**AWS Security Specialty Review Questions Based on Failed Exam Attempt**

**What is Athena?**

**What are the use cases of Athena?**

**What is Amazon Quick Sights?**

**How do you make sure you do not use AWS provided DNS?**

**What is Cognito Sync Trigger?**

**What is AWS App Sync?**

**What is the port number you need to open for SES?**

**What is Elasti Search?**

**How should you secure ECS?**

**How should you implement write once read many glacier policy?**

**What does the aws:MultiFactorAuthAge condition key mean?**

**What does the aws:MultiFactorAuthPresent condition key mean?**

**What is a principle?**

AWS Security Specialty Review Questions Linux Academy Domain 1.1

What is an incident?

What is an AWS Abuse Notice?

What is the acceptable use policy?

What services allow for pen testing?

What are some instance types that don’t allow for pen testing? Why is this?

How should you respond when you receive an abuse notice?

What should you do if your root or IAM users leak their login credentials? What can you do to automate this at a large scale?

What is the other thing you should do? How would you go about doing each?

What should you do if your EC2 has been hacked been someone obtaining key pairs? What 2 things you can do and why would you choose one over the other?

What should you do if you access keys get leaked?

What should you always check for after being attacked?

What things can you do to be proactive and avoid being compromised in the future?

AWS Security Specialty Review Questions Linux Academy Domain 1.2

What is an incident? Give an AWS example.

What is incident response?

What are the 7 phases in the incident framework?

What are AWS organizations? What are 2 ways to segment your teams and why is one better than the other?

What is centralized logging?

What is a live box investigation and what is a dead box investigation. Why would you use one over the other?

What is the preparation step? What are the 4 things you should do? What do they mean, how should you go about doing them, and what services can you use to help?

What should you do for the identification step? What services can help you do that?

What could you do in the containment step? What services can help you do that?

What can you do in the investigation step? What services can help you do that?

What can you do in the eradication step? What services can help you do that?

What would you do in the recovery step? What services help you do that?

What do you do in the follow up step?

AWS Security Specialty Review Questions Linux Academy Domain 1.3

What is automated alerting?

What are 3 phases in automated alerting? What does each mean?

What is Route 53 DNS Logs?

How can you use EC2 for the detection phase?

What is CloudWatch event rules?

What are different targets?

What are the 2 different types of automations you can use?

Explain how they are different and how to set up each? Which one is better? Why would you use one over the other?

What are the benefits of adding incident automation?

What are automated responses? What can each target do specifically?

What is special about the SNS target?

AWS Security Specialty Review Questions Linux Academy Domain 2.3

What is the default configuration of cloudtrail?

What is a trail?

What are 3 configuration options?

What are the limitations to a digest file?

In terms of CloudWatch logs, what is a log event? Log stream? Log group? Metric filter? Retention setting?

How do you configure CloudWatch logs with CloudTrail? What role do you need?

What is the capture point of VPC Flow Logs? What are the 3 types?

What can you see from a VPC Flow Logs log? What is the order in which you see it?

How do you set up VPC flow logs? What role does it need?

If you make a flow log at the VPC level what will automatically happen?

Are flow logs real time?

How can you automate real time security analysis with ip traffic? What do you have to watch our for?

What type of traffic do flow logs not log?

What phase should you turn on flow logs?

What is the cloudwatch agent?

What are system level metrics? What are log metrics?

How do you setup the cloudwatch agent? What role do you need? What about for on prim?

What AWS service can you use to store secure pieces of information such as username and password or config files that may have secure elements?

Can you do metric filters on logs pushed up from EC2? Why would you do this?

What are DNS query logs?

What are the limitations for enabling them?

How do you set up dns query logging?

What are the 2 log streams it will have?

Is it real time?

What is S3 role in storage logging?

What are S3 access logs?

What do log events contain in S3 access logs?

What are some important features of S3 Access logging?

What are some reasons you may want to export cloudwatch logs to an S3 bucket?

How can you configure logging on a bucket?

Which one would you use for real time logging? Apache log files pushed to cloudwatch logs from an instance or a serverless static website hosted in an S3 bucket with access logs turned on?

What is the multi account strategy?

What are 2 ways you can set up organizations for best practice?

What will this reduce?

What are the steps to setup cross account logging?

What is the more secure way for centralized logging?

What is a best practice for the encryption of these files?

**AWS Security Specialty Review Questions Linux Academy Domain 2.4**

**What should you check if your cloudtrail isn’t logging?**

**What should you check if your cloudtrail, vpc flow logs, route 53 dns logs, or EC2 logs are not logging to cloudwatch logs?**

**What should you check if you S3 access logs are not logging?**

**What is the limit of trail per region?**

**Where do global service events come from? Why might you have duplicates? How can you stop duplication of global events?**

**Why are you not receiving object level events from S3 or lambda?**

**Why might your mult account cloutrail solution might not be logging?**

**Why might your cloudwatch logs multi account solution might not be logging?**

AWS Security Specialty Review Questions Linux Academy Domain 2.1

What are S3 events? What are the 3 things it can trigger?

What are the 2 types of events and what are their differences?

How do you set it up?

Why might you use S3 events?

What is cloudwatch? What are metric filters?

What is a metric namespace?

What is a metric name?

What is an alarm? What actions can an alarm trigger?

Where can cloudwatch logs stream data too? Where can it export data too?

When would you use the metric filter and why?

What are the 3 parts of cloudwatch events?

What are the 2 event types?

What are some targets?

Why would you use this?

What are some examples you would use this?

What are the 2 types of event types from a non time based event?

What are some limitations? How can you get around it?

What are some benefits?

What is a cloudwatch bus?

How do you set it up?

What are the 2 types of ways you can allow access?

What do you need to do to the rules if you allow everybody?

Is an event bus global?

What are the uses of config?

What can you do with it?

What is the configuration recorder?

What is the configuration item?

What is the configuration history?

What is the configuration stream?

What are config rules?

How can you specify your rules?

What are the 2 ways rules can get checked?

What does inspector allow for?

What is a target?

What is an assessment template?

What is an assessment run?

What are some of its features?

How can you specify your instances?

What are the package types you can evaluate with?

What does each package evaluate?

How do you set it up?

What can you download?

Can you use inspector as an event source?

What are the differences between config and inspector?

AWS Security Specialty Review Questions Linux Academy Domain 2.2

How should you go about trouble shooting cloudwatch events?

What are some common issues?

What region do global resources come from?

How can you use automation to monitor automation?

What event metric should you filter for failed events?

What should you do if your event rules are not being triggered?

What are the 2 types of permissions you should check?

With multi account what should you check?

If you have an s3 rule and it is not working what might be wrong?

**AWS Security Specialty Review Questions Linux Academy Domain 3.1**

**What does cloudfront remove at the edge?**

**What are the 2 ways cloudfront can be configured for internet access support? What are their differences and when would you use one over the other?**

**What is the viewer protocol policy?**

**What are the advanced security features?**

**What are the 3 viewer protocol policy options and what is the default?**

**What is the default restrict origin ssl protocols and what can you optionally enable?**

**How can you restrict viewer access to the distribution?**

**What is lambda@edge? Why might you use it?**

**How do WAF’s work from an architectural standpoint for cloudfront?**

**How can you have end to end encryption? Can you use a self-signed certificate?**

**What is field level encryption? Why might you use it?**

**What type of logging does it support?**

**How do you restrict content to where it can only be accessed to cloudfront?**

**How is an OAI used in terms of the bucket policy?**

**How do you set up an OAI on an already made distribution?**

**What are signed URL’s? what are signed cookies?**

**What are some features or limits for these?**

**What is the TrustedSigners key mean?**

**How can a pre-signed url generate an access denied message?**

**How should you generate pre-signed URL’s according to best practices? Why is that?**

**When should you use either? In what scenario?**

**What 2 ways can CloudFront restrict content?**

**What are some features of cloudfronts geo restriction?**

**How do you set it up? Can you black list some countries and whitelist others on the same distribution?**

**What are 3rd party geolocation?**

**When would you use either?**

**What does S3 encrypt? How can you set up default encryption? How can you set it up so that a user cannot upload an unencrypted object?**

**How is this evaluated and what does that mean?**

**What command can you use to upload objects to a bucket encrypted?**

**What are some features and limits of Cross Region replication?**

**How do you setup standard cross region replication?**

**How do you setup cross region replication to another account?**

**What direction is cross region replication in?**

**What do you need to update to allow cross region replication to use KMS keys?**

**What type of things can a WAF watch out for?**

**When multiple conditions exist in the same rule what must be true for the rule to take effect?**

**What is AWS shield standard and what does it protect?**

**What are some benefits of using AWS shield advanced? What other AWS services does it effect?**

**Where does WAF sit?**

**What are conditions? What are rules?**

**What are the 2 rule types and what are there differences?**

AWS Security Specialty Review Questions Linux Academy Domain 3.2

What is the AWS public space?

What are security groups? What are they associated with? What does this mean?

What is the traffic journey?

What are the filter points for inbound traffic? What about outbound?

What are some features of NACL’S?

How are they processed? What does this mean?

In what ways can vpc’s be peered?

What are 2 things to remember with vpc peering?

How do you set up peering for vpc in the same region and account?

How do you set up peering in different regions in the same account?

When can you do logical references for security groups in terms of peering?

Why is it better to use specific ip’s then CIDR ranges?

How do you create a peering connection between 2 acc in the same region?

What are VPC endpoints? What are the 2 types?

What are some things you need to remember with Gateway Endpoints?

What services does it support?

How do you setup a gateway endpoints?

How can you restrict access? Why might you do this?

How can you do this via a bucket policy? What does this allow?

What are some things to remember with gateway endpoints?

What are interface endpoints and how does their architecture differ then gateway endpoints?

What is a private link?

How can you secure interface endpoints?

What are the steps to create them?

What are some features of interface endpoints that gateway endpoints don’t have? What type of services can you use them for?

What is the lambda function policy?

What is the difference between push and pull and what do you need to do to the function policy for both?

What is the IAM execution role?

What is a NAT gateway? What are some security implications?

What is an Egrees only internet gateway?

What are some features?

How do you set it up?

What are some limitations of it?

What is a bastion host?

How can you lock it down for security? How can you increase that security?

How can you configure a bastion host to allow id federations where using direct connect or a vpn is not an option and the org needs the ability to connect into private instances using existing identity providers?

AWS Security Specialty Review Questions Linux Academy Domain 3.3

How should you trouble shoot the routing of a VPC?

How should you trouble shoot a NACL?

How should you trouble shoot a Security Group?

How should you trouble shoot logging and monitoring of a vpc?

AWS Security Specialty Review Questions Linux Academy Domain 3.4

How is isolation made in AWS?

How is memory scrubbed?

How is disk scrubbed?

What can you optionally do to comply better with you company?

What is a host proxy server?

What are the 2 filter points you get in AWS? When would you use the proxy server?

What is and IDS and an IPS?

What solutions do these compliment in AWS?

How can ids inject logs into aws?

What should you use if you want true intrusion detection?

What is system manager and what does it provide?

What are the 2 core areas of it?

What does the inventory allow?

What does the compliance allow?

What do you need to use SSM?

What is SSM state manager, patch manager, run command and how can you configure centralized logging on your buckets with it?

What is the actions?

What is the automation?

What is the shared tooling? What is managed instance? What is authenticators? What are documents? What is the parameter store?

What are some limitations?

What is the personal health dashboard?

How can you do packet capture on instances?

What are some common scenarios you would do this in?

What service does this compliment and why?

How should you log that data?

**AWS Security Specialty Review Questions Linux Academy Domain 4.1**

**What are the 2 types of IAM policies?**

**When can you use a condition? What is the example given? What does that condition do and why is it effective?**

**How should you monitor access key use?**

**What is the access advisor?**

**What is the credential report?**

**What is a trust policy?**

**What are some common uses of a trust policy?**

**How can you revoke active sessions?**

**How does this work using a role?**

**What are permissions boundaries?**

**How are policies evaluated?**

**Where can permissions boundaries apply?**

**What is organizations?**

**What is a service control policy? Can this policy effect the master account? Can it effect root accounts?**

**How is organizations access controlled?**

**What are bucket policies?**

**What does the aws:Refer condition do?**

**What does condition do you need to require MFA?**

**What does the aws:MultiFactorAuthAge do?**

**What can key admins do on the key?**

**What can key usage do on the key?**

**What size object can CMK’s encrypt?**

**How can implement cross account capabilities to kms keys?**

**What are the 3 ways to provide cross account access to s3 buckets and objects?**

**What are their differences?**

**What is identity federation?**

**What are the 2 types?**

**Why would you do this?**

**When would you use web identity federations?**

**When would you use saml 2.0 federation?**

**What is the AWS systems manager param store?**

**What are its key features?**

**What are the 3 types?**

**AWS Security Specialty Review Questions Linux Academy Domain 4.2**

**What is the permissions union?**

**What are service trusts?**

**What is a resource policy?**

**How do you troubleshoot cross account roles?**

**How should you log your roles to check if it is working?**

**What does the condition sts:ExternalID allow?**

**What are the 3 api calls for the 3 federation types?**

**What are the 2 different ways you can get federated and there steps?**

**How large of data can cmk’s encrypt?**

**What is the rate limit?**

**What should you do if you have an application that needs to do a lot of encryption or decryption?**

AWS Security Specialty Review Questions Linux Academy Domain 5.1

How should you audit it and grant CMK’s permissions?

How can you generate CMK’s?

What is the key ID?

What is an alias?

What are some limits to aliases?

How do CMK’s work for encryption?

What are backing keys?

Why would you want to import your own key material?

What does the ReEncrypt api do?

What is the encryption context?

What are grants?

Why would you use a multi account kms architecture this?

What is cloudHSM?

What are some differences between CloudHSM and KMS?

**AWS Security Specialty Review Questions Linux Academy Domain 5.2**

**How should you go about troubleshooting kms permissions?**

**What will a key policy have when first created?**

**What do you need to do if you delete that policy?**

**How can you give cross account access to CMK’s?**

**What are the kms limits?**

**If using a cmk in a different account where would the service limits build up?**

What is the message you get if you exceed limits?

AWS Security Specialty Review Questions Linux Academy Domain 5.3

What services can kms integrate with?

At what point does managing keys end with kms?

How is encryption with EBS performed? DynamoDB? RDS? S3?

What is SSE-C? when would you use it?

What does the x-amz-server-side-encryption-customer-key header do?

What does the x-amz-server-side-encryption-customer-key-MD5 header do?

What does the x-amz-server-side-encryption-customer-algorithm = AES256 header do?

What is ACM?

What are some key features?

What is x509 v3 ssl/tls mean?

What are the encryption SDK’s? what can you do with them?

What does compliance mean?

What is AWS artifact?

Why would you use Artifact?

AWS Security Section 2 Review

What is CIA? What do these parts mean? When would they apply and what ways can you make sure they are in place properly?

What are some AWS services that will help with the CIA model?

What is AAA? What AWS services can help with this model?

**What is non-repudiation? Elaborate**

**What are the 6 things AWS is responsible for? How does AWS meet this requirement? Read whitepaper**

What are AWS security responsibilities?

What are some of your security responsibilities?

**What are the 3 different service types?**

What are their differences? What are you responsible for each? What are some AWS services that go into each category?

What are the 6 cloud contols

**What services apply for all control?**

**What is non-repudiation and what services apply?**

**Why should we trust AWS?**

AWS Security Specialty Section 3 Full Review

What are some benefits of IAM?

What are groups? **Can you have 1 user in 2 groups?**

Can you attach multiple policies to a single user, group, or role? **What about a bucket?**

What level is IAM at?

What are the 4 steps to locking down a root account after you take over for someone else?

What are policies? What are the 3 types and their differences? **What are services you can attach policies too?**

What is the difference between root users, admin users, and power users?

What is a bucket policy?

What are the use cases for it?

What overwrites what, an IAM policy or a bucket policy? How would this work?

What do you need to put at the end of a resource line of your policy generator?

What are principles?

What is a resources?

What can a bucket policy do to an IAM user with no denies?

Can a bucket policy overwrite a root use?

What is an explicit deny and why is it important?

What is an S3 ACL? What are the use cases?

How can you make ACL’s for specific users? What 2 things do you need to perform this?

How are authorization decisions evaluated in S3?

What is least privileged?

What is explicit deny?

Draw the policy conflict diagram and explain what it means?

What condition operator would you use to make sure your bucket uses SSL. How would you write that code?

What is cross region replication? By default, what is done in the replication process to your file?

How many destination buckets can the source bucket be mapped too? How many destination buckets can be mapped to more destination buckets?

What are the requirements to enable cross region replication?

What does the object owner need to do to enable his file on a bucket he does not own?

What do you need to do to enable cross region replication to cross accounts?

What can you do in the replication config when using cross region replication for cross account?

How can you secure your cloudtrail logs for a security best practice?

What is replicated in cross region replication?

What is replicated in terms of deletes?

What is not replicated?

When are you going to use aws:SecureTransport, and when do you not need to use it? Why?

What is an orgin domain name in cloudfront?

**What is an orgin path?**

How can you use cloudfront to restrict access to your bucket?

How can you use a custom SSL certificate for cloudfront? Can you use an existing certificate that you made for your ELB? **What about for a different cloudfront distribution?**

What are the steps to change the cloudfront settings to an existing distribution to force people accessing your bucket to use cloudfront URL’s?

What is an orgin access identity?

What does the option grant read permissions do?

How long does it take for cloudfront to force users to use it’s URL’s instead of a bucket after you change the settings?

What are presigned URL’s?

How can you generate them?

What is the command to assign them? How can change the time? What is the default time and the max time for presighned url’s?

Do you need to change bucket policies or ACL’s to use presigned url’s?

AWS Security Specialty Section 4 Full Review

What is cloudtrail? How does it work?

Cloudtrail has a public control plane that you access. It logs API calls to that control plane

What doesn’t it log?

What does cloudtrail enable?

What does cloudtrail provide?

What is logged for each API call?

Where are cloudtrail events logged?

What is the default time cloudtrail will keep logs if you do not set up anything?

Does cloudtrail log all the time? If nothing happens in your AWS account will you get logs during that time?

When going from inactive to active how long may it take for cloudtrail to recognize and deliver new log files?

How often are events delivered while you are active?

**What is a good example of non repudiation with cloudtrail and S3?**

How can cloudtrail be aggregated across multi regions and across accounts**?**

What are management events?

What is read-only access on your cloudtrail do?

What does write only access on your cloudtrail do?

What is the digest file?

Can you fake a digest file? Why or why not?

How long may it take to create a digest file?

CloudTrail logs contain metadata not application data. Why should I consider securing them?

How do we stop unauthorized access to log files?

How do we restrict log access to only employees with a security responsibility?

What are the 2 cloudtrail policies by default? Who should you assign each too?

How can we be notified that log file has been created, and then validate that its not been modified?

How can we prevent logs from being deleted?

How can we ensure that logs are retained for x years in accordance with our compliance

How are cloudtrail files encrypted? Can you change this?

What are 5 things you should do to lockdown your cloudtrail log files?

What is cloudwatch? What does it enable?

What does it provide?

What are the 3 components of CloudWatch?

What can you do with cloudwatch?

What can you do with cloudwatch logs?

What are 3 things cloudwatch logs mention you can monitor on the splash screen? Can cloudwatch be used for more then just your AWS environment?

How does cloudwatch work?

What are cloudwatch events?

What are the 4 types of events cloudwatch can respond too?

What are rules?

What are targets?

What are the 2 rule event sources you can have in cloudwatch?

What are the steps in creating a cloudwatch event rule? What are examples for each step in terms of what you can use?

Why is cloudwatch events good?

How do we control who can access cloudwatch and what they can do?

How are unauthorized users prevented from accessing cloudwatch?

What is AWS config?

What are some advantages of AWS config?

What does it enable?

What does it provide?

What are the 2 types of config rules and what are their differences?

Can you enable config for all regions at once?

How does config work? How does config differ from cloudwatch events?

What are configuration items, snapshots, streams, history, and recorders?

What is the recorder setup?

What can we see?

What does the timeline show?

What are the 2 trigger types? What are the time periods for the time based trigger type?

How many managed rules are in config?

What does the config role allow for config to work?

How can you force your environment to evaluate quickly?

What are some AWS config benefits?

How should you restrict access to config? What do admins need? What do day-day users need?

How should you monitor config? Why does this work so well?

How do you set up alerts when the root user logs in?

What is CloudHSM?

What does it enable?

What does it provide?

Compare HSM and KMS

How is HSM key control secured?

How is tampering handled in HSM?

What is a crypto officer and what is a crypto user?

How should you monitor HSM?

What are the compliance checks HSM supports?

What is AWS inspector?

What is the difference between inpector and trusted advisor?

How do you set inspector up?

What are the prerequisites to AWS inpector?

How do you define an assessment target?

How do you define an assessment template?

What are the 4 rule packages?

What are ways you can download the report?

What are the severity levels?

What is trusted advisor?

What are the 5 checks in trusted advisor? **What do you get by default**? How do you get more?

What does inspector do? What wont it do?

What are the 4 logging services and what do each log?

How should you control access to log files?

How do you ensure role based access?

How do you obtain alerts on log file creation and misconfiguration?

How do you manage changes to AWS resources and log files?

How can you prevent modifications to logs?

How should you manage the storage of log files?

AWS Security Specialty Section 5 Full Review

What is KMS? Is KMS global or regional?

What are the steps you need to take when creating an AWS managed key?

What are the 2 types of key material origins?

What are key administrators?

What does the option key usage define?

If you use SSE-KMS and the object is public will you be able to view it over the S3 bucket URL? What about if you use SSE-S3?

How can a user who has the key view the object in S3?

What happens if a full admin IAM user does the same thing? What happens if a sys admin tries it?

What else can full admins do that you should watch out for?

Why should you give users sys admin permissions over full admin access?

What is schedule key deletion and what are the values you can assign it?

What happens if you disable a key?

How do you create a customer managed key?

What are the disadvantages of using an external key?

When does the wrapping key and import token expire?

What files do you need to upload?

What 2 options can you choose for the expiration of the key?

Can you reuse the same import token or the same encrypted key material?

Can you enable auto key rotation for a CMK with imported key material?

How should you go about key rotations with a CMK?

What relationship does a ciphertext have with the original CMK?

If you use SSE-S3 will it generate a new key for you? What can you do with it in the console?

Can you delete AWS CMK’s immediately? What about if you use external key materials?

What are other services that you can use KMS with?

What does the CMK consist of?

Can you export a key from KMS?

How can you import a key from your management infrastructure?

Why should you consider importing your own key material?

What happens when you delete the key material of a CCMK immediately? Does it still take 7 days to delete?

What are some considerations for imported key materials?

How can you use cloudtrail and cloudwatch logs to protect your keys and data?

How can you use config to notify you of config changes?

What type of key do you use if you encrypt an extra EBS drive on your EC2 instance?

Once encrypted can you change the encryption type?

How do you encrypt root device volumes?

How can you change the encryption key type of a root device volume?

If you copy an AMI to a different region what KMS keys can you use?

How can you modify image permissions? What type of options can you do?

Can you use KMS to generate a public key and private key to log in to EC2?

Can you use EC2 key pairs to encrypt EBS volumes?

What file does your public key get stored in?

How can you view your keys on your instance?

How can add a new public key?

What happens if you delete a key pair that your EC2 instance is still running and still using it? Does it affect the instance metadata?

How can you access an instance that you lost the keys too?

Can you use KMS for your EC2 keys? Can you use cloudHSM? Why is this?

What can you do in the AWS market place? What type of security products can you purchase?

How are they sort by? What are the billing options?

How can protect against brute force?

What is AWS WAF, what 2 services can you use with it and is it global or by region?

What error code does a WAF give to a failed request?

What are 3 different WAF behaviors?

What are conditions you can define?

How do you associate a WAF with a resource?

Can you manual block ip addresses?

When you associate a WAF why might it not work immediately to your cloudfront distribution?

What is the differences between dedicated instances and dedicated hosts? When would you use each?

What are hyptervisors? What are host machines? What are guest machines?

What hypervisor does EC2 run on?

What are the 2 types of guest OS you can have running? What are their differences and when would you use them?

What guest OS can linux use? What about windows?

How is access delegated by pv?

How does isolation work in AWS?

Who has access to the management plane? How is the plan secured? When would the privileges be revoked?

What is memory scrubbing and when it is used?

AWS Security Specialty Section 8 Full Review

What is a DDOS attack? How might this happen?

What are the 5 ways to help mitigate DDOS attacks? How can you go about implementing these?

What are some scaling benefits?

How can you prevent entry points?

How can use cloudfront?

How can you use Route 53?

How can you use WAF?

What AWS technologies can help mitigate DDOS attacks?

What is AWS shield? What are the benefits of using advanced shield?

What is WAF? What services does WAF integrate with?

What services does it not integrate with?

What should you do if your EC2 has been hacked? Why might it have been hacked?

What should you do if you leak your keys? For a regular user and the root user? For a regular

What does Cloudtrail log? How are cloudtrail logs formatted? What should you do for best practices with cloudtrail?

What do you need to do to perform penetration testing?

What services does AWS permit for pen testing?

Are there pen testing tools in the AWS market place?

What is not permitted with pen testing in terms of instances?

What are other simulated events you can do in AWS?

What is ACM?

How long can you extend your route 53 domain name for?

What is auto renew in AWS?

Can you import existing ssl certs into AWS?

What do you need to make a new certificate?

What are 2 ways to validate your certs? Why should you do each?

How do you have to validate your ACM?

Can you update the record in route 53 automatically?

What is manual renewal? What doesn’t get renewed manually?

What 2 services does ACM work with? When you add a certificate to one does it automatically add it to the other?

Can you export AWS certificates?

What is perfect forward secrecy?

How do you secure your app load balancer? What ports are http and https?

What is ssl?

In order to enable perfect forward secrecy what cipher do you need?

What policy should you use to enable that?

What is API gateway throttling? What are the limits for steady state request rate and the api bust limits?

Why does API throttle?

What is API caching?

How can up the throttle and the burst?

What is the default TTL for caching? What is the max? what does TTL=0 mean in API gateway?

Why would you use API caching?

What is system manager parameter store?

How do you create a parameter with it?

Why would you use it?

How can you store volumes?

How do you reference the volumes? What does this mean?

What services can reference them?

What is system manager run command?

Why would you use it?

What role do you need for it to work?

What needs to be installed on your instances to do this?

What are the 3 compliance things you should remember and what do they mean?

How do you get FIPS-140 in AWS? What level does this service support?

Security Specialty Outside of ACloudGuru Review

What does envelope encryption mean?

What are Data Keys?

What is Data Key Caching? What are the reasons to use it?

How should you audit CMK usage?

What is a CMK Alias? What are some things you should keep in mind with aliases?

What is the Kinesis Client Library? What does the policy need to allow for you to use it?

What is Amazon GuardDuty? Why would you use it? What data sources does it process?

What is Amazon Macie?

What is Amazon Cognito?

What are user pools and identity pools in AWS?

What are the use cases for Cognito?

What are the 2 types of VPC endpoints? Why would you use them?

What are the best practices for carrying out security audits?

What should you do for NACL’s if you need to send traffic to HTTPS and then have that same traffic come back inbound?

Why would you use direct connect and why would you use VPN? What happens if you combine them?

What is a DHCP option set? How can you use your own DNS server?

What is a WAF sandwich?

How are KMS Keys with the Redshift cluster service encrypted?

What are the 2 types of events cloudtrail can monitor and what are their differences?

What is Amazon Data Lifecycle manager?

What do EBS Snapshots allow you to do?

What is the Lambda Authorizer?

What is the Trust Policy?

What is IAM credential Report?

What is a Viewer protocol policy for?

What are the difference between signed cookies and pre signed URL’s. when would you use them?

What is Lambda@Edge?

What is a Remote Desktop Gateway?

What does the condition policy kms:ViaService, aws:Referer, and aws:PrincipalOrgID do?

How should you troubleshoot your instances that are having an error using SSM?

What is AWS System Manager Patch Manager allow you to do? Run Command? Parameter Store?

When should you use Inspector vs Trusted Advisor?

When would you monitor your environment with CloudTrail, Config, VPC Flow Logs, CloudWatch Logs, AWS Marketplace, and AWS GuardDuty?