Questions I got wrong

Saturday, September 12, 2020 12:20 AM

Use resource based policies instead of assuming roles when you need original permissions.
AWS managed directory is needed to create two-way-trust for SSO, ad connector is not enough.
IAM user integration with cloudhsm would have to be done via ssm parameter store, iam for cloudhsm is only for CRUD cluster modifications.
Use elastic ip to limit access to S3 bucket utilizing bucket policy.
AWSVPC ecs networking mode gives your ecs task a different eni
Only async will allow lambda dlq, so SNS, not SQS or API
Api gateway timeout is 29 seconds.
Use EMR for hive..
Kinesis agent can send to firehose directly without going thru streams from ec2
No way to automatcially increase limits, manual only. - as of 2019 you can do api calls via service quota
You can create storage file gateways in AWS as well!
OnPrem ES cluster to AWS by exporting index, transfer to s3, then import index from s3 into amazon ES.
AWS:SourceVpce is used to ensure private vpc endpoint access
AWS:SourceIP can only do public ip ranges
SSO can only source from one identity source
StackSet to deploy across regions and accounts
CORS is to set origin, so you need to set it on the secondary site not the original.
502 error is related to concurrency limit in lambda.
Lambda can be triggered by sqs queue.. Special trigger.
Kinesis data stream has a limit of 1mb/s
storage gateways does do backups on s3, just make an ebs volume from it.
sync database replication is bad for data corruption
iam user cannot map to sts service.
Once you load ssl private key to lb you cannot retrieve it
Use cloudfront with geo-restriction to blacklist countries
Use cloudfront origin failover to switch when one origin fails.
Lambda functions have security groups
Secrets manager does key rotation. SECRETS = ROTATION
Aurora multi master instances must be in the same region.
Cant use spot instances for redshift
Use direct connect with multiple virtual private gateways for dedicated private secure connections.
You can turn off reserved instance sharing on master account for all member accounts in a business unit.
"proceed without key pair" uses the same key as before when migrating from a region to another.
AWS WAF will not help you against DDoS attacks, but apparently aws config can.
For redis data durability enable append-only file feature, also for warming of data, there is automated backups but only once a day.
Need to make new bucket and have iam roles to keep logs safe in s3, with mfa delete and bucket polciies
Trusted access running enable-sharing-with-aws-org command
Adding read replicas in each AZ is better than vertically scaling mysql RDS.
Patch baseline patch groups for different environments, and tags for os and environments in smpm (systrms manager patch manager)
Aws firewall mananger to control across accts, not track changes
Serverless is regional

Practice test 2 boson

Stack is the type of thing you're deploying for a purpose, layers are groups of components like lb, app servers - grouped by function I guess
Alias records cannot be used for instances, it can only go to s3 buckets, cf, and another record.
You can monitor multiple regions with one CW dashboard
Use proxies to filter urls, ids/ips, dlp, monitoring, etc. NACL can't deny by url
EBS wont let you manage infrastructure as code. CloudFormation will.
Cold hdd is for infrequent access, duh.
RDS does not support oracle RAC, multitenant database, unified auditing, database vault, and others.
ECS uses service auto scaling, not ASG.
Putting in RDS is an example of replatforming. Rearchitecture is more advanced changes.
Using stateless is better for scaling and storing it all in a session state cache db.
Disposable upgrade means rolling a new EC2 instance and terminating old one (not using Elastic Bean Stalk or CF)
Stored volumes only fit 512tb, cached holds 1024tb.
Redshift Workload Management can manage priorities for queries.
Redshift does not have read replicas heh.

Practice test 3
you can expand your existing VPC by adding four secondary IPv4 IP ranges (CIDRs) to your VPC
Aws config scans for approved ids using approved-amis-by-id, aws inspector does automated security assessments but does not do ami related scans.
Enabling versioning in s3 does not invalidate presigned urls. However, not having AWS creds in ~/.aws/credentials means you cannot generate a new pre-signed url
Immutable deployments of elastic beanstalk ensures new versions fully pass health checks and avoid degradation of existing servers.
Don't use spot instances for master and core nodes for EMR clusters.
If redshift queries stop responding try: lower MTU, view STV_Locks and STL_Conflict tables to find conflicts, PG_CANCEL_BACKEND function to cancel queries, PG_TERMINATE_BACKEND to terminate session.
If queries take too long try running vacuum and increasing memory using wlm_query_slot_count, or use single copy command for long loads.
Lambda canary deployment does two shifts using codedeploy. Rolling with additional batch is for elastic beanstalk.
You must set up a snapshot copy grant for a master key to enable cross region snapshots for redshift
504 errors are associated with integration timeout or failures, so 29 seconds.
S3 block public access is a thing. Aws config will only notify, not restrict. SCP will work but its more effort.
Only one VGW can be attached to a VPC at a time.
To enforce HTTPS on CF, set either HTTPS Only or redirect http to https, and configure viewer protocol policy to require https.
To make AWS orgs master account connect, send invitation to all member accounts from master accounts with OrganizationAccountAccessRole IAM role in member accounts and grant that to master to have full admin control.
BGP/MD5 is needed for direct connect to work.
Master account can activate billing tags, not member accounts. AWS Config cannot add tags for you, it can only check if you have tags or not on something. CloudFormation resource tags and service catalog will tag for you, IAM can enforce tag restrictions as well.

Practice test 4
Use direct connect gateway to merge two vpcs, duh.
If you use default CF SSL cert you cant use own domain name.
You can store certs in iam
Elasticache cluster is easier than redis-in memory cache to setup for mulitple az

Snowball has AWS Greengrass, durable local storage, local compute also with aws lambda, and is able to use in a cluster of devices.
Cloudfront does not do database caching
AWSELB is the cookie ELBs create to map sessions to ec2 instances for sticky sessions.
Only s3 has bucket policies, iam does not -duh
Redis AOF downtime is higher than multi-az with auto failover
You can move a instance into or out of a placement group once it is stopped
SCP does not grant permissions, they are the max permissions. You still need to be granted permissions via iam.