



Amazon

Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Exam Topic 1)

A company has an AWS account and allows a third-party contractor who uses another AWS account, to assume certain IAM roles. The company wants to ensure that IAM roles can be assumed by the contractor only if the contractor has multi-factor authentication enabled on their IAM user accounts

What should the company do to accomplish this?

A)

Add the following condition to the IAM policy attached to all IAM roles:

```
"Effect" : "Deny",  
"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : false } }
```

B)

Add the following condition to the IAM policy attached to all IAM roles:

```
"Effect" : "Deny",  
"Condition" : { "Bool" : { "aws:MultiFactorAuthPresent" : false } }
```

C)

Add the following condition to the IAM policy attached to all IAM roles:

```
"Effect" : "Allow",  
"Condition" : { "Null" : { "aws:MultiFactorAuthPresent" : false } }
```

D)

Add the following condition to the IAM policy attached to all IAM roles:

```
"Effect" : "Allow",  
"Condition" : { "BoolIfExists" : { "aws:MultiFactorAuthPresent" : false } }
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

NEW QUESTION 2

- (Exam Topic 1)

A company has an encrypted Amazon S3 bucket. An Application Developer has an IAM policy that allows access to the S3 bucket, but the Application Developer is unable to access objects within the bucket.

What is a possible cause of the issue?

A. The S3 ACL for the S3 bucket fails to explicitly grant access to the Application Developer

B. The AWS KMS key for the S3 bucket fails to list the Application Developer as an administrator

C. The S3 bucket policy fails to explicitly grant access to the Application Developer

D. The S3 bucket policy explicitly denies access to the Application Developer

Answer: C

NEW QUESTION 3

- (Exam Topic 1)

Authorized Administrators are unable to connect to an Amazon EC2 Linux bastion host using SSH over the internet. The connection either fails to respond or generates the following error message:

Network error: Connection timed out.

What could be responsible for the connection failure? (Select THREE)

A. The NAT gateway in the subnet where the EC2 instance is deployed has been misconfigured

B. The internet gateway of the VPC has been reconfigured

C. The security group denies outbound traffic on ephemeral ports

D. The route table is missing a route to the internet gateway

E. The NACL denies outbound traffic on ephemeral ports

F. The host-based firewall is denying SSH traffic

Answer: BDF

NEW QUESTION 4

- (Exam Topic 1)

A company is configuring three Amazon EC2 instances with each instance in a separate Availability Zone. The EC2 instances will be used as transparent proxies for outbound internet traffic for ports 80 and 443 so the proxies can block traffic to certain internet destinations as required by the company's security policies. A Security Engineer completed the following:

- Set up the proxy software on the EC2 instances.

- Modified the route tables on the private subnets to use the proxy EC2 instances as the default route.

- Created a security group rule opening inbound port 80 and 443 TCP protocols on the proxy EC2 instance security group.

However, the proxy EC2 instances are not successfully forwarding traffic to the internet.

What should the Security Engineer do to make the proxy EC2 instances route traffic to the internet?

A. Put all the proxy EC2 instances in a cluster placement group.

B. Disable source and destination checks on the proxy EC2 instances.

C. Open all inbound ports on the proxy EC2 instance security group.

D. Change the VPC's DHCP domain-name-servers options set to the IP addresses of proxy EC2 instances.

Answer: B

NEW QUESTION 5

- (Exam Topic 1)

A company has multiple production AWS accounts. Each account has AWS CloudTrail configured to log to a single Amazon S3 bucket in a central account. Two of the production accounts have trails that are not logging anything to the S3 bucket.

Which steps should be taken to troubleshoot the issue? (Choose three.)

- A. Verify that the log file prefix is set to the name of the S3 bucket where the logs should go.
- B. Verify that the S3 bucket policy allows access for CloudTrail from the production AWS account IDs.
- C. Create a new CloudTrail configuration in the account, and configure it to log to the account's S3 bucket.
- D. Confirm in the CloudTrail Console that each trail is active and healthy.
- E. Open the global CloudTrail configuration in the master account, and verify that the storage location is set to the correct S3 bucket.
- F. Confirm in the CloudTrail Console that the S3 bucket name is set correctly.

Answer: BDF

NEW QUESTION 6

- (Exam Topic 1)

A company had one of its Amazon EC2 key pairs compromised. A Security Engineer must identify which current Linux EC2 instances were deployed and used the compromised key pair.

How can this task be accomplished?

- A. Obtain the list of instances by directly querying Amazon EC2 using: `aws ec2 describe-instances --filters "Name=key-name,Values=KEYNAMEHERE"`.
- B. Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in the Amazon Inspector logs.
- C. Obtain the output from the EC2 instance metadata using: `curl http://169.254.169.254/latest/meta-data/public-keys/0/`.
- D. Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in Amazon CloudWatch Logs using: `aws logs filter-log-events`.

Answer: A

NEW QUESTION 7

- (Exam Topic 1)

A Security Engineer has launched multiple Amazon EC2 instances from a private AMI using an AWS CloudFormation template. The Engineer notices instances terminating right after they are launched.

What could be causing these terminations?

- A. The IAM user launching those instances is missing `ec2:RunInstances` permission.
- B. The AMI used as encrypted and the IAM does not have the required AWS KMS permissions.
- C. The instance profile used with the EC2 instances is unable to query instance metadata.
- D. AWS currently does not have sufficient capacity in the Region.

Answer: C

NEW QUESTION 8

- (Exam Topic 1)

Users report intermittent availability of a web application hosted on AWS. Monitoring systems report an excess of abnormal network traffic followed by high CPU utilization on the application web tier. Which of the following techniques will improve the availability of the application? (Select TWO.)

- A. Deploy AWS WAF to block all unsecured web applications from accessing the internet.
- B. Deploy an Intrusion Detection/Prevention System (IDS/IPS) to monitor or block unusual incoming network traffic.
- C. Configure security groups to allow outgoing network traffic only from hosts that are protected with up-to-date antivirus software.
- D. Create Amazon CloudFront distribution and configure AWS WAF rules to protect the web applications from malicious traffic.
- E. Use the default Amazon VPC for external-facing systems to allow AWS to actively block malicious network traffic affecting Amazon EC2 instances.

Answer: BD

NEW QUESTION 9

- (Exam Topic 1)

A company's Security Officer is concerned about the risk of AWS account root user logins and has assigned a Security Engineer to implement a notification solution for near-real-time alerts upon account root user logins.

How should the Security Engineer meet these requirements?

- A. Create a cron job that runs a script to download the AWS IAM security credentials W
- B. parse the file for account root user logins and email the Security team's distribution list
- C. Run AWS CloudTrail logs through Amazon CloudWatch Events to detect account root user logins and trigger an AWS Lambda function to send an Amazon SNS notification to the Security team's distribution list.
- D. Save AWS CloudTrail logs to an Amazon S3 bucket in the Security team's account Process the CloudTrail logs with the Security Engineer's logging solution for account root user logins Send an Amazon SNS notification to the Security team upon encountering the account root user login events
- E. Save VPC Flow Logs to an Amazon S3 bucket in the Security team's account and process the VPC Flow Logs with their logging solutions for account root user logins Send an Amazon SNS notification to the Security team upon encountering the account root user login events

Answer: B

NEW QUESTION 10

- (Exam Topic 1)

A company requires that SSH commands used to access its AWS instance be traceable to the user who executed each command.

How should a Security Engineer accomplish this?

- A. Allow inbound access on port 22 at the security group attached to the instance Use AWS Systems Manager Session Manager for shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch logging for Systems Manager sessions
- B. Use Amazon S3 to securely store one Privacy Enhanced Mail Certificate (PEM file) for each user Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on port 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance
- C. Deny inbound access on port 22 at the security group attached to the instance Use AWS Systems Manager Session Manager for shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch logging for Systems Manager sessions
- D. Use Amazon S3 to securely store one Privacy Enhanced Mail Certificate (PEM file) for each team or group Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on port 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

An application developer is using an AWS Lambda function that must use AWS KMS to perform encrypt and decrypt operations for API keys that are less than 2 KB Which key policy would allow the application to do this while granting least privilege?

- A.

```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:*"
  ],
  "Resource": "*"
}
```
- B.

```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```
- C.

```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:DescribeKey",
    "kms:GenerateDataKey*",
    "kms:Encrypt",
    "kms:ReEncrypt*",
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```
- D.

```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
    "kms:DescribeKey",
    "kms:GenerateDataKey*",
    "kms:Encrypt",
    "kms:ReEncrypt*",
    "kms:Disable*",
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

NEW QUESTION 13

- (Exam Topic 1)

A Security Engineer is looking for a way to control access to data that is being encrypted under a CMK. The Engineer is also looking to use additional authenticated data (AAD) to prevent tampering with ciphertext.

Which action would provide the required functionality?

- A. Pass the key alias to AWS KMS when calling Encrypt and Decrypt API actions.
- B. Use IAM policies to restrict access to Encrypt and Decrypt API actions.
- C. Use kms:EncryptionContext as a condition when defining IAM policies for the CMK.
- D. Use key policies to restrict access to the appropriate IAM groups.

Answer: B

NEW QUESTION 16

- (Exam Topic 1)

A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and is able to connect to external hosts on the internet. The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses.

Which action should the Security Engineer take to allow communication over the public IP addresses?

- A. Associate the instances to the same security groups.
- B. Add 0.0.0.0/0 to the egress rules of the instance security groups.
- C. Add the instance IDs to the ingress rules of the instance security groups.
- D. Add the public IP addresses to the ingress rules of the instance security groups.

Answer: D

Explanation:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules-reference.html#sg-rules-other-ins>

NEW QUESTION 19

- (Exam Topic 1)

A company is running an application on Amazon EC2 instances in an Auto Scaling group. The application stores logs locally. A security engineer noticed that logs were lost after a scale-in event. The security engineer needs to recommend a solution to ensure the durability and availability of log data. All logs must be kept for a minimum of 1 year for auditing purposes.

What should the security engineer recommend?

- A. Within the Auto Scaling lifecycle, add a hook to create and attach an Amazon Elastic Block Store (Amazon EBS) log volume each time an EC2 instance is created.
- B. When the instance is terminated, the EBS volume can be reattached to another instance for log review.
- C. Create an Amazon Elastic File System (Amazon EFS) file system and add a command in the user data section of the Auto Scaling launch template to mount the EFS file system during EC2 instance creation. Configure a process on the instance to copy the logs once a day from an instance Amazon Elastic Block Store (Amazon EBS) volume to a directory in the EFS file system.
- D. Build the Amazon CloudWatch agent into the AMI used in the Auto Scaling group.
- E. Configure the CloudWatch agent to send the logs to Amazon CloudWatch Logs for review.
- F. Within the Auto Scaling lifecycle, add a lifecycle hook at the terminating state transition and alert the engineering team by using a lifecycle notification to Amazon Simple Notification Service (Amazon SNS). Configure the hook to remain in the Terminating:Wait state for 1 hour to allow manual review of the security logs prior to instance termination.

Answer: B

NEW QUESTION 24

- (Exam Topic 1)

To meet regulatory requirements, a Security Engineer needs to implement an IAM policy that restricts the use of AWS services to the us-east-1 Region.

What policy should the Engineer implement?

A

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

B

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:Region": "us-east-1"
        }
      }
    }
  ]
}
```

C

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

D

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "NotAction": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    }
  ]
}
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

NEW QUESTION 26

- (Exam Topic 1)

A company is operating an open-source software platform that is internet facing. The legacy software platform no longer receives security updates. The software platform operates using Amazon route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon POS cluster a recent report suggests this software platform is vulnerable to SQL injection attacks. with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The secure, engineer's solution involve the least amount of effort and maintain normal operations during implementation.

What should the security engineer do to meet these requirements?

- A. Create an Application Load Balancer with the existing EC2 instances as a target group Create an AWS WAF web ACL containing rules mat protect the application from this attac
- B. then apply it to the ALB Test to ensure me vulnerability has been mitigated, then redirect thee Route 53 records to point to the ALB Update security groups on the EC 2 instances to prevent direct access from the internet
- C. Create an Amazon CloudFront distribution specifying one EC2 instance as an origin Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to me distribution Test to ensure the vulnerability has mitigated, then redirect the Route 53 records to point toCloudFront
- D. Obtain me latest source code for the platform and make ire necessary updates Test me updated code to ensure that the vulnerability has been irrigated, then deploy me patched version of the platform to the EC2 instances
- E. Update the security group mat is attached to the EC2 instances, removing access from the internet to the TCP port used by the SQL database Create an AWS WAF web ACL containing rules mat protect me application from this attack, men apply it to the EC2 instances Test to ensure me vulnerability has been mitigate
- F. then restore the security group to me original setting

Answer: A

NEW QUESTION 30

- (Exam Topic 1)

An company is using AWS Secrets Manager to store secrets that are encrypted using a CMK and are stored in the security account 111122223333. One of the company's production accounts. 444455556666, must to retrieve the secret values from the security account 111122223333. A security engineer needs to apply a policy to the secret in the security account based on least privilege access so the production account can retrieve the secret value only.

Which policy should the security engineer apply?

- A.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Principal": {"AWS": "444455556666"},
      "Resource": "*"
    }
  ]
}
```
- B.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Principal": {"AWS": "111122223333"},
      "Resource": "*"
    }
  ]
}
```
- C.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Principal": {"AWS": "111122223333"},
      "Resource": "*"
    }
  ]
}
```
- D.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Principal": {"AWS": "444455556666"},
      "Resource": "*"
    }
  ]
}
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

NEW QUESTION 32

- (Exam Topic 1)

A security engineer has noticed an unusually high amount of traffic coming from a single IP address. This was discovered by analyzing the Application Load Balancer's access logs. How can the security engineer limit the number of requests from a specific IP address without blocking the IP address?

