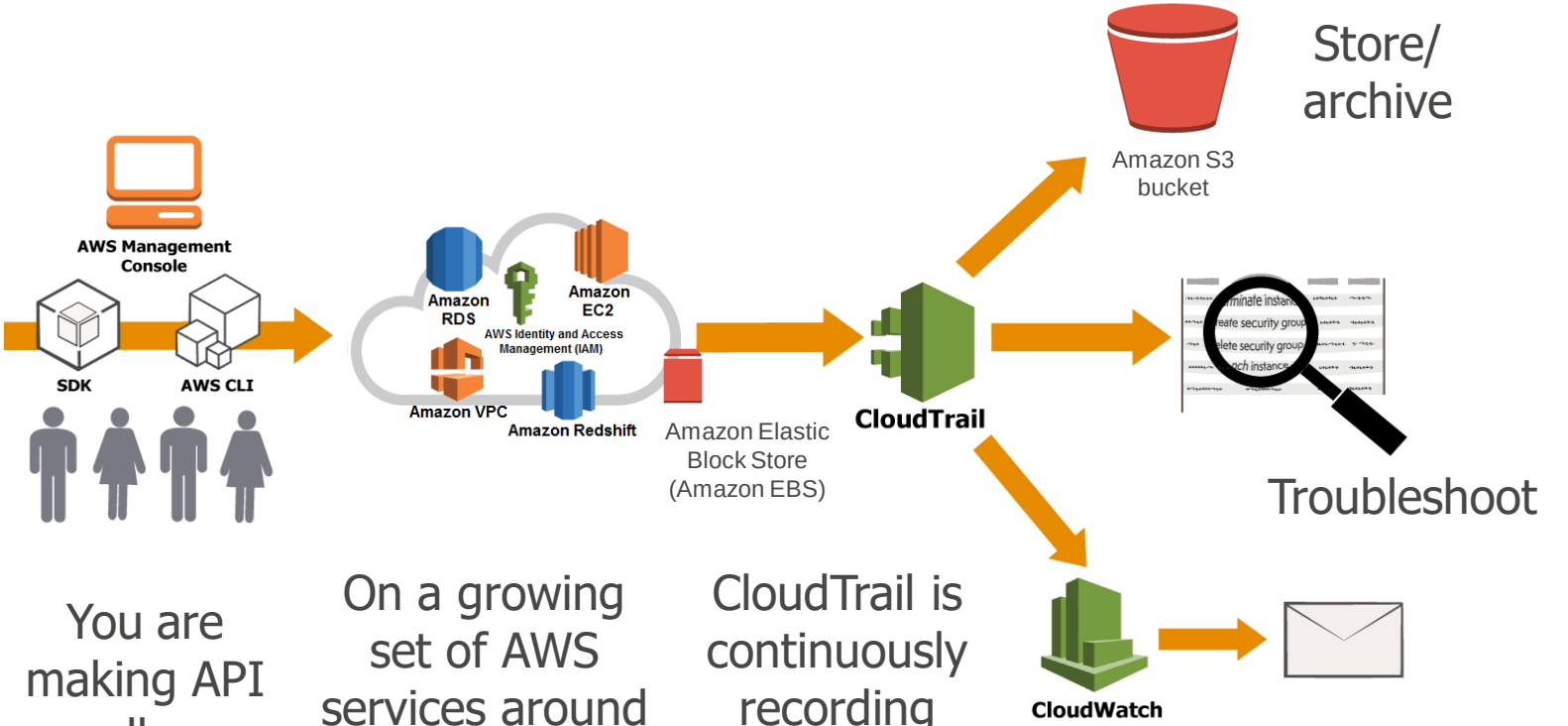
AWS CloudTrail



AWS CloudTrail

AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service

AWS CloudTrail - Overview

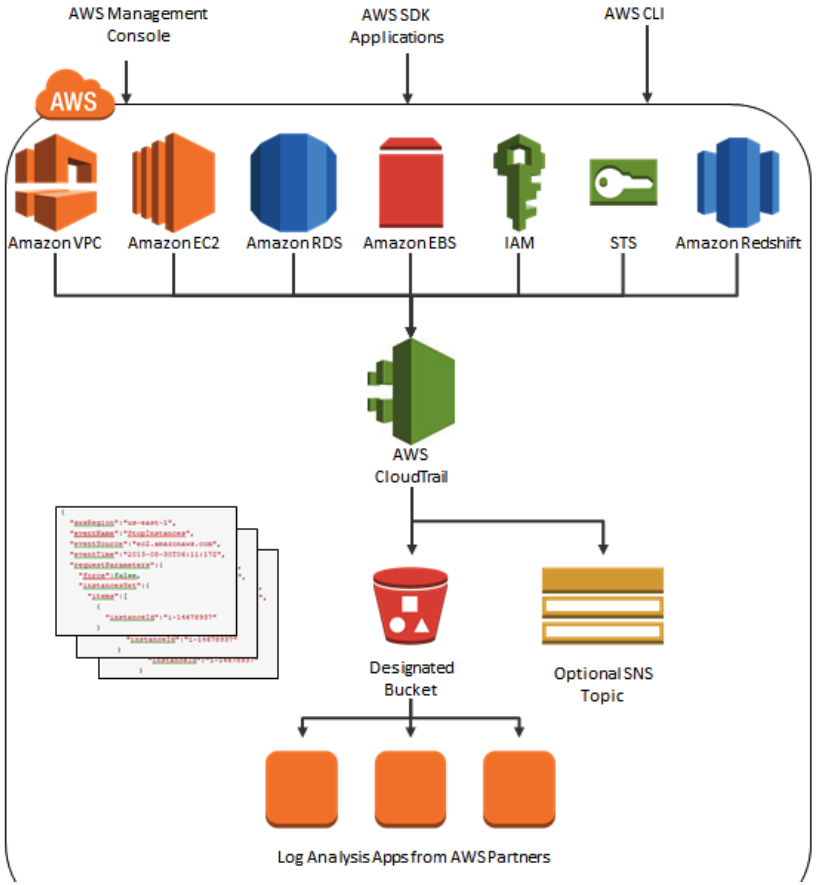


You are making API calls...

