Topic 1 - Exam A

Question #1 *Topic 1*

A company has an AWS Lambda function that creates image thumbnails from larger images. The Lambda function needs read and write access to an Amazon S3 bucket in the same AWS account.
Which solutions will provide the Lambda function this access? (Choose two.)

A. Create an IAM user that has only programmatic access. Create a new access key pair. Add environmental variables to the Lambda function with the access key ID and secret access key. Modify the Lambda function to use the environmental variables at run time during communication with Amazon S3.

B. Generate an Amazon EC2 key pair. Store the private key in AWS Secrets Manager. Modify the Lambda function to retrieve the private key from Secrets Manager and to use the private key during communication with Amazon S3.

C. Create an IAM role for the Lambda function. Attach an IAM policy that allows access to the S3 bucket.

D. Create an IAM role for the Lambda function. Attach a bucket policy to the S3 bucket to allow access. Specify the function's IAM role as the principal.

E. Create a security group. Attach the security group to the Lambda function. Attach a bucket policy that allows access to the S3 bucket through the security group ID.

Correct Answer: *BE*

Community vote distribution

CD (100%)

tulmegusto Highly Voted 2 months, 1 week ago

Selected Answer: CD

itexamstest.com

no disscusion cd :)

upvoted 13 times

Certified101 Highly Voted 4 months, 3 weeks ago

Selected Answer: CD

C & D - The other 3 are defiantly wrong

upvoted 5 times

Raphaello Most Recent 2 weeks, 3 days ago

Selected Answer: CD

CD

Always create execution role for your lambda function, as a best practice.

upvoted 1 times

aescudero51 2 weeks, 4 days ago

Respuesta seleccionada: CD

upvoted 1 times

sarcactus 1 month, 1 week ago

Selected Answer: CD

CD are the correct ones!
But do i need to put these correct answers or answers marked as "Correct Answer" on the real exam?

upvoted 1 times

Raphaello 2 months, 2 weeks ago

CD
Why the answers for many questions are categorically wrong?

upvoted 3 times

awssecuritynewbie 3 months ago

Selected Answer: CD

for sure this will be the use of AWS ROLES it is simple, you attach a role to the lambda to be able to access certain S3 bucket.

upvoted 1 times

Daniel76 3 months, 2 weeks ago

Selected Answer: CD

Refer to this:
https://repost.aws/knowledge-center/lambda-execution-role-s3-bucket

upvoted 2 times

[Removed] 3 months, 4 weeks ago

Selected Answer: CD

C and D

upvoted 1 times

lalee2 4 months ago

Selected Answer: CD

same account. for ABAC IAM role w/ policy will do. RBAC requires principal

upvoted 1 times

pupsik 4 months ago

Selected Answer: CD

Permission needs to be specified either from Lambda's role policy, or from S3 bucket's resource policy.

upvoted 2 times

KR693 4 months ago

c and d

upvoted 2 times

dhax12 4 months, 3 weeks ago

Any type of key means a long term access. Always use IAM roles to keep access temporarily. Answer should be C&D

upvoted 2 times

RayHK 4 months, 3 weeks ago

vote for C and D

upvoted 3 times

Question #2 *Topic 1*

A security engineer is configuring a new website that is named example.com. The security engineer wants to secure communications with the website by requiring users to connect to example.com through HTTPS.
Which of the following is a valid option for storing SSL/TLS certificates?

A. Custom SSL certificate that is stored in AWS Key Management Service (AWS KMS)

B. Default SSL certificate that is stored in Amazon CloudFront

C. Custom SSL certificate that is stored in AWS Certificate Manager (ACM)

D. Default SSL certificate that is stored in Amazon S3

Correct Answer: *C*

Community vote distribution

C (100%)

tulmegusto Highly Voted 2 months, 1 week ago

Selected Answer: C

itexamstest.com

no disscusion c :)

upvoted 13 times

Raphaello Most Recent 2 weeks, 3 days ago

Selected Answer: C

Correct answer is C

upvoted 1 times

aescudero51 2 weeks, 4 days ago

Respuesta seleccionada: C

upvoted 1 times

awssecuritynewbie 3 months, 1 week ago

Did anyone take this exam? Is these dumps valid?

upvoted 1 times

Daniel76 3 months, 2 weeks ago

Selected Answer: C

ACM is the natural choice.

upvoted 1 times

[Removed] 3 months, 4 weeks ago

Selected Answer: C

Answer C

upvoted 1 times

imymoco 4 months ago

Answer is C

upvoted 1 times

lalee2 4 months ago

Selected Answer: C

ACM do the job

upvoted 1 times

pupsik 4 months ago

Selected Answer: C

ACM is where you would normally store SSL certificates.

upvoted 1 times

KR693 4 months ago

Answer C

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: C

Answer C

upvoted 1 times

Certified101 4 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

aragon_saa 4 months, 3 weeks ago

https://www.examtopics.com/discussions/amazon/view/88394-exam-aws-certified-security-specialty-topic-1-question-359/

upvoted 2 times

Question #3 *Topic 1*

A security engineer needs to develop a process to investigate and respond to potential security events on a company's Amazon EC2 instances. All the EC2 instances are backed by Amazon Elastic Block Store (Amazon EBS). The company uses AWS Systems Manager to manage all the EC2 instances and has installed Systems Manager Agent (SSM Agent) on all the EC2 instances.
The process that the security engineer is developing must comply with AWS security best practices and must meet the following requirements:
A compromised EC2 instance's volatile memory and non-volatile memory must be preserved for forensic purposes.
A compromised EC2 instance's metadata must be updated with corresponding incident ticket information.
A compromised EC2 instance must remain online during the investigation but must be isolated to prevent the spread of malware.
Any investigative activity during the collection of volatile data must be captured as part of the process.
Which combination of steps should the security engineer take to meet these requirements with the LEAST operational overhead? (Choose three.)

A. Gather any relevant metadata for the compromised EC2 instance. Enable termination protection. Isolate the instance by updating the instance's security groups to restrict access. Detach the instance from any Auto Scaling groups that the instance is a member of. Deregister the instance from any Elastic Load Balancing (ELB) resources.

B. Gather any relevant metadata for the compromised EC2 instance. Enable termination protection. Move the instance to an isolation subnet that denies all source and destination traffic. Associate the instance with the subnet to restrict access. Detach the instance from any Auto Scaling groups that the instance is a member of. Deregister the instance from any Elastic Load Balancing (ELB) resources.

C. Use Systems Manager Run Command to invoke scripts that collect volatile data.

D. Establish a Linux SSH or Windows Remote Desktop Protocol (RDP) session to the compromised EC2 instance to invoke scripts that collect volatile data.

E. Create a snapshot of the compromised EC2 instance's EBS volume for follow-up investigations. Tag the instance with any relevant metadata and incident ticket information.

F. Create a Systems Manager State Manager association to generate an EBS volume snapshot of the compromised EC2 instance. Tag the instance with any relevant metadata and incident ticket information.

Correct Answer: *BCE*

Community vote distribution

ACE (100%)

tulmegusto Highly Voted 2 months, 1 week ago

Selected Answer: ACE

itexamstest.com

no disscusion ace :)

upvoted 13 times

pupsik Highly Voted 4 months ago

Selected Answer: ACE

The reason it is not "B" is because you cannot move a running instance into a different subnet.

upvoted 8 times

Raphaello Most Recent 2 weeks, 3 days ago

Selected Answer: ACE

Correct answers: ACE
These describe the ideal steps to isolate an instance, and collect data required for forensics investigation, all limiting the spread of malware.

upvoted 1 times

csG13 1 month, 3 weeks ago

A & C are correct. Since it's an SSM managed node already, why not F?

upvoted 1 times

Sab31 2 months ago

Can someone share why not F? As it automated the EBS backup process. Hence reducing the overhead.

upvoted 1 times

Daniel76 1 month, 3 weeks ago

F is technically feasible but SSM state manager is used for routine backup of EC2 instances. In this case the snapshot is one-off and you cannot automate the second part that is tagging with metadata and incident ticket info. So it is not appropriate.

upvoted 3 times

Daniel76 2 months, 1 week ago

Selected Answer: ACE

between C and D,
D is a traditional method which has more overhead: need to preconfigure instance connectivity to external storage medium for writing memory
And it risk altering the memory and storage artifacts in the process. Using system manager is a comparatively better way.

https://d1.awsstatic.com/events/aws-reinforce-2022/TDR401_Instance-memory-acquisition-techniques-for-effective-incident-response.pdf

upvoted 1 times

Raphaello 2 months, 2 weeks ago

A C E
It's not possible to move an existing instance to another subnet; rather, one can associate it with a restricted SG.

upvoted 1 times

awssecuritynewbie 3 months ago

Selected Answer: ACE

A C E, for sure.

upvoted 1 times

[Removed] 3 months, 4 weeks ago

Selected Answer: ACE

A, C, E

upvoted 1 times

lalee2 4 months ago

Selected Answer: ACE

Gather info -> isolate -> detach ->snapshot

upvoted 1 times

KR693 4 months ago

A, C and E

upvoted 1 times

0dd 4 months, 3 weeks ago

ACE. B is incorrect because once a EC2 instance created, it could not be moved to other subnets

upvoted 3 times

kk2000 4 months, 3 weeks ago

ACE makes more sense.Updating Security group(Least operational overhead) rather than moving the EC2 to different subnet which needs more steps required.

upvoted 1 times

Question #4 *Topic 1*

A company has an organization in AWS Organizations. The company wants to use AWS CloudFormation StackSets in the organization to deploy various AWS design patterns into environments. These patterns consist of Amazon EC2 instances, Elastic Load Balancing (ELB) load balancers, Amazon RDS databases, and Amazon Elastic Kubernetes Service (Amazon EKS) clusters or Amazon Elastic Container Service (Amazon ECS) clusters.
Currently, the company's developers can create their own CloudFormation stacks to increase the overall speed of delivery. A centralized CI/CD pipeline in a shared services AWS account deploys each CloudFormation stack.
The company's security team has already provided requirements for each service in accordance with internal standards. If there are any resources that do not comply with the internal standards, the security team must receive notification to take appropriate action. The security team must implement a notification solution that gives developers the ability to maintain the same overall delivery speed that they currently have.
Which solution will meet these requirements in the MOST operationally efficient way?

A. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the security team's email addresses to the SNS topic. Create a custom AWS Lambda function that will run the aws cloudformation validate-template AWS CLI command on all CloudFormation templates before the build stage in the CI/CD pipeline. Configure the CI/CD pipeline to publish a notification to the SNS topic if any issues are found.

B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the security team's email addresses to the SNS topic. Create custom rules in CloudFormation Guard for each resource configuration. In the CI/CD pipeline, before the build stage, configure a Docker image to run the cfn-guard command on the CloudFormation template. Configure the CI/CD pipeline to publish a notification to the SNS topic if any issues are found.

C. Create an Amazon Simple Notification Service (Amazon SNS) topic and an Amazon Simple Queue Service (Amazon SQS) queue. Subscribe the security team's email addresses to the SNS topic. Create an Amazon S3 bucket in the shared services AWS account. Include an event notification to publish to the SQS queue when new objects are added to the S3 bucket. Require the developers to put their CloudFormation templates in the S3 bucket. Launch EC2 instances that automatically scale based on the SQS queue depth. Configure the EC2 instances to use CloudFormation Guard to scan the templates and deploy the templates if there are no issues. Configure the CI/CD pipeline to publish a notification to the SNS topic if any issues are found.

D. Create a centralized CloudFormation stack set that includes a standard set of resources that the developers can deploy in each AWS account. Configure each CloudFormation template to meet the security requirements. For any new resources or configurations, update the CloudFormation template and send the template to the security team for review. When the review is completed, add the new CloudFormation stack to the repository for the developers to use.

Correct Answer: *A*

Community vote distribution

B (79%) A (21%)

tulmegusto Highly Voted 2 months, 1 week ago
itexamstest.com
no disscusion b :)
upvoted 13 times

ET1857 Most Recent 1 day, 16 hours ago
Selected Answer: A
because of line "configure a Docker image to run the cfn-guard command on the CloudFormation template."

Option B should not be considered because its not a optimal solution
upvoted 1 times

Raphaello 2 weeks, 3 days ago
Selected Answer: B
You may use a lambda function to validate the syntax and semantics of CloudFormation templates.
But when it comes to validate to a compliance policy, CloudFormation Guard makes more sense.
Option B is correct.
upvoted 1 times

trashbox 2 months, 1 week ago
Exam on 2023-12-18
upvoted 1 times

Raphaello 2 months, 2 weeks ago

Command "aws cloudformation validate-template" checks only the syntax of cfn template.
I'd go with answer B, CloudFormation Guard, as it evaluates and validates cfn templates.

upvoted 1 times

Aamee 3 months ago

Selected Answer: B

Def. going with B as it doesn't ask to improve the delivery speed. Had that been the case then probably would have gone with option A IMO.

upvoted 1 times

Christina666 3 months, 1 week ago

Selected Answer: B

BBB The ask is to send notification and not affecting current delivery speed. So only need to add a validation step to send SNS

upvoted 1 times

Daniel76 3 months, 2 weeks ago

Selected Answer: A

Option A likely is utilizing cfn-guard as well but by Lambda/cli command, instead of creating custom rules for each resource config.More operationally efficient than B.
https://github.com/aws-cloudformation/cloudformation-guard

upvoted 1 times

[Removed] 3 months, 4 weeks ago

Selected Answer: B

validate-template is only for syntax and some semantic errors. cfn-guard is for policy compliance.

upvoted 1 times

lalee2 4 months ago

Selected Answer: B

CloudFormation Guard and SNS

upvoted 2 times

pupsik 4 months ago

Selected Answer: B

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html#:~:text=Validate%20templates%20for,non%2Dcompliant%20resources.

upvoted 2 times

leoaquinods 4 months ago

Selected Answer: A

most operationally efficient

upvoted 1 times

KR693 4 months ago

Option B.

The aws cloudformation validate-template command is designed to check only the syntax of your template.

Using Guard, you can write policy rules to validate any JSON- or YAML-formatted structured data against, including but not limited to AWS CloudFormation templates. Guard supports the entire spectrum of end-to-end evaluation of policy checks

upvoted 3 times

100fold 4 months, 1 week ago

Answer A. Most operationally efficient

upvoted 1 times

100fold 3 months, 3 weeks ago

Answer B. My original selection

upvoted 1 times

Lunga778 4 months, 1 week ago

answerer is A

upvoted 2 times

100fold 4 months, 1 week ago

Selected Answer: B

Answer B.
You can use cfn-guard automatically as part of a CI/CD pipeline to stop deployment of non-compliant resources.
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html

upvoted 3 times

100fold 4 months, 1 week ago

Changed to answer A

upvoted 1 times

100fold 3 months, 3 weeks ago

Original selection B

upvoted 1 times

Question #5 *Topic 1*

A company is migrating one of its legacy systems from an on-premises data center to AWS. The application server will run on AWS, but the database must remain in the on-premises data center for compliance reasons. The database is sensitive to network latency. Additionally, the data that travels between the on-premises data center and AWS must have IPsec encryption.
Which combination of AWS solutions will meet these requirements? (Choose two.)

A. AWS Site-to-Site VPN

B. AWS Direct Connect

C. AWS VPN CloudHub

D. VPC peering

E. NAT gateway

Correct Answer: *AB*

Community vote distribution

AB (100%)

usmanbaigmughal 2 months, 1 week ago

AB is the correct answer.

upvoted 1 times

Daniel76 3 months, 2 weeks ago

Selected Answer: AB

C. AWS VPN CloudHub - this is hub-and-spoke solution to connect multiple sites.
D. VPC peering - this is to connect cloud VPC to VPC.
E. NAT gateway - public or private NAT gateway? the public type is to access the internet, and a private NAT gateway is often used for communication between VPCs or between VPCs and Transit Gateway.

upvoted 3 times

[Removed] 3 months, 4 weeks ago

Selected Answer: AB

A and B

upvoted 1 times

lalee2 4 months ago

Selected Answer: AB

A and B provide IPsec encryption and minimized latency

upvoted 1 times

pupsik 4 months ago

Selected Answer: AB

DirectConnect for reliable connection and VPN for IPSec tunnel.

upvoted 1 times

KR693 4 months ago

A and B

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: AB

Answer AB
https://docs.aws.amazon.com/directconnect/latest/UserGuide/encryption-in-transit.html

upvoted 1 times

aragon_saa 4 months, 3 weeks ago

https://www.examtopics.com/discussions/amazon/view/88132-exam-aws-certified-security-specialty-topic-1-question-363/

upvoted 1 times

Question #6 *Topic 1*

A company has an application that uses dozens of Amazon DynamoDB tables to store data. Auditors find that the tables do not comply with the company's data protection policy.
The company's retention policy states that all data must be backed up twice each month: once at midnight on the 15th day of the month and again at midnight on the 25th day of the month. The company must retain the backups for 3 months.
Which combination of steps should a security engineer take to meet these requirements? (Choose two.)

A. Use the DynamoDB on-demand backup capability to create a backup plan. Configure a lifecycle policy to expire backups after 3 months.

B. Use AWS DataSync to create a backup plan. Add a backup rule that includes a retention period of 3 months.

C. Use AWS Backup to create a backup plan. Add a backup rule that includes a retention period of 3 months.

D. Set the backup frequency by using a cron schedule expression. Assign each DynamoDB table to the backup plan.

E. Set the backup frequency by using a rate schedule expression. Assign each DynamoDB table to the backup plan.

Correct Answer: *DC*

Community vote distribution

CD (100%)

trashbox 2 months, 1 week ago
Exam on 2023-12-18
upvoted 1 times

Raphaello 2 months, 2 weeks ago
A C
What happened to DynamoDB on-demand backup?
upvoted 2 times

Hisayuki 1 month, 3 weeks ago
DynamoDB's Backup function is only 0 days ~ 35 days. So, Backup from Outside like Lambda or AWS Backup is fine for this requirement.
upvoted 1 times

Raphaello 2 weeks, 4 days ago
Wrong!
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/BackupRestore.html
It explicitly says "You can use the DynamoDB on-demand backup capability to create full backups of your tables for long-term retention,"
LONG TERM RETENTION.
upvoted 2 times

Aamee 2 months, 3 weeks ago
Selected Answer: CD
AWS Backup and Cron Job schedule comb. makes sense...
upvoted 1 times

Christina666 3 months, 1 week ago
Selected Answer: CD
DynamoDB on-demand backup capability to create full backups of your tables for long-term retention and archival for regulatory compliance needs.
upvoted 3 times

Daniel76 3 months, 2 weeks ago
Selected Answer: CD
A. the DynamoDB on-demand backup capability creates full backup while the backup plan of 3 months is by AWS Backup.
B. AWS DataSync is for data discovery and migration, not backup DynamoDB.
E. Rate schedule expression is not suitable for fixed date scheduling.
upvoted 3 times

imymoco 4 months ago
C and D
upvoted 1 times

lalee2 4 months ago
Selected Answer: CD
C and D
upvoted 1 times

pupsik 4 months ago

Selected Answer: CD

C and D

upvoted 1 times

KR693 4 months ago

C and D

upvoted 1 times

AgboolaKun 4 months, 2 weeks ago

Selected Answer: CD

https://aws.amazon.com/blogs/database/set-up-scheduled-backups-for-amazon-dynamodb-using-aws-backup/

upvoted 3 times

PrabhuGr 4 months, 2 weeks ago

A and C are the answer.

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/BackupRestore.html

upvoted 2 times

Question #7 *Topic 1*

A company needs a security engineer to implement a scalable solution for multi-account authentication and authorization. The solution should not introduce additional user-managed architectural components. Native AWS features should be used as much as possible. The security engineer has set up AWS Organizations with all features activated and AWS IAM Identity Center (AWS Single Sign-On) enabled.
Which additional steps should the security engineer take to complete the task?

A. Use AD Connector to create users and groups for all employees that require access to AWS accounts. Assign AD Connector groups to AWS accounts and link to the IAM roles in accordance with the employees' job functions and access requirements. Instruct employees to access AWS accounts by using the AWS Directory Service user portal.

B. Use an IAM Identity Center default directory to create users and groups for all employees that require access to AWS accounts. Assign groups to AWS accounts and link to permission sets in accordance with the employees' job functions and access requirements. Instruct employees to access AWS accounts by using the IAM Identity Center user portal.

C. Use an IAM Identity Center default directory to create users and groups for all employees that require access to AWS accounts. Link IAM Identity Center groups to the IAM users present in all accounts to inherit existing permissions. Instruct employees to access AWS accounts by using the IAM Identity Center user portal.

D. Use AWS Directory Service for Microsoft Active Directory to create users and groups for all employees that require access to AWS accounts. Enable AWS Management Console access in the created directory and specify IAM Identity Center as a source of information for integrated accounts and permission sets. Instruct employees to access AWS accounts by using the AWS Directory Service user portal.

Correct Answer: *B*

Community vote distribution

B (100%)

Daniel76 Highly Voted 3 months, 2 weeks ago

Selected Answer: B

A. AD Connector only provides connectivity, not managing users.
C. IAM users should not need to be created in all accounts - results in admin overhead. assume role instead.
D. Letting end users DIY access in AWS Management Console, AWS Directory Service user portal is not a good idea.

upvoted 5 times

Raphaello Most Recent 4 days, 3 hours ago

Selected Answer: B

Keywords: "Native AWS features should be used as much as possible"
Therefore choose to use Identity Center's own directory, plus there is no mention to on-prem AD and hence AD connector does not make sense.
For the same reason, using AWS Directory Service - Managed MS AD does not fit with native AWS feature.

Option B is the right answer.

upvoted 1 times

lalee2 4 months ago

Selected Answer: B

https://aws.amazon.com/ko/iam/identity-center/faqs/

upvoted 2 times

pupsik 4 months ago

Selected Answer: B

Normally we would use AD Connector to connect to on-premises AD. But option A doesn't come close to that. Hence option B.

upvoted 4 times

KR693 4 months ago

Option B

upvoted 3 times

Question #8 *Topic 1*

A company has deployed Amazon GuardDuty and now wants to implement automation for potential threats. The company has decided to start with RDP brute force attacks that come from Amazon EC2 instances in the company's AWS environment. A security engineer needs to implement a solution that blocks the detected communication from a suspicious instance until investigation and potential remediation can occur.
Which solution will meet these requirements?

A. Configure GuardDuty to send the event to an Amazon Kinesis data stream. Process the event with an Amazon Kinesis Data Analytics for Apache Flink application that sends a notification to the company through Amazon Simple Notification Service (Amazon SNS). Add rules to the network ACL to block traffic to and from the suspicious instance.

B. Configure GuardDuty to send the event to Amazon EventBridge. Deploy an AWS WAF web ACL. Process the event with an AWS Lambda function that sends a notification to the company through Amazon Simple Notification Service (Amazon SNS) and adds a web ACL rule to block traffic to and from the suspicious instance.

C. Enable AWS Security Hub to ingest GuardDuty findings and send the event to Amazon EventBridge. Deploy AWS Network Firewall. Process the event with an AWS Lambda function that adds a rule to a Network Firewall firewall policy to block traffic to and from the suspicious instance.

D. Enable AWS Security Hub to ingest GuardDuty findings. Configure an Amazon Kinesis data stream as an event destination for Security Hub. Process the event with an AWS Lambda function that replaces the security group of the suspicious instance with a security group that does not allow any connections.

Correct Answer: *A*

Community vote distribution

C (74%) D (26%)

Daniel76 Highly Voted 3 months, 2 weeks ago

Selected Answer: C

Let Guardduty detections be sent to Security Hub as findings is a simple and elegant way.
https://docs.aws.amazon.com/guardduty/latest/ug/securityhub-integration.html

Use eventbridge to respond by invoke Lambda. Amazon Kinesis data stream not needed.
https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-cloudwatch-events.html

Suggest to only block specific port 389 against thse suspicious EC2 instance instead of isolate it in a security group, to minimize the impact while it has not been verified as a confirmed attack.

upvoted 5 times

Raphaello Most Recent 2 weeks, 3 days ago

Selected Answer: C

1. No point to use Kinesis Data Stream/analytics/Apache flink to stream and process event.
2. Neither WAF nor NACL is an effective solution to the mentioned case
3. GuardDuty findings can be sent directly to Amazon EventBridge to trigger action, but deploying SecurityHub is not entirely wrong.
4. AWS Network Firewall is better suited to block suspicious instances.

Option C is the correct answer.

upvoted 1 times

awssecuritynewbie 1 month ago

Selected Answer: C

I would go with C, as option D will block any connection to the Ec2 machine, which is not what you want, and security groups are easier and at the endpoint level.

upvoted 1 times

mynickc 1 month ago

Selected Answer: C

Here is some basics: WAF protects the port 443 / 80. RDP is different port and nothing to do with Layer 7 nor WAF

upvoted 1 times

happy34 1 month, 2 weeks ago

D is the answer. we need identify the best method - tech and cost. implied. WAF is layer 7 prevention . FW is layer 3 - 7. WEB ACL can prevent layer 7. RDP is mostly Layer 7. password guessing etc
https://repost.aws/knowledge-center/waf-prevent-brute-force-attacks

upvoted 1 times

brpjp 1 month, 3 weeks ago

Hello, correct my understanding agree with answer C.

upvoted 1 times

brpjp 1 month, 3 weeks ago

When GuardDuty is there, do not understand what is requirement to integrate Security Hub.

upvoted 1 times

brpjp 1 month, 3 weeks ago

Answer B correct. Requested first scenario of RDP brute force attack. Neither NACL, Network Firewall, and Security Group support to block, only WAF help to block traffic based on pattern.

upvoted 2 times

3633f8f 2 months, 1 week ago

Selected Answer: C

C is the answer

upvoted 1 times

tulmegusto 2 months, 1 week ago

Selected Answer: C

itexamstest.com

no disscusion c :)

upvoted 1 times

3633f8f 2 months, 1 week ago

Selected Answer: D

To isolate there is nothing more powerful that an ACL at subnet level, which immediately denies traffic in any direction. Wishing to automate, there is no choice to use ACL, as you do not know the exact IP of the source is attacking, thus, you do apply security group restiction.

The need of Kinesys Data Streams is to process real-time events while happening.
A firewall you do not usually automate at his has complex features needs to be set via IaC or console.

upvoted 2 times

3633f8f 2 months, 1 week ago

Correcting as RDP handles directly in layer 3. C

upvoted 1 times

Raphaello 2 months, 2 weeks ago

Selected Answer: C

C
SecurityGroup is a simpler way of isolating a suspicious instance, unlike Network Firewall that is a paid service.
EventBridge is needed to relay events to Kinesis Data Stream. At that point, what is the need to Kinesis Data Stream? Lambda function could be invoked directly from EventBridge.
For that, I'd go with C.

upvoted 2 times

Raphaello 2 months, 2 weeks ago

C
SecurityGroup is a simpler way of isolating a suspicious instance, unlike Network Firewall that is a paid service.
EventBridge is needed to relay events to Kinesis Data Stream. At that point, what is the need to Kinesis Data Stream? Lambda function could be invoked directly from EventBridge.
For that, I'd go with C.

upvoted 1 times

WeepingMaplte 2 months, 2 weeks ago

AWS Network Firewall is a better option unless the question wants the most cost-effective method.
https://docs.aws.amazon.com/network-firewall/latest/developerguide/rule-group-stateful-creating.html#:~:text=Stateful%20actions.-,To%20define%20IP%20sets%20and%20ports%20as%20variables%20that%20you%20can,variables%20and%20values%20for%20IP%20set%20variables%20and%20Port%20variables.,-To%20add%20one

upvoted 1 times

Aamee 3 months ago

Selected Answer: C

Would go with C since it has asked specifically for automating the security findings... and that's where Security Hub comes into play with EventBridge combination..

upvoted 1 times

marlonchin 3 months ago

Why network firewall can't block ips in its own security group: I think I will also go with C

upvoted 1 times

awssecuritynewbie 3 months ago

Selected Answer: D

so people that are saying to use option C, listen up .

you are using " web ACL" to block traffic? web ACL is only for HTTP/S so it would note be blocking port 3389... so it cannot be that! the best option so far would be D.

upvoted 1 times

mav3r1ck 2 months, 3 weeks ago

Option C is NOT webACL. It is using AWS Network Firewall.

upvoted 3 times

Question #9 *Topic 1*

A company has an AWS account that hosts a production application. The company receives an email notification that Amazon GuardDuty has detected an Impact:IAMUser/AnomalousBehavior finding in the account. A security engineer needs to run the investigation playbook for this security incident and must collect and analyze the information without affecting the application.
Which solution will meet these requirements MOST quickly?

A. Log in to the AWS account by using read-only credentials. Review the GuardDuty finding for details about the IAM credentials that were used. Use the IAM console to add a DenyAll policy to the IAM principal.

B. Log in to the AWS account by using read-only credentials. Review the GuardDuty finding to determine which API calls initiated the finding. Use Amazon Detective to review the API calls in context.

C. Log in to the AWS account by using administrator credentials. Review the GuardDuty finding for details about the IAM credentials that were used. Use the IAM console to add a DenyAll policy to the IAM principal.

D. Log in to the AWS account by using read-only credentials. Review the GuardDuty finding to determine which API calls initiated the finding. Use AWS CloudTrail Insights and AWS CloudTrail Lake to review the API calls in context.

Correct Answer: *B*

Community vote distribution

B (100%)

pupsik Highly Voted 4 months ago

Selected Answer: B

https://aws.amazon.com/blogs/security/how-you-can-use-amazon-guardduty-to-detect-suspicious-activity-within-your-aws-account/#:~:text=Start%20an%20investigation%20with%20Amazon%20Detective

upvoted 5 times

Raphaello Most Recent 2 weeks, 3 days ago

Selected Answer: B

Using CloudTrail (Insights & Lake) is not entirely wrong for the the aforementioned case, however, since the ask is to analyze the events "QUICKLY", I think Detective provides a good integration with GuardDuty to correlate data and analyze them.

I would go with B only for this.."quickly"!

upvoted 1 times

Aamee 2 months, 3 weeks ago

Selected Answer: B

Option B since Detective is integrated with GuardDuty by native... contrast to option D where Insights and Lake are NA to GuardDuty..

upvoted 1 times

Daniel76 3 months, 1 week ago

Selected Answer: B

A. Read-only login should not allow user to add DenyAllPolicy.
C. Add DenyAllPolicy to the principal is very intrusive intervention.
D. Use AWS CloudTrail Insights and AWS CloudTrail Lake are not integrated with GuardDuty (as opposed to AWS Detective) hence it might lack correlationship

upvoted 1 times

lalee2 4 months ago

Selected Answer: B

'Qs says collect and analyze the info' read-only credential is enough. Detective provides API activities.

upvoted 2 times

KR693 4 months ago

Option B

upvoted 1 times

Lunga778 4 months, 1 week ago

correct answer is be
https://aws.amazon.com/blogs/aws/new-aws-cloudtrail-lake-supports-ingesting-activity-events-from-non-aws-sources/

https://aws.amazon.com/about-aws/whats-new/2019/11/aws-cloudtrail-announces-cloudtrail-insights/

upvoted 1 times

Lunga778 4 months, 1 week ago

i mean is D

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: B

Answer B

upvoted 1 times

AgboolaKun 4 months, 2 weeks ago

Selected Answer: B

https://aws.amazon.com/blogs/security/how-you-can-use-amazon-guardduty-to-detect-suspicious-activity-within-your-aws-account/

upvoted 2 times

Question #10 *Topic 1*

Company A has an AWS account that is named Account A. Company A recently acquired Company B, which has an AWS account that is named Account B. Company B stores its files in an Amazon S3 bucket. The administrators need to give a user from Account A full access to the S3 bucket in Account B.
After the administrators adjust the IAM permissions for the user in Account A to access the S3 bucket in Account B, the user still cannot access any files in the S3 bucket.
Which solution will resolve this issue?

A. In Account B, create a bucket ACL to allow the user from Account A to access the S3 bucket in Account B.

B. In Account B, create an object ACL to allow the user from Account A to access all the objects in the S3 bucket in Account B.

C. In Account B, create a bucket policy to allow the user from Account A to access the S3 bucket in Account B.

D. In Account B, create a user policy to allow the user from Account A to access the S3 bucket in Account B.

Correct Answer: *A*

Community vote distribution

C (100%)

Raphaello 2 weeks, 3 days ago

Selected Answer: C
Bucket POLICY.
upvoted 1 times

trashbox 2 months, 1 week ago
Exam on 2023-12-18
upvoted 1 times

Raphaello 2 months, 2 weeks ago
Selected Answer: C
S3 bucket policy should be edited to allow cross-account access.
upvoted 1 times

raj0011 3 months ago
why they correct answer A
upvoted 1 times

Daniel76 3 months, 1 week ago

Selected Answer: C
https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-walkthroughs-managing-access-example2.html
upvoted 1 times

[Removed] 3 months, 4 weeks ago

Selected Answer: C
It's C
upvoted 1 times

lalee2 4 months ago
it is cross-account, requires S3 bucket policy update
upvoted 2 times

pupsik 4 months ago

Selected Answer: C
For cross-account access, got to update S3 bucket policy to allow principal from other account to access it.
upvoted 4 times

KR693 4 months ago
Option C
upvoted 2 times

100fold 4 months, 1 week ago

Selected Answer: C
Answer C
upvoted 2 times

aragon_saa 4 months, 3 weeks ago

https://www.examtopics.com/discussions/amazon/view/88380-exam-aws-certified-security-specialty-topic-1-question-423/

upvoted 4 times

Question #11 *Topic 1*

A company wants to receive an email notification about critical findings in AWS Security Hub. The company does not have an existing architecture that supports this functionality.
Which solution will meet the requirement?

A. Create an AWS Lambda function to identify critical Security Hub findings. Create an Amazon Simple Notification Service (Amazon SNS) topic as the target of the Lambda function. Subscribe an email endpoint to the SNS topic to receive published messages.