- A. Add a rule to the Application Load Balancer to route the traffic originating from the IP address in question and show a static webpage.
- B. Implement a rate-based rule with AWS WAF
- C. Use AWS Shield to limit the originating traffic hit rate.
- D. Implement the GeoLocation feature in Amazon Route 53.

Answer: B

NEW QUESTION 34

- (Exam Topic 1)

After a recent security audit involving Amazon S3, a company has asked assistance reviewing its S3 buckets to determine whether data is properly secured. The first S3 bucket on the list has the following bucket policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            "10.10.10.0/24"
          ]
        }
      }
    }
  ]
}
```

Is this bucket policy sufficient to ensure that the data is not publicly accessible?

- A. Yes, the bucket policy makes the whole bucket publicly accessible despite now the S3 bucket ACL or object ACLs are configured.
- B. Yes, none of the data in the bucket is publicly accessible, regardless of how the S3 bucket ACL and object ACLs are configured.
- C. No, the IAM user policy would need to be examined first to determine whether any data is publicly accessible.
- D. No, the S3 bucket ACL and object ACLs need to be examined first to determine whether any data is publicly accessible.

Answer: A

NEW QUESTION 35

- (Exam Topic 1)

After multiple compromises of its Amazon EC2 instances, a company's Security Officer is mandating that memory dumps of compromised instances be captured for further analysis. A Security Engineer just received an EC2 abuse notification report from AWS stating that an EC2 instance running the most recent Windows Server 2019 Base AMI is compromised.

How should the Security Engineer collect a memory dump of the EC2 instance for forensic analysis?

- A. Give consent to the AWS Security team to dump the memory core on the compromised instance and provide it to AWS Support for analysis.
- B. Review memory dump data that the AWS Systems Manager Agent sent to Amazon CloudWatch Logs.
- C. Download and run the EC2Rescue for Windows Server utility from AWS.
- D. Reboot the EC2 Windows Server, enter safe mode, and select memory dump.

Answer: B

NEW QUESTION 38

- (Exam Topic 1)

A company is outsourcing its operational support to an external company. The company's security officer must implement an access solution for delegating operational support that minimizes overhead.

Which approach should the security officer take to meet these requirements?

- A. implement Amazon Cognito identity pools with a role that uses a policy that denies the actions related to Amazon Cognito API management Allow the external company to federate through its identity provider
- B. Federate AWS identity and Access Management (IAM) with the external company's identity provider Create an IAM role and attach a policy with the necessary permissions
- C. Create an IAM group for the external company Add a policy to the group that denies IAM modifications Securely provide the credentials to the external company.
- D. Use AWS SSO with the external company's identity provider
- E. Create an IAM group to map to the identity provider user group, and attach a policy with the necessary permissions.

Answer: B

NEW QUESTION 39

- (Exam Topic 1)

The Development team receives an error message each time the team members attempt to encrypt or decrypt a Secure String parameter from the SSM Parameter Store by using an AWS KMS customer managed key (CMK).

Which CMK-related issues could be responsible? (Choose two.)

- A. The CMK specified in the application does not exist.
- B. The CMK specified in the application is currently in use.
- C. The CMK specified in the application is using the CMK KeyID instead of CMK Amazon Resource Name.
- D. The CMK specified in the application is not enabled.
- E. The CMK specified in the application is using an alias.

Answer: AD

Explanation:

https://docs.amazonaws.cn/en_us/kms/latest/developerguide/services-parameter-store.html

NEW QUESTION 43

- (Exam Topic 1)

The Security Engineer is managing a traditional three-tier web application that is running on Amazon EC2 instances. The application has become the target of increasing numbers of malicious attacks from the Internet.

What steps should the Security Engineer take to check for known vulnerabilities and limit the attack surface? (Choose two.)

- A. Use AWS Certificate Manager to encrypt all traffic between the client and application servers.
- B. Review the application security groups to ensure that only the necessary ports are open.
- C. Use Elastic Load Balancing to offload Secure Sockets Layer encryption.
- D. Use Amazon Inspector to periodically scan the backend instances.
- E. Use AWS Key Management Services to encrypt all the traffic between the client and application servers.

Answer: BD

NEW QUESTION 44

- (Exam Topic 1)

A security engineer is asked to update an AWS CloudTrail log file prefix for an existing trail. When attempting to save the change in the CloudTrail console, the security engineer receives the following error message. "There is a problem with the bucket policy"

What will enable the security engineer to save the change?

- A. Create a new trail with the updated log file prefix, and then delete the original trail. Update the existing bucket policy in the Amazon S3 console with the new log file prefix, and then update the log file prefix in the CloudTrail console.
- B. Update the existing bucket policy in the Amazon S3 console to allow the security engineer's principal to perform PutBucketPolicy, and then update the log file prefix in the CloudTrail console.
- C. Update the existing bucket policy in the Amazon S3 console to allow the security engineer's principal to perform PutBucketPolicy, and then update the log file prefix in the CloudTrail console.
- D. Update the existing bucket policy in the Amazon S3 console with the new log file prefix, and then update the log file prefix in the CloudTrail console.
- E. Update the existing bucket policy in the Amazon S3 console to allow the security engineer's principal to perform GetBucketPolicy, and then update the log file prefix in the CloudTrail console.

Answer: B

NEW QUESTION 49

- (Exam Topic 1)

An AWS account administrator created an IAM group and applied the following managed policy to require that each individual user authenticate using multi-factor authentication:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    },
    {
      "Sid": "BlockAnyAccessUnlessSignedInWithMFA",
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "BoolIfExists": {
          "aws:MultiFactorAuthPresent": false
        }
      }
    }
  ]
}
```

After implementing the policy, the administrator receives reports that users are unable to perform Amazon EC2 commands using the AWS CLI. What should the administrator do to resolve this problem while still enforcing multi-factor authentication?

- A. Change the value of aws:MultiFactorAuthPresent to true.
- B. Instruct users to run the `aws sts get-session-token` CLI command and pass the multi-factor authentication—serial-number and —token-code parameter.
- C. Use these resulting values to make API/CLI calls.
- D. Implement federated API/CLI access using SAML 2.0, then configure the identity provider to enforce multi-factor authentication.
- E. Create a role and enforce multi-factor authentication in the role trust policy. Instruct users to run the `sts assume-role` CLI command and pass --serial-number and —token-code parameters. Store the resulting values in environment variables.
- F. Add sts:AssumeRole to NotAction in the policy.

Answer: B

NEW QUESTION 51

- (Exam Topic 1)

A Security Engineer for a large company is managing a data processing application used by 1,500 subsidiary companies. The parent and subsidiary companies all use AWS. The application uses TCP port 443 and runs on Amazon EC2 behind a Network Load Balancer (NLB). For compliance reasons, the application should only be accessible to the subsidiaries and should not be available on the public internet. To meet the compliance requirements for restricted access, the Engineer has received the public and private CIDR block ranges for each subsidiary.

What solution should the Engineer use to implement the appropriate access restrictions for the application?

- A. Create a NACL to allow access on TCP port 443 from the 1,500 subsidiary CIDR block ranges. Associate the NACL to both the NLB and EC2 instances.
- B. Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range.
- C. Associate the security group to the NLB.
- D. Create a second security group for EC2 instances with access on TCP port 443 from the NLB security group.
- E. Create an AWS PrivateLink endpoint service in the parent company account attached to the NLB.
- F. Create an AWS security group for the instances to allow access on TCP port 443 from the AWS PrivateLink endpoint.
- G. Use AWS PrivateLink interface endpoints in the 1,500 subsidiary AWS accounts to connect to the data processing application.
- H. Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range.
- I. Associate the security group with EC2 instances.

Answer: D

NEW QUESTION 54

- (Exam Topic 1)

A Developer signed in to a new account within an AWS Organizations organizations unit (OU) containing multiple accounts. Access to the Amazon S3 service is restricted with the following SCP:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

How can the Security Engineer provide the Developer with Amazon S3 access without affecting other accounts?

- A. Move the SCP to the root OU of Organizations to remove the restriction to access Amazon S3.
- B. Add an IAM policy for the Developer, which grants S3 access.
- C. Create a new OU without applying the SCP restricting S3 access.
- D. Move the Developer account to this new OU.
- E. Add an allow list for the Developer account for the S3 service.

Answer: B

NEW QUESTION 58

- (Exam Topic 1)

A company is collecting AWS CloudTrail log data from multiple AWS accounts by managing individual trails in each account and forwarding log data to a centralized Amazon S3 bucket residing in a log archive account. After CloudTrail introduced support for AWS Organizations trails, the company decided to further centralize management and automate deployment of the CloudTrail logging capability across all of its AWS accounts.

The company's security engineer created an AWS Organizations trail in the master account, enabled server-side encryption with AWS KMS managed keys (SSE-KMS) for the log files, and specified the same bucket as the storage location. However, the engineer noticed that logs recorded by the new trail were not delivered to the bucket.

Which factors could cause this issue? (Select TWO.)

- A. The CMK key policy does not allow CloudTrail to make encrypt and decrypt API calls against the key.
- B. The CMK key policy does not allow CloudTrail to make GenerateDataKey API calls against the key.
- C. The IAM role used by the CloudTrail trail does not have permissions to make PutObject API calls against a folder created for the Organizations trail.
- D. The S3 bucket policy does not allow CloudTrail to make PutObject API calls against a folder created for the Organizations trail.
- E. The CMK key policy does not allow the IAM role used by the CloudTrail trail to use the key for cryptographic operations.

Answer: AD

NEW QUESTION 60

- (Exam Topic 1)

A company's development team is designing an application using AWS Lambda and Amazon Elastic Container Service (Amazon ECS). The development team needs to create IAM roles to support these systems. The company's security team wants to allow the developers to build IAM roles directly, but the security team wants to retain control over the permissions the developers can delegate to those roles. The development team needs access to more permissions than those required for the application's AWS services. The solution must minimize management overhead.

How should the security team prevent privilege escalation for both teams?

- A. Enable AWS CloudTrail.
- B. Create a Lambda function that monitors the event history for privilege escalation events and notifies the security team.
- C. Create a managed IAM policy for the permissions required.
- D. Reference the IAM policy as a permissions boundary within the development team's IAM role.
- E. Enable AWS Organizations. Create an SCP that allows the IAM CreateUser action but that has a condition that prevents API calls other than those required by the development team.

- F. Create an IAM policy with a deny on the IAMCreateUser action and assign the policy to the development team
- G. Use a ticket system to allow the developers to request new IAM roles for their application
- H. The IAM roles will then be created by the security team.

Answer: A

NEW QUESTION 64

- (Exam Topic 1)

A Security Engineer accidentally deleted the imported key material in an AWS KMS CMK. What should the Security Engineer do to restore the deleted key material?

- A. Create a new CM
- B. Download a new wrapping key and a new import token to import the original key material
- C. Create a new CMK Use the original wrapping key and import token to import the original key material.
- D. Download a new wrapping key and a new import token Import the original key material into the existing CMK.
- E. Use the original wrapping key and import token Import the original key material into the existing CMK

Answer: C

NEW QUESTION 66

- (Exam Topic 1)

A security engineer needs to ensure their company's uses of AWS meets AWS security best practices. As part of this, the AWS account root user must not be used for daily work. The root user must be monitored for use, and the Security team must be alerted as quickly as possible if the root user is used. Which solution meets these requirements?

