

AB1 Study Guide

From Ilan's AB1

Slide	Question	Answer
What is AWS	We are already a big company. We already have big data centers. Why would we use AWS? Seems like it is catered more towards start ups.	Because we do the undifferentiated heavy lifting for you, it allows you to bring back your attention for creating services that differentiates your business.
Key Drivers	Rent vs. Own	If it's baseline workload, then own with price discount. If it's infrequent, then rent for hours, or weeks.
	Overwhelming number of services	We offer a lot of training - 11 certifications - and other SA's, Account teams, follow up meetings, and even our partner networks.
Architecture	Sync Replication between regions or AZ's?	AZ: Sync Re. Regions: Async Rep. failover capabilities* over RDS
	Taking advantage of regions and AZ's when designing	3 guidelines: Latency goal for users (location of users), DR requirement, Residency or Governance rules that requires your data to stay in one certain region (like GDPR)
	No region in Russia?	You can use CDN or AWS outpost
	Content Delivery Network	You can push static data like images, audio or video files. Brings closer presence to users. However, CDN does not have any compute powers.
Services		
Ecosystem	If I run one of the marketplace products, who do we call for help?	ISV provides support. We provide integrated platform and billing
Compliances	Artifacts help you achieve your own certifications within AWS	
Responsibility	AWS is responsibility for the architecture.	
	Edge location security and compliances?	CDN, DNS (Route 53), Lambda at edge
Ref. Arch		Why is this important to you? for more information.
		Fail over can refer to HA and DR, really depends. I have a web server that's across 2 AZs with load balancer. 1 Webserver goes down, and my load balancer requests from another AZ's.
		If your primary DB goes down, then FO is HA. RDS itself will take a standby and promote to master, and DNS. Regions it's Disaster Recovery RDS multi AZ failover. > Amazon docs!

From Brandon's AB1

Slide	Question	Answer
Services	How long does migration take?	SA's and Professional Services Teams are here to identify the best practices for migration. Every customer starts small, pick a particular workload. Stages of Adoption. Choose what you need.
		S&P migrated 150 applications - mission critical like ratings - workload in 8 months
	Highest Complexities in Financial Services?	Specific Compliances, Hardware, Mainframes, Low-Latency Sensitive applications legacy type of solutions. You can't lift and shift. You have to rearchitect it to move/emulate. In general, we see customers moving very wide variety of workloads to the cloud. However, there are certain applications that may be more challenging - not impossible - to move to the cloud. Super low latency application (Micro seconds): High frequency trading applications.
	AIX Workloads? Lift and Shift? or try to rearchitect?	What's your drive to move to the cloud? For example, if you are in a position where you have to get out of the data center. Lift and shift. But if you want to optimize your application, agile, and taking advantage of cloud elasticity, managed AWS services, then they would rearchitect. *why would you rearchitect if you want to take advantage of AWS services.
	Going Open source for new apps (cassandra Databases)	Manage Cassandra. AWS offers various open source techs that you can deploy on top of
	Locked in?	No. Open Source Techs are Open Source Techs. There are portability in our services. Leveraging containers. You can build within the containers
Ecosystem	Microsoft Licenses, can we bring to cloud for cost saving?	Depends. Licensing Agreement with AWS for portability. Many of our customers are running windows on AWS. Bring in Licensing Specialist for viable migration path for interest
Responsibility	Built in Encryption	Depends. You can leverage KMS, or decide on CSE or SSE for specific services
Compliance	PCI Workloads. How would compliance work on AWS	You can build PCI compliant workloads, but you will be responsible for configuration on top of the service.* QSA Audit and AWS Certification
	AWS services are compliant and but application that are deployed on top are responsible for customers.	Static Architecture is too costly for cloud vendors.
	dev, bus, enterprise support	

Past Dry runs

Slide	Question	Answer
Intro	Capital One Data Breach?	AWS was not compromised in any way and functioned as designed. The perpetrator gained access through a misconfiguration of the web application and not the underlying cloud-based infrastructure. As Capital One explained clearly in its disclosure, this type of vulnerability is not specific to the cloud.
Services	Services	AWS Support offers a range of plans that provide access to tools and expertise that support the success and operational health of your AWS solutions. All support plans provide 24/7 access to customer service, AWS documentation, technical papers, and support forums. For technical support and more resources to plan, deploy, and improve your AWS environment, you can choose a support plan that best aligns with your AWS use case.

		choose a support plan that best aligns with your AWS use case.
Compliance	SOCs 1-3	While the SOC 1 report is mainly concerned with examining controls over financial reporting, the SOC 2 and SOC 3 reports focus more on the pre-defined, standardized benchmarks for controls related to security, processing integrity, confidentiality, or privacy of the data center's system and information
	GLBA	
		The perpetrator gained access through a misconfiguration of a third-party web application, and not as a result of the underlying cloud-based infrastructure. As Capital One explained in its disclosure, this type of vulnerability is not specific to the cloud, meaning it doesn't matter where the application was running, whether in the cloud or on premises, because the attack targeted the application and not the underlying infrastructure. Customers fully control the applications they build on top of AWS, as is the case no matter where an application is hosted. AWS services and infrastructure were not compromised in any way. More secure on the cloud than in on prem. We offer a lot of services for security. Not sure which exact interest Happy to have a follow up.

Slide	Feedbacks
Cloud Journey	Research about mainframes
	Research lift and shift
	Improve on KMS messaging
	Improve on Shared Responsibility
Ilya	KMS Messaging, the example. BYOK is Goldman. The terminology: key store. Cloud HSM. don't have the feature that you can keep your keys on prem. You can generate key material from on prem. The key material stays in the cloud. Its not that kms is calling from on prem. The keys are in the cloud. Use cases: it was a requirement for internal compliance that required to generate their keys on prem. then import them to KMS. Whats driving this requirement? it varies; because they need to use a certain type of hardware. because it allows them to quickly and definitely delete the key *RESEARCH deletion of keys and how CMK works. CMK is a container object. it contains a certain cyphertext which is the key. it can be generated in which KMS owns, or pointed to Key material that was imported into KMS. You still have* another key is pointing to another key that was stored into another system that was not generated by KMS HM. not instantaneous. No visibility. No inter look of how they do it. Its not less or more secure. Unless you know about that, avoid saying one is more secure. DO the steps. try creating a new CMK and you will see options!
	Certifications. do you have to pay to be compliant with certifications? Shared Respoinsibilty model needs to be crystal clear. Certifications tie directly with shared responsibility model. When you postion the SRM, when you talk about. Memorize the shared responsibility model!!! How do you know that AWS is doing what they said we were going to do? Certifications We have procedures and controls in place in part of the SRM. PCI is a good example. The infrastructre (underlying services) AWS provides the 3rd party auditing, but for applications, they need to do themselves. GDPR is not a compliance program, we say that we are compliant with the globe. Implemented processes we have. they are all consistent. Take a look at the GDPR page, look at the wording. Only the AWS services are GDPR ready. Our services can be used and ready for GDPR. Customers can use our services to help them comply with the GDPR compliance.
	Licensing specialist? As an SA, you own that. You navigate and own all the technical relationships for support. I will coordinate that resource. it undermines you. *Oracle*
	Partner messaging needs to be cleaned up a bit. Partner relationships work. If something is wrong, then aws provides the best effort and support guidance, but beyond 400 level, you reach out to Oracle. licensing agreement. Can't be so absolute. Oracle related, but it's with misconfiguration with Oracle with EC2 instance. For Enterprise independent vendor.
Cloud Journey	don't spend too much slide on the slide. It's not linear. In general, there are 4 key phases of adoption, and a lot of enterprises follow, but it's not like you MUST follow this pattern. It depends on your goals. No focus on migrations if you only want to take advantage of the innovation. The beginning parts are important. Want to build a strong foundation in terms of government and requirements.
	Where should we start? It's always good to start building out ur landing zone. Understand early on what your goals are so we can customize your journey to get you to your goals the most effectively.
	Mainframe one: BIG one!! It's not the question that you can't migrate mainframe applications to the cloud. You can't lift and shift the hardware mainframe natively onto the cloud. Our tools like MigrateCode like java migrates to unix!! No mainframe as a service. We have specialists for migrating mainframes to position mainframes that could run with AWS with the right resources and people in place for that.
	Phrases like "i know from research" just say im not sure and do more research.
Overall	Getting there. Being able to take questions better, hold your position, terminology and annoucing good job with regions and AZ's. Confidence drops. You can see it in your face. Don't give away your confidence. When someone asks a question and and you don't know? don't waste time. Security & Compliance: KNOW THAT. How is it different from on-prem? good! How do you enforce security of/in the cloud? How does support work? SA's are pre-sales at free cost. We are not preminary contact of escalation. Cost? flat rate or \$30,000/mo. basic model: 24 hr. SLA. email only. Entprical: 15 min for mission critical. Ran out of time. PCI date in the cloud. Goldman Sachs marqus. PCI compliant workloads (Capital One. mobile banking application). Not all services are ready for all regulations. If customer needs help with compliance, then they need to contact partners, or pro-serve. Compliance: 3rd party tells you that you are abiding by the regulations. AWS artifacts + how they enabled encrypton. How all workloads need to be compliant. if they don't have cetain layers of data. It's the same things over agian: confidence. Don't say UM too much. Know how to persent the services slide. Start slow. Have examples for each of the categories.

1. Andrew: Dow Jones - good! Direcrty referenced him!! Elasticity.

2. Improvement: big scale!! stay away from [Amazon.com - in 2014, we were adding enough capacity to power amazon.com when it was a 7 BB business](#). | Golman Sachs Grids Deployment. AZ no pyramid visual!! Start right to left. Data centers and AZ then Regions!! Answer the prod vs. DR comparison question!! multi AZ's give high availability.
3. Julie: Goldman Sachs!! example of talk track: GS is comfortable with our security. is comfortable bank safe deposit box of the cloud. Treat China as a stand alone zone, isolation. Availability Zone explanation!! Just so that you can work the prospect through. Good examples!!
4. David: Good 6 values adds!! Good good good!! Understand better about the question. Question about Capacity and Guarantee. Platform is scalable but there are limitations to it. We ask a second or third questions. Dive Deeper!!
5. you have to have a separate aws account to operate in AWS. Technically not even aws employees. Have to have a legal entity to operate in china. If you are interested in we - isolated region.
6. CPU can burn out, memory can fail, storage device, network switch goes out on web app.
7. 100% not sure. Ill research and get back to you. Absolutely expect to get a question that you don't know.
8. HA vs. DR: HA is being able to continue my workload even if i have certain failures/ If loose a web servers, always rub 2. Databases primary and stand by in another AZ. Do more research on DR vs. HA. DR: if i have a big event like major catastrophe, (business continuity) no expectation to instantaneously recover from other regions. You can achieve HA with multiple availability zones, but not cross regions. | what do you mean Disaster Recovery? data centers being 250-500 miles apart. Worried about regional outage? Really depends by your your requirements and how you define disaster recovery.
9. Sync replication: when your client acknowledges my write doesn't get acknowledged until the data has been copied/propagated to replica. put statement will not say successful unless copied onto both. | Async: happening behind the scenes. when I write to the primary, I get an ack back. Behind the scene, you don't have to wait for the acknowledgment. Ramification of waiting to write to stand by | between Az's we can do synchronous replication (less than 2 milli seconds) but if you go between regions: DO A SIMPLE LATENCY TEST BETWEEN TWO REGIONS. LIKE ONE INSTANCE IN EACH 2 REGIONS. TRY TO CONNECT THEM (CREATE INTO AN ACCESSIBLE) then PING two Machines. going to be a lot more than 2 milliseconds. → always asynchronous. synchronous replication allows fail-over from primary to secondary data storage to occur nearly instantaneous, to ensure little to no application downtime. However as noted above, it requires the bandwidth of a LAN between the servers, possibly with an extended LAN in two geographically remote computer zones and may also require specialized hardware (depending on the implementation).

Julie's Help

- Surveillance use cases. When FINRA spoke at our NY summit last June, it talked about how they use various AWS services to monitor 155B market events per day. That was its peak as of last year. With the U.S. securities market volatility hitting record highs – FINRA says that it has seen 2-3 times increase in market volume since March. (<https://www.forbes.com/sites/moorinsights/2020/05/20/aws-covid-19-and-the-need-for-speed-in-time-of-crisis/#57d86ac87ad8>) While this represents a record-setting peak, AWS's automatic provisioning capabilities enabled it to process the surge, and then scale it back without any human effort required.
- Another example is AQR Capital Management who uses core application services from AWS to automatically scale compute while lowering costs. AQR can backtest 20,000 equities times 20 years' worth of data without job schedulers and queues and was able to run a trading model across 500 compute cores for \$15!
- Is the Cloud Secure? • Same security isolations you would find in a typical data center. • AWS has achieved internationally recognized certifications demonstrating compliance on 3rd party assurance frameworks such as ISO 27017 for cloud security, ISO 27108 on cloud privacy and SOC1, 2 and 3. Customers can be PCI and HIPAA compliant on AWS and we have many public sector certification like FedRamp for government workloads. • Enabling Customers to secure their environments (encryption & authentication) along with AWS security partners (policy management, security monitoring, data protection).
- Roy Joseph, Managing Director at Goldman Sachs – As Data Privacy of their client data is paramount - they use bring your own cloud security keys to secure their environment. "Working with AWS is like having a safety deposit

box in a bank.”

- DTCC build a Derivatives Warehouse on AWS. They looked into putting this on-prem and realized it would cost \$4mill in capex. They had a team of engineers who worked over the weekend to put together a simple prototype on AWS and they realized it would work. Initially (2015) it cost them around \$3k/month; now this costs around \$1k/month to run (separate from the storage that has grown).
- That's a great way to pivot - andrew asks you a security question you answer it and give the customer example to validate.

go through the our infrastructure document, and how other people use our applications like RDS in multiple regions. Practice more!! You should couple of MB's,

Compliance Testimonials:

<https://aws.amazon.com/compliance/testimonials/>