System Operations Associate Exam tips

General

This is not a brain dump. Questions and answers are not given here. Rather it is a guide for further research.

As of October 2018 there were 65 questions in 130 minutes.

The exam was updated just prior to this date.

Most questions had a single answer. A very small number had multiple answers.

There were no questions on maximums or limits, probably because these are subject to change.

There were very few questions involving CLI syntax.

Many questions were similar to the Architecture Associate exam ie choosing the right solution for a use case. In fact, it might be possible to pass the exam based on the knowledge required for the Architect exam. I recommend studying my exam tips for that exam.

Shared responsibility model

Know what Amazon are responsible for verses what the customer is responsible for.

IAM

Know IAM best practice, eg use of MFA and least privilege

Know the console login URL for the IAM user:

https:// AWS_Account_ID.signin.aws.amazon.com/console/

Know that IAM policies can include conditions eg allow access when the source IP is from a particular subnet.

Know how can a mobile app can have permissions to use DynamoDB. The application should use an IAM role with web identity federation.

Know how an IAM user can be given permissions to manage particular EC2 instances? Use tagging and reference the tags in the policy.

VPC

Know the detail of security groups and NACLs, where they are applied and the default rules.

Know the use case for placement groups.

Know the default entry in any Route Table. Destination: CIDR range of VPC: Target: Local.

Know the uses case for NAT Instance/Nat GW/IGW/VGW

Know the rules about public and private subnets. Know the allowed CIDR mask lengths. Know the default routing rules in a new VPC.

Know how many IPs are available given a particular mask.

Recognise when two CIDR ranges overlap.

Know that instances behind an ELB can use a private subnet

Know how you would allow a custom monitoring application on EC2 to monitor other EC2 applications ie SG rules to allow the required IP and port outbound from the monitoring application, and inbound on the monitored applications.

If you have a legacy application on EC2 with a hard coded IP address, how could you allow the application to failover to a new instance without the need for reconfiguration.

Know the use cases for VPN and Direct Connect. Use Direct Connect if low latency is required.

Know that you cannot delete a subnet while there are ENIs associated with the subnet.

Know what the VPC wizards create.

Know that AWS independently maps AZ identifiers for each account. In other words, your AZ-A is not necessarily the same AZ as another accounts AZ-A.

EC2

Know that software on an instance can determine its public and private IP by querying the metadata.

Know that instance log files are available in the console

Know about termination protection.

Know that to remedy network throughput as a bottleneck on EC2, changing to larger instance type may be a solution

If an instance system status check shows “impaired”, you could stop and start the instance. it will be placed on a healthy host.

Know the standard CW metrics for EC2 instances and that something like memory utilization would require the CW agent and a custom metric.

Know that an EBS volume can continue to be used while a snapshot is in progress

Know that once an instance is launched, you cannot change the zone of the instance. You could create an AMI and launch an instance from it.

When starting an instance it is possible to receive an "InsufficientInstanceCapacity" error. AWS does not have sufficient capacity in that AZ. You can try again later or change the AZ.

Know the use cases for the different EC2 pricing options.

Know that CW allows you to see an aggregated metric eg CPU utilization across multiple EC2 instances eg all instances launched from a particular AMI.

Auto scaling

Know that autoscaling can be based on a schedule or a policy.

Know that an ASG can scale based on the size of an SQS queue.

Know that you must check service limits to avoid potential service disruption and that Trusted Advisor can help you determine your limits, and that you can request higher limits.

Know that the health of an instance in an ASG can be determined using EC2 system status checks, and if behind a load balancer, also using load balancer health checks.

Know that for something like a Bastion host, an ASG with min, max, desired of 1:1:1 would provide HA without human intervention.

EBS

Know how to migrate a volume from one AZ to another ie you have to use snapshots.

Know that snapshots are incremental.

Know that if you set up a CW alarm for a volume which is subsequently detached, the status of the alarm will be Insufficient Data.

ELB

Know what a sticky session is.

Know what connection draining is.

Know that you can configure the load balancer to create access logs.

Know that there is an SG associated with the load balancer and an SG associated with the back-end instances and the rules that would be required.

Know that a security policy is used for the SSL negotiation, and the policy includes SSL protocols and SSL Ciphers. If no policy has been associated, it will use a default policy.

S3/Glacier

Know the basic facts eg 5TB per object, unlimited bucket storage, 4 9's availability for standard S3, 11 9's durability.

Know the other storage tiers and when Glacier is a good option including the different Glacier retrieval options.

Know that you could prevent a particular IP range from accessing a public bucket using a bucket policy.

Know how to interpret a bucket policy which uses conditions based on subnets and IP addresses.

There were no questions on S3 ACLs probably as they are considered legacy.

Know the 4 encryption options.

Know about multi-part upload.

Know about the use case for MFA and versioning.

Know that a bucket policy can be applied to a bucket and not an object, but that the policy can apply to objects within a bucket.

RDS

Know about Multi-AZ, automatic backups and manual snapshots.

Know the failover process ie when the primary fails, the connection string remains the same.

Know the use case for Read Replicas – eg large analytics jobs

Know that you can configure SNS to notify when an event occurs such as RDS creation, deletion, restoration, backup.

Know the SNS subscription types.

Know the use case for the maintenance window.

CloudWatch

Know that Cloud Trail can monitor calls made to APIs including to CW

Know that the console allows you to filter using relative or absolute dates and times.

Know that CW supports custom metrics. An application can publish data to CW and you can view the data in the console.

Know that CW supports basic monitoring at a granularity of 5 minutes, and detailed monitoring at a granularity of 1 minute or less. Some services involve extra charges for detailed monitoring. Some use detailed monitoring by default.

SQS

Know the use case for SQS and the basic facts

Route53

Know the use case for the different policies eg you have a multi-region web facing app where a controlled portion of traffic is being processed by an alternative region. You would use WRR and health checks.

Cloud Formation

Know how a template can use the output of another template

Know the main sections eg the use case for parameters and wait conditions.

Know that the resource section is the only required section.

Opsworks

Useful to know some terminology in case its one of the answer choices even if its not the usually the best solution in the exam scenarios.

Elastic Beanstalk

Same comment as for Opsworks.

IAM

Know that you can apply policy to a user, group or role.

SNS

Know the SNS subscription options ie SMS, HTTP(S), Email, SQS

Backups

Know which services provide out of the box user configurable automatic backup as a service. Eg RDS

Security

Know services allow the customer to retain run administrator privileges on the underlying instance ie Elastic Beanstalk, EMR, but not LB, RDS, Elasticache.

Know that you have to obtain approval to perform penetration tests against your systems instances and endpoints.

Know the use case for signed URLs

HA

Know which services are implicitly HA, and which can be with the right architecture. There is a slide in the course.

Know the use case for CloudFront, Read Replicas and Elasticache in the context of scaling.

Authentication

Know the options for single sign on including AD connector and the use of an on-prem AD.

Organisations/Billing/Tagging

Know the features of Organisations including consolidated billing.

Know the use case for tagging in the context of costs.