- A. Set up an Amazon CloudWatch Events rule that triggers an Amazon SNS notification.
- B. Set up an Amazon CloudWatch Events rule that triggers an Amazon SNS notification logs from S3 and generate notifications using Amazon SNS.
- C. Set up a rule in AWS config to trigger root user event
- D. Trigger an AWS Lambda function and generate notifications using Amazon SNS.
- E. Use Amazon Inspector to monitor the usage of the root user and generate notifications using Amazon SNS

Answer: A

NEW QUESTION 71

- (Exam Topic 1)

A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running in Amazon Elastic Container Service (Amazon ECS). This solution will also handle volatile traffic patterns. Which solution would have the MOST scalability and LOWEST latency?

- A. Configure a Network Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers
- B. Configure an Application Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers
- C. Configure a Network Load Balancer with a TCP listener to pass through TLS traffic to the containers
- D. Configure Amazon Route 53 to use multivalued answer routing to send traffic to the containers

Answer: A

NEW QUESTION 73

- (Exam Topic 1)

A company is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information. The security team has the following requirements for the architecture:

- Data must be encrypted in transit.
- Data must be encrypted at rest.
- The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential. Which combination of steps would meet the requirements? (Select THREE.)

- A. Enable AES-256 encryption using server-side encryption with Amazon S3-managed encryption keys (SSE-S3) on the S3 bucket
- B. Enable default encryption with server-side encryption with AWS KMS-managed keys (SSE-KMS) on the S3 bucket.
- C. Add a bucket policy that includes a deny if a PutObject request does not include aws:SecureTransport.
- D. Add a bucket policy with ws: SourceIp to Allow uploads and downloads from the corporate intranet only.
- E. Add a bucket policy that includes a deny if a PutObject request does not include s3:x-amz-server-side-encryption: "aws: kms".
- F. Enable Amazon Macie to monitor and act on changes to the data lake's S3 bucket.

Answer: BDF

NEW QUESTION 74

- (Exam Topic 1)

A company is using AWS Organizations to manage multiple AWS accounts. The company has an application that allows users to assume the AppUser IAM role to download files from an Amazon S3 bucket that is encrypted with an AWS KMS CMK. However, when users try to access the files in the S3 bucket, they get an access denied error.

What should a Security Engineer do to troubleshoot this error? (Select THREE)

- A. Ensure the KMS policy allows the AppUser role to have permission to decrypt for the CMK
- B. Ensure the S3 bucket policy allows the AppUser role to have permission to get objects for the S3 bucket
- C. Ensure the CMK was created before the S3 bucket.
- D. Ensure the S3 block public access feature is enabled for the S3 bucket.
- E. Ensure that automatic key rotation is disabled for the CMK
- F. Ensure the SCPs within Organizations allow access to the S3 bucket.

Answer: ABF

NEW QUESTION 78

- (Exam Topic 1)

A company is designing the securely architecture (or a global latency-sensitive web application it plans to deploy to AWS. A Security Engineer needs to configure a highly available and secure two-tier architecture. The security design must include controls to prevent common attacks such as DDoS, cross-site scripting, and SQL injection.

Which solution meets these requirements?

- A. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Region
- B. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- C. Create an AmazonCloudFront distribution that uses the ALB as its origin
- D. Create appropriate AWS WAF ACLs and enable them on the CloudFront distribution.
- E. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Region
- F. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- G. Create an Amazon CloudFront distribution that uses the ALB as its origin
- H. Create appropriate AWS WAF ACLs and enable them on the CloudFront distribution.
- I. Create an Application Load Balancer (ALB) that uses public subnets across multiple Availability Zones within a single Region
- J. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- K. Create appropriate AWS WAF ACLs and enable them on the ALB.
- L. Create an Application Load Balancer (ALB) that uses private subnets across multiple Availability Zones within a single Region
- M. Point the ALB to an Auto Scaling group with Amazon EC2 instances in private subnets across multiple Availability Zones within the same Region
- N. Create appropriate AWS WAF ACLs and enable them on the ALB.

Answer: A

NEW QUESTION 79

- (Exam Topic 1)

A security engineer has noticed that VPC Flow Logs are getting a lot REJECT traffic originating from a single Amazon EC2 instance in an Auto Scaling group. The security engineer is concerned that this EC2 instance may be compromised.

What immediate action should the security engineer take? What immediate action should the security engineer take?

- A. Remove the instance from the Auto Scaling group Close the security group ingress only from a single forensic IP address to perform an analysis.
- B. Remove the instance from the Auto Scaling group Change the network ACL rules to allow traffic only from a single forensic IP address to perform an analysis. Add a rule to deny all other traffic.
- C. Remove the instance from the Auto Scaling group Enable Amazon GuardDuty in that AWS account Install the Amazon Inspector agent on the suspicious EC2 instance to perform a scan.
- D. Take a snapshot of the suspicious EC2 instance
- E. Create a new EC2 instance from the snapshot in a closed security group with ingress only from a single forensic IP address to perform an analysis

Answer: B

NEW QUESTION 81

- (Exam Topic 1)

A security engineer is responsible for providing secure access to AWS resources for thousands of developers in a company's corporate identity provider (IdP). The developers access a set of AWS services from the corporate premises using IAM credentials. Due to the volume of requests for provisioning new IAM users, it is taking a long time to grant access permissions. The security engineer receives reports that developers are sharing their IAM credentials with others to avoid provisioning delays. This causes concern about overall security for the security engineer.

Which actions will meet the program requirements that address security?

- A. Create an Amazon CloudWatch alarm for AWS CloudTrail Events Create a metric filter to send a notification when the same set of IAM credentials is used by multiple developers
- B. Create a federation between AWS and the existing corporate IdP Leverage IAM roles to provide federated access to AWS resources
- C. Create a VPN tunnel between the corporate premises and the VPC Allow permissions to all AWS services only if it originates from corporate premises.
- D. Create multiple IAM roles for each IAM user Ensure that users who use the same IAM credentials cannot assume the same IAM role at the same time.

Answer: B

NEW QUESTION 85

- (Exam Topic 1)

A company hosts its public website on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an EC2 Auto Scaling group across multiple Availability Zones. The website is under a DDoS attack by a specific IoT device brand that is visible in the user agent. A security engineer needs to mitigate the attack without impacting the availability of the public website.

What should the security engineer do to accomplish this?

- A. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the IoT device
- B. Associate the web ACL with the ALB.
- C. Configure an Amazon CloudFront distribution to use the ALB as its origin
- D. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the IoT device
- E. Associate the web ACL with the ALB Change the public DNS entry of the website to point to the CloudFront distribution.
- F. Configure an Amazon CloudFront distribution to use a new ALB as its origin
- G. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the IoT device
- H. Change the ALB security group to allow access from CloudFront IP address ranges only Change the public DNS entry of the website to point to the CloudFront distribution.
- I. Activate AWS Shield Advanced to enable DDoS protection
- J. Apply an AWS WAF ACL to the ALB
- K. and configure a listener rule on the ALB to block IoT devices based on the user agent.

Answer: D

NEW QUESTION 87

- (Exam Topic 1)

A security engineer needs to configure monitoring and auditing for AWS Lambda.

Which combination of actions using AWS services should the security engineer take to accomplish this goal? (Select TWO.)

- A. Use AWS Config to track configuration changes to Lambda functions, runtime environments, tags, handler names, code sizes, memory allocation, timeout settings, and concurrency settings, along with Lambda IAM execution role, subnet, and security group associations.
- B. Use AWS CloudTrail to implement governance, compliance, operational, and risk auditing for Lambda.
- C. Use Amazon Inspector to automatically monitor for vulnerabilities and perform governance, compliance, operational, and risk auditing for Lambda.
- D. Use AWS Resource Access Manager to track configuration changes to Lambda functions, runtime environments, tags, handler names, code sizes, memory allocation, timeout settings, and concurrency settings, along with Lambda IAM execution role, subnet, and security group associations.
- E. Use Amazon Macie to discover, classify, and protect sensitive data being executed inside the Lambda function.

Answer: AB

NEW QUESTION 89

- (Exam Topic 1)

A Security Engineer creates an Amazon S3 bucket policy that denies access to all users. A few days later, the Security Engineer adds an additional statement to the bucket policy to allow read-only access to one other employee. Even after updating the policy the employee still receives an access denied message.

What is the likely cause of this access denial?

- A. The ACL in the bucket needs to be updated.
- B. The IAM policy does not allow the user to access the bucket
- C. It takes a few minutes for a bucket policy to take effect
- D. The allow permission is being overridden by the deny.

Answer: D

NEW QUESTION 91

- (Exam Topic 1)

A large government organization is moving to the cloud and has specific encryption requirements. The first workload to move requires that a customer's data be immediately destroyed when the customer makes that request.

Management has asked the security team to provide a solution that will securely store the data, allow only authorized applications to perform encryption and decryption and allow for immediate destruction of the data.

Which solution will meet these requirements?

- A. Use AWS Secrets Manager and an AWS SDK to create a unique secret for the customer-specific data
- B. Use AWS Key Management Service (AWS KMS) and the AWS Encryption SDK to generate and store a data encryption key for each customer.
- C. Use AWS Key Management Service (AWS KMS) with service-managed keys to generate and store customer-specific data encryption keys
- D. Use AWS Key Management Service (AWS KMS) and create an AWS CloudHSM custom key store. Use CloudHSM to generate and store a new CMK for each customer.

Answer: A

NEW QUESTION 92

- (Exam Topic 1)

A Security Administrator at a university is configuring a fleet of Amazon EC2 instances. The EC2 instances are shared among students, and non-root SSH access is allowed. The Administrator is concerned about students attacking other AWS account resources by using the EC2 instance metadata service.

What can the Administrator do to protect against this potential attack?

- A. Disable the EC2 instance metadata service.
- B. Log all student SSH interactive session activity.
- C. Implement IP tables-based restrictions on the instances.
- D. Install the Amazon Inspector agent on the instances.

Answer: A

Explanation:

"To turn off access to instance metadata on an existing instance....." <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html> You can disable the service for existing (running or stopped) ec2 instances. <https://docs.aws.amazon.com/cli/latest/reference/ec2/modify-instance-metadata-options.html>

NEW QUESTION 93

- (Exam Topic 1)

A security engineer must use AWS Key Management Service (AWS KMS) to design a key management solution for a set of Amazon Elastic Block Store (Amazon EBS) volumes that contain sensitive data. The solution needs to ensure that the key material automatically expires in 90 days.

Which solution meets these criteria?

- A. A customer managed CMK that uses customer provided key material
- B. A customer managed CMK that uses AWS provided key material
- C. An AWS managed CMK
- D. Operating system-native encryption that uses GnuPG

Answer: B

NEW QUESTION 97

- (Exam Topic 1)

A company recently performed an annual security assessment of its AWS environment. The assessment showed that audit logs are not available beyond 90 days and that unauthorized changes to IAM policies are made without detection. How should a security engineer resolve these issues?

- A. Create an Amazon S3 lifecycle policy that archives AWS CloudTrail trail logs to Amazon S3 Glacier after 90 day
- B. Configure Amazon Inspector to provide a notification when a policy change is made to resources.
- C. Configure AWS Artifact to archive AWS CloudTrail logs Configure AWS Trusted Advisor to provide a notification when a policy change is made to resources.
- D. Configure Amazon CloudWatch to export log groups to Amazon S3. Configure AWS CloudTrail to provide a notification when a policy change is made to resources.
- E. Create an AWS CloudTrail trail that stores audit logs in Amazon S3. Configure an AWS Config rule to provide a notification when a policy change is made to resources.

Answer: A

NEW QUESTION 99

- (Exam Topic 1)

A Security Engineer has discovered that, although encryption was enabled on the Amazon S3 bucket example bucket, anyone who has access to the bucket has the ability to retrieve the files. The Engineer wants to limit access to each IAM user can access an assigned folder only. What should the Security Engineer do to achieve this?

- A. Use envelope encryption with the AWS-managed CMK aws/s3.
- B. Create a customer-managed CMK with a key policy granting “kms:Decrypt” based on the “\${aws:username}” variable.
- C. Create a customer-managed CMK for each use
- D. Add each user as a key user in their corresponding key policy.
- E. Change the applicable IAM policy to grant S3 access to “Resource”: “arn:aws:s3:::examplebucket/\${aws:username}/*”

Answer: B

Explanation:

Reference: <https://aws.amazon.com/premiumsupport/knowledge-center/iam-s3-user-specific-folder/>

NEW QUESTION 104

- (Exam Topic 1)

A company has a website with an Amazon CloudFront HTTPS distribution, an Application Load Balancer (ALB) with multiple web instances for dynamic website content, and an Amazon S3 bucket for static website content. The company's security engineer recently updated the website security requirements:

- HTTPS needs to be enforced for all data in transit with specific ciphers.
- The CloudFront distribution needs to be accessible from the internet only. Which solution will meet these requirements?

