

Things to review

Saturday, September 12, 2020 12:24 AM

AD with AWS for user federation uses AssumeRoleWithSAML

Api gateway errors:

4xx is client, 429 is throttle (api gateway), 403 is access denied, 400 is bad request
5xx is server errors, 502 bad gateway lambda under heavy load, 503 service unavailable, 504
endpoint request timed out exception api gateway requests timeout after 29 second maximum.

Stacksets - stacks across accounts and regions

Service quotas api

Does s3 support js?

Yes

Max size for sqs?

2gb

Was EMR or kinesis real time?

S3 over direct connect.. Public or private interface? Bgp or static route better?

Public, gbp

Review stored vs cached gateway.

Stored is on prem

Decider instance?

Part of SWF

SES?

Simple email service

DynamoDB or RDS for user info?

Apparently user info isnt login stuff so dynamo...

Aws redshift backups... how do they work.

snapshots

Can you use spot instances for EMR

yes

What about reserved instances for redshift?

yes

Cloudfront behaviors, is that a thing?

Cache behaviors yes

Can beanstalk deploy docker?

yes

What does AWS Inspector do?

assess security compliance

Practice exam 1

Cloudfront w/ geo-restriction vs route53 with geolocation

Use cloudfront for low latency

What is AWS SAM?

Serverless application model

What is lower effort, rehost or replatform? Rehost is my guess.

Rehost is lower. Replatform does a bit of optimization

Which one allows rotation of keys again.. SSM or secrets manager?

secrets

Systems manager state manager or session manager for startup config?

Systems manager state manager for startup config and other config

Session manager is for policies

Link aggregation group?

Aggregate multiple connections at a direct connect gateway

When to use volume gateway instead of file gateway?

When you want to back up a whole file system instead of just a file

What is AWS Macie??

Amazon Macie is just a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS.

Aws x-ray agent.. Hmmm

Used for debugging

Practice exam 2

Opsworks stacks layers and recipes.. What are they?

Stacks are a bigger split then layers. Custom recipes are custom scripts

Non-alias record.. When to use?

When you are not using s3 or cloudfront, like CNAME etc, trying to refer to specific instances, ips.

Retain vs snapshot

Guesseedc right but yes s3 should be set to retain, and rds to snapshot.

AWS Systems manager.. Patch manager?

Yes that's the name. install SSM agent and then automate patch schedule using AWS systems manage maintenance windows.

Practice exam 3

How to implement s3 sse-c?

For presigned urls, specify using x-amz-server-side-encryption-customer-algorithm header

For s3 rest api calls use the headers: x-amz-server-side-encryption-customer-algorithy x-amz-server-side-encryption-customer-key x-amz-server-side-encryption-customer-key-md5

STS - assumerolewithwebidentity or SAML?

Web identity.

timeout behavior of a nat instance?

Sends fin packet to close connection upon timeout without retry. Use gateway instead for better performance.

Redshift queries stopped responding how to solve?

See wrong notes. If they stopped responding entirely you need to 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.

What does aws inspector do anyway?

Security and compliance automation

Organizatuonaccountaccessrole

Yes needed as an IAM ROLE in member account for master account to have full admin control

Practice exam 4

Composite primary key dynamodb?

Yes it's the primary + sort key.

CLB sticky cookie

AWSELB

Amazon workdocs?

Yes fully managed collaboration service

Mysqldump?

Yes use it to replicate mysql databases, you can do it to onprem too from RDS mysql or mariaDB.

Is amazon connect for AD? Crap..

No its for call centers

Ec2rescue?

Yes it works with system manager, diagnoses and troubleshoots problems with ec2 instances on both linux and windows

Ec2throttled

Lambda gets throttled when there are not enough ENIs or IPs

Do I have to stop a cluster group to move a new instance into the group?

No

How to get dynamodb creds with CF templates?

IAM role, reference it in the InstanceProfileName property of the app instance

Key/value cache, that's no-sql right?

yes

Review SSO options pls

done

Review classic load balancer

done

Iam policy vs scp

Scp is "MAX" permissions, iam actually grants permissions

How to update aws stack in opsworks with patches?

Opsworks will automatically install latest updates during setup. You can also run update dependencies for linux.

Do you need server migration connector for SMS to work?

Yes

Review how to enforce tags from last practice exam.

Cloudformation resource tags, iam can enforce tags, and service catalog can require tags too.

Can you store ssl certs in IAM even? Maybe the IAM cert manager..

Yes IAM will allow you to store certs

Which database does sharding again? Aurora?

Kinesis and elasticache

Other notes

A record vs alias

Alias A is for cloudfront, elb, or s3, A records are for ips and are non-alias records.

CNAME points a hostname (ONLY NON ROOT DOMAINS for e.g. something.domain.com)

to any other hostname

Alias (option for A) points a hostname to an AWS resource, works for ROOT domain and NON ROOT DOMAIN

Alias is free of charge and has native health checks.