

# Module 4: Secure your cloud applications

Navjot Singh  
Technical Trainer  
AWS



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Secure your infrastructure

# Security is our top priority



Designed for security



Constantly monitored



Highly automated



Highly available



Highly accredited

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



## Security of the cloud

- Hosts, network, software, facilities
- Protection of the AWS global infrastructure is top priority
- Availability of third-party audit reports

AWS

### Foundation services

Compute

Storage

Database

Network

### AWS global infrastructure

Availability zones

Regions

Edge locations

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



# Security in the cloud

Customer

Customer data

Platform, applications, identity & access management

Operating system, network & firewall configuration

Client-side data encryption &  
Data integrity authentication

Server-side encryption  
(File system and/or data)

Network traffic protection  
(Encryption/integrity/identity)

## Considerations

- What you should store
- Which AWS services you should use
- Who has access
- Which region to store in

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



# AWS shared responsibility model

Customer

Customer data

Platform, applications, identity & access management

Operating system, network & firewall configuration

Client-side data encryption &  
Data integrity authentication

Server-side encryption  
(File system and/or data)

Network traffic protection  
(Encryption/integrity/identity)

AWS

## Foundation services

Compute

Storage

Database

Network

AWS global  
infrastructure

Availability zones

Regions

Edge locations

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



# Security, identity, and compliance products

AWS Artifact

AWS Certificate Manager

Amazon Cloud Directory

AWS CloudHSM

Amazon Cognito

AWS Directory Service

AWS Firewall Manager

Amazon GuardDuty

**AWS Identity and Access Management**

**Amazon Inspector**

AWS Key Management Service

Amazon Macie

AWS Organizations

**AWS Shield**

AWS Secrets Manager

AWS Single Sign-On

AWS WAF

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



## Manage authentication and authorization

# AWS Identity and Access Management (IAM)

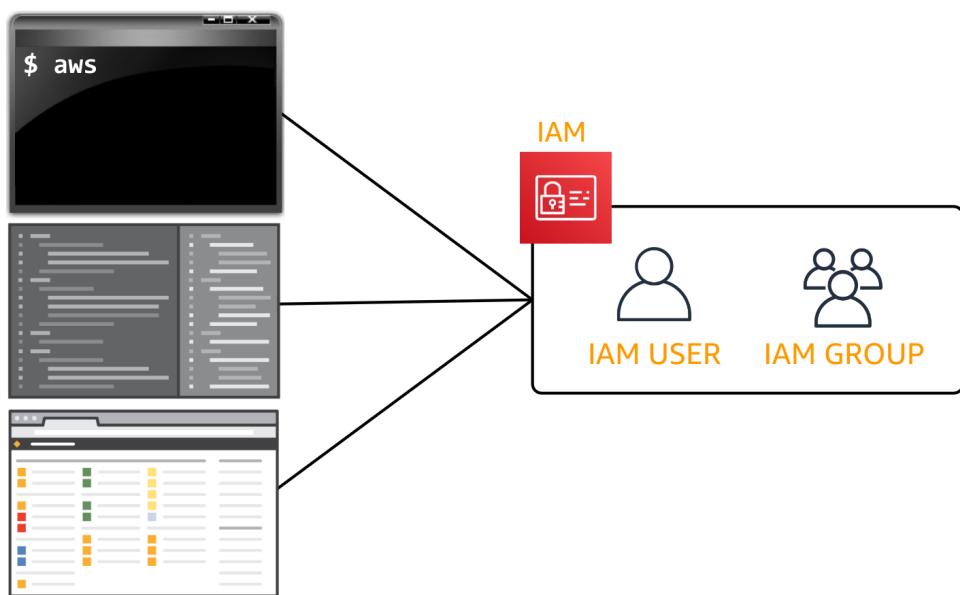


© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



## Authentication: Who are you?

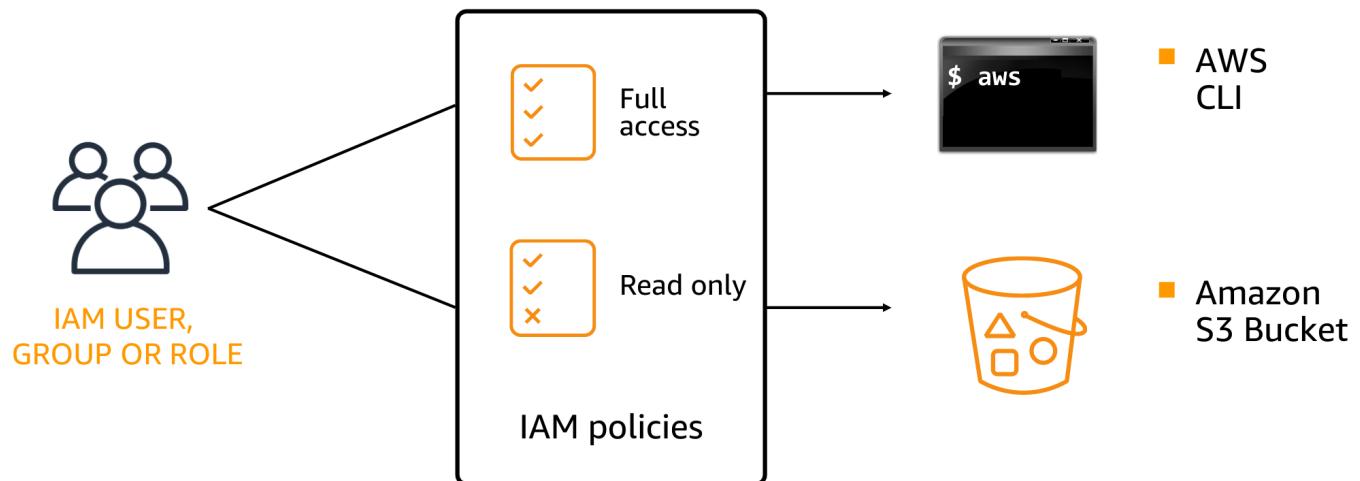
- AWS CLI
- AWS SDKs
- AWS Management Console



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



# Authorization: What can you do?



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



## IAM roles



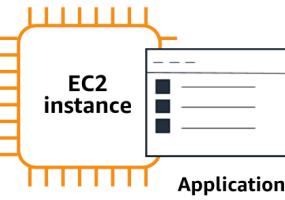
IAM ROLE

- IAM users, applications, and services may assume IAM roles
- Roles uses an IAM policy for permissions

