Module 3

Security, Identity and Access Management

VIRTUAL

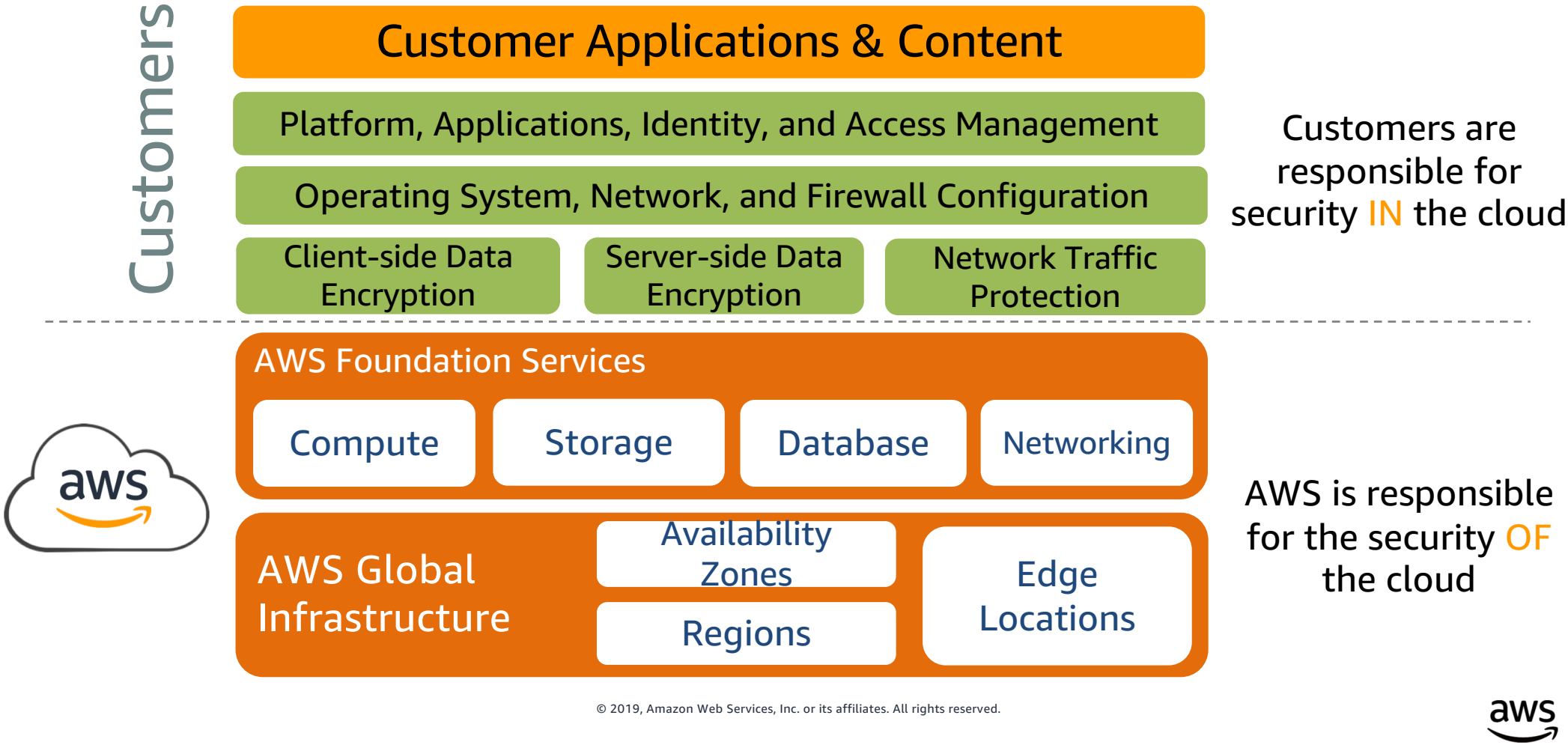
AWSOME DAY

aws

Certifications and Accreditation

aws

AWS Shared Responsibility Model



Physical Security

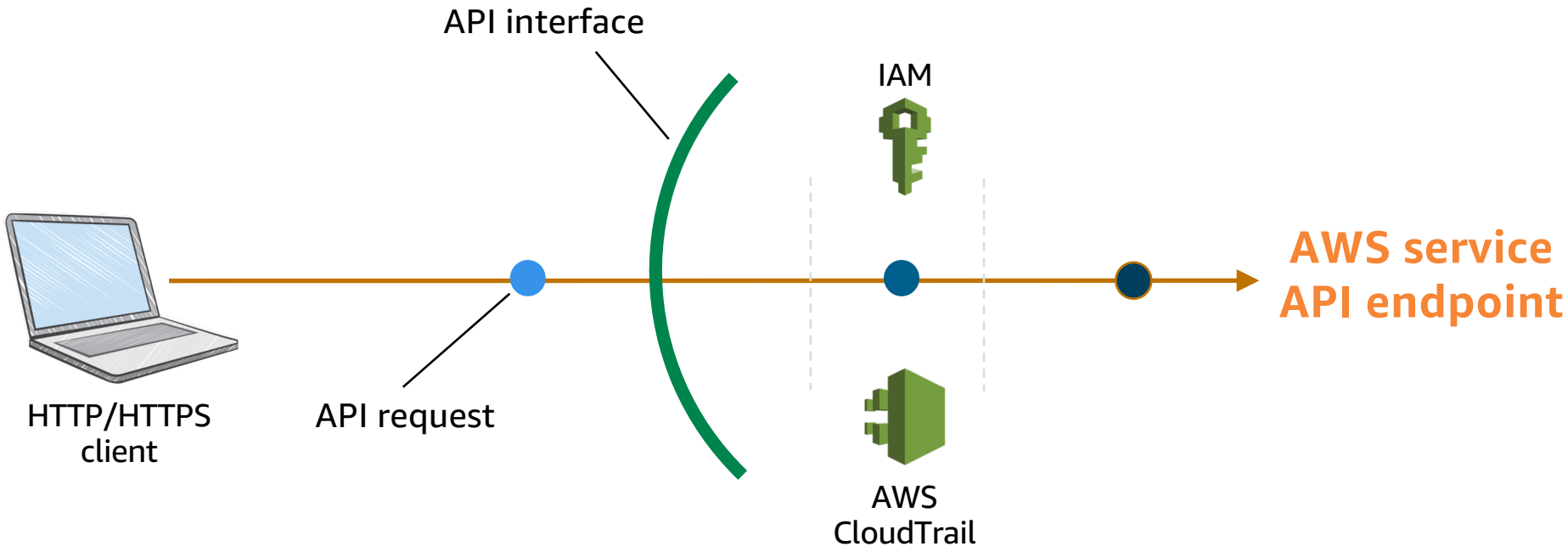
- 24/7 trained security staff
- AWS data centers in nondescript and undisclosed facilities
- Two-factor authentication for authorized staff
- Authorization for data center access

SSL Endpoints

SSL Endpoints	Security Groups	VPC
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.

aws

API Request Flow

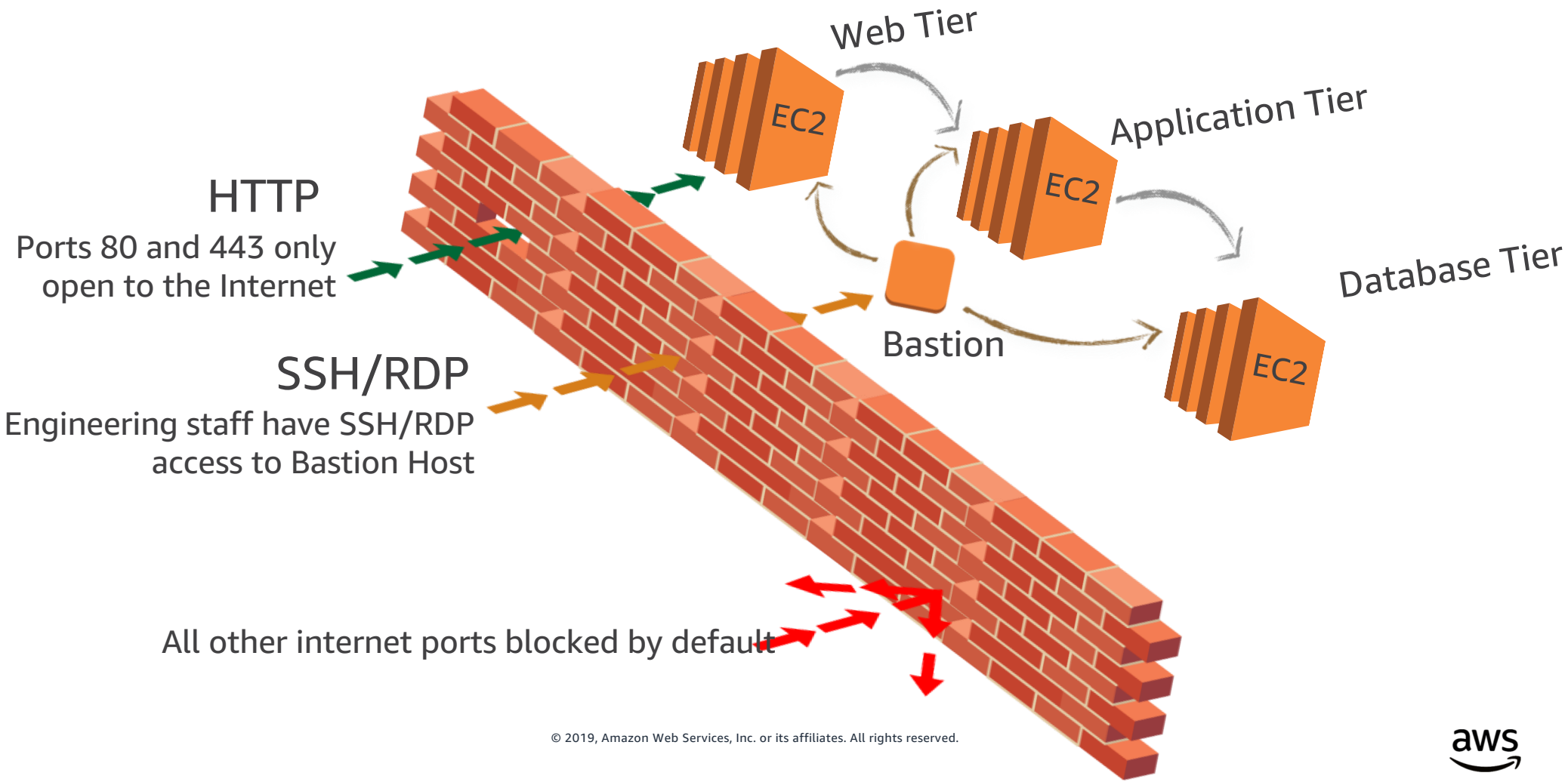


Security Groups

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.

aws

AWS Multi-Tier Security Groups



aws

Amazon Virtual Private Cloud (VPC)

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.

aws

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

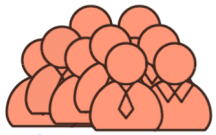
Securely control access to AWS resources

AWS users

Manage users and their access

Roles

Manage roles and their permissions



Corp users

Manage federated users and their permissions

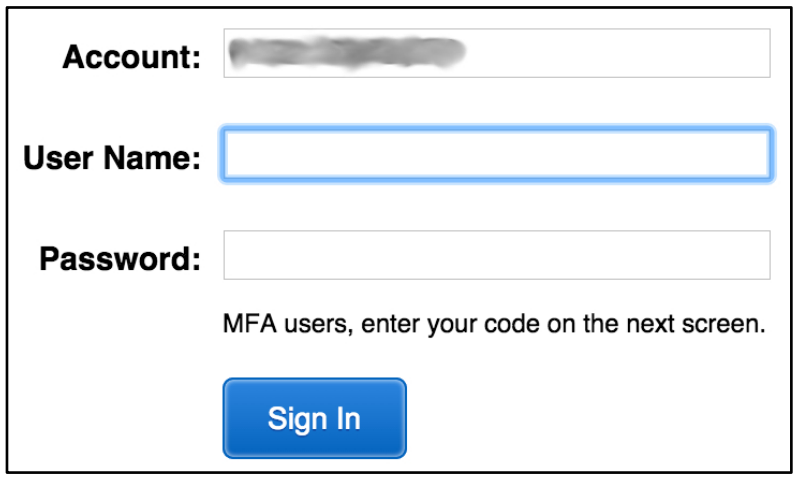
aws

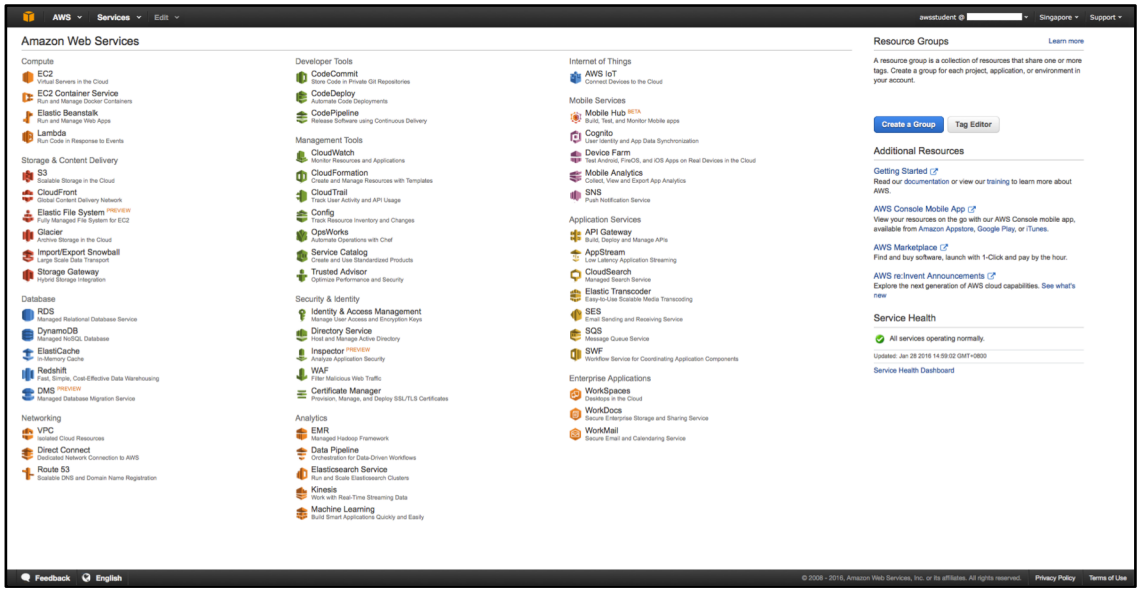
AWS IAM Authentication

- Authentication
- AWS Management Console
  - User Name and Password

IAM User

IAM group





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

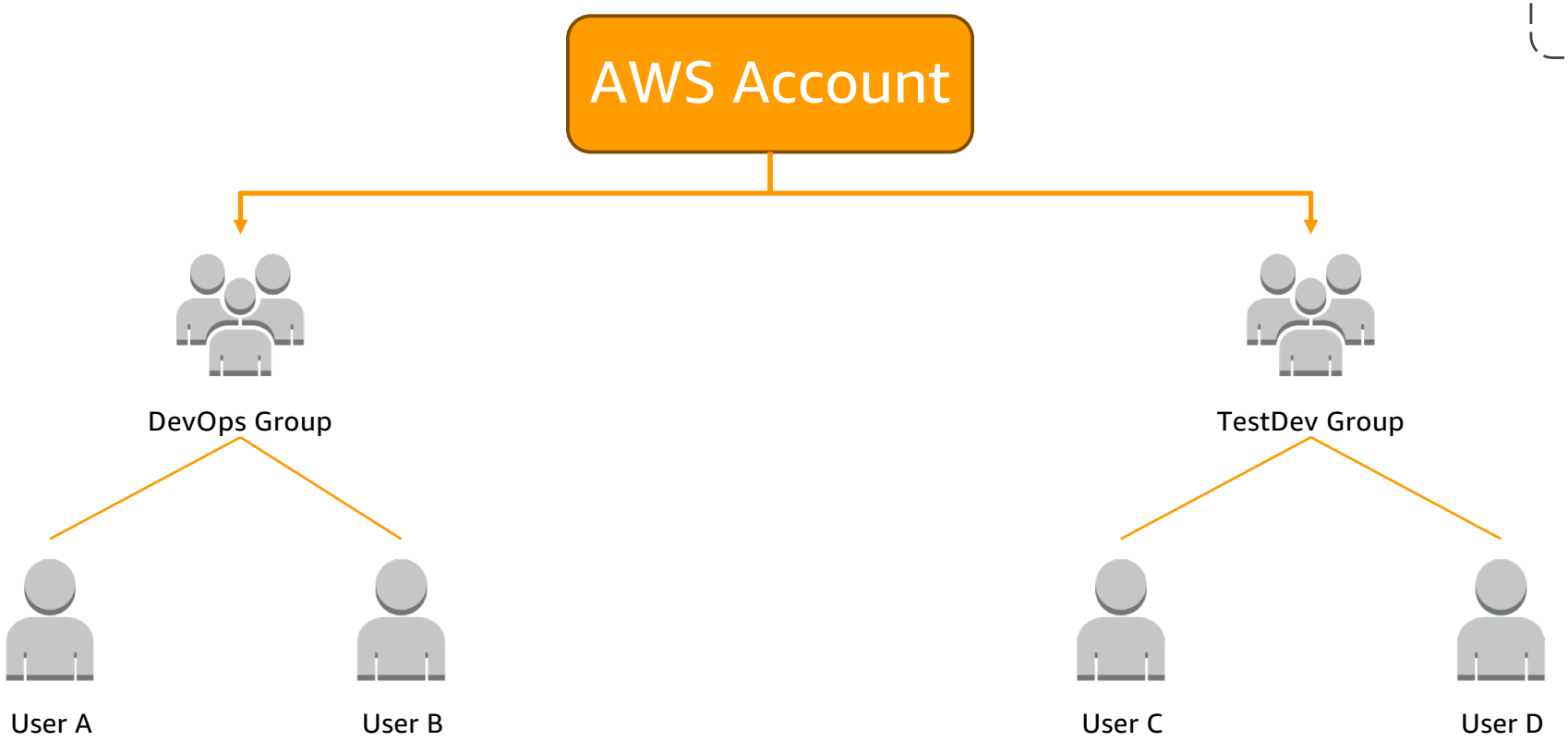
Java

Python

.NET

aws

AWS IAM User Management - Groups



aws

AWS IAM Authorization

Authorization

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

IAM User

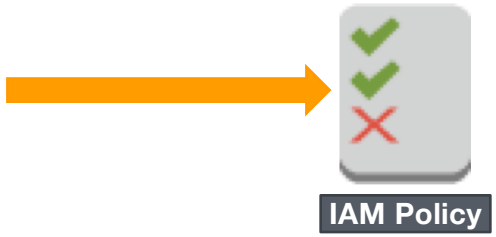
IAM Group

IAM Roles

aws

AWS IAM Policy Elements

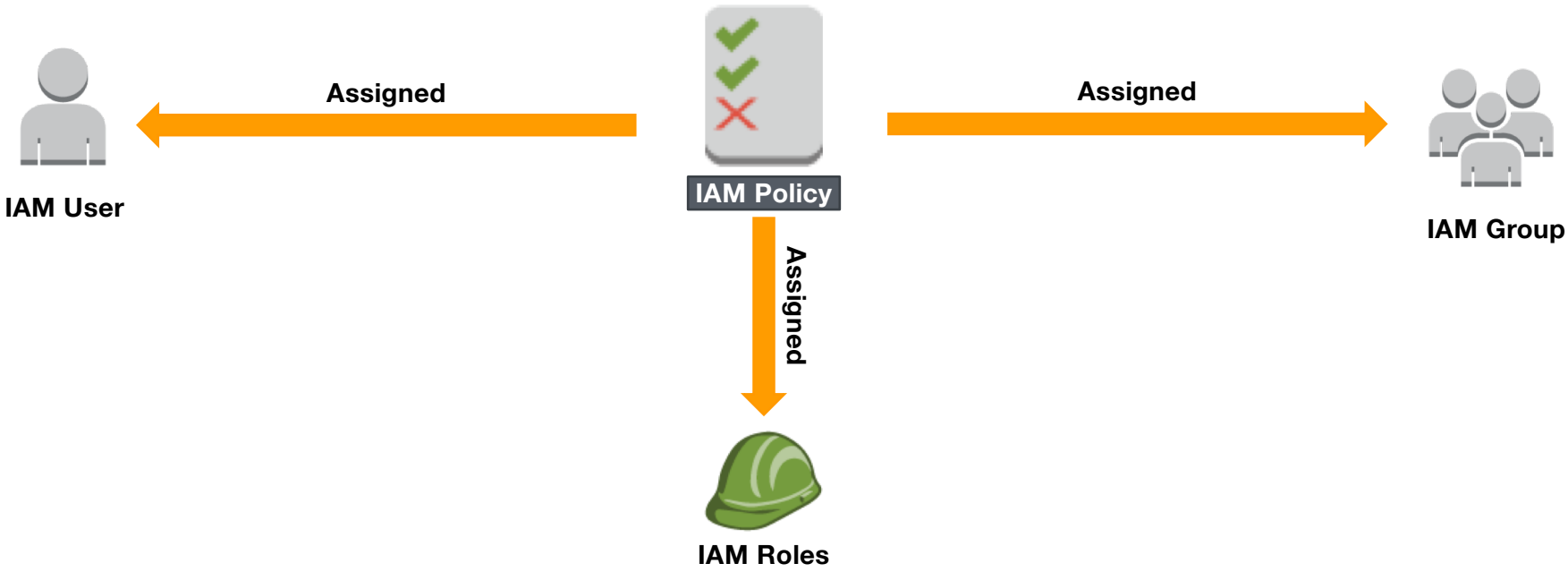
```
{
   "Version": "2012-10-17",
   "Statement": [
     {
       "Sid": "Stmt1453690971587",
            "Action": [
             "ec2:Describe*",
             "ec2:StartInstances",
             "ec2:StopInstances"
             ],
             "Effect": "Allow",
             "Resource": "*",
      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



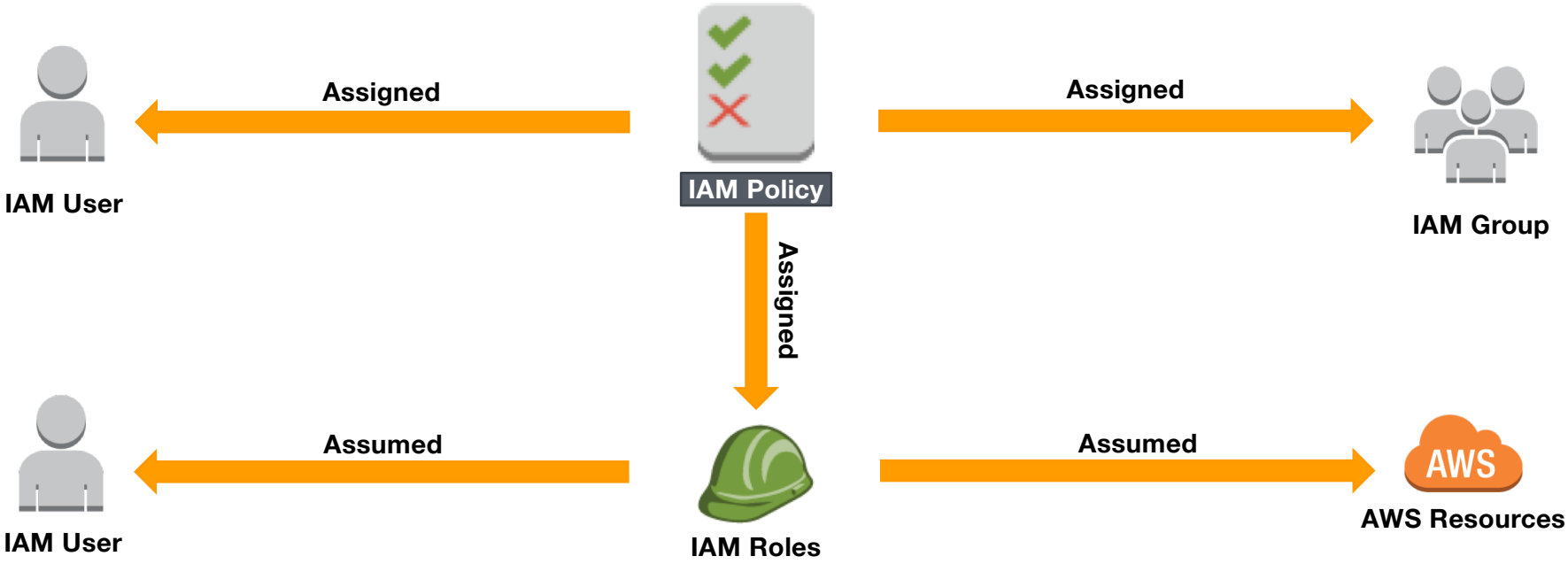
aws

AWS IAM Policy Assignment

AWS IAM Policy Assignment



AWS IAM Policy Assignment



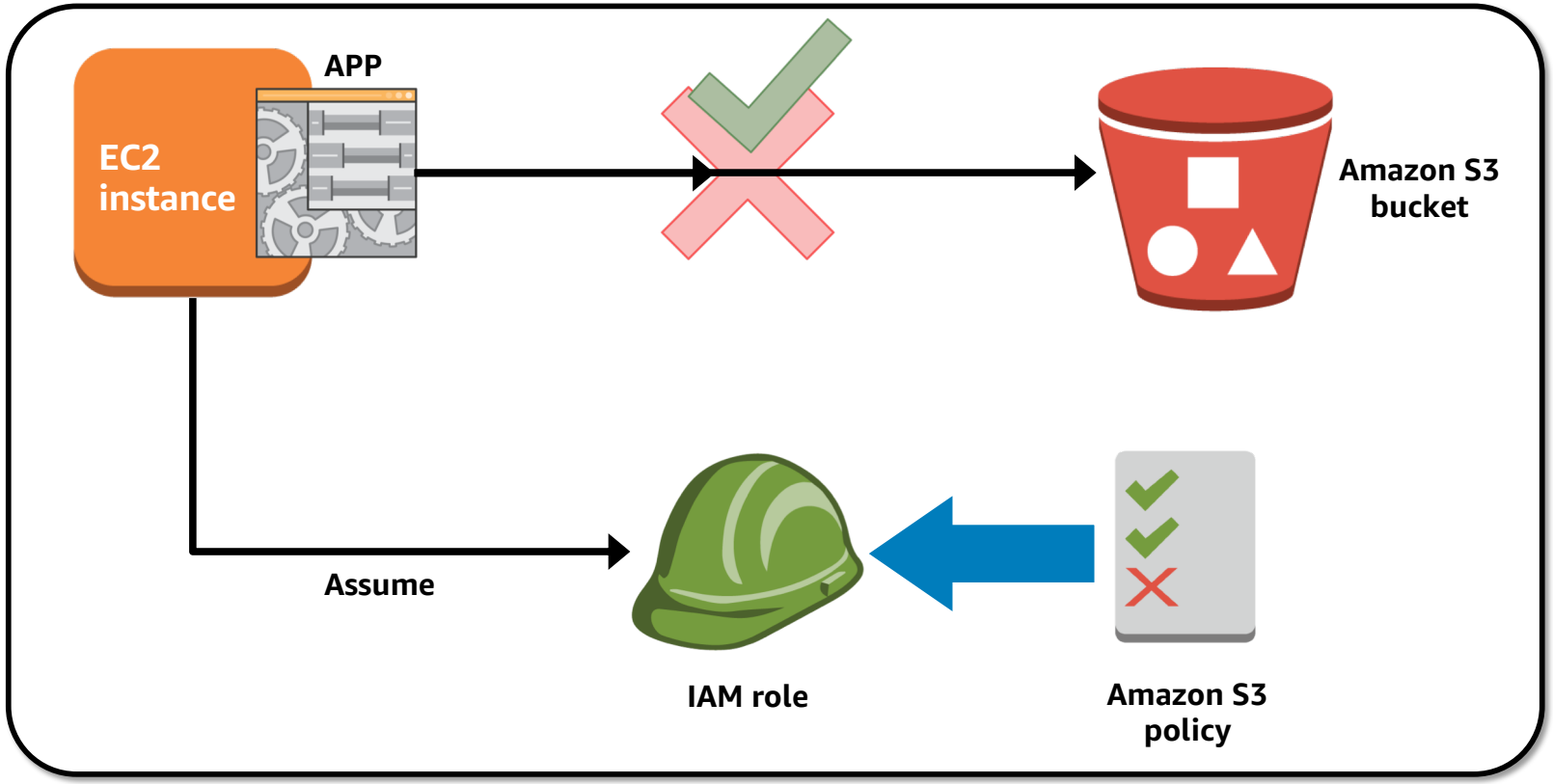
Example: Application Access to AWS Resources

- 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.

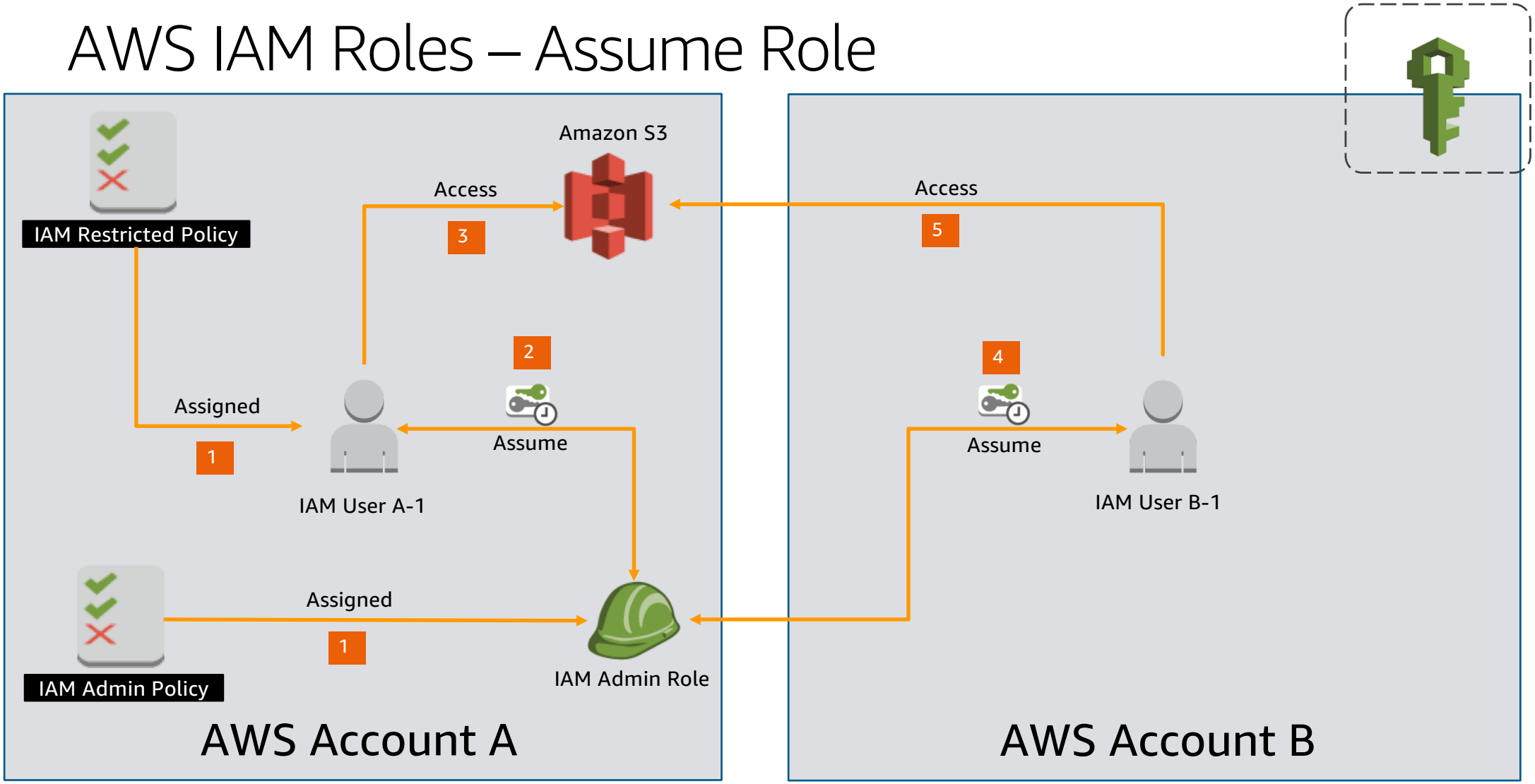
IAM Roles

aws

Using role for Temporary Security Credentials



AWS IAM Roles – Assume Role



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

aws