On a growing set of AWS services around the world..

CloudTrail is continuously recording API calls

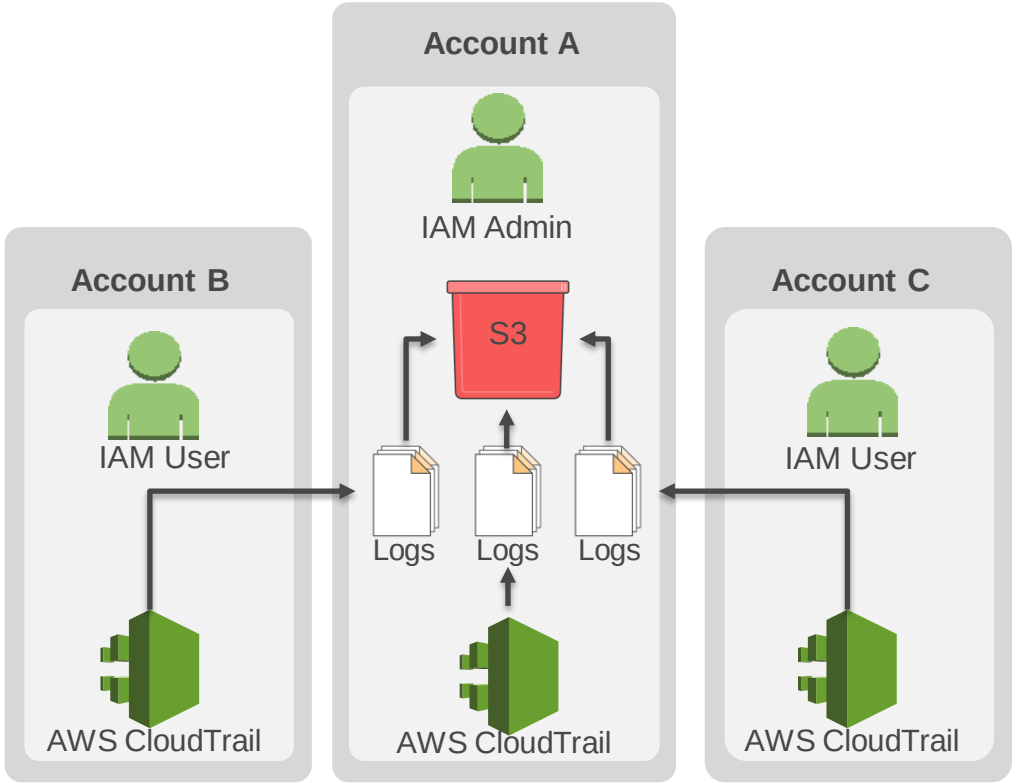
AWS CloudTrail – Helping You



CloudTrail can help you achieve many tasks

- Security analysis
- Track changes to AWS resources, for example VPC security groups and NACLs
- Compliance – log and understand AWS API call history
- Prove that you did not:
  - Use the wrong region
  - Use services you don't want
- Troubleshoot operational issues – quickly identify the most recent changes to your environment

AWS CloudTrail - Cross-Account



CloudTrail can help you achieve many tasks

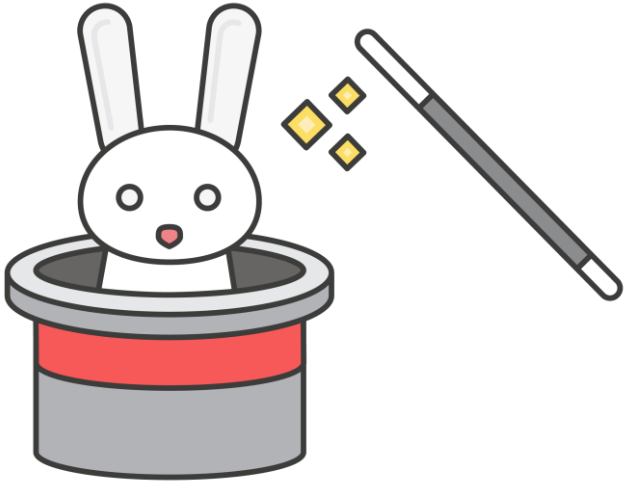
- Accounts can send their trails to a central account
- Central account can then do analytics
- Central account can:
  - Redistribute the trails
  - Grant access to the trails
  - Filter and reformat Trails (to meet privacy requirements)

Services for todays Webinar

AWS Identity and Access Management (IAM)

AWS Config Rules

AWS CloudTrail



Show and Tell

AWS Tools - Summary

Service	Type	Use cases
IAM	Access Control	Manage access to your AWS resources
Config Rules	Continuous evaluations	Best practices, misconfigurations, or actions on changes
CloudTrail	Audit	Audit trail of API activity. Who did what, when and from where

AWS Security and Compliance

Services and tools to aid security **in** the cloud

Security **of** the cloud

amazon web services™

AWS Resources

AWS IAM:
https://aws.amazon.com/IAM

AWS Config:
https://aws.amazon.com/config/

AWS CloudTrail:
https://aws.amazon.com/cloudtrail/

AWS Policy Generator:
https://awspolicygen.s3.amazonaws.com/policygen.html

AWS IAM Policy Simulator:
https://policysim.aws.amazon.com

Thank you!