Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

https://www.2passeasy.com/dumps/AWS-Certified-Security-Specialty/

NEW QUESTION 1
You are designing a custom 1AM policy that would allow uses to list buckets in S3 only if they are MFA authenticated. Which of the following would best match this requirement?
A.

B.

C.

D.

A.

Answer: A

Explanation:
The Condition clause can be used to ensure users can only work with resources if they are MFA authenticated.
Option B and C are wrong since the aws:MultiFactorAuthPresent clause should be marked as true. Here you are saying that onl if the user has been MFA activated, that means it is true, then allow access.
Option D is invalid because the "boor clause is missing in the evaluation for the condition clause. Boolean conditions let you construct Condition elements that restrict access based on comparing a key to "true" or "false."
Here in this scenario the boot attribute in the condition element will return a value True for option A which will ensure that access is allowed on S3 resources.
For more information on an example on such a policy, please visit the following URL:

NEW QUESTION 2
You have a vendor that needs access to an AWS resource. You create an AWS user account. You want to restrict access to the resource using a policy for just that user over a brief period. Which of the following would be an ideal policy to use?
Please select:

A. An AWS Managed Policy
B. An Inline Policy
C. A Bucket Policy
D. A bucket ACL

Answer: B

Explanation:
The AWS Documentation gives an example on such a case
Inline policies are useful if you want to maintain a strict one-to-one relationship between a policy and the principal entity that if s applied to. For example, you want

to be sure that the permissions in a policy are not inadvertently assigned to a principal entity other than the one they're intended for. When you use an inline policy, the permissions in the policy cannot be inadvertently attached to the wrong principal entity. In addition, when you use the AWS Management Console to delete that principal entit the policies embedded in the principal entity are deleted as well. That's because they are part of the principal entity.
Option A is invalid because AWS Managed Polices are ok for a group of users, but for individual users,
inline policies are better.
Option C and D are invalid because they are specifically meant for access to S3 buckets For more information on policies, please visit the following URL:
https://docs.aws.amazon.com/IAM/latest/UserGuide/access managed-vs-inline
The correct answer is: An Inline Policy Submit your Feedback/Queries to our Experts

NEW QUESTION 3
Your company has a requirement to monitor all root user activity by notification. How can this best be achieved? Choose 2 answers from the options given below. Each answer forms part of the solution
Please select:

A. Create a Cloudwatch Events Rule s
B. Create a Cloudwatch Logs Rule
C. Use a Lambda function
D. Use Cloudtrail API call

Answer: AC

Explanation:
Below is a snippet from the AWS blogs on a solution

Option B is invalid because you need to create a Cloudwatch Events Rule and there is such thing as a Cloudwatch Logs Rule Option D is invalid because Cloud Trail API calls can be recorded but cannot be used to send across notifications For more information on this blog article, please visit the following URL:
https://aws.amazon.com/blogs/mt/monitor-and-notify-on-aws-account-root-user-activityy
The correct answers are: Create a Cloudwatch Events Rule, Use a Lambda function Submit your Feedback/Queries to our Experts

NEW QUESTION 4
Your company has an EC2 Instance that is hosted in an AWS VPC. There is a requirement to ensure that logs files from the EC2 Instance are stored accordingly. The access should also be limited for the destination of the log files. How can this be accomplished? Choose 2 answers from the options given below. Each answer forms part of the solution
Please select:

A. Stream the log files to a separate Cloudtrail trail
B. Stream the log files to a separate Cloudwatch Log group
C. Create an 1AM policy that gives the desired level of access to the Cloudtrail trail
D. Create an 1AM policy that gives the desired level of access to the Cloudwatch Log group

Answer: BD

Explanation:
You can create a Log group and send all logs from the EC2 Instance to that group. You can then limit the access to the Log groups via an 1AM policy.
Option A is invalid because Cloudtrail is used to record API activity and not for storing log files Option C is invalid because Cloudtrail is the wrong service to be used for this requirement
For more information on Log Groups and Log Streams, please visit the following URL:
* https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Workinj
For more information on Access to Cloudwatch logs, please visit the following URL:
* https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/auth-and-access-control-cwl.html The correct answers are: Stream the log files to a separate Cloudwatch Log group. Create an 1AM policy that gives the desired level of access to the Cloudwatch Log group
Submit your Feedback/Queries to our Experts

NEW QUESTION 5
When you enable automatic key rotation for an existing CMK key where the backing key is managed by AWS, after how long is the key rotated?
Please select:

A. After 30 days
B. After 128 days
C. After 365 days
D. After 3 years

Answer: D

Explanation:
The AWS Documentation states the following
• AWS managed CM Ks: You cannot manage key rotation for AWS managed CMKs. AWS KMS automatically rotates AWS managed keys every three years (1095 days).
Note: AWS-managed CMKs are rotated every 3yrs, Customer-Managed CMKs are rotated every 365- days from when rotation is enabled.
Option A, B, C are invalid because the dettings for automatic key rotation is not changeable. For more information on key rotation please visit the below URL
https://docs.aws.amazon.com/kms/latest/developereuide/rotate-keys.html
AWS managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an AWS service that is integrated with AWS KMS. This CMK is unique to your AWS account and region. Only the service that created the AWS managed CMK can use it
You can login to you 1AM dashbaord . Click on "Encryption Keys" You will find the list based on the services you are using as follows:
• aws/elasticfilesystem 1 aws/lightsail
• aws/s3
• aws/rds and many more Detailed Guide: KMS
You can recognize AWS managed CMKs because their aliases have the format aws/service-name, such as aws/redshift. Typically, a service creates its AWS managed CMK in your account when you set up the service or the first time you use the CMfC
The AWS services that integrate with AWS KMS can use it in many different ways. Some services create AWS managed CMKs in your account. Other services require that you specify a customer managed CMK that you have created. And, others support both types of CMKs to allow you the ease of an AWS managed CMK or the control of a customer-managed CMK
Rotation period for CMKs is as follows:
• AWS managed CMKs: 1095 days
• Customer managed CMKs: 365 days
Since question mentions about "CMK where backing keys is managed by AWS", its Amazon(AWS) managed and its rotation period turns out to be 1095 days{every 3 years)
For more details, please check below AWS Docs: https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html The correct answer is: After 3 years
Submit your Feedback/Queries to our Experts

NEW QUESTION 6
A company wants to have an Intrusion detection system available for their VPC in AWS. They want to have complete control over the system. Which of the following would be ideal to implement?
Please select:

A. Use AWS WAF to catch all intrusions occurring on the systems in the VPC
B. Use a custom solution available in the AWS Marketplace
C. Use VPC Flow logs to detect the issues and flag them accordingly.
D. Use AWS Cloudwatch to monitor all traffic

Answer: B

Explanation:
Sometimes companies want to have custom solutions in place for monitoring Intrusions to their systems. In such a case, you can use the AWS Marketplace for looking at custom solutions.