B. Create an Amazon Kinesis Data Firehose delivery stream. Integrate the delivery stream with Amazon EventBridge. Create an EventBridge rule that has a filter to detect critical Security Hub findings. Configure the delivery stream to send the findings to an email address.

C. Create an Amazon EventBridge rule to detect critical Security Hub findings. Create an Amazon Simple Notification Service (Amazon SNS) topic as the target of the EventBridge rule. Subscribe an email endpoint to the SNS topic to receive published messages.

D. Create an Amazon EventBridge rule to detect critical Security Hub findings. Create an Amazon Simple Email Service (Amazon SES) topic as the target of the EventBridge rule. Use the Amazon SES API to format the message. Choose an email address to be the recipient of the message.

Correct Answer: *D*

Community vote distribution

C (100%)

Raphaello 2 weeks, 3 days ago
SecurityHub >>EventBridge >>SNS.

{
"source": ["aws.securityhub"],
"detail-type": ["Security Hub Findings - Imported"],
"detail": {
"findings": {"Severity": {"Label": ["Critical"]}}
}
}
upvoted 2 times

trashbox 2 months, 1 week ago
Exam on 2023-12-18
upvoted 1 times

3633f8f 2 months, 1 week ago
Selected Answer: C
Marked D is defenitely wrong
upvoted 1 times

Raphaello 2 months, 2 weeks ago
C
SES? Seriously?
upvoted 1 times

Daniel76 3 months, 1 week ago
Selected Answer: C
To filter for critical only finding:

https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-cwe-all-findings.html
upvoted 2 times

YR4591 3 months, 1 week ago
Selected Answer: C
C is right
securityhub > eventbridge > sns
upvoted 1 times

Karamen 3 months, 3 weeks ago
C is right. confirmed
upvoted 1 times

[Removed] 3 months, 4 weeks ago
Selected Answer: C

C is right

upvoted 1 times

lalee2 4 months ago

Selected Answer: C

EventBridge -> SNS is right

upvoted 1 times

pupsik 4 months ago

Selected Answer: C

EventBridge Rule -> SNS -> Email delivery

upvoted 1 times

KR693 4 months ago

Option C

upvoted 1 times

jabilrn 4 months, 1 week ago

I think C is right.
I dont believe SES can be the target for Eventbridge

upvoted 1 times

Question #12 *Topic 1*

An international company has established a new business entity in South Korea. The company also has established a new AWS account to contain the workload for the South Korean region. The company has set up the workload in the new account in the ap-northeast-2 Region. The workload consists of three Auto Scaling groups of Amazon EC2 instances. All workloads that operate in this Region must keep system logs and application logs for 7 years.
A security engineer must implement a solution to ensure that no logging data is lost for each instance during scaling activities. The solution also must keep the logs for only the required period of 7 years.
Which combination of steps should the security engineer take to meet these requirements? (Choose three.)

A. Ensure that the Amazon CloudWatch agent is installed on all the EC2 instances that the Auto Scaling groups launch. Generate a CloudWatch agent configuration file to forward the required logs to Amazon CloudWatch Logs.

B. Set the log retention for desired log groups to 7 years.

C. Attach an IAM role to the launch configuration or launch template that the Auto Scaling groups use. Configure the role to provide the necessary permissions to forward logs to Amazon CloudWatch Logs.

D. Attach an IAM role to the launch configuration or launch template that the Auto Scaling groups use. Configure the role to provide the necessary permissions to forward logs to Amazon S3.

E. Ensure that a log forwarding application is installed on all the EC2 instances that the Auto Scaling groups launch. Configure the log forwarding application to periodically bundle the logs and forward the logs to Amazon S3.

F. Configure an Amazon S3 Lifecycle policy on the target S3 bucket to expire objects after 7 years.

Correct Answer: *ABC*

Community vote distribution

ABC (83%) ACF (17%)

Raphaello 2 weeks, 3 days ago

Selected Answer: ABC

ABC.
EC2 (with a role allowing sending events) >> CloudWatch agent >> CloudWatch Logs >> CloudWatch Logs retention period

upvoted 2 times

Daniel76 3 months, 1 week ago

Selected Answer: ACF

As the log data for 7 years will be expensive, use AWS S3 Lifecycle Management to transfer data to lower cost storage class will be more cost effective solution.
https://medium.com/avmconsulting-blog/aws-s3-lifecycle-management-1ed2f67c3b73

upvoted 1 times

mav3r1ck 2 months, 3 weeks ago

I would go for ACF if the asked is "COST-EFFECTIVE" solution. But leaning to ABF, as Cloudwatch logs support up to 10yrs of retention as well. Feel free to disagree if you think I'm wrong. https://docs.aws.amazon.com/managedservices/latest/userguide/log-customize-retention.html

upvoted 3 times

Daniel76 1 month, 3 weeks ago

Agree it should not be ACF but ABC. ACF does not explain how cloudwatch log end s up in s3. (seems that it requires a lambda function to automate)
In fact, if S3 is the chosen path then it can only be DEF for consistency. But this combination assume that s3 bucket policy has been configured and the log forwarding application configured can reliably send all logs data without losing any.

upvoted 1 times

Karamen 3 months, 3 weeks ago

ABC

there isn't good option to forwarding log from EC2 to S3 bucket.

upvoted 3 times

lalee2 4 months ago

Selected Answer: ABC

CloudWatch agent -> CloudWatch Logs, IAM role to launch template -> CloudWatch Logs

upvoted 1 times

pupsik 4 months ago

Selected Answer: ABC

ABC it is.

upvoted 1 times

KR693 4 months ago

A, B and C

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: ABC

Answer ABC

upvoted 1 times

aragon_saa 4 months, 3 weeks ago

https://www.examtopics.com/discussions/amazon/view/89514-exam-aws-certified-security-specialty-topic-1-question-451/

upvoted 2 times

Question #13 *Topic 1*

A security engineer is designing an IAM policy to protect AWS API operations. The policy must enforce multi-factor authentication (MFA) for IAM users to access certain services in the AWS production account. Each session must remain valid for only 2 hours. The current version of the IAM policy is as follows:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeInstances",
            "ec2:StopInstances",
            "ec2:TerminateInstances"
        ],
        "Resource": ["*"]
    }]
}
```

Which combination of conditions must the security engineer add to the IAM policy to meet these requirements? (Choose two.)

A. "Bool": {"aws:MultiFactorAuthPresent": "true"}

B. "Bool": {"aws:MultiFactorAuthPresent": "false"}

C. "NumericLessThan": {"aws:MultiFactorAuthAge": "7200"}

D. "NumericGreaterThan": {"aws:MultiFactorAuthAge": "7200"}

E. "NumericLessThan": {"MaxSessionDuration": "7200"}

Correct Answer: *AD*

Community vote distribution

AC (100%)

kk2000 Highly Voted 4 months, 3 weeks ago

Correct Answer is AC

upvoted 6 times

PareshBPatel Most Recent 2 weeks, 2 days ago

C. "NumericLessThan": {"aws:MultiFactorAuthAge": "7200"}

This condition ensures that the action is allowed only if the MFA session age is less than 7200 seconds (2 hours), meaning it enforces the requirement that each MFA session remains valid for only 2 hours. This is a correct choice as it directly addresses the session validity requirement.
D. "NumericGreaterThan": {"aws:MultiFactorAuthAge": "7200"}

This condition would allow the action only if the MFA session age is greater than 7200 seconds, which is contrary to the requirement. Therefore, this option is incorrect.

upvoted 1 times

Raphaello 2 weeks, 3 days ago

Selected Answer: AC

AC ofc

upvoted 1 times

mtzanida 1 month, 1 week ago

Selected Answer: AC

A and C

upvoted 1 times

Raphaello 2 months, 2 weeks ago

AC
Action is ALLOW..as long as the auth. age is LESS 7200 seconds.

upvoted 1 times

Daniel76 3 months, 1 week ago

Selected Answer: AC

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html

upvoted 2 times

kejam 3 months, 3 weeks ago

A and C
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html#MFAProtectedAPI-overview

upvoted 3 times

lalee2 4 months ago

Selected Answer: AC

A and C

upvoted 1 times

denied 4 months ago

Selected Answer: AC

A and C

upvoted 2 times

KR693 4 months ago

A and C

upvoted 2 times

Question #14 *Topic 1*

A company uses AWS Organizations and has production workloads across multiple AWS accounts. A security engineer needs to design a solution that will proactively monitor for suspicious behavior across all the accounts that contain production workloads.
The solution must automate remediation of incidents across the production accounts. The solution also must publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic when a critical security finding is detected. In addition, the solution must send all security incident logs to a dedicated account.
Which solution will meet these requirements?

A. Activate Amazon GuardDuty in each production account. In a dedicated logging account, aggregate all GuardDuty logs from each production account. Remediate incidents by configuring GuardDuty to directly invoke an AWS Lambda function. Configure the Lambda function to also publish notifications to the SNS topic.

B. Activate AWS Security Hub in each production account. In a dedicated logging account, aggregate all Security Hub findings from each production account. Remediate incidents by using AWS Config and AWS Systems Manager. Configure Systems Manager to also publish notifications to the SNS topic.

C. Activate Amazon GuardDuty in each production account. In a dedicated logging account, aggregate all GuardDuty logs from each production account. Remediate incidents by using Amazon EventBridge to invoke a custom AWS Lambda function from the GuardDuty findings. Configure the Lambda function to also publish notifications to the SNS topic.

D. Activate AWS Security Hub in each production account. In a dedicated logging account, aggregate all Security Hub findings from each production account. Remediate incidents by using Amazon EventBridge to invoke a custom AWS Lambda function from the Security Hub findings. Configure the Lambda function to also publish notifications to the SNS topic.

Correct Answer: *D*

Community vote distribution

C (100%)

Raphaello 2 months, 2 weeks ago
Best answer is C
One would not need SecurityHub to launch a response to GuardDuty finding.
SecurityHub is security posture management tool, but without it GuardDuty can still responds to findings.

https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings_cloudwatch.html
upvoted 1 times

Daniel76 3 months, 1 week ago
Selected Answer: C
Security Hub by itself does not detect suspicious activity, but GuardDuty.
Eventbridge rule is required to trigger remediation actions and SNS topic.
upvoted 2 times

[Removed] 3 months, 4 weeks ago
Selected Answer: C
SecurityHub checks posture. GuardDuty monitors for malicious activity.
upvoted 1 times

[Removed] 3 months, 4 weeks ago
It's C.
SecurityHub checks posture. GuardDuty monitors for malicious activity.
upvoted 1 times

lalee2 4 months ago
Selected Answer: C
Option C responds to all requirements; automate remediation, notification via SNS, send logs to a dedicated account
upvoted 1 times

bhui 4 months ago
I would say it is C as Guardduty must be turned on even for the security hub options. Also you can aggregate GuardDuty Findings and trigger Events.
https://aws.amazon.com/blogs/security/how-to-manage-amazon-guardduty-security-findings-across-multiple-accounts/
https://repost.aws/knowledge-center/guardduty-eventbridge-sns-rule
upvoted 3 times

pupsik 4 months ago

Selected Answer: C

Agree, it is C

upvoted 1 times

KR693 4 months ago

Option C

upvoted 1 times

Sumi81 4 months ago

Answer is C

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: C

Answer C

https://www.youtube.com/watch?v=RGNMkhaT_GY

upvoted 2 times

Question #15 *Topic 1*

A company is designing a multi-account structure for its development teams. The company is using AWS Organizations and AWS IAM Identity Center (AWS Single Sign-On). The company must implement a solution so that the development teams can use only specific AWS Regions and so that each AWS account allows access to only specific AWS services.
Which solution will meet these requirements with the LEAST operational overhead?

A. Use IAM Identity Center to set up service-linked roles with IAM policy statements that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.

B. Deactivate AWS Security Token Service (AWS STS) in Regions that the developers are not allowed to use.

C. Create SCPs that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.

D. For each AWS account, create tailored identity-based policies for IAM Identity Center. Use statements that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.

Correct Answer: *C*

Community vote distribution

C (86%) 14%

awssecuritynewbie 1 week, 1 day ago
you cannot use "NOTACTION" with SCP though? Anyone can help?
upvoted 1 times

Raphaello 2 weeks, 3 days ago
Selected Answer: C
SCP to allow certain services in certain regions for specific accounts.
upvoted 1 times

Raphaello 1 week, 1 day ago
As explained here https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_syntax.html#scp-elements-table "Condition", "Resource", and "NotAction" elements can only be used with "Deny" effect, but answer C says "to allow access to only the Regions and services that are needed" as the ultimate outcome, not by the meaning with "Allow" effect.

It tries to trick you into thinking "those elements cannot be used with "Allow", then not C" !

Still believe C is the best answer here.
upvoted 1 times

NoCrapEva 2 weeks, 3 days ago
Selected Answer: C
SCP is the GOTO solution for multiple accounts in AWS Organisations.
upvoted 1 times

habros 3 weeks, 2 days ago
Selected Answer: C
C. If AWS organizations is enabled, why not take advantage of region deny feature? SCP is the actual mechanism to enforce this rule!
upvoted 1 times

mynickc 1 month ago
Selected Answer: A
C is wrong becoz notaction, resource & condition can support deny only.
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_syntax.html
upvoted 1 times

Sab31 1 month, 3 weeks ago
C seems a good option but can someone share if SCPs can have "NotAction" element?
upvoted 1 times

Raphaello 2 months, 2 weeks ago
Correct answer is C.
SCP to control which organization node can operate on which region(s).
upvoted 1 times

Daniel76 3 months, 1 week ago

Selected Answer: C

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_general.html#example-scp-deny-region

upvoted 1 times

lalee2 4 months ago

Selected Answer: C

Under Organization SCP is the least operational overhead.

upvoted 1 times

KR693 4 months ago

Option C

upvoted 1 times

Sumi81 4 months ago

C is right

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: C

Agree answer C

upvoted 1 times

aragon_saa 4 months, 3 weeks ago

https://www.examtopics.com/discussions/amazon/view/88434-exam-aws-certified-security-specialty-topic-1-question-431/

upvoted 2 times

Question #16 *Topic 1*

A company is developing an ecommerce application. The application uses Amazon EC2 instances and an Amazon RDS MySQL database. For compliance reasons, data must be secured in transit and at rest. The company needs a solution that minimizes operational overhead and minimizes cost.
Which solution meets these requirements?

A. Use TLS certificates from AWS Certificate Manager (ACM) with an Application Load Balancer. Deploy self-signed certificates on the EC2 instances. Ensure that the database client software uses a TLS connection to Amazon RDS. Enable encryption of the RDS DB instance. Enable encryption on the Amazon Elastic Block Store (Amazon EBS) volumes that support the EC2 instances.

B. Use TLS certificates from a third-party vendor with an Application Load Balancer. Install the same certificates on the EC2 instances. Ensure that the database client software uses a TLS connection to Amazon RDS. Use AWS Secrets Manager for client-side encryption of application data.

C. Use AWS CloudHSM to generate TLS certificates for the EC2 instances. Install the TLS certificates on the EC2 instances. Ensure that the database client software uses a TLS connection to Amazon RDS. Use the encryption keys from CloudHSM for client-side encryption of application data.

D. Use Amazon CloudFront with AWS WAF. Send HTTP connections to the origin EC2 instances. Ensure that the database client software uses a TLS connection to Amazon RDS. Use AWS Key Management Service (AWS KMS) for client-side encryption of application data before the data is stored in the RDS database.

Correct Answer: *A*

Community vote distribution

A (100%)

Raphaello 2 weeks, 3 days ago

Selected Answer: A

A..ofc!

upvoted 1 times

awssecuritynewbie 4 weeks ago

Selected Answer: A

Non of them talk about the encryption at rest for the EBS apart from Option A

upvoted 1 times

3633f8f 2 months, 1 week ago

Selected Answer: A

TLS In-Flight encryption is core funcitionality of ACM. Others are invalidated based on this.

upvoted 1 times

Daniel76 3 months, 1 week ago

Selected Answer: A

Only A address data encryption at rest at RDS and EBS and is the most cost-effective and efficient method.
TLS certificates from a third-party vendor or generated by CloudHSM is unnecessarily increase cost and ops overhead.
CloudFront with WAF is irrelevant to the requirement.

upvoted 2 times

[Removed] 3 months, 4 weeks ago

Selected Answer: A

Answer A

upvoted 1 times

lalee2 4 months ago

Selected Answer: A

Option A talks about ACM which is encryption in transit

upvoted 1 times

pupsik 4 months ago

Selected Answer: A

Option A

upvoted 1 times

KR693 4 months ago

Option A

upvoted 1 times

Sumi81 4 months ago

A. No other solution talks about encryption at rest

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: A

Agree answer A.
TLS certificates from (ACM) secures data in transit

upvoted 1 times

aragon_saa 4 months, 3 weeks ago

https://www.examtopics.com/discussions/amazon/view/60895-exam-aws-certified-security-specialty-topic-1-question-265/

upvoted 2 times

Question #17 *Topic 1*

A security engineer is working with a company to design an ecommerce application. The application will run on Amazon EC2 instances that run in an Auto Scaling group behind an Application Load Balancer (ALB). The application will use an Amazon RDS DB instance for its database.
The only required connectivity from the internet is for HTTP and HTTPS traffic to the application. The application must communicate with an external payment provider that allows traffic only from a preconfigured allow list of IP addresses. The company must ensure that communications with the external payment provider are not interrupted as the environment scales.
Which combination of actions should the security engineer recommend to meet these requirements? (Choose three.)

A. Deploy a NAT gateway in each private subnet for every Availability Zone that is in use.

B. Place the DB instance in a public subnet.

C. Place the DB instance in a private subnet.

D. Configure the Auto Scaling group to place the EC2 instances in a public subnet.

E. Configure the Auto Scaling group to place the EC2 instances in a private subnet.

F. Deploy the ALB in a private subnet.

Correct Answer: *DEF*

Community vote distribution

ACE (100%)

Raphaello 2 months, 2 weeks ago

Keyword: " preconfigured allow list of IP addresses"
However, the question missed an important detail alongside these keywords..that the communication has to be routed to a VPN and through a virtual private gateway (VGW).
That's the only reason you can place NAT GW in a private subnet.
Without that piece of detail, placing NAT GW seems unreasonable.
Poorly written question, but if you considered that, A C E would make sense.

https://docs.aws.amazon.com/vpc/latest/userguide/nat-gateway-scenarios.html#private-nat-allowed-range

upvoted 2 times

Daniel76 3 months, 1 week ago

Selected Answer: ACE

C and E are definitely correct.
A is confusing because NAT gateway should be created in public subnets. It should be referring to created *for each private subnets instead.
F is wrong because ALB should be in public subnet.

upvoted 2 times

confusedyeti69 2 months, 2 weeks ago

There is private NAT gateway as well, but I'm not sure if private NAT gateway is deployed to public or private subnet.
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
Private – Instances in private subnets can connect to other VPCs or your on-premises network through a private NAT gateway. You can route traffic from the NAT gateway through a transit gateway or a virtual private gateway. You cannot associate an elastic IP address with a private NAT gateway. You can attach an internet gateway to a VPC with a private NAT gateway, but if you route traffic from the private NAT gateway to the internet gateway, the internet gateway drops the traffic.

upvoted 1 times

[Removed] 3 months, 4 weeks ago

Selected Answer: ACE

A,C and E, except that NAT gateways are created in public subnets, so that private subnets can reach the Internet. Option A is worded wrong.

upvoted 3 times

lalee2 4 months ago

Selected Answer: ACE

A, C, E

upvoted 2 times

KR693 4 months ago

A, C and E

upvoted 2 times

Sumi81 4 months ago

I think its ACD

upvoted 3 times

100fold 4 months, 1 week ago

Selected Answer: ACE

Answer ACE

upvoted 3 times

aragon_saa 4 months, 3 weeks ago

https://www.examtopics.com/discussions/amazon/view/69095-exam-aws-certified-security-specialty-topic-1-question-299/

upvoted 4 times

Question #18 *Topic 1*

A company uses several AWS CloudFormation stacks to handle the deployment of a suite of applications. The leader of the company's application development team notices that the stack deployments fail with permission errors when some team members try to deploy the stacks. However, other team members can deploy the stacks successfully.
The team members access the account by assuming a role that has a specific set of permissions that are necessary for the job responsibilities of the team members. All team members have permissions to perform operations on the stacks.
Which combination of steps will ensure consistent deployment of the stacks MOST securely? (Choose three.)

A. Create a service role that has a composite principal that contains each service that needs the necessary permissions. Configure the role to allow the sts:AssumeRole action.

B. Create a service role that has cloudformation.amazonaws.com as the service principal. Configure the role to allow the sts:AssumeRole action.

C. For each required set of permissions, add a separate policy to the role to allow those permissions. Add the ARN of each CloudFormation stack in the resource field of each policy.

D. For each required set of permissions, add a separate policy to the role to allow those permissions. Add the ARN of each service that needs the permissions in the resource field of the corresponding policy.

E. Update each stack to use the service role.

F Add a policy to each member role to allow the iam:PassRole action. Set the policy's resource field to the ARN of the service role.

Correct Answer: *DEA*

Community vote distribution

BD (67%) BDE (33%)

PareshBPatel 2 weeks, 1 day ago

BEF are the correct selection
Thought to consistent deployment of CloudFormation stacks would actually be
B. Create a service role that has cloudformation.amazonaws.com as the service principal. Configure the role to allow the sts:AssumeRole action.
E. Update each stack to use the service role.
F. Add a policy to each member role to allow the iam:PassRole action. Set the policy's resource field to the ARN of the service role.
These steps ensure that CloudFormation has the necessary permissions through a service role designed specifically for it (B), that each stack is configured to use this service role for deployments (E), and that users have the permission to pass this role to CloudFormation (F), aligning with best practices for security and consistency.

upvoted 1 times

Raphaello 2 weeks, 3 days ago

Selected Answer: BDE

BDE
Create a service role to be used by CloudFormation.
For each service to be used by the CF stack, create the associated set of permissions.
Assign the service role to the stack.

The question does not feel right though, since it mentions all user assume an IAM role to access the account, therefore the stack they launch should use the permissions given to that IAM role, therefore the result should be the same for all users either (they don't launch the stack using their individual IAM users).

upvoted 1 times

Raphaello 1 week ago

Ok, looking again at the options of this question, option D is a bit tricky.
Yes you need to create permissions to CF service role, but there's nothing like "ARN of each service" to be added to the resource field. ARN's belong to resources not services, and in CF service role, resource element usually takes "*"; but even if you want to specify a resource it will be something like (arn:aws:s3:::my_bucket/*) NOT ARN OF EACH SERVICE!
ARN <--> Resource..not service.

For that, I would go with BEF.
"F" (users being able to iam:PassRole) is important and the option is worded correctly.
D is not worded correctly, as it starts with a correct part, but ended it with bogus!

BEF.

upvoted 1 times

mynickc 4 weeks, 1 day ago

I took the exam today (Jan/28) and the choices E & F are two separate as per this question. In some of the comments, it was mentioned that E&F are considered as one choice.

upvoted 3 times

brpjp 1 month, 3 weeks ago

Yes, Correct answer is B D F, based on numbers of linked already provided and passrole from ChatGpt.

upvoted 1 times

WeepingMaplte 2 months, 1 week ago

Selected Answer: BD

Ans: B D F.
In Cloud formation, you select the required role during a new creation. The team members will deploy using the new role. updating the current stacks is not a priority as compared to IAM:PassRole.

upvoted 2 times

Raphaello 2 months, 2 weeks ago

B D E

To be able to update each stack to use the service role (E), user needs to be able to pass the role using iam:PassRole (F).
But it is done once.

I would go with E along side B & D.

upvoted 2 times

vincentsr7 2 months, 2 weeks ago

why not A , dont we need a composite principal

upvoted 1 times

Daniel76 3 months, 1 week ago

Selected Answer: BD

B,D and F.
https://blog.awsfundamentals.com/aws-cloudformation-execution-permissions

upvoted 1 times

Daniel76 1 month, 3 weeks ago

Consider this article to justify F: passrole is needed so that team member who has limited permission by their own role, can run the stack using service role's permissions.
https://medium.com/@sapna.mandhare/demystifying-iam-passrole-permission-d62a2dc69778

upvoted 1 times

Ciara123456 3 months, 2 weeks ago

BDF, https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-iam-servicerole.html

upvoted 3 times

Lunga778 3 months, 2 weeks ago

B D And F

upvoted 1 times

Karamen 3 months, 3 weeks ago

BEF
- Create a CloudFormation service role
- Update your stack using the role when deploying
- ensure iam:passrole

upvoted 2 times

Karamen 3 months, 3 weeks ago

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-iam-servicerole.html

upvoted 2 times

Christina666 3 months, 3 weeks ago

Selected Answer: BD

BDF
By creating a service role specifically for AWS CloudFormation, you can limit the permissions to just what CloudFormation needs, and this reduces the risk of excessive permissions or accidental permission conflicts.

upvoted 3 times

[Removed] 3 months, 4 weeks ago

Selected Answer: BDE

B, D, E & F (E&F show up as a single option?)
https://docs.aws.amazon.com/prescriptive-guidance/latest/least-privilege-cloudformation/service-roles-for-cloudformation.html

upvoted 2 times

KR693 4 months ago

B, D and F

upvoted 1 times

Question #19 *Topic 1*

A company used a lift-and-shift approach to migrate from its on-premises data centers to the AWS Cloud. The company migrated on-premises VMs to Amazon EC2 instances. Now the company wants to replace some of components that are running on the EC2 instances with managed AWS services that provide similar functionality.
Initially, the company will transition from load balancer software that runs on EC2 instances to AWS Elastic Load Balancers. A security engineer must ensure that after this transition, all the load balancer logs are centralized and searchable for auditing. The security engineer must also ensure that metrics are generated to show which ciphers are in use.
Which solution will meet these requirements?

A. Create an Amazon CloudWatch Logs log group. Configure the load balancers to send logs to the log group. Use the CloudWatch Logs console to search the logs. Create CloudWatch Logs filters on the logs for the required metrics.

B. Create an Amazon S3 bucket. Configure the load balancers to send logs to the S3 bucket. Use Amazon Athena to search the logs that are in the S3 bucket. Create Amazon CloudWatch filters on the S3 log files for the required metrics.

C. Create an Amazon S3 bucket. Configure the load balancers to send logs to the S3 bucket. Use Amazon Athena to search the logs that are in the S3 bucket. Create Athena queries for the required metrics. Publish the metrics to Amazon CloudWatch.

D. Create an Amazon CloudWatch Logs log group. Configure the load balancers to send logs to the log group. Use the AWS Management Console to search the logs. Create Amazon Athena queries for the required metrics. Publish the metrics to Amazon CloudWatch.

Correct Answer: *B*

Community vote distribution

C (56%) A (31%) 13%

Daniel76 Highly Voted 3 months, 1 week ago

Selected Answer: A

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-cloudwatch-metrics.html#view-metric-data
s3 buckets and athena are not needed.

upvoted 5 times

Aamee 2 months, 4 weeks ago

No, if you look at the reqs. of this question, it specifically asks for this query:
"All the load balancer logs are centralized and searchable for auditing"..
So if you select A for CloudWatch Log groups, it has the default retention policy set. After which it will clear off all the saved logs!... so how would you be able to do the audit on the logs after 14 days lets say??
That's why I'm going with Option C here..

upvoted 2 times

Daniel76 1 month, 3 weeks ago

By default, cloudWatch log retention is indefinite unless you set it to limited duration due to audit requirement.
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Working-with-log-groups-and-streams.html#SettingLogRetention

upvoted 3 times

Daniel76 1 month, 3 weeks ago

However i tend to agree it is C after reviewing this qn: enable access log can keep logs in s3 where you can search for ssl_cipher string using SQL like query:
https://docs.aws.amazon.com/athena/latest/ug/application-load-balancer-logs.html
you can indeed publish athena query metrics to cloudwatch by enabling the option.
https://docs.aws.amazon.com/athena/latest/ug/query-metrics-viewing.html

upvoted 2 times

PareshBPatel Most Recent 2 weeks, 1 day ago

B is not correct choice
Option B involves using S3 for storage and Athena for searching, but it suggests creating CloudWatch filters on S3 log files, which isn't directly possible as CloudWatch filters work on logs stored in CloudWatch Logs, not on S3.

upvoted 1 times

PareshBPatel 2 weeks, 1 day ago

C
For ensuring centralized and searchable logging for auditing purposes after transitioning to AWS Elastic Load Balancers, and for generating metrics to show which ciphers are in use, the most effective solution among the provided options is:

C. Create an Amazon S3 bucket. Configure the load balancers to send logs to the S3 bucket. Use Amazon Athena to search the logs that are in the S3 bucket. Create Athena queries for the required metrics. Publish the metrics to Amazon CloudWatch.

upvoted 1 times

Raphaello 2 weeks, 3 days ago

Selected Answer: B

Weird set of answers. Mixing between access logs and performance metrics.
Check out this
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-monitoring.html

CloudWatch is responsible about collecting performance metrics.
Whereas, access logs are captured and sent to S3. You can use these logs to analyze traffic patterns, but NOT TO QUERY METRICS using Athena (it does not make sense even).

Therefore, the closest answer to correctness is B!

upvoted 2 times

Raphaello 4 days, 2 hours ago

Correct answer is C.

Athena is in fact capable of query metrics and publish them to CloudWatch.
https://docs.aws.amazon.com/athena/latest/ug/athena-cloudwatch-metrics-enable.html

upvoted 1 times

smanzana 1 month, 1 week ago

A or C?? I choose C because I think that AWS ELB cant send logs to CloudWatch

upvoted 1 times

Gafa255 1 month, 1 week ago

Selected Answer: C

ELB cant send log to CloudWatch.

upvoted 1 times

trashbox 2 months, 1 week ago

Exam on 2023-12-18

upvoted 1 times

Raphaello 2 months, 2 weeks ago

Correct Answer is B.
We're talking about ELB access logs, not metrics, which always get forwarded to S3 bucket.
From there one can use Athena for SQL querying.

upvoted 1 times

[Removed] 3 months, 4 weeks ago

Selected Answer: C

Answer is C

upvoted 1 times

lalee2 4 months ago

Selected Answer: C

I think C is right

upvoted 1 times

pupsik 4 months ago

Selected Answer: C

Agree with C.

upvoted 2 times

bhui 4 months ago

Selected Answer: C

The Correct Answer should be C.
A,D is wrong as - ELB cannot publish log directly to CloudWatch Log.
B is wrong as - CloudWatch filter on S3 is not available. The filter is for CloudWatch Log.

Instead you can publish query-related metrics to CloudWatch with custom widget
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/add_custom_widget_samples.html

upvoted 4 times

100fold 4 months ago

Thinking also A

upvoted 1 times

100fold 3 months, 3 weeks ago

Correction to answer C.

upvoted 2 times

Sumi81 4 months ago

I think A

upvoted 1 times

Question #20 *Topic 1*

A company uses AWS Organizations to manage a multi-account AWS environment in a single AWS Region. The organization's management account is named management-01. The company has turned on AWS Config in all accounts in the organization. The company has designated an account named security-01 as the delegated administrator for AWS Config.
All accounts report the compliance status of each account's rules to the AWS Config delegated administrator account by using an AWS Config aggregator. Each account administrator can configure and manage the account's own AWS Config rules to handle each account's unique compliance requirements.
A security engineer needs to implement a solution to automatically deploy a set of 10 AWS Config rules to all existing and future AWS accounts in the organization. The solution must turn on AWS Config automatically during account creation.
Which combination of steps will meet these requirements? (Choose two.)

A. Create an AWS CloudFormation template that contains the 10 required AWS Config rules. Deploy the template by using CloudFormation StackSets in the security-01 account.

B. Create a conformance pack that contains the 10 required AWS Config rules. Deploy the conformance pack from the security-01 account.

C. Create a conformance pack that contains the 10 required AWS Config rules. Deploy the conformance pack from the management-01 account.

D. Create an AWS CloudFormation template that will activate AWS Config. Deploy the template by using CloudFormation StackSets in the security-01 account.

E. Create an AWS CloudFormation template that will activate AWS Config. Deploy the template by using CloudFormation StackSets in the management-01 account.

Correct Answer: *AD*

Community vote distribution

BE (94%) 6%

Christina666 Highly Voted 3 months, 1 week ago

Selected Answer: BE

Use management account to delegate accounts for auditing, security or compliance, then use delegated account to deploy conformance packs

upvoted 5 times

walter_white_008 Most Recent 6 days, 13 hours ago

why is D not correct ? a delegated admin can deploy the stacks to enable the AWS config and its preferable to use the delegated account over admin account.

What am I missing ?

upvoted 1 times

Daibin 1 month, 3 weeks ago

I'd go with B and E
https://aws.amazon.com/blogs/mt/using-delegated-admin-for-aws-config-operations-and-aggregation/

upvoted 1 times

trashbox 2 months, 1 week ago

Exam on 2023-12-18

upvoted 1 times

Raphaello 2 months, 2 weeks ago

"security-01 account" is a delegated administrator account, so let's agree that either Cfn stacksets or Config rules will be deployed from this account.
Now, since there are multiple accounts, deploying AWS Config rules (conformance pack) would be through CloudFormation template/stackset.
AD seems right choices for me, albeit B is not wrong but it misses the deployment part of Config rules.

upvoted 1 times

Raphaello 2 weeks, 3 days ago

Obviously I was wrong.
BE are the best answers.

upvoted 1 times

Daniel76 3 months ago

Selected Answer: BE

I go with B and E.
https://aws.amazon.com/blogs/mt/deploying-conformance-packs-across-an-organization-with-automatic-remediation/

Delegated administrator for AWS Organizations
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_delegate_policies.html

upvoted 3 times

Aamee 3 months, 1 week ago

Selected Answer: CE

I'd probably go with C and E since the AWS documentation shows that it's only the management account from where the CFN stack can be deployed at along with the Conformance Packs which can also be deployed at the Management/Master account level.
But pls. correct me if I understood it incorrectly somewhere... Thnx!

upvoted 1 times

Aamee 3 months, 1 week ago

https://aws.amazon.com/blogs/mt/deploying-conformance-packs-across-an-organization-with-automatic-remediation/

From the source above, it looks like the Conformance Packs can be setup only by the Master Account (Which probably in this usecase, it's the Management account I guess).

"These conformance packs and their underlying config rules and remediations actions are not modifiable by your organization's member accounts. Only master accounts can create, update, and delete organization conformance packs."

Still confused as to why we've the Security-01 account setup as the AWS Config Delegated administrator for all the member accounts?..

upvoted 1 times

[Removed] 3 months, 4 weeks ago

Selected Answer: BE

B and E

upvoted 1 times

lalee2 4 months ago

Selected Answer: BE

B and E. Conformance should be set up in admin account but in the question it says 'security-01 as the delegated administrator for AWS Config'. I would pick B and E here.

upvoted 3 times

pupsik 4 months ago

Selected Answer: BE

Agree with @bhui.

upvoted 1 times

bhui 4 months ago

Selected Answer: BE

Should be BE
https://aws.amazon.com/blogs/mt/deploying-conformance-packs-across-an-organization-with-automatic-remediation/
B as security account is the AWS Config delegated admin

upvoted 4 times

bhui 4 months ago

Supplementing my thoughts with this blog.
https://aws.amazon.com/blogs/mt/org-aggregator-delegated-admin/
1. To enable AWS Config access to AWS Organizations
- Run the following command from your organization management account:
2. To set up an aggregator using delegated admin

upvoted 4 times

Sumi81 4 months ago

CE
https://aws.amazon.com/blogs/mt/deploying-conformance-packs-across-an-organization-with-automatic-remediation/

upvoted 3 times

Question #21 *Topic 1*

A company has a legacy application that runs on a single Amazon EC2 instance. A security audit shows that the application has been using an IAM access key within its code to access an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET1 in the same AWS account. This access key pair has the s3:GetObject permission to all objects in only this S3 bucket. The company takes the application offline because the application is not compliant with the company's security policies for accessing other AWS resources from Amazon EC2.
A security engineer validates that AWS CloudTrail is turned on in all AWS Regions. CloudTrail is sending logs to an S3 bucket that is named DOC-EXAMPLE-BUCKET2. This S3 bucket is in the same AWS account as DOC-EXAMPLE-BUCKET1. However, CloudTrail has not been configured to send logs to Amazon CloudWatch Logs.
The company wants to know if any objects in DOC-EXAMPLE-BUCKET1 were accessed with the IAM access key in the past 60 days. If any objects were accessed, the company wants to know if any of the objects that are text files (.txt extension) contained personally identifiable information (PII).
Which combination of steps should the security engineer take to gather this information? (Choose two.)

A. Use Amazon CloudWatch Logs Insights to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.

B. Use Amazon OpenSearch Service to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for API calls that used the access key to access an object that contained PII.

C. Use Amazon Athena to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for any API calls that used the access key to access an object that contained PII.

D. Use AWS Identity and Access Management Access Analyzer to identify any API calls that used the access key to access objects that contained PII in DOC-EXAMPLE-BUCKET1.

E. Configure Amazon Macie to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.

Correct Answer: *AE*

Community vote distribution

CE (90%) 10%

3633f8f 2 months, 1 week ago

Selected Answer: CE

CE without further discussion.

upvoted 1 times

Raphaello 2 months, 2 weeks ago

CE

A does not add anything.

upvoted 1 times

Raphaello 2 months, 2 weeks ago

CE

CloudTrail is not configured to forward findings to CloudWatch in this scenario.

upvoted 1 times

Daniel76 3 months ago

Selected Answer: CE

D - using access analyzer seems to be a possible answer too:
https://docs.aws.amazon.com/IAM/latest/UserGuide/logging-using-cloudtrail.html
However, C should be better as Athena is used which able to return results to answer whether any object is accessed.
Macie is definitely needed to answer whether PII is present.

upvoted 1 times

Daniel76 2 months ago

Correction, C is only referring to the information captured in the cloudtrail through access analyzer api. You still need Athena for a quick and convenient search in the logs stored in s3.
https://docs.aws.amazon.com/IAM/latest/UserGuide/logging-using-cloudtrail.html#service-name-info-in-cloudtrail

upvoted 1 times

YR4591 3 months, 1 week ago

Selected Answer: CE

Athena send the query results to s3 bucket > Macie can scan s3 bucket

upvoted 3 times

[Removed] 3 months, 3 weeks ago

Selected Answer: C

C and E

upvoted 1 times

lalee2 4 months ago

my pick is C and E also

upvoted 1 times

pupsik 4 months ago

Selected Answer: CE

CE it is.

upvoted 2 times

Sumi81 4 months ago

CE is correct

upvoted 2 times

100fold 4 months, 1 week ago

Selected Answer: CE

Agree answer CE

upvoted 2 times

tecte 4 months, 2 weeks ago

CE is correct.

upvoted 2 times

aragon_saa 4 months, 3 weeks ago

https://www.examtopics.com/discussions/amazon/view/89893-exam-aws-certified-security-specialty-topic-1-question-450/

upvoted 2 times

Question #22 *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 sill 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.

Correct Answer: *D*

Community vote distribution

D (100%)

trashbox 2 months, 1 week ago

Exam on 2023-12-18

upvoted 1 times

[Removed] 3 months, 3 weeks ago

Selected Answer: D

"An explicit deny in any policy overrides any allows."
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html#policy-eval-denyallow

upvoted 3 times

lalee2 4 months ago

Selected Answer: D

D is my answer

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: D

Agree answer D

upvoted 2 times

aragon_saa 4 months, 3 weeks ago

https://www.examtopics.com/discussions/amazon/view/30027-exam-aws-certified-security-specialty-topic-1-question-177/

upvoted 2 times

Question #23 *Topic 1*

A company is using Amazon Macie, AWS Firewall Manager, Amazon Inspector, and AWS Shield Advanced in its AWS account. The company wants to receive alerts if a DDoS attack occurs against the account.
Which solution will meet this requirement?

A. Use Macie to detect an active DDoS event. Create Amazon CloudWatch alarms that respond to Macie findings.

B. Use Amazon inspector to review resources and to invoke Amazon CloudWatch alarms for any resources that are vulnerable to DDoS attacks.

C. Create an Amazon CloudWatch alarm that monitors Firewall Manager metrics for an active DDoS event.

D. Create an Amazon CloudWatch alarm that monitors Shield Advanced metrics for an active DDoS event.

Correct Answer: *D*

Community vote distribution

D (100%)

trashbox 2 months, 1 week ago
Exam on 2023-12-18
upvoted 1 times

Raphaello 2 months, 2 weeks ago
D is the correct answer.
upvoted 1 times

Daniel76 3 months ago
Selected Answer: D
https://docs.aws.amazon.com/waf/latest/developerguide/ddos-cloudwatch-metrics.html
upvoted 1 times

lalee2 4 months ago
Selected Answer: D
Shield Advanced for DDoS
upvoted 1 times

Sumi81 4 months ago
D is right
upvoted 2 times

100fold 4 months, 1 week ago
Selected Answer: D
Agree answer D.
Shield Advanced for DDoS
upvoted 3 times

aragon_saa 4 months, 3 weeks ago
https://www.examtopics.com/discussions/amazon/view/89223-exam-aws-certified-security-specialty-topic-1-question-452/
upvoted 1 times

Question #24 *Topic 1*

A company hosts a web application on an Apache web server. The application runs on Amazon EC2 instances that are in an Auto Scaling group. The company configured the EC2 instances to send the Apache web server logs to an Amazon CloudWatch Logs group that the company has configured to expire after 1 year.
Recently, the company discovered in the Apache web server logs that a specific IP address is sending suspicious requests to the web application. A security engineer wants to analyze the past week of Apache web server logs to determine how many requests that the IP address sent and the corresponding URLs that the IP address requested.
What should the security engineer do to meet these requirements with the LEAST effort?

A. Export the CloudWatch Logs group data to Amazon S3. Use Amazon Macie to query the logs for the specific IP address and the requested URL.

B. Configure a CloudWatch Logs subscription to stream the log group to an Amazon OpenSearch Service cluster. Use OpenSearch Service to analyze the logs for the specific IP address and the requested URLs.

C. Use CloudWatch Logs Insights and a custom query syntax to analyze the CloudWatch logs for the specific IP address and the requested URLs.

D. Export the CloudWatch Logs group data to Amazon S3. Use AWS Glue to crawl the S3 bucket for only the log entries that contain the specific IP address. Use AWS Glue to view the results.

Correct Answer: *A*

Community vote distribution

C (100%)

AgboolaKun Highly Voted 4 months, 1 week ago

Selected Answer: C

The correct answer here is C. Please check the Queries for Apache server logs section of the following document - https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_QuerySyntax-examples.html

upvoted 9 times

i7ovemyself Most Recent 1 week, 1 day ago

A is not the answer as macie is used to scan s3 buckets for PII.

upvoted 1 times

Raphaello 2 months, 2 weeks ago

C
A classic usage of CloudWatch Logs Insights
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_QuerySyntax-examples.html#CWL_QuerySyntax-examples-Apache

upvoted 2 times

Aamee 2 months, 3 weeks ago

Selected Answer: C

Option C only among all others can only get this sol. done with the 'LEAST' effort as per the ask/reqs.

upvoted 1 times

[Removed] 3 months, 3 weeks ago

Selected Answer: C

Answer is C

upvoted 1 times

lalee2 4 months ago

Selected Answer: C

C seems to be correct

upvoted 1 times

Sumi81 4 months ago

C is correct

upvoted 2 times

kk2000 4 months, 3 weeks ago

Correct Answer is C

upvoted 2 times

Question #25 *Topic 1*

While securing the connection between a company's VPC and its on-premises data center, a security engineer sent a ping command from an on-premises host (IP address 203.0.113.12) to an Amazon EC2 instance (IP address 172.31.16.139). The ping command did not return a response. The flow log in the VPC showed the following:

```
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK

2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
```

What action should be performed to allow the ping to work?

A. In the security group of the EC2 instance, allow inbound ICMP traffic.

B. In the security group of the EC2 instance, allow outbound ICMP traffic.

C. In the VPC's NACL, allow inbound ICMP traffic.

D. In the VPC's NACL, allow outbound ICMP traffic.

Correct Answer: *A*

Community vote distribution

D (100%)

i7ovemyself 20 hours, 8 minutes ago

For security group outbound rule is automatically allowed as security groups are stateful, NACL is stateless, so answer will be D as we need to allow the outbound rule in VPC's NACL.

upvoted 1 times

Daniel76 3 months ago

Selected Answer: D

There are multiple possible cause.
https://arcadian.cloud/aws/2022/07/01/4-reasons-you-cannot-ping-your-aws-ec2-instance-and-how-to-fix-them/
Base on the logs, only one direction is not successful. Likely its #4 - NACL.

upvoted 1 times

Aamee 3 months, 1 week ago

Selected Answer: D

It's the EC2 instance IP area from where the ping didn't get the response back to the on-prem location which is clearly a usecase of NACL area. Therefore, def. going with 'D'.

upvoted 1 times

Christina666 3 months, 1 week ago

Selected Answer: D

NACLs are stateless and do not track the state of a connection, while Security Groups are stateful and allow traffic based on the response to previous traffic.

Default rule: NACLs have a default rule that denies all traffic, while Security Groups have a default rule that allows all traffic.

upvoted 3 times

[Removed] 3 months, 3 weeks ago

Selected Answer: D

Answer D

upvoted 1 times

lalee2 4 months ago

Selected Answer: D

Answer D

upvoted 1 times

pupsik 4 months ago

Selected Answer: D

Outbound communication on NACL is blocked.

upvoted 1 times

allcertcracker 4 months ago

it is D

upvoted 1 times

Sumi81 4 months ago

I think its B

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: D

Answer D

upvoted 1 times

aragon_saa 4 months, 3 weeks ago

https://www.examtopics.com/discussions/amazon/view/16473-exam-aws-certified-security-specialty-topic-2-question-8/

upvoted 2 times

Question #26 *Topic 1*

A company developed an application by using AWS Lambda, Amazon S3, Amazon Simple Notification Service (Amazon SNS), and Amazon DynamoDB. An external application puts objects into the company's S3 bucket and tags the objects with date and time. A Lambda function periodically pulls data from the company's S3 bucket based on date and time tags and inserts specific values into a DynamoDB table for further processing.
The data includes personally identifiable information (PII). The company must remove data that is older than 30 days from the S3 bucket and the DynamoDB table.
Which solution will meet this requirement with the MOST operational efficiency?

A. Update the Lambda function to add a TTL S3 flag to S3 objects. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using the TTL S3 flag.

B. Create an S3 Lifecycle policy to expire objects that are older than 30 days. Update the Lambda function to add the TTL attribute in the DynamoDB table. Enable TTL on the DynamoDB table to expire entries that are older than 30 days based on the TTL attribute.

C. Create an S3 Lifecycle policy to expire objects that are older than 30 days and to add all prefixes to the S3 bucket. Update the Lambda function to delete entries that are older than 30 days.

D. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using object tags. Update the Lambda function to delete entries that are older than 30 days.

Correct Answer: *A*

Community vote distribution

B (100%)

i7ovemyself 20 hours, 7 minutes ago

Lifecycle Policy for s3 and TTL for Dynamo DB, best combination.
Answer will be B.

upvoted 1 times

Daniel76 3 months ago

Selected Answer: B

https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-configuration-examples.html
Just need to set expiration days in the LifecycleConfiguration- add prefix, object tags are not needed.
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html
TTL is used for housekeeping data in DynamoDB by enabling TTL attribute by console or CLI, without the need for any lambda function/

upvoted 1 times

[Removed] 3 months, 3 weeks ago

Selected Answer: B

Lifecycle policy for S3, TTL for dynamodb.

upvoted 2 times

lalee2 4 months ago

Selected Answer: B

B is right

upvoted 1 times

pupsik 4 months ago

Selected Answer: B

B is correct... although wording is not quite right.

upvoted 2 times

abhishek007 4 months ago

B is the correct answer

upvoted 1 times

Sumi81 4 months ago

B is right

upvoted 2 times

kk2000 4 months, 3 weeks ago

Correct Answer is B

upvoted 2 times

Question #27 *Topic 1*

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. Use AWS KMS to encrypt all AWS account root user and AWS IAM access keys and set automatic rotation to 30 days.

D. Do not create access keys for the AWS account root user; instead, create AWS IAM users.

E. Enable multi-factor authentication for the AWS account root user.

Correct Answer: *CE*

Community vote distribution

DE (100%)

i7ovemyself 20 hours, 3 minutes ago

A is not correct as it is not preferable to create access keys for root user.
B is not correct as enabling MFA for other user won't help the root user in any way.
C is not right as access keys shouldn't be created for root user.

Correct Answer is DE

upvoted 1 times

[Removed] 3 months, 3 weeks ago

Selected Answer: DE

Answer D and E

upvoted 1 times

lalee2 4 months ago

Selected Answer: DE

Answer DE

upvoted 1 times

abhishek007 4 months ago

DE seems to be the correct answer

upvoted 2 times

Sumi81 4 months ago

DE is correct

upvoted 2 times

100fold 4 months, 1 week ago

Selected Answer: DE

Answer DE

upvoted 3 times

aragon_saa 4 months, 3 weeks ago

https://www.examtopics.com/discussions/amazon/view/16530-exam-aws-certified-security-specialty-topic-1-question-135/

upvoted 3 times

Question #28 *Topic 1*

A company is expanding its group of stores. On the day that each new store opens, the company wants to launch a customized web application for that store. Each store's application will have a non-production environment and a production environment. Each environment will be deployed in a separate AWS account. The company uses AWS Organizations and has an OU that is used only for these accounts.
The company distributes most of the development work to third-party development teams. A security engineer needs to ensure that each team follows the company's deployment plan for AWS resources. The security engineer also must limit access to the deployment plan to only the developers who need access. The security engineer already has created an AWS CloudFormation template that implements the deployment plan.
What should the security engineer do next to meet the requirements in the MOST secure way?

A. Create an AWS Service Catalog portfolio in the organization's management account. Upload the CloudFormation template. Add the template to the portfolio's product list. Share the portfolio with the OU.

B. Use the CloudFormation CLI to create a module from the CloudFormation template. Register the module as a private extension in the CloudFormation registry. Publish the extension. In the OU, create an SCP that allows access to the extension.

C. Create an AWS Service Catalog portfolio in the organization's management account. Upload the CloudFormation template. Add the template to the portfolio's product list. Create an IAM role that has a trust policy that allows cross-account access to the portfolio for users in the OU accounts. Attach the AWSServiceCatalogEndUserFullAccess managed policy to the role.

D. Use the CloudFormation CLI to create a module from the CloudFormation template. Register the module as a private extension in the CloudFormation registry. Publish the extension. Share the extension with the OU.

Correct Answer: *A*

Community vote distribution

A (79%) D (21%)

i7ovemyself 20 hours, 1 minute ago

AWS Service Catalog is a service that enables organizations to create and manage catalogs of IT services that are approved for use on AWS. These catalogs can include everything from virtual machine images, servers, software, and databases to entire multi-tier application architectures.

Correct answer is A

C will not be correct as providing full access will not be secure as per AWS standards.

upvoted 1 times

Raphaello 1 week ago

Selected Answer: A

Sharing Service Catalog portfolio is more secure than allowing full access.

Correct answer is A.

upvoted 1 times

Raphaello 4 days, 1 hour ago

I spent some time looking into this question.
CF modules vs Service Catalog
It is resource centric vs service centric. Infra. provisioning vs service management. A low level building block vs service approval.
The scenario talks about ensuring "DEVELOPER" sticking to "deployment plan", which implies assurance at a lower level than service catalog.

Therefore, D could be the right answer.
Again, It all depends on the interpretation, but no clear "right" or "wrong" answer in this one.

https://stackshare.io/stackups/aws-cloudformation-vs-aws-service-catalog#:~:text=In%20summary%2C%20AWS%20CloudFormation%20is,catalogs%20of%20pre%2Dapproved%20services.

upvoted 1 times

longns 3 weeks, 5 days ago

Selected Answer: A

C: incorrect because allows cross-account access to the portfolio for users in the OU accounts. Attach the AWSServiceCatalogEndUserFullAccess managed policy to the role --> this violate rule give least privilege
Privilege of https://docs.aws.amazon.com/aws-managed-policy/latest/reference/AWSServiceCatalogEndUserFullAccess.html

upvoted 1 times

Christina666 3 months, 1 week ago

Selected Answer: A

To use Service Catalog with multiple AWS accounts, you need to enable AWS Organizations with all features enabled. This allows you to centrally manage your accounts and apply policies across your organization. You can also use Service Catalog as a service principal for AWS

Organizations, which lets you share your portfolios with organizational units (OUs) or accounts in your organization.

To create a Service Catalog portfolio, you need to use an administrator account, such as the organization's management account. You can upload your CloudFormation template as a product in your portfolio, and define constraints and tags for it. You can then share your portfolio with the OU that contains the accounts for the web applications. This will allow the developers in those accounts to launch products from the shared portfolio using the Service Catalog end user console.

upvoted 4 times

Christina666 3 months, 1 week ago

Option C is incorrect because creating an IAM role that has a trust policy that allows cross-account access to the portfolio is not secure. It would allow any user in the OU accounts to assume the role and access the portfolio, regardless of their job function or access requirements.

upvoted 4 times

Aamee 3 months, 1 week ago

Still a bit ambigious btw A and D... Not sure fully :/

upvoted 1 times

kejam 3 months, 2 weeks ago

Selected Answer: A

You can share a Service Catalog portfolio to an Org OU
https://docs.aws.amazon.com/organizations/latest/userguide/services-that-can-integrate-servicecatalog.html

upvoted 2 times

[Removed] 3 months, 3 weeks ago

Selected Answer: A

Service Catalog sounds like the right tool for the job

upvoted 1 times

M2ao 3 months, 3 weeks ago

why not C

upvoted 1 times

bannium 4 months ago

Selected Answer: A

I think Option A is sufficient for our needs.
https://aws.amazon.com/about-aws/whats-new/2022/11/aws-service-catalog-sharing-principal-names-portfolio-organization/

upvoted 2 times

100fold 4 months, 1 week ago

B instead of D
SCP limits the access

upvoted 2 times

Aamee 3 months, 1 week ago

Are you sure that it should be B?... cuz will SCP going to work under the OU level?..

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: D

Answer D. You can use the CloudFormation (CLI).
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/registry.html
https://docs.aws.amazon.com/cloudformation-cli/latest/userguide/modules.html
https://aws.amazon.com/blogs/mt/introducing-aws-cloudformation-modules/

upvoted 3 times

Raphaello 4 days, 1 hour ago

You probably have a point there. I learned something. Thank you.

upvoted 1 times

Question #29 *Topic 1*

A team is using AWS Secrets Manager to store an application database password. Only a limited number of IAM principals within the account can have access to the secret. The principals who require access to the secret change frequently. A security engineer must create a solution that maximizes flexibility and scalability.
Which solution will meet these requirements?

A. Use a role-based approach by creating an IAM role with an inline permissions policy that allows access to the secret. Update the IAM principals in the role trust policy as required.

B. Deploy a VPC endpoint for Secrets Manager. Create and attach an endpoint policy that specifies the IAM principals that are allowed to access the secret. Update the list of IAM principals as required.

C. Use a tag-based approach by attaching a resource policy to the secret. Apply tags to the secret and the IAM principals. Use the aws:PrincipalTag and aws:ResourceTag IAM condition keys to control access.

D. Use a deny-by-default approach by using IAM policies to deny access to the secret explicitly. Attach the policies to an IAM group. Add all IAM principals to the IAM group. Remove principals from the group when they need access. Add the principals to the group again when access is no longer allowed.

Correct Answer: *C*

Community vote distribution

C (90%) 10%

100fold Highly Voted 4 months, 1 week ago

Selected Answer: C

Answer C

https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_attribute-based-access-control.html
https://aws.amazon.com/blogs/security/simplify-granting-access-to-your-aws-resources-by-using-tags-on-aws-iam-users-and-roles/

upvoted 6 times

Raphaello Most Recent 4 days, 1 hour ago

Selected Answer: C

ABAC (aka tag-based policy control) provides flexible and scalable control.

upvoted 1 times

awssecuritynewbie 3 months ago

Selected Answer: A

A ,,,,,,,,,,,,,,

upvoted 1 times

1c7c461 2 months, 2 weeks ago

It is not A, it is not best-practice to use inline policies on a role.

upvoted 1 times

kejam 3 months, 2 weeks ago

Selected Answer: C

https://docs.aws.amazon.com/secretsmanager/latest/userguide/managing-secrets_tagging.html

upvoted 2 times

Question #30 *Topic 1*

A company is hosting a web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The application has become the target of a DoS attack. Application logging shows that requests are coming from a small number of client IP addresses, but the addresses change regularly.
The company needs to block the malicious traffic with a solution that requires the least amount of ongoing effort.
Which solution meets these requirements?

A. Create an AWS WAF rate-based rule, and attach it to the ALB.

B. Update the security group that is attached to the ALB to block the attacking IP addresses.

C. Update the ALB subnet's network ACL to block the attacking client IP addresses.

D. Create an AWS WAF rate-based rule, and attach it to the security group of the EC2 instances.

Correct Answer: *A*

Community vote distribution

A (100%)

Raphaello 2 months, 2 weeks ago

Selected Answer: A

A
WAF rate-based rule and attach it to ALB.

upvoted 1 times

Aamee 2 months, 4 weeks ago

Selected Answer: A

WAF protects CloudFront, R53 and ALB as they're tightly integrated with WAF.

upvoted 1 times

Daniel76 2 months, 4 weeks ago

Selected Answer: A

AWS WAF can be deployed on Amazon CloudFront, the Application Load Balancer (ALB), Amazon API Gateway, and AWS AppSync.

upvoted 4 times

smanzana 1 month, 1 week ago

Indeed, AWS WAF cannot be directly attached to the Security Group of EC2 instances.

upvoted 1 times

awssecuritynewbie 3 months ago

They could of used the VPC flow logs to figure out the IPs that are attacking then use lambda to update the ACL NACL for the LB. it would be better than actually applying rate limiting.

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: A

Answer A
https://www.examtopics.com/discussions/amazon/view/61173-exam-aws-certified-security-specialty-topic-1-question-259/

upvoted 4 times

Question #31 *Topic 1*

A company has hundreds of AWS accounts in an organization in AWS Organizations. The company operates out of a single AWS Region. The company has a dedicated security tooling AWS account in the organization. The security tooling account is configured as the organization's delegated administrator for Amazon GuardDuty and AWS Security Hub. The company has configured the environment to automatically enable GuardDuty and Security Hub for existing AWS accounts and new AWS accounts.
The company is performing control tests on specific GuardDuty findings to make sure that the company's security team can detect and respond to security events. The security team launched an Amazon EC2 instance and attempted to run DNS requests against a test domain, example.com, to generate a DNS finding. However, the GuardDuty finding was never created in the Security Hub delegated administrator account.
Why was the finding was not created in the Security Hub delegated administrator account?

A. VPC flow logs were not turned on for the VPC where the EC2 instance was launched.

B. The VPC where the EC2 instance was launched had the DHCP option configured for a custom OpenDNS resolver.

C. The GuardDuty integration with Security Hub was never activated in the AWS account where the finding was generated.

D. Cross-Region aggregation in Security Hub was not configured.

Correct Answer: *C*

Community vote distribution

B (86%) 14%

[Removed] Highly Voted 3 months ago

Selected Answer: B

Guardduty cannot detect DNS requests if a custom resolver is setup

See below:

https://repost.aws/knowledge-center/guardduty-finding-types#:~:text=Note%3A%20GuardDuty%20only%20processes%20DNS%20logs%20if%20you%20use%20the%20default%20VPC%20DNS%20resolver.%20All%20other%20types%20of%20DNS%20resolvers%20won%27t%20generated%20DNS%20based%20findings.

upvoted 5 times

Daniel76 2 months, 4 weeks ago

"GuardDuty only processes DNS logs if you use the default VPC DNS resolver. All other types of DNS resolvers won't generated DNS based findings."

upvoted 3 times

mynickc Most Recent 1 month, 1 week ago

Selected Answer: B

B is correct. https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-internal-providers.html#integration-amazon-guardduty

upvoted 1 times

CloudRover 1 month, 2 weeks ago

Selected Answer: B

"GuardDuty only processes DNS logs if you use the default VPC DNS resolver. All other types of DNS resolvers won't generated DNS based findings."
As Daniel76 pointed out, this is the correct answer.

upvoted 2 times

trashbox 2 months, 1 week ago

Exam on 2023-12-18

upvoted 1 times

Raphaello 2 months, 2 weeks ago

Selected Answer: D

Going with D.
https://docs.aws.amazon.com/securityhub/latest/userguide/finding-aggregation-enable.html#finding-aggregation-enable-console

upvoted 1 times

Raphaello 1 week ago

Correction: correct answer is B.
Missed that in the scenario the company operates from a single region, additionally, without using Route53 resolver and DNS query logs, GuardDuty would not be able to produce DNS findings.

upvoted 1 times

KaiW 1 month, 3 weeks ago

but didn't the question said that the company operates out of a single region?

upvoted 1 times

kejam 3 months, 2 weeks ago

Selected Answer: D

Choosing D through a process of elimination.

A. VPC flow logs are not required to be turned on.
https://aws.amazon.com/guardduty/faqs/

B. Custom DNS resolver? GuardDuty should have picked that up from the VPC flow logs:
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-ec2.html#defenseevasion-ec2-unusualdnsresolver

C. GuardDuty and Security Hub integration is enabled automatically:
https://docs.aws.amazon.com/guardduty/latest/ug/securityhub-integration.html#securityhub-integration-enable

D. Cross-Region aggregation. Regions weren't mentioned in the question, but it is the only possible answer left.
https://docs.aws.amazon.com/securityhub/latest/userguide/finding-aggregation.html

upvoted 1 times

kejam 3 months ago

Just noticed "The company operates out of a single AWS Region." So changing my answer to none of the above ;-)

upvoted 1 times

bannium 4 months ago

Selected Answer: B

> Note: GuardDuty only processes DNS logs if you use the default VPC DNS resolver. All other types of DNS resolvers won't generated DNS based findings.
https://repost.aws/knowledge-center/guardduty-finding-types

upvoted 4 times

Question #32 *Topic 1*

An ecommerce company has a web application architecture that runs primarily on containers. The application containers are deployed on Amazon Elastic Container Service (Amazon ECS). The container images for the application are stored in Amazon Elastic Container Registry (Amazon ECR). The company's security team is performing an audit of components of the application architecture. The security team identifies issues with some container images that are stored in the container repositories.

The security team wants to address these issues by implementing continual scanning and on-push scanning of the container images. The security team needs to implement a solution that makes any findings from these scans visible in a centralized dashboard. The security team plans to use the dashboard to view these findings along with other security-related findings that they intend to generate in the future. There are specific repositories that the security team needs to exclude from the scanning process.

Which solution will meet these requirements?

A. Use Amazon Inspector. Create inclusion rules in Amazon ECR to match repositories that need to be scanned. Push Amazon Inspector findings to AWS Security Hub.

B. Use ECR basic scanning of container images. Create inclusion rules in Amazon ECR to match repositories that need to be scanned. Push findings to AWS Security Hub.

C. Use ECR basic scanning of container images. Create inclusion rules in Amazon ECR to match repositories that need to be scanned. Push findings to Amazon Inspector.

D. Use Amazon Inspector. Create inclusion rules in Amazon Inspector to match repositories that need to be scanned. Push Amazon Inspector findings to AWS Config.

Correct Answer: *A*

Community vote distribution

A (85%) B (15%)

AgboolaKun Highly Voted 4 months, 1 week ago

Selected Answer: A

Amazon Inspector supports the configuration of inclusion rules to select which ECR repositories are scanned. Please see more information here - https://aws.amazon.com/inspector/faqs/

upvoted 6 times

Raphaello Most Recent 1 week ago

Selected Answer: A

For continual and on-push scanning, use Amazon Inspector. Push findings to Security Hub.

upvoted 1 times

Aamee 3 months, 1 week ago

Selected Answer: A

Def. it's A as per the features described for Amazon Inspector here:
https://aws.amazon.com/inspector/faqs/

upvoted 1 times

kejam 3 months, 2 weeks ago

Selected Answer: A

Answer A
Inspector can continuously scan ECR and send findings to Security Hub
https://docs.aws.amazon.com/inspector/latest/user/scanning-ecr.html

upvoted 1 times

bannium 4 months ago

Selected Answer: A

using Amazon ECR integrates with Amazon Inspector with filters
https://docs.aws.amazon.com/AmazonECR/latest/userguide/image-scanning.html#image-scanning-filters

upvoted 2 times

bengalister 4 months ago

Answer A
Amazon inspector can definitely scan ECR repositories
https://docs.aws.amazon.com/inspector/latest/user/scanning-ecr.html

upvoted 2 times

pupsik 4 months ago

Selected Answer: B

Inspector scans EC2 instances.

upvoted 2 times

lightrod 3 weeks ago

it can scan ec2, ecr, and lambda

upvoted 1 times

angelsrp 4 months, 2 weeks ago

B

ECR does provide basic image scanning functionality, which can detect software vulnerabilities in your container images. AWS Security Hub provides a centralized view for security alert and compliance posture across AWS accounts. This solution seems to meet the requirements. Amazon Inspector is used for analyzing EC2 instances and identifying potential security vulnerabilities, but not for container images.

upvoted 2 times

Daniel76 2 months ago

ECR basic scanning only can be configured to on push, or do manual. it does not support continously scan as required.
ECR enhanced scanning integrates with AWS Inspector - so yes it covers not just EC2 instance but container.

upvoted 1 times

Question #33 *Topic 1*

A company has a single AWS account and uses an Amazon EC2 instance to test application code. The company recently discovered that the instance was compromised. The instance was serving up malware. The analysis of the instance showed that the instance was compromised 35 days ago.
A security engineer must implement a continuous monitoring solution that automatically notifies the company's security team about compromised instances through an email distribution list for high severity findings. The security engineer must implement the solution as soon as possible.
Which combination of steps should the security engineer take to meet these requirements? (Choose three.)

A. Enable AWS Security Hub in the AWS account.

B. Enable Amazon GuardDuty in the AWS account.

C. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the security team's email distribution list to the topic.

D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Subscribe the security team's email distribution list to the queue.

E. Create an Amazon EventBridge rule for GuardDuty findings of high severity. Configure the rule to publish a message to the topic.

F. Create an Amazon EventBridge rule for Security Hub findings of high severity. Configure the rule to publish a message to the queue.

Correct Answer: *BCE*

Community vote distribution

BCE (100%)

100fold Highly Voted 4 months, 1 week ago

Selected Answer: BCE

Answer BCE

upvoted 6 times

Raphaello Most Recent 1 week ago

Selected Answer: BCE

BCE..obviously.
GuardDuty + EventBridge + SNS

upvoted 1 times

WeepingMaplte 2 months, 2 weeks ago

AWS Security Hub does not have any scanning capabilities. It provides you with a comprehensive view of your security state only.

upvoted 3 times

Daniel76 2 months, 3 weeks ago

Selected Answer: BCE

GuardDuty, Eventbridge, SNS topics

upvoted 2 times

Daniel76 2 months, 4 weeks ago

Selected Answer: BCE

https://repost.aws/knowledge-center/guardduty-eventbridge-sns-rule

upvoted 2 times

Aamee 3 months, 1 week ago

Selected Answer: BCE

BCE options look most relevant.

upvoted 1 times

pupsik 4 months ago

Selected Answer: BCE

BCE it is.

upvoted 2 times

Question #34 *Topic 1*

A company uses identity federation to authenticate users into an identity account (987654321987) where the users assume an IAM role named IdentityRole. The users then assume an IAM role named JobFunctionRole in the target AWS account (123456789123) to perform their job functions.

A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/JobFunctionRole"
            ],
            "Effect": "Allow"
        }
    ]
}
```

What should be done to enable the user to assume the appropriate role in the target account?

