

 Practice Tests 2020 AC-SAA
by Neal Davis

SET 1-3. "to block access for specific countries".

- CloudFront has a geo-restriction feature to block content for specific countries.
- NACL is another way to block IP ranges of specific countries, but this is super hard to manage.

SET 1-9. "S3 access pattern is unknown and need to keep cost as low as possible".

- S3 Intelligent-Tiering is the recommended access type for "unknown" access patterns.
- Other tiers e.g. Glacier, Standard IA, Standard IA+GeoZone can be expensive in some cases.

SET 1-11. "to deploy an application running on EC2 from one region to another".

- Copy the AMI from Region A to Region B. And then launch a new EC2 instance from the AMI.
- For EBS, the new instance in Region B will be able to access the same EBS volume.
- There is no feature for "cross region" snapshots of EC2 instance.
- EBS cannot be restored into S3 or the vice versa.

SET 1-16 "To make API call to DynamoDB and do not traverse the Internet".

- Create a Gateway Endpoint for DynamoDB and then create a route table entry

for the endpoint.

- Note that only DynamoDB & S3 use Gateway Endpoint, other AWS services use interface endpoint.

SET 1-22. "to enable DynamoDB access permission for task running in ECS using EC2 launch type".

- Create an IAM policy enabling permission and assign it to a task using the `taskRoleArn` parameter.
- Note that the AmazonECSTaskExecutionRolePolicy is not for the TaskRole, it is TaskExecution role, used by agent to pull images, write logs, etc.

SET 1-31. "to restrict certain EC2 type for an OU under AWS Organization".

- Use SCP (service control policy) to block specific instance types by a deny rule.
- AWS RAM (Resource Access Manager) is not for this. RAM is for sharing resources within org.

SET 1-33 "create an ^{encrypted} cross-region RDS replica from an unencrypted master"

- You cannot create an encrypted replica directly from an unencrypted master.
- You cannot enable encryption directly for the master DB instance after launch.
- You can:
 - Take a snapshot of master;
 - Encrypt the snapshot
 - Restore to a master instance with encryption.
 - Make a replica.

SET 1-60. "Data lake SQL query solution. Infrequent access with minimum infrastructure cost".

- Amazon Athena is preferred as SAW solution, for "infrequent" and "cost-saving"
- Amazon Redshift Spectrum is another solution but not the best here as underlying runs on EC2 which is not serverless from cost point of view.

SET 2-3 "Need a distributed database for several EC2 instances. need low latency and super high throughput, data will be replicated so can tolerate instance loss".

- EC2 instance store will be ideal as instance loss is tolerable with loss.
- If data is not replicated across instances, then EFS is the solution.

SET 2-16 "Migrate 500 TB data from on-premises to S3 Glacier. need the most cost-effective way, knowing that the Internet is slow for the company".

- Order 7 AWS Snowball (each can hold up to 80 TB) specify destination as standard S3, and add a lifecycle policy to move data to Glacier.
- Note that Snowball only supports standard S3 as destination.

SET 2-41 "Which options meet the in-transit requirement of an application running on EC2 behind an ELB?"

1. NLB with a TCP listener and terminates SSL on EC2 instances (layer 4)
2. ALB with an HTTPS listener and then installs SSL certification on both ALB and EC2 instances (layer 7)

SET 2-59 "A fleet of EC2 instances running in a private subnet need to connect to Internet-based hosts using IPv6 protocol".

- An egress-only Internet Gateway will be the right answer.
- Note that NAT cannot be used here as NAT doesn't support IPv6.
- Also note that any choice associating NAT to subnet instead of instance are wrong, as you can only add NAT to EC2 instances level.

SET 3-14 / SET 1-1 "requires to monitor EC2's swapUtilization/memoryUtilization"

- Install the CloudWatch Agent on instance, run an appropriate script with cron job on instance, and monitor the metrics.
- EC2 doesn't come with memory utilization metrics by default.

SET 3-37 "Find solution for provisioning a connection for an application to the Internet to pull large amount of data. Need to have no constraint on bandwidth"

- Attach an Internet Gateway is the right approach.
- Cannot use NAT Gateway as it has a bandwidth limit of 45 Gbps.

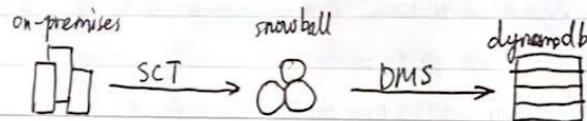
SET 4-11. "Let Lambda function to get database credentials but cannot write credentials in code."

- Use System Manager Parameter Stores to update function and execution role.
- AWS Authentication Plugin cannot be used as it's for RDS not Lambda function.
- AWS KMS is not correct: it's for managing encryption key not access credential.

SET 4-12. "DR strategy for getting a limited set of core services up and running with all other services switched off".

- Pilot light. is the right one.
- Warm standby : a full set of replicas working, at downscaled capacity.
- Multi-site: Active - Active.

SET 4-15. "MongoDB running on on-premises needs to be migrated to DynamoDB with limited Internet bandwidth for a super large table."



SET 4-18. "Most cost-effective way to enable a backup for the Direct Connect connection?"

- Implement an IPsec VPN connection using the same ~~BGP~~ BGP prefix.
- Note that creating another DX is feasible but not cost-effective.

SET 4-24. "Attempted to restart a stopped EC2 instance but it immediately changed from a pending state to terminated state."

- You've reached EBS volume limit.
- An EBS snapshot is corrupt.
- The root EBS volume is encrypted but you don't have permission to correspond key.
- The instance AMI you used missed a needed part.

SET 4-43. "Create a URL to allow signing in AWS Management Console. The URL needs a sign-in token and Microsoft AD Federation Service is used as the identity provider (IdP). What are the steps needed?"

- Steps:
 1. Verify that the user is authenticated by your local identity system.
 2. Call AWS Security Token Service (STS) "AssumeRole" or "GetFederatedToken" API operations to obtain a temporary security credential.
 3. Call AWS federation endpoint and supply the temporary security credential to request a sign-in token.
 4. Construct URL with the token and send to user.

SET 5-3. "The easiest approach for handling repeated bursting calls to API Gateway".

- Enable a cache for a stage of API Gateway and configure a TTL.
- Note that API Gateway can only add stage level cache, cannot add method level cache. The default cache TTL is 5 min. TTL range [0, 1 hr]

SET 5-35 "Statement right / wrong on EBS encryptions".

- All EBS types supports encryption and all instance "families" supports encryption.
- Not all instance "types" supports encryption.
- Data in transit is also encrypted once EBS encryption is on.
- Encrypted / Unencrypted EBS can co-exist in an instance.

- Snapshots of an encrypted EBS are also encrypted.
- EBS Volumes restored from an encrypted snapshot is also encrypted.
- EBS Volume created from an encrypted snapshot is also encrypted.

SET 5-38. "Need a cloud solution for on-premises large media files, using SMB or NFS protocols."

- AWS Storage Gateway File Gateway is the right solution. File Gateway supports file related protocols of SMB / NFS.
- AWS Storage Gateway Volume Gateway is not. It uses block-based on S3, doesn't support file protocols.

SET 5-52. "AWS's policy on penetration-testing".

- AWS customers are welcome to carry out security assessment ~~or~~ / or penetration tests against their AWS infrastructure without prior approval for 8 services.

SET 5-61. "CloudWatch is used by Lambda. What metrics are generated?"

1. Total connects / calls
2. Duration
3. Total errors.

SET 5-62. "EC2 hosting video for on-demand streaming on web. Requests increased impacting EC2 performance."

- Solution: CloudFront for distributing video contents.
- Note that: CloudFront RTMP RTMP is not a choice here as CloudFront RTMP only supports S3 as origin not EC2.

SET 6-10. "Needs to capture information about the traffic that reached ELB, The info should include the source, destination, and protocol."

- Use a VPC flow log for capturing each network activity associated with ELB.
- Note that Amazon CloudTrail is not an option as it doesn't have info at packet level. Also, it's for user activity auditing, not for requests in traffic.

SET 6-47. "What's the default rules for a newly created NACL? (Not the one that's created along with VPC)."

- Inbound: denying all traffics.
- Outbound: denying all traffics.
- Btw: for the default one created along with VPC: allowing all.

SET 6-63. "What's the newly added security group's default inbound and outbound rules?"

- Inbound: No inbound rule hence implicitly denying all.
- Outbound: Allow all traffic to all IP addresses.

SET 6-50. "Need ELB for load balancing and uses TCP protocol, which type of ELB to use?"

- NLB. at layer 4, supports TCP, HTTP, HTTPS etc. at network layer.
- ALB. (wrong answer). at layer 7. supports only HTTP and HTTPS.