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



# Using roles for temporary security credentials

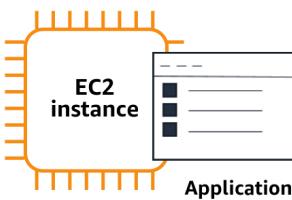


Amazon  
S3 bucket

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws | intel

# Using roles for temporary security credentials

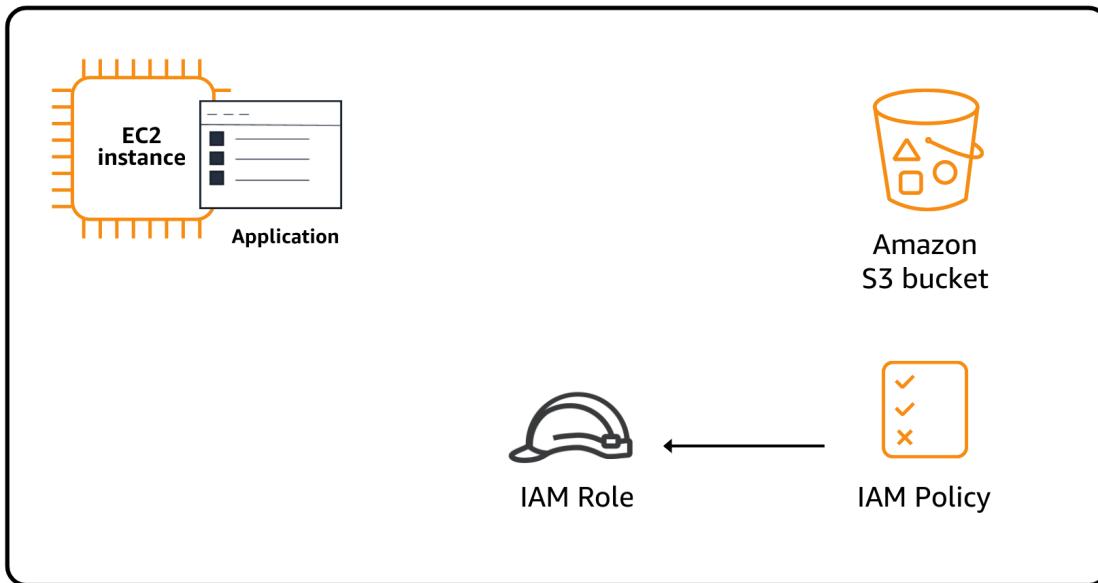


Amazon  
S3 bucket

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws | intel

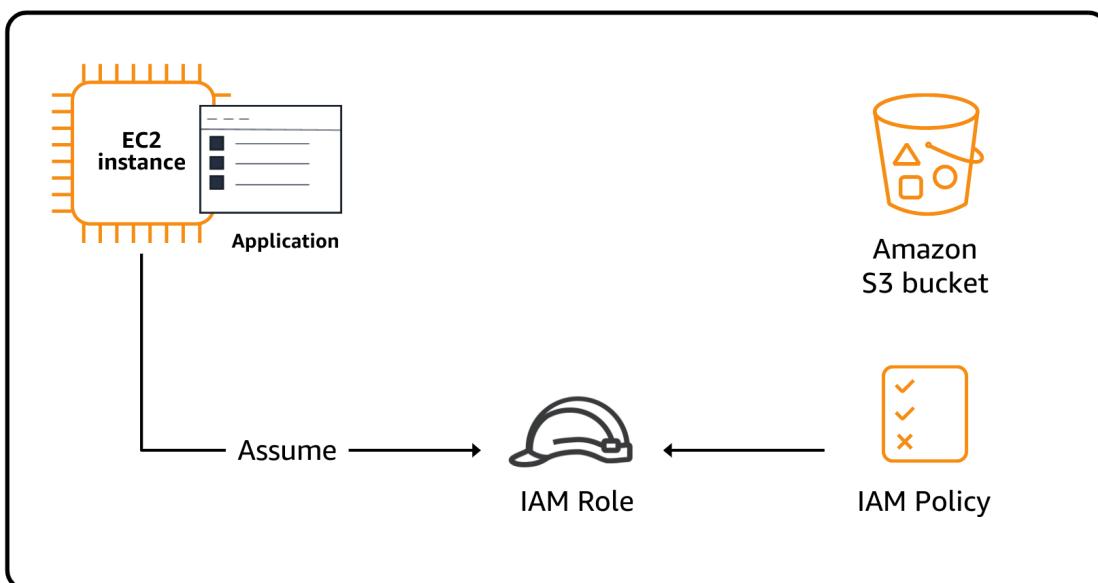
# Using roles for temporary security credentials



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



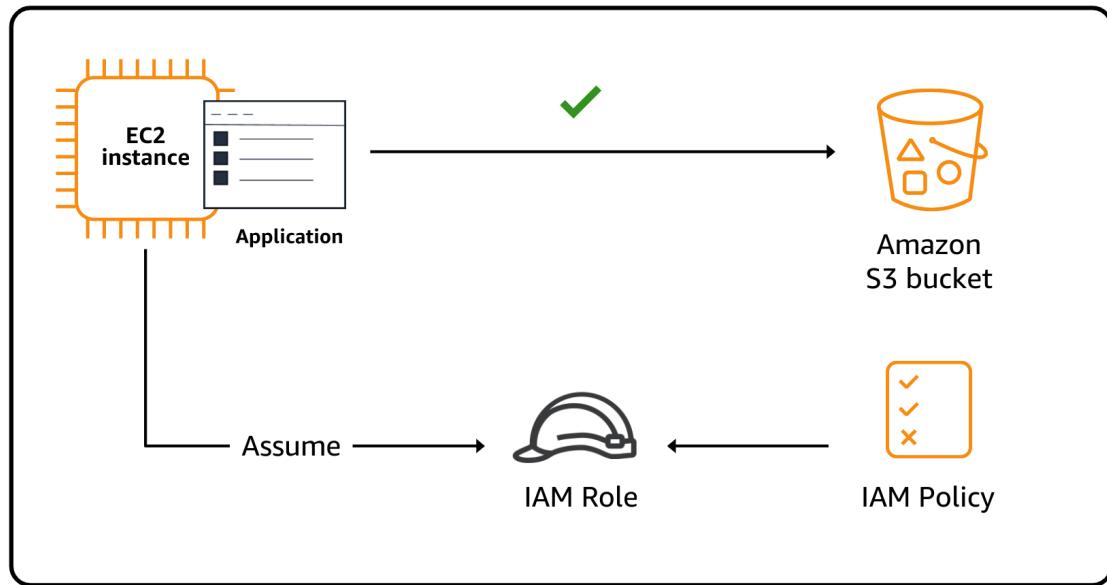
# Using roles for temporary security credentials



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



# Using roles for temporary security credentials



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



## Demo

# Best practices

- Delete access keys for the AWS account root user
- 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

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



## Access your security and compliance

# Challenges of threat assessment



- Expensive
- Complex
- Time-consuming
- Difficult to track IT changes

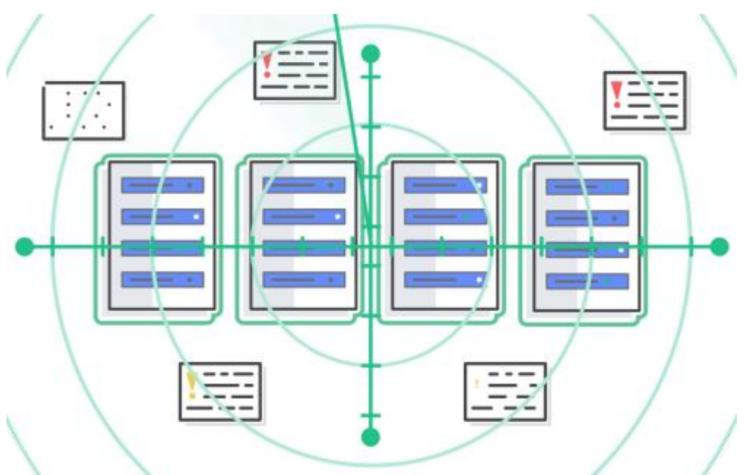
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws | intel

## What is Amazon Inspector?

Automated security assessment as a service

- Assesses applications for vulnerabilities
- Produces a detailed list of security findings
- Leverages security best practices



aws | intel

# Amazon Inspector findings

Amazon Inspector - Findings					
Inspector findings are potential security issues discovered during Inspector's assessment of the specified application. <a href="#">Learn more</a> .					
<a href="#">Add/Edit attributes</a>					
<a href="#">Filter</a>					
Severity	Application	Assessment	Rule package	Finding	
High ⓘ	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	Instance i-aac4c46f is config...	
High ⓘ	Customer Processing	Comprehensive-Assessment	Common Vulnerabilities and Ex...	Instance i-aac4c46f is vulne...	
High ⓘ	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	No password complexity me...	
Informational ⓘ	Customer Processing	Comprehensive-Assessment	Operating System Security Best...	No potential security issues	
Informational ⓘ	Customer Processing	Comprehensive-Assessment	Network Security Best Practices	No potential security issues	

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



## Remediation recommendation

Finding for application - Customer Processing	
<b>Application name</b>	Customer Processing
<b>Assessment name</b>	Comprehensive-Assessment
<b>Rule package</b>	Authentication Best Practices
<b>Finding</b>	Instance i-aac4c46f is configured to allow users to log in with root credentials over SSH. This increases the likelihood of a successful brute-force attack.
<b>Severity</b>	High ⓘ
<b>Description</b>	This rule helps determine whether the SSH daemon is configured to permit logging in to your EC2 instance as root.
<b>Recommendation</b>	It is recommended that you configure your EC2 instance to prevent root logins over SSH. Instead, log in as a non-root user and use <b>sudo</b> to escalate.

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

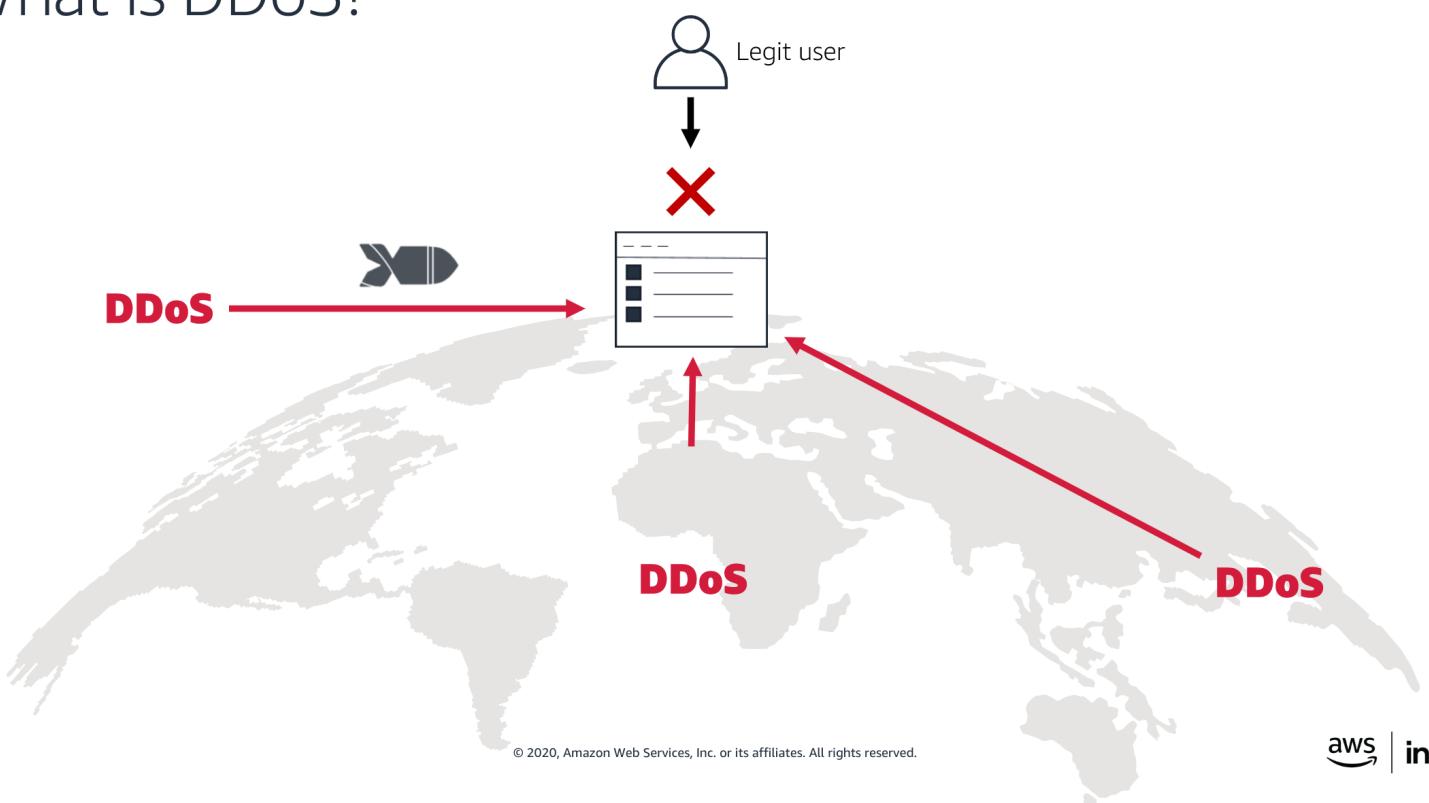


# Protect your infrastructure from Distributed Denial of Service (DDoS) attacks

**AWSOME DAY**  
ONLINE CONFERENCE

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

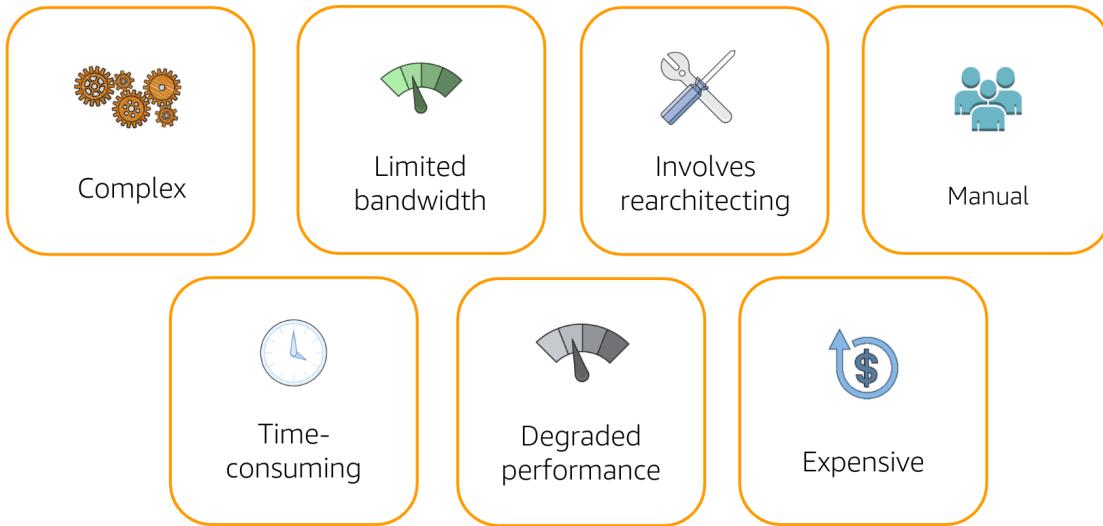
## What is DDoS?