A. Update the IAM policy attached to the role in the identity account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::123456789123:role/JobFunctionRole"
            ],
            "Effect": "Allow"
        }
    ]
}
```

B. Update the trust policy on the role in the target account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::987654321987:role/IdentityRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

C. Update the trust policy on the role in the identity account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": { "AWS": "arn:aws:iam::987654321987:root"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

D. Update the IAM policy attached to the role in the target account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1502946463000",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::123456789123:role/JobFunctionRole"
        }
    ]
}
```

Correct Answer: *D*

Community vote distribution

B (100%)

Daniel76 2 months, 3 weeks ago

Selected Answer: B

When an user is unable to assume a role in the target account, one should check the principal element in the trust policy in the JobFunctionRole in the target account.
Refer to this article to understand permission vs trust policies.
https://www.linkedin.com/pulse/permission-policy-vs-trust-aws-rupesh-tiwari/

upvoted 3 times

kejam 3 months, 2 weeks ago

Selected Answer: B

Answer B
In IAM roles, use the Principal element in the role trust policy to specify who can assume the role.
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_principal.html

upvoted 2 times

bengalister 4 months ago

B is the correct answer

upvoted 2 times

pupsik 4 months ago

Selected Answer: B

B it is.

upvoted 2 times

100fold 4 months, 1 week ago

Selected Answer: B

Agree with answer B

upvoted 2 times

kk2000 4 months, 3 weeks ago

Correct Answer is B

upvoted 3 times

Question #35 *Topic 1*

A company is using AWS Organizations to manage multiple AWS accounts for its human resources, finance, software development, and production departments. All the company's developers are part of the software development AWS account.
The company discovers that developers have launched Amazon EC2 instances that were preconfigured with software that the company has not approved for use. The company wants to implement a solution to ensure that developers can launch EC2 instances with only approved software applications and only in the software development AWS account.
Which solution will meet these requirements?

A. In the software development account, create AMIs of preconfigured instances that include only approved software. Include the AMI IDs in the condition section of an AWS CloudFormation template to launch the appropriate AMI based on the AWS Region. Provide the developers with the CloudFormation template to launch EC2 instances in the software development account.

B. Create an Amazon EventBridge rule that runs when any EC2 RunInstances API event occurs in the software development account. Specify AWS Systems Manager Run Command as a target of the rule. Configure Run Command to run a script that will install all approved software onto the instances that the developers launch.

C. Use an AWS Service Catalog portfolio that contains EC2 products with appropriate AMIs that include only approved software. Grant the developers permission to access only the Service Catalog portfolio to launch a product in the software development account.

D. In the management account, create AMIs of preconfigured instances that include only approved software. Use AWS CloudFormation StackSets to launch the AMIs across any AWS account in the organization. Grant the developers permission to launch the stack sets within the management account.

Correct Answer: *A*

Community vote distribution

C (100%)

AgboolaKun Highly Voted 4 months, 1 week ago

Selected Answer: C

You can use AWS Service Catalog to build a customized AMI from which a team can only launch products from. Please see - https://aws.amazon.com/blogs/mt/use-aws-service-catalog-to-build-a-custom-catalog-of-products-from-aws-marketplace/

upvoted 8 times

Raphaello Most Recent 2 months, 1 week ago

Selected Answer: C

AWS Service Catalog is introduced for this specific purpose: govern and pre-configure provisioning of approved products

upvoted 1 times

WeepingMaplte 2 months, 2 weeks ago

Selected Answer: C

AWS Service Catalog is a service that enables organizations to govern, manage, and automate the provisioning of IT services across their AWS accounts.

upvoted 2 times

100fold 4 months, 1 week ago

Selected Answer: C

Answer C

upvoted 4 times

kk2000 4 months, 3 weeks ago

C should be the correct answer

upvoted 4 times

Question #36 *Topic 1*

A company has enabled Amazon GuardDuty in all AWS Regions as part of its security monitoring strategy. In one of its VPCs, the company hosts an Amazon EC2 instance that works as an FTP server. A high number of clients from multiple locations contact the FTP server. GuardDuty identifies this activity as a brute force attack because of the high number of connections that happen every hour.
The company has flagged the finding as a false positive, but GuardDuty continues to raise the issue. A security engineer must improve the signal-to-noise ratio without compromising the company's visibility of potential anomalous behavior.
Which solution will meet these requirements?

A. Disable the FTP rule in GuardDuty in the Region where the FTP server is deployed.

B. Add the FTP server to a trusted IP list. Deploy the list to GuardDuty to stop receiving the notifications.

C. Create a suppression rule in GuardDuty to filter findings by automatically archiving new findings that match the specified criteria.

D. Create an AWS Lambda function that has the appropriate permissions to delete the finding whenever a new occurrence is reported.

Correct Answer: *C*

Community vote distribution

C (100%)

100fold Highly Voted 4 months, 1 week ago

Selected Answer: C

Answer C
https://docs.aws.amazon.com/guardduty/latest/ug/findings_suppression-rule.html

upvoted 6 times

WeepingMaplte Most Recent 2 months, 2 weeks ago

Selected Answer: C

A suppression rule is a set of criteria, consisting of a filter attribute paired with a value, used to filter findings by automatically archiving new findings that match the specified criteria.

upvoted 2 times

Daniel76 2 months, 3 weeks ago

Selected Answer: C

Suppression rule with specific criteria is the most appropriate solution.
Disable FTP entirely, trust everything from the FTP server reduces the GuardDuty effectiveness.
Creating lambda to delete the finding is counter productive and the finding might have already trigger SNS topic if there's one.

upvoted 3 times

Aamee 2 months, 4 weeks ago

Selected Answer: C

Self-explanatory from the link provided below.

upvoted 1 times

Question #37 *Topic 1*

A company is running internal microservices on Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type. The company is using Amazon Elastic Container Registry (Amazon ECR) private repositories.
A security engineer needs to encrypt the private repositories by using AWS Key Management Service (AWS KMS). The security engineer also needs to analyze the container images for any common vulnerabilities and exposures (CVEs).
Which solution will meet these requirements?

A. Enable KMS encryption on the existing ECR repositories. Install Amazon Inspector Agent from the ECS container instances' user data. Run an assessment with the CVE rules.

B. Recreate the ECR repositories with KMS encryption and ECR scanning enabled. Analyze the scan report after the next push of images.

C. Recreate the ECR repositories with KMS encryption and ECR scanning enabled. Install AWS Systems Manager Agent on the ECS container instances. Run an inventory report.

D. Enable KMS encryption on the existing ECR repositories. Use AWS Trusted Advisor to check the ECS container instances and to verify the findings against a list of current CVEs.

Correct Answer: *B*

Community vote distribution

B (100%)

100fold Highly Voted 4 months, 1 week ago

Selected Answer: B

Answer B

https://docs.aws.amazon.com/AmazonECR/latest/userguide/repository-create.html
https://docs.aws.amazon.com/AmazonECR/latest/userguide/repository-edit.html

upvoted 7 times

Raphaello Most Recent 3 days, 12 hours ago

Selected Answer: B

Need to recreate ECR to enable encryption using KMS key.
Option B is correct.

upvoted 1 times

Jonu 1 month, 2 weeks ago

How about the CVE part of the question?

upvoted 2 times

Osirus 2 months, 2 weeks ago

Answer B

upvoted 1 times

Osirus 2 months, 2 weeks ago

This should be correct

upvoted 1 times

Daniel76 2 months, 3 weeks ago

Selected Answer: B

ECR repositories need to be recreated not enabled, with KMS encryption.
The inventory for AWS system manager does not contain anything about vulnerability.

upvoted 2 times

ahrentom 4 months ago

Selected Answer: B

should be the right anwser

upvoted 2 times

Question #38 *Topic 1*

A company's security engineer has been tasked with restricting a contractor's IAM account access to the company's Amazon EC2 console without providing access to any other AWS services. The contractor's IAM account must not be able to gain access to any other AWS service, even if the IAM account is assigned additional permissions based on IAM group membership.
What should the security engineer do to meet these requirements?

A. Create an inline IAM user policy that allows for Amazon EC2 access for the contractor's IAM user.

B. Create an IAM permissions boundary policy that allows Amazon EC2 access. Associate the contractor's IAM account with the IAM permissions boundary policy.

C. Create an IAM group with an attached policy that allows for Amazon EC2 access. Associate the contractor's IAM account with the IAM group.

D. Create a IAM role that allows for EC2 and explicitly denies all other services. Instruct the contractor to always assume this role.

Correct Answer: *A*

Community vote distribution

B (93%) 7%

WeepingMaplte Highly Voted 2 months, 2 weeks ago

Selected Answer: B

IAM permissions boundary policy is a managed policy that defines the maximum permissions that an identity-based policy can grant to an IAM entity (user or role). It essentially acts as a safety net to prevent users and roles from exceeding their intended permissions.

upvoted 6 times

Raphaello Most Recent 2 weeks, 4 days ago

Selected Answer: B

IAM permissions boundary definition use.

upvoted 1 times

trashbox 2 months, 1 week ago

Exam on 2023-12-18

upvoted 2 times

Raphaello 2 weeks, 4 days ago

What do you mean?

upvoted 1 times

Daniel76 2 months, 3 weeks ago

Selected Answer: B

Only B talks about restricting the access, by using permission boundary.
D - if you assign more than one role to the vendor, there's always risk that the instruction is not followed.
A, C- regardless of feasibility, by creating allow doesn't block the vendor from accessing services other than EC2 instance.

upvoted 2 times

Aamee 2 months, 4 weeks ago

Selected Answer: B

B makes more sense to me as it would explicitly define the specific service based IAM permissions policy which then can be associated with the contractor's IAM account which then help in restricting down his access to only at that service level in question.

upvoted 1 times

awssecuritynewbie 3 months ago

Selected Answer: C

he Answer should be C, creating a inline does not deny him access to everything else and it also makes it harder to manager and scale.

upvoted 1 times

awssecuritynewbie 3 months ago

the Answer should be C, creating a inline does not deny him access to everything else and it also makes it harder to manager and scale.

upvoted 1 times

YR4591 3 months, 1 week ago

Selected Answer: B

B is right

upvoted 2 times

kejam 3 months, 2 weeks ago

Answer B
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html#policies_bound

upvoted 2 times

100fold 4 months, 1 week ago

Selected Answer: B

Answer B

upvoted 2 times

kk2000 4 months, 3 weeks ago

B is the correct answer

upvoted 2 times

Question #39 *Topic 1*

A company manages multiple AWS accounts using AWS Organizations. The company's security team notices that some member accounts are not sending AWS CloudTrail logs to a centralized Amazon S3 logging bucket. The security team wants to ensure there is at least one trail configured for all existing accounts and for any account that is created in the future.

Which set of actions should the security team implement to accomplish this?

A. Create a new trail and configure it to send CloudTrail logs to Amazon S3. Use Amazon EventBridge to send notification if a trail is deleted or stopped.

B. Deploy an AWS Lambda function in every account to check if there is an existing trail and create a new trail, if needed.

C. Edit the existing trail in the Organizations management account and apply it to the organization.

D. Create an SCP to deny the cloudtrail:Delete* and cloudtrail:Stop* actions. Apply the SCP to all accounts.

Correct Answer: *C*

Community vote distribution

C (100%)

100fold Highly Voted 4 months, 1 week ago

Selected Answer: C

Answer C
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html

upvoted 6 times

Raphaello Most Recent 2 weeks, 4 days ago

Selected Answer: C

OrganizationTrail

upvoted 1 times

Daniel76 2 months, 3 weeks ago

Selected Answer: C

Only C mention the use of management account.
By editing an existing trail in their account, and apply it to an organization, an organization trail is ready to log events for the management account and all member accounts in the organization. This do away with the need to manually create and monitor trail in every accounts.

upvoted 2 times

Question #40 *Topic 1*

A company recently had a security audit in which the auditors identified multiple potential threats. These potential threats can cause usage pattern changes such as DNS access peak, abnormal instance traffic, abnormal network interface traffic, and unusual Amazon S3 API calls. The threats can come from different sources and can occur at any time. The company needs to implement a solution to continuously monitor its system and identify all these incoming threats in near-real time.
Which solution will meet these requirements?

A. Enable AWS CloudTrail logs, VPC flow logs, and DNS logs. Use Amazon CloudWatch Logs to manage these logs from a centralized account.

B. Enable AWS CloudTrail logs, VPC flow logs, and DNS logs. Use Amazon Macie to monitor these logs from a centralized account.

C. Enable Amazon GuardDuty from a centralized account. Use GuardDuty to manage AWS CloudTrail logs, VPC flow logs, and DNS logs.

D. Enable Amazon Inspector from a centralized account. Use Amazon Inspector to manage AWS CloudTrail logs, VPC flow logs, and DNS logs.

Correct Answer: *C*

Community vote distribution

C (100%)

100fold Highly Voted 4 months, 1 week ago

Selected Answer: C

Answer C

upvoted 6 times

Raphaello Most Recent 2 weeks, 4 days ago

Selected Answer: C

GuardDuty (C)

upvoted 1 times

smanzana 1 month ago

C- near-real time -> GuardDuty

upvoted 1 times

Daniel76 2 months, 3 weeks ago

Selected Answer: C

Guardduty draw data sources from: AWS CloudTrail logs, VPC flow logs, and DNS logs
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_data-sources.html
Only GuardDuty detects abnormal and unusual activities among all choices.

upvoted 3 times

Aamee 2 months, 4 weeks ago

Selected Answer: C

Monitoring threats, abnormal traffic etc always leads towards GuardDuty.

upvoted 2 times

Question #41 *Topic 1*

A company that uses AWS Organizations is using AWS IAM Identity Center (AWS Single Sign-On) to administer access to AWS accounts. A security engineer is creating a custom permission set in IAM Identity Center. The company will use the permission set across multiple accounts. An AWS managed policy and a customer managed policy are attached to the permission set. The security engineer has full administrative permissions and is operating in the management account.
When the security engineer attempts to assign the permission set to an IAM Identity Center user who has access to multiple accounts, the assignment fails.
What should the security engineer do to resolve this failure?

A. Create the customer managed policy in every account where the permission set is assigned. Give the customer managed policy the same name and same permissions in each account.

B. Remove either the AWS managed policy or the customer managed policy from the permission set. Create a second permission set that includes the removed policy. Apply the permission sets separately to the user.

C. Evaluate the logic of the AWS managed policy and the customer managed policy. Resolve any policy conflicts in the permission set before deployment.

D. Do not add the new permission set to the user. Instead, edit the user's existing permission set to include the AWS managed policy and the customer managed policy.

Correct Answer: *A*

Community vote distribution

A (73%) C (27%)

[Removed] Highly Voted 3 months ago

Selected Answer: A

Give this a read y'all. Answer indeed is A. You must create the CMP in each account unlike the AWS Managed Policies

https://aws.amazon.com/blogs/security/how-to-use-customer-managed-policies-in-aws-single-sign-on-for-advanced-use-cases/#:~:text=Configure%20an%20IAM%20Identity%20Center%20permission%20set%20to%20use%20a%20CMP

upvoted 6 times

pupsik Highly Voted 4 months ago

Selected Answer: A

https://docs.aws.amazon.com/singlesignon/latest/userguide/permissionsetcustom.html#:~:text=When%20you%20create%20a%20permission%20set%20with%20a%20customer%20managed%20policy%2C%20you%20must%20create%20an%20IAM%20policy%20with%20the%20same%20name%20and%20path%20in%20each%20AWS%20account%20where%20IAM%20Identity%20Center%20assigns%20your%20permission%20set.

upvoted 6 times

walter_white_008 Most Recent 5 days, 2 hours ago

Selected Answer: C

Answer is C.
Dont blindly accept the answer selected by most of the people, it may be wrong sometimes.
https://docs.aws.amazon.com/singlesignon/latest/userguide/permissionsetsconcept.html

IAM Identity Center assigns access to a user or group in one or more AWS accounts with permission sets. When you assign a permission set, IAM Identity Center creates corresponding IAM Identity Center-controlled IAM roles in each account, and attaches the policies specified in the permission set to those roles.

Solve the policy conflicts as per option C and you are good.

upvoted 1 times

NoCrapEva 2 weeks, 3 days ago

Selected Answer: A

Answer C - does not resolve the failure - It will only highlight where the issue is..

https://docs.aws.amazon.com/singlesignon/latest/userguide/permissionsetcustom.html
"You can attach customer managed policies to your permission set. Customer managed policies are IAM policies in your account that you create and maintain. In contrast, AWS managed policies are IAM policies in your account that AWS maintains. You can assign an customer managed policy as permissions for the role that IAM Identity Center creates, or as a permissions boundary.

When you create a permission set with a customer managed policy, you must create an IAM policy with the same name and path in each AWS account where IAM Identity Center assigns your permission set. If you are specifying a custom path, make sure to specify the same path in each AWS account. For more information, see Friendly names and paths in the IAM User Guide. IAM Identity Center attaches the IAM policy to the IAM role that it creates in your AWS account."

upvoted 1 times

Raphaello 2 weeks, 4 days ago

Selected Answer: A

Identity Center's permission set actually creates IAM role in the target (member) AWS accounts. Therefore, when you include a customer managed policy into a permission set, you need to make sure that the member accounts recognize the customer managed policy, by creating the policy and giving it same name in every AWS member acocunt.

Answer is A.

upvoted 1 times

mynickc 1 month, 1 week ago

Selected Answer: C

Answer is C. Because, when you assign a permissionset via the identity center; it automatically creates IAM controlled role in all the org.
https://docs.aws.amazon.com/singlesignon/latest/userguide/permissionsetsconcept.html

upvoted 1 times

Daniel76 2 months, 3 weeks ago

Selected Answer: A

https://docs.aws.amazon.com/singlesignon/latest/userguide/howtocmp.html

"Before you assign your permission set with IAM policies, you must prepare your member account. The name of an IAM policy in your member account must be a case-sensitive match to name of the policy in your management account. IAM Identity Center fails to assign the permission set if the policy doesn't exist in your member account."

upvoted 2 times

AWSvad 3 months, 1 week ago

The correct answer is:

C. Evaluate the logic of the AWS managed policy and the customer managed policy. Resolve any policy conflicts in the permission set before deployment.

In this scenario, the assignment of the permission set to an IAM Identity Center user is failing, indicating a potential conflict between the AWS managed policy and the customer managed policy. It is important to review and evaluate the logic of both policies and resolve any conflicts before deploying the permission set.

Options A and B suggest alternative actions but do not directly address the issue of policy conflicts. Option A involves creating the customer managed policy in every account, which may not resolve the underlying problem. Option B suggests removing either the AWS managed policy or the customer managed policy, which may not be the most appropriate solution.

Option D suggests editing the user's existing permission set, but it does not address the potential conflicts between the AWS managed policy and the customer managed policy.

Therefore, option C is the most appropriate choice to resolve the issue by thoroughly evaluating and resolving policy conflicts in the permission set before deployment.

- ChatGPT

upvoted 2 times

alexleely 1 month, 3 weeks ago

The correct answer is:

A. Create the customer managed policy in every account where the permission set is assigned. Give the customer managed policy the same name and same permissions in each account.

Explanation:

When using IAM Identity Center (AWS Single Sign-On) to administer access to AWS accounts across multiple accounts, and attaching a customer managed policy to a permission set, it's essential to create the corresponding IAM policy with the same name and permissions in each AWS account where the permission set is assigned. This ensures consistency and avoids issues during the assignment process.

Option A aligns with this requirement by recommending the creation of the customer managed policy in every account where the permission set is assigned, with the same name and permissions. This approach helps in maintaining uniformity across accounts and resolving the assignment failure.

Options B, C, and D do not directly address the need to create the customer managed policy in each account or ensure consistency across accounts, making option A the appropriate solution in this scenario.

- ChatGPT

upvoted 1 times

kejam 3 months, 2 weeks ago

Selected Answer: C

Answer C

Not A: AWS IAM Identity Center enables you to centrally manage permissions across multiple AWS accounts without configuring each account manually.
https://docs.aws.amazon.com/singlesignon/latest/userguide/manage-your-accounts.html

Not B: You can assign more than one permission set to a user.
https://docs.aws.amazon.com/singlesignon/latest/userguide/permissionsets.html

Not D: A custom permission set can use up to 10 AWS managed or customer managed policies.
https://docs.aws.amazon.com/singlesignon/latest/userguide/howtocreatepermissionset.html

upvoted 1 times

ahrentom 4 months ago

Selected Answer: C

I would go with C here, seems to be the most logical anwser

upvoted 3 times

ahrentom 3 months, 2 weeks ago

have to correct me, the right one here is A

upvoted 3 times

mynickc 1 month, 1 week ago

when you're using permissionset you don't need to create the customer managed policy in every org manually. so its C

upvoted 1 times

Question #42 *Topic 1*

A company has thousands of AWS Lambda functions. While reviewing the Lambda functions, a security engineer discovers that sensitive information is being stored in environment variables and is viewable as plaintext in the Lambda console. The values of the sensitive information are only a few characters long.
What is the MOST cost-effective way to address this security issue?

A. Set up IAM policies from the Lambda console to hide access to the environment variables.

B. Use AWS Step Functions to store the environment variables. Access the environment variables at runtime. Use IAM permissions to restrict access to the environment variables to only the Lambda functions that require access.

C. Store the environment variables in AWS Secrets Manager, and access them at runtime. Use IAM permissions to restrict access to the secrets to only the Lambda functions that require access.

D. Store the environment variables in AWS Systems Manager Parameter Store as secure string parameters, and access them at runtime. Use IAM permissions to restrict access to the parameters to only the Lambda functions that require access.

Correct Answer: *D*

Community vote distribution

D (86%) 14%

kejam Highly Voted 3 months, 2 weeks ago

Selected Answer: D

Answer D
There is no charge from Parameter Store to create a SecureString parameter.
https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-parameter-store.html#what-is-a-parameter

upvoted 5 times

100fold Highly Voted 4 months, 1 week ago

Selected Answer: D

Store the environment variables as secure strings in Parameter Store. Most cost-effective way.

upvoted 5 times

Raphaello Most Recent 2 weeks, 4 days ago

Selected Answer: D

SSM Parameter Store standard is the most cost-effective solution.

upvoted 1 times

trashbox 2 months, 1 week ago

Exam on 2023-12-18

upvoted 1 times

[Removed] 3 months ago

Selected Answer: D

cost efficient.

upvoted 1 times

stream3652 4 months ago

Selected Answer: C

Isn't C more secure?

upvoted 2 times

AgboolaKun 3 months, 3 weeks ago

That is a good question. However, the emphasis here is MOST cost-effective. Using secure string in Parameter Store is free, hence D is cost effective.

upvoted 5 times

M2ao 4 months ago

the question is asking for cost-effective way

upvoted 3 times

Question #43 *Topic 1*

A security engineer is using AWS Organizations and wants to optimize SCPs. The security engineer needs to ensure that the SCPs conform to best practices.
Which approach should the security engineer take to meet this requirement?

A. Use AWS IAM Access Analyzer to analyze the polices. View the findings from policy validation checks.

B. Review AWS Trusted Advisor checks for all accounts in the organization.

C. Set up AWS Audit Manager. Run an assessment for all AWS Regions for all accounts.

D. Ensure that Amazon Inspector agents are installed on all Amazon EC2 instances in all accounts.

Correct Answer: *A*

Community vote distribution

A (89%) 11%

Raphaello 2 weeks, 4 days ago

Selected Answer: A

IAM Access Analyzer.

upvoted 1 times

trashbox 2 months, 1 week ago

Exam on 2023-12-18

upvoted 1 times

AgboolaKun 3 months, 3 weeks ago

Selected Answer: A

You can create AWS IAM Access Analyzer in AWS Organizations as the zone of trust.
https://aws.amazon.com/blogs/aws/new-use-aws-iam-access-analyzer-in-aws-organizations/

upvoted 2 times

bannium 3 months, 4 weeks ago

Selected Answer: A

It seems IAM Access Analyzer
> This powerful new feature will help you to construct IAM policies and SCPs that take advantage of time-tested AWS best practices.
https://aws.amazon.com/jp/blogs/aws/iam-access-analyzer-update-policy-validation/

upvoted 4 times

pupsik 4 months ago

Selected Answer: A

I don't think Trusted Advisor would give insights regarding SCP configurations, hence A.

upvoted 1 times

ahrentom 4 months ago

Selected Answer: B

best practices --> Trusted Advisor

upvoted 1 times

Aamee 2 months, 3 weeks ago

No, cuz Trusted Advisor doesn't analyze anything with the SCP level so hence A is correct here.

upvoted 1 times

Question #44 *Topic 1*

A company uses Amazon RDS for MySQL as a database engine for its applications. A recent security audit revealed an RDS instance that is not compliant with company policy for encrypting data at rest. A security engineer at the company needs to ensure that all existing RDS databases are encrypted using server-side encryption and that any future deviations from the policy are detected.
Which combination of steps should the security engineer take to accomplish this? (Choose two.)

A. Create an AWS Config rule to detect the creation of unencrypted RDS databases. Create an Amazon EventBridge rule to trigger on the AWS Config rules compliance state change and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.

B. Use AWS System Manager State Manager to detect RDS database encryption configuration drift. Create an Amazon EventBridge rule to track state changes and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.

C. Create a read replica for the existing unencrypted RDS database and enable replica encryption in the process. Once the replica becomes active, promote it into a standalone database instance and terminate the unencrypted database instance.

D. Take a snapshot of the unencrypted RDS database. Copy the snapshot and enable snapshot encryption in the process. Restore the database instance from the newly created encrypted snapshot. Terminate the unencrypted database instance.

E. Enable encryption for the identified unencrypted RDS instance by changing the configurations of the existing database.

Correct Answer: *AD*

Community vote distribution

AD (100%)

ahrentom Highly Voted 4 months ago

Selected Answer: AD

A and D, here´s another source
https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automatically-remediate-unencrypted-amazon-rds-db-instances-and-clusters.html

upvoted 7 times

Raphaello Most Recent 2 weeks, 4 days ago

Selected Answer: AD

AD
Config to track drift, and taking snapshot to encrypt current RDS.

upvoted 1 times

trashbox 2 months, 1 week ago

Exam on 2023-12-18

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: AD

Answer is AD.
https://www.examtopics.com/discussions/amazon/view/60595-exam-aws-certified-security-specialty-topic-1-question-275/

upvoted 2 times

Question #45 *Topic 1*

A company has recently recovered from a security incident that required the restoration of Amazon EC2 instances from snapshots. The company uses an AWS Key Management Service (AWS KMS) customer managed key to encrypt all Amazon Elastic Block Store (Amazon EBS) snapshots. The company performs a gap analysis of its disaster recovery procedures and backup strategies. A security engineer needs to implement a solution so that the company can recover the EC2 instances if the AWS account is compromised and the EBS snapshots are deleted.
Which solution will meet this requirement?

A. Create a new Amazon S3 bucket. Use EBS lifecycle policies to move EBS snapshots to the new S3 bucket. Use lifecycle policies to move snapshots to the S3 Glacier Instant Retrieval storage class. Use S3 Object Lock to prevent deletion of the snapshots.

B. Use AWS Systems Manager to distribute a configuration that backs up all attached disks to Amazon S3.

C. Create a new AWS account that has limited privileges. Allow the new account to access the KMS key that encrypts the EBS snapshots. Copy the encrypted snapshots to the new account on a recurring basis.

D. Use AWS Backup to copy EBS snapshots to Amazon S3. Use S3 Object Lock to prevent deletion of the snapshots.

Correct Answer: *C*

Community vote distribution

C (75%) D (17%) 8%

Raphaello 4 days, 12 hours ago

Selected Answer: A

Option A seems very good solution to me!

C is a fine solution, but why not A? What makes A less appealing than C?!!!

In fact, using Glacier Vault Lock is the ONLY way to protect against data deletion, and even after moving snapshots/backups to a different account, Glacier Vault Lock would be required to protect against data deletion from the new account.

upvoted 1 times

Raphaello 4 days, 12 hours ago

Sorry, that's the answer for a different question.

For this one, C is the best option

upvoted 1 times

walter_white_008 5 days, 1 hour ago

Selected Answer: C

C makes sense.

upvoted 1 times

Raphaello 2 weeks, 4 days ago

Selected Answer: C

This is a bit vague.
1. If the fear to lose account A, and subsequently the encrypted snapshots, that would apply to KMS keys used for snapshot encryption.
2. A solution to backup the encrypted snapshots to a different account, B, has to include creating new KMS key in account B, and not just access to KMS key in account A, cause it is subject to the fear of being compromised as well.
3. Answer C is the only one that taking KMS key into consideration, even if not in an ideal way. I would go with C only for that fact, and it mentioned a new account.

upvoted 2 times

Th3Dud3 1 month, 3 weeks ago

c. You can add a vault lock to your AWS Backup Vault. So no need to use S3 object lock.

upvoted 1 times

confusedyeti69 2 months, 3 weeks ago

How compromise is compromised? You wouldn't have access to KMS if you choose C and your snapshots are in the same account if you choose D.

upvoted 1 times

Aamee 2 months, 3 weeks ago

This statement in option C "Allow the new account to access the KMS key that encrypts the EBS snapshots" clearly means that when you're creating a new account for a backup solution, you also have the appropriate 'Access' to encrypt and decrypt the keys as well. That's why it's further said to copy out the encrypted snapshots in the new account too for performing any future decrypt operations.

Hope it helps..

upvoted 1 times

confusedyeti69 2 months, 2 weeks ago

If you store the snapshot in account B that is encrypted with account A's key, and then lose access to the key (compromised), would you still be able to use the snapshot?

upvoted 1 times

Daniel76 2 months ago

The key is in the KMS and account B has access to it.
if account A is gone, account B can still decrypt the snapshot, provided the account A did not have the right to delete this key in the KMS..

upvoted 1 times

Daniel76 2 months, 3 weeks ago

Selected Answer: C

You cant use D because the snapshot can still be deleted even if under compliance mode, if the compromised AWS account is deleted.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html

upvoted 1 times

awssecuritynewbie 3 months ago

but if the AWS account is compromised and they are worried about the AWS account being deleted...so it will lose the KMS key as well. It is a tricky question the S3 lock is not enough because you will lose the KMS keys.. but it should have a solution to copy the keys into the new account as well.

upvoted 1 times

NoCrapEva 2 weeks, 3 days ago

The question only says Account compromised (not deleted)... But the question specifically asks you "...to implement a solution so that the company can recover the EC2 instances" IF ..."the EBS snapshots are deleted"
Therefore only Answer C will allow this

upvoted 1 times

AgboolaKun 3 months, 3 weeks ago

Selected Answer: C

C is the correct answer to me.

New AWS account with limited privileges - prevents the account from being compromised
Access to AWS KMS key - access to the key to decrypt data in the recovery account.
Copy snapshots to the recovery account (new account) on a recurring basis - This could be using AWS Backup as well or any other services.

upvoted 1 times

pupsik 4 months ago

Selected Answer: D

"Use S3 Object Lock to prevent deletion of the snapshots." makes this option vert viable, even if account gets compromised.

upvoted 2 times

AgboolaKun 3 months, 3 weeks ago

The only concern I have with D is that there is no mention of how to access the AWS KMS CMK key used for the encryption of EBS snpshots. Therefore, I will go for C.

upvoted 2 times

confusedyeti69 2 months, 3 weeks ago

It is creating a snapshot and storing it in S3 of the same account, there is no need for any KMS policy to be explicitly mention in the answer. But like another previous comment mentioned, it would be better to backup the keys as well if storing the backup snapshot in another account. I vote D as answer.

upvoted 1 times

bannium 3 months, 4 weeks ago

How I can export ebs Snapshot data to S3 bucket using AWS Backup?

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: C

Answer C. The wording is rearranged, but same answer selections.
https://www.examtopics.com/discussions/amazon/view/69464-exam-aws-certified-security-specialty-topic-1-question-315/

upvoted 4 times

Question #46 *Topic 1*

A company's security engineer is designing an isolation procedure for Amazon EC2 instances as part of an incident response plan. The security engineer needs to isolate a target instance to block any traffic to and from the target instance, except for traffic from the company's forensics team. Each of the company's EC2 instances has its own dedicated security group. The EC2 instances are deployed in subnets of a VPC. A subnet can contain multiple instances.
The security engineer is testing the procedure for EC2 isolation and opens an SSH session to the target instance. The procedure starts to simulate access to the target instance by an attacker. The security engineer removes the existing security group rules and adds security group rules to give the forensics team access to the target instance on port 22.
After these changes, the security engineer notices that the SSH connection is still active and usable. When the security engineer runs a ping command to the public IP address of the target instance, the ping command is blocked.
What should the security engineer do to isolate the target instance?

A. Add an inbound rule to the security group to allow traffic from 0.0.0.0/0 for all ports. Add an outbound rule to the security group to allow traffic to 0.0.0.0/0 for all ports. Then immediately delete these rules.

B. Remove the port 22 security group rule. Attach an instance role policy that allows AWS Systems Manager Session Manager connections so that the forensics team can access the target instance.

C. Create a network ACL that is associated with the target instance's subnet. Add a rule at the top of the inbound rule set to deny all traffic from 0.0.0.0/0. Add a rule at the top of the outbound rule set to deny all traffic to 0.0.0.0/0.

D. Create an AWS Systems Manager document that adds a host-level firewall rule to block all inbound traffic and outbound traffic. Run the document on the target instance.

Correct Answer: *B*

Community vote distribution

B (73%) A (18%) 9%

yedaselself 1 month, 2 weeks ago

Selected Answer: A

Answer is A. It is about connection tracking. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-connection-tracking.html#untracked-connections
B is not relevant because question doesn't asks a way to connect to instance it asks why a tracked connection is not interrupted when security group rules changed.

upvoted 2 times

rxhan 6 days, 9 hours ago

Always use AWS products for the answer, why would you allow full access just to ping and remove.

upvoted 1 times

dodino 1 month, 2 weeks ago

but the question says "The security engineer removes the existing security group rules and adds security group rules to give the forensics team access to the target instance on port 22." so this practice was already done for the port 22...

upvoted 1 times

Daniel76 2 months ago

Selected Answer: B

To isolate a specific EC2, security group is the way to go as it can affect targeted instance not the entire network.
A does not make sense, as security group is stateful network control.
B is using security group to isolate the EC2, and using session manager ensure exclusive access via management console.

upvoted 1 times

trashbox 2 months, 1 week ago

Exam on 2023-12-18

upvoted 1 times

Aamee 2 months, 3 weeks ago

Selected Answer: B

No doubt, it's B.

upvoted 1 times

AgboolaKun 3 months, 3 weeks ago

Selected Answer: B

There is no need for SSH port 22 since Systems Manager Session Manager can give the necessary access that the security team needs to the EC2 instances.

upvoted 4 times

tatarevick 3 months, 3 weeks ago

Selected Answer: B

There can be multiple ec2 instances per subnet and C would block access to ALL of them. It is B

upvoted 2 times

snowmaggedon 4 months ago

Definitely B

upvoted 3 times

M2ao 4 months ago

Selected Answer: C

shoud be C

upvoted 1 times

Aamee 2 months, 4 weeks ago

It can't be C for sure since it will block all ingress and outgress connections from the subnet level via NACL changes... that's not what's the ask is for in this use case... Def. it's B IMO.

upvoted 1 times

snowmaggedon 4 months ago

There can be multiple ec2 instances per subnet and C would block access to ALL of them. It is B

upvoted 3 times

Question #47 *Topic 1*

A startup company is using a single AWS account that has resources in a single AWS Region. A security engineer configures an AWS CloudTrail trail in the same Region to deliver log files to an Amazon S3 bucket by using the AWS CLI.
Because of expansion, the company adds resources in multiple Regions. The security engineer notices that the logs from the new Regions are not reaching the S3 bucket.
What should the security engineer do to fix this issue with the LEAST amount of operational overhead?

A. Create a new CloudTrail trail. Select the new Regions where the company added resources.

B. Change the S3 bucket to receive notifications to track all actions from all Regions.

C. Create a new CloudTrail trail that applies to all Regions.

D. Change the existing CloudTrail trail so that it applies to all Regions.

Correct Answer: *B*

Community vote distribution

D (100%)

kk2000 Highly Voted 4 months, 3 weeks ago
Correct Answer is D
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/receive-cloudtrail-log-files-from-multiple-regions.html
upvoted 10 times

Raphaello Most Recent 2 weeks, 4 days ago
Selected Answer: D
Change CloudTrail trail to ne multi-region.
upvoted 1 times

brpjp 2 months, 4 weeks ago
Question is new region trail not reaching to s3 bucket and not trail created from new region.
upvoted 1 times

smanzana 1 month, 1 week ago
But each trail is independent and its region cannot be changed after the initial configuration…and the answer D says “change the trail” not “create a new trail”
upvoted 1 times

Aamee 2 months, 3 weeks ago
Question specifically emphasis on the solution with 'LEAST amount of operational overhead' which is doable only through option D. All other options still involves some kind of operational overhead. Hope it helps..
upvoted 1 times

ahrentom 4 months ago
Selected Answer: D
go with D
upvoted 2 times

100fold 4 months, 1 week ago
Selected Answer: D
Agree answer is D. Change the existing CloudTrail using AWS CLI, add the --is-multi-region-trail option to the update-trail command.
upvoted 3 times

Question #48 *Topic 1*

A company's public Application Load Balancer (ALB) recently experienced a DDoS attack. To mitigate this issue, the company deployed Amazon CloudFront in front of the ALB so that users would not directly access the Amazon EC2 instances behind the ALB.
The company discovers that some traffic is still coming directly into the ALB and is still being handled by the EC2 instances.
Which combination of steps should the company take to ensure that the EC2 instances will receive traffic only from CloudFront? (Choose two.)

A. Configure CloudFront to add a cache key policy to allow a custom HTTP header that CloudFront sends to the ALB.

B. Configure CloudFront to add a custom HTTP header to requests that CloudFront sends to the ALB.

C. Configure the ALB to forward only requests that contain the custom HTTP header.

D. Configure the ALB and CloudFront to use the X-Forwarded-For header to check client IP addresses.

E. Configure the ALB and CloudFront to use the same X.509 certificate that is generated by AWS Certificate Manager (ACM).

Correct Answer: *BC*

Community vote distribution

BC (100%)

100fold Highly Voted 4 months, 1 week ago

Selected Answer: BC

Answer is BC.
https://www.examtopics.com/discussions/amazon/view/88447-exam-aws-certified-security-specialty-topic-1-question-437/

upvoted 5 times

xusang Most Recent 5 days, 21 hours ago

Selected Answer: BC

Restricting access to Application Load Balancers：https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/restrict-access-to-load-balancer.html

upvoted 1 times

Raphaello 2 weeks, 4 days ago

Selected Answer: BC

BC
Add custom origin-request header (CloudFron > ALB), set ALB to only accept request with such HTTP header.

upvoted 1 times

Aamee 2 months, 3 weeks ago

Selected Answer: BC

W/o any doubt..

upvoted 1 times

Daniel76 2 months, 3 weeks ago

Selected Answer: BC

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/example-function-add-true-client-ip-header.html
https://aws.amazon.com/blogs/security/three-most-important-aws-waf-rate-based-rules/

upvoted 1 times

Question #49 *Topic 1*

A company discovers a billing anomaly in its AWS account. A security consultant investigates the anomaly and discovers that an employee who left the company 30 days ago still has access to the account. The company has not monitored account activity in the past.
The security consultant needs to determine which resources have been deployed or reconfigured by the employee as quickly as possible.
Which solution will meet these requirements?

A. In AWS Cost Explorer, filter chart data to display results from the past 30 days. Export the results to a data table. Group the data table by resource.

B. Use AWS Cost Anomaly Detection to create a cost monitor. Access the detection history. Set the time frame to Last 30 days. In the search area, choose the service category.

C. In AWS CloudTrail, filter the event history to display results from the past 30 days. Create an Amazon Athena table that contains the data. Partition the table by event source.

D. Use AWS Audit Manager to create an assessment for the past 30 days. Apply a usage-based framework to the assessment. Configure the assessment to assess by resource.

Correct Answer: *B*

Community vote distribution

C (100%)

100fold Highly Voted 4 months, 1 week ago

Selected Answer: C

Answer C. CloudTrail for as quickly as possible. Look up events related to the creation, modification, or deletion of resources in your AWS account.

AWS Cost Anomaly Detection: For a new service subscription, 10 days of historical service usage data is needed before anomalies can be detected for that service. If you create a new monitor, it can take up to 24 hours to begin detecting new anomalies.

upvoted 8 times

Raphaello Most Recent 2 weeks, 3 days ago

Selected Answer: C

To investigate a certain user and find what resources that IAM user created over past period, CloudTrail is the tool to use.

upvoted 1 times

awssecuritynewbie 3 weeks, 2 days ago

Selected Answer: C

I think C is the best answer but Athena is over kill

upvoted 1 times

WeepingMaplte 2 months, 2 weeks ago

Think only Cloudtrail records down resources reconfigured by the employee.

upvoted 1 times

Daniel76 2 months, 3 weeks ago

Selected Answer: C

The investigation was triggered by cost anomaly but that is not the only concern. The security engineer needs to find out what has been deployed as well as reconfigured, so AWS Cost explorer or Anomaly detection will not do the job. Only CloudTrail and Anthena will be the most effective method. Cost should have nothing to do with compliance so audit manager will not help.

upvoted 2 times

Ernestokoro 3 months, 1 week ago

Ans is B! Please see link below: https://docs.aws.amazon.com/cost-management/latest/userguide/getting-started-ad.html

upvoted 1 times

Aamee 3 months ago

Don't think it can be B. See this comment above:
"AWS Cost Anomaly Detection: For a new service subscription, 10 days of historical service usage data is needed before anomalies can be detected for that service. If you create a new monitor, it can take up to 24 hours to begin detecting new anomalies."

upvoted 2 times

Question #50 *Topic 1*

A security engineer is checking an AWS CloudFormation template for vulnerabilities. The security engineer finds a parameter that has a default value that exposes an application's API key in plaintext. The parameter is referenced several times throughout the template. The security engineer must replace the parameter while maintaining the ability to reference the value in the template.
Which solution will meet these requirements in the MOST secure way?

A. Store the API key value as a SecureString parameter in AWS Systems Manager Parameter Store. In the template, replace all references to the value with {{resolve:ssm:MySSMParameterName:1}}.

B. Store the API key value in AWS Secrets Manager. In the template, replace all references to the value with {{resolve:secretsmanager:MySecretId:SecretString}}.

C. Store the API key value in Amazon DynamoDB. In the template, replace all references to the value with {{resolve:dynamodb:MyTableName:MyPrimaryKey}}.

D. Store the API key value in a new Amazon S3 bucket. In the template, replace all references to the value with {{resolve:s3:MyBucketName:MyObjectName}}.

Correct Answer: *A*

Community vote distribution

B (100%)

100fold Highly Voted 4 months, 1 week ago

Selected Answer: B

Agree answer B.

Not A. {{resolve:ssm:MySSMParameterName:1}}
ssm: Systems Manager Parameter Store plaintext parameter.
ssm-secure: Systems Manager Parameter Store secure string parameter.

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/dynamic-references.html

upvoted 9 times

dexterryu Most Recent 2 months, 1 week ago

This is a bit of a trick question. A is correct outside of the syntax in the ssm reference. Therefor B. Had it been resolve:ssm-secure:MySSMParam then A would be correct.

upvoted 2 times

Raphaello 2 weeks, 3 days ago

Spot on.
ssm: Systems Manager Parameter Store plaintext parameter.
ssm-secure: Systems Manager Parameter Store secure string parameter.

Option B is the right answer.

upvoted 1 times

Aamee 2 months, 3 weeks ago

Selected Answer: B

MOST secure way..

upvoted 2 times

confusedyeti69 2 months, 3 weeks ago

Selected Answer: B

Secure. B

upvoted 1 times

kk2000 4 months, 3 weeks ago

Answer: B using secrets manager.(More secure way)
https://docs.aws.amazon.com/secretsmanager/latest/userguide/cfn-example_reference-secret.html

upvoted 4 times

AgboolaKun 4 months, 1 week ago

Agree. SSM can create secure API string as well but the emphasis here is on MOST secure. Therefore, Secret Manager is the answer.

upvoted 3 times

Question #51 *Topic 1*

A company's AWS CloudTrail logs are all centrally stored in an Amazon S3 bucket. The security team controls the company's AWS account. The security team must prevent unauthorized access and tampering of the CloudTrail logs.
Which combination of steps should the security team take? (Choose three.)

A. Configure server-side encryption with AWS KMS managed encryption keys (SSE-KMS).

B. Compress log files with secure gzip.

C. Create an Amazon EventBridge rule to notify the security team of any modifications on CloudTrail log files.

D. Implement least privilege access to the S3 bucket by configuring a bucket policy.

E. Configure CloudTrail log file integrity validation.

F. Configure Access Analyzer for S3.

Correct Answer: *ADE*

Community vote distribution

ADE (100%)

Raphaello 2 weeks, 3 days ago

Selected Answer: ADE

ADE
We agree.

upvoted 1 times

Aamee 3 months ago

Selected Answer: ADE

Here's what it describes about the usage of log file integration and the SSE-KMS usecase scenario:

"If you use SSE-KMS and log file validation, and you have modified your Amazon S3 bucket policy to only allow SSE-KMS encrypted files, you will not be able to create trails that utilize that bucket unless you modify your bucket policy to specifically allow AES256 encryption, as shown in the following example policy line.

"StringNotEquals": { "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"] }
"

upvoted 2 times

ahrentom 4 months ago

Selected Answer: ADE

ADE
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html

upvoted 3 times

Question #52 *Topic 1*

A company has several petabytes of data. The company must preserve this data for 7 years to comply with regulatory requirements. The company's compliance team asks a security officer to develop a strategy that will prevent anyone from changing or deleting the data.
Which solution will meet this requirement MOST cost-effectively?

A. Create an Amazon S3 bucket. Configure the bucket to use S3 Object Lock in compliance mode. Upload the data to the bucket. Create a resource-based bucket policy that meets all the regulatory requirements.

B. Create an Amazon S3 bucket. Configure the bucket to use S3 Object Lock in governance mode. Upload the data to the bucket. Create a user-based IAM policy that meets all the regulatory requirements.

C. Create a vault in Amazon S3 Glacier. Create a Vault Lock policy in S3 Glacier that meets all the regulatory requirements. Upload the data to the vault.

D. Create an Amazon S3 bucket. Upload the data to the bucket. Use a lifecycle rule to transition the data to a vault in S3 Glacier. Create a Vault Lock policy that meets all the regulatory requirements.

Correct Answer: *D*

Community vote distribution

C (75%) A (25%)

Raphaello 2 weeks, 3 days ago

Selected Answer: C

The data is already there, we just want to keep it for COMPLIANCE for SEVEN years.
There's no need to place the date in S3 bucket then use lifecycle to move it to Glacier.
Option C is correct.

upvoted 1 times

trashbox 2 months, 1 week ago

Exam on 2023-12-18

upvoted 1 times

kejam 3 months, 2 weeks ago

Selected Answer: C

https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-lock-policy.html

upvoted 1 times

cjkuga 3 months, 3 weeks ago

Selected Answer: C

Both A and C work here but C is the MOST cost-effective.

upvoted 4 times

pupsik 4 months ago

Selected Answer: A

Question doesn't ask for a backup solution, so Glacier is not a good fir here.

upvoted 2 times

Aamee 3 months ago

No, it clearly states that "The company must preserve this data for 7 years"... so how would you keep such large data safe and specifically complianced with all the regulatory reqs. That's why going with C here.

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: C

Correction, answer C

upvoted 2 times

AgboolaKun 4 months, 1 week ago

Selected Answer: C

The correct answer here is C. This option ticks all the boxes.

Several petabytes of data + 7 years + Regulatory Compliance + MOST cost-effective solution.

D is close but we don't S3 at all.

upvoted 1 times

100fold 4 months, 1 week ago

Thanks AgboolKun! What are your thoughts on #49?
Agree with answer C as well. Can set the policy on Vault Lock that cannot be altered.
https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-access-policy.html

upvoted 2 times

AgboolaKun 3 months, 3 weeks ago

@100fold, I agree with your answer (C) in #49. There is no better option to C!!

I upvoted your answer already!!

upvoted 1 times

100fold 3 months, 3 weeks ago

@AgboolaKun, I sat the exam Friday and marked 926. 80% from this study were on my exam. 6-7 new questions, one related to AWS KMS keyrings. Good luck everyone!

upvoted 5 times

AgboolaKun 3 months, 2 weeks ago

Wow!! Congratulations!! I am happy for you. I will be sitting for the exam soon. I will let you know!!

upvoted 1 times

100fold 3 months, 1 week ago

@AgboolKun. Awesome! All The Best wishes throughout your career 👍

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: A

Answer A.
Compliance mode will prevent anyone from changing or deleting the data including the root user. Requested by the company's compliance team.

https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html

upvoted 1 times

100fold 4 months, 1 week ago

Correction to Answer C.
https://docs.aws.amazon.com/amazonglacier/latest/dev/vault-access-policy.html

upvoted 1 times

Question #53 *Topic 1*

A-company uses a third-party identity provider and SAML-based SSO for its AWS accounts. After the third-party identity provider renewed an expired signing certificate, users saw the following message when trying to log in:
Error: Response Signature Invalid (Service: AWSSecurityTokenService; Status Code: 400; Error Code: InvalidIdentityToken)
A security engineer needs to provide a solution that corrects the error and minimizes operational overhead.
Which solution meets these requirements?

A. Upload the third-party signing certificate's new private key to the AWS identity provider entity defined in AWS Identity and Access Management (IAM) by using the AWS Management Console.

B. Sign the identity provider's metadata file with the new public key. Upload the signature to the AWS identity provider entity defined in AWS Identity and Access Management (IAM) by using the AWS CLI.

C. Download the updated SAML metadata file from the identity service provider. Update the file in the AWS identity provider entity defined in AWS Identity and Access Management (IAM) by using the AWS CLI.

D. Configure the AWS identity provider entity defined in AWS Identity and Access Management (IAM) to synchronously fetch the new public key by using the AWS Management Console.

Correct Answer: *C*

Community vote distribution

C (100%)

100fold Highly Voted 4 months, 1 week ago

Selected Answer: C

Answer C.

https://docs.aws.amazon.com/IAM/latest/UserGuide/troubleshoot_saml.html#troubleshoot_saml_invalid-metadata
https://www.examtopics.com/discussions/amazon/view/69166-exam-aws-certified-security-specialty-topic-1-question-292/

upvoted 8 times

Raphaello Most Recent 2 weeks, 3 days ago

Selected Answer: C

Download the updated SAML metadata file from your identity service provider, then update it in AWS.

upvoted 1 times

yorkicurke 2 months ago

Selected Answer: C

nice link by user: 100fold
thanks bud

upvoted 1 times

awssecuritynewbie 2 months, 3 weeks ago

Selected Answer: C

C is the correct answer

upvoted 1 times

Question #54 *Topic 1*

A company has several workloads running on AWS. Employees are required to authenticate using on-premises ADFS and SSO to access the AWS Management Console. Developers migrated an existing legacy web application to an Amazon EC2 instance. Employees need to access this application from anywhere on the internet, but currently, there is no authentication system built into the application.
How should the security engineer implement employee-only access to this system without changing the application?

A. Place the application behind an Application Load Balancer (ALB). Use Amazon Cognito as authentication for the ALB. Define a SAML-based Amazon Cognito user pool and connect it to ADFS.

B. Implement AWS IAM Identity Center (AWS Single Sign-On) in the management account and link it to ADFS as an identity provider. Define the EC2 instance as a managed resource, then apply an IAM policy on the resource.

C. Define an Amazon Cognito identity pool, then install the connector on the Active Directory server. Use the Amazon Cognito SDK on the application instance to authenticate the employees using their Active Directory user names and passwords.

D. Create an AWS Lambda custom authorizer as the authenticator for a reverse proxy on Amazon EC2. Ensure the security group on Amazon EC2 only allows access from the Lambda function.

Correct Answer: *A*

Community vote distribution

A (100%)

100fold Highly Voted 4 months, 1 week ago

Selected Answer: A

Answer A.

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html
https://www.examtopics.com/discussions/amazon/view/30063-exam-aws-certified-security-specialty-topic-1-question-143/

upvoted 9 times

Raphaello Most Recent 2 weeks, 3 days ago

Selected Answer: A

Add SAML IdP to Cognito user pool.
https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-configuring-federation-with-saml-2-0-idp.html

upvoted 1 times

Question #55 *Topic 1*

A company is using AWS to run a long-running analysis process on data that is stored in Amazon S3 buckets. The process runs on a fleet of Amazon EC2 instances that are in an Auto Scaling group. The EC2 instances are deployed in a private subnet of a VPC that does not have internet access. The EC2 instances and the S3 buckets are in the same AWS account.
The EC2 instances access the S3 buckets through an S3 gateway endpoint that has the default access policy. Each EC2 instance is associated with an instance profile role that has a policy that explicitly allows the s3:GetObject action and the s3:PutObject action for only the required S3 buckets.
The company learns that one or more of the EC2 instances are compromised and are exfiltrating data to an S3 bucket that is outside the company's organization in AWS Organizations. A security engineer must implement a solution to stop this exfiltration of data and to keep the EC2 processing job functional.
Which solution will meet these requirements?

A. Update the policy on the S3 gateway endpoint to allow the S3 actions only if the values of the aws:ResourceOrgID and aws:PrincipalOrgID condition keys match the company's values.

B. Update the policy on the instance profile role to allow the S3 actions only if the value of the aws:ResourceOrgID condition key matches the company's value.

C. Add a network ACL rule to the subnet of the EC2 instances to block outgoing connections on port 443.

D. Apply an SCP on the AWS account to allow the S3 actions only if the values of the aws:ResourceOrgID and aws:PrincipalOrgID condition keys match the company's values.

Correct Answer: *B*

Community vote distribution

D (45%) A (27%) B (27%)

kejam Highly Voted 3 months, 2 weeks ago

Selected Answer: D

Answer D based on the syntax of these answers.

A. This could work, but you don't need aws:ResourceOrgID and aws:PrincipalOrgID You can add allowed buckets (internal or external) as needed which is much more flexible IMO. https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html#edit-vpc-endpoint-policy-s3

B. This doesn't prevent S3 actions on external accounts.

C. This does nothing as the S3 endpoint is inside the VPC.

D. This solution matches the answer exactly.
Example 3: https://aws.amazon.com/blogs/security/how-to-control-access-to-aws-resources-based-on-aws-account-ou-or-organization/

upvoted 9 times

Raphaello 1 week ago

In fact Example 3 Restrict access to AWS resources (in this case S3) within my organization, which means denying access from principals (e.g. EC2 instance roles) that do not belong to S3 Org. That example does not correspond to what we need to do here!
"Deny",
"Action": "s3:*",
"Resource": "arn:aws:s3:::*/*",
"Condition": { "StringNotEquals": { "aws:ResourceOrgID": "${aws:PrincipalOrgID}"}
Note the "PrincipalOrgID" is a variable.

Whereas, we basically want our own EC2 instances not to access S3 that belong to another account.
"Allow",
"Action": "s3:*",
"Resource": "arn:aws:s3:::*/*",
"Condition": {"StringEquals": {"aws:PrincipalOrgID": ["o-yyyyyyyyyy"]}
Or
maybe even add an explicit deny statement if the "aws:ResourceOrgID" does not equal my Org ID "0-yyyyyyyyyy".

upvoted 1 times

NoCrapEva 2 weeks ago

Also the question states the company has AWS Organisations - therefore any policy restrictions SHOULD be done at the Organisation level - In this case with a SCP

upvoted 1 times

AgboolaKun 3 months, 2 weeks ago

I agree totally. I have always thought that D is the correct answer but I could not locate any supported documentation online. Thank you for providing the link. The example 3 in the link as you pointed out tallies with the scenario in this question.

upvoted 1 times

100fold Highly Voted 4 months, 1 week ago

D
https://aws.amazon.com/blogs/security/how-to-control-access-to-aws-resources-based-on-aws-account-ou-or-organization/

upvoted 6 times

Raphaello Most Recent 2 weeks, 3 days ago

Selected Answer: B

The problem is that EC2 instance exfiltrating data to an S3 bucket that is outside the company's organization in AWS Organizations.
So we need to make sure those instance cannot put the data to an external account's bucket.

Therefore, we need to restrict access ONLY to resources within an organization using condition "aws:ResourceOrgID".

Remember, it is not about controlling access to our own S3 bucket. It is about stopping EC2 instances from exfiltrate our data to accounts outside our Org.

Option B is the correct answer.

upvoted 1 times

LazyAutonomy 3 weeks ago

Selected Answer: A

Answer is A.
D is wrong because attackers wont use EC2 instance credentials to exfil data - no attacker is that stupid.

upvoted 1 times

LazyAutonomy 3 weeks ago

https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html#edit-vpc-endpoint-policy-s3
https://developer.squareup.com/blog/adopting-aws-vpc-endpoints-at-square/

upvoted 1 times

mark16dc 3 weeks, 1 day ago

Given the effectiveness and direct impact on preventing data exfiltration to external S3 buckets, Option D is the correct solution. It leverages the organizational control provided by AWS Organizations to enforce policy restrictions at the account level, ensuring that S3 actions are confined to the company's organizational boundaries, thus meeting the security requirements without disrupting the EC2 processing jobs.

upvoted 1 times

RNan 1 month, 3 weeks ago

Answer: B
The compromised EC2 instances are exfiltrating data to an S3 bucket outside the company's organization. By updating the policy on the instance profile role, you can restrict the S3 actions to only allow access to the required S3 buckets within the company's organization.

upvoted 1 times

Daniel76 1 month, 3 weeks ago

Selected Answer: D

Between A and D, A must be ruled out because:
"An endpoint policy does not override or replace identity-based policies or resource-based policies. " So, either the compromised ec2 instance or the external s3 can override the endpoint policy.
https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-access.html

upvoted 1 times

DebbieB67 1 month, 4 weeks ago

Selected Answer: D

Answer D

upvoted 1 times

yorkicurke 2 months ago

Selected Answer: A

This ensures that only resources from within the company's AWS Organization can access the S3 bucket through the endpoint. This prevents any exfiltration of data from compromised EC2 instances to external S3 buckets, while STILL allowing the processing job on the instances to function normally by accessing the company's internal S3 resources through the private endpoint.
https://repost.aws/questions/QU2Qx3s51DQ9SyrlWueh9L_Q/restrict-access-to-s3-bucket

upvoted 1 times

Oralinux 2 months, 1 week ago

Answer B

upvoted 1 times

1c7c461 2 months, 1 week ago

Selected Answer: B

The answer is B. You all missed the part that EC2 instance is compromised. The restriction has to be added to the instance profile of the ec2 instance to restrict which S3 buckets it can connect to. This question is about limiting access from EC2 to external S3 buckets.

upvoted 5 times

WeepingMaplte 2 months, 2 weeks ago

Selected Answer: A

I will go with A although D is also a possible method.

upvoted 1 times

Aamee 2 months, 3 weeks ago

Selected Answer: D

D is the correct option.

upvoted 2 times

snowmaggedon 2 months, 3 weeks ago

D. I have seen this is many other practice tests.

upvoted 1 times

awssecuritynewbie 2 months, 3 weeks ago

Selected Answer: A

if they are exfiltrating data via the EC2 to a S3 bucket, then ACL will not help either SCP, you would need to modify the S3 endpoint so allow access to only the Aws Org and not other S3 buckets in AWS.
Answer would be A:

upvoted 2 times

marco25 2 months, 3 weeks ago

Selected Answer: D

Choosing between a and D, A has the issue of not able to prevent direct we access bypassing the gateway.So voted d

upvoted 2 times

marlonchin 3 months ago

Does this Q mention any company resources needed to access the S3? EC2 access only through the S3 gateway endpoint. I think it should be A

upvoted 1 times

Question #56 *Topic 1*

A company that operates in a hybrid cloud environment must meet strict compliance requirements. The company wants to create a report that includes evidence from on-premises workloads alongside evidence from AWS resources. A security engineer must implement a solution to collect, review, and manage the evidence to demonstrate compliance with company policy.
Which solution will meet these requirements?

A. Create an assessment in AWS Audit Manager from a prebuilt framework or a custom framework. Upload manual evidence from the on-premises workloads. Add the evidence to the assessment. Generate an assessment report after Audit Manager collects the necessary evidence from the AWS resources.

B. Install the Amazon CloudWatch agent on the on-premises workloads. Use AWS Config to deploy a conformance pack from a sample conformance pack template or a custom YAML template. Generate an assessment report after AWS Config identifies noncompliant workloads and resources.

C. Set up the appropriate security standard in AWS Security Hub. Upload manual evidence from the on-premises workloads. Wait for Security Hub to collect the evidence from the AWS resources. Download the list of controls as a .csv file.

D. Install the Amazon CloudWatch agent on the on-premises workloads. Create a CloudWatch dashboard to monitor the on-premises workloads and the AWS resources. Run a query on the workloads and resources. Download the results.

Correct Answer: *C*

Community vote distribution

A (100%)

Raphaello 2 weeks, 3 days ago

Selected Answer: A

AWS Audit Manager helps you to collect evidences as per a selected framework.
Option A is correct.

upvoted 1 times

WeepingMaplte 2 months, 2 weeks ago

Selected Answer: A

The keyword in the question is "evidence". AWS Audit Manager manages evidences.
https://docs.aws.amazon.com/audit-manager/latest/userguide/what-is.html

upvoted 2 times

confusedyeti69 2 months, 3 weeks ago

Selected Answer: A

voted A

upvoted 1 times

brpjp 2 months, 4 weeks ago

Requirement is company policy compliance, which security hub supports and not Audit Manager. C is correct answer.

upvoted 2 times

Aamee 2 months, 3 weeks ago

Source for this statement pls?... See the below Audit Manager link which justifies option A instead:
https://aws.amazon.com/blogs/aws/aws-audit-manager-simplifies-audit-preparation/

upvoted 2 times

100fold 4 months, 1 week ago

Selected Answer: A

Answer A

upvoted 4 times

kk2000 4 months, 3 weeks ago

A
https://aws.amazon.com/blogs/aws/aws-audit-manager-simplifies-audit-preparation/

upvoted 4 times

Question #57 *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"
                }
            }
        }
    ]
}
```

Correct Answer: *B*

Community vote distribution

C (100%)

100fold Highly Voted 4 months, 1 week ago

Selected Answer: C

Answer C

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_deny-requested-region.html

upvoted 6 times

Raphaello Most Recent 6 days, 14 hours ago

Selected Answer: C

The request is to restrict (deny) use of services outside a specific region, therefore an "allow" policy for that specific region is not enough.

Option C does just that, it denies all services if the "requested region" is no the specific one.

upvoted 1 times

rahav 2 months ago

Selected Answer: C

Answer is C

upvoted 1 times

lmimi 3 months, 1 week ago

Why not A? C is just not denied, but not explicit allow.

upvoted 1 times

Aamee 3 months ago

A can't be correct since the 'Deny' always takes the precedence over 'Allow' if any similar SID policy statement is defined. The option C looks correct since it denies the access of the aws resources explicitly through the condition that 'IF' the region is not equal to 'us-east-1'. Since the question states that the access restriction should be limited to just us-east-1 region only.

upvoted 2 times

kk2000 4 months, 3 weeks ago

C is Correct

upvoted 2 times

Question #58 *Topic 1*

A company has a web server in the AWS Cloud. The company will store the content for the web server in an Amazon S3 bucket. A security engineer must use an Amazon CloudFront distribution to speed up delivery of the content. None of the files can be publicly accessible from the S3 bucket directly.
Which solution will meet these requirements?

A. Configure the permissions on the individual files in the S3 bucket so that only the CloudFront distribution has access to them.

B. Create an origin access control (OAC). Associate the OAC with the CloudFront distribution. Configure the S3 bucket permissions so that only the OAC can access the files in the S3 bucket.

C. Create an S3 role in AWS Identity and Access Management (IAM). Allow only the CloudFront distribution to assume the role to access the files in the S3 bucket.

D. Create an S3 bucket policy that uses only the CloudFront distribution ID as the principal and the Amazon Resource Name (ARN) as the target.

Correct Answer: *B*

Community vote distribution

B (100%)

100fold Highly Voted 4 months, 1 week ago

Selected Answer: B

Answer B.
Amazon CloudFront introduces Origin Access Control (OAC)
https://aws.amazon.com/blogs/networking-and-content-delivery/amazon-cloudfront-introduces-origin-access-control-oac/

upvoted 9 times

Raphaello Most Recent 3 days, 4 hours ago

Selected Answer: B

Correct answer is B.
Set OAC to restrict access to S3 bucket to only CF distribution.

upvoted 1 times

nouns 2 months ago

Selected Answer: B

Option B: When you associate an OAI with a CloudFront distribution, it acts as a pseudo-user for the distribution, and you can configure S3 bucket permissions to grant access only to that OAI. This allows CloudFront to fetch and serve objects from the S3 bucket on behalf of the end-users without making the objects directly accessible from the S3 bucket.

upvoted 2 times

Question #59 *Topic 1*

A security engineer logs in to the AWS Lambda console with administrator permissions. The security engineer is trying to view logs in Amazon CloudWatch for a Lambda function that is named myFunction. When the security engineer chooses the option in the Lambda console to view logs in CloudWatch, an "error loading Log Streams" message appears.
The IAM policy for the Lambda function's execution role contains the following:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "arn:aws:logs:us-east-1:111111111111:*"
        },
        {
            "Effect": "Allow",
            "Action": ["logs:PutLogEvents"],
            "Resource": ["arn:aws:logs:us-east-1:111111111111:log-group:/aws/lambda/myFunction:*"]
        }
    ]
}
```

How should the security engineer correct the error?

A. Move the logs:CreateLogGroup action to the second Allow statement.

B. Add the logs:PutDestination action to the second Allow statement.

C. Add the logs:GetLogEvents action to the second Allow statement.

D. Add the logs:CreateLogStream action to the second Allow statement.

Correct Answer: *A*

Community vote distribution

D (80%) C (20%)

Raphaello 6 days, 13 hours ago

Selected Answer: D

Action "logs:GetLogEvents" gets log events from log stream (https://docs.aws.amazon.com/AmazonCloudWatchLogs/latest/APIReference/API_GetLogEvents.html), but there no log stream on first place!

Correct answer is allowing the function to create log stream (through logs:CreateLogStream).

D.

upvoted 2 times

mynickc 1 month ago

Selected Answer: D

putlogevent require logstream. so it is createlogstream. https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/permissions-reference-cwl.html

upvoted 1 times

Gafa255 1 month ago

Selected Answer: C

C is correct options because Security Engineer wants to see LOG. logs:GetLogEvents
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/iam-identity-based-access-control-cwl.html

upvoted 1 times

Gafa255 1 month ago

Sorry the correct options is D because the issue is when the Lambda function want to create the streams.

upvoted 1 times

marlonchin 3 months ago

D I don't think adding logs is not the responsibility of the Lamda function here

upvoted 1 times

[Removed] 3 months ago

Seems poorly written to me.. The engineer is trying to view the logs. So they'll need "logs:GetLogEvents " permission. However the policy is also missing "logs:CreateLogStream" so they will also need that in order for the Lambda to "create a new log stream". Doubt something this bad will

be on the exam

upvoted 1 times

YR4591 3 months, 1 week ago

Selected Answer: D

When creating log group, there should be a permission to put log streams in the log group

upvoted 2 times

kejam 3 months, 2 weeks ago

Selected Answer: C

Answer C. The security engineer wants to view logs in CloudWatch.

A. logs:CreateLogGroup - Required to create a new log group
B. logs:PutDestination - Required to create or update a destination log stream
C. Add the logs:GetLogEvents - Required to retrieve log events from a log stream
D. Add the logs:CreateLogStream - Required to create a new log stream in a log group

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/permissions-reference-cwl.html

upvoted 1 times

Aamee 2 months, 3 weeks ago

But w/o creating the LogStream, how can the PutLogStream going to work from option C?.. that looks missing to me though..

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: D

Answer D
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/iam-identity-based-access-control-cwl.html

upvoted 3 times

kk2000 4 months, 3 weeks ago

Correct Answer is D

upvoted 3 times

Question #60 *Topic 1*

A company has a new partnership with a vendor. The vendor will process data from the company's customers. The company will upload data files as objects into an Amazon S3 bucket. The vendor will download the objects to perform data processing. The objects will contain sensitive data. A security engineer must implement a solution that prevents objects from residing in the S3 bucket for longer than 72 hours.
Which solution will meet these requirements?

A. Use Amazon Macie to scan the S3 bucket for sensitive data every 72 hours. Configure Macie to delete the objects that contain sensitive data when they are discovered.

B. Configure an S3 Lifecycle rule on the S3 bucket to expire objects that have been in the S3 bucket for 72 hours.

C. Create an Amazon EventBridge scheduled rule that invokes an AWS Lambda function every day. Program the Lambda function to remove any objects that have been in the S3 bucket for 72 hours.

D. Use the S3 Intelligent-Tiering storage class for all objects that are uploaded to the S3 bucket. Use S3 Intelligent-Tiering to expire objects that have been in the $3 bucket for 72 hours.

Correct Answer: *B*

Community vote distribution

B (100%)

100fold Highly Voted 4 months, 1 week ago

Selected Answer: B

B

https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lifecycle-mgmt.html
https://docs.aws.amazon.com/AmazonS3/latest/userguide/how-to-set-lifecycle-configuration-intro.html

upvoted 6 times

Raphaello Most Recent 6 days, 13 hours ago

Selected Answer: B

Correct answer is B.
The question tries to trick to select Macie, since data contains sensitive data, but Macie discover and classify data, and send findings to SecurityHub or EventBridge for any action that might be needed. It does NOT delete objects.

Another thing is that S3 object lifecycle is used for 2 roles, both transition and EXPIRATION of objects.

B is the correct answer.

upvoted 1 times

Aamee 2 months, 3 weeks ago

Selected Answer: B

B is self-explanatory and sufficient.

upvoted 1 times

Question #61 *Topic 1*

A company accidentally deleted the private key for an Amazon Elastic Block Store (Amazon EBS)-backed Amazon EC2 instance. A security engineer needs to regain access to the instance.
Which combination of steps will meet this requirement? (Choose two.)

A. Stop the instance. Detach the root volume. Generate a new key pair.

B. Keep the instance running. Detach the root volume. Generate a new key pair.

C. When the volume is detached from the original instance, attach the volume to another instance as a data volume. Modify the authorized_keys file with a new public key. Move the volume back to the original instance. Start the instance.

D. When the volume is detached from the original instance, attach the volume to another instance as a data volume. Modify the authorized_keys file with a new private key. Move the volume back to the original instance. Start the instance.

E. When the volume is detached from the original instance, attach the volume to another instance as a data volume. Modify the authorized_keys file with a new public key. Move the volume back to the original instance that is running.

Correct Answer: *AC*

Community vote distribution

AC (100%)

100fold Highly Voted 4 months, 1 week ago

Selected Answer: AC

Answer AC

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html#replacing-lost-key-pair

upvoted 7 times

Raphaello Most Recent 6 days, 13 hours ago

Selected Answer: AC

AC are the correct answers.
There are other ways to add/replace pub key into "authorized_keys" file without stopping the instance, but within the context of this scenario, AC are good.

Remember, "authorized_keys" file resides on the root volume. You cannot keep the instance running without the root volume.

upvoted 1 times

jeff001 2 months, 3 weeks ago

Selected Answer: AC

A & C. Stop the instance, detach its root volume and attach it to another instance as a data volume, modify the authorized_keys file with a new public key, move the volume back to the original instance, and restart the instance

upvoted 2 times

352ae9a 3 months ago

Answer AC

upvoted 2 times

Question #62 *Topic 1*

A company purchased a subscription to a third-party cloud security scanning solution that integrates with AWS Security Hub. A security engineer needs to implement a solution that will remediate the findings from the third-party scanning solution automatically.
Which solution will meet this requirement?

A. Set up an Amazon EventBridge rule that reacts to new Security Hub findings. Configure an AWS Lambda function as the target for the rule to remediate the findings.

B. Set up a custom action in Security Hub. Configure the custom action to call AWS Systems Manager Automation runbooks to remediate the findings.

C. Set up a custom action in Security Hub. Configure an AWS Lambda function as the target for the custom action to remediate the findings.

D. Set up AWS Config rules to use AWS Systems Manager Automation runbooks to remediate the findings.

Correct Answer: *A*

Community vote distribution

A (62%) B (38%)

100fold Highly Voted 4 months, 1 week ago

Selected Answer: A

Answer A
https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automate-remediation-for-aws-security-hub-standard-findings.html

upvoted 5 times

Raphaello Most Recent 6 days, 13 hours ago

Selected Answer: A

Another tricking question.
EventBridge integrates with SecurityHub in 3 different ways..
1. All findings (SH Imported)
2. Findings for custom actions (SH Custom Actions)
3. Insights for custom actions (SH Insights)
(https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-cwe-integration-types.html)

You do not always need custom actions for EB integration, and to automatically remediate findings as in this scenario, 1st type of integration is required.

Answer is A.

upvoted 2 times

Derets 1 month ago

Selected Answer: B

Answer B
Custom action is a native feature for Security Hub when using a 3rd-party library. Then you need to use Systems Manager Automation runbooks. Answer A (EventBridge+Lambda) can be used for standard findings.

upvoted 2 times

yorkicurke 2 months ago

Selected Answer: B

Verty tricky one. A,B and C can all be implemented. and we havent asked for easy,quickly or something like that a solution. so reason for not picking others

A:- could also be used but would require additional steps to configure rules to route findings from this specific third-party source to the appropriate target. Custom actions provide a native option within Security Hub.

C:- identical to B. same reasoning that Custom actions provide a native option within Security Hub.

to be honest i could go for any out of these three. even though i chose B. Arghhhh

upvoted 3 times

Raphaello 6 days, 13 hours ago

I beg to disagree.
EventBridge integration type "SH Imported" with automatically send all findings to EB.
EB does not care how the findings ended up in SH. SH integration with the third party handle this, and as long as the third party tool actually integrates with SH, that means it can send findings to it.
Once done, findings in SH automatically sent over to EB
(https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-cwe-integration-types.html#securityhub-cwe-integration-types-all-findings)

There you can build the action that you want.

Answer is A.

upvoted 2 times

Aamee 2 months, 3 weeks ago

Selected Answer: A

To remediate the findings automatically, option A describes about the best practices..

upvoted 1 times

Question #63 *Topic 1*

An application is running on an Amazon EC2 instance that has an IAM role attached. The IAM role provides access to an AWS Key Management Service (AWS KMS) customer managed key and an Amazon S3 bucket. The key is used to access 2 TB of sensitive data that is stored in the S3 bucket.
A security engineer discovers a potential vulnerability on the EC2 instance that could result in the compromise of the sensitive data. Due to other critical operations, the security engineer cannot immediately shut down the EC2 instance for vulnerability patching.
What is the FASTEST way to prevent the sensitive data from being exposed?

A. Download the data from the existing S3 bucket to a new EC2 instance. Then delete the data from the S3 bucket. Re-encrypt the data with a client-based key. Upload the data to a new S3 bucket.

B. Block access to the public range of S3 endpoint IP addresses by using a host-based firewall. Ensure that internet-bound traffic from the affected EC2 instance is routed through the host-based firewall.

C. Revoke the IAM role's active session permissions. Update the S3 bucket policy to deny access to the IAM role. Remove the IAM role from the EC2 instance profile.

D. Disable the current key. Create a new KMS key that the IAM role does not have access to, and re-encrypt all the data with the new key. Schedule the compromised key for deletion.

Correct Answer: *C*

Community vote distribution

C (90%) 10%

tapupa Highly Voted 2 months, 2 weeks ago

Selected Answer: C

itexamstest.com

no disscusion c :)

upvoted 13 times

Raphaello Most Recent 6 days, 12 hours ago

Selected Answer: C

D is a valid solution, but not the fastest as requested. Creating a batch operation to re-encrypt 2TB to data on S3 might take time.
Plus, old or new KMS key are both equally same for an attacker who has access to the EC2/role that's allowed to use the key.

The solution needs to be with the role itself to eliminate further access to sensitive data.

Revoke current active session permissions, set S3 bucket policy to deny the role, and remove the role altogether from EC2 instance profile.

C.

upvoted 1 times

Oralinux 2 months, 2 weeks ago

C. Revoke the IAM role's active session permissions.

upvoted 3 times

Daniel76 2 months, 2 weeks ago

Selected Answer: C

This contains more detail response. Refer to part 2 for containment step. The first step is always to deal with the role access first.
https://www.bicarait.com/2021/04/27/aws-incident-response-unintended-access-to-s3-bucket/
It only takes a few minutes for policy updates to effectively revoke the role's temporary security credentials to force all users assuming the role to reauthenticate and request new credentials. (as compare to re-encrypt entire s3 bucket data to a single new key)
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_control-access_disable-perms.html#deny-access-to-all-sessions
Furthermore, though unrelated to the requirement:
The s3 bucket may be encrypted by multiple data keys which is intended. by re-encrypting the entire bucket, you may affect data that are encrypted by other legitimate keys unaffected by this vulnerable ec2.

upvoted 2 times

Aamee 3 months ago

Still v confusing btw C and D.... but I'd probably go with C.

upvoted 1 times

kejam 3 months, 2 weeks ago

Selected Answer: D

Answer D. The fastest way to prevent sensitive data from being exposed is to disable the current key.

A. Not fast
B. Not fast
C. AWSRevokeOlderSessions is fast, however bad actors can immediately reconnect with new sessions before you remove the IAM role from the EC2 instance profile. If these steps were reversed to prevent that its no longer the fastest solution because its 2 steps.
D. Disable the current key... 1st step prevents sensitive data exposure and the rest of the steps to re-encrypt the data with a new key can follow.

upvoted 2 times

confusedyeti69 2 months, 3 weeks ago

If your bucket has millions of objects, re-encryption is slower. Ans is C

upvoted 1 times

Aamee 2 months, 3 weeks ago

No, that's not the point here. The req. is to implement it 'FASTER' to get it secured on the first attempt which I also feel Option D provides it. Disabling the key right away can atleast help ensure that no sensitive data would get exposed further IMO... and then the rest of the steps to re-encrypting the data can be done as a 2nd step to follow...

upvoted 1 times

100fold 4 months, 1 week ago

Selected Answer: C

Answer C
https://www.examtopics.com/discussions/amazon/view/60659-exam-aws-certified-security-specialty-topic-1-question-287/

upvoted 2 times

Question #64 *Topic 1*

A company is building an application on AWS that will store sensitive information. The company has a support team with access to the IT infrastructure, including databases. The company's security engineer must introduce measures to protect the sensitive data against any data breach while minimizing management overhead. The credentials must be regularly rotated.
What should the security engineer recommend?

A. Enable Amazon RDS encryption to encrypt the database and snapshots. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instances. Include the database credential in the EC2 user data field. Use an AWS Lambda function to rotate database credentials. Set up TLS for the connection to the database.

B. Install a database on an Amazon EC2 instance. Enable third-party disk encryption to encrypt the Amazon Elastic Block Store (Amazon EBS) volume. Store the database credentials in AWS CloudHSM with automatic rotation. Set up TLS for the connection to the database.

C. Enable Amazon RDS encryption to encrypt the database and snapshots. Enable Amazon Elastic Black Store (Amazon EBS) encryption on Amazon EC2 instances. Store the database credentials in AWS Secrets Manager with automatic rotation. Set up TLS for the connection to the RDS hosted database.

D. Set up an AWS CloudHSM cluster with AWS Key Management Service (AWS KMS) to store KMS keys. Set up Amazon RDS encryption using AWS KMS to encrypt the database. Store database credentials in the AWS Systems Manager Parameter Store with automatic rotation. Set up TLS for the connection to the RDS hosted database.

Correct Answer: *C -*

Community vote distribution

C (100%)

Raphaello 6 days, 3 hours ago

Selected Answer: C

Correct answer is C.
It covers the required areas to protect sensitive data, without least overhead.

upvoted 1 times

kejam 3 months, 2 weeks ago

Selected Answer: C

Answer C
https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotate-secrets_turn-on-for-db.html

upvoted 3 times

100fold 4 months, 1 week ago

Selected Answer: C

Answer C
https://www.examtopics.com/discussions/amazon/view/60739-exam-aws-certified-security-specialty-topic-1-question-268/

upvoted 4 times

Question #65 *Topic 1*

A company is using Amazon Route 53 Resolver for its hybrid DNS infrastructure. The company has set up Route 53 Resolver forwarding rules for authoritative domains that are hosted on on-premises DNS servers.

A new security mandate requires the company to implement a solution to log and query DNS traffic that goes to the on-premises DNS servers. The logs must show details of the source IP address of the instance from which the query originated. The logs also must show the DNS name that was requested in Route 53 Resolver.

Which solution will meet these requirements?

A. Use VPC Traffic Mirroring. Configure all relevant elastic network interfaces as the traffic source, include amazon-dns in the mirror filter, and set Amazon CloudWatch Logs as the mirror target. Use CloudWatch Insights on the mirror session logs to run queries on the source IP address and DNS name.

B. Configure VPC flow logs on all relevant VPCs. Send the logs to an Amazon S3 bucket. Use Amazon Athena to run SQL queries on the source IP address and DNS name.

C. Configure Route 53 Resolver query logging on all relevant VPCs. Send the logs to Amazon CloudWatch Logs. Use CloudWatch Insights to run queries on the source IP address and DNS name.

D. Modify the Route 53 Resolver rules on the authoritative domains that forward to the on-premises DNS servers. Send the logs to an Amazon S3 bucket. Use Amazon Athena to run SQL queries on the source IP address and DNS name.

Correct Answer: *A*

Community vote distribution

C (100%)

Daniel76 1 month, 3 weeks ago

Selected Answer: C

C is the only answer as you need to config resolver query logging on all vpc, and cloudwatch log insight indeed allow you to query the source IP address.

https://aws.amazon.com/blogs/aws/log-your-vpc-dns-queries-with-route-53-resolver-query-logs/

upvoted 1 times

brpjp 1 month, 3 weeks ago

Correct answer is D. https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver.html. Please read this statement : Resolver rules enable you to create one forwarding rule for each domain name and specify the name of the domain for which you want to forward DNS queries from your VPC to an on-premises DNS resolver and from your on-premises to your VPC. Rules are applied directly to your VPC and can be shared across multiple accounts. so correct answer, based on above statement is D and not C, as it does not specify the requirements to send outbound connections to on-premise.

upvoted 1 times

ahrentom 2 months, 3 weeks ago

Selected Answer: C

For me it´s anwser C
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-query-logs.html

upvoted 3 times

[Removed] 3 months ago

Selected Answer: C

Seems like it's C

https://medium.com/@sisodiyapradeep/dns-query-logging-aggregation-control-tower-environment-well-architected-telemetry-workload-266dcdbf7195

upvoted 2 times

oioi 3 months ago

Selected Answer: C

correct.

upvoted 1 times

marlonchin 3 months ago

https://repost.aws/knowledge-center/route53-view-endpoint-traffic

upvoted 2 times

Question #66 *Topic 1*

A security engineer is configuring account-based access control (ABAC) to allow only specific principals to put objects into an Amazon S3 bucket. The principals already have access to Amazon S3.

The security engineer needs to configure a bucket policy that allows principals to put objects into the S3 bucket only if the value of the Team tag on the object matches the value of the Team tag that is associated with the principal. During testing, the security engineer notices that a principal can still put objects into the S3 bucket when the tag values do not match.

Which combination of factors are causing the PutObject operation to succeed when the tag values are different? (Choose two.)

A. The principal's identity-based policy grants access to put objects into the S3 bucket with no conditions.

B. The principal's identity-based policy overrides the condition because the identity-based policy contains an explicit allow.

C. The S3 bucket's resource policy does not deny access to put objects.

D. The S3 bucket's resource policy cannot allow actions to the principal.

E. The bucket policy does not apply to principals in the same zone of trust.

Correct Answer: *D E*

Community vote distribution

AC (100%)

rahav 2 months ago

Selected Answer: AC

AC is the correct ones

upvoted 1 times

Daniel76 2 months, 2 weeks ago

Selected Answer: AC

https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_attribute-based-access-control.html
Look out for step 2- create ABAC policy example.
To ensure that resources is only granted when principal and resource tag match, there should be condition for the access, and disallow when tag not match.

upvoted 2 times

[Removed] 3 months ago

BDE Don't appear to make much sense. So A C it is.

The resource policy should be setup to DENY if a tag DOES NOT MATCH the desired tags. Not ALLOW the tag listed alone. Otherwise, a IAM policy without conditions may be enough to provide access. Not a fan of this question as it leaves a ton up in the air but hey..

upvoted 3 times

oioi 3 months ago

Selected Answer: AC

correct

upvoted 3 times

marlonchin 3 months ago

Sorry not D I need the explanation for E if it is right answer

upvoted 1 times

marlonchin 3 months ago

BE can some explain how it is possible for D to be answer

upvoted 1 times

Question #67 *Topic 1*

A company is hosting multiple applications within a single VPC in its AWS account. The applications are running behind an Application Load Balancer that is associated with an AWS WAF web ACL. The company's security team has identified that multiple port scans are originating from a specific range of IP addresses on the internet.

A security engineer needs to deny access from the offending IP addresses.

Which solution will meet these requirements?

A. Modify the AWS WAF web ACL with an IP set match rule statement to deny incoming requests from the IP address range.

B. Add a rule to all security groups to deny the incoming requests from the IP address range.

C. Modify the AWS WAF web ACL with a rate-based rule statement to deny the incoming requests from the IP address range.

D. Configure the AWS WAF web ACL with regex match conditions. Specify a pattern set to deny the incoming requests based on the match condition.

Correct Answer: *A*

Community vote distribution

A (83%) C (17%)

Raphaello 6 days, 2 hours ago

Selected Answer: A

The offending IP's are specified, and the request is to "DENY" access from them. There's no reason to rate-limit the flow. Just block it.

A.

upvoted 1 times

MikeRach 2 weeks, 2 days ago

AWS WAF--> Inspects the request against a set of IP addresses and address ranges.
https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-ipset-match.html

upvoted 1 times

3633f8f 2 months, 1 week ago

Selected Answer: A

As per below discussion.

upvoted 1 times

Daniel76 2 months, 2 weeks ago

Selected Answer: C

https://docs.aws.amazon.com/waf/latest/developerguide/listing-managed-ips.html

upvoted 1 times

Daniel76 1 month, 3 weeks ago

agree, should be C.

upvoted 1 times

Daniel76 1 month, 3 weeks ago

agree, should be A instead.

upvoted 1 times

WeepingMaplte 2 months, 1 week ago

You will use rate limit if it is normal HTTP/s traffic. For port scanning is a network reconnaissance technique used to identify which ports on a computer system are open and potentially vulnerable. You will want to block it 100%.

upvoted 2 times

3633f8f 2 months, 1 week ago

The question is how to apply what the security engineer wants to do which is to block every single request coming from that IP set. Hence, I also think correct answer is A.

upvoted 2 times

[Removed] 3 months ago

Selected Answer: A

Agreed on A

upvoted 1 times

oioi 3 months ago

Selected Answer: A

correct

upvoted 2 times

Question #68 *Topic 1*

A company has contracted with a third party to audit several AWS accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The auditor is having trouble accessing some of the accounts.

Which of the following may be causing this problem? (Choose three.)

A. The external ID used by the auditor is missing or incorrect.

B. The auditor is using the incorrect password.

C. The auditor has not been granted sts:AssumeRole for the role in the destination account.

D. The Amazon EC2 role used by the auditor must be set to the destination account role.

E. The secret key used by the auditor is missing or incorrect.

F. The role ARN used by the auditor is missing or incorrect.

Correct Answer: *ABD*

Community vote distribution

ACF (100%)

Raphaello 6 days, 12 hours ago

Selected Answer: ACF

ACF the correct answers to this case.
* ExternalID is incorrect or missing
* Auditor is not allowed to assume the role on first place
* The role ARN is incorrect

upvoted 1 times

rahav 2 months ago

Selected Answer: ACF

ACF for sure

upvoted 1 times

Daniel76 2 months, 2 weeks ago

Selected Answer: ACF

B &E, if its due to external ID or secret key used by auditor, then access to all accounts shd be affected.
D, ec2 is irrelevant in account access.

upvoted 2 times

[Removed] 3 months ago

Selected Answer: ACF

ACF for sure

upvoted 3 times

oioi 3 months ago

Selected Answer: ACF

correct

upvoted 2 times

Question #69 *Topic 1*

A security engineer needs to configure an Amazon S3 bucket policy to restrict access to an S3 bucket that is named DOC-EXAMPLE-BUCKET. The policy must allow access to only DOC-EXAMPLE-BUCKET from only the following endpoint: vpce-1a2b3c4d. The policy must deny all access to DOC-EXAMPLE-BUCKET if the specified endpoint is not used.

Which bucket policy statement meets these requirements?

A.
```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Allow",
        "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                     "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"],
        "Condition": {
            "StringNotEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

B.
```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                     "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"],
        "Condition": {
            "StringNotEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

C.
```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                     "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"],
        "Condition": {
            "StringEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

D.
```
"Statement": [
    {
        "Sid": "Access-to-specific-VPCE-only",
        "Principal": "*",
        "Action": "s3:*",
        "Effect": "Allow",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:sourceVpce": "vpce-1a2b3c4d"
            }
        }
    }
]
```

Correct Answer: *A*

Community vote distribution

B (100%)

sz1234 1 week, 1 day ago

B is correct

upvoted 1 times

awssecuritynewbie 2 weeks, 1 day ago

Selected Answer: B

B

The option D does not even have the bucket in it lol

upvoted 1 times

rahav 2 months ago

Selected Answer: B

B is the correct one

upvoted 1 times

Aamee 2 months, 3 weeks ago

Selected Answer: B

No doubt, it's B.

upvoted 1 times

[Removed] 3 months ago

Selected Answer: B

B is correcto

upvoted 2 times

oioi 3 months ago

Selected Answer: B

correct

upvoted 3 times

Question #70 *Topic 1*

A company has a group of Amazon EC2 instances in a single private subnet of a VPC with no internet gateway attached. A security engineer has installed the Amazon CloudWatch agent on all instances in that subnet to capture logs from a specific application. To ensure that the logs flow securely, the company's networking team has created VPC endpoints for CloudWatch monitoring and CloudWatch logs. The networking team has attached the endpoints to the VPC.

The application is generating logs However, when the security engineer queries CloudWatch, the logs do not appear.

Which combination of steps should the security engineer take to troubleshoot this issue? (Choose three.)

A. Ensure that the EC2 instance profile that is attached to the EC2 instances has permissions to create log streams and write logs.

B. Create a metric filter on the logs so that they can be viewed in the AWS Management Console.

C. Check the CloudWatch agent configuration file on each EC2 instance to make sure that the CloudWatch agent is collecting the proper log files.

D. Check the VPC endpoint policies of both VPC endpoints to ensure that the EC2 instances have permissions to use them.

E. Create a NAT gateway in the subnet so that the EC2 instances can communicate with CloudWatch.

F. Ensure that the security groups allow all the EC2 instances to communicate with each other to aggregate logs before sending.

Correct Answer: *AFE*

Community vote distribution

ACD (100%)

rahav 2 months ago

Selected Answer: ACD

ACD are the correct ones. for sure

upvoted 1 times

Aamee 2 months, 3 weeks ago

Selected Answer: ACD

ACD makes a good comb. logically.

upvoted 2 times

[Removed] 3 months ago

Selected Answer: ACD

ACD seem correct

upvoted 3 times

oioi 3 months ago

Selected Answer: ACD

correct

upvoted 1 times

Question #71 *Topic 1*

A company uses AWS Signer with all of the company's AWS Lambda functions. A developer recently stopped working for the company. The company wants to ensure that all the code that the developer wrote can no longer be deployed to the Lambda functions.

Which solution will meet this requirement?

A. Revoke all versions of the signing profile assigned to the developer.

B. Examine the developer's IAM roles. Remove all permissions that grant access to Signer.

C. Re-encrypt all source code with a new AWS Key Management Service (AWS KMS) key.

D. Use Amazon CodeGuru to profile all the code that the Lambda functions use.

Correct Answer: *C*

Community vote distribution

A (89%) 11%

rahav 2 months ago

Selected Answer: A

https://docs.aws.amazon.com/signer/latest/developerguide/revocation.html

upvoted 1 times

vincentsr7 2 months, 2 weeks ago

The privilege has to be removed from signer , for this option b is the right answer

upvoted 1 times

vincentsr7 2 months, 2 weeks ago

Option A suggests revoking all versions of the signing profile assigned to the developer, but this is not the most effective solution for preventing the developer from deploying code to Lambda functions. Signing profiles primarily deal with the integrity and authenticity of code, rather than controlling the ability to deploy code

upvoted 1 times

kejam 3 months ago

Selected Answer: A

Answer A
New URL: https://docs.aws.amazon.com/signer/latest/developerguide/revocation.html

upvoted 3 times

lmimi 3 months ago

A
Refer to https://docs.aws.amazon.com/signer/latest/developerguide/revoking.html
https://docs.aws.amazon.com/signer/latest/developerguide/revoking.html

upvoted 3 times

AgboolaKun 3 months ago

Selected Answer: A

A is the correct answer. Revoke the developer signing profile - https://docs.aws.amazon.com/signer/latest/developerguide/revocation.html

upvoted 2 times

[Removed] 3 months ago

Selected Answer: A

A will handle prevention

upvoted 2 times

oioi 3 months ago

Selected Answer: B

correct

upvoted 1 times

Aamee 3 months ago

Source pls?

upvoted 1 times

Question #72 *Topic 1*

A company plans to use AWS Key Management Service (AWS KMS) to implement an encryption strategy to protect data at rest. The company requires client-side encryption for company projects. The company is currently conducting multiple projects to test the company's use of AWS KMS. These tests have led to a sudden increase in the company's AWS resource consumption. The test projects include applications that issue multiple requests each second to KMS endpoints for encryption activities.

The company needs to develop a solution that does not throttle the company's ability to use AWS KMS. The solution must improve key usage for client-side encryption and must be cost optimized.

Which solution will meet these requirements?

A. Use keyrings with the AWS Encryption SDK. Use each keyring individually or combine keyrings into a multi-keyring. Decrypt the data by using a keyring that has the primary key in the multi-keyring.

B. Use data key caching. Use the local cache that the AWS Encryption SDK provides with a caching cryptographic materials manager.

C. Use KMS key rotation. Use a local cache in the AWS Encryption SDK with a caching cryptographic materials manager.

D. Use keyrings with the AWS Encryption SDK. Use each keyring individually or combine keyrings into a multi-keyring. Use any of the wrapping keys in the multi-keyring to decrypt the data.

Correct Answer: *D*

Community vote distribution

B (100%)

Daniel76 1 month, 4 weeks ago

Selected Answer: B

"Caching can reduce your use of cryptographic services, such as AWS Key Management Service (AWS KMS). If you are hitting your AWS KMS requests-per-second limit, caching can help."
https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/data-key-caching.html

upvoted 1 times

WeepingMaplte 2 months, 1 week ago

Local key cache: Implement local key caching in your applications to store frequently used encryption keys, reducing the number of calls to KMS. Consider libraries like AWS Encryption SDK for secure key cache management.

upvoted 1 times

Aamee 3 months ago

Shouldn't it be 'D'? Couldn't verify the source for the option of 'C' being correct anywhere.

upvoted 1 times

Imimi 3 months ago

I vote for B

upvoted 1 times

AgboolaKun 3 months ago

Selected Answer: B

Data key caching helps to improve performance, reduce cost, and help stay within limit as your key usage increases without throttling - https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/data-key-caching.html

upvoted 4 times

[Removed] 3 months ago

Selected Answer: B

B seems right

https://repost.aws/knowledge-center/kms-throttlingexception-error

upvoted 1 times

oioi 3 months ago

Selected Answer: B

correct

upvoted 1 times

oioi 3 months ago

C is correct

upvoted 1 times

Question #73 *Topic 1*

A security team is working on a solution that will use Amazon EventBridge to monitor new Amazon S3 objects. The solution will monitor for public access and for changes to any S3 bucket policy or setting that result in public access. The security team configures EventBridge to watch for specific API calls that are logged from AWS CloudTrail. EventBridge has an action to send an email notification through Amazon Simple Notification Service (Amazon SNS) to the security team immediately with details of the API call.

Specifically, the security team wants EventBridge to watch for the s3:PutObjectAcl, s3:DeleteBucketPolicy, and s3:PutBucketPolicy API invocation logs from CloudTrail. While developing the solution in a single account, the security team discovers that the s3:PutObjectAcl API call does not invoke an EventBridge event However, the s3:DeleteBucketPolicy API call and the s3:PutBucketPolicy API call do invoke an event.

The security team has enabled CloudTrail for AWS management events with a basic configuration in the AWS Region in which EventBridge is being tested. Verification of the EventBridge event pattern indicates that the pattern is set up correctly. The security team must implement a solution so that the s3:PutObjectAcl API call will invoke an EventBridge event. The solution must not generate false notifications.

Which solution will meet these requirements?

A. Modify the EventBridge event pattern by selecting Amazon S3. Select All Events as the event type.

B. Modify the EventBridge event pattern by selecting Amazon S3. Select Bucket Level Operations as the event type.

C. Enable CloudTrail Insights to identify unusual API activity.

D. Enable CloudTrail to monitor data events for read and write operations to S3 buckets.

Correct Answer: *B*

Community vote distribution

D (100%)

[Removed] Highly Voted 3 months ago

Selected Answer: D

You need to enable data events for that API event to trigger

https://docs.aws.amazon.com/AmazonS3/latest/userguide/cloudtrail-logging-s3-info.html#cloudtrail-object-level-tracking

upvoted 7 times

rahav Most Recent 2 months ago

Selected Answer: D

you need to enable data events in cloudtrail

upvoted 1 times

WeepingMaplte 2 months, 1 week ago

By default, CloudTrail only logs bucket-level API calls in S3, not object-level actions. This means it logs events like creating or deleting buckets, but not actions like uploading or downloading objects.
To enable object-level logging, you need to explicitly configure CloudTrail for your S3 buckets. You can do this in the S3 console, CLI, or SDK.

upvoted 4 times

oioi 3 months ago

Selected Answer: D

correct

upvoted 1 times

Question #74 *Topic 1*

A company uses Amazon GuardDuty. The company's security team wants all High severity findings to automatically generate a ticket in a third-party ticketing system through email integration.

Which solution will meet this requirement?

A. Create a verified identity for the third-party ticketing email system in Amazon Simple Email Service (Amazon SES). Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty findings. Specify the SES identity as the target for the EventBridge rule.

B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the third-party ticketing email system to the SNS topic. Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty findings. Specify the SNS topic as the target for the EventBridge rule.

C. Use the GuardDuty CreateFilter API operation to build a filter in GuardDuty to monitor for High severity findings. Export the results of the filter to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the third-party ticketing email system to the SNS topic.

D. Use the GuardDuty CreateFilter API operation to build a filter in GuardDuty to monitor for High severity findings. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the third-party ticketing email system to the SNS topic. Create an Amazon EventBridge rule that includes an event pattern that matches GuardDuty findings that are selected by the filter. Specify the SNS topic as the target for the EventBridge rule.

Correct Answer: *C*

Community vote distribution

B (90%) 10%

rahav 2 months ago

Selected Answer: B

B is the right one- you do it with EventBridge

upvoted 2 times

3633f8f 2 months, 1 week ago

Selected Answer: B

Create a high severity Eventbridge based on GuardDuty High Severity Findings:
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings_cloudwatch.html

upvoted 2 times

WeepingMaplte 2 months, 1 week ago

Key steps for integration:
1. Create a Eventbridge/CloudWatch event rule: Define the event pattern to trigger the rule based on specific GuardDuty findings.
2. Configure the rule target: Choose where to send the findings data, like an SNS topic

upvoted 1 times

lmimi 3 months ago

B.
Users can define filter in EventBridge. Not necessary to use GuardDuty CreateFilter API.

upvoted 2 times

Aamee 3 months ago

Selected Answer: D

D sounds pretty legit IMO.

upvoted 1 times

Aamee 3 months ago

Sorry, after reviewing it again, looks like Option 'B' looks to be more correct ans.

upvoted 1 times

[Removed] 3 months ago

Selected Answer: B

B.. Use Eventbridge (formally Cloudwatch Events)

https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings_cloudwatch.html

upvoted 4 times

oioi 3 months ago

Selected Answer: B

correct

upvoted 1 times

oioi 3 months ago

D is correct

upvoted 1 times

Question #75 *Topic 1*

A company is using AWS Organizations to implement a multi-account strategy. The company does not have on-premises infrastructure. All workloads run on AWS. The company currently has eight member accounts. The company anticipates that it will have no more than 20 AWS accounts total at any time.

The company issues a new security policy that contains the following requirements:

- No AWS account should use a VPC within the AWS account for workloads.
- The company should use a centrally managed VPC that all AWS accounts can access to launch workloads in subnets.
- No AWS account should be able to modify another AWS account's application resources within the centrally managed VPC.
- The centrally managed VPC should reside in an existing AWS account that is named Ac-count-A within an organization.

The company uses an AWS CloudFormation template to create a VPC that contains multiple subnets in Account-A. This template exports the subnet IDs through the CloudFormation Outputs section.

Which solution will complete the security setup to meet these requirements?

A. Use a CloudFormation template in the member accounts to launch workloads. Configure the template to use the Fn::ImportValue function to obtain the subnet ID values.

B. Use a transit gateway in the VPC within Account-A. Configure the member accounts to use the transit gateway to access the subnets in Account-A to launch workloads.

C. Use AWS Resource Access Manager (AWS RAM) to share Account-A's VPC subnets with the remaining member accounts. Configure the member accounts to use the shared subnets to launch workloads.

D. Create a peering connection between Account-A and the remaining member accounts. Configure the member accounts to use the subnets in Account-A through the VPC peering connection to launch workloads.

Correct Answer: *D*

Community vote distribution

C (100%)

vikasj1in 1 month, 2 weeks ago

C. Explanation:
using AWS RAM, allows for centralized control over the VPC in Account-A, shared access to subnets with other member accounts, and isolation between the resources of different accounts within the VPC. This aligns well with the specified security requirements.

VPC Peering or Transit Gateway: While VPC peering (Option D) or Transit Gateway (Option B) could facilitate communication between VPCs, they might not provide the level of isolation required in this scenario. With VPC peering, all resources in the peered VPCs have the ability to communicate with each other directly.

CloudFormation Fn::ImportValue: While using CloudFormation's Fn::ImportValue (Option A) is a common approach to share values between stacks, in this scenario, AWS RAM provides a more structured and scalable way to share resources (subnets) across accounts.

upvoted 3 times

rahav 2 months ago

Selected Answer: C

RAM is used to share subnets

upvoted 1 times

AgboolaKun 3 months ago

Selected Answer: C

Yes, you can use the AWS Resource Access Manager (AWS RAM) to share your subnets and resources in VPC owner, Account-A with other accounts - https://aws.amazon.com/blogs/networking-and-content-delivery/vpc-sharing-a-new-approach-to-multiple-accounts-and-vpc-management/

upvoted 3 times

[Removed] 3 months ago

Selected Answer: C

C is correct. B and D will require multiple VPCs and A is not applicable here

upvoted 2 times

oioi 3 months ago

Selected Answer: C

correct

upvoted 2 times

Question #76 *Topic 1*

A company's security team needs to receive a notification whenever an AWS access key has not been rotated in 90 or more days. A security engineer must develop a solution that provides these notifications automatically.

Which solution will meet these requirements with the LEAST amount of effort?

A. Deploy an AWS Config managed rule to run on a periodic basis of 24 hours. Select the access-keys-rotated managed rule, and set the maxAccessKeyAge parameter to 90 days. Create an Amazon EventBridge rule with an event pattern that matches the compliance type of NON_ COMPLIANT from AWS Config for the managed rule. Configure EventBridge to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.

B. Create a script to export a .csv file from the AWS Trusted Advisor check for IAM access key rotation. Load the script into an AWS Lambda function that will upload the .csv file to an Amazon S3 bucket. Create an Amazon Athena table query that runs when the .csv file is uploaded to the S3 bucket. Publish the results for any keys older than 90 days by using an invocation of an Amazon Simple Notification Service (Amazon SNS) notification to the security team.

C. Create a script to download the IAM credentials report on a periodic basis. Load the script into an AWS Lambda function that will run on a schedule through Amazon EventBridge. Configure the Lambda script to load the report into memory and to filter the report for records in which the key was last rotated at least 90 days ago. If any records are detected, send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.

D. Create an AWS Lambda function that queries the IAM API to list all the users. Iterate through the users by using the ListAccessKeys operation. Verify that the value in the CreateDate field is not at least 90 days old. Send an Amazon Simple Notification Service (Amazon SNS) notification to the security team if the value is at least 90 days old. Create an Amazon EventBridge rule to schedule the Lambda function to run each day.

Correct Answer: *A*

Community vote distribution

A (100%)

vikasj1in 1 month, 2 weeks ago

Selected Answer: A

AWS Config managed rule (access-keys-rotated): This managed rule checks whether IAM access keys have been rotated within a specified timeframe. By configuring it to run on a periodic basis of 24 hours and setting the maxAccessKeyAge parameter to 90 days, it will automatically detect access keys that haven't been rotated in 90 or more days.

Amazon EventBridge rule: Create an EventBridge rule with an event pattern that matches the compliance type of NON_COMPLIANT from AWS Config for the access-keys-rotated managed rule. This ensures that EventBridge triggers an action when the IAM access keys are found to be non-compliant.

Amazon SNS Notification: Configure EventBridge to send an SNS notification to the security team when the event pattern matches. This will automatically notify the security team when access keys have not been rotated within the specified timeframe.

upvoted 2 times

yorkicurke 2 months ago

Selected Answer: A

The rest of the options are garbage

upvoted 2 times

[Removed] 3 months ago

Selected Answer: A

Yup.. A

upvoted 3 times

oioi 3 months ago

Selected Answer: A

correct

upvoted 2 times

Question #77 *Topic 1*

A company maintains an open-source application that is hosted on a public GitHub repository. While creating a new commit to the repository, an engineer uploaded their AWS access key and secret access key. The engineer reported the mistake to a manager, and the manager immediately disabled the access key.

The company needs to assess the impact of the exposed access key. A security engineer must recommend a solution that requires the least possible managerial overhead.

Which solution meets these requirements?

A. Analyze an AWS Identity and Access Management (IAM) use report from AWS Trusted Advisor to see when the access key was last used.

B. Analyze Amazon CloudWatch Logs for activity by searching for the access key.

C. Analyze VPC flow logs for activity by searching for the access key.

D. Analyze a credential report in AWS Identity and Access Management (IAM) to see when the access key was last used.

Correct Answer: *B*

Community vote distribution

D (100%)

brpjp 1 month, 3 weeks ago

Selected Answer: B is correct. Question is to analyze impact of exposed access key. From credential report you know only key last used, but not able to determine how many times key used and what activities performed.

upvoted 1 times

rahav 2 months ago

Selected Answer: D

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

upvoted 1 times

3633f8f 2 months, 1 week ago

Selected Answer: D

Least effort.

upvoted 1 times

kejam 3 months ago

Selected Answer: D

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

upvoted 2 times

[Removed] 3 months ago

Selected Answer: D

D 99.999999% sure

upvoted 3 times

oioi 3 months ago

Selected Answer: D

correct

upvoted 1 times

Question #78 *Topic 1*

A company plans to create individual child accounts within an existing organization in AWS Organizations for each of its DevOps teams. AWS CloudTrail has been enabled and configured on all accounts to write audit logs to an Amazon S3 bucket in a centralized AWS account. A security engineer needs to ensure that DevOps team members are unable to modify or disable this configuration.

How can the security engineer meet these requirements?

A. Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to the AWS account root user.

B. Create an S3 bucket policy in the specified destination account for the CloudTrail trail that prohibits configuration changes from the AWS account root user in the source account.

C. Create an SCP that prohibits changes to the specific CloudTrail trail and apply the SCP to the appropriate organizational unit or account in Organizations.

D. Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to a new IAM group. Have team members use individual IAM accounts that are members of the new IAM group.

Correct Answer: *C*

Community vote distribution

C (100%)

Raphaello 6 days, 2 hours ago

Selected Answer: C

Correct answer is C.
Use SCP to deny changes to the specific trail, apply the policy to designated OU or accounts.

upvoted 1 times

vikasj1in 1 month, 2 weeks ago

SCPs in AWS Organizations are used to set fine-grained permissions and restrictions on AWS accounts within an organization. They operate at the root level or organizational unit level.
the security engineer can enforce a policy at the organizational level, ensuring that no accounts under the specified organizational unit can make modifications or disable the CloudTrail configuration.While IAM policies and S3 bucket policies can control access to resources, they are typically more focused on granting permissions rather than restricting actions on CloudTrail trails globally across the organization.

Option C, using an SCP, provides centralized control and is well-suited for enforcing organization-wide policies. It ensures that even if DevOps team members have administrative permissions in their individual accounts, they won't be able to modify or disable the specified CloudTrail trail due to the SCP restrictions.

upvoted 1 times

3633f8f 2 months, 1 week ago

Selected Answer: C

C is correct.

upvoted 1 times

Aamee 3 months ago

Selected Answer: C

For sure it should be 'D'.

upvoted 2 times

Aamee 3 months ago

typo: 'C'.

upvoted 2 times

[Removed] 3 months ago

Selected Answer: C

C sounds good

upvoted 2 times

oioi 3 months ago

Selected Answer: C

correct

upvoted 1 times

Question #79 *Topic 1*

A company's policy requires that all API keys be encrypted and stored separately from source code in a centralized security account. This security account is managed by the company's security team. However, an audit revealed that an API key is stored with the source code of an AWS Lambda function in an AWS CodeCommit repository in the DevOps account.

How should the security team securely store the API key?

A. Create a CodeCommit repository in the security account using AWS Key Management Service (AWS KMS) for encryption. Require the development team to migrate the Lambda source code to this repository.

B. Store the API key in an Amazon S3 bucket in the security account using server-side encryption with Amazon S3 managed encryption keys (SSE-S3) to encrypt the key. Create a presigned URL for the S3 key, and specify the URL in a Lambda environmental variable in the AWS CloudFormation template. Update the Lambda function code to retrieve the key using the URL and call the API.

C. Create a secret in AWS Secrets Manager in the security account to store the API key using AWS Key Management Service (AWS KMS) for encryption. Grant access to the IAM role used by the Lambda function so that the function can retrieve the key from Secrets Manager and call the API.

D. Create an encrypted environment variable for the Lambda function to store the API key using AWS Key Management Service (AWS KMS) for encryption. Grant access to the IAM role used by the Lambda function so that the function can decrypt the key at runtime.

Correct Answer: *D*

Community vote distribution

C (100%)

Raphaello 4 days, 11 hours ago

Selected Answer: C

Correct answer is C.

Secrets Manager to store API key securely using KMS key. Grant access to KSM key to Lambda exec role.

upvoted 1 times

3633f8f 2 months, 1 week ago

Selected Answer: C

C is correct among others. In case there is something related to AWS Systems Manager Parameter Store as Secure String would be even better more accurate choice.

upvoted 1 times

Raphaello 2 months, 2 weeks ago

C
Whenever there is an AWS can do the job, in this scenario Secrets Manager, then it is the right choice.
Environment variable is not the right answer, despite using KMS for encryption.

upvoted 1 times

Aamee 3 months ago

Selected Answer: C

Def. 'C' is the best practice way.

upvoted 2 times

[Removed] 3 months ago

Selected Answer: C

C for the win

upvoted 2 times

oioi 3 months ago

Selected Answer: C

correct

upvoted 1 times

Question #80 *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 with the new log file prefix, and then update the log file prefix in the CloudTrail console.

D. 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.

Correct Answer: *D*

Community vote distribution

C (90%) 10%

SHERLOCKAWS 3 weeks, 1 day ago

Selected Answer: C

Explained here >> https://docs.aws.amazon.com/awscloudtrail/latest/userguide/create-s3-bucket-policy-for-cloudtrail.html#cloudtrail-add-change-or-remove-a-bucket-prefix

upvoted 2 times

vikasj1in 1 month, 2 weeks ago

C. Updating Bucket Policy: The error message indicates that there is a problem with the bucket policy. To resolve this, the security engineer needs to update the existing bucket policy in the Amazon S3 console with the new log file prefix. This ensures that the bucket policy is correctly configured to allow CloudTrail to write logs to the specified location.

Updating Log File Prefix in CloudTrail Console: Once the bucket policy is updated, the security engineer can then go back to the CloudTrail console and update the log file prefix there. This will ensure that CloudTrail knows the correct destination in the S3 bucket for storing the log files.

Option C is the correct choice as it addresses the issue by first updating the bucket policy and then updating the log file prefix in the CloudTrail console. The other options involve unnecessary steps or do not directly address the reported problem.

upvoted 1 times

WeepingMaplte 2 months, 1 week ago

Verify the S3 bucket policy:
Open the S3 bucket policy in the S3 console, CLI, or SDK.
Ensure the policy grants CloudTrail permission to write log files with the new prefix to the specified S3 bucket. Look for permissions like s3:PutObject with the correct bucket prefix included.

upvoted 1 times

vincentsr7 2 months, 2 weeks ago

B. As C does not provide the required privileges to the security engineer

upvoted 1 times

Aamee 3 months ago

Selected Answer: C

C looks legit.

upvoted 1 times

AgboolaKun 3 months ago

Selected Answer: C

The correct answer is C - https://docs.aws.amazon.com/awscloudtrail/latest/userguide/create-s3-bucket-policy-for-cloudtrail.html#cloudtrail-add-change-or-remove-a-bucket-prefix

upvoted 3 times

[Removed] 3 months ago

Selected Answer: C

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/create-s3-bucket-policy-for-cloudtrail.html#cloudtrail-add-change-or-remove-a-bucket-prefix

upvoted 3 times

oioi 3 months ago

Selected Answer: B

correct

upvoted 1 times

Question #81 *Topic 1*

A company uses AWS Organizations. The company wants to implement short-term credentials for third-party AWS accounts to use to access accounts within the company's organization. Access is for the AWS Management Console and third-party software-as-a-service (SaaS) applications. Trust must be enhanced to prevent two external accounts from using the same credentials. The solution must require the least possible operational effort.

Which solution will meet these requirements?

A. Use a bearer token authentication with OAuth or SAML to manage and share a central Amazon Cognito user pool across multiple Amazon API Gateway APIs.

B. Implement AWS IAM Identity Center (AWS Single Sign-On), and use an identity source of choice. Grant access to users and groups from other accounts by using permission sets that are assigned by account.

C. Create a unique IAM role for each external account. Create a trust policy Use AWS Secrets Manager to create a random external key.

D. Create a unique IAM role for each external account. Create a trust policy that includes a condition that uses the sts:ExternalId condition key.

Correct Answer: *C*

Community vote distribution

D (100%)

SHERLOCKAWS 3 weeks, 1 day ago

Selected Answer: D

Explained here > https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html

upvoted 1 times

vikasj1in 1 month, 2 weeks ago

Creating a unique IAM role for each external account allows you to grant specific permissions to each external account independently. Including a condition in the trust policy that uses the sts:ExternalId condition key allows you to enhance the trust between the accounts and prevent one external account from using the credentials intended for another external account. The sts:ExternalId condition ensures that the request is accompanied by the expected external ID, adding an extra layer of security.

Options A, B, and C do not specifically address the requirement to prevent two external accounts from using the same credentials and may introduce unnecessary complexity or dependencies.

upvoted 1 times

WeepingMaplte 2 months, 1 week ago

Selected Answer: D

What is an external ID:
An external ID is a unique identifier that is managed by a third-party identity provider (IdP). It's used to verify the identity of a user without requiring them to have an AWS IAM account.

Creating a role with an external ID:

You can create a role in your AWS account and specify an external ID source (e.g., SAML provider, OIDC provider).
You can define trust relationships between the role and the external IdP. This ensures that only authorized users with the correct external ID can assume the role.
You can attach IAM policies to the role to grant specific permissions to access AWS resources.

upvoted 2 times

kejam 2 months, 4 weeks ago

Selected Answer: D

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html

upvoted 3 times

Aamee 3 months ago

Selected Answer: D

C looks a bit reasonable but with a condition on the role makes it more secured so going with 'D'.

upvoted 1 times

[Removed] 3 months ago

Selected Answer: D

D will do it. The rest are distractors / incorrect

upvoted 2 times

oioi 3 months ago

Selected Answer: D

correct

upvoted 1 times

Question #82 *Topic 1*

A company is evaluating its security posture. In the past, the company has observed issues with specific hosts and host header combinations that affected the company's business. The company has configured AWS WAF web ACLs as an initial step to mitigate these issues.

The company must create a log analysis solution for the AWS WAF web ACLs to monitor problematic activity. The company wants to process all the AWS WAF logs in a central location. The company must have the ability to filter out requests based on specific hosts.

A security engineer starts to enable access logging for the AWS WAF web ACLs.

What should the security engineer do next to meet these requirements with the MOST operational efficiency?

A. Specify Amazon Redshift as the destination for the access logs. Deploy the Amazon Athena Redshift connector. Use Athena to query the data from Amazon Redshift and to filter the logs by host.

B. Specify Amazon CloudWatch as the destination for the access logs. Use Amazon CloudWatch Logs Insights to design a query to filter the logs by host.

C. Specify Amazon CloudWatch as the destination for the access logs. Export the CloudWatch logs to an Amazon S3 bucket. Use Amazon Athena to query the logs and to filter the logs by host.

D. Specify Amazon CloudWatch as the destination for the access logs. Use Amazon Redshift Spectrum to query the logs and to filter the logs by host.

Correct Answer: *B*

Community vote distribution

B (89%) 11%

vikasj1in 1 month, 2 weeks ago

B.
CloudWatch Logs Insights is a fully managed service that enables you to search and analyze your log data efficiently. It allows you to interactively explore and analyze your logs directly in the CloudWatch console.

Operational Efficiency: CloudWatch is a native AWS service that can directly receive and store AWS WAF access logs. Using CloudWatch Logs Insights, you can design and run queries to filter logs based on specific hosts. This provides a quick and efficient way to analyze and monitor AWS WAF logs centrally.

Options C and D involve additional steps such as exporting logs to S3 or using Amazon Redshift Spectrum, which may introduce additional complexity and operational overhead. Option A suggests using Amazon Redshift directly, which may not be the most efficient option for log analysis in this scenario.

Therefore, option B is the most operationally efficient solution for analyzing and filtering AWS WAF access logs in a central location.

upvoted 2 times

3633f8f 2 months, 1 week ago

Selected Answer: B

B indeed.

upvoted 1 times

WeepingMaplte 2 months, 1 week ago

Selected Answer: B

Log Insights: Provides a powerful query interface for searching and analyzing WAF logs based on various criteria like IP addresses, user agents, and rule IDs.

upvoted 1 times

AgboolaKun 3 months ago

Selected Answer: B

Agree. B is the MOST operational efficiency - https://aws.amazon.com/blogs/mt/analyzing-aws-waf-logs-in-amazon-cloudwatch-logs/

upvoted 3 times

Aamee 3 months ago

Selected Answer: B

Agreed. It asks specifically about the Operational Efficiency on this. Option C seems to be good as well but it takes a bit more steps to setup/configure those steps. Where from Option 'B', you can get it from the CW Insights features.

upvoted 1 times

lmimi 3 months ago

I think B is the MOST operational efficiency

upvoted 2 times

[Removed] 3 months ago

Selected Answer: B

voting B

upvoted 2 times

[Removed] 3 months ago

I'd argue B is more efficient. Less moving parts than C.

https://aws.amazon.com/blogs/mt/analyzing-aws-waf-logs-in-amazon-cloudwatch-logs/

upvoted 2 times

oioi 3 months ago

Selected Answer: C

correct

upvoted 1 times

Question #83 *Topic 1*

A security engineer is trying to use Amazon EC2 Image Builder to create an image of an EC2 instance. The security engineer has configured the pipeline to send logs to an Amazon S3 bucket. When the security engineer runs the pipeline, the build fails with the following error: "AccessDenied: Access Denied status code: 403".

The security engineer must resolve the error by implementing a solution that complies with best practices for least privilege access.

Which combination of steps will meet these requirements? (Choose two.)

A. Ensure that the following policies are attached to the IAM role that the security engineer is using·EC2InstanceProfileForImageBuilder, EC2InstanceProfileForImageBuilderECRContainerBuilds, and AmazonSSMManagedInstanceCore.

B. Ensure that the following policies are attached to the instance profile for the EC2 instance: EC2InstanceProfileForImageBuilder, EC2InstanceProfileForImageBuilderECRContainerBuilds, and AmazonSSMManagedInstanceCore.

C. Ensure that the AWSImageBuilderFullAccess policy is attached to the instance profile for the EC2 instance.

D. Ensure that the security engineer's IAM role has the s3:PutObject permission for the S3 bucket.

E. Ensure that the instance profile for the EC2 instance has the s3:PutObject permission for the S3 bucket.

Correct Answer: *AC*

Community vote distribution

BE (90%) 10%

Mandla97 5 days, 11 hours ago

BE
Cause
Possible causes include:

The instance profile does not have the required permissions to access APIs or component resources.

The instance profile role is missing permissions that are required for logging to Amazon S3. Most commonly, this occurs when the instance profile role does not have PutObject permissions for your S3 buckets.

Solution
Depending on the cause, this issue can be resolved as follows:

Instance profile is missing managed policies – Add the missing policies to your instance profile role. Then run the pipeline again.

Instance profile is missing write permissions for S3 bucket – Add a policy to your instance profile role that grants PutObject permissions to write to your S3 bucket. Then run the pipeline again.

upvoted 1 times

vikasj1in 1 month, 2 weeks ago

A. The IAM role used by Amazon EC2 Image Builder needs to have the necessary policies attached to perform the required actions. In this case, the role needs policies such as EC2InstanceProfileForImageBuilder,EC2InstanceProfileForImageBuilderECRContainerBuilds, and AmazonSSMManagedInstanceCore.

D: The IAM role must have the s3:PutObject permission for the specified S3 bucket. This permission is required for storing logs in the S3 bucket.

Options B and E involve attaching policies directly to the instance profile, which is not the recommended approach for Amazon EC2 Image Builder. The IAM role associated with EC2 Image Builder is used for the build process, and it is the role that needs the required permissions.

Option C is not specific to the IAM role or instance profile used by Amazon EC2 Image Builder, and it's generally not recommended to attach broad policies like AWSImageBuilderFullAccess without following the principle of least privilege.

upvoted 1 times

giancesarini2023 2 months ago

The correct answer is B/E.

upvoted 1 times

3633f8f 2 months, 1 week ago

Selected Answer: BE

BE choice as Instance Profile >> Role for the Instance on start up - usually -

upvoted 1 times

WeepingMaplte 2 months, 1 week ago

Selected Answer: BE

EC2InstanceProfileForImageBuilder, EC2InstanceProfileForImageBuilderECRContainerBuilds, and AmazonSSMManagedInstanceCore are policies.
https://docs.aws.amazon.com/imagebuilder/latest/userguide/security-iam-awsmanpol.html

Ensure the IAM roles used by Image Builder have the necessary permissions to access resources involved in the build process, like S3 buckets, EC2 instances, and SSM automation documents.

upvoted 1 times

Aamee 2 months, 3 weeks ago

Selected Answer: BE

Thanks folks!... got the EC2 Instance profile concept now so def. going with B and E now.

upvoted 1 times

snowmaggedon 2 months, 4 weeks ago

A pipeline is running so that means the engineer's role is not relevant. Answer is BE

upvoted 1 times

AgboolaKun 3 months ago

Selected Answer: BE

Please note that an instance profile is an IAM role for the EC2 instance. Therefore, the option A which states that "IAM role attached to the engineer" is wrong. Please check this link for more information - https://docs.aws.amazon.com/imagebuilder/latest/userguide/troubleshooting.html#ts-access-denied

upvoted 3 times

Aamee 3 months ago

"Solution:

Depending on the cause, this issue can be resolved as follows:
Instance profile is missing managed policies – Add the missing policies to your instance profile role. Then run the pipeline again.
Instance profile is missing write permissions for S3 bucket – Add a policy to your instance profile role that grants PutObject permissions to write to your S3 bucket. Then run the pipeline again."

The sol. states that it's EC2 Instance Profile "Role" as per their documentation. Whereas, in option B and E, it states EC2 Instance profile only. Does it mean the same thing? Can someone pls. help clarify on this.

upvoted 1 times

[Removed] 3 months ago

Selected Answer: BE

B and E as per the following

https://docs.aws.amazon.com/imagebuilder/latest/userguide/troubleshooting.html#ts-access-denied

upvoted 3 times

oioi 3 months ago

Selected Answer: DE

correct

upvoted 1 times

Question #84 *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 key that uses customer provided key material

B. A customer managed key that uses AWS provided key material

C. An AWS managed key

D. Operating system encryption that uses GnuPG

Correct Answer: *A*

Community vote distribution

A (88%) 13%

Raphaello 5 days, 7 hours ago

Selected Answer: A

Correct answer is A.
You can select your KMS key with imported key material expiration date.
https://docs.aws.amazon.com/kms/latest/developerguide/importing-keys-managing.html

upvoted 1 times

vikasj1in 1 month, 2 weeks ago

AWS Managed Key (AWS KMS): AWS managed keys (AWS KMS keys) are created, managed, and rotated by AWS KMS. AWS automatically handles key rotation for these keys. With an AWS managed key, you can set the key rotation interval, and AWS KMS will automatically rotate the key material.

Expiration: While AWS managed keys don't have an explicit "expiration" property, you can achieve similar functionality by configuring key rotation every 90 days. This ensures that the key material is automatically rotated, effectively providing a new key every 90 days.

Options A and B refer to customer managed keys, and the expiration of key material would need to be managed manually by the customer. Option D mentions GnuPG, which is not applicable for managing AWS EBS volume encryption keys.

Therefore, option C (AWS managed key) is the most suitable choice for this scenario.

upvoted 1 times

rahav 2 months ago

Selected Answer: A

You may set an expiration period for an imported key. AWS KMS will automatically delete the key material after the expiration period. You can also delete imported key material on demand. In both cases the key material itself is deleted but the KMS key reference in AWS KMS and associated metadata are retained so that the key material can be re-imported in the future. Keys generated by AWS KMS do not have an expiration time and cannot be deleted immediately; there is a mandatory 7 to 30 day wait period. All customer managed KMS keys, regardless of whether the key material was imported, can be manually disabled or scheduled for deletion. In this case the KMS key itself is deleted, not just the underlying key material.

https://aws.amazon.com/kms/faqs/

upvoted 2 times

WeepingMaplte 2 months, 1 week ago

Selected Answer: A

A will be the answer. The key word in the question is automatically expires. For answer B and C, it does not have the expiration date option. It only has the rotate option.

upvoted 1 times

vincentsr7 2 months, 2 weeks ago

Option C.
A customer managed key (option A) that uses customer provided key material would not have the automatic expiration capability by default.

upvoted 1 times

Daniel76 2 months, 2 weeks ago

When you import key material, you can set an optional expiration time.
https://docs.aws.amazon.com/kms/latest/developerguide/importing-keys-managing.html

upvoted 2 times

Aamee 3 months ago

Selected Answer: A

A sounds legit.

upvoted 1 times

[Removed] 3 months ago

Selected Answer: A

Definitely A

upvoted 1 times

AgboolaKun 3 months ago

Selected Answer: A

A is correct - https://awscli.amazonaws.com/v2/documentation/api/latest/reference/kms/import-key-material.html

upvoted 1 times

oioi 3 months ago

Selected Answer: B

correct

upvoted 1 times

Question #85 *Topic 1*

A security engineer is building a Java application that is running on Amazon EC2. The application communicates with an Amazon RDS instance and authenticates with a user name and password.

Which combination of steps can the engineer take to protect the credentials and minimize downtime when the credentials are rotated? (Choose two.)

A. Have a database administrator encrypt the credentials and store the ciphertext in Amazon S3. Grant permission to the instance role associated with the EC2 instance to read the object and decrypt the ciphertext.

B. Configure a scheduled job that updates the credential in AWS Systems Manager Parameter Store and notifies the engineer that the application needs to be restarted.

C. Configure automatic rotation of credentials in AWS Secrets Manager.

D. Store the credential in an encrypted string parameter in AWS Systems Manager Parameter Store. Grant permission to the instance role associated with the EC2 instance to access the parameter and the AWS KMS key that is used to encrypt it.

E. Configure the Java application to catch a connection failure and make a call to AWS Secrets Manager to retrieve updated credentials when the password is rotated. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.

Correct Answer: *BC*

Community vote distribution

CE (100%)

vikasj1in 1 month, 2 weeks ago

AWS Secrets Manager (Option C and E): AWS Secrets Manager provides a solution for managing and rotating sensitive information, such as database credentials. You can configure automatic rotation of credentials in AWS Secrets Manager, and the Java application can catch a connection failure and make a call to Secrets Manager to retrieve updated credentials when the password is rotated.

Systems Manager Parameter Store (Option D): While storing credentials in an encrypted string parameter in AWS Systems Manager Parameter Store is a valid approach, Secrets Manager provides a more specialized solution for credential rotation.

Option A involves storing ciphertext in Amazon S3, which adds complexity and may not be as secure as using dedicated services like AWS Secrets Manager.

Option B suggests manually updating the credential in Systems Manager Parameter Store and notifying the engineer, which is less automated and may introduce downtime.

upvoted 2 times

3633f8f 2 months, 1 week ago

Selected Answer: CE

Systems Manager provides integration with RDS and in combination with Java Try and Catch makes possible rotate credentials as frequent as required.

upvoted 1 times

rxhan 1 day, 9 hours ago

Secrets*

upvoted 1 times

Aamee 2 months, 3 weeks ago

Selected Answer: CE

Def. C and E makes perfect comb.

upvoted 1 times

Aamee 3 months ago

V confusing btw CE and DE. The question states about protecting the creds which gives the hint towards option D since it talks about leveraging KMS keys with SSM parameter store options too... No doubt on option E cuz that looks more reasonable but there's a confusion over option C or D... :(

upvoted 1 times

AgboolaKun 3 months ago

C is correct because Systems Manager Parameter Store cannot be used for key rotation. Key rotation is a feature of Secrets Manager. I hope that helps.

upvoted 4 times

Aamee 2 months, 3 weeks ago

Ah ok, got it now, thanks so much AgboolaKun! :)

upvoted 1 times

[Removed] 3 months ago

Selected Answer: CE

I'll vote C and E. Secrets Manager for rotation

upvoted 2 times

oioi 3 months ago

Selected Answer: CE

correct

upvoted 2 times

Question #86 *Topic 1*

A company uses SAML federation to grant users access to AWS accounts. A company workload that is in an isolated AWS account runs on immutable infrastructure with no human access to Amazon EC2. The company requires a specialized user known as a break glass user to have access to the workload AWS account and instances in the case of SAML errors. A recent audit discovered that the company did not create the break glass user for the AWS account that contains the workload.

The company must create the break glass user. The company must log any activities of the break glass user and send the logs to a security team.

Which combination of solutions will meet these requirements? (Choose two.)

A. Create a local individual break glass IAM user for the security team. Create a trail in AWS CloudTrail that has Amazon CloudWatch Logs turned on. Use Amazon EventBridge to monitor local user activities.

B. Create a break glass EC2 key pair for the AWS account. Provide the key pair to the security team. Use AWS CloudTrail to monitor key pair activity. Send notifications to the security team by using Amazon Simple Notification Service (Amazon SNS).

C. Create a break glass IAM role for the account. Allow security team members to perform the AssumeRoleWithSAML operation. Create an AWS CloudTrail trail that has Amazon CloudWatch Logs turned on. Use Amazon EventBridge to monitor security team activities.

D. Create a local individual break glass IAM user on the operating system level of each workload instance. Configure unrestricted security groups on the instances to grant access to the break glass IAM users.

E. Configure AWS Systems Manager Session Manager for Amazon EC2. Configure an AWS CloudTrail filter based on Session Manager. Send the results to an Amazon Simple Notification Service (Amazon SNS) topic.

Correct Answer: *DE*

Community vote distribution

AE (77%) CE (23%)

kejam Highly Voted 2 months, 4 weeks ago

Selected Answer: AE

A and E
"Although the use and creation of AWS IAM users is highly discouraged, break glass users are an exception.
To ensure human break-glass access to your environment, we recommend that you create the following in your AWS organization:
At least two IAM users..."
https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/break-glass-access.html

upvoted 5 times

Aamee 2 months, 3 weeks ago

I think ur option A might be right here cuz it asks about the IAM break-glass user and not any roles for the whole security team if I understood the question correctly...

upvoted 1 times

mynickc Most Recent 1 month ago

Selected Answer: AE

read the question carefully, it is asking for a user incase SAML error so assuming role with AssumeRoleWithSAML is not gonna work.

upvoted 1 times

vikasj1in 1 month, 2 weeks ago

C, E.
Creating a break glass IAM role allows for temporary access when needed. Allowing security team members to perform the AssumeRoleWithSAML operation ensures that the break glass user can assume the role during incidents. Configuring AWS CloudTrail with CloudWatch Logs turned on allows for the logging of activities, and EventBridge can be used to monitor those logs for security team activities.Configuring CloudTrail filters based on Session Manager actions allows logging of activities, and sending the results to an SNS topic can notify the security team.

A & B involve local user or key pair management, which may not be as scalable or auditable compared to using IAM roles and Systems Manager Session Manager.

D suggests creating local individual IAM users on the operating system level, which is not the recommended approach, as it's more challenging to manage and audit compared to IAM roles and System Manager Session Manager.

upvoted 1 times

Daniel76 1 month, 4 weeks ago

Selected Answer: AE

The rest of the options:
B- key pair is very vulnerable. very often, breakglass is sealed in physical envelope and kept in safe.
C- the question requires breakglass user. This option did not provide any user but role.
D- the question require breakglass user at account level but this option provide instance level. Besides, unrestricted security group for all such instances make them vulnerable to password guessing.

The best approach is still create breakglass at account level, seal the breakglass accounts with procedure and physical security, use cloudtrail to ensure its usage is accountable and notification to the entire security team is sent via SNS topic. The account level user allows breakglass user to access to all EC2 instances through session manager.

upvoted 2 times

brpjp 2 months ago

Correct Answer D & E:
Question is to log any activities of the break glass user and send the logs to a security team. Because of sending logs to security team, security can not be a break glass user to have adequate segregation of duties. Answer A, B and C refer to security team be a break glass user.
So correct answer is D and E.

upvoted 1 times

yorkicurke 2 months ago

Selected Answer: AE

and why i did not go for C;
Because it relies on SAML for the AssumeRoleWithSAML operation. Question mentions that there might be SAML errors. If SAML is not functioning correctly, then the AssumeRoleWithSAML operation would also fail. This means that the security team members would not be able to assume the break glass IAM role when needed, defeating the purpose of having a break glass user for emergency access.
Peace Out:)

upvoted 2 times

tayman 2 months, 1 week ago

Selected Answer: AE

Vote for A and E.

upvoted 1 times

dexterryu 2 months, 1 week ago

Selected Answer: AE

AE are correct. C would not work in the case of SAML issues which the question specifically states is the purpose.

upvoted 1 times

dexterryu 2 months, 1 week ago

AE are correct. C would not work in the case of SAML issues which the question specifically states is the purpose.

upvoted 1 times

AgboolaKun 2 months, 3 weeks ago

Selected Answer: CE

CE are the correct answers to this question. Folks choosing AE need to read these "A break glass role that is deployed to all the accounts in the organization, and that can only be 'assumed' by the break glass users from the management account. These roles are needed to allow access from the management account to apply and update guardrails, to troubleshoot and resolve issues with the automation tooling from the security tooling account, or to remediate security and operational issues in one of the member accounts in the AWS organization." sentences from the following link - https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/break-glass-access.html

upvoted 1 times

Aamee 2 months, 3 weeks ago

But if you read the question again, this is what they're asking specifically:
"The company must create the break glass user. The company must log any activities of the break glass user and send the logs to a security team."
When even the break glass user doesn't exist then how can the role be a choice here for this usecase??... You must need to create a local users first inorder to grant the role to it right?... I know it's still v confusing but that's how I interpreted this question..

upvoted 1 times

[Removed] 2 months, 3 weeks ago

Selected Answer: AE

Its A rather than C due to SAML att while using IAM roles.

upvoted 2 times

marco25 2 months, 3 weeks ago

Selected Answer: AE

A is correct need local user in case same is broken

upvoted 3 times

Aamee 3 months ago

Selected Answer: CE

C and E makes a good combo imo.

upvoted 1 times

[Removed] 3 months ago

Selected Answer: CE

I'll vote C E as well

https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/break-glass-access.html

upvoted 2 times

oioi 3 months ago

Selected Answer: CE

correct

upvoted 1 times

Question #87 *Topic 1*

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 allow 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.

Correct Answer: *ADF*

Community vote distribution

BCF (100%)

Daniel76 1 month, 4 weeks ago

Selected Answer: BCF

For API to refer to Cognito user pool, use "COGNITO_USER_POOLS" authorizer
https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-enable-cognito-user-pool.html

For Cognito user pool to act as relying party to SAML IdP
https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-saml-idp.html

Other options:
A- "As an alternative to using IAM roles and policies or Lambda authorizers (formerly known as custom authorizers), you can use an Amazon Cognito user pool to control who can access your API in Amazon API Gateway."
https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html
D - social login users not required for this question.
E - Dynamo DB is irrelevant- never store store password in db without all the additional overheads required to keep them secure.

upvoted 1 times

rahav 2 months ago

Selected Answer: BCF

BCF is logical here

upvoted 1 times

[Removed] 3 months ago

Selected Answer: BCF

BCF. This was on the other exam topics practice set

upvoted 2 times

oioi 3 months ago

Selected Answer: BCF

correct

upvoted 1 times

Question #88 *Topic 1*

A company needs to improve its ability to identify and prevent IAM policies that grant public access or cross-account access to resources. The company has implemented AWS Organizations and has started using AWS Identity and Access Management Access Analyzer to refine overly broad access to accounts in the organization.

A security engineer must automate a response in the company's organization for any newly created policies that are overly permissive. The automation must remediate external access and must notify the company's security team.

Which combination of steps should the security engineer take to meet these requirements? (Choose three.)

A. Create an AWS Step Functions state machine that checks the resource type in the finding and adds an explicit Deny statement in the trust policy for the IAM role. Configure the state machine to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.

B. Create an AWS Batch job that forwards any resource type findings to an AWS Lambda function. Configure the Lambda function to add an explicit Deny statement in the trust policy for the IAM role. Configure the AWS Batch job to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.

C. In Amazon EventBridge, create an event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution.

D. In Amazon CloudWatch, create a metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution.

E. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the queue to forward a notification to the security team that an external principal has been granted access to the specific IAM role and has been blocked.

F. Create an Amazon Simple Notification Service (Amazon SNS) topic for external or cross-account access notices. Subscribe the security team's email addresses to the topic.

Correct Answer: *ADE*

Community vote distribution

ACF (88%) 13%

[Removed] Highly Voted 3 months ago

Selected Answer: ACF

ACF make thr most sense Herr. See below:

https://aws.amazon.com/blogs/compute/orchestrating-a-security-incident-response-with-aws-step-functions/

upvoted 5 times

[Removed] 3 months ago

the* here*

upvoted 1 times

tayman Most Recent 2 months, 1 week ago

Selected Answer: ACF

Vote for A C F

upvoted 1 times

Aamee 3 months ago

Selected Answer: ACF

ACF most likely.

upvoted 1 times

oioi 3 months ago

Selected Answer: CEF

correct

upvoted 1 times

Question #89 *Topic 1*

A security engineer is configuring a mechanism to send an alert when three or more failed sign-in attempts to the AWS Management Console occur during a 5-minute period. The security engineer creates a trail in AWS CloudTrail to assist in this work.

Which solution will meet these requirements?

A. In CloudTrail, turn on Insights events on the trail. Configure an alarm on the insight with eventName matching ConsoleLogin and errorMessage matching "Failed authentication". Configure a threshold of 3 and a period of 5 minutes.

B. Configure CloudTrail to send events to Amazon CloudWatch Logs. Create a metric filter for the relevant log group. Create a filter pattern with eventName matching ConsoleLogin and errorMessage matching "Failed authentication". Create a CloudWatch alarm with a threshold of 3 and a period of 5 minutes.

C. Create an Amazon Athena table from the CloudTrail events. Run a query for eventName matching ConsoleLogin and for errorMessage matching "Failed authentication". Create a notification action from the query to send an Amazon Simple Notification Service (Amazon SNS) notification when the count equals 3 within a period of 5 minutes.

D. In AWS Identity and Access Management Access Analyzer, create a new analyzer. Configure the analyzer to send an Amazon Simple Notification Service (Amazon SNS) notification when a failed sign-in event occurs 3 times for any IAM user within a period of 5 minutes.

Correct Answer: *C*

Community vote distribution

B (100%)

cloudbusting 3 weeks, 5 days ago

Because it says alert the answer is B

upvoted 1 times

brpjp 1 month, 4 weeks ago

C is correct. Because SNS generated using detail information on finding that help security, while only CloudWatch Alarm generated do not have information as with SNS notification.

upvoted 1 times

Daniel76 2 months ago

Selected Answer: B

This is how it is done:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html#cloudwatch-alarms-for-cloudtrail-signin

upvoted 1 times

Daniel76 2 months ago

For option c, you will need Eventbridge, Lambda on top of SNS topic.
https://stackoverflow.com/questions/62823521/i-need-to-create-alerts-based-on-the-results-returned-by-queries-in-amazon-athen
Option b doesnt include SNS topic, but that is fine because the question ask for "alert" (you can find it in the console) but not "notification".

upvoted 1 times

rahav 2 months ago

Selected Answer: B

B is the answer. need an Alarm here

upvoted 1 times

Aamee 3 months ago

Selected Answer: B

CW alarm is best suited here for this scenario.

upvoted 1 times

[Removed] 3 months ago

Selected Answer: B

B it is. Insights does not do alarming

upvoted 2 times

oioi 3 months ago

Selected Answer: B

correct

upvoted 1 times

Question #90 *Topic 1*

A company's security engineer is developing an incident response plan to detect suspicious activity in an AWS account for VPC hosted resources. The security engineer needs to provide visibility for as many AWS Regions as possible.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

A. Turn on VPC Flow Logs for all VPCs in the account.

B. Activate Amazon GuardDuty across all AWS Regions.

C. Activate Amazon Detective across all AWS Regions.

D. Create an Amazon Simple Notification Service (Amazon SNS) topic. Create an Amazon EventBridge rule that responds to findings and publishes the findings to the SNS topic.

E. Create an AWS Lambda function. Create an Amazon EventBridge rule that invokes the Lambda function to publish findings to Amazon Simple Email Service (Amazon SES).

Correct Answer: *BE*

Community vote distribution

BD (79%) AB (21%)

AgboolaKun Highly Voted 3 months ago

Selected Answer: BD

BD are the correct options here. The keywords here are "developing an incident response plan to detect suspicious activity". There is no better way to develop incident response plan without providing a way for the relevant stakeholders to take actions or respond to suspicious activities.

B is an obvious option because GuardDuty can monitor and analyze API calls across all AWS Regions, and network activities found in Amazon CloudTrail Events, Amazon VPC Flow Logs, and DNS Logs. Therefore, option A is not needed since GuardDuty monitoring activities include the VPC Flow Logs.

There is no better way to respond to the findings generated by GuardDuty than the services described in option D.

upvoted 8 times

Aamee 2 months, 3 weeks ago

Ok, but why the Detective svc. wasn't a good choice here as it's for developing an incident response plan to 'detect' right?... Agree with option D on the other hand cuz it makes sense..

upvoted 1 times

lightrod Most Recent 2 weeks, 4 days ago

Selected Answer: BD

GuardDuty analyzes VPC flow logs regardless of if you have turned them on or not

upvoted 1 times

rahav 2 months ago

Selected Answer: BD

VPC Flow logs are very expensive.... Guardduty is the right tool to do that with eventbridge

upvoted 1 times

WeepingMaplte 2 months, 1 week ago

Selected Answer: BD

A. Turn on VPC Flow Logs for all VPCs in the account: While VPC Flow Logs offer detailed information about network traffic, analyzing and storing logs for all VPCs across Regions can incur significant storage and processing costs.
C. Activate Amazon Detective across all AWS Regions: Detective focuses on root cause analysis and investigation, which might be overkill for initial detection and notification. Additionally, its per-hour billing model can quickly become expensive for continuous monitoring across multiple Regions.
E. Create an AWS Lambda function for publishing findings to SES: While Lambda offers flexibility, creating and maintaining a custom Lambda function specifically for publishing findings can add development and operational overhead compared to the readily available options with EventBridge and SNS.

upvoted 1 times

Aamee 3 months ago

Selected Answer: AB

AB options best suited. Self-explantory too.

upvoted 1 times

[Removed] 3 months ago

Selected Answer: AB

AB are correcto

upvoted 1 times

oioi 3 months ago

Selected Answer: AB

correct

upvoted 1 times

Question #91 *Topic 1*

A company stores images for a website in an Amazon S3 bucket. The company is using Amazon CloudFront to serve the images to end users. The company recently discovered that the images are being accessed from countries where the company does not have a distribution license.

Which actions should the company take to secure the images to limit their distribution? (Choose two.)

A. Update the S3 bucket policy to restrict access to a CloudFront origin access control (OAC).

B. Update the website DNS record to use an Amazon Route 53 geolocation record deny list of countries where the company lacks a license.

C. Add a CloudFront geo restriction deny list of countries where the company lacks a license.

D. Update the S3 bucket policy with a deny list of countries where the company lacks a license.

E. Enable the Restrict Viewer Access option in CloudFront to create a deny list of countries where the company lacks a license.

Correct Answer: *AB*

Community vote distribution

AC (91%) 9%

Raphaello 5 days, 14 hours ago

Selected Answer: AC

Restrict access to CF distro through OAC might not directly help with geo-restriction, until you pick option C alongside it. It enforces flow to be only through CF, where the geo-restriction in place.

AC are correct.

upvoted 1 times

Gafa255 1 month ago

Selected Answer: AC

AC correct options. https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html

upvoted 1 times

Gafa255 1 month ago

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

upvoted 1 times

kejam 2 months, 4 weeks ago

Selected Answer: AC

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html

upvoted 3 times

Aamee 3 months ago

Selected Answer: AC

A describes how to limit the access via the policy to bound the access within OAC.
C describes about using the geo restriction based R53 policy you can use to limit the access on the unwanted countries.

upvoted 1 times

Aamee 3 months ago

typo: It's Geo restriction list in CloudFront and not R53 policy, my bad!...

upvoted 1 times

[Removed] 3 months ago

Selected Answer: AC

A so the object requests do not bypass Cloudfront, and C for georestrictions. Careful with this oioi fella 👀

upvoted 4 times

Aamee 3 months ago

Fully agreed on ur 'oioi' feedback :D..

upvoted 1 times

oioi 3 months ago

Selected Answer: CE

correct

upvoted 1 times

Question #92 *Topic 1*

A company has deployed servers on Amazon EC2 instances in a VPC. External vendors access these servers over the internet. Recently, the company deployed a new application on EC2 instances in a new CIDR range. The company needs to make the application available to the vendors.

A security engineer verified that the associated security groups and network ACLs are allowing the required ports in the inbound direction. However, the vendors cannot connect to the application.

Which solution will provide the vendors access to the application?

A. Modify the security group that is associated with the EC2 instances to have the same outbound rules as inbound rules.

B. Modify the network ACL that is associated with the CIDR range to allow outbound traffic to ephemeral ports.

C. Modify the inbound rules on the internet gateway to allow the required ports.

D. Modify the network ACL that is associated with the CIDR range to have the same outbound rules as inbound rules.

Correct Answer: *C*

Community vote distribution

B (89%) 11%

NoCrapEva 1 week, 6 days ago

Selected Answer: B

Ephemeral ports are necessary for certain network responses and are dependant on the client type (O/S)...
The client that initiates the request chooses the ephemeral port range. The range varies depending on the client's operating system.
Many Linux kernels (including the Amazon Linux kernel) use ports 32768-61000.
Requests originating from Elastic Load Balancing use ports 1024-65535.
Windows operating systems through Windows Server 2003 use ports 1025-5000.
Windows Server 2008 and later versions use ports 49152-65535.
A NAT gateway uses ports 1024-65535.
AWS Lambda functions use ports 1024-65535.
For example, if a request comes into a web server in your VPC from a Windows 10 client on the internet, your network ACL must have an outbound rule to enable traffic destined for ports 49152-65535.
REF:
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#nacl-ephemeral-ports

upvoted 1 times

Jamshif01 1 month ago

I don't understand why they are called 'ephmeral' ports

upvoted 1 times

tayman 2 months, 1 week ago

Selected Answer: B

Definitely B.

upvoted 2 times

ykhan321 2 months, 1 week ago

Did someone take the test recently? How many questons appeared from here?

upvoted 2 times

Aamee 3 months ago

Selected Answer: B

Agreed with B.

upvoted 1 times

[Removed] 3 months ago

Selected Answer: B

B. You must allow the ephemeral ports in the outbound NACL for the CIDR range.

upvoted 4 times

oioi 3 months ago

Selected Answer: D

correct

upvoted 1 times

Question #93 *Topic 1*

A company uses infrastructure as code (IaC) to create AWS infrastructure. The company writes the code as AWS CloudFormation templates to deploy the infrastructure. The company has an existing CI/CD pipeline that the company can use to deploy these templates.

After a recent security audit, the company decides to adopt a policy-as-code approach to improve the company's security posture on AWS. The company must prevent the deployment of any infrastructure that would violate a security policy, such as an unencrypted Amazon Elastic Block Store (Amazon EBS) volume.

Which solution will meet these requirements?

A. Turn on AWS Trusted Advisor. Configure security notifications as webhooks in the preferences section of the CI/CD pipeline.

B. Turn on AWS Config. Use the prebuilt rules or customized rules. Subscribe tile CI/CD pipeline to an Amazon Simple Notification Service (Amazon SNS) topic that receives notifications from AWS Config.

C. Create rule sets in AWS CloudFormation Guard. Run validation checks for CloudFormation templates as a phase of the CI/CD process.

D. Create rule sets as SCPs. Integrate the SCPs as a part of validation control in a phase of the CI/CD process.

Correct Answer: *A*

Community vote distribution

C (100%)

Daniel76 2 months, 2 weeks ago

Selected Answer: C

https://aws.amazon.com/blogs/mt/policy-as-code-for-securing-aws-and-third-party-resource-types/

upvoted 1 times

Aamee 3 months ago

Selected Answer: C

C definitely. CFN Guard defined rule sets help in preventing from the derivation of Infrastructure resource security policies..

upvoted 2 times

[Removed] 3 months ago

Selected Answer: C

C for sure

upvoted 2 times

oioi 3 months ago

Selected Answer: C

correct

upvoted 1 times

Question #94 *Topic 1*

A company is running an Amazon RDS for MySQL DB instance in a VPC. The VPC must not send or receive network traffic through the internet.

A security engineer wants to use AWS Secrets Manager to rotate the DB instance credentials automatically. Because of a security policy, the security engineer cannot use the standard AWS Lambda function that Secrets Manager provides to rotate the credentials.

The security engineer deploys a custom Lambda function in the VPC. The custom Lambda function will be responsible for rotating the secret in Secrets Manager. The security engineer edits the DB instance's security group to allow connections from this function. When the function is invoked, the function cannot communicate with Secrets Manager to rotate the secret properly.

What should the security engineer do so that the function can rotate the secret?

A. Add an egress-only internet gateway to the VPC. Allow only the Lambda function's subnet to route traffic through the egress-only internet gateway.

B. Add a NAT gateway to the VPC. Configure only the Lambda function's subnet with a default route through the NAT gateway.

C. Configure a VPC peering connection to the default VPC for Secrets Manager. Configure the Lambda function's subnet to use the peering connection for routes.

D. Configure a Secrets Manager interface VPC endpoint. Include the Lambda function's private subnet during the configuration process.

Correct Answer: *D*

Community vote distribution

D (100%)

Daniel76 2 months, 2 weeks ago

Selected Answer: D

https://docs.aws.amazon.com/secretsmanager/latest/userguide/vpc-endpoint-overview.html

upvoted 1 times

Aamee 3 months ago

Selected Answer: D

D looks legit.

upvoted 2 times

[Removed] 3 months ago

Selected Answer: D

D is the winner

upvoted 1 times

oioi 3 months ago

Selected Answer: D

correct

upvoted 1 times

Question #95 *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 Service (AWS KMS) to encrypt all the traffic between the client and application servers.

Correct Answer: *AC*

Community vote distribution

BD (100%)

AgboolaKun Highly Voted 3 months ago

Selected Answer: BD

Security groups for reducing the attack surface,
Amazon Inspector to scan for and mitigate known vulnerabilities

upvoted 7 times

Aamee Most Recent 3 months ago

Selected Answer: BD

B and D , self-explanatory..

upvoted 1 times

[Removed] 3 months ago

Selected Answer: BD

B D. Moderator, please correct the default answers

upvoted 1 times

oioi 3 months ago

Selected Answer: BD

correct

upvoted 1 times

Question #96 *Topic 1*

A company is using Amazon Elastic Container Service (Amazon ECS) to run its container-based application on AWS. The company needs to ensure that the container images contain no severe vulnerabilities. The company also must ensure that only specific IAM roles and specific AWS accounts can access the container images.

Which solution will meet these requirements with the LEAST management overhead?

A. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use identity-based policies to restrict access to which IAM principals can access the images.

B. Pull images from the public container registry. Publish the images to a private container registry that is hosted on Amazon EC2 instances in a centralized AWS account. Deploy host-based container scanning tools to EC2 instances that run Amazon ECS. Restrict access to the container images by using basic authentication over HTTPS.

C. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.

D. Pull images from the public container registry. Publish the images to AWS CodeArtifact repositories in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.

Correct Answer: *A*

Community vote distribution

C (100%)

Gafa255 1 month ago

Selected Answer: C

https://docs.aws.amazon.com/AmazonECR/latest/userguide/repository-policies.html

upvoted 1 times

Daniel76 2 months, 2 weeks ago

Selected Answer: C

https://docs.aws.amazon.com/AmazonECR/latest/userguide/repository-policies.html

upvoted 1 times

AgboolaKun 3 months ago

Selected Answer: C

C is the correct answer. Please refer to https://aws.amazon.com/premiumsupport/knowledge-center/secondary-account-access-ecr/

upvoted 2 times

Aamee 3 months ago

Selected Answer: C

Should be C as it logically answers for not only the question of providing a solution of vulnerable free container image process but also covers the method of its access restrictions via IAM roles/principals and accounts as well.

upvoted 1 times

[Removed] 3 months ago

Selected Answer: C

I like C. More hardened than A?

upvoted 1 times

[Removed] 3 months ago

A also doesn't mention account restrictions so C for sure

upvoted 2 times

oioi 3 months ago

Selected Answer: C

correct

upvoted 1 times

Question #97 *Topic 1*

A company's data scientists want to create artificial intelligence and machine learning (AI/ML) training models by using Amazon SageMaker. The training models will use large datasets in an Amazon S3 bucket. The datasets contain sensitive information.

On average, the data scientists need 30 days to train models. The S3 bucket has been secured appropriately. The company's data retention policy states that all data that is older than 45 days must be removed from the S3 bucket.

Which action should a security engineer take to enforce this data retention policy?

A. Configure an S3 Lifecycle rule on the S3 bucket to delete objects after 45 days.

B. Create an AWS Lambda function to check the last-modified date of the S3 objects and delete objects that are older than 45 days. Create an S3 event notification to invoke the Lambda function for each PutObject operation.

C. Create an AWS Lambda function to check the last-modified date of the S3 objects and delete objects that are older than 45 days. Create an Amazon EventBridge rule to invoke the Lambda function each month.

D. Configure S3 Intelligent-Tiering on the S3 bucket to automatically transition objects to another storage class.

Correct Answer: *D*

Community vote distribution

A (100%)

rahav 2 months ago

Selected Answer: A

A is correct. need to be removed

upvoted 1 times

ykhan321 2 months, 1 week ago

Selected Answer: A

correct

upvoted 1 times

Aamee 3 months ago

Selected Answer: A

Option A is sufficient to complete the required asks.

upvoted 3 times

[Removed] 3 months ago

Selected Answer: A

A. The rest are just pure comedy

upvoted 2 times

AgboolaKun 3 months ago

Laughing!!! I agree, they are just pure comedy.

upvoted 1 times

oioi 3 months ago

Selected Answer: A

correct

upvoted 1 times

Question #98 *Topic 1*

A security engineer is troubleshooting an AWS Lambda function that is named MyLambdaFunction. The function is encountering an error when the function attempts to read the objects in an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET. The S3 bucket has the following bucket policy:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "lambda.amazonaws.com"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:lambda:::function:MyLambdaFunction"
        }
    }
}
```

Which change should the security engineer make to the policy to ensure that the Lambda function can read the bucket objects?

A. Remove the Condition element. Change the Principal element to the following:

```
{
    "AWS": "arn:aws:lambda:::function:MyLambdaFunction"
}
```

B. Change the Action element to the following:

```
[
    "s3:GetObject*",
    "s3:GetBucket*"
]
```

C. Change the Resource element to "arn:aws:s3:::DOC-EXAMPLE- BUCKET/*".

D. Change the Resource element to "arn:aws:lambda:::function:MyLambdaFunction". Change the Principal element to the following:

```
{
    "Service": "s3.amazonaws.com"
}
```

Correct Answer: *B*

Community vote distribution

C (100%)

Aamee Highly Voted 3 months ago

Selected Answer: C

Yup, option C is absolutely correct since there's nothing wrong on any other areas except the missing ' * ' under the Resource element.

upvoted 6 times

Gafa255 Most Recent 1 month ago

Selected Answer: C

missing the *

upvoted 1 times

[Removed] 3 months ago

Selected Answer: C

C. Missing the *

upvoted 2 times

Question #99 *Topic 1*

An IAM user receives an Access Denied message when the user attempts to access objects in an Amazon S3 bucket. The user and the S3 bucket are in the same AWS account. The S3 bucket is configured to use server-side encryption with AWS KMS keys (SSE-KMS) to encrypt all of its objects at rest by using a customer managed key from the same AWS account. The S3 bucket has no bucket policy defined. The IAM user has been granted permissions through an IAM policy that allows the kms:Decrypt permission to the customer managed key. The IAM policy also allows the s3:List* and s3:Get* permissions for the S3 bucket and its objects.

Which of the following is a possible reason that the IAM user cannot access the objects in the S3 bucket?

A. The IAM policy needs to allow the kms:DescribeKey permission.

B. The S3 bucket has been changed to use the AWS managed key to encrypt objects at rest.

C. An S3 bucket policy needs to be added to allow the IAM user to access the objects.

D. The KMS key policy has been edited to remove the ability for the AWS account to have full access to the key.

Correct Answer: *B*

Community vote distribution

D (100%)

vikasj1in 1 month, 1 week ago

The IAM user has been granted the kms:Decrypt permission for the customer managed key used for server-side encryption in the S3 bucket. If the KMS key policy has been modified to restrict access, it might override the IAM user's permissions, resulting in an Access Denied error.

It's crucial to ensure that the KMS key policy grants the necessary permissions to the AWS account (and by extension, the IAM user) to perform the required decryption operations.

upvoted 1 times

Daniel76 2 months ago

Selected Answer: D

If you allow by IAM policy to a key, it still can be denied by key policy (which is another policy) unless you explicitly allows.
"Unless the key policy explicitly allows it, you cannot use IAM policies to allow access to a KMS key. Without permission from the key policy, IAM policies that allow permissions have no effect."

upvoted 2 times

Daniel76 2 months ago

https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html

upvoted 1 times

azure4life 2 months, 2 weeks ago

Selected Answer: D

The possible reason that the IAM user cannot access the objects in the S3 bucket is that the KMS key policy has been edited to remove the ability for the AWS account to have full access to the key.

Since the S3 bucket is using SSE-KMS encryption with a customer managed key, the key policy for that KMS key needs to grant the appropriate permissions to allow decryption of the objects. The IAM policy grants the kms:Decrypt permission, but if the key policy no longer gives the AWS account full access, the decrypt permission will still be denied.

Options A and B relate to the kms:DescribeKey permission and AWS managed keys, but a customer managed key is being used here. Option C is incorrect because an S3 bucket policy is not required when using IAM policies for permissions. Therefore, option D that mentions the KMS key policy having inappropriate access for the account is the likely reason for the access being denied.

upvoted 3 times

kejam 2 months, 4 weeks ago

Selected Answer: D

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

upvoted 1 times

Aamee 3 months ago

Selected Answer: D

The following statement leads me to believe that option D could be the best option:
'The S3 bucket is configured to use server-side encryption with AWS KMS keys (SSE-KMS) to encrypt all of its objects at rest by using a customer managed key from the same AWS account'.

upvoted 1 times

[Removed] 3 months ago

Selected Answer: D

D is correct

upvoted 2 times

oioi 3 months ago

Selected Answer: D

correct

upvoted 1 times

Question #100 *Topic 1*

A company has a guideline that mandates the encryption of all Amazon S3 bucket data in transit. A security engineer must implement an S3 bucket policy that denies any S3 operations if data is not encrypted.

Which S3 bucket policy will meet this requirement?

A.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowSSLRequestsOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        ],
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "true"
            }
        },
        "Principal": "*"
    }]
}
```

B.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowSSLRequestsOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        ],
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "false"
            }
        },
        "Principal": "*"
    }]
}
```

C.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowSSLRequestsOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        ],
        "Condition": {
            "StringNotEquals": {
                "s3:x-amz-server-side-encryption": "AES256"
            }
        },
        "Principal": "*"
    }]
}
```

D.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowSSLRequestsOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        ],
        "Condition": {
            "StringNotEquals": {
                "s3:x-amz-server-side-encryption": true
            }
        },
        "Principal": "*"
    }]
}
```

Correct Answer: *A*

Community vote distribution

B (91%) 9%

awssecuritynewbie 5 days, 6 hours ago

Selected Answer: B

yeah is not good question, it should of been allow if thestring not equal : encrypted"

upvoted 1 times

awssecuritynewbie 1 week, 2 days ago

Selected Answer: B

It is defo B, you are denying access if the condition is set not to encrypt in trasnit

upvoted 1 times

cannoe 1 month, 1 week ago

The question is a bit tricky for me.

The requirement is: "A security engineer must implement an S3 bucket policy that denies any S3 operations if data is not encrypted."

Using HTTPS as a connection does not encrypt the data, it encrypts the connection. When using HTTPS to access an Amazon S3 bucket, the HTTPS encryption is de-encapsulated at the S3 service endpoint. This means the data transmitted between your application and the S3 endpoint is encrypted in transit using HTTPS, but once it reaches the S3 endpoint, the encryption is removed before the data is stored in S3.

upvoted 1 times

Aamee 2 months, 3 weeks ago

Selected Answer: B

Updated selection: Def. B

upvoted 2 times

kejam 2 months, 4 weeks ago

Selected Answer: B

Enforce encryption of data in transit
https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html#security-best-practices-prevent

upvoted 1 times

AgboolaKun 3 months ago

Selected Answer: B

This question is requesting to make objects accessible only through HTTPS. Option B is correct because it specifies the bucket policy condition with correct syntax.

Please refer to "Defense-in-depth requirement 2: Data must be accessible only by a limited set of public IP addresses" section in this link - https://aws.amazon.com/blogs/security/how-to-use-bucket-policies-and-apply-defense-in-depth-to-help-secure-your-amazon-s3-data/

upvoted 3 times

Aamee 2 months, 3 weeks ago

Thnx so much... got the concept cleared now so def. going with B here now..

upvoted 1 times

Aamee 3 months ago

Selected Answer: C

Not sure if I'm fully correct here in selecting this ans. I'd go with C here cuz I feel like it is asked about no S3 bucket operation IF the data is not encrypted. It doesn't say about if the data is not securely in transit. That's why in my opinion, the AES256 encryption method should be mentioned under the conditional logic area in the bucket policy.

But I'd appreciate if anyone else would like to discuss and clarify my understandings on this if I'm incorrect here... Thnx so much!

upvoted 1 times

[Removed] 3 months ago

Selected Answer: B

B. You want to deny where secure transport is false

upvoted 2 times

Wije1 3 months ago

https://repost.aws/knowledge-center/s3-bucket-policy-for-config-rule

upvoted 2 times

Question #101 *Topic 1*

A security engineer wants to use Amazon Simple Notification Service (Amazon SNS) to send email alerts to a company's security team for Amazon GuardDuty findings that have a High severity level. The security engineer also wants to deliver these findings to a visualization tool for further examination.

Which solution will meet these requirements?

A. Set up GuardDuty to send notifications to an Amazon CloudWatch alarm with two targets in CloudWatch. From CloudWatch, stream the findings through Amazon Kinesis Data Streams into an Amazon Open Search Service domain as the first target for delivery. Use Amazon QuickSight to visualize the findings. Use OpenSearch queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for the CloudWatch alarm. Use event pattern matching with an Amazon EventBridge event rule to send only High severity findings in the alerts.

B. Set up GuardDuty to send notifications to AWS CloudTrail with two targets in CloudTrail. From CloudTrail, stream the findings through Amazon Kinesis Data Firehose into an Amazon OpenSearch Service domain as the first target for delivery. Use OpenSearch Dashboards to visualize the findings. Use OpenSearch queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for CloudTrail. Use event pattern matching with a CloudTrail event rule to send only High severity findings in the alerts.

C. Set up GuardDuty to send notifications to Amazon EventBridge with two targets. From EventBridge, stream the findings through Amazon Kinesis Data Firehose into an Amazon OpenSearch Service domain as the first target for delivery. Use OpenSearch Dashboards to visualize the findings. Use OpenSearch queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for EventBridge. Use event pattern matching with an EventBridge event rule to send only High severity findings in the alerts.

D. Set up GuardDuty to send notifications to Amazon EventBridge with two targets. From EventBridge, stream the findings through Amazon Kinesis Data Streams into an Amazon OpenSearch Service domain as the first target for delivery. Use Amazon QuickSight to visualize the findings. Use OpenSearch queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for EventBridge. Use event pattern matching with an EventBridge event rule to send only High severity findings in the alerts.

Correct Answer: *D*

Community vote distribution

C (82%) D (18%)

mynickc 1 month ago

Selected Answer: C

D is not right because you need to perform a few activities to establish connection b/w Opensearch and QuickSight which is missing in choice D

upvoted 1 times

vikasj1in 1 month, 1 week ago

Selected Answer: C

This option involves using EventBridge to handle the GuardDuty findings and then routing them to two targets:

Streaming the findings through Kinesis Data Firehose into an Amazon OpenSearch Service domain for visualization.
Sending email alerts to the security team via SNS, with event pattern matching to filter only high severity findings.
This approach leverages the flexibility of EventBridge to manage the workflow and routing of events to different services based on specific criteria.

upvoted 1 times

happy34 1 month, 2 weeks ago

C - it filters only High alerts.

upvoted 1 times

WeepingMaplte 2 months ago

https://github.com/aws-samples/siem-on-amazon-opensearch-service

upvoted 1 times

dexterryu 2 months ago

D is correct due to Quicksight which is AWS's preferred visualization tool. The blog linked below is dated (from 2018), and while still valid not the best way to do visualization in AWS.

You can still use the OS querry in Quicksight.
https://docs.aws.amazon.com/quicksight/latest/user/connecting-to-os.html

upvoted 1 times

happy34 1 month, 1 week ago

Quick sight works with Cloudwatch Open Seach has its own dashboard. Not sure if Quicksight works with OpenSearch

upvoted 1 times

Daniel76 2 months ago

Selected Answer: C

According to this AWS article, it is GuardDuty -> EventBrdige -> Firehouse -> OpenSearch -> OpenSearch visualization.
https://aws.amazon.com/blogs/security/visualizing-amazon-guardduty-findings/

upvoted 4 times

tayman 2 months ago

Selected Answer: C

Vote for C

upvoted 1 times

ykhan321 2 months, 1 week ago

Selected Answer: D

QuickSight is the hint for Visualization.

upvoted 2 times

azure4life 2 months, 2 weeks ago

Selected Answer: D

Option D is the correct solution.

GuardDuty can send findings to Amazon EventBridge. EventBridge can then stream to targets like Kinesