1. Understand bastion hosts, and which subnet one might live on. Here's a good, brief summary of bastion hosts taken from http://cloudacademy.com/blog/aws-bastion-host-nat-instances-vpc-peering-security/ - "Bastion hosts are instances that sit within your public subnet and are typically accessed using SSH or RDP. Once remote connectivity has been established with the bastion host, it then acts as a ‘jump’ server, allowing you to use SSH or RDP to login to other instances (within private subnets) deeper within your network. When properly configured through the use of security groups and Network ACLs, the bastion essentially acts as a bridge to your private instances via the Internet."

<http://cloudacademy.com/blog/aws-bastion-host-nat-instances-vpc-peering-security/>

3. Know the difference between Directory Service's AD Connector and Simple AD. "Use Simple AD if you need an inexpensive Active Directory–compatible service with the common directory features. AD Connector lets you simply connect your existing on-premises Active Directory to AWS."

<http://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html>

4. Know how to enable cross-account access with IAM. "To delegate permission to access a resource, you create an IAM role that has two policies attached. The permissions policy grants the user of the role the needed permissions to carry out the desired tasks on the resource. The trust policy specifies which trusted accounts are allowed to grant its users permissions to assume the role. The trust policy on the role in the trusting account is one-half of the permissions. The other half is a permissions policy attached to the user in the trusted account that allows that user to switch to, or assume the role."

<http://docs.aws.amazon.com/IAM/latest/UserGuide/idrolesterms-and-concepts.html>

5. Have a good understanding of how Route53 supports all of the different DNS record types, and when you would use certain ones over others.

<http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html>

<https://aws.amazon.com/route53/faqs/>

6. Know which services have native encryption at rest within the region, and which do not.

<http://jayendrapatil.com/aws-storage-gateway/>

7. Know which services allow you to retain full admin privileges of the underlying EC2 instances, or conversely know which ones definitely do not.

8. Know When Elastic IPs are free or not. "If you associate additional EIPs with that instance, you will be charged for each additional EIP associated with that instance per hour on a pro rata basis. Additional EIPs are only available in Amazon VPC. To ensure efficient use of Elastic IP addresses, we impose a small hourly charge when these IP addresses are not associated with a running instance or when they are associated with a stopped instance or unattached network interface."

<https://aws.amazon.com/ec2/pricing/>

9. Know what four high level categories of information Trusted Advisor supplies.

<https://aws.amazon.com/premiumsupport/trustedadvisor/>

10. Know how to troubleshoot a connection time out error when trying to connect to an instance in your VPC. "You need a security group rule that allows inbound traffic from your public IP address on the proper port, you need a route that sends all traffic destined outside the VPC (0.0.0.0/0) to the Internet gateway for the VPC, the network ACLs must allow inbound and outbound traffic from your public IP address on the proper port," etc.

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html#TroubleshootingInstancesConnectionTimeout>

11. Be able to identify multiple possible use cases and eliminate non-use cases for SWF.

<https://aws.amazon.com/swf/faqs/>

12. Understand how you might set up consolidated billing and cross-account access such that individual divisions' resources are isolated from each other, but corporate IT can oversee all of it.

<http://jayendrapatil.com/aws-consolidated-billing/>

13. Know how you would go about making changes to an Auto Scaling group, fully understanding what you can and can't change. "You can only specify one launch configuration for an Auto Scaling group at a time, and you can't modify a launch configuration after you've created it. Therefore, if you want to change the launch configuration for your Auto Scaling group, you must create a launch configuration and then update your Auto Scaling group with the new launch configuration. When you change the launch configuration for your Auto Scaling group, any new instances are launched using the new configuration parameters, but existing instances are not affected."

<http://docs.aws.amazon.com/autoscaling/latest/userguide/LaunchConfiguration.html>

14. Know which field you use to run a script upon launching your instance.

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html#user-data-shell-scripts>

15. Know how DynamoDB (durable, and you can pay for strong consistency), Elasticache (great for speed, not so durable), and S3 (eventual consistency results in lower latency) compare to each other in terms of durability and low latency.

<https://d0.awsstatic.com/whitepapers/AWS%20Storage%20Services%20Whitepaper-v9.pdf>

16. Know the difference between bucket policies, IAM policies, and ACLs for use with S3, and examples of when you would use each. "With IAM policies, companies can grant IAM users fine-grained control to their Amazon S3 bucket or objects while also retaining full control over everything the users do. With bucket policies, companies can define rules which apply broadly across all requests to their Amazon S3 resources, such as granting write privileges to a subset of Amazon S3 resources. Customers can also restrict access based on an aspect of the request, such as HTTP referrer and IP address. With ACLs, customers can grant specific permissions (i.e. READ, WRITE, FULL\_CONTROL) to specific users for an individual bucket or object."

<https://aws.amazon.com/s3/faqs/>

17. Know when and how you can encrypt snapshots. "Public snapshots of encrypted volumes are not supported, but you can share an encrypted snapshot with specific accounts."

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

18. Understand how you can use ELB cross-zone load balancing to ensure even distribution of traffic to EC2 instances in multiple AZs registered with a load balancer.

<http://jayendrapatil.com/tag/elastic-load-balancer/>

Please correct me if I've included errant information, and happy studying!

how would you allow users to long into the AWS console using active directory integration. Here is a link to some good reference material. <https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/>

what instance types supported encryption, migrating from unencrypted EBS volume => encrypted EBS volume) <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

* Bastion host scenarios
* Changing instance type in an autoscaling group. Where does that get done?..Launch Configuration

Public/Private subnet scenarios. By default can they connect to each other?

The Put/Deletes is a guaranteed question.

/32 subnet doesn't exist 🡺 this is an IP address

Make sure to understand well the application and implications of IAM roles.  🡺 sometimes the exam may have 5-6 questions on this topic

* Make sure to know which services are available globally, which ones are per region and whats only per AZ
* Set and break cloud watch for all the services and understand how to implicate logging, SNS etc..
* Understand the use of services like Kinesis, DynamoDB... etc..
* Make sure to understand the difference and impact of using SG vs ACLs. Just understanding wont be enough, you need to think of practical situations cause the questions will come like < server 1 can ping server 2 but server 2 cant ping server 1, what could be the cause? >
* Understand practical situations of Multi AZ

Kinesis - Question related to Shipping and coordinates being updated 3 times every minute.. this is usually Kinesis-DynamoDB choice of architecture.

S3 - Bucket policy, ACL - how can you give readonly access to all the objects in the bucket. (Do you make a run time changes via policy, or update all ACLs to public, Update bucket policy to public.. e.t.c.)

S3 - version control and 2 factor IAM for accidental deletion and recovery of data

Know that which AWS components fall outside the Region (Route53, DB cross region replication, IAM) & With in region (ELB, RDS, Security groups), One Subnet- one availability zone.

Multiple EBS backed storage snapshot, recovery to other regions scenerios.

Avalability of volume encryptions to all available for - All EC2 types, All ebs volume types, Only to ebs-backed volumes..

Retaining of data on Instance store volumes is a definite question.

By default all subnets can communicate each other in a VPC.

I was bumped with how to handle forecasted traffic spikes 5 choices were given choices - Desired Capacity, (I will update with other 4 choices later .. dont remember now.. )

Another question on elastic load balencer - Do you enable "accesslogs or cloud watch metrics" for monitoring all the information every 5 minutes to analyse them later for detailed analysis on the traffic. I choose accesslogs. (http://jayendrapatil.com/tag/elastic-load-balancer/)

* You can use a NAT gateway when you have burstable traffic e.g 200Mb to 3Gb
* Know how to encrypt data at rest in S3. (SSL DOES NOT ENCRYPT DATA AT REST)
* You CAN NOT change instances on autoscaling group instead, create a new one
* By default security groups are allow all outbound. read the questions carefully they may say all outbound have traffic is denied on the security group
* It leaned extremely heavily on VPCs, and networking concepts in general, including elastic IPs, NAT, IGW, public/private subnet concepts, security roles, network ACLs, etc. Also learn how bastion hosts work.
* Thoroughly understanding building highly available web tier systems is a must.
* 6. Dynamo DB came up a surprisingly high number of times. It drilled me a few times asking for durable, high performance storage of key pairs, session info, small text items, etc.
* 7. EBS features, such as encryption, snapshotting, copying, etc was covered in probably 5 questions. Definitely understand the minutia of how to work with EBS volumes.

One question on Elastic Beanstalk (when to use it)

10. One question on Chef, one on Lambda, but super easy questions.

11. One STS question (I probably got it wrong). Asked something about why when you deploy an Ubuntu instance it does show up in the cluster.

12. Know what services cross regions, availability zones, and which ones don't

* **Amazon Simple Storage Service (Amazon S3)** - most asked questions were basic just need the basic understanding with few other related service like CroudFront, Storage Gateway, **EVENTUAL CONSISTENCY** was waiting there to increase your score in exam, so please read it and please read scenarios or create one yourself for using S3. Do know it’s durable and scalable. Please understand when to use IAM, Bucket Policies, and Access Control Lists (ACLs). Storage Class with Lifecycle policies, please do remember in some scenarios you will upload all files to S3 IA - Infrequent Access as per scenario. I was given a scenario in which data was on site and now the company want to use AWS for the storage and backup purposes, and every single report was of 1GB and they were receiving multiple reports in a month but once report is collected, only 10% was required to view by the company per 30 days but data needs to be available quickly and after that it’s never used but needed to be backed up for company regulatory conditions. So in this use S3 IA for storing infrequent data and apply lifecycle policy to transfer to Glacier for archival. For optimal PUT performance use **some randomness** in the key name prefixes, the key names, and the I/O load, will be distributed across multiple index partitions. For confidence's sake, just be aware that the S3 200 code comes with an MD5 checksum in the success message.
* **Amazon Elastic Compute Cloud (Amazon EC2),** Amazon EBS Storage and difference between EBS and Instance store(ephemeral storage), this can be asked other way around EBS-Backed-AMI and S3-Backed-AMI, **Amazon Autoscaling**, please note that there are 4 Autoscaling plans namely, Main Current Instance Levels, Manual Scaling, Scheduled Scaling, and Dynamic Scaling. Remember if you want AS to launch different AMI’s than the one set up please remember you can’t modify Launch Configuration, which is the template for AS you **must** create new LC and then assign it to your AS, all the new instances will be launched with new AMI and all the previous one will still be running. Remember when to use On-Demand, Reserved and Spot instances. Placement Groups I got 2 questions. Elastic IP when you are charged? Well you’re charged when you have not associated with the instance or your instance is stopped or you have assigned more than 1 EIP to one instance, then you’re charged minimal fee for it. Why? Because IPv4 addresses are getting depleted so AWS wants you to use it efficiently. Auto Scaling Lifecycle Hook, didn’t know before today’s exam so please have a look by googling it. EBS encryption please know about encryption more than little bit, all instance type doesn't support EBS encryption. Know that to run a script upon launching your instance even with Auto Scaling, you would enter the script in the instance's User Data field. How can we take the snapshot of the RAID volumes with efficiency.
* **Virtual Private Cloud (Amazon VPC)** I will say just one thing know VPC in and out there is possibility of losing points if you miss any single VPC offerings and how they work. Please know if an instance is configured properly on custom VPC with Internet Gateway routing the traffic to internet in public subnet and Security Group and Network ACLs defining right ports for connection and still not able to connect to your instance consider assigning Public IP/Elastic IP. Know what does stateless and stateful are, I got a scenario based question not straightforward question that which is what, so know well how SG works, if you allow any INBOUND rule, OUTBOUND is defined automatically while not the case in NACLs you have to define both separately. Please know how Virtual Private Network (VPN) connection works and Direct Gateway for **private connections,** don’t mix with PRIVATE SUBNET, you can use public subnet with VPN. NAT is no miss guys. Remember AWS recommends using NAT gateways because it’s fully managed so you don’t have to launch any instance or manage network throughput, all of this managed by AWS. While if you using a NAT instance and you have configured it all correct but when connecting your private subnet instance to internet for outbound traffic it’s connecting, but WHY? You forgot to Disable Source/Destination checks flag, exactly this was question on my exam. Wait do you know what we can use other than NAT instance and NAT gateway to give secure outbound internet connect to our private subnet, that’s bastion host or call it jump server, and it resides in **public subnet,**got 2 questions on this single point with different scenarios.
* **Identity and Access Management (IAM)** most of you may not paying attention to this topic too much but in exam it was one of the main topic. IAM users, groups, roles. Everyone knows this but there is much more which IAM can do and you need to know so that you don’t scratch your head in exam. Please note you can enable cross account access. I don’t remember exactly what scenarios were but it was not simple that you think of, so please go through this topic very well. I do remember one scenario where you hired third-party to access your bucket and transfer data to Glacier so what will you use? IAM or Bucket Policies, there were 4 options but two for IAM with different scenarios and two for Bucket Policies. Please do look at IAM federation with other services.
* **Databases, Relational Database(Amazon RDS), NoSQL Database (DynamoDB) and Data Warehousing(Redshift)** know them well especially firm understanding what you can do and what you can’t do with each of these and AZs are for **failover** not for performance and read replicas are to increase the **read performance** if the website needs much more reads than writes. Expect at least 1-2 questions from each of these DB types. How to increase storage sizes and how they affect the performance.
* **Application Service** such as **Simple Queue Service (SQS)**, **Simple Notification Service (SNS)** what protocols it support? and **Simple Workflow (SWF)** know when it is used i.e. for works which need coordinating task across the application service.
* **Route53** how weighted latency work? To spread even traffic to instances/ELB. Keep in mind AWS use **ALIAS** record for zone apex (naked domain) not CNAME.
* **Amazon Elasticache** there were 2 question on the exam, sorry don’t remember the question or scenario.
* **Amazon Storage Gateway** 1 Question
* **Amazon CloudFront** - 2 Questions
* **AWS Directory Service** - 2 Questions
* **AWS CloudTrail** - 1 Question
* **Amazon Kinesis** - 2 Questions
* **AWS Import/Export** - 1 Question
* **Elastic Beanstalk** - 1 Question
* **AWS Trusted Advisor** - 1 Question, it was about identifying 4 inspections available on Dashboard i.e. Cost Optimization, Performance, Security, Fault Tolerance.
* **Amazon Elastic Container Services** - 2 Questions
* **Amazon API Gateway** - 2 Questions
* **Amazon Security Token Service(STS)** - 1 Question
* **Amazon AMI** - 1 Question
* **AWS Whitepapers** - 8-10 Questions were solely from the following 3 Whitepapers: [Security on AWS](https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf), [AWS Risk and Compliance](https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf), and [Architecture Best Practices](https://d0.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf).

One good news, there was no such questions where you have to know the numbers, like how many EC2 instances you can launch by default? What maximum EBS volume you can allocate? What is S3 durability and blah blah…

How I prepared myself?

Ryan's course is well structured and defined for AWS CSA-A so go through each and every single details. Exam Tips are simply amazing for overview before going for exam. Additionally all the labs, you must practice it until you understand what you doing and why and how.

I also prepared myself from [Official Study Guide](https://www.amazon.com/Certified-Solutions-Architect-Official-Study/dp/1119138558), though there are more than 400 pages book and a lot boring but beneficial and aid in your deep understanding and it includes more than 300 questions which includes detailed answers and they are designed in exam pattern so you get good beforehand practice to tackle to nervousness of exam. Few questions were from the Official Study Guide questions though.

After all these learning sources, I used some other questions app because remember you need a lot of practice to be able to understand the concepts and you can also retain your information this way so go ahead and practice more.

I used acloud guru [app](http://exam.acloud.guru/) and study guide quizzes. I also used acloud guru [forum](https://acloud.guru/forums/aws-certified-solutions-architect-associate" \t "_blank)to have the latest information on contents, quizzes, topics, and scenarios appearing in exam and honestly I was able to correct few tens of questions only because of this.

In last I went through FAQs, Whitepapers, and Jayendra Patel’s [Exam Cheat Sheet](http://jayendrapatil.com/tag/cheat-sheet/). Recommended FAQs are: [Amazon EC2](https://aws.amazon.com/ec2/faqs/) | [Amazon S3](https://aws.amazon.com/s3/faqs/) | [Amazon VPC](https://aws.amazon.com/vpc/faqs/) | [Amazon Route 53](https://aws.amazon.com/route53/faqs/) | [Amazon RDS](https://aws.amazon.com/rds/faqs/) | [Amazon SQS.](https://aws.amazon.com/sqs/faqs/)

There were 7 questions on **lambda** functions. Understand how they can be provisioned, secured and optimised. Rayn please add more content on lambda. I lost about 4 marks on this.

5 questions on ECS. You must understand how the are provisioned, secured, and integrated with other services. Deep dive into EC2 Container Service. Lambda and ECS service made up about 15%.

2 questions on S3 backed instances. I assumed they were instance stores. Look into this for easy marks.

VPN vs Direct Connect. How do you introduce redundancy, resilience and recovery?. Understand their performance characteristics.

Throughput optimised HDD vs General purpose IOPS. What are their preferred use cases? Understand their cost vs bursting characteristics.

Security group VS Network ACL. Understand their combined effect. The key to distinguishing them is when you see the word "denied" in one of the answers (ACL).

1) EBS Snapshots and its impact on the performance while the snapshot is in progress

2) S3 encryption

3) VPC subnets and troubleshooting the connectivity issues

4) Connecting VPC and corporate network

5) Backing up in-house storage to the AWS cloud - Storage Gateway

6) Route53 - CNAME, Alias and a record set

7) RDS - Read replica vs standby

8) ELB - Multi Zone load balancing and how it load balances across EC2 instances running in multiple AZs with different number of instances in each AZ

9) ACL vs Security groups

10) Which services provide root access to the underlying operating system - EC2, EMR, BeanStalk and OpsWorks

11) CloudWatch vs CloudTrail

12) Well Architected Framework - Security, Cost, Performance and, Reliability of the solution

13) VPC Peering

14) EC2 Placement Groups

15) Bastian/Jump Host

* SNS recipients 1 question  
  -Having root access on which services. Needing to choose 2
* Lots of VPC questions about how to allow SSH, NAT Gw, Bastion host and of course source/destination disable on Nat instance. Wanting to have high availibilt with secure access on public bastion host.
* A question where you have a web app that need to have high avaiable, asking how to autoscale with load balancers
* S3 at rest encryption and another question about EBS at rest cryption
* A question I was unprepared was what Ami should certain instance use: instance or EBS backed, hardware virtual machine or para virtual .
* Consolidated billing and resouce management like  
  https://acloud.guru/forums/aws-certified-sysops-administrator-associate/discussion/-KZLTFIvKuZYbgbZK-kx/?answer=-KcRJibN4zIEqnlmtTWt  
  -Auto scaling Launch options , where to select ami and where to put user scripts

I passed my exam today with 87% but there was one topic which is not covered in course . It is about Auto scaling Lifecycle hooks . My advice is to study about it before going into exam

**1.** PV EBS and instance store : C3 M3

instance types require an HVM AMI : ALL

**2.** bastion hosts

* sit in public subnet
* backed by SSH or RDP
* SSH or RDP to login into the instances
* Launch an EC2 instance as you normally would for any other instance.
* Apply your OS hardening as required
* Set up the appropriate security groups (SG)
* Implement either SSH-Agent Forwarding (Linux connectivity) or Remote Desktop Gateway (Windows connectivity).
* Deploy an AWS bastion host in each of the Availability Zones you’re using.
* outbound connection in bastion : Security group of private subnet

3. AWS Directory Service

AWS Directory Service provides multiple ways to use Amazon Cloud Directory and Microsoft Active Directory with other AWS services.

Use Amazon Cloud Directory if you need a highly scalable directory store for your application’s hierarchical data.

AWS Directory Service for Microsoft Active Directory (Enterprise Edition) for a feature-rich managed Microsoft Active Directory hosted on the AWS cloud.

Use Simple AD if you need an inexpensive Active Directory–compatible service with the common directory features.

Another option, AD Connector, lets you simply connect your existing on-premises Active Directory to AWS.

4. cross-account access with IAM

* To delegate permission to access a resource, you create an IAM role that has two policies attached.
* The permissions policy grants the user of the role the needed permissions to carry out the desired tasks on the resource.
* The trust policy specifies which trusted accounts are allowed to grant its users permissions to assume the role.
* The trust policy on the role in the trusting account is one-half of the permissions.
* The other half is a permissions policy attached to the user in the trusted account that allows that user to switch to, or assume the role

5. Have a good understanding of how Route53 supports all of the different DNS record types, and when you would use certain ones over others.

If an alias resource record set points to

* a CloudFront distribution
* an Elastic Beanstalk environment
* an ELB load balancer
* an Amazon S3 bucket

you cannot set the time to live (TTL)

6. Which of the following services natively encrypts data at rest within an AWS region?

* AWS Storage Gateway
* Amazon Glacier

AWS Storage Gateway : allows to integrate on-premises IT environments with Cloud Storage

7. AWS provides the root or system privileges only for a limited set of services, which includes

* Elastic Cloud Compute (EC2)
* Elastic MapReduce (EMR)
* Elastic BeanStalk
* Opswork

8. when Elastic IPs are free ?

* when they are assigned
* when they are not assigned there will be some charge involved.

9. Know what four high level categories of information Trusted Advisor supplies.

* Cost Optimization
* Performance
* Security
* Fault tolerance

(Remember CaPe town,San Francisco are trusted towns )

11. SWF

* Workflow, which is the automation of a business process
* Each workflow runs in an AWS resource called a Domain
* A Decider implements a Workflow’s coordination logic
* SWF Coordinate synchronous and asynchronous tasks which are distributed and fault tolerant
* SWF uses deciders and workers to complete tasks
* Markers enable you to record information in the workflow execution history that you can use for any custom or scenario-specific purpose.
* Workers and Deciders are both stateless

more details : http://jayendrapatil.com/aws-swf/

12. consolidated billing

* enables consolidating payments from multiple AWS accounts (Linked Accounts)
* Payer account is billed for all charges of the linked accounts.
* Payer account cannot access data belonging to the linked account owners
* However, access to the Payer account users can be granted through Cross Account Access roles
* The payee account will send a request to the linked account to be a part of consolidated billing

Advantages :

One Bill

Easy Tracking

Combined Usage & Volume Discounts

Free Tier

13. Auto Scaling

* Autoscaling launch configuration which allows you to select an

AMI

Instance type

IAM role (optional)

Security group

Key pair file

* Autoscaling group configuration allows you to select AZ to be used to launch the EC2 instances with the selected launch configuration , Desired capacity
* Auto Scaling can span across multiple AZs, within the same region
* Auto Scaling group determines the health state of each instance by periodically checking the results of EC2 instance status checks
* BEST COMBO : Auto Scaling, Amazon CloudWatch and Elastic Load Balancing
* Auto Scaling groups cannot span multiple regions.
* Auto Scaling terminates the instance first and then launches a new instance

Scaling types : Manual , Scheduled , Dynamic

Termination Policies

* selects the AZ, in multiple AZs environment, with the most instances
* selects the AZ with instances that use the oldest launch configuration
* unprotected instances closest to the next billing hour

more details : http://jayendrapatil.com/tag/auto-scaling/

14. Userdata is used to run scripts

15. comparisions

* DynamoDB (durable, and you can pay for strong consistency)
* Elasticache (great for speed, not so durable)
* S3 (eventual consistency results in lower latency)

17. Encryption

EBS Encryption

* supported with all EBS volume types
* Snapshots of encrypted volumes and volumes created from encrypted snapshots are automatically encrypted using the same volume encryption key
* EBS encryption uses AWS Key Management Service (AWS KMS) customer master keys (CMK) when creating encrypted volumes and any snapshots created from the encrypted volumes.
* Existing unencrypted volumes cannot be encrypted
* Transparent Data Encryption (TDE) can be provisioned for Microsoft SQL Server on Amazon RDS.
* Glacier provide encryption of the data, by default

AWS CloudHSM

* AWS CloudHSM appliance has both physical and logical tamper detection and response mechanisms that trigger zeroization of the appliance.
* Zeroization erases the HSM’s volatile memory where any keys in the process of being decrypted were stored and destroys the key that encrypts stored objects, effectively causing all keys on the HSM to be inaccessible and unrecoverable.
* AWS CloudHSM can be used to generate and store key material and can perform encryption and decryption operations,
* AWS CloudHSM, however, does not perform any key lifecycle management functions (e.g., access control policy, key rotation) and needs a compatible KMI.

more info : http://jayendrapatil.com/tag/encryption/

Brief Summary of exam Around 10-15 question Direct kind of questions (like where will you put your booting up scripts -user Data ...etc Around 5 question on what should be your source Dynamo/S3/elastic cache...etc. 3-4 question on VPC peering 1-2 question involving VPN 3-5 question on ECS 3-5 Questions on API gateway 2-3 questions on Security Couple of question on EBS Encryption 3-5 ELB+ Auto Scaling 1-2 CloudWatch vs. Cloud trail 1 Question on calculating the total cost when you use a Spot Instance ( like you got it for .20 then market rate went to .25 , after 90 minutes aws terminated your session , now how much you need to pay) 1-2 question on SQS or SWF is better for the current scenario In troubleshooting section ACL vs. Security group which one needs to be opened type? Couple of questions with lambda as one of the answers No Questions on workspaces , Cloud formation , Chef, Dynamo DB internals , Redshift , EMR , Route 53 ,Classic vs. Application LB Overall I feel course should focus a lot more on ECS + API gateway + Elastic Cache this will help to get around 10+ questions more correct.

Topics-

* vpc CIDR
* vpc routing amoung subnets
* vpc peering
* vpc flowlogs
* nat gateway and nat instance
* bastion host
* security groups and nacl
* spot instance pricing
* Cross-Zone Load Balancing
* application load balancer
* autoscaling termination policy
* autoscaling launch configuration
* route53 alias and CNAME record
* Storage gateway - stored volumes
* AWS import/export
* cloudtrail
* s3 storage catogeries
* s3 limits and capabilities
* STS, web federation and SSO
* cross-account access by assuming roles
* encrypting existing ebs volume
* decoupling application usig sqs
* which services can triger a lambda function
* benifits of using api gateway
* ways to protect s3 bucket and objects

**Questions on new topics :**

**Lambda**

1. AWS Lambda: Question were on : Events or services which can invoke a Lambda function (choices were SNS, Dynamo DB, Redshift, Cloud front and Load balancer) ... Read http://docs.aws.amazon.com/lambda/latest/dg/welcome.html for correct answer

2. You are using Lambda along with a web application. the application is expecting a spike. What changes would you do in the lambda function (cannot recollect all the choices but one of them was you would allocate more memory to lambda function)

\*\*ECS \*\*

1.How to give ECS access to an application without sharing the credentials. (Please read about IAM role usage in ECS)

\*\*Kinesis \*\*

Know the difference between Firehose and Streams. which one is used to stream the data ?

\*\*Cloud Trail and VPC log flows \*\*

Know What is used to audit the API calls and when VPC log flows are used

**Enhanced Network** - 1 Question

One quesiton on **CORS** which i was not able to comprehend. something is uploaded on s3/cloud front and it was throwing error. the question why ?

**IAM :** how can developers get access into production account wherein creation of users is not allowed

**Repeated questions :**

1. A company has configured and peered two VPCs: VPC-1 and VPC-2. VPC-1 contains only private subnets, and

VPC-2 contains only public subnets. The company uses a single AWS Direct Connect connection and private

virtual interface to connect their on-premises network with VPC-1. Which two methods increases the fault

tolerance of the connection to VPC-1? Choose 2 answers

A.Establish a hardware VPN over the internet between VPC-2 ana the on-premises network.

B.Establish a hardware VPN over the internet between VPC-1 and the on-premises network.

C.Establish a new AWS Direct Connect connection and private virtual interface in the same region as VPC-2.

D.Establish a new AWS Direct Connect connection and private virtual interface in a different AWS region than

VPC-1.

E.Establish a new AWS Direct Connect connection and private virtual interface in the same AWS region as

VPC-1

1. An existing application stores sensitive information on a non-boot Amazon EBS data volume attached to an Amazon Elastic Compute Cloud instance. Which of the following approaches would protect the sensitive data on an Amazon EBS volume?

a. Upload your customer keys to AWS CloudHSM. Associate the Amazon EBS volume with AWS CloudHSM. Remount the Amazon EBS volume.

b. Create and mount a new, encrypted Amazon EBS volume. Move the data to the new volume. Delete the old Amazon EBS volume.

c. Unmount the EBS volume. Toggle the encryption attribute to True. Re-mount the Amazon EBS volume.

d. Snapshot the current Amazon EBS volume. Restore the snapshot to a new, encrypted Amazon EBS volume. Mount the Amazon EBS volume (Need to create a snapshot, create an encrypted copy of snapshot and then create a EBS volume and mount it)

note: the answer options were bit different. you need to create a snapshot, copy it as escrypted snapshot and then make a volume out of it

3. Which of the following are true regarding encrypted Amazon Elastic Block Store (EBS) volumes? Choose 2 answers

a. Supported on all Amazon EBS volume types

b. Snapshots are automatically encrypted

c. Available to all instance types

d. Existing volumes can be encrypted

e. Shared volumes can be encrypted

4. A company is building software on AWS that requires access to various AWS services. Which configuration should be used to ensure that AWS credentials (i.e., Access Key ID/Secret Access Key combination) are not compromised?

a. Enable Multi-Factor Authentication for your AWS root account.

b. Assign an IAM role to the Amazon EC2 instance.

c. Store the AWS Access Key ID/Secret Access Key combination in software comments.

d. Assign an IAM user to the Amazon EC2 Instance.

5. Which of the following services natively encrypts data at rest within an AWS region?Choose 2 answers

a. AWS Storage Gateway

b. Amazon DynamoDB

c. Amazon CloudFront

d. Amazon Glacier

e. Amazon Simple Queue Service

6. You need to pass a custom script to new Amazon Linux instances created in your Auto Scaling group. Which feature allows you to accomplish this?

a. User data

b. EC2Config service

c. IAM roles

d. AWS Config

EC2Config services is used in Windows instance while User data is used in passing custom scripts to Linux instances

7. < this question was not repeated BUT a similar question was asked where in largest DB was already used and you were expecting a spike. i think the answer is to use elastic cache and read replica> Your company has HQ in Tokyo and branch offices all over the world and is using a logistics software with a

multi-regional deployment on AWS in Japan, Europe and USA. The logistic software has a 3-tier architecture

and currently uses MySQL 5.6 for data persistence. Each region has deployed its own database. In the HQ

region you run an hourly batch process reading data from every region to compute cross-regional reports that

are sent by email to all offices this batch process must be completed as fast as possible to quickly optimize

logistics how do you build the database architecture in order to meet the requirements?

A.For each regional deployment, use RDS MySQL with a master in the region and a read replica in the HQ

region.

B.For each regional deployment, use MySQL on EC2 with a master in the region and send hourly EBS

snapshots to the HQ region.

C.For each regional deployment, use RDS MySQL with a master in the region and send hourly RDS

snapshots to the HQ region.

D.For each regional deployment, use MySQL on EC2 with a master in the region and use S3 to copy data files

hourly to the HQ region.

E.Use Direct Connect to connect all regional MySQL deployments to the HQ region and reduce network

latency for the batch process.

8. You have a distributed application that periodically processes large volumes of data across multiple Amazon

EC2 Instances. The application is designed to recover gracefully from Amazon EC2 instance failures. You are

required to accomplish this task in the most cost-effective way. Which of the following will meet your

requirements?

A. Spot Instances

B. Reserved instances

C. Dedicated instances

D. On-Demand instances

Per the AWS Acceptable Use Policy, penetration testing of EC2 instances:

A.May be performed by AWS, and will be performed by AWS upon customer request.

B.May be performed by AWS, and is periodically performed by AWS.

C.Are expressly prohibited under all circumstances.

D.May be performed by the customer on their own instances with prior authorization from AWS.

E. May be performed by the customer on their own instances, only if performed from EC2 instances.

9. When creation of an EBS snapshot is initiated, but not completed, the EBS volume:

A. Can be used while the snapshot is in progress.

B. Cannot be detached or attached to an EC2 instance until the snapshot completes.

C. Can be used in read-only mode while the snapshot is in progress.

D. Cannot be used until the snapshot completes.

10. An instance is launched into a VPC subnet with the network ACL configured to allow all inbound traffic and deny

all outbound traffic. The instance’s security group is configured to allow SSH from any IP address and deny all

outbound traffic. What changes need to be made to allow SSH access to the instance?

A. The outbound security group needs to be modified to allow outbound traffic.

B. The outbound network ACL needs to be modified to allow outbound traffic.

C. Nothing, it can be accessed from any IP address using SSH.

D. Both the outbound security group and outbound network ACL need to be modified to allow outbound traffic

A customer is leveraging Amazon Simple Storage Service in eu-west-1 to store static content for a web-based

property. The customer is storing objects using the Standard Storage class. Where are the customers objects

replicated?

A. A single facility in eu-west-1 and a single facility in eu-central-1

B. A single facility in eu-west-1 and a single facility in us-east-1

C. Multiple facilities in eu-west-1

D. A single facility in eu-west-1

You have a video transcoding application running on Amazon EC2. Each instance polls a queue to find out

which video should be transcoded, and then runs a transcoding process. If this process is interrupted, the video

will be transcoded by another instance based on the queuing system. You have a large backlog of videos which

need to be transcoded and would like to reduce this backlog by adding more instances. You will need these

instances only until the backlog is reduced. Which type of Amazon EC2 instances should you use to reduce the

backlog in the most cost efficient way?

A. Reserved instances

B. Spot instances

C. Dedicated instances

D. On-demand instances

Will share more later in the day

1- Api gateway benefits

2- Api gateway wih lambda especially the ability of lambda to scale with the increase of load

3- api gateway with CROS feature

4- which services invoke lampda

5- ecs components

6- why ubunto container ec2 doesn't shown in the dashboard of ecs >>>> the answer is to install ecs agent for them

7- auto scaling termination policy

8- cloud watch based on cloud trail

9- vpc flowlogs ( chose when the instance inside the vpc and you want to cach the logs for the vpc )

10 - application loadbalancer dynamic mapping port

11- which services based on sts ( like saml v02 , roles )

12- decoupling applications >>>>> always SQS

13- enhanced networking for placement group

14- spot ec2 pricing especially when aws terminate them

15 - shared responsibilities model on aws not the customer

16 - kinesis firehose against kinesis stream ( just know the difference )

17- dynamodb used cases and features like ( millisecond latency , durability , shared store )

18- cloud front features like ( can it server different origins from different regions and so on ) also look for the way it looks the script of cloud front distributions

19 - finally ofcourse he ask about old topics like ec2 , rds , iam roles , cloud watch , sns , and so on >>>>> but once you solve the questions ( a lot of them ) and study the new parts even with just reading you will pass with score

Good luck all , I really get used of this feedback and it works for me , so thank you all for every contribution you made.

VPC - perhaps the most important thing you need to study. Private and public subnets, NAT gateways/instances, security groups/network ACLs, and basic direct connect/VPN concepts - study these thoroughly. I don't remember any questions asking about subnetting or CIDR blocks. There was a flow logs question.

-EC2. Know the different instance pricing models, when you would use each, and what you'd pay (I didn't get any questions about the instance types, i.e. don't worry about Dr. McGiftPx too much). Know the details of reserved instances.

Understand EBS - snapshots, encryption, and each storage type - know when to use provisioned IOPS vs. general purpose SSD. Study load balancers - different types, auto scaling groups/launch configurations (you can't edit a launch config; you have to create a new one!) and know how AWS chooses which auto scaled instances to terminate first (this is in the AWS documentation).

-S3. Know the different storage classes (plus Glacier) and when to use each, understand lifecycle policies, and multi-part upload. EFS was mentioned on one question.

-IAM - Be sure to understand access keys vs. passwords, roles for EC2, and the differences between users/groups/roles. There were a couple of questions about STS - know what it does and how it's used - and know about giving access to AWS using Active Directory and cross account access.

-RDS. Understand the difference between multi-AZ and read replicas. Redshift was mentioned as an answer for one or two questions, but not covered in-depth.

-DynamoDB - I had 2-3 questions asking "which service should you use for [X] purpose" - I answered DynamoDB for all of them. I think one was wrong. Nothing crazy about partition keys, data types, or anything like that, but know the fundamental advantages of DDB and when it would be used (as a session store, for example) and that it's cross region capable.

-Lambda and API Gateway. Know the benefits of API gateway and that Lambda is automatically scalable.

-CloudTrail and CloudWatch - for API logging and instance monitoring, respectively. Know about the CloudWatch Logs Agent and CW alarms/events.

-At least one question about the shared responsibility model (what you are responsible for in the cloud vs. what AWS is responsible for doing/maintaining). It intuitively makes sense, but read the whitepapers on the AWS certification site.

-The biggest curveball/most difficult topic: Elastic Container Service. I think I had at least 3-4 questions on this topic alone and didn't study it much except for a quick review before the exam. One particularly tricky question was about IAM roles and ECS tasks.

-Basic questions about SQS. Know that it's used to decouple applications from tasks, make applications stateless, etc.

-Kinesis - know the difference between Firehose vs. Streams. (Only one question)

-CloudFront - I had a tricky question about troubleshooting Path Patterns. I don't remember seeing this in the course. This dictates what CloudFront uses as the origin (ELB vs S3 bucket) based on the file name/folder path.

Some details/lists to memorize: which services are encrypted by default, which service can trigger Lambda (like SNS and DynamoDB), which endpoints can SNS publish to (SMS, email, among others), and what can serve as an origin for CloudFront.

I don't recall any questions on my exam about KMS, CloudHSM, Elastic Beanstalk, CloudFormation, or OpsWorks,