- A. Set up an S3 bucket policy with the awssecuretransport key Configure the CloudFront origin access identity (OAI) with the S3 bucket Configure CloudFront to use specific cipher
- B. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers Link the ALB with AWS WAF to allow access from the CloudFront IP ranges.
- C. Set up an S3 bucket policy with the aws:securetransport ke
- D. Configure the CloudFront origin access identity (OAI) with the S3 bucke
- E. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers.
- F. Modify the CloudFront distribution to use AWS WA
- G. Force HTTPS on the S3 bucket with specific ciphers in the bucket polic
- H. Configure an HTTPS listener only for the AL
- I. Set up a security group to limit access to the ALB from the CloudFront IP ranges
- J. Modify the CloudFront distribution to use the ALB as the origi
- K. Enforce an HTTPS listener on the AL
- L. Create a path-based routing rule on the ALB with proxies that connect lo Amazon S3. Create a bucket policy to allow access from these proxies only.A company Is trying to replace its on-premises bastion hosts used to access on-premises Linux servers with AWS Systems Manager Session Manage
- M. A security engineer has installed the Systems Manager Agent on all server
- N. The security engineer verifies that the agent is running on all the servers, but Session Manager cannot connect to the
- O. The security engineer needs to perform verification steps before Session Manager will work on the servers.Which combination of steps should the security engineer perform? (Select THREE.)
- P. Open inbound port 22 to 0 0.0.0/0 on all Linux servers.
- Q. Enable the advanced-instances tier in Systems Manager.
- R. Create a managed-instance activation for the on-premises servers.
- S. Reconfigure the Systems Manager Agent with the activation code and ID.
- T. Assign an IAM role to all of the on-premises servers.
- . Initiate an inventory collection with Systems Manager on the on-premises servers

Answer: CEF

NEW QUESTION 105

- (Exam Topic 1)

A company hosts a web-based application that captures and stores sensitive data in an Amazon DynamoDB table. A security audit reveals that the application does not provide end-to-end data protection or the ability to detect unauthorized data changes The software engineering team needs to make changes that will address the audit findings.

Which set of steps should the software engineering team take?

- A. Use an AWS Key Management Service (AWS KMS) CM
- B. Encrypt the data at rest.
- C. Use AWS Certificate Manager (ACM) Private Certificate Authority Encrypt the data in transit.
- D. Use a DynamoDB encryption clien
- E. Use client-side encryption and sign the table items
- F. Use the AWS Encryption SD
- G. Use client-side encryption and sign the table items.

Answer: A

NEW QUESTION 106

- (Exam Topic 1)

A company's security information events management (SIEM) tool receives new AWS CloudTrail logs from an Amazon S3 bucket that is configured to send all object created event notification to an Amazon SNS topic. An Amazon SQS queue is subscribed to this SNS topic. The company's SEM tool then ports this SQS queue for new messages using an IAM role and fetches new log events from the S3 bucket based on the SQS messages.

After a recent security review that resulted in restricted permissions, the SEM tool has stopped receiving new CloudTrail logs.

Which of the following are possible causes of this issue? (Select THREE)

- A. The SQS queue does not allow the SQS SendMessage action from the SNS topic
- B. The SNS topic does not allow the SNS Publish action from Amazon S3
- C. The SNS topic is not delivering raw messages to the SQS queue
- D. The S3 bucket policy does not allow CloudTrail to perform the PutObject action
- E. The IAM role used by the SEM tool does not have permission to subscribe to the SNS topic
- F. The IAM role used by the SEM tool does not allow the SQS DeleteMessage action

Answer: ADF

NEW QUESTION 110

- (Exam Topic 2)

A Security Engineer who was reviewing AWS Key Management Service (AWS KMS) key policies found this statement in each key policy in the company AWS account.

```
{
  "Sid": "Enable IAM User Permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
  },
  "Action": "kms:*",
  "Resource": "*"
}
```

What does the statement allow?

- A. All principals from all AWS accounts to use the key.
- B. Only the root user from account 111122223333 to use the key.
- C. All principals from account 111122223333 to use the key but only on Amazon S3.
- D. Only principals from account 111122223333 that have an IAM policy applied that grants access to this key to use the key.

Answer: D

NEW QUESTION 115

- (Exam Topic 2)

A Software Engineer wrote a customized reporting service that will run on a fleet of Amazon EC2 instances. The company security policy states that application logs for the reporting service must be centrally collected.

What is the MOST efficient way to meet these requirements?

- A. Write an AWS Lambda function that logs into the EC2 instance to pull the application logs from the EC2 instance and persists them into an Amazon S3 bucket.
- B. Enable AWS CloudTrail logging for the AWS account, create a new Amazon S3 bucket, and then configure Amazon CloudWatch Logs to receive the application logs from CloudTrail.
- C. Create a simple cron job on the EC2 instances that synchronizes the application logs to an Amazon S3 bucket by using rsync.
- D. Install the Amazon CloudWatch Logs Agent on the EC2 instances, and configure it to send the application logs to CloudWatch Logs.

Answer: D

Explanation:

<https://aws.amazon.com/blogs/aws/cloudwatch-log-service/>

NEW QUESTION 120

- (Exam Topic 2)

Your company has defined a number of EC2 Instances over a period of 6 months. They want to know if any of the security groups allow unrestricted access to a resource. What is the best option to accomplish this requirement?

Please select:

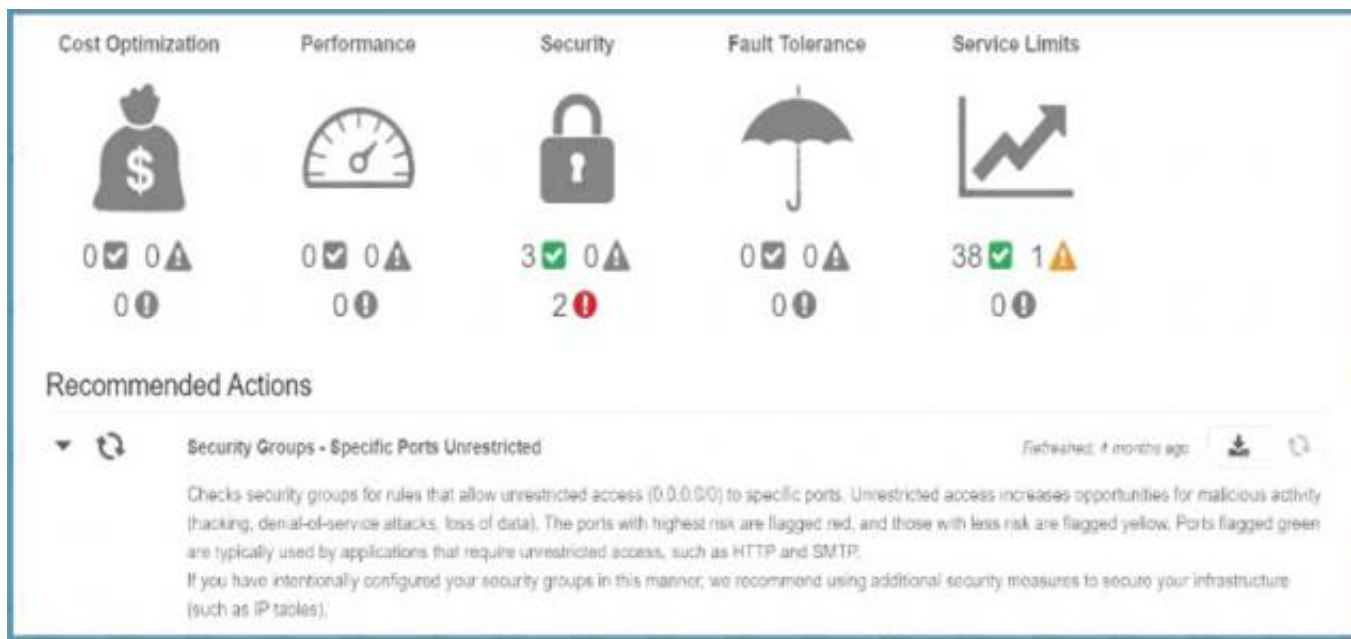
- A. Use AWS Inspector to inspect all the security Groups
- B. Use the AWS Trusted Advisor to see which security groups have compromised access.
- C. Use AWS Config to see which security groups have compromised access.
- D. Use the AWS CLI to query the security groups and then filter for the rules which have unrestricted access

Answer: B

Explanation:

The AWS Trusted Advisor can check security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).

If you go to AWS Trusted Advisor, you can see the details C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option A is invalid because AWS Inspector is used to detect security vulnerabilities in instances and not for security groups.

Option C is invalid because this can be used to detect changes in security groups but not show you security groups that have compromised access.

Option D is partially valid but would just be a maintenance overhead

For more information on the AWS Trusted Advisor, please visit the below URL: <https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices>;

The correct answer is: Use the AWS Trusted Advisor to see which security groups have compromised access. Submit your Feedback/Queries to our Experts

NEW QUESTION 122

- (Exam Topic 2)

A company's security policy requires that VPC Flow Logs are enabled on all VPCs. A Security Engineer is looking to automate the process of auditing the VPC resources for compliance.

What combination of actions should the Engineer take? (Choose two.)

- A. Create an AWS Lambda function that determines whether Flow Logs are enabled for a given VPC.
- B. Create an AWS Config configuration item for each VPC in the company AWS account.
- C. Create an AWS Config managed rule with a resource type of AWS::Lambda::Function.
- D. Create an Amazon CloudWatch Event rule that triggers on events emitted by AWS Config.
- E. Create an AWS Config custom rule, and associate it with an AWS Lambda function that contains the evaluating logic.

Answer: AE

Explanation:

<https://medium.com/mudita-misra/how-to-audit-your-aws-resources-for-security-compliance-by-using-custom-a>

NEW QUESTION 126

- (Exam Topic 2)

A Systems Administrator has written the following Amazon S3 bucket policy designed to allow access to an S3 bucket for only an authorized AWS IAM user from the IP address range 10.10.10.0/24:


```
{
  "Version": "2012-10-17",
  "Id": "S3Policy1",
  "Statement": [
    {
      "Sid": ["OfficeAllowIP"],
      "Effect": ["Allow"],
      "Principal": ["*"],
      "Action": ["s3:*"],
      "Resource": ["arn:aws:s3:::Bucket"],
      "Condition": {
        "IpAddress": [
          {
            "aws:SourceIp": "10.10.10.0/24"
          }
        ]
      }
    }
  ]
}
```

When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message. What does the Administrator need to change to grant access to the user?

- A. Change the "Resource" from "arn: aws:s3:::Bucket" to "arn:aws:s3:::Bucket/*".
- B. Change the "Principal" from "*" to {AWS:"arn:aws:iam: : account-number: user/username"}
- C. Change the "Version" from "2012-10-17" to the last revised date of the policy
- D. Change the "Action" from ["s3:*"] to ["s3:GetObject", "s3:ListBucket"]

Answer: A

NEW QUESTION 130

- (Exam Topic 2)

An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing. Which steps should be taken to troubleshoot the issue? (Choose two.)

- A. Use an EC2 run command to confirm that the "awslogs" service is running on all instances.
- B. Verify that the permissions used by the agent allow creation of log groups/streams and to put log events.
- C. Check whether any application log entries were rejected because of invalid time stamps by reviewing/var/cwlogs/rejects.log.
- D. Check that the trust relationship grants the service "cwlogs.amazonaws.com" permission to write objects to the Amazon S3 staging bucket.
- E. Verify that the time zone on the application servers is in UTC.

Answer: AB

Explanation:

EC2 run command - can run scripts, install software, collect metrics and log files, manage patches and more. Bringing these two services together - can create CloudWatch Events rules that use EC2 Run Command to perform actions on EC2 instances or on-premises servers.

NEW QUESTION 135

- (Exam Topic 2)

A pharmaceutical company has digitized versions of historical prescriptions stored on premises. The company would like to move these prescriptions to AWS and perform analytics on the data in them. Any operation with this data requires that the data be encrypted in transit and at rest. Which application flow would meet the data protection requirements on AWS?

- A. Digitized files -> Amazon Kinesis Data Analytics
- B. Digitized files -> Amazon Kinesis Data Firehose -> Amazon S3 -> Amazon Athena
- C. Digitized files -> Amazon Kinesis Data Streams -> Kinesis Client Library consumer -> Amazon S3 -> Athena
- D. Digitized files -> Amazon Kinesis Data Firehose -> Amazon Elasticsearch

Answer: B

NEW QUESTION 139

- (Exam Topic 2)

A Security Engineer received an AWS Abuse Notice listing EC2 instance IDs that are reportedly abusing other hosts. Which action should the Engineer take based on this situation? (Choose three.)

- A. Use AWS Artifact to capture an exact image of the state of each instance.
- B. Create EBS Snapshots of each of the volumes attached to the compromised instances.
- C. Capture a memory dump.
- D. Log in to each instance with administrative credentials to restart the instance.
- E. Revoke all network ingress and egress except for to/from a forensics workstation.
- F. Run Auto Recovery for Amazon EC2.

Answer: BEF

NEW QUESTION 140

- (Exam Topic 2)

An AWS account includes two S3 buckets: bucket1 and bucket2. The bucket2 does not have a policy defined, but bucket1 has the following bucket policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam: : 123456789012: user/alice" },
      "Action": "s3:*",
      "Resource": [ "arn:aws:s3: : bucket1", "arn:aws:s3: : bucket1/*" ]
    }
  ]
}
```

In addition, the same account has an IAM User named "alice", with the following IAM policy.

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Action": "s3:*",
    "Resource": [ "arn:aws:s3: : bucket2", "arn:aws:s3: : bucket2/*" ]
  } ]
}
```

Which buckets can user "alice" access?

- A. Bucket1 only
- B. Bucket2 only
- C. Both bucket1 and bucket2
- D. Neither bucket1 nor bucket2

Answer: C

Explanation:

Both S3 policies and IAM policies can be used to grant access to buckets. IAM policies specify what actions are allowed or denied on what AWS resources (e.g. allow ec2:TerminateInstance on the EC2 instance with instance_id=i-8b3620ec). You attach IAM policies to IAM users, groups, or roles, which are then subject to the permissions you've defined. In other words, IAM policies define what a principal can do in your AWS environment. S3 bucket policies, on the other hand, are attached only to S3 buckets. S3 bucket policies specify what actions are allowed or denied for which principals on the bucket that the bucket policy is attached to (e.g. allow user Alice to PUT but not DELETE objects in the bucket).

<https://aws.amazon.com/blogs/security/iam-policies-and-bucket-policies-and-acls-oh-my-controlling-access-to-s>

NEW QUESTION 145

- (Exam Topic 2)

A Security Engineer is trying to determine whether the encryption keys used in an AWS service are in compliance with certain regulatory standards. Which of the following actions should the Engineer perform to get further guidance?

- A. Read the AWS Customer Agreement.
- B. Use AWS Artifact to access AWS compliance reports.
- C. Post the question on the AWS Discussion Forums.
- D. Run AWS Config and evaluate the configuration outputs.

Answer: A

Explanation:

<https://aws.amazon.com/artifact/>

NEW QUESTION 149

- (Exam Topic 2)

A company wants to have a secure way of generating, storing and managing cryptographic exclusive access for the keys. Which of the following can be used for this purpose?

Please select:

- A. Use KMS and the normal KMS encryption keys
- B. Use KMS and use an external key material
- C. Use S3 Server Side encryption
- D. Use Cloud HSM

Answer: D

Explanation:

The AWS Documentation mentions the following

The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the AWS cloud. AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary. CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are design and validated to government standards for secure key management. CloudHSM allows you to securely generate, store and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.

Option A,B and Care invalid because in all of these cases, the management of the key will be with AWS. Here the question specifically mentions that you want to have exclusive access over the keys. This can be achieved with Cloud HSM

For more information on CloudHSM, please visit the following URL: <https://aws.amazon.com/cloudhsm/faq>:

The correct answer is: Use Cloud HSM Submit your Feedback/Queries to our Experts

NEW QUESTION 151

- (Exam Topic 2)

A company has a few dozen application servers in private subnets behind an Elastic Load Balancer (ELB) in an AWS Auto Scaling group. The application is accessed from the web over HTTPS. The data must always be encrypted in transit. The Security Engineer is worried about potential key exposure due to vulnerabilities in the application software.

Which approach will meet these requirements while protecting the external certificate during a breach?

- A. Use a Network Load Balancer (NLB) to pass through traffic on port 443 from the internet to port 443 on the instances.
- B. Purchase an external certificate, and upload it to the AWS Certificate Manager (for use with the ELB) and to the instance
- C. Have the ELB decrypt traffic, and route and re-encrypt with the same certificate.
- D. Generate an internal self-signed certificate and apply it to the instance
- E. Use AWS Certificate Manager to generate a new external certificate for the EL
- F. Have the ELB decrypt traffic, and route andre-encrypt with the internal certificate.
- G. Upload a new external certificate to the load balance
- H. Have the ELB decrypt the traffic and forward it on port 80 to the instances.

Answer: C

NEW QUESTION 153

- (Exam Topic 2)

An application makes calls to AWS services using the AWS SDK. The application runs on Amazon EC2 instances with an associated IAM role. When the application attempts to access an object within an Amazon S3 bucket; the Administrator receives the following error message: HTTP 403: Access Denied.

Which combination of steps should the Administrator take to troubleshoot this issue? (Select three.)

- A. Confirm that the EC2 instance's security group authorizes S3 access.
- B. Verify that the KMS key policy allows decrypt access for the KMS key for this IAM principle.
- C. Check the S3 bucket policy for statements that deny access to objects.
- D. Confirm that the EC2 instance is using the correct key pair.
- E. Confirm that the IAM role associated with the EC2 instance has the proper privileges.
- F. Confirm that the instance and the S3 bucket are in the same Region.

Answer: BCE

NEW QUESTION 158

- (Exam Topic 2)

What are the MOST secure ways to protect the AWS account root user of a recently opened AWS account? (Choose two.)

- A. Use the AWS account root user access keys instead of the AWS Management Console
- B. Enable multi-factor authentication for the AWS IAM users with the AdministratorAccess managed policy attached to them
- C. Enable multi-factor authentication for the AWS account root user
- D. Use AWS KMS to encrypt all AWS account root user and AWS IAM access keys and set automatic rotation to 30 days
- E. Do not create access keys for the AWS account root user; instead, create AWS IAM users

Answer: CE

NEW QUESTION 163

- (Exam Topic 2)

A company stores data on an Amazon EBS volume attached to an Amazon EC2 instance. The data is asynchronously replicated to an Amazon S3 bucket. Both the EBS volume and the S3 bucket are encrypted with the same AWS KMS Customer Master Key (CMK). A former employee scheduled a deletion of that CMK before leaving the company.

The company's Developer Operations department learns about this only after the CMK has been deleted. Which steps must be taken to address this situation?

- A. Copy the data directly from the EBS encrypted volume before the volume is detached from the EC2 instance.
- B. Recover the data from the EBS encrypted volume using an earlier version of the KMS backing key.
- C. Make a request to AWS Support to recover the S3 encrypted data.
- D. Make a request to AWS Support to restore the deleted CMK, and use it to recover the data.

Answer: C

NEW QUESTION 168

- (Exam Topic 2)

An IAM user with full EC2 permissions could not start an Amazon EC2 instance after it was stopped for a maintenance task. Upon starting the instance, the instance state would change to "Pending", but after a few seconds, it would switch back to "Stopped".

An inspection revealed that the instance has attached Amazon EBS volumes that were encrypted by using a Customer Master Key (CMK). When these encrypted volumes were detached, the IAM user was able to start the EC2 instances.

The IAM user policy is as follows:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        <Action>
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:012345678910:key/ebs-encryption-key"
      ]
    }
  ]
}
```

What additional items need to be added to the IAM user policy? (Choose two.)

- A. kms:GenerateDataKey
- B. kms:Decrypt
- C. kms:CreateGrant
- D. "Condition": {"Bool": {"kms:ViaService": "ec2.us-west-2.amazonaws.com"}}
- E. "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}

Answer: CE

Explanation:

The EBS which is AWS resource service is encrypted with CMK and to allow EC2 to decrypt, the IAM user should create a grant (action) and a boolean condition for the AWS resource. This link explains how AWS keys work: <https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html>

NEW QUESTION 170

- (Exam Topic 2)

Example.com hosts its internal document repository on Amazon EC2 instances. The application runs on EC2 instances and previously stored the documents on encrypted Amazon EBS volumes. To optimize the application for scale, example.com has moved the files to Amazon S3. The security team has mandated that all the files are securely deleted from the EBS volume, and it must certify that the data is unreadable before releasing the underlying disks.

Which of the following methods will ensure that the data is unreadable by anyone else?

- A. Change the volume encryption on the EBS volume to use a different encryption mechanism.
- B. Then, release the EBS volumes back to AWS.
- C. Release the volumes back to AWS.
- D. AWS immediately wipes the disk after it is deprovisioned.
- E. Delete the encryption key used to encrypt the EBS volume.
- F. Then, release the EBS volumes back to AWS.
- G. Delete the data by using the operating system delete command.
- H. Run Quick Format on the drive and then release the EBS volumes back to AWS.

Answer: D

Explanation:

Amazon EBS volumes are presented to you as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs immediately before reuse so that you can be assured that the wipe process completed. If you have procedures requiring that all data be wiped via a specific method, such as those detailed in NIST 800-88 ("Guidelines for Media Sanitization"), you have the ability to do so on Amazon EBS. You should conduct a specialized wipe procedure prior to deleting the volume for compliance with your established requirements.

<https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf>

NEW QUESTION 174

- (Exam Topic 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 it is 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 entity 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 Policies 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 175

- (Exam Topic 2)

The Accounting department at Example Corp. has made a decision to hire a third-party firm, AnyCompany, to monitor Example Corp.'s AWS account to help optimize costs.

The Security Engineer for Example Corp. has been tasked with providing AnyCompany with access to the required Example Corp. AWS resources. The Engineer has created an IAM role and granted permission to AnyCompany's AWS account to assume this role.

When customers contact AnyCompany, they provide their role ARN for validation. The Engineer is concerned that one of AnyCompany's other customers might deduce Example Corp.'s role ARN and potentially compromise the company's account.

What steps should the Engineer perform to prevent this outcome?

- A. Create an IAM user and generate a set of long-term credential
- B. Provide the credentials to AnyCompany. Monitor access in IAM access advisor and plan to rotate credentials on a recurring basis.
- C. Request an external ID from AnyCompany and add a condition with sts:ExternalId to the role's trust policy.
- D. Require two-factor authentication by adding a condition to the role's trust policy with aws:MultiFactorAuthPresent.
- E. Request an IP range from AnyCompany and add a condition with aws:SourceIp to the role's trust policy.

Answer: B

NEW QUESTION 178

- (Exam Topic 2)

The Security Engineer implemented a new vault lock policy for 10TB of data and called initiate-vault-lock 12 hours ago. The Audit team identified a typo that is allowing incorrect access to the vault.

What is the MOST cost-effective way to correct this?

- A. Call the abort-vault-lock operation, fix the typo, and call the initiate-vault-lock again.
- B. Copy the vault data to Amazon S3, delete the vault, and create a new vault with the data.
- C. Update the policy, keeping the vault lock in place.
- D. Update the policy and call initiate-vault-lock again to apply the new policy.

Answer: A

Explanation:

Initiate the lock by attaching a vault lock policy to your vault, which sets the lock to an in-progress state and returns a lock ID. While in the in-progress state, you have 24 hours to validate your vault lock policy before the lock ID expires. Use the lock ID to complete the lock process. If the vault lock policy doesn't work as expected, you can abort the lock and restart from the beginning. For information on how to use the S3 Glacier API to lock a vault, see Locking a Vault by Using the Amazon S3 Glacier API. <https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock-policy.html>

NEW QUESTION 179

- (Exam Topic 2)

An organization receives an alert that indicates that an EC2 instance behind an ELB Classic Load Balancer has been compromised.

What techniques will limit lateral movement and allow evidence gathering?

- A. Remove the instance from the load balancer and terminate it.
- B. Remove the instance from the load balancer, and shut down access to the instance by tightening the security group.
- C. Reboot the instance and check for any Amazon CloudWatch alarms.
- D. Stop the instance and make a snapshot of the root EBS volume.

Answer: B

Explanation:

https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

NEW QUESTION 182

- (Exam Topic 2)

A company is hosting a website that must be accessible to users for HTTPS traffic. Also port 22 should be open for administrative purposes. The administrator's workstation has a static IP address of 203.0.113.1/32. Which of the following security group configurations are the MOST secure but still functional to support these requirements? Choose 2 answers from the options given below

Please select:

- A. Port 443 coming from 0.0.0.0/0
- B. Port 443 coming from 10.0.0.0/16
- C. Port 22 coming from 0.0.0.0/0
- D. Port 22 coming from 203.0.113.1/32

Answer: AD

Explanation:

Since HTTPS traffic is required for all users on the Internet, Port 443 should be open on all IP addresses. For port 22, the traffic should be restricted to an internal subnet.

Option B is invalid, because this only allow traffic from a particular CIDR block and not from the internet Option C is invalid because allowing port 22 from the internet is a security risk

For more information on AWS Security Groups, please visit the following UR <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-secunty.html>

The correct answers are: Port 443 coming from 0.0.0.0/0, Port 22 coming from 203.0.113.1 /32 Submit your Feedback/Queries to our Experts

NEW QUESTION 185

- (Exam Topic 2)

The InfoSec team has mandated that in the future only approved Amazon Machine Images (AMIs) can be used.

How can the InfoSec team ensure compliance with this mandate?

- A. Terminate all Amazon EC2 instances and relaunch them with approved AMIs.
- B. Patch all running instances by using AWS Systems Manager.
- C. Deploy AWS Config rules and check all running instances for compliance.
- D. Define a metric filter in Amazon CloudWatch Logs to verify compliance.

Answer: C

Explanation:

<https://docs.aws.amazon.com/config/latest/developerguide/approved-amis-by-id.html>

NEW QUESTION 187

- (Exam Topic 2)

Your company has mandated that all calls to the AWS KMS service be recorded. How can this be achieved? Please select:

- A. Enable logging on the KMS service
- B. Enable a trail in Cloudtrail
- C. Enable Cloudwatch logs
- D. Use Cloudwatch metrics

Answer: B

Explanation:

The AWS Documentation states the following

AWS KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of AWS KMS in your AWS account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures API calls from the AWS KMS console or from the AWS KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP address from which the request was made, who made the request when it was made, and so on.

Option A is invalid because logging is not possible in the KMS service

Option C and D are invalid because Cloudwatch cannot be used to monitor API calls For more information on logging using Cloudtrail please visit the below URL

<https://docs.aws.amazon.com/kms/latest/developerguide/loeeing-usine-cloudtrail.html> The correct answer is: Enable a trail in Cloudtrail

Jubmit your Feedback/Queries to our Experts

NEW QUESTION 192

- (Exam Topic 2)

An application has been built with Amazon EC2 instances that retrieve messages from Amazon SQS. Recently, IAM changes were made and the instances can no longer retrieve messages.

What actions should be taken to troubleshoot the issue while maintaining least privilege. (Select two.)

- A. Configure and assign an MFA device to the role used by the instances.
- B. Verify that the SQS resource policy does not explicitly deny access to the role used by the instances.
- C. Verify that the access key attached to the role used by the instances is active.
- D. Attach the AmazonSQSFullAccess managed policy to the role used by the instances.
- E. Verify that the role attached to the instances contains policies that allow access to the queue.

Answer: BE

NEW QUESTION 195

- (Exam Topic 2)

A Development team has asked for help configuring the IAM roles and policies in a new AWS account. The team using the account expects to have hundreds of master keys and therefore does not want to manage access control for customer master keys (CMKs).

Which of the following will allow the team to manage AWS KMS permissions in IAM without the complexity of editing individual key policies?

- A. The account's CMK key policy must allow the account's IAM roles to perform KMS EnableKey.
- B. Newly created CMKs must have a key policy that allows the root principal to perform all actions.
- C. Newly created CMKs must allow the root principal to perform the kms CreateGrant API operation.
- D. Newly created CMKs must mirror the IAM policy of the KMS key administrator.

Answer: B

Explanation:

<https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html#key-policy-default-allow-root-enable>

NEW QUESTION 197

- (Exam Topic 2)

A Developer's laptop was stolen. The laptop was not encrypted, and it contained the SSH key used to access multiple Amazon EC2 instances. A Security Engineer has verified that the key has not been used, and has blocked port 22 to all EC2 instances while developing a response plan. How can the Security Engineer further protect currently running instances?

- A. Delete the key-pair key from the EC2 console, then create a new key pair.
- B. Use the modify-instance-attribute API to change the key on any EC2 instance that is using the key.
- C. Use the EC2 RunCommand to modify the authorized_keys file on any EC2 instance that is using the key.
- D. Update the key pair in any AMI used to launch the EC2 instances, then restart the EC2 instances.

Answer: C

NEW QUESTION 198

- (Exam Topic 2)

A Software Engineer is trying to figure out why network connectivity to an Amazon EC2 instance does not appear to be working correctly. Its security group allows inbound HTTP traffic from 0.0.0.0/0, and the outbound rules have not been modified from the default. A custom network ACL associated with its subnet allows inbound HTTP traffic from 0.0.0.0/0 and has no outbound rules. What would resolve the connectivity issue?

- A. The outbound rules on the security group do not allow the response to be sent to the client on the ephemeral port range.
- B. The outbound rules on the security group do not allow the response to be sent to the client on the HTTP port.
- C. An outbound rule must be added to the network ACL to allow the response to be sent to the client on the ephemeral port range.
- D. An outbound rule must be added to the network ACL to allow the response to be sent to the client on the HTTP port.

Answer: C

Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

NEW QUESTION 201

- (Exam Topic 2)

Some highly sensitive analytics workloads are to be moved to Amazon EC2 hosts. Threat modeling has found that a risk exists where a subnet could be maliciously or accidentally exposed to the internet. Which of the following mitigations should be recommended?

- A. Use AWS Config to detect whether an Internet Gateway is added and use an AWS Lambda function to provide auto-remediation.
- B. Within the Amazon VPC configuration, mark the VPC as private and disable Elastic IP addresses.
- C. Use IPv6 addressing exclusively on the EC2 hosts, as this prevents the hosts from being accessed from the internet.
- D. Move the workload to a Dedicated Host, as this provides additional network security controls and monitoring.

Answer: A

Explanation:

By default, Private instance has a private IP address, but no public IP address. These instances can communicate with each other, but can't access the Internet. You can enable Internet access for an instance launched into a nondefault subnet by attaching an Internet gateway to its VPC (if its VPC is not a default VPC) and associating an Elastic IP address with the instance. Alternatively, to allow an instance in your VPC to initiate outbound connections to the Internet but prevent unsolicited inbound connections from the Internet, you can use a network address translation (NAT) instance. NAT maps multiple private IP addresses to a single public IP address. A NAT instance has an Elastic IP address and is connected to the Internet through an Internet gateway. You can connect an instance in a private subnet to the Internet through the NAT instance, which routes traffic from the instance to the Internet gateway, and routes any responses to the instance.

NEW QUESTION 206

- (Exam Topic 2)

A Systems Engineer is troubleshooting the connectivity of a test environment that includes a virtual security appliance deployed inline. In addition to using the virtual security appliance, the Development team wants to use security groups and network ACLs to accomplish various security requirements in the environment. What configuration is necessary to allow the virtual security appliance to route the traffic?

- A. Disable network ACLs.
- B. Configure the security appliance's elastic network interface for promiscuous mode.
- C. Disable the Network Source/Destination check on the security appliance's elastic network interface
- D. Place the security appliance in the public subnet with the internet gateway

Answer: C

Explanation:

Each EC2 instance performs source/destination checks by default. This means that the instance must be the source or destination of any traffic it sends or receives. In this case virtual security appliance instance must be able to send and receive traffic when the source or destination is not itself. Therefore, you must disable source/destination checks on the NAT instance."

NEW QUESTION 211

- (Exam Topic 2)

Amazon CloudWatch Logs agent is successfully delivering logs to the CloudWatch Logs service. However, logs stop being delivered after the associated log stream has been active for a specific number of hours. What steps are necessary to identify the cause of this phenomenon? (Choose two.)

- A. Ensure that file permissions for monitored files that allow the CloudWatch Logs agent to read the file have not been modified.
- B. Verify that the OS Log rotation rules are compatible with the configuration requirements for agent streaming.
- C. Configure an Amazon Kinesis producer to first put the logs into Amazon Kinesis Streams.
- D. Create a CloudWatch Logs metric to isolate a value that changes at least once during the period before logging stops.
- E. Use AWS CloudFormation to dynamically create and maintain the configuration file for the CloudWatch Logs agent.

Answer: AB

Explanation:

[https://acloud.guru/forums/aws-certified-security-specialty/discussion/-Lm5A3w6_NybQPhh6tRP/Cloudwatch%](https://acloud.guru/forums/aws-certified-security-specialty/discussion/-Lm5A3w6_NybQPhh6tRP/Cloudwatch%20agent%20streaming%20requirements)

NEW QUESTION 213

- (Exam Topic 2)

An application outputs logs to a text file. The logs must be continuously monitored for security incidents.

Which design will meet the requirements with MINIMUM effort?

- A. Create a scheduled process to copy the component's logs into Amazon S3. Use S3 events to trigger a Lambda function that updates Amazon CloudWatch metrics with the log data.
- B. Set up CloudWatch alerts based on the metrics.
- C. Install and configure the Amazon CloudWatch Logs agent on the application's EC2 instance.
- D. Create a CloudWatch metric filter to monitor the application log.
- E. Set up CloudWatch alerts based on the metrics.
- F. Create a scheduled process to copy the application log files to AWS CloudTrail.
- G. Use S3 events to trigger Lambda functions that update CloudWatch metrics with the log data.
- H. Set up CloudWatch alerts based on the metrics.
- I. Create a file watcher that copies data to Amazon Kinesis when the application writes to the log file. Have Kinesis trigger a Lambda function to update Amazon CloudWatch metrics with the log data.
- J. Set up CloudWatch alerts based on the metrics.

Answer: B

Explanation:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/QuickStartEC2Instance.html>

NEW QUESTION 214

- (Exam Topic 2)

An Amazon EC2 instance is part of an EC2 Auto Scaling group that is behind an Application Load Balancer (ALB). It is suspected that the EC2 instance has been compromised.

Which steps should be taken to investigate the suspected compromise? (Choose three.)

- A. Detach the elastic network interface from the EC2 instance.
- B. Initiate an Amazon Elastic Block Store volume snapshot of all volumes on the EC2 instance.
- C. Disable any Amazon Route 53 health checks associated with the EC2 instance.
- D. De-register the EC2 instance from the ALB and detach it from the Auto Scaling group.
- E. Attach a security group that has restrictive ingress and egress rules to the EC2 instance.
- F. Add a rule to an AWS WAF to block access to the EC2 instance.

Answer: BDE

Explanation:

https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

NEW QUESTION 218

- (Exam Topic 2)

The Security Engineer is given the following requirements for an application that is running on Amazon EC2 and managed by using AWS CloudFormation templates with EC2 Auto Scaling groups:

-Have the EC2 instances bootstrapped to connect to a backend database.

-Ensure that the database credentials are handled securely.

-Ensure that retrievals of database credentials are logged.

Which of the following is the MOST efficient way to meet these requirements?

- A. Pass database credentials to EC2 by using CloudFormation stack parameters with the property set to true.
- B. Ensure that the instance is configured to log to Amazon CloudWatch Logs.
- C. Store database passwords in AWS Systems Manager Parameter Store by using SecureString parameters. Set the IAM role for the EC2 instance profile to allow access to the parameters.
- D. Create an AWS Lambda that ingests the database password and persists it to Amazon S3 with server-side encryption.
- E. Have the EC2 instances retrieve the S3 object on startup, and log all script invocations to syslog.
- F. Write a script that is passed in as UserData so that it is executed upon launch of the EC2 instance. Ensure that the instance is configured to log to Amazon CloudWatch Logs.

Answer: B

NEW QUESTION 220

- (Exam Topic 2)

You have an S3 bucket hosted in AWS. This is used to host promotional videos uploaded by yourself. You need to provide access to users for a limited duration of time. How can this be achieved?

Please select:

- A. Use versioning and enable a timestamp for each version.

- B. Use Pre-signed URL's
- C. Use IAM Roles with a timestamp to limit the access
- D. Use IAM policies with a timestamp to limit the access

Answer: B

Explanation:

The AWS Documentation mentions the following

All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects.

Option A is invalid because this can be used to prevent accidental deletion of objects Option C is invalid because timestamps are not possible for Roles

Option D is invalid because policies is not the right way to limit access based on time For more information on pre-signed URL's, please visit the URL:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>

The correct answer is: Use Pre-signed URL's Submit your Feedback/Queries to our Experts

NEW QUESTION 223

- (Exam Topic 2)

You have just recently set up a web and database tier in a VPC and hosted the application. When testing the app , you are not able to reach the home page for the app. You have verified the security groups. What can help you diagnose the issue.

Please select:

- A. Use the AWS Trusted Advisor to see what can be done.
- B. Use VPC Flow logs to diagnose the traffic
- C. Use AWS WAF to analyze the traffic
- D. Use AWS Guard Duty to analyze the traffic

Answer: B

Explanation:

Option A is invalid because this can be used to check for security issues in your account, but not verify as to why you cannot reach the home page for your application

Option C is invalid because this used to protect your app against application layer attacks, but not verify as to why you cannot reach the home page for your application

Option D is invalid because this used to protect your instance against attacks, but not verify as to why you cannot reach the home page for your application

The AWS Documentation mentions the following

VPC Flow Logs capture network flow information for a VPC, subnet or network interface and stores it in Amazon CloudWatch Logs. Flow log data can help customers troubleshoot network issues; for example, to diagnose why specific traffic is not reaching an instance, which might be a result of overly restrictive security group rules. Customers can also use flow logs as a security tool to monitor the traffic that reaches their instances, to profile network traffic, and to look for abnormal traffic behaviors.

For more information on AWS Security, please visit the following URL: <https://aws.amazon.com/answers/networking/vpc-security-capabilities>

The correct answer is: Use VPC Flow logs to diagnose the traffic Submit your Feedback/Queries to our Experts

NEW QUESTION 226

- (Exam Topic 2)

The Security Engineer is managing a web application that processes highly sensitive personal information. The application runs on Amazon EC2. The application has strict compliance requirements, which instruct that all incoming traffic to the application is protected from common web exploits and that all outgoing traffic from the EC2 instances is restricted to specific whitelisted URLs.

Which architecture should the Security Engineer use to meet these requirements?

- A. Use AWS Shield to scan inbound traffic for web exploit
- B. Use VPC Flow Logs and AWS Lambda to restrict egress traffic to specific whitelisted URLs.
- C. Use AWS Shield to scan inbound traffic for web exploit
- D. Use a third-party AWS Marketplace solution to restrict egress traffic to specific whitelisted URLs.
- E. Use AWS WAF to scan inbound traffic for web exploit
- F. Use VPC Flow Logs and AWS Lambda to restrict egress traffic to specific whitelisted URLs.
- G. Use AWS WAF to scan inbound traffic for web exploit
- H. Use a third-party AWS Marketplace solution to restrict egress traffic to specific whitelisted URLs.

Answer: D

Explanation:

AWS Shield is mainly for DDos Attacks. AWS WAF is mainly for some other types of attacks like Injection and XSS etc. In this scenario, It seems it is WAF functionality that is needed. VPC logs do show the source and destination IP and Port , they never show any URL .. because URL are level 7 while VPC are concerned about lower network levels.

<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>

NEW QUESTION 227

- (Exam Topic 2)

A distributed web application is installed across several EC2 instances in public subnets residing in two Availability Zones. Apache logs show several intermittent brute-force attacks from hundreds of IP addresses at the layer 7 level over the past six months.

What would be the BEST way to reduce the potential impact of these attacks in the future?

- A. Use custom route tables to prevent malicious traffic from routing to the instances.
- B. Update security groups to deny traffic from the originating source IP addresses.
- C. Use network ACLs.
- D. Install intrusion prevention software (IPS) on each instance.

Answer: D

Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html> NACL has limit 20 (can increase to maximum 40 rule), and more rule will make more low-latency

NEW QUESTION 228

- (Exam Topic 2)

A Security Engineer must add additional protection to a legacy web application by adding the following HTTP security headers:

- Content Security-Policy
- X-Frame-Options
- X-XSS-Protection

The Engineer does not have access to the source code of the legacy web application. Which of the following approaches would meet this requirement?

- A. Configure an Amazon Route 53 routing policy to send all web traffic that does not include the required headers to a black hole.
- B. Implement an AWS Lambda@Edge origin response function that inserts the required headers.
- C. Migrate the legacy application to an Amazon S3 static website and front it with an Amazon CloudFront distribution.
- D. Construct an AWS WAF rule to replace existing HTTP headers with the required security headers by using regular expressions.

Answer: B

NEW QUESTION 232

- (Exam Topic 2)

Your company has a set of resources defined in the AWS Cloud. Their IT audit department has requested to get a list of resources that have been defined across the account. How can this be achieved in the easiest manner?

Please select:

- A. Create a powershell script using the AWS CL
- B. Query for all resources with the tag of production.
- C. Create a bash shell script with the AWS CL
- D. Query for all resources in all region
- E. Store the results in an S3 bucket.
- F. Use Cloud Trail to get the list of all resources
- G. Use AWS Config to get the list of all resources



Answer: D

Explanation:

The most feasible option is to use AWS Config. When you turn on AWS Config, you will get a list of resources defined in your AWS Account.

A sample snapshot of the resources dashboard in AWS Config is shown below C:\Users\wk\Desktop\mudassar\Untitled.jpg



Resources	
Total resource count	131
Top 10 resource types	
 IAM Policy	45
 IAM Role	40
 EC2 Subnet	7
 EC2 SecurityGroup	6
 EC2 RouteTable	6
 EC2 VPC	4
 EC2 NetworkAcl	4

Option A is incorrect because this would give the list of production based resources and now all resources Option B is partially correct But this will just add more maintenance overhead.

Option C is incorrect because this can be used to log API activities but not give an account of all resou For more information on AWS Config, please visit the below URL: <https://docs.aws.amazon.com/config/latest/developereuide/how-does-confie-work.html>

The correct answer is: Use AWS Config to get the list of all resources Submit your Feedback/Queries to our Experts

NEW QUESTION 236

- (Exam Topic 2)

Your company has defined privileged users for their AWS Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security authentication for these users. How can this be accomplished?

Please select:

- A. Enable MFA for these user accounts
- B. Enable versioning for these user accounts

- C. Enable accidental deletion for these user accounts
- D. Disable root access for the users

Answer: A

Explanation:

The AWS Documentation mentions the following as a best practices for IAM users. For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).

Option B,C and D are invalid because no such security options are available in AWS For more information on IAM best practices, please visit the below URL

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html> The correct answer is: Enable MFA for these user accounts

Submit your Feedback/Queries to our Experts

NEW QUESTION 237

- (Exam Topic 2)

A company plans to move most of its IT infrastructure to AWS. They want to leverage their existing on-premises Active Directory as an identity provider for AWS. Which combination of steps should a Security Engineer take to federate the company's on-premises Active Directory with AWS? (Choose two.)

- A. Create IAM roles with permissions corresponding to each Active Directory group.
- B. Create IAM groups with permissions corresponding to each Active Directory group.
- C. Configure Amazon Cloud Directory to support a SAML provider.
- D. Configure Active Directory to add relying party trust between Active Directory and AWS.
- E. Configure Amazon Cognito to add relying party trust between Active Directory and AWS.

Answer: AD

Explanation:

<https://aws.amazon.com/blogs/security/how-to-establish-federated-access-to-your-aws-resources-by-using-activ>

NEW QUESTION 238

- (Exam Topic 2)

You have an instance setup in a test environment in AWS. You installed the required application and the promoted the server to a production environment. Your IT Security team has advised that there maybe traffic flowing in from an unknown IP address to port 22. How can this be mitigated immediately?

Please select:

- A. Shutdown the instance
- B. Remove the rule for incoming traffic on port 22 for the Security Group
- C. Change the AMI for the instance
- D. Change the Instance type for the instance

Answer: B

Explanation:

In the test environment the security groups might have been opened to all IP addresses for testing purpose. Always to ensure to remove this rule once all testing is completed.

Option A, C and D are all invalid because this would affect the application running on the server. The easiest way is just to remove the rule for access on port 22.

For more information on authorizing access to an instance, please visit the below URL: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html>

The correct answer is: Remove the rule for incoming traffic on port 22 for the Security Group Submit your Feedback/Queries to our Experts

NEW QUESTION 243

- (Exam Topic 2)

Which approach will generate automated security alerts should too many unauthorized AWS API requests be identified?

- A. Create an Amazon CloudWatch metric filter that looks for API call error codes and then implement an alarm based on that metric's rate.
- B. Configure AWS CloudTrail to stream event data to Amazon Kinesi
- C. Configure an AWS Lambda function on the stream to alarm when the threshold has been exceeded.
- D. Run an Amazon Athena SQL query against CloudTrail log file
- E. Use Amazon QuickSight to create an operational dashboard.
- F. Use the Amazon Personal Health Dashboard to monitor the account's use of AWS services, and raise an alert if service error rates increase.

Answer: A

Explanation:

[https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html#cloudwatch-](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html#cloudwatch) Open the CloudWatch console at

<https://console.aws.amazon.com/cloudwatch/>. In the navigation pane, choose Logs. In the list of log groups, select the check box next to the log group that you created for CloudTrail log events. Choose Create Metric Filter. On the Define Logs Metric Filter screen, choose Filter Pattern and then type the following: { (\$errorCode = "UnauthorizedOperation") || (\$errorCode = "AccessDenied")} Choose Assign Metric. For Filter Name, type AuthorizationFailures. For Metric Namespace, type CloudTrailMetrics. For Metric Name, type AuthorizationFailureCount.

NEW QUESTION 246

- (Exam Topic 2)

You have enabled Cloudtrail logs for your company's AWS account. In addition, the IT Security department has mentioned that the logs need to be encrypted. How can this be achieved?

Please select:

- A. Enable SSL certificates for the Cloudtrail logs
- B. There is no need to do anything since the logs will already be encrypted

- C. Enable Server side encryption for the trail
- D. Enable Server side encryption for the destination S3 bucket

Answer: B

Explanation:

The AWS Documentation mentions the following.

By default CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encryption your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about log file delivery and validation, you can set up Amazon SNS notifications.

Option A,C and D are not valid since logs will already be encrypted

For more information on how Cloudtrail works, please visit the following URL: <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/how-cloudtrail-works.html>

The correct answer is: There is no need to do anything since the logs will already be encrypted Submit your Feedback/Queries to our Experts

NEW QUESTION 249

- (Exam Topic 2)

During a recent internal investigation, it was discovered that all API logging was disabled in a production account, and the root user had created new API keys that appear to have been used several times.

What could have been done to detect and automatically remediate the incident?

- A. Using Amazon Inspector, review all of the API calls and configure the inspector agent to leverage SNS topics to notify security of the change to AWS CloudTrail, and revoke the new API keys for the root user.
- B. Using AWS Config, create a config rule that detects when AWS CloudTrail is disabled, as well as any calls to the root user create-api-key
- C. Then use a Lambda function to re-enable CloudTrail logs and deactivate the root API keys.
- D. Using Amazon CloudWatch, create a CloudWatch event that detects AWS CloudTrail deactivation and a separate Amazon Trusted Advisor check to automatically detect the creation of root API key
- E. Then use a Lambda function to enable AWS CloudTrail and deactivate the root API keys.
- F. Using Amazon CloudTrail, create a new CloudTrail event that detects the deactivation of CloudTrail logs, and a separate CloudTrail event that detects the creation of root API key
- G. Then use a Lambda function to enable CloudTrail and deactivate the root API keys.

Answer: B

Explanation:

<https://docs.aws.amazon.com/config/latest/developerguide/cloudtrail-enabled.html> <https://docs.aws.amazon.com/config/latest/developerguide/iam-root-access-key-check.html>

NEW QUESTION 254

- (Exam Topic 2)

A Security Engineer has been asked to create an automated process to disable IAM user access keys that are more than three months old.

Which of the following options should the Security Engineer use?

- A. In the AWS Console, choose the IAM service and select "Users". Review the "Access Key Age" column.
- B. Define an IAM policy that denies access if the key age is more than three months and apply to all users.
- C. Write a script that uses the GenerateCredentialReport, GetCredentialReport, and UpdateAccessKey APIs.
- D. Create an Amazon CloudWatch alarm to detect aged access keys and use an AWS Lambda function to disable the keys older than 90 days.

Answer: C

Explanation:

https://docs.aws.amazon.com/IAM/latest/APIReference/API_UpdateAccessKey.html

https://docs.aws.amazon.com/IAM/latest/APIReference/API_GenerateCredentialReport.html

https://docs.aws.amazon.com/IAM/latest/APIReference/API_GetCredentialReport.html

NEW QUESTION 256

- (Exam Topic 2)

You have a 2 tier application hosted in AWS. It consists of a web server and database server (SQL Server) hosted on separate EC2 Instances. You are devising the security groups for these EC2 Instances. The Web tier needs to be accessed by users across the Internet. You have created a web security group(wg-123) and database security group(db-345). Which combination of the following security group rules will allow the application to be secure and functional. Choose 2 answers from the options given below.

Please select:

- A. wg-123 -Allow ports 80 and 443 from 0.0.0.0/0
- B. db-345 - Allow port 1433 from wg-123
- C. wg-123 - Allow port 1433 from wg-123
- D. db-345 -Allow ports 1433 from 0.0.0.0/0

Answer: AB

Explanation:

The Web security groups should allow access for ports 80 and 443 for HTTP and HTTPS traffic to all users from the internet.

The database security group should just allow access from the web security group from port 1433. Option C is invalid because this is not a valid configuration

Option D is invalid because database security should not be allowed on the internet For more information on Security Groups please visit the below URL:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-security.html>

The correct answers are: wg-123 - Allow ports 80 and 443 from 0.0.0.0/0, db-345 - Allow port 1433 from wg-123

Submit your Feedback/Queries to our Experts

NEW QUESTION 259

- (Exam Topic 2)

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 IAM 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 263

- (Exam Topic 2)

A Systems Engineer has been tasked with configuring outbound mail through Simple Email Service (SES) and requires compliance with current TLS standards. The mail application should be configured to connect to which of the following endpoints and corresponding ports?

- A. email.us-east-1.amazonaws.com over port 8080
- B. email-pop3.us-east-1.amazonaws.com over port 995
- C. email-smtp.us-east-1.amazonaws.com over port 587
- D. email-imap.us-east-1.amazonaws.com over port 993

Answer: C

Explanation:

<https://docs.aws.amazon.com/ses/latest/DeveloperGuide/smtp-connect.html>

NEW QUESTION 268

- (Exam Topic 2)

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 IAM access keys
- C. Keep all resources running to avoid disruption
- D. Change the password for all IAM users.

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 IAM users.

Delete or rotate all root and AWS Identity and Access Management (IAM) access keys.

Delete any resources on your account you didn't create, especially running EC2 instances, EC2 spot bids, or IAM 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/knowledge-center/potential-account-compromise>>

The correct answers are: Change the root account password. Rotate all IAM access keys. Change the password for all IAM users. Submit your Feedback/Queries to our Experts

NEW QUESTION 271

- (Exam Topic 2)

A Security Engineer is working with a Product team building a web application on AWS. The application uses Amazon S3 to host the static content, Amazon API Gateway to provide RESTful services; and Amazon DynamoDB as the backend data store. The users already exist in a directory that is exposed through a SAML identity provider.

Which combination of the following actions should the Engineer take to enable users to be authenticated into the web application and call APIs? (Choose three.)

- A. Create a custom authorization service using AWS Lambda.
- B. Configure a SAML identity provider in Amazon Cognito to map attributes to the Amazon Cognito user pool attributes.
- C. Configure the SAML identity provider to add the Amazon Cognito user pool as a relying party.
- D. Configure an Amazon Cognito identity pool to integrate with social login providers.
- E. Update DynamoDB to store the user email addresses and passwords.
- F. Update API Gateway to use a COGNITO_USER_POOLS authorizer.

Answer: BDE

NEW QUESTION 274

- (Exam Topic 2)

You are hosting a web site via website hosting on an S3 bucket - <http://demo.s3-website-us-east-1.amazonaws.com>. You have some web pages that use Javascript that access resources in another bucket which has web site hosting also enabled. But when users access the web pages , they are getting a blocked Javascript error. How can you rectify this?

Please select:

- A. Enable CORS for the bucket
- B. Enable versioning for the bucket
- C. Enable MFA for the bucket
- D. Enable CRR for the bucket

Answer: A

Explanation:

Your answer is incorrect Answer-A

Such a scenario is also given in the AWS Documentation Cross-Origin Resource Sharing: Use-case Scenarios The following are example scenarios for using CORS:

- Scenario 1: Suppose that you are hosting a website in an Amazon S3 bucket named website as described in Hosting a Static Website on Amazon S3. Your users load the website endpoint <http://website.s3-website-us-east-1.amazonaws.com>. Now you want to use JavaScript on the webpages that are stored in this bucket to be able to make authenticated GET and PUT requests against the same bucket by using the Amazon S3 API endpoint for the bucket website.s3.amazonaws.com. A browser would normally block JavaScript from allowing those requests, but with CORS you can configure your bucket to explicitly enable cross-origin requests from website.s3-website-us-east-1.amazonaws.com.

- Scenario 2: Suppose that you want to host a web font from your S3 bucket. Again, browsers require a CORS check (also called a preflight check) for loading web fonts. You would configure the bucket that is hosting the web font to allow any origin to make these requests.

Option B is invalid because versioning is only to create multiple versions of an object and can help in accidental deletion of objects

Option C is invalid because this is used as an extra measure of caution for deletion of objects Option D is invalid because this is used for Cross region replication of objects

For more information on Cross Origin Resource sharing, please visit the following URL

- <https://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html> The correct answer is: Enable CORS for the bucket

Submit your Feedback/Queries to our Experts

NEW QUESTION 275

- (Exam Topic 2)

An application running on EC2 instances must use a username and password to access a database. The developer has stored those secrets in the SSM Parameter Store with type SecureString using the default KMS CMK. Which combination of configuration steps will allow the application to access the secrets via the API? Select 2 answers from the options below

Please select:

- A. Add the EC2 instance role as a trusted service to the SSM service role.
- B. Add permission to use the KMS key to decrypt to the SSM service role.
- C. Add permission to read the SSM parameter to the EC2 instance role
- D. .
- E. Add permission to use the KMS key to decrypt to the EC2 instance role
- F. Add the SSM service role as a trusted service to the EC2 instance role.

Answer: CD

Explanation:

The below example policy from the AWS Documentation is required to be given to the EC2 Instance in order to read a secure string from AWS KMS. Permissions need to be given to the Get Parameter API and the KMS API call to decrypt the secret.

C:\Users\wk\Desktop\mudassar\Untitled.jpg

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameter*"
      ],
      "Resource": "arn:aws:ssm:us-west-2:111122223333:parameter/ReadableParameters/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ]
}
```

Option A is invalid because roles can be attached to EC2 and not EC2 roles to SSM Option B is invalid because the KMS key does not need to decrypt the SSM service role.

Option E is invalid because this configuration is valid For more information on the parameter store, please visit the below URL:
<https://docs.aws.amazon.com/kms/latest/developerguide/services-parameter-store.html>

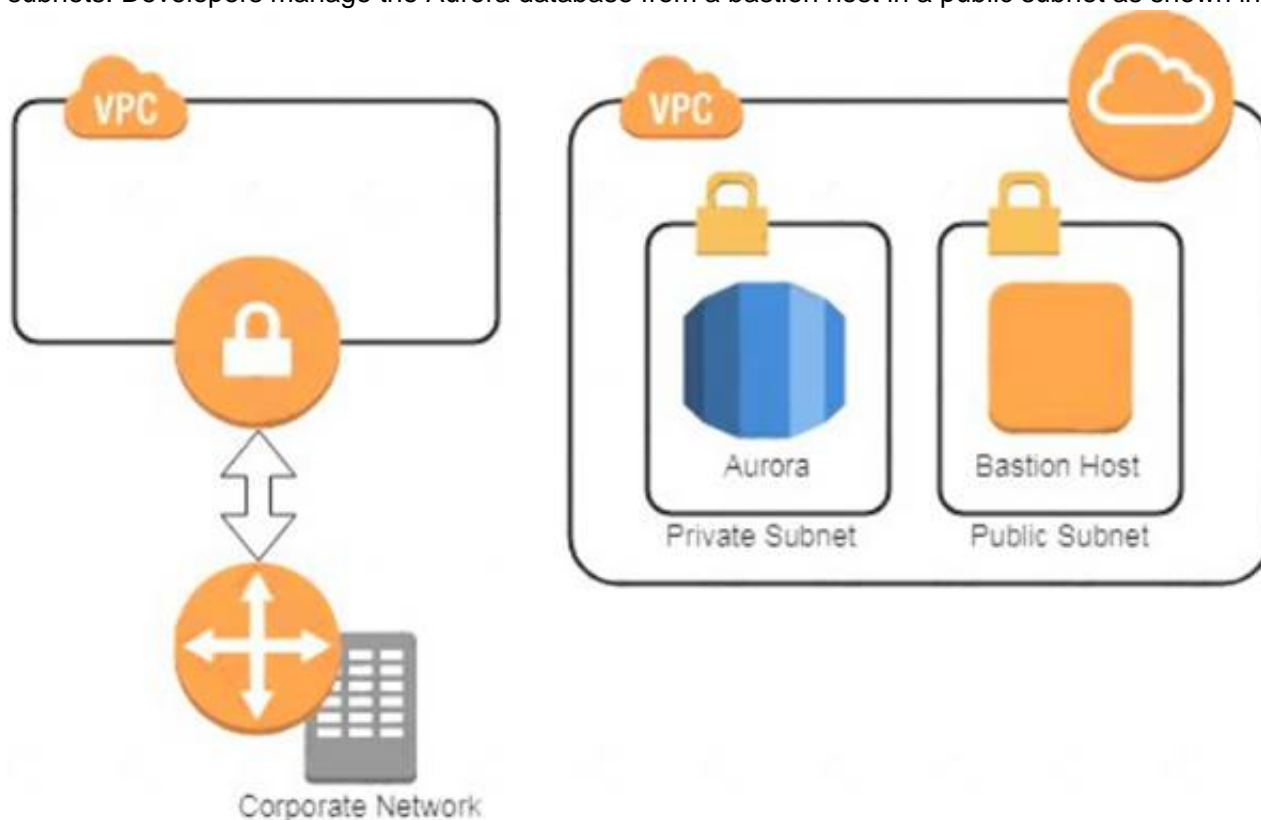
The correct answers are: Add permission to read the SSM parameter to the EC2 instance role., Add permission to use the KMS key to decrypt to the EC2 instance role

Submit your Feedback/Queries to our Experts

NEW QUESTION 278

- (Exam Topic 2)

A company has two AWS accounts, each containing one VPC. The first VPC has a VPN connection with its corporate network. The second VPC, without a VPN, hosts an Amazon Aurora database cluster in private subnets. Developers manage the Aurora database from a bastion host in a public subnet as shown in the image.



A security review has flagged this architecture as vulnerable, and a Security Engineer has been asked to make this design more secure. The company has a short deadline and a second VPN connection to the Aurora account is not possible.

How can a Security Engineer securely set up the bastion host?

- A. Move the bastion host to the VPC with VPN connectivity
- B. Create a VPC peering relationship between the bastion host VPC and Aurora VPC.
- C. Create a SSH port forwarding tunnel on the Developer's workstation to the bastion host to ensure that only authorized SSH clients can access the bastion host.
- D. Move the bastion host to the VPC with VPN connectivity
- E. Create a cross-account trust relationship between the bastion VPC and Aurora VPC, and update the Aurora security group for the relationship.
- F. Create an AWS Direct Connect connection between the corporate network and the Aurora account, and adjust the Aurora security group for this connection.

Answer: A

NEW QUESTION 283

- (Exam Topic 2)

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 IAM policy that gives the desired level of access to the Cloudtrail trail
- D. Create an IAM 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 IAM 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/Working>

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 IAM policy that gives the desired level of access to the Cloudwatch Log group

Submit your Feedback/Queries to our Experts

NEW QUESTION 287

- (Exam Topic 2)

Which of the following is the most efficient way to automate the encryption of AWS CloudTrail logs using a Customer Master Key (CMK) in AWS KMS?

- A. Use the KMS direct encrypt function on the log data every time a CloudTrail log is generated.
- B. Use the default Amazon S3 server-side encryption with S3-managed keys to encrypt and decrypt the CloudTrail logs.
- C. Configure CloudTrail to use server-side encryption using KMS-managed keys to encrypt and decrypt CloudTrail logs.
- D. Use encrypted API endpoints so that all AWS API calls generate encrypted CloudTrail log entries using the TLS certificate from the encrypted API call.

Answer: C

Explanation:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html>

NEW QUESTION 288

- (Exam Topic 2)

Compliance requirements state that all communications between company on-premises hosts and EC2 instances be encrypted in transit. Hosts use custom proprietary protocols for their communication, and EC2 instances need to be fronted by a load balancer for increased availability.

Which of the following solutions will meet these requirements?

- A. Offload SSL termination onto an SSL listener on a Classic Load Balancer, and use a TCP connection between the load balancer and the EC2 instances.
- B. Route all traffic through a TCP listener on a Classic Load Balancer, and terminate the TLS connection on the EC2 instances.
- C. Create an HTTPS listener using an Application Load Balancer, and route all of the communication through that load balancer.
- D. Offload SSL termination onto an SSL listener using an Application Load Balancer, and re-spawn and SSL connection between the load balancer and the EC2 instances.

Answer: B

Explanation:

<https://aws.amazon.com/blogs/compute/maintaining-transport-layer-security-all-the-way-to-your-container-usin>

NEW QUESTION 292

.....

Relate Links

100% Pass Your AWS-Certified-Security-Specialty Exam with Examible Prep Materials

<https://www.exambible.com/AWS-Certified-Security-Specialty-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>