**Topic Hints and Tips**

I’ve grouped my hints ‘n’ tips into topic areas below … I hope it helps.

**COMPUTE**

Ensure you are fully comfortable with the terms EC2 Family, Type, Size and generation. It’s not essential to remember them all, but understanding the concepts and the major differences is an advanced.

Understand what each family of instances is useful for in terms of workload types. A problem in a question could be a bad instance type selection - or it could be irrelevant.

You need a good understanding of the SPOT pricing model - benefits and downsides of the model. What type of work is it suited for and not suited for - i.e applications which can tolerate interruption.

What options exist for reserved purchases of instances. Scheduled vs term, Zonal vs Regional, 1 v 3 year, All upfront, partial vs no upfront.

If you need to reserve EC2 capacity, which reserved option(s) should you pick?

Understand how you can you create a ‘simple’ HA EC2 instance - ASG 1:1:1 (Lazy HA)

Can you copy an EC2 instance to another AZ? If so, how? If not, is there a workaround?

Learn the architectures of Cluster, Spread and Partition Placement groups. Make sure you are comfortable when you would use each. What are the requirements, limitations and supporting infrastructure.

Detailed knowledge of Launch Templates vs Launch Configurations - features of each, limitations of each, when to use one vs the other.

ECS Architecture - high level container understanding. When to use container services … pros vs cons. When to pick Fargate vs EC2. What’s the difference between the two? when would you pick to use one vs the other.

How do you allocate permissions to ECS Containers .. ? TASK Role.

Understand the Lambda Architecture - Runtime, execution limits, execution roles. How to grant permissions & how it scales.

What events can lambda be invoked by? What services integrate with lambda - a general understanding of what can be used as an event source is enough.

Understand how instance profiles work? How do they relate to instance roles. How are credentials passed into an instance. Understand access, rotation etc.

**STORAGE**

The SAA-C02 exam is full of S3 Questions. I’ve received a lot of feedback from students suggestions ~40% or more of the exam is focussed on S3.

Review the Storage type & Performance of EFS vs Instance Store vs EBS vs S3.

Object Storage Classes - what each does & offers. When to use one vs the other. Go into the exam with architectural patterns and anti-patterns for each class.

Understand how to configure and use an S3 static Website - and be comfortable with offloading style architectures from traditional applications to S3.

S3 Bucket policies, multi account access, public access. How does ownership work with cross-account access.

Understand Block Public Access Settings - it overrides things, know that it is the highest priority.

Consistency Model - write something (A), write an update (B), read it… is it A or B ?

Limit : Number of buckets per account …. this influences architecture. 1 bucket per user = bad, 1 prefix per user = good.

S3 can’t be mounted, its object storage - what does this mean. What is object vs file vs block storage.

S3 Versioning, how it works. Delete markers and Un-delete functionality (delete the delete marker)

MFA Delete - what is it, how does it work.

Understand S3 Events in general - using it for event-driven architectures.

Cross-Region and Same-Region Replication, features and architecture benefits. When would you use this.

When to use Snowball vs uploading data to AWS over a network connection (speeds, amounts, costs)

When to use Snowmobile vs uploading data vs using Snowball (speeds, amounts, costs)

For S3 encryption, understand for each (client-side encryption, SSE-C, SSE-S3, SSE-KMS) who manages the encryption/decryption process and who manages the keys. When would you use SSE-KMS vs SSE-S3 (Role separation)

EFS when should you use it ? Shared instance storage. For logs? Or cloud watch logs?

FSX - architecture, different file systems. The use cases for each. Windows systems feature more in SAA-C02 so FSx is more important vs SAA-C01.

Storage gateway - what the different modes are used for … file, volume, VTL

What IO levels are required to exclude EBS - It’s best to know the EBS volume and Instance limits.

EBS encryption - Architecture

EBS Snapshots - Architecture

EBS Encryption & Snapshots - Architecture

What is an AMI ? Creating an AMI.. copying an AMI, sharing an AMI.

**NETWORKING**

Basic VPC Architecture and config - IPv4 CIDR, IPv6

Subnet structure … limitations (1 subnet = 1AZ)

DHCP Option Sets - what can be adjusted.

Reserved IPs - for popular /XX prefixes.. how many usable IPs in a subnet.

Route Tables - architecture, how are they used. What is the route priority.

IPv4 and IPv6 default routes

Internet gateway .. features and limits, is it HA? Can it be made HA? how..

What is NAT.. how does it work. When is it used.

NAT Instances (Features, architecture, limitations), NAT Gateways (Same), GW vs Instances, SRC/DST check.

NAT and IPv6 ..why is it not needed? Can you explain why IPv6 doesn’t need NAT ?

Know what services an egress-only internet gateway provides and how they are configured.

DNS in a VPC .. public and private DNS what IPs are resolved?

SGs - features, limits, what are they attached too.. stateful

NACLs - features, limits, what are they attached too … explicit DENY & stateless.

You need to REALLY understand what an Ephemeral port is. Specifically know that an incoming tcp/80 stream of data has a return stream using ephemeral port range (not port 80!!) ..

How to secure a multi-tier application in a VPC … routes, NACL/SG

Know the common ports .. SSH, SQL, HTTP, HTTPS, RDP, SMTP, TELNET (it makes it easier to parse questions)

VPC Peering - limits and features, transitive (NOT). DNS resolution.

How does VPN work … IPSEC, Gateways, Authentication, IPs, Static v Dynamic.

Direct Connect, architecture, VIFs, public v private. Encryption over DX. Provisioning time vs VPN

Understand why you would provision a VPN First, then DX ..

When should DX be used … latency/large data amounts/complex networks.

Data transfer costs , internet IPs vs External.

General understanding of Instance Interfaces, IPs, DNS, using MAC address (for licensing)

Elastic IP - features, limitations, billing.

**DATABASES**

Understand the differences between OLTP and OLAP .. what is each used for.

For a given type of data (fnd keywords) know if SQL or NOSQL is required.

For SQL and NOSQL, for a give reliability, cost and performance situation know which DB product to pick.

DynamoDB capabilities … simple key value, wide column, no relations, no structure querying.

HA Capabilities of MSSQL (diff versions), RDS, Aurora and Aurora server less.

Aurora serverless questions were mentioned around scaling back to 0 - understanding that its capable of running with 0 load - paused cluster

When to use a read replica .. including multi-AZ RR

Knowing what MultiAZ does, vs Read Replica - for HA, MultiAZ = availability, RR = read scaling and improved RPO/RTO

Know that RDS (non-aurora) can’t access the standby instance, Aurora can - what benefits does this provide ….

Using Reporting via a RR as the source is a great architecture

How to create an encrypted version of an existing database …

Diagnose bad DB performance … only at 60% CPU .. what is the cause ? Disk? Use a read replica?

Understand which DB’s in AWS are delivered as a service, vs a Database Server as a service.

Understand EMR .. and how its architected at a high level, specifically which components an EMR cluster has…

**CONTENT DELIVERY**

CloudFront architecture - edge locations & regional caches.

Preventing access to a resource directly OAI .. how to do this if the origin is an ALB, one answer was custom headers.

Caching static and dynamic, how ? And how to optimize caching performance.

S3 transfer acceleration .. how is this different from cloud front

Any object size limit in cloud front ? know the answer to this.

**ARCHITECTURE**

Understand ASG’s - The different scaling policies. Scheduled Scaling, when would you use..? Target Scaling, when would you use..?

What configuration elements are configured in a LC/LT vs ASG

SQS as a decoupling architecture - allows one part of an architecture not to be held up by another.

S3 events … how do they link in with SNS and SQS.

If you want TWO different things to happen when an object is uploaded to s3 ..how is this architected … one SNS, 2 queues subbed. Make sure you understand this architecture.

How to achieve HA in region - ALB + EC2

How to achieve Global HA … S3 transfer acceleration, cross region replication, cloud front + S3

How does R53 work, how does it integrate with other services Latency/Geo DNS routing/

SQS vs Kinesis … there was a question about picking between the two. Be really sure on HOW to pick between. Make sure you are REALLY clear on this one, and ideally make it instinctive.

**IAM, ACCOUNTS AND SECURITY**

Detailed knowledge of Users, Groups, Roles - what each one provides, which ones you can login too, which ones you can assume. WHich can have policies. WHich have long term keys, which have short term keys.

policy 1 - ec2:\*, IAM READ,DS:\*, logs read, policy 2 - deny DS:delete, What is the result … can DS be deleted ?

Giving cross account permissions to S3 bucket … easiest way

Can you move an existing account in an ORG, what about between ORGS?

Understand AWS organizations - features, benefits, RAM

Service control policies - how they can be used to restrict access from a single management location.

Know the Process to invite accounts to an ORG

Cross account permissions, vs Cross account roles, via making identities in account - when and where, security, admin overhead etc.

KMS - when to use KMS, vs S3 encryption - don’t want to manage keys, but want to control access.

Securing the root account - strong password and MFA

How WAF integrates with services … applying an ACL

How to add white lists and blacklists

What do you change … the stuff on the ACL, not the ACL on the service.