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws | intel

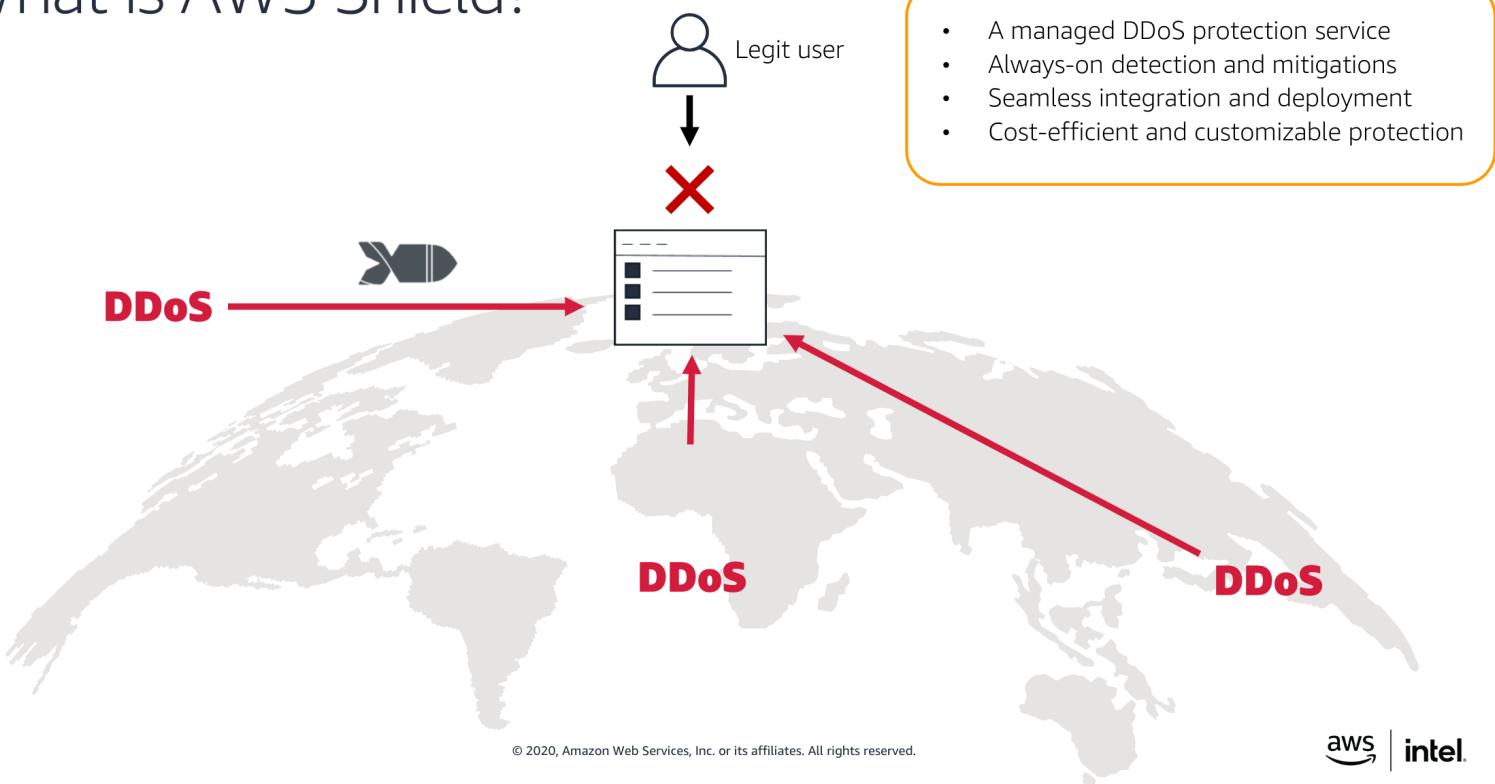
# DDoS mitigation challenges



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



## What is AWS Shield?



# AWS Shield Standard and AWS Shield Advanced

## AWS Shield Standard

(Included)

- Quick detection
- Inline attack mitigation

## AWS Shield Advanced

(Optional)

- Enhanced detection
- Advanced attack mitigation
- Visibility and attack notification
- DDoS cost protection
- Specialized support

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



## AWS security compliance

# Assurance programs



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws | intel

## How AWS helps customers achieve compliance

### Sharing information

- Industry certifications
- Security and control practices
- Compliance reports directly under NDA

### Assurance program

- Certifications/attestations
- Laws, regulations, and privacy
- Alignments/frameworks

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws | intel

# Demo

**AWSOME DAY**  
ONLINE CONFERENCE

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

## Customer responsibility

You own your certification.

**Review – Design – Identify – Verify**

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



# End of Module 4

## Test your knowledge

Access the quizzes with the "test your knowledge" button at the bottom of the page.