Option A.C and D are all invalid because they cannot be used to conduct intrusion detection or prevention.
For more information on using custom security solutions please visit the below URL
https://d1.awsstatic.com/Marketplace/security/AWSMP_Security_Solution%200verview.pdf For more information on using custom security solutions please visit the below URL: https://d1 .awsstatic.com/Marketplace/security/AWSMP Security Solution%20Overview.pd1 The correct answer is: Use a custom solution available in the AWS Marketplace Submit your Feedback/Queries to our Experts

NEW QUESTION 7
You want to get a list of vulnerabilities for an EC2 Instance as per the guidelines set by the Center of Internet Security. How can you go about doing this?
Please select:

A. Enable AWS Guard Duty for the Instance
B. Use AWS Trusted Advisor
C. Use AWS inspector
D. UseAWSMacie

Answer: C

Explanation:
The AWS Inspector service can inspect EC2 Instances based on specific Rules. One of the rules packages is based on the guidelines set by the Center of Internet Security
Center for Internet security (CIS) Benchmarks
The CIS Security Benchmarks program provides well-defined, un-biased and consensus-based industry best practices to help organizations assess and improve their security. Amazon Web Services is a CIS Security Benchmarks Member company and the list of Amazon Inspector certifications can be viewed nere.
Option A is invalid because this can be used to protect an instance but not give the list of vulnerabilities
Options B and D are invalid because these services cannot give a list of vulnerabilities For more information on the guidelines, please visit the below URL:
* https://docs.aws.amazon.com/inspector/latest/userguide/inspector_cis.html The correct answer is: Use AWS Inspector
Submit your Feedback/Queries to our Experts

NEW QUESTION 8
You have just received an email from AWS Support stating that your AWS account might have been compromised. Which of the following steps would you look to carry out immediately. Choose 3 answers from the options below.
Please select:

A. Change the root account password.
B. Rotate all 1AM access keys
C. Keep all resources running to avoid disruption
D. Change the password for all 1AM user

Answer: ABD

Explanation:
One of the articles from AWS mentions what should be done in such a scenario
If you suspect that your account has been compromised, or if you have received a notification from AWS that the account has been compromised, perform the following tasks:
Change your AWS root account password and the passwords of any 1AM users. Delete or rotate all root and AWS Identity and Access Management (1AM) access keys.
Delete any resources on your account you didn't create, especially running EC2 instances, EC2 spot bids, or 1AM users.
Respond to any notifications you received from AWS Support through the AWS Support Center. Option C is invalid because there could be compromised instances or resources running on your environment. They should be shutdown or stopped immediately.
For more information on the article, please visit the below URL: https://aws.amazon.com/premiumsupport/knowledee-center/potential-account-compromise>
The correct answers are: Change the root account password. Rotate all 1AM access keys. Change the password for all 1AM users. Submit your Feedback/Queries to our Experts

NEW QUESTION 9
A security team must present a daily briefing to the CISO that includes a report of which of the company's thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day's report.
How can the security team fulfill these requirements?
Please select:

A. Use Amazon QuickSight and Cloud Trail to generate the report of out of compliance instances/server
B. Redeploy all out of compliance instances/servers using an AMI with the latest patches.
C. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ server
D. Use Systems Manager Patch Manger to install the missing patches.
E. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ server
F. Redeploy all out of1 compliance instances/servers using an AMI with the latest patches.
G. Use Trusted Advisor to generate the report of out of compliance instances/server
H. Use Systems Manger Patch Manger to install the missing patches.

Answer: B

Explanation:
Use the Systems Manger Patch Manger to generate the report and also install the missing patches The AWS Documentation mentions the following
AWS Systems Manager Patch Manager automates the process of patching managed instances with security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fileets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu
Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. You can scan instances to see only a report of missing patches, or you can scan and automatically install
all missing patches.
Option A is invalid because Amazon QuickSight and Cloud Trail cannot be used to generate the list of servers that don't meet compliance needs.
Option C is wrong because deploying instances via new AMI'S would impact the applications hosted on these servers
Option D is invalid because Amazon Trusted Advisor cannot be used to generate the list of servers that don't meet compliance needs.
For more information on the AWS Patch Manager, please visit the below URL: https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html (
The correct answer is: Use Systems Manger Patch Manger to generate the report of out of compliance instances/ servers. Use Systems Manager Patch Manger to install the missing patches. Submit your Feedback/Queries to our Experts

NEW QUESTION 10
Every application in a company's portfolio has a separate AWS account for development and production. The security team wants to prevent the root user and all 1AM users in the production accounts from accessing a specific set of unneeded services. How can they control this functionality? Please select:

A. Create a Service Control Policy that denies access to the service
B. Assemble all production accounts in an organizational uni
C. Apply the policy to that organizational unit.
D. Create a Service Control Policy that denies access to the service
E. Apply the policy to the root account.
F. Create an 1AM policy that denies access to the service
G. Associate the policy with an 1AM group and enlist all users and the root users in this group.
H. Create an 1AM policy that denies access to the service
I. Create a Config Rule that checks that all users have the policy m assigne
J. Trigger a Lambda function that adds the policy when found missing.

Answer: A

Explanation:
As an administrator of the master account of an organization, you can restrict which AWS services and individual API actions the users and roles in each member account can access. This restriction even overrides the administrators of member accounts in the organization. When AWS Organizations blocks access to a service or API action for a member account a user or role in that account can't access any prohibited service or API action, even if an administrator of a member account explicitly grants such permissions in an 1AM policy. Organization permissions overrule account permissions. Option B is invalid because service policies cannot be assigned to the root account at the account
level.
Option C and D are invalid because 1AM policies alone at the account level would not be able to suffice the requirement
For more information, please visit the below URL id=docs_orgs_console https://docs.aws.amazon.com/IAM/latest/UserGi manage attach-policy.html
The correct answer is: Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the policy to that organizational unit
Submit your Feedback/Queries to our Experts

NEW QUESTION 10
You are working in the media industry and you have created a web application where users will be able to upload photos they create to your website. This web

application must be able to call the S3 API in order to be able to function. Where should you store your API credentials whilst maintaining the maximum level of security?
Please select:

A. Save the API credentials to your PHP files.
B. Don't save your API credentials, instead create a role in 1AM and assign this role to an EC2 instance when you first create it.
C. Save your API credentials in a public Github repository.
D. Pass API credentials to the instance using instance userdat

Answer: B

Explanation:
Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, whil protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance. especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.
1AM roles are designed so that your applications can securely make API requests from your instances, without requiring yo manage the security credentials that the applications use.
Option A.C and D are invalid because using AWS Credentials in an application in production is a direct no recommendation 1 secure access
For more information on 1AM Roles, please visit the below URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html
The correct answer is: Don't save your API credentials. Instead create a role in 1AM and assign this role to an EC2 instance when you first create it
Submit your Feedback/Queries to our Experts

NEW QUESTION 12
You want to launch an EC2 Instance with your own key pair in AWS. How can you achieve this?
Choose 3 answers from the options given below. Please select:

A. Use a third party tool to create the Key pair
B. Create a new key pair using the AWS CLI
C. Import the public key into EC2
D. Import the private key into EC2

Answer: ABC

Explanation:
This is given in the AWS Documentation Creating a Key Pair
You can use Amazon EC2 to create your key pair. For more information, see Creating a Key Pair Using Amazon EC2.
Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. For more information, see Importing Your Own Public Key to Amazon EC2.
Option B is Correct, because you can use the AWS CLI to create a new key pair 1 https://docs.aws.amazon.com/cli/latest/userguide/cli-ec2-keypairs.html
Option D is invalid because the public key needs to be stored in the EC2 Instance For more information on EC2 Key pairs, please visit the below URL:
* https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs
The correct answers are: Use a third party tool to create the Key pair. Create a new key pair using the AWS CLI, Import the public key into EC2
Submit your Feedback/Queries to our Experts

NEW QUESTION 13
You have a set of Keys defined using the AWS KMS service. You want to stop using a couple of keys , but are not sure of which services are currently using the keys. Which of the following would be a
safe option to stop using the keys from further usage. Please select:

A. Delete the keys since anyway there is a 7 day waiting period before deletion
B. Disable the keys
C. Set an alias for the key
D. Change the key material for the key

Answer: B

Explanation:
Option A is invalid because once you schedule the deletion and waiting period ends, you cannot come back from the deletion process.
Option C and D are invalid because these will not check to see if the keys are being used or not The AWS Documentation mentions the following
Deleting a customer master key (CMK) in AWS Key Management Service (AWS KMS) is destructive and potentially dangerous. It deletes the key material and all metadata associated with the CMK, and is irreversible. After a CMK is deleted you can no longer decrypt the data that was encrypted under that CMK, which means that data becomes unrecoverable. You should delete a CMK only when you are sure that you don't need to use it anymore. If you are not sure, consider disabling the CMK
instead of deleting it. You can re-enable a disabled CMK if you need to use it again later, but you cannot recover a deleted CMK.
For more information on deleting keys from KMS, please visit the below URL: https://docs.aws.amazon.com/kms/latest/developereuide/deleting-keys.html
The correct answer is: Disable the keys Submit your Feedback/Queries to our Experts

NEW QUESTION 15
You are building a large-scale confidential documentation web server on AWSand all of the documentation for it will be stored on S3. One of the requirements is that it cannot be publicly accessible from S3 directly, and you will need to use Cloud Front to accomplish this. Which of the methods listed below would satisfy the requirements as outlined? Choose an answer from the options below
Please select:

A. Create an Identity and Access Management (1AM) user for CloudFront and grant access to the objects in your S3 bucket to that 1AM User.
B. Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
C. Create individual policies for each bucket the documents are stored in and in that policy grant access to only CloudFront.
D. Create an S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).

Answer: B

Explanation:
If you want to use CloudFront signed URLs or signed cookies to provide access to objects in your Amazon S3 bucket you probably also want to prevent users from accessing your Amazon S3 objects using Amazon S3 URLs. If users access your objects directly in Amazon S3, they bypass the controls provided by CloudFront signed URLs or signed cookies, for example, control over the date and time that a user can no longer access your content and control over which IP addresses can be used to access content. In addition, if user's access objects both through CloudFront and directly by using Amazon S3 URLs, CloudFront ace logs are less useful because they're incomplete.
Option A is invalid because you need to create a Origin Access Identity for Cloudfront and not an 1AM user
Option C and D are invalid because using policies will not help fulfil the requirement For more information on Origin Access Identity please see the below Link:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-contentrestrictine- access-to-s3.htmll
The correct answer is: Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.
(
Submit your Feedback/Queries to our Experts

NEW QUESTION 16
Your company makes use of S3 buckets for storing dat

A. There is a company policy that all services should have logging enable
B. How can you ensure thatlogging is always enabled for created S3 buckets in the AWS Account? Please select:
C. Use AWS Inspector to inspect all S3 buckets and enable logging for those where it is not enabled
D. Use AWS Config Rules to check whether logging is enabled for buckets
E. Use AWS Cloudwatch metrics to check whether logging is enabled for buckets
F. Use AWS Cloudwatch logs to check whether logging is enabled for buckets

Answer: B

Explanation:
This is given in the AWS Documentation as an example rule in AWS Config Example rules with triggers
Example rule with configuration change trigger
1. You add the AWS Config managed rule, S3_BUCKET_LOGGING_ENABLED, to your account to check whether your Amazon S3 buckets have logging enabled.
2. The trigger type for the rule is configuration changes. AWS Config runs the evaluations for the rule when an Amazon S3 bucket is created, changed, or deleted.
3. When a bucket is updated, the configuration change triggers the rule and AWS Config evaluates whether the bucket is compliant against the rule.
Option A is invalid because AWS Inspector cannot be used to scan all buckets
Option C and D are invalid because Cloudwatch cannot be used to check for logging enablement for buckets.
For more information on Config Rules please see the below Link: https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html
The correct answer is: Use AWS Config Rules to check whether logging is enabled for buckets Submit your Feedback/Queries to our Experts

NEW QUESTION 20
A security engineer must ensure that all infrastructure launched in the company AWS account be monitored for deviation from compliance rules, specifically that all EC2 instances are launched from one of a specified list of AM Is and that all attached EBS volumes are encrypted. Infrastructure not in compliance should be terminated. What combination of steps should the Engineer implement? Select 2 answers from the options given below.
Please select:

A. Set up a CloudWatch event based on Trusted Advisor metrics
B. Trigger a Lambda function from a scheduled CloudWatch event that terminates non-compliant infrastructure.
C. Set up a CloudWatch event based on Amazon inspector findings
D. Monitor compliance with AWS Config Rules triggered by configuration changes
E. Trigger a CLI command from a CloudWatch event that terminates the infrastructure

Answer: BD

Explanation:
You can use AWS Config to monitor for such Event
Option A is invalid because you cannot set Cloudwatch events based on Trusted Advisor checks.
Option C is invalid Amazon inspector cannot be used to check whether instances are launched from a specific A
Option E is invalid because triggering a CLI command is not the preferred option, instead you should use Lambda functions for all automation purposes.
For more information on Config Rules please see the below Link: https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html
These events can then trigger a lambda function to terminate instances For more information on Cloudwatch events please see the below Link:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents.
(
The correct answers are: Trigger a Lambda function from a scheduled Cloudwatch event that terminates non-compliant infrastructure., Monitor compliance with AWS Config Rules triggered by configuration changes
Submit your Feedback/Queries to our Experts

NEW QUESTION 23
You need to have a cloud security device which would allow to generate encryption keys based on FIPS 140-2 Level 3. Which of the following can be used for this purpose.
Please select:

A. AWS KMS
B. AWS Customer Keys
C. AWS managed keys
D. AWS Cloud HSM

Answer: AD

Explanation:
AWS Key Management Service (KMS) now uses FIPS 140-2 validated hardware security modules (HSM) and supports FIPS 140-2 validated endpoints, which

provide independent assurances about the confidentiality and integrity of your keys.
All master keys in AWS KMS regardless of their creation date or origin are automatically protected using FIPS 140-2 validated
HSMs. defines four levels of security, simply named "Level 1" to "Level 4". It does not specify in detail what level of security is required by any particular application.
• FIPS 140-2 Level 1 the lowest, imposes very limited requirements; loosely, all components must
be "production-grade" anc various egregious kinds of insecurity must be absent
• FIPS 140-2 Level 2 adds requirements for physical tamper-evidence and role-based authentication.
• FIPS 140-2 Level 3 adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.
• FIPS 140-2 Level 4 makes the physical security requirements more stringent and requires robustness against environmental attacks.
AWSCIoudHSM provides you with a FIPS 140-2 Level 3 validated single-tenant HSM cluster in your Amazon Virtual Private Cloud (VPQ to store and use your keys. You have exclusive control over how your keys are used via an authentication mechanism independent from AWS. You interact with keys in your AWS CloudHSM cluster similar to the way you interact with your applications running in Amazon EC2.
AWS KMS allows you to create and control the encryption keys used by your applications and supported AWS services in multiple regions around the world from a single console. The service uses a FIPS 140-2 validated HSM to protect the security of your keys. Centralized management of all your keys in AWS KMS lets you enforce who can use your keys under which conditions, when they get rotated, and who can manage them.
AWS KMS HSMs are validated at level 2 overall and at level 3 in the following areas:
• Cryptographic Module Specification
• Roles, Services, and Authentication
• Physical Security
• Design Assurance
So I think that we can have 2 answers for this question. Both A & D.
• https://aws.amazon.com/blo15s/security/aws-key-management-service- now-ffers-flps-140-2- validated-cryptographic-m< enabling-easier-adoption-of-the-service-for-regulated-workloads/
• https://a ws.amazon.com/cloudhsm/faqs/
• https://aws.amazon.com/kms/faqs/
• https://en.wikipedia.org/wiki/RPS
The AWS Documentation mentions the following
AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud. With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs. CloudHSM offers you the filexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java
Cryptography Extensions ()CE). and Microsoft CryptoNG (CNG) libraries. CloudHSM is also standardscompliant and enables you to export all of your keys to most other commercially-available HSMs. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups. CloudHSM also enables you to scale quickly by adding and removing HSM capacity on-demand, with no up-front costs.
All other options are invalid since AWS Cloud HSM is the prime service that offers FIPS 140-2 Level 3 compliance
For more information on CloudHSM, please visit the following url https://aws.amazon.com/cloudhsm;
The correct answers are: AWS KMS, AWS Cloud HSM Submit your Feedback/Queries to our Experts

NEW QUESTION 25
Which technique can be used to integrate AWS 1AM (Identity and Access Management) with an on Questions & Answers PDF P-63
premise LDAP (Lightweight Directory Access Protocol) directory service? Please select:

A. Use an 1AM policy that references the LDAP account identifiers and the AWS credentials.
B. Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP.
C. Use AWS Security Token Service from an identity broker to issue short-lived AWS credentials.
D. Use 1AM roles to automatically rotate the 1AM credentials when LDAP credentials are update

Answer: B

Explanation:
On the AWS Blog site the following information is present to help on this context
The newly released whitepaper. Single Sign-On: Integrating AWS, OpenLDAP, and Shibboleth, will help you integrate your existing LDAP-based user directory with AWS. When you integrate your existing directory with AWS, your users can access AWS by using their existing credentials. This means that your users don't need to maintain yet another user name and password just to access AWS resources.
Option A.C and D are all invalid because in this sort of configuration, you have to use SAML to enable single sign on.
For more information on integrating AWS with LDAP for Single Sign-On, please visit the following URL:
https://aws.amazon.eom/blogs/security/new-whitepaper-sinEle-sign-on-inteErating-aws-openldapand- shibboleth/l
The correct answer is: Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP. Submit your Feedback/Queries to our Experts

NEW QUESTION 30
You have a requirement to serve up private content using the keys available with Cloudfront. How can this be achieved?
Please select:

A. Add the keys to the backend distribution.
B. Add the keys to the S3 bucket
C. Create pre-signed URL's
D. Use AWS Access keys

Answer: C

Explanation:
Option A and B are invalid because you will not add keys to either the backend distribution or the S3 bucket.
Option D is invalid because this is used for programmatic access to AWS resources
You can use Cloudfront key pairs to create a trusted pre-signed URL which can be distributed to users Specifying the AWS Accounts That Can Create Signed URLs and Signed Cookies (Trusted Signers) Topics
• Creating CloudFront Key Pairs for Your Trusted Signers
• Reformatting the CloudFront Private Key (.NET and Java Only)
• Adding Trusted Signers to Your Distribution

• Verifying that Trusted Signers Are Active (Optional) 1 Rotating CloudFront Key Pairs
To create signed URLs or signed cookies, you need at least one AWS account that has an active CloudFront key pair. This accou is known as a trusted signer.
The trusted signer has two purposes:
• As soon as you add the AWS account ID for your trusted signer to your distribution, CloudFront starts to require that users us signed URLs or signed cookies to access your objects.
' When you create signed URLs or signed cookies, you use the private key from the trusted signer's key pair to sign a portion of the URL or the cookie. When someone requests a restricted object CloudFront compares the signed portion of the URL or cookie with the unsigned portion to verify that the URL or cookie hasn't been tampered with. CloudFront also verifies that the URL or cookie is valid, meaning, for example, that the expiration date and time hasn't passed.
For more information on Cloudfront private trusted content please visit the following URL:
• https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-contenttrusted- s
The correct answer is: Create pre-signed URL's Submit your Feedback/Queries to our Experts

NEW QUESTION 32
Your application currently uses customer keys which are generated via AWS KMS in the US east region. You now want to use the same set of keys from the EU-Central region. How can this be accomplished?
Please select:

A. Export the key from the US east region and import them into the EU-Central region
B. Use key rotation and rotate the existing keys to the EU-Central region
C. Use the backing key from the US east region and use it in the EU-Central region
D. This is not possible since keys from KMS are region specific

Answer: D

Explanation:
Option A is invalid because keys cannot be exported and imported across regions. Option B is invalid because key rotation cannot be used to export keys
Option C is invalid because the backing key cannot be used to export keys This is mentioned in the AWS documentation
What geographic region are my keys stored in?
Keys are only stored and used in the region in which they are created. They cannot be transferred to another region. For example; keys created in the EU-Central (Frankfurt) region are only stored and used within the EU-Central (Frankfurt) region
For more information on KMS please visit the following URL: https://aws.amazon.com/kms/faqs/
The correct answer is: This is not possible since keys from KMS are region specific Submit your Feedback/Queries to our Experts

NEW QUESTION 33
You have a set of Customer keys created using the AWS KMS service. These keys have been used for around 6 months. You are now trying to use the new KMS features for the existing set of key's but are not able to do so. What could be the reason for this.
Please select:

A. You have not explicitly given access via the key policy
B. You have not explicitly given access via the 1AM policy
C. You have not given access via the 1AM roles
D. You have not explicitly given access via 1AM users

Answer: A

Explanation:
By default, keys created in KMS are created with the default key policy. When features are added to KMS, you need to explii update the default key policy for these keys.
Option B,C and D are invalid because the key policy is the main entity used to provide access to the keys
For more information on upgrading key policies please visit the following URL: https://docs.aws.ama20n.com/kms/latest/developerguide/key-policy-upgrading.html
(
The correct answer is: You have not explicitly given access via the key policy Submit your Feedback/Queries to our Experts

NEW QUESTION 37
A customer has an instance hosted in the AWS Public Cloud. The VPC and subnet used to host the Instance have been created with the default settings for the Network Access Control Lists. They need to provide an IT Administrator secure access to the underlying instance. How can this be accomplished.
Please select:

A. Ensure the Network Access Control Lists allow Inbound SSH traffic from the IT Administrator's Workstation
B. Ensure the Network Access Control Lists allow Outbound SSH traffic from the IT Administrator's Workstation
C. Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation
D. Ensure that the security group allows Outbound SSH traffic from the IT Administrator's Workstation

Answer: C

Explanation:
Options A & B are invalid as default NACL rule will allow all inbound and outbound traffic.
The requirement is that the IT administrator should be able to access this EC2 instance from his workstation. For that we need to enable the Security Group of EC2 instance to allow traffic from the IT administrator's workstation. Hence option C is correct.
Option D is incorrect as we need to enable the Inbound SSH traffic on the EC2 instance Security Group since the traffic originate' , from the IT admin's workstation.
The correct answer is: Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation Submit your Feedback/Queries to our Experts

NEW QUESTION 39
A company hosts data in S3. There is now a mandate that going forward all data in the S3 bucket needs to encrypt at rest. How can this be achieved?
Please select:

A. Use AWS Access keys to encrypt the data
B. Use SSL certificates to encrypt the data

C. Enable server side encryption on the S3 bucket
D. Enable MFA on the S3 bucket

Answer: C

Explanation:
The AWS Documentation mentions the following
Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects.
Options A and B are invalid because neither Access Keys nor SSL certificates can be used to encrypt data.
Option D is invalid because MFA is just used as an extra level of security for S3 buckets For more information on S3 server side encryption, please refer to the below Link: https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html
Submit your Feedback/Queries to our Experts

NEW QUESTION 43
One of your company's EC2 Instances have been compromised. The company has strict po thorough investigation on finding the culprit for the security breach. What would you do in from the options given below.
Please select:

A. Take a snapshot of the EBS volume
B. Isolate the machine from the network
C. Make sure that logs are stored securely for auditing and troubleshooting purpose
D. Ensure all passwords for all 1AM users are changed
E. Ensure that all access keys are rotate

Answer: ABC

Explanation:
Some of the important aspects in such a situation are
1) First isolate the instance so that no further security harm can occur on other AWS resources
2) Take a snapshot of the EBS volume for further investigation. This is incase if you need to shutdown the initial instance and do a separate investigation on the data
3) Next is Option C. This indicates that we have already got logs and we need to make sure that it is stored securely so that n unauthorised person can access it and manipulate it.
Option D and E are invalid because they could have adverse effects for the other 1AM users. For more information on adopting a security framework, please refer to below URL https://d1 .awsstatic.com/whitepapers/compliance/NIST Cybersecurity Framework
Note:
In the question we have been asked to take actions to find the culprit and to help the investigation or to further reduce the damage that has happened due to the security breach. So by keeping logs secure is one way of helping the investigation.
The correct answers are: Take a snapshot of the EBS volume. Isolate the machine from the network. Make sure that logs are stored securely for auditing and troubleshooting purpose
Submit your Feedback/Queries to our Experts

NEW QUESTION 46
A company has a large set of keys defined in AWS KMS. Their developers frequently use the keys for the applications being developed. What is one of the ways that can be used to reduce the cost of accessing the keys in the AWS KMS service.
Please select:

A. Enable rotation of the keys
B. Use Data key caching
C. Create an alias of the key
D. Use the right key policy

Answer: B

Explanation:
The AWS Documentation mentions the following
Data key caching stores data keys and related cryptographic material in a cache. When you encrypt or decrypt data, the AWS Encryption SDK looks for a matching data key in the cache. If it finds a match, it uses the cached data key rather than generatir a new one. Data key caching can improve performance, reduce cost, and help you stay within service limits as your application scales. Option A.C and D are all incorrect since these options will not impact how the key is used.
For more information on data key caching, please refer to below URL: https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/data-key-cachine.htmll
The correct answer is: Use Data key caching Submit your Feedback/Queries to our Experts

NEW QUESTION 47
A company has set up the following structure to ensure that their S3 buckets always have logging enabled

If there are any changes to the configuration to an S3 bucket, a config rule gets checked. If logging is disabled , then Lambda function is invoked. This Lambda function will again enable logging on the S3 bucket. Now there is an issue being encoutered with the entire flow. You have verified that the Lambda function is being invoked. But when logging is disabled for the bucket, the lambda function does not enable it again. Which of the following could be an issue
Please select:

A. The AWS Config rule is not configured properly
B. The AWS Lambda function does not have appropriate permissions for the bucket
C. The AWS Lambda function should use Node.js instead of python.
D. You need to also use the API gateway to invoke the lambda function

Answer: B

Explanation:
The most probable cause is that you have not allowed the Lambda functions to have the appropriate permissions on the S3 bucket to make the relevant changes.
Option A is invalid because this is more of a permission instead of a configuration rule issue. Option C is invalid because changing the language will not be the core solution.
Option D is invalid because you don't necessarily need to use the API gateway service
For more information on accessing resources from a Lambda function, please refer to below URL https://docs.aws.amazon.com/lambda/latest/ds/accessing-resources.htmll
The correct answer is: The AWS Lambda function does not have appropriate permissions for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 51
Your company has a set of EC2 Instances defined in AWS. They need to ensure that all traffic packets are monitored and inspected for any security threats. How can this be achieved? Choose 2 answers from the options given below
Please select:

A. Use a host based intrusion detection system
B. Use a third party firewall installed on a central EC2 instance
C. Use VPC Flow logs
D. Use Network Access control lists logging

Answer: AB

Explanation:
If you want to inspect the packets themselves, then you need to use custom based software A diagram representation of this is given in the AWS Security best practices

Option C is invalid because VPC Flow logs cannot conduct packet inspection. For more information on AWS Security best practices, please refer to below URL:
The correct answers are: Use a host based intrusion detection system. Use a third party firewall installed on a central EC2
Submit your Feedback/Queries to our Experts

NEW QUESTION 55
Your company use AWS KMS for management of its customer keys. From time to time, there is a requirement to delete existing keys as part of housekeeping activities. What can be done during the deletion process to verify that the key is no longer being used.
Please select:

A. Use CloudTrail to see if any KMS API request has been issued against existing keys
B. Use Key policies to see the access level for the keys
C. Rotate the keys once before deletion to see if other services are using the keys
D. Change the 1AM policy for the keys to see if other services are using the keys

Answer: A

Explanation:
The AWS lentation mentions the following
You can use a combination of AWS CloudTrail, Amazon CloudWatch Logs, and Amazon Simple Notification Service (Amazon SNS) to create an alarm that notifies you of AWS KMS API requests that attempt to use a customer master key (CMK) that is pending deletion. If you receive a notification from such an alarm, you might want to cancel deletion of the CMK to give yourself more time to determine whether you want to delete it
Options B and D are incorrect because Key policies nor 1AM policies can be used to check if the keys are being used.
Option C is incorrect since rotation will not help you check if the keys are being used. For more information on deleting keys, please refer to below URL:
https://docs.aws.amazon.com/kms/latest/developereuide/deletine-keys-creatine-cloudwatchalarm. html
The correct answer is: Use CloudTrail to see if any KMS API request has been issued against existing keys Submit your Feedback/Queries to our Experts

NEW QUESTION 59
You want to track access requests for a particular S3 bucket. How can you achieve this in the easiest possible way?
Please select:

A. Enable server access logging for the bucket
B. Enable Cloudwatch metrics for the bucket
C. Enable Cloudwatch logs for the bucket
D. Enable AWS Config for the S3 bucket

Answer: A

Explanation:
The AWS Documentation mentions the foil

To track requests for access to your bucket you can enable access logging. Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code, if any.
Options B and C are incorrect Cloudwatch is used for metrics and logging and cannot be used to track access requests.
Option D is incorrect since this can be used for Configuration management but for not for tracking S3 bucket requests.
For more information on S3 server logs, please refer to below UF https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLoes.html
The correct answer is: Enable server access logging for the bucket Submit your Feedback/Queries to our Experts

NEW QUESTION 63
A company has hired a third-party security auditor, and the auditor needs read-only access to all AWS resources and logs of all VPC records and events that have occurred on AWS. How can the company meet the auditor's requirements without comprising security in the AWS environment? Choose the correct answer from the options below
Please select:

A. Create a role that has the required permissions for the auditor.
B. Create an SNS notification that sends the CloudTrail log files to the auditor's email when CIoudTrail delivers the logs to S3, but do not allow the auditor access to the AWS environment.
C. The company should contact AWS as part of the shared responsibility model, and AWS will grant required access to th^ third-party auditor.
D. Enable CloudTrail logging and create an 1AM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs.

Answer: D

Explanation:
AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure. CloudTrail provides a history of AWS API calls for your account including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This history simplifies security analysis, resource change tracking, and troubleshooting.
Option A and C are incorrect since Cloudtrail needs to be used as part of the solution Option B is incorrect since the auditor needs to have access to Cloudtrail
For more information on cloudtrail, please visit the below URL: https://aws.amazon.com/cloudtraiL
The correct answer is: Enable CloudTrail logging and create an 1AM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs. Submit your Feedback/Queries to our Experts

NEW QUESTION 65
A large organization is planning on AWS to host their resources. They have a number of autonomous departments that wish to use AWS. What could be the strategy to adopt for managing the accounts. Please select:

A. Use multiple VPCs in the account each VPC for each department
B. Use multiple 1AM groups, each group for each department
C. Use multiple 1AM roles, each group for each department
D. Use multiple AWS accounts, each account for each department

Answer: D

Explanation:
A recommendation for this is given in the AWS Security best practices

Option A is incorrect since this would be applicable for resources in a VPC Options B and C are incorrect since operationally it would be difficult to manage For more information on AWS Security best practices please refer to the below URL
https://d1.awsstatic.com/whitepapers/Security/AWS Security Best Practices.pdl
The correct answer is: Use multiple AWS accounts, each account for each department Submit your Feedback/Queries to our Experts

NEW QUESTION 69
Your company has been using AWS for the past 2 years. They have separate S3 buckets for logging the various AWS services that have been used. They have hired an external vendor for analyzing their log files. They have their own AWS account. What is the best way to ensure that the partner account can access the log files in the company account for analysis. Choose 2 answers from the options given below
Please select:

A. Create an 1AM user in the company account
B. Create an 1AM Role in the company account
C. Ensure the 1AM user has access for read-only to the S3 buckets
D. Ensure the 1AM Role has access for read-only to the S3 buckets

Answer: BD

Explanation:
The AWS Documentation mentions the following
To share log files between multiple AWS accounts, you must perform the following general steps. These steps are explained in detail later in this section.
Create an 1AM role for each account that you want to share log files with.
For each of these 1AM roles, create an access policy that grants read-only access to the account you want to share the log files with.
Have an 1AM user in each account programmatically assume the appropriate role and retrieve the log files.
Options A and C are invalid because creating an 1AM user and then sharing the 1AM user credentials with the vendor is a direct 'NO' practise from a security perspective.
For more information on sharing cloudtrail logs files, please visit the following URL https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-sharine-loes.htmll
The correct answers are: Create an 1AM Role in the company account Ensure the 1AM Role has access for read-only to the S3 buckets
Submit your Feedback/Queries to our Experts

NEW QUESTION 74
Which of the below services can be integrated with the AWS Web application firewall service. Choose 2 answers from the options given below

Please select:

A. AWS Cloudfront
B. AWS Lambda
C. AWS Application Load Balancer
D. AWS Classic Load Balancer

Answer: AC

Explanation:
The AWS documentation mentions the following on the Application Load Balancer
AWS WAF can be deployed on Amazon CloudFront and the Application Load Balancer (ALB). As part of Amazon CloudFront it car be part of your Content Distribution Network (CDN) protecting your resources and content at the Edge locations and as part of the Application Load Balancer it can
protect your origin web servers running behind the ALBs.
Options B and D are invalid because only Cloudfront and the Application Load Balancer services are supported by AWS WAF.
For more information on the web application firewall please refer to the below URL: https://aws.amazon.com/waf/faq;
The correct answers are: AWS Cloudfront AWS Application Load Balancer Submit your Feedback/Queries to our Experts

NEW QUESTION 75
A company hosts critical data in an S3 bucket. Even though they have assigned the appropriate permissions to the bucket, they are still worried about data deletion. What measures can be taken to restrict the risk of data deletion on the bucket. Choose 2 answers from the options given below Please select:

A. Enable versioning on the S3 bucket
B. Enable data at rest for the objects in the bucket
C. Enable MFA Delete in the bucket policy
D. Enable data in transit for the objects in the bucket

Answer: AC

Explanation:
One of the AWS Security blogs mentions the followinj
Versioning keeps multiple versions of an object in the same bucket. When you enable it on a bucket Amazon S3 automatically adds a unique version ID to every object stored in the bucket. At that point, a simple DELETE action does not permanently delete an object version; it merely associates a delete marker with the object. If you want to permanently delete an object version, you must specify its version ID in your DELETE request.
You can add another layer of protection by enabling MFA Delete on a versioned bucket. Once you do so, you must provide your AWS accounts access keys and a valid code from the account's MFA device in order to permanently delete an object version or suspend or reactivate versioning on the bucket. Option B is invalid because enabling encryption does not guarantee risk of data deletion.
Option D is invalid because this option does not guarantee risk of data deletion.
For more information on AWS S3 versioning and MFA please refer to the below URL: https://aws.amazon.com/blogs/security/securing-access-to-aws-using-mfa-part-3/

NEW QUESTION 80
You are designing a connectivity solution between on-premises infrastructure and Amazon VPC. Your server's on-premises will be communicating with your VPC instances. You will be establishing IPSec
tunnels over the internet. Yo will be using VPN gateways and terminating the IPsec tunnels on AWSsupported customer gateways. Which of the following objectives would you achieve by
implementing an IPSec tunnel as outlined above? Choose 4 answers form the options below Please select:

A. End-to-end protection of data in transit
B. End-to-end Identity authentication
C. Data encryption across the internet
D. Protection of data in transit over the Internet
E. Peer identity authentication between VPN gateway and customer gateway
F. Data integrity protection across the Internet

Answer: CDEF

Explanation:
Since the Web server needs to talk to the database server on port 3306 that means that the database server should allow incoming traffic on port 3306. The below table from the aws documentation shows how the security groups should be set up.

Option B is invalid because you need to allow incoming access for the database server from the WebSecGrp security group.
Options C and D are invalid because you need to allow Outbound traffic and not inbound traffic For more information on security groups please visit the below Link: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC Scenario2.html
The correct answer is: Allow Inbound on port 3306 for Source Web Server Security Group WebSecGrp. Submit your Feedback/Queries to our Experts

NEW QUESTION 82
Your developer is using the KMS service and an assigned key in their Java program. They get the below error when
running the code
arn:aws:iam::113745388712:user/UserB is not authorized to perform: kms:DescribeKey Which of the following could help resolve the issue?
Please select:

A. Ensure that UserB is given the right IAM role to access the key
B. Ensure that UserB is given the right permissions in the IAM policy
C. Ensure that UserB is given the right permissions in the Key policy
D. Ensure that UserB is given the right permissions in the Bucket policy

Answer: C

Explanation:

You need to ensure that UserB is given access via the Key policy for the Key

Option is invalid because you don't assign roles to 1AM users For more information on Key policies please visit the below Link:
https://docs.aws.amazon.com/kms/latest/developerguide/key-poli
The correct answer is: Ensure that UserB is given the right permissions in the Key policy

NEW QUESTION 86
Your company has an external web site. This web site needs to access the objects in an S3 bucket. Which of the following would allow the web site to access the objects in the most secure manner? Please select:

A. Grant public access for the bucket via the bucket policy
B. Use the aws:Referer key in the condition clause for the bucket policy
C. Use the aws:sites key in the condition clause for the bucket policy
D. Grant a role that can be assumed by the web site

Answer: B

Explanation:
An example of this is given intheAWS Documentatioi Restricting Access to a Specific HTTP Referrer
Suppose you have a website with domain name (www.example.com or example.com) with links to photos and videos stored in your S3 bucket examplebucket. By default, all the S3 resources are private, so only the AWS account that created the resources can access them. To allow read access to these objects from your website, you can add a bucket policy that allows s3:GetObject permission with a condition, using the aws:referer key, that the get request must originate from specific webpages. The following policy specifies the StringLike condition with the aws:Referer condition key.

Option A is invalid because giving public access is not a secure way to provide access Option C is invalid because aws:sites is not a valid condition key Option D is invalid because 1AM roles will not be assigned to web sites
For more information on example bucket policies please visit the below Link:
1 https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html
The correct answer is: Use the aws:Referer key in the condition clause for the bucket policy Submit your Feedback/Queries to our Experts

NEW QUESTION 89
An organization has setup multiple 1AM users. The organization wants that each 1AM user accesses the 1AM console only within the organization and not from outside. How can it achieve this? Please select:

A. Create an 1AM policy with the security group and use that security group for AWS console login
B. Create an 1AM policy with a condition which denies access when the IP address range is not from the organization
C. Configure the EC2 instance security group which allows traffic only from the organization's IP range
D. Create an 1AM policy with VPC and allow a secure gateway between the organization and AWS Console

Answer: B

Explanation:
You can actually use a Deny condition which will not allow the person to log in from outside. The below example shows the Deny condition to ensure that any address specified in the source address is not allowed to access the resources in aws.
Option A is invalid because you don't mention the security group in the 1AM policy Option C is invalid because security groups by default don't allow traffic
Option D is invalid because the 1AM policy does not have such an option For more information on 1AM policy conditions, please visit the URL: http://docs.aws.amazon.com/IAM/latest/UserGuide/access pol examples.htm l#iam-policy-example-ec2-two-condition!
The correct answer is: Create an 1AM policy with a condition which denies access when the IP address range is not from the organization
Submit your Feedback/Queries to our Experts

NEW QUESTION 92
You are creating a Lambda function which will be triggered by a Cloudwatch Event. The data from these events needs to be stored in a DynamoDB table. How should the Lambda function be given access to the DynamoDB table?
Please select:

A. Put the AWS Access keys in the Lambda function since the Lambda function by default is secure
B. Use an 1AM role which has permissions to the DynamoDB table and attach it to the Lambda function.
C. Use the AWS Access keys which has access to DynamoDB and then place it in an S3 bucket.
D. Create a VPC endpoint for the DynamoDB tabl
E. Access the VPC endpoint from the Lambda function.

Answer: B

Explanation:
AWS Lambda functions uses roles to interact with other AWS services. So use an 1AM role which has permissions to the DynamoDB table and attach it to the Lambda function.
Options A and C are all invalid because you should never use AWS keys for access. Option D is invalid because the VPC endpoint is used for VPCs
For more information on Lambda function Permission model, please visit the URL https://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html
The correct answer is: Use an 1AM role which has permissions to the DynamoDB table and attach it to the Lambda function. Submit your Feedback/Queries to our Experts

NEW QUESTION 93
Your company is planning on using AWS EC2 and ELB for deployment for their web applications. The security policy mandates that all traffic should be encrypted. Which of the following options will ensure that this requirement is met. Choose 2 answers from the options below.
Please select:

A. Ensure the load balancer listens on port 80
B. Ensure the load balancer listens on port 443
C. Ensure the HTTPS listener sends requests to the instances on port 443
D. Ensure the HTTPS listener sends requests to the instances on port 80

Answer: BC

Explanation:
The AWS Documentation mentions the following
You can create a load balancer that listens on both the HTTP (80) and HTTPS (443) ports. If you specify that the HTTPS listener sends requests to the instances on port 80, the load balancer terminates the requests and communication from the load balancer to the instances is not encrypted, if the HTTPS listener sends requests to the instances on port 443, communication from the load balancer to the instances is encrypted.
Option A is invalid because there is a need for secure traffic, so port 80 should not be used Option D is invalid because for the HTTPS listener you need to use port 443
For more information on HTTPS with ELB, please refer to the below Link: https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-loadbalancer. htmll
The correct answers are: Ensure the load balancer listens on port 443, Ensure the HTTPS listener sends requests to the instances on port 443
Submit your Feedback/Queries to our Experts

NEW QUESTION 95
You have private video content in S3 that you want to serve to subscribed users on the Internet. User
IDs, credentials, and subscriptions are stored in an Amazon RDS database. Which configuration will allow you to securely serve private content to your users?
Please select:

A. Generate pre-signed URLs for each user as they request access to protected S3 content
B. Create an 1AM user for each subscribed user and assign the GetObject permission to each 1AM user
C. Create an S3 bucket policy that limits access to your private content to only your subscribed users'credentials
D. Crpafp a Cloud Front Clriein Identity user for vnur suhsrrihprl users and assign the GptOhiprt oprmissinn to this user

Answer: A

Explanation:
All objects and buckets by default are private. The pre-signed URLs are useful if you want your user/customer to be able upload a specific object to your bucket but you don't require them to have AWS security credentials or permissions. When you create a pre-signed URL, you must provide your security credentials, specify a bucket name, an object key, an HTTP method (PUT for uploading objects), and an expiration date and time. The pre-signed URLs are valid only for the specified duration.
Option B is invalid because this would be too difficult to implement at a user level. Option C is invalid because this is not possible
Option D is invalid because this is used to serve private content via Cloudfront For more information on pre-signed urls, please refer to the Link: http://docs.aws.amazon.com/AmazonS3/latest/dev/PresienedUrlUploadObiect.htmll
The correct answer is: Generate pre-signed URLs for each user as they request access to protected S3 content Submit your Feedback/Queries to our Experts

NEW QUESTION 98
You currently operate a web application In the AWS US-East region. The application runs on an autoscaled layer of EC2 instances and an RDS Multi-AZ database. Your IT security compliance officer has

tasked you to develop a reliable and durable logging solution to track changes made to your EC2.IAM and RDS resources. The solution must ensure the integrity and confidentiality of your log dat

A. Which of these solutions would you recommend? Please select:
B. Create a new CloudTrail trail with one new S3 bucket to store the logs and with the global services option selecte
C. Use 1AM roles S3 bucket policies and Mufti Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.
D. Create a new CloudTrail with one new S3 bucket to store the log
E. Configure SNS to send log file delivery notifications to your management syste
F. Use 1AM roles and S3 bucket policies on the S3 bucket that stores your logs.
G. Create a new CloudTrail trail with an existing S3 bucket to store the logs and with the global services option selecte
H. Use S3 ACLsand Multi Factor Authentication (MFA) Delete on the S3 bucket that stores your logs.
I. Create three new CloudTrail trails with three new S3 buckets to store the logs one for the AWS Management console, one for AWS SDKs and one for command line tool
J. Use 1AM roles and S3 bucket policies on the S3 buckets that store your logs.

Answer: A

Explanation:
AWS Identity and Access Management (1AM) is integrated with AWS CloudTrail, a service that logs AWS events made by or on behalf of your AWS account. CloudTrail logs authenticated AWS API calls and also AWS sign-in events, and collects this event information in files that are delivered to Amazon S3 buckets.
You need to ensure that all services are included. Hence option B is partially correct. Option B is invalid because you need to ensure that global services is select
Option C is invalid because you should use bucket policies
Option D is invalid because you should ideally just create one S3 bucket For more information on Cloudtrail, please visit the below URL: http://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-inteeration.html
The correct answer is: Create a new CloudTrail trail with one new S3 bucket to store the logs and with
the global services o selected. Use 1AM roles S3 bucket policies and Mulrj Factor Authentication (MFA) Delete on the S3 bucket that stores your l(
Submit your Feedback/Queries to our Experts

NEW QUESTION 102
Your company has just set up a new central server in a VPC. There is a requirement for other teams who have their servers located in different VPC's in the same region to connect to the central server. Which of the below options is best suited to achieve this requirement.
Please select:

A. Set up VPC peering between the central server VPC and each of the teams VPCs.
B. Set up AWS DirectConnect between the central server VPC and each of the teams VPCs.
C. Set up an IPSec Tunnel between the central server VPC and each of the teams VPCs.
D. None of the above options will work.

Answer: A

Explanation:
A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single region. Options B and C are invalid because you need to use VPC Peering
Option D is invalid because VPC Peering is available
For more information on VPC Peering please see the below Link: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html
The correct answer is: Set up VPC peering between the central server VPC and each of the teams VPCs. Submit your Feedback/Queries to our Experts

NEW QUESTION 106
A company's AWS account consists of approximately 300 IAM users. Now there is a mandate that an access change is required for 100 IAM users to have unlimited privileges to S3.As a system administrator, how can you implement this effectively so that there is no need to apply the policy at the individual user level?
Please select:

A. Create a new role and add each user to the IAM role
B. Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group
C. Create a policy and apply it to multiple users using a JSON script
D. Create an S3 bucket policy with unlimited access which includes each user's AWS account ID

Answer: B

Explanation:
Option A is incorrect since you don't add a user to the 1AM Role Option C is incorrect since you don't assign multiple users to a policy Option D is incorrect since this is not an ideal approach
An 1AM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group
For more information on 1AM Groups, just browse to the below URL:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_eroups.html
The correct answer is: Use the 1AM groups and add users, based upon their role, to different groups and apply the policy to group
Submit your Feedback/Queries to our Experts

NEW QUESTION 108
Your CTO is very worried about the security of your AWS account. How best can you prevent hackers from completely hijacking your account?
Please select:

A. Use short but complex password on the root account and any administrators.
B. Use AWS 1AM Geo-Lock and disallow anyone from logging in except for in your city.
C. Use MFA on all users and accounts, especially on the root account.
D. Don't write down or remember the root account password after creating the AWS accoun

Answer: C

Explanation:
Multi-factor authentication can add one more layer of security to your AWS account Even when you go to your Security Credentials dashboard one of the items is to enable MFA on your root account

Option A is invalid because you need to have a good password policy Option B is invalid because there is no 1AM Geo-Lock Option D is invalid because this is not a recommended practices For more information on MFA, please visit the below URL http://docs.aws.amazon.com/IAM/latest/UserGuide/id credentials mfa.htmll
The correct answer is: Use MFA on all users and accounts, especially on the root account. Submit your Feedback/Queries to our Experts

NEW QUESTION 109
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual AWS-Certified-Security-Specialty Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the AWS-Certified-Security-Specialty Product From:

https://www.2passeasy.com/dumps/AWS-Certified-Security-Specialty/

Money Back Guarantee

AWS-Certified-Security-Specialty Practice Exam Features:

* AWS-Certified-Security-Specialty Questions and Answers Updated Frequently

* AWS-Certified-Security-Specialty Practice Questions Verified by Expert Senior Certified Staff

* AWS-Certified-Security-Specialty Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* AWS-Certified-Security-Specialty Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year