AWS Security Specialty Study

- Study Notes
- Testrun of the AWS Sample Questions
- Testrun of the AWS 20 Practice Questions
- Real Exam Results
- Gotchas from the Real Exam

Study Notes

✔ KMS — AWS Key Management Service FAQs

Guess: KMS is an encrypt/decrypt/key management service that allows users to encrypt data up to 4KB in size via encrypt/decrypt APIs or generate and store keys used by other AWS services on your behalf to encrypt data at rest. Solutions requiring the encryption of large amounts of data use envelope encryption where the service decrypts a key with KMS and then uses this key to encrypt/decrypt the large dataset. The key storage is backed by HSM so it uses special hardware security modules to control the encryption/decryption which reduces the chance of a software based exploit compromising keys because the private key material is kept in a guaranteed secured location.
After Review: Supports auto rotating annually as an option. Audit logging is in cloudtrail. Accessible via the AWS encryption SDKs. Default service keys exist e.g. for s3 or you can choose to create a CMK customer managed key. You can BYOK if you want (256bit).

✔ CloudHSM — FAQs | AWS CloudHSM | Amazon Web Services (AWS)

Guess: Cloud HSM is a hardware security module to provide a physical layer of security when it comes to sensitive information handling. ~~Internally used for KMS and can be connected to some compute services.~~
After Review: The data in the HSM is invisible to AWS and provides a root of trust that can be used for DRM etc. and can provide a level of compliance required for certain levels of trust like PCI. KMS can be directed to use the self-managed HSM cluster as a key store. HSM is a clustered self-managed service.

✔ NACL — Control traffic to subnets using Network ACLs - Amazon Virtual Private Cloud

Guess: Network ACLs are network level access control lists that provide a lower level of control for network security policies, these can be used to achieve a simple layer of network security like dropping data for specific port ranges similarly to security groups but the source and destination are defined purely by IP.
After Review: A subnet can only be associated with one NACL and the rules are stateless so they impact traffic immediately at the packet level. These have a default deny-all catch-all rule that is used to ensure all traffic needs to be explicitly allowed. The default subnet ACL is to allow all traffic in and out of the subnet e.g. 0.0.0.0/0 ALLOW.

✔ Elastic Beanstalk

AWS Elastic Beanstalk FAQs - Amazon Web Services (AWS)

Guess: Elastic Beanstalk is an application stack specifically for hosting web applications that allows easy configuration of web/app~~/data tiers~~ without needing to know all the complex parts of networking policy etc. ~~This can be templated so it's easy to handover a deployment template for a full stack application to development teams. I was thinking of OpsWorks Stacks…~~
After Review: Simple solution for deploying auto-scaling web applications on managed infrastructure e.g. choose to deploy a .net website on IIS and patching is managed. It uses Cloudformation behind the scenes.

✔ OpsWorks

AWS OpsWorks – Configuration Management - Amazon Web Services

Guess: Literally no idea what this is, I can't even guess. Maybe it's a system for managing and scheduling maintenance and stuff like cert expiry.
After Review: It's literally managed chef & puppet for a portion of it. AWS OpsWorks Stacks can be used to define recipes for provisioning infrastructure down to the configuration management level with "layers".

✔ CloudFormation

AWS CloudFormation FAQs

Guess: A general purpose declarative language for defining cloud infrastructure in AWS, similar to Terraform but AWS specific. Builds Cloud Formation Stacks which can be turned up and torn down easily.
After Review: Pretty much, it's defined in JSON/YAML.

✔ AWS SAM

What is the AWS Serverless Application Model (AWS SAM)?

Guess: SAM uses cloudformation behind the scenes but provides a simple to use API for building serverless applications e.g. `sam init` will create a simple lambda with an api gateway.
After Review: It's an extension of Cloudformation so it's CF with extra functionality to make developing serverless applications more easily and has features that allow local lambda execution and debugging.

✔ Cloudwatch

Amazon CloudWatch FAQs - Amazon Web Services (AWS)

Guess: Cloudwatch is the AWS metrics collection framework that can be used to build alarms on top with Cloudwatch alerts. AWS services are integrated with cloudwatch and can usually have "enhanced" metrics turned on which collects metrics in a more granular detail.
After Review: Monitoring service is a better name for it because it's not just metrics, it's a metric store and alert system. It now has anomaly detection too and also is the logging framework + x-ray.

✔ AWS Cloudtrail

Multiple Trails - AWS CloudTrail FAQs - Amazon Web Services

Guess: ~~Cloudtrail is the built-in AWS logging framework, applications create log streams and write logs to them. The cloudtrail UI provides basic querying and metrics can be generated from cloudtrail data that can be queried in Cloudwatch~~
After Review: Trails can be configured to send events to s3 or cloudwatch logs but on its own Cloudtrail is just the account events for AWS events triggered via APIs.

✔ AWS Artifact

Self-service compliance portal - AWS Artifact

Guess: If you need details about AWS certifications like SOC, ISO etc. Artifact is a self service portal for downloading the latest versions of these.
After Review: Same as guess.

✔ Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) FAQs

Guess: The big dog. Everything is controlled by IAM by way of principals (users, services etc.), groups (collections of principals), roles (groups of policies) and policies which are the access management part of IAM.
After Review: Too broad to summarize, IAM is everywhere.

✔ IAM Policy - Policy Options

IAM JSON policy reference - AWS Identity and Access Management

Guess: Policies define how to allow or deny on specific resources by conditional logic using expressions based on tags etc. or by simple pattern matching based on ARNs (amazon resource name) and the allowed actions for the resource e.g. s3:ListBucket etc.
After Review: Nothing to add.

✔ IAM Policy - Cross Account Rules

Cross-account policy evaluation logic - IAM

Guess: When creating cross account policies, policies need to be defined on both sides e.g if Service A in Account B needs to access a Bucket C in Account D there needs to be rules to allow the Service A to s3:GetResource and in Account D there needs to be a policy that allows Account A to access Bucket C with something like aws:account:123451231:root which delegates control to allow policies in Account B to be able to allow resources access to the bucket.
After Review: arn:aws:iam:123451231:user/abc123 can also be used to specify the user in the destination account.

✔ IAM Policy - Order of Evaluation

Policy evaluation logic - AWS Identity and Access Management

Guess: Not really sure, multiple policy statements will be evaluated in the order they are found in the policy and will cascade so if there is a “deny all” at the start and then a later policy that allows access for a subset of principals then all principals apart from the specified ones will be denied.
After Review: Deny all is the implicit default and explicit denies take precedence if two statements are impacting the same resource.

✔ IAM Policy - Assuming Roles

AssumeRole - AWS Security Token Service

Guess: When assuming a role an account talks to the STS simple ticket service to get short term credentials for a target role, the principal needs to have the IAM AssumeRole permission for the target role for the STS to return valid credentials.
After Review: This is also used as the mechanism to get cross-account access by assuming a role in another account the way we have it set up for local dev machines.

✔ **Bucket Policies** [Bucket policy examples - Amazon Simple Storage Service]

Guess: Bucket policies are S3 specific policies that are more purposed for the general public e.g. allowing access to certain IP addresses ~~or enforcing S3 specific details like data retention or encryption details~~.
After Review: This has better disambiguation of the policies vs IAM vs ACLs. Bucket policies are policies directly attached to buckets that control access similarly to IAM policies and you can basically just use IAM policies to enforce the same controls. S3 ACLs are an earlier version of policies and should not be used if it can be avoided.

✔ **Amazon Cognito** [Amazon Cognito - Simple and Secure User Sign Up & Sign In]

Guess: Cognito is an AWS service that maps IAM principles and policies to web users via identity pools. This service can be integrated with SAML providers and other social OAuth logins.
After Review: Cognito does provide a way to integrate IAM policies with users via identity pools but it's primary purpose is to allow users to sign up to a web service and provides features like "verify by email" and MFA for authorisation. SAML IDPs can be added in IAM and used to link with Cognito Identity pools which allows things like mobile applications to directly connect to aws services like S3 with short lived credentials linked to the user or SAML can be used with user pools. Groups can be created in the user pool and assigned IAM roles.

✔ **Amazon GuardDuty** [Intelligent Threat Detection – Amazon GuardDuty FAQs – Amazon Web Services]

Guess: ~~Guard Duty is a tool that will monitor security controls in an AWS account e.g. you may define a rule saying an EC2 instance can not have a public IP address and when this happens in the account an alert will fire which can be used to kick off automated remediation via something like SNS -> Lambda etc~~.
After Review: Guard duty is a threat detection service that actively monitors EBS/S3/EKS/EC2 instances etc. in an agentless manner so it doesn't have a performance impact. It detects malware and malicious behaviors like command and control communications and data exfil.

✔ **Amazon Macie** [Amazon Macie FAQs – Amazon Web Services]

Guess: ~~Macie is a best practice analysis tool that will tell you if shit is configured unsafely in your account~~.
After Review: Macie is a sensitive data discovery service that operates on all your S3 data to find potentially sketchy data you've shared and this can generate alerts in EventBridge which can be used for triggering remediation. It also provides a system of identifying unencrypted buckets, buckets publicly available or shared with external actors.

✔ **Secrets Manager** [AWS Secrets Manager - Amazon Web Services]

Guess: Secrets manager is a secrets vault that can be used to store and retrieve application secrets.
After Review: Secrets manager provides a way of auto-rotating credentials for some AWS services like RDS.

✔ **Amazon Inspector** [Automated Vulnerability Management – Amazon Inspector – Amazon Web Services]

Guess: Literally no idea.
After Review: Vulnerability scanner for EC2 instances and container images that detects vulnerable software and inventories the findings. Can run network reachability scans.

✔ AWS Config AWS Config FAQs - Amazon Web Services

Guess: AWS config can be used to monitor configuration changes and publish them to cloudtrail.
After Review: Config rules can be defined and validated against all infrastructure to assess compliance based on configuration e.g. is buckets public, is public ip address attached to instance. Conformance packs are available to ensure that best practice is being followed for specific situations. All config changes are fired through SNS that can be used for remediation or analysis. As well as infra changes internal systems changes like updates and software installations can be tracked. Remediation can also be configured through SSM.

✔ SSM AWS Systems Manager

Guess: (Simple) Systems Manager is used with an agent running on the host to manage hosts remotely via the AWS tooling rather than using a bastion and remoting directly to machines.
After Review: Systems manager also has a lot of additional functionality like managing state, patching, maintenance windows. Incident response plans can also be defined with runbook automation.

✔ Shield FAQs - AWS Shield - Amazon Web Services (AWS)

Guess: Shield is used to protect from network level DDoS attacks.
After Review: Shield is enabled by default like a silent service. There is a paid advanced version but it’s not that much fancier.

✔ AWS WAF FAQs - AWS WAF - Amazon Web Services (AWS)

Guess: WAF is a standard web application firewall, where Shield will protect against things like SYN flooding at a network level. The WAF reads application layer traffic to identify things like SQLi.
After Review: WAF can run at the edge when used with cloudfront or in-region when used with load balancers.

✔ Trusted Advisor AWS Trusted Advisor

Guess: Trusted Advisor is a recommendations engine that will recommend best practice configuration changes for price management like “machine is over provisioned”.
After Review: Trusted advisor also identifies basic security best practice failures like exposed access key notifications, bad RDS security groups etc. and warning when approaching service quotas in AWS.

⚠️Service Health Dashboard AWS Health Dashboard

Guess: The service health dashboard is the first thing to check for any suspected AWS level issues/incidents.
After Review: Literally just the public service dashboard, nothing more to it.
After Exam: Shit, I mixed up AWS Health with the service health dashboard. I should have studied Security in AWS Health.

✔ AWS Detective Amazon Detective FAQs

Guess: Detective is for threat hunting?
After Review: Detective collates data from cloudtrail, flow logs audit logs and guard duty to show links between entities.

Testrun of the AWS Sample Questions

Prior to starting any study I attempt the sample questions to give myself a quick reality-check to find out the areas I'll need to put the most effort into. At this stage I've watched a few videos on Youtube of what to expect in this exam but not much else. I've been tinkering indirectly in AWS for ~ 4-5 years on personal projects, a couple of cloud migrations and have some experience in GCP and Azure so I have an understanding of the fundamentals but not the depth of knowledge expected for this exam.

Results (80%, 8/10)

1) Failed because I didn't know you could use IAM to lock down access to a KMS resource by VPC endpoint ID.
2) Correct.
3) Correct.
4) Correct.
5) Correct.
6) Correct.
7) Correct.
8) Failed because I didn't know S3 provides an HTTP service endpoint as well as HTTPS, I assumed all S3 uploads would be over HTTPS but that is incorrect and a policy needs to be applied to disable HTTP uploads for a bucket.
9) Correct.
10) Correct.

Gotchas

- At this point I was overly confident and scheduled this exam, DevOps Pro and Solutions Architect Pro all to happen over a 2 week period which was a mistake because the other exams were much harder because they covered a lot of concepts and technology I hadn't used much or at all. The sample questions are much easier than practice and real exam questions.
- KMS can encrypt 4KB of data at a time. Envelope encryption can be used to encrypt large objects e.g. with S3 where it generates a symmetrical key and stores this in KMS retrieves it at runtime to decrypt payloads outside of KMS with a KMS managed key inside of S3 before sending it to the client
- sourceVpce is an endpoint policy that can restrict access in an IAM policy to a specific VPC endpoint
- aws:SecureTransport will enforce HTTPS access to buckets, http is allowed by default but most clients use https, don't trust everyone to be smart with this just deny http incase somebody downloads a secured object over a plaintext connection.
- Trusted advisor (recommendations engine), config (resource configuration history), inspector (reachability and vuln scanning), macie (data leaks and bucket access) and guard duty (IDS) are all confusingly named…

Testrun of the AWS 20 Practice Questions

As a final test of what I've learnt from the study I redo the Sample Questions above to see if I still remember what's going on and if the questions seem easier to comprehend then I do the official 20 practice questions which shows me weak areas I need to do some extra study in.

Results (65%, 13/20) - Rerun (100%, 20/20)

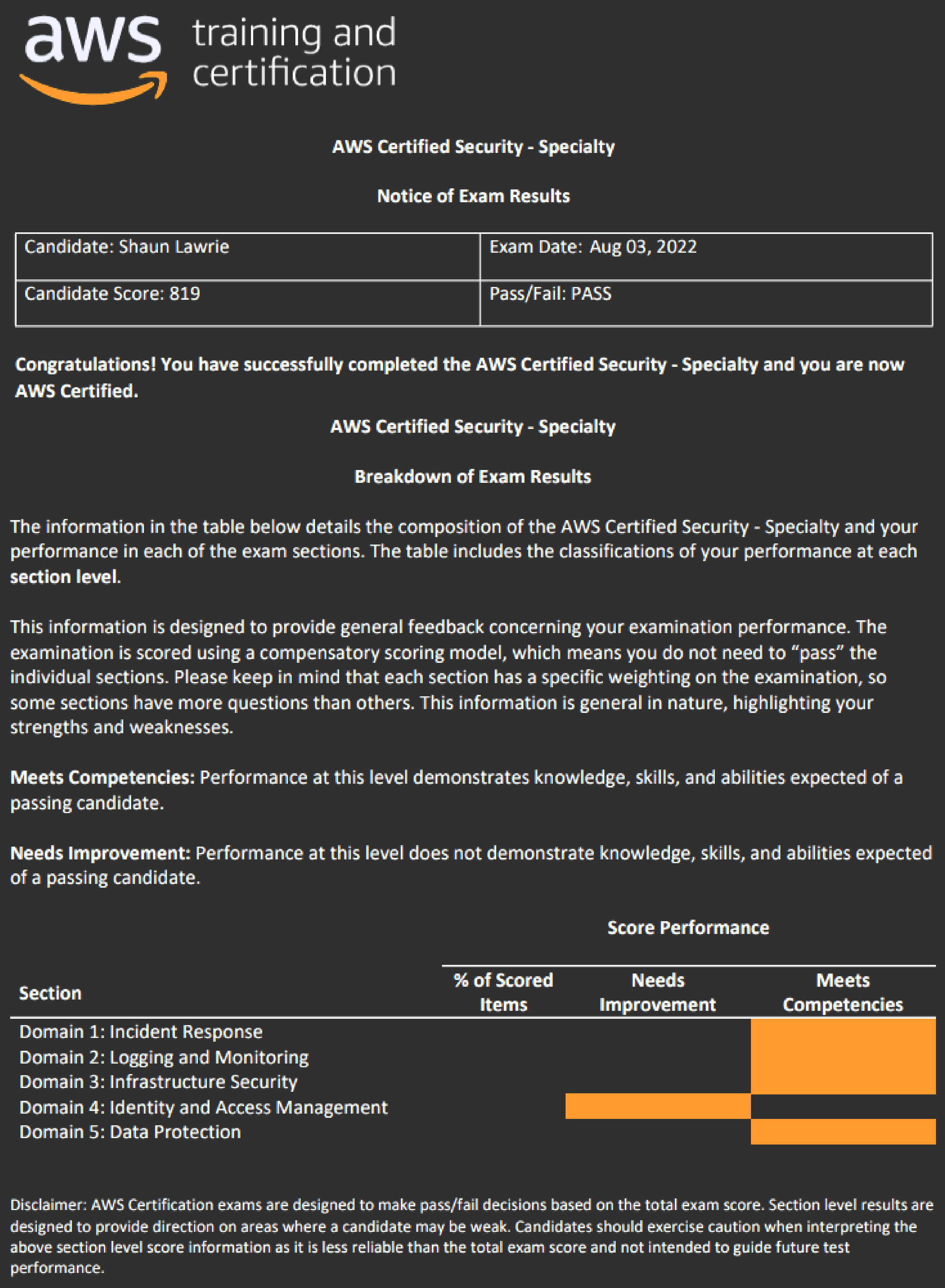
The questions are in random order so I can't number these. 65% is pretty bad but it just gives more areas to study and the practice exam immediately tells you the answer after each question so I use that to do a bit of study into my failures as I fail each question. Pretty soon after failing this practice exam I do it again to see if I can remember the parts I failed and do better the second time around to gain confidence.

1. Failed half of the multichoice question because I didn't understand the practical implementations of AWS Config and remediating unwanted config changes. Got 1/2 of the multichoice answers.
2. Failed the entire question because I didn't know all the use cases of AWS Inspector.
3. Failed half of the multichoice question because I didn't read the answer wording correctly and thought the IAM role was to be attached to a user who wanted access to a bucket but instead chose to try to attach a role to a bucket.
4. Failed half of the multichoice question because I chose to deny traffic from dodgy IP addresses by a security group rule to protect a site from DDoS but the expected answer was to auto-scale the application to soak the traffic.
5. Failed half of the multichoice question because I didn't know anything about External IDs and how to use them in cross-account AssumeRole API calls.
6. Failed the entire question because I didn't know how to scope SCP's to OUs in an AWS Organization.
7. Failed the entire multichoice question because I didn't understand KMS key aliases and how to use them to allow transparent key rotation to applications/services relying on the key. I also didn't know the AWS managed automatic key rotation options for CMKs.

Gotchas

- S3 object ownership can be enforced with ACLs disabled and "bucket owner enforced" https://docs.aws.amazon.com/AmazonS3/latest/userguide/about-object-ownership.html
- Service Control Policies are policies applied to organizations in AWS OUs, e.g. you can have the maximum permissions allowed for an OU e.g. for all dev accounts you could deny "create ec2 instance" if you felt mean. You can use this to restrict the maximum permissions in an account. https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html
- Can you auto rotate CMK? Yes but only yearly, faster than that requires a creative solution.
- Amazon Inspector reachability rules are able to be used to validate internet facing infrastructure.
- Inspector has an agent? It uses the SSM agent now.
- When assuming a role across accounts an external ID is required. https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-roles/ https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html
- Don't use key id's, use key aliases in application configurations. https://docs.aws.amazon.com/kms/latest/developerguide/kms-alias.html
- IAM access analyser can show resources shared with external entities.

Real Exam Results



AWS Certified Security - Specialty

Notice of Exam Results

Candidate: Shaun Lawrie	Exam Date: Aug 03, 2022
Candidate Score: 819	Pass/Fail: PASS

Congratulations! You have successfully completed the AWS Certified Security - Specialty and you are now AWS Certified.

AWS Certified Security - Specialty

Breakdown of Exam Results

The information in the table below details the composition of the AWS Certified Security - Specialty and your performance in each of the exam sections. The table includes the classifications of your performance at each **section level**.

This information is designed to provide general feedback concerning your examination performance. The examination is scored using a compensatory scoring model, which means you do not need to “pass” the individual sections. Please keep in mind that each section has a specific weighting on the examination, so some sections have more questions than others. This information is general in nature, highlighting your strengths and weaknesses.

Meets Competencies: Performance at this level demonstrates knowledge, skills, and abilities expected of a passing candidate.

Needs Improvement: Performance at this level does not demonstrate knowledge, skills, and abilities expected of a passing candidate.

	Score Performance		
Section	**% of Scored Items**	**Needs Improvement**	**Meets Competencies**
Domain 1: Incident Response			🟧
Domain 2: Logging and Monitoring			🟧
Domain 3: Infrastructure Security			🟧
Domain 4: Identity and Access Management		🟧	
Domain 5: Data Protection			🟧

Disclaimer: AWS Certification exams are designed to make pass/fail decisions based on the total exam score. Section level results are designed to provide direction on areas where a candidate may be weak. Candidates should exercise caution when interpreting the above section level score information as it is less reliable than the total exam score and not intended to guide future test performance.

Gotchas from the Real Exam

- This is the AWS security high level overview by Becky Weiss who is really good at explaining the fundamentals with easy to understand analogies. If I hadn't reinforced what I know with this I would have done worse ▶ AWS re:Inforce 2019: The Fundamentals of AWS Cloud Security (FND209-R)
- KMS is heavily referred to in the exam content and you need to be familiar with pretty much everything here in AWS KMS concepts. I had the high level concepts down around key rotation etc. but there was still a lot I didn't know.
- I was weak in IAM and I think that came down a lot to the fact that I rely on the policy editor to build policies most of the time and didn't know the specific actions and resource types for specifically Amazon S3 Actions/Policies and AWS KMS Actions/Policies.
- I've had problems with VMs with encrypted storage but have never memorized the required permissions to allow them to launch from secured images. I Google it every time but it would have been worth remembering this.
- I screwed up the study on AWS Health and have added an update directly in the study notes.