Course Title: AWS Certified Cloud Practitioner (CLF-C01) Cert Prep: 2 Security

Description: As part of any good IT infrastructure, security plays an important part in creating a stable technical environment. In the AWS Certified Cloud Practitioner exam, the Security module makes up a fourth of the exam questions. With cloud computing becoming more relevant to many professionals' lives, even if tangentially, it's a vital topic to explore. This course, the second in a four-part series designed to help professionals in non-technical roles, provides you with a high-level grasp of the major security services and concepts in AWS. Instructor Hiroko Nishimura—founder of Intro to AWS for Newbies—provides an overview of security in the cloud. She then delves into the different security services available: Identity Access Management (IAM), Shield, Inspector, and more.Note: This course also maps to the second domain of the AWS Certified Cloud Practitioner exam. Taking all four courses in the Introduction to AWS for Non-Engineers series will help you prepare for the exam.

****

Chapter: 1. Security in the Cloud

****

Video: Shared responsibility model

Note Time: Note Text:

0:00:14 Security and Compliance

IT infrastructure (traditional in the past) :
- Server rooms with key cards
- Off site data centers
- Lots of security devices and people
- Difficult to access

Now, it's being replaced by cloud providers which takes care of managing security on our behalf so that we can focus on other aspects of IT infrastructure management.

0:02:51 Shared responsibility model ?

- security of cloud computing infra and data is a shared responsibility between the customer and AWS
- AWS responsible for security of cloud : Physical security of data centers hosting cloud, hardware, networking that runs the cloud services etc..
- customer is responsible for security in cloud : protecting customer data, encryption, IAM, patching OS of VM's, configuring firewalls

----

Video: Well-architected framework

Note Time: Note Text:

0:02:32 Well architected framework of security ?

- Operational excellence
- Security
- Reliability
- Performance efficiency

- Cost Optimization

IAM ?

- Identity and access management
- Actively manage all-user access
- Use strong identity foundation
- Principle of least privilege

Detective controls ?

- Enable traceability : who did what, when ?
- Actively monitor alerts
- Audit actions and changes to environment in real time

Infrastructure protection

- Apply security on all layers of infra
- Not just the outer layer like physical data center
- Virtual servers: Secure multiple layers like subnet, load balancer, OS
- Security best practices should be automated to save time and money when scaling

Data should be protected at Rest and In Transit

- At rest : image stored in S3 bucket
- In Transit : Email being sent from one server to another

Data protection

- Security mechanisms should be adjusted depending on sensitivity of the data
- Keep people away from data

Incident response

- Intervene, investigate and deal with all security events
- Once issue is resolved, update incident management process, continue to learn and update.

Video: Principle of least privilege

Note Time: Note Text:

0:02:58 Principle of least privilege ?

- you should have access to only resources that is required to complete your Job and no more.
- acheived using IAM policies

Video: Study break: Security domain

Note Time: Note Text:

0:00:45 AWS compliance programs : Like HIPPA for healthcare data etc...

****

Chapter: 2. Security Services

****

Video: Identity and Access Management (IAM)

Note Time: Note Text:

0:03:45   IAM :

- granular access permissions to every user and service while still being able to manage them easily.
- manage users and groups
- permissions are global : any access setting will be true across all regions
- follow principle of least privilege

How it’s being used ?

- Manage users
- Manage IAM roles (it can be used to provide access from another AWS account to your AWS account)
- Manage federated users (it can allow existing identities in your enterprise to access AWS without having to create IAM user for each identity ideal for lists), SAML 2.0

Video: Web application firewall (WAF)

Note Time: Note Text:

0:01:10   WAF (Web application Firewall) ?

- Protect apps from common exploits
- It can be deployed on Amazon cloud front as part of CDN or via AWS API gateway.

Video: Shield

Note Time: Note Text:

0:02:56   AWS shield ?

- Protect against DDoS attacks (multiple requests from unique IP addresses)
- provides detection and automatic mitigations
- minimize application downtime and latency when an attack happens
- Standard tier and Advanced tier

Video: Inspector

Note Time: Note Text:

0:01:05 AWS Inspector ?

- Automated security assessment service for applications
- Automatically assess for exposure, vulnerabilities and derivations from best practises
- Gnerates detailed reports for security teams
- can define security standards or choose to use AWS standards which are updated

----

Video: Trusted Advisor

Note Time: Note Text:

0:01:59 AWS trusted advisor ?

- Guides provisioning of resources to follow AWS best practices
- Scans your infra and advises on how to optimize for cost, performance, security, fault tolerance and serv ice limits

Seven core Trusted Advisor checks :

- S3 bucket permissions
- Security groups - specific ports unrestricted
- IAM role
- MFA on root account
- EBS public snapshots
- RDS public snapshots
- Service limits

Enterprise checks -

- Along with above , more type of checks
- Notifications for weekly updates, automated actions in response to alerts using cloudWatch

----

Video: GuardDuty

Note Time: Note Text:

0:00:58 AWS GuardDuty ?

- 24/7 threat detection service for the AWS Cloud
- uses machine learning, anamoly detection and integrated threat intelligence to identify potential threats