

Module 3

Security, Identity and Access Management

VIRTUAL

AWSOME DAY

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Certifications and Accreditation



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.



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

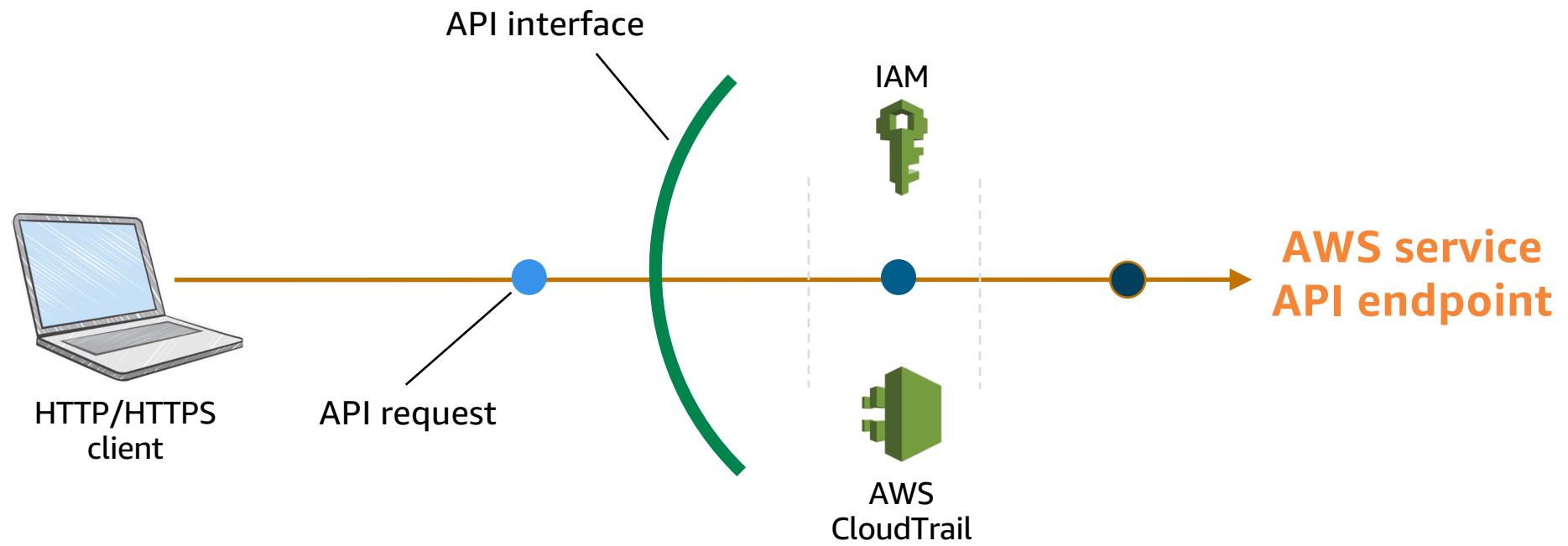
- 24/7 trained security staff
- AWS data centers in nondescript and undisclosed facilities
- Two-factor authentication for authorized staff
- Authorization for data center access



SSL Endpoints

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

API Request Flow



Security Groups

SSL Endpoints

Secure Transmission

Use secure endpoints to establish secure communication sessions (HTTPS).

Security Groups

Instance Firewalls

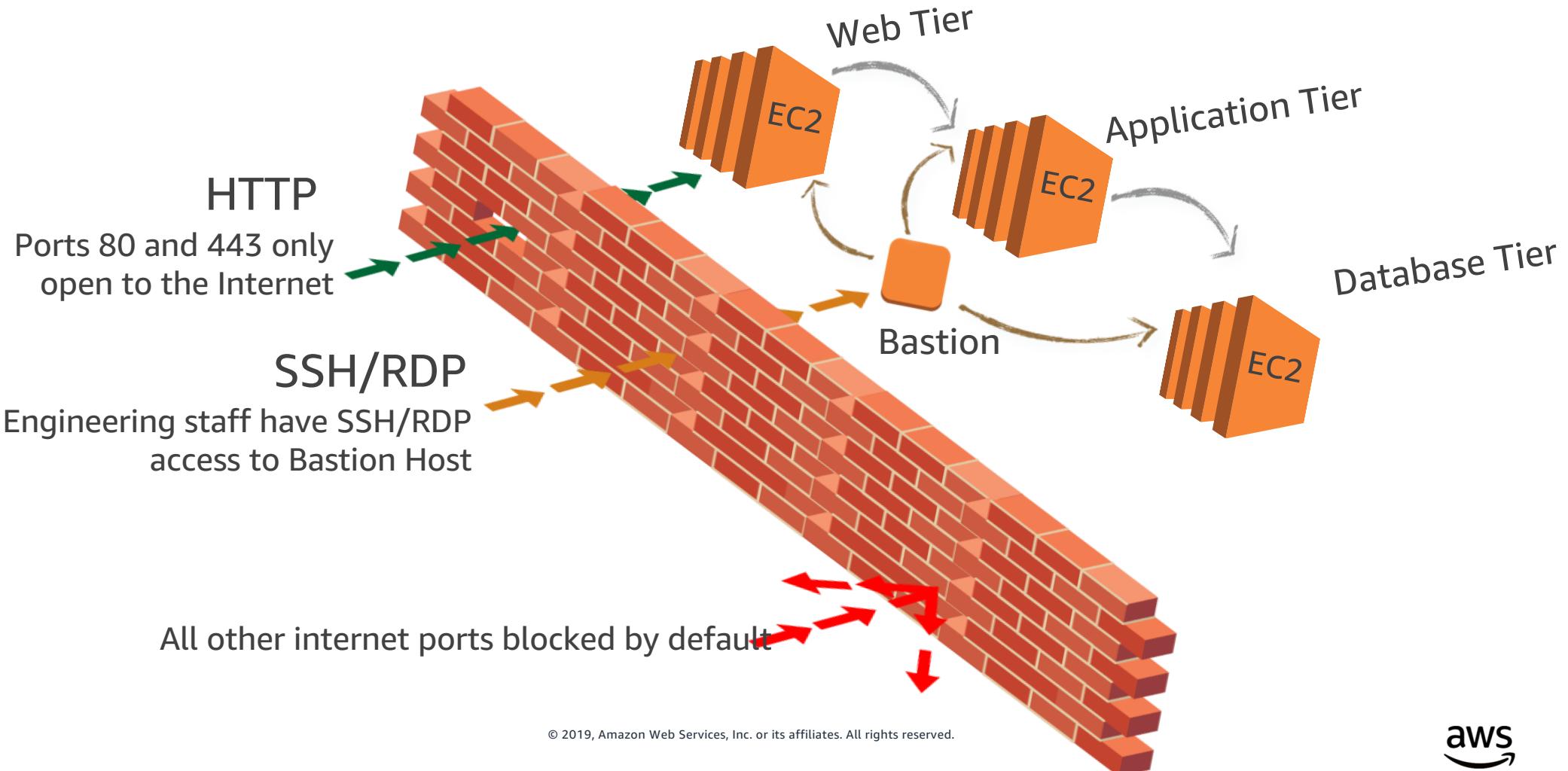
Use security groups to configure firewall rules for instances.

VPC

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.

AWS Multi-Tier Security Groups



Amazon Virtual Private Cloud (VPC)

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

What is IAM? (*Identity and Access Management*)

Securely control access to AWS resources



AWS users

Manage users and their access



Roles

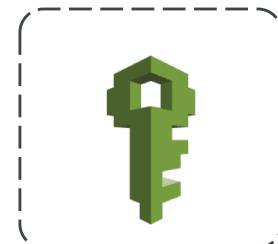
Manage roles and their permissions



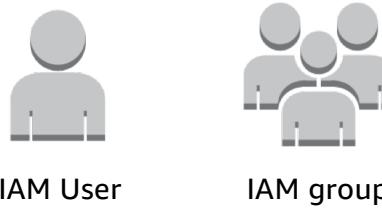
Corp users

Manage federated users and their permissions

AWS IAM Authentication



- Authentication
 - AWS Management Console
 - User Name and Password



Account: [REDACTED]

User Name: [REDACTED]

Password: [REDACTED]

MFA users, enter your code on the next screen.

Sign In



AWS Services Edit

awsstudent@ 9:00 AM Singapore Support

Amazon Web Services

Compute

- ECS Run Containers in the Cloud
- ECD Container Service Run and Manage Docker Containers
- Elastic Beanstalk Run Applications as Web Apps
- Lambda Run Code in Response to Events

Storage & Content Delivery

- S3 Scalable Storage in the Cloud
- CloudFront Global Content Delivery Network
- Elastic File System PREVIEW Managed File System for EC2
- Glacier Archive Storage in the Cloud
- Import/Export Snowball Transfer Data Between Your Premises and AWS
- Storage Gateway Hybrid Storage Integration

Databases

- RDS Fully Managed Relational Database Service
- DynamoDB Managed NoSQL Database
- ElastiCache In-Memory Data Store
- Redshift Fast, Simple, Cost-Effective Data Warehousing
- DMS PREVIEW Managed Database Migration Service

Networking

- VPC Connected Cloud Resources
- Direct Connect Dedicated 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 Metrics Monitoring and Applications
- CloudFormation Create and Manage Resources with Templates
- CloudTrail Log AWS Activity and API Usage
- Config Continuous Monitoring and Changes
- OpsWorks Automate Operations with Chef
- Service Catalog Discover and Provision Products
- Trusted Advisor Optimize Performance and Security

Security & Identity

- Identity & Access Management Manage User Access and Encryption Keys
- CloudHSM Host and Manage Active Directory
- Inspector PREVIEW Assess Application Security
- WAF Filter Malicious Web Traffic
- Certificate Manager Renew, Manage, and Deploy SSL/TLS Certificates

Analytics

- EMR Build Big Data Framework
- Data Pipeline Create and Run Data-Driven Workflows
- Elasticsearch Service Run and Scale Elasticsearch Clusters
- Kinesis Real-Time Data Processing and Real-Time Streaming Data
- Machine Learning Build Smart Applications Quickly and Easily

Internet of Things

- AWS IoT Connect Devices to the Cloud

Mobile Services

- Mobile Hub Build, Test, and Monitor Mobile Apps
- Cognito User Identity and App Data Synchronization
- Device Farm Test Android, iOS, and WebGL 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 Live Video Application Streaming
- CloudSearch Managed Search Service
- Elastic Transcoder Extract and Reencode Media Transcoding
- SES Email Sending and Receiving Service
- SQS Message Queue Service
- SWF Workflow Service for Coordinating Application Components

Enterprise Applications

- WorkSpaces Secure Remote Desktop Cloud
- WorkDocs Secure Enterprise Storage and Sharing Service
- WorkMail Secure Email and calendaring Service

Resource Groups [Learn more](#)

A resource group is a collection of resources that share one or more tags. Create a group for each project, application, or environment in your account.

[Create a Group](#) [Tag Editor](#)

Additional Resources

[Getting Started](#)

Read our documentation or view our training to learn more about AWS.

[AWS Console Mobile App](#)

Use the AWS mobile app to interact with the AWS Console mobile app, available from Amazon Appstore, Google Play, or iTunes.

[AWS Marketplace](#)

Find and buy software, launch with 1-Click and pay by the hour.

[AWS re:Invent Announcements](#)

Explore the next generation of AWS cloud capabilities. See what's new

Service Health

All services operating normally.

Updated: Jan 28 2016 14:59:02 GMT+0800

[Service Health Dashboard](#)

Feedback English

© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

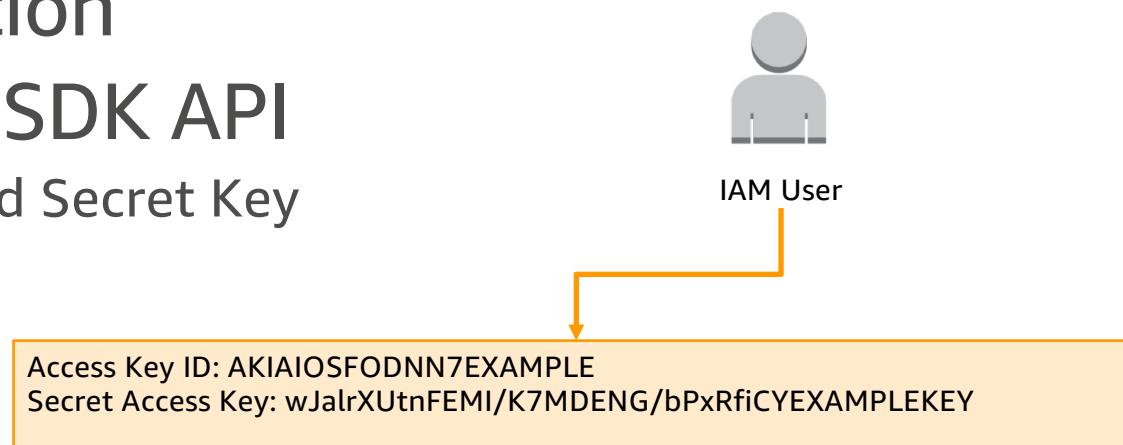
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.



AWS IAM Authentication



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



AWS CLI

```
:~ $ aws configure
AWS Access Key ID [*****022A]:
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.



IAM User



IAM Group



IAM Roles

AWS IAM Policy Elements

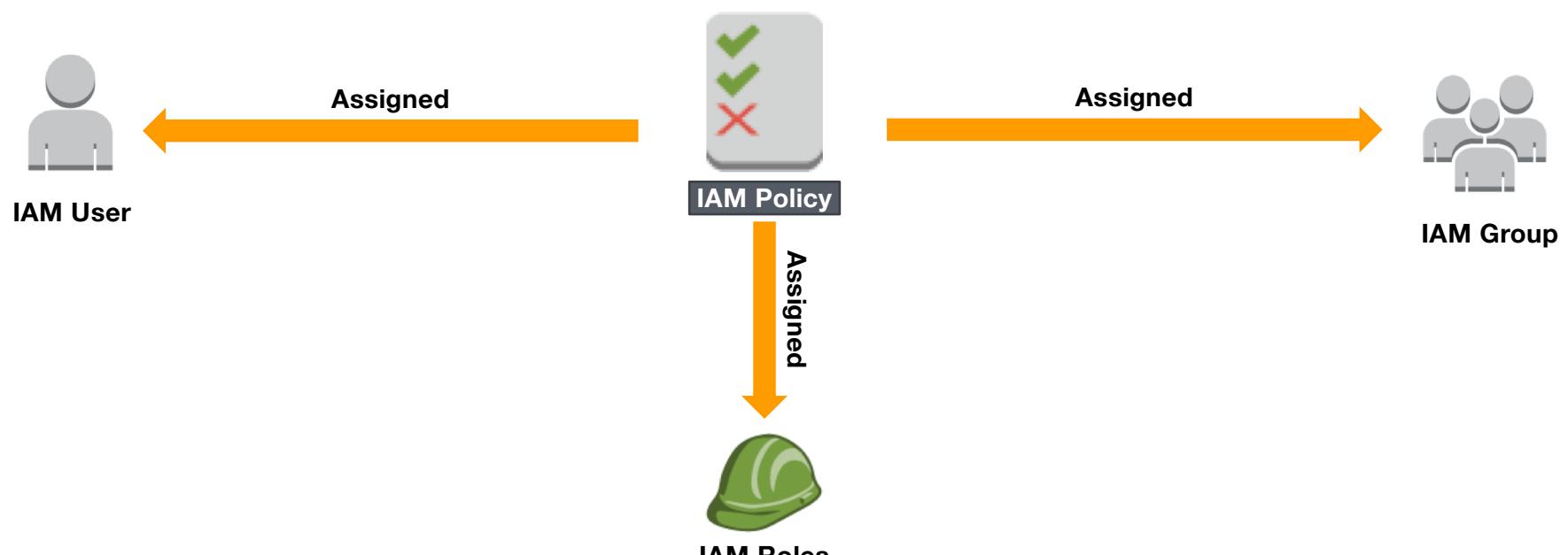
```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "Stmt1453690971587",  
            "Action": [  
                "ec2:Describe*",  
                "ec2:StartInstances",  
                "ec2:StopInstances"  
            ],  
            "Effect": "Allow",  
            "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



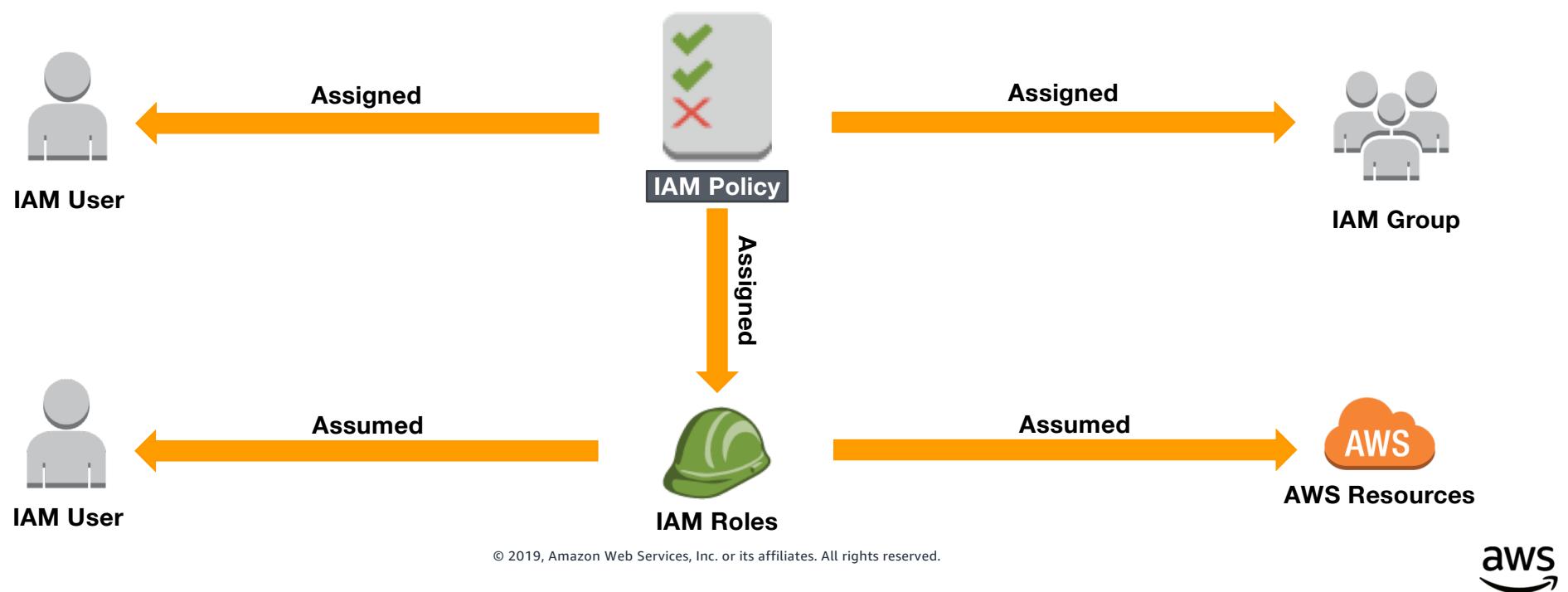
AWS IAM Policy Assignment



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.



AWS IAM Policy Assignment



Example: Application Access to AWS Resources

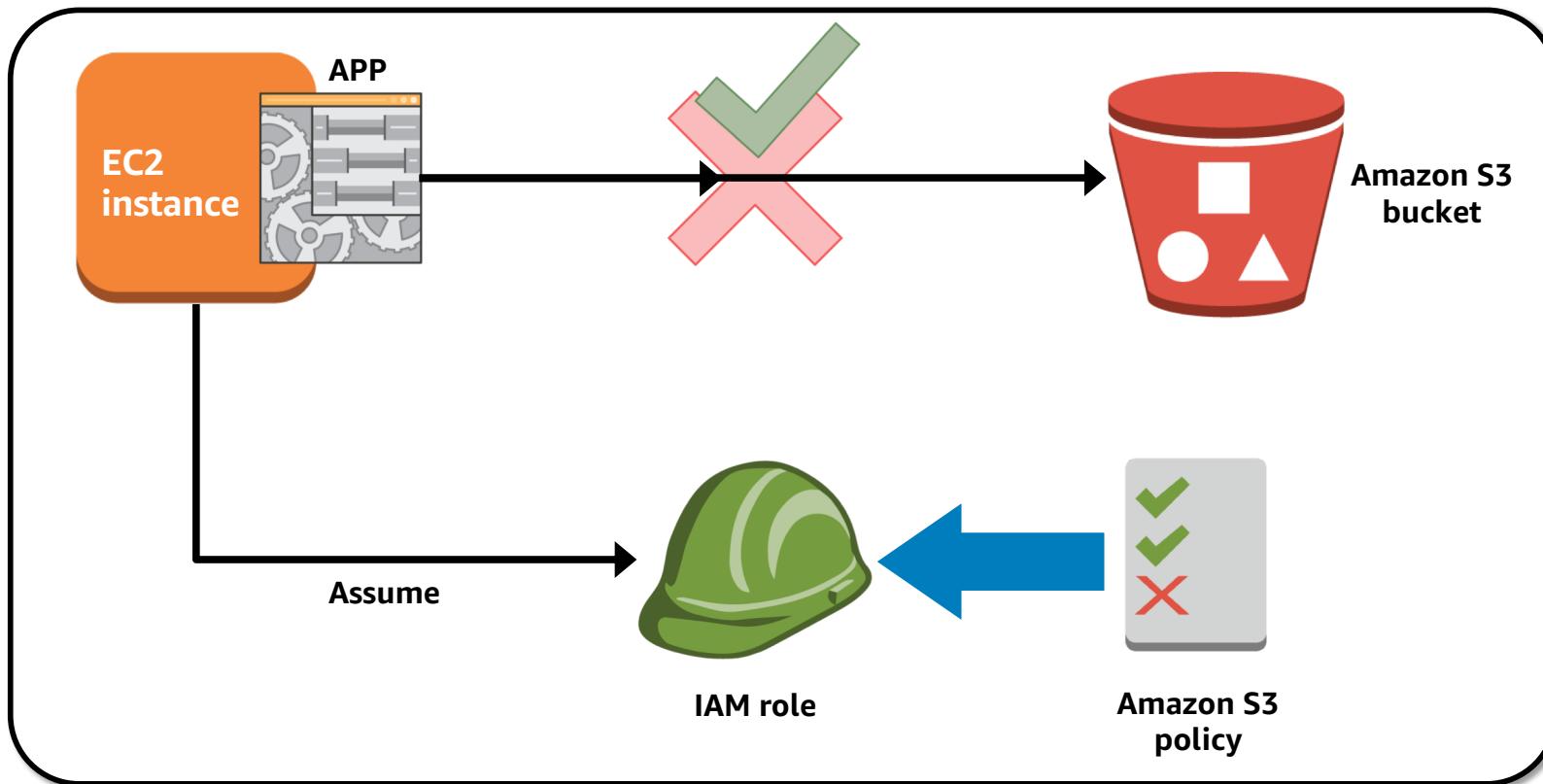


- Python application hosted on an Amazon EC2 Instance needs to interact with Amazon S3.
- AWS credentials are required:
 - ~~Option 1: Store AWS Credentials on the Amazon EC2 instance.~~
 - Option 2: Securely distribute AWS credentials to AWS Services and Applications.

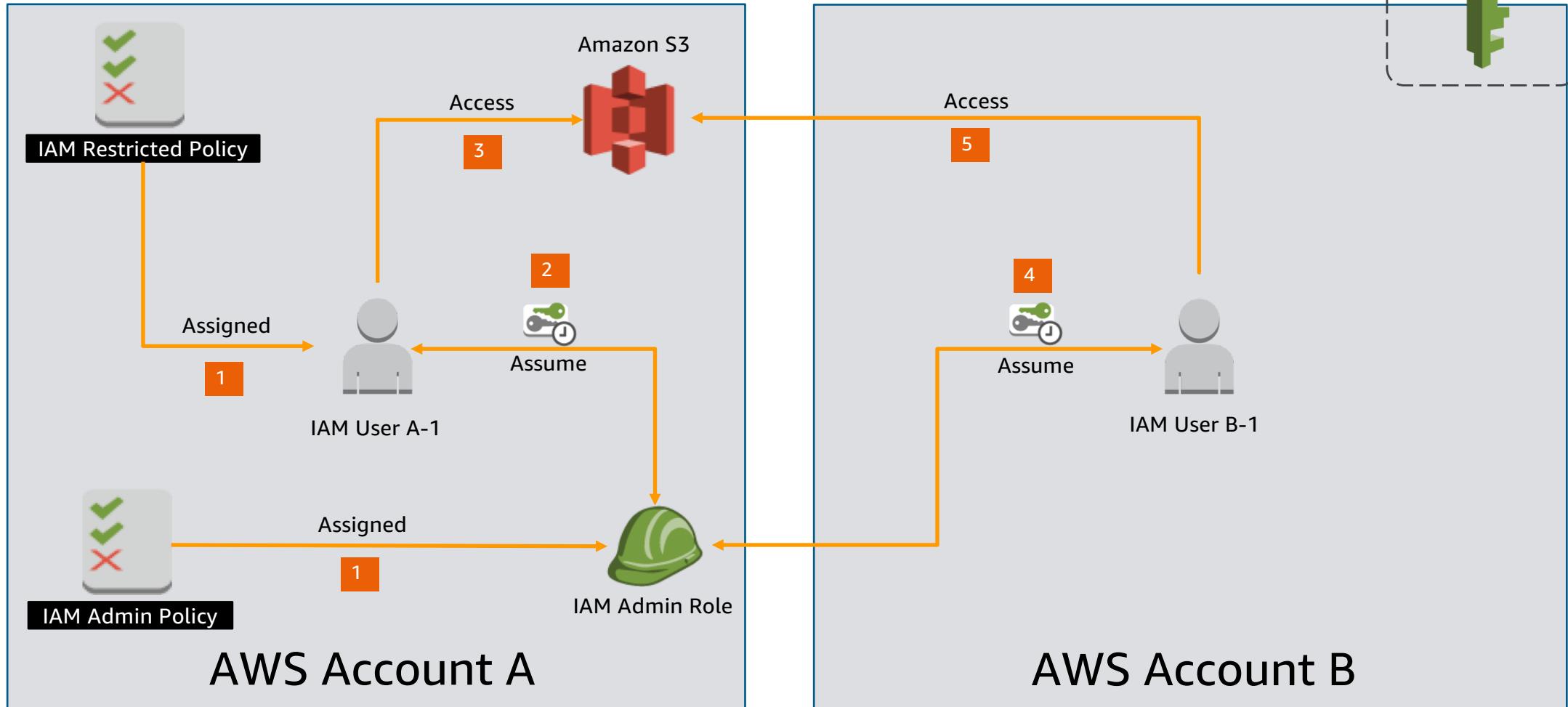


IAM Roles

Using role for Temporary Security Credentials



AWS IAM Roles – Assume Role



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.



IAM Best Practices

- Delete AWS root account access keys
- Activate multi-factor authentication (MFA)
- Only give IAM users permissions they need
- Use roles for applications
- Rotate credentials regularly
- Remove unnecessary users and credentials
- Monitor activity in your AWS account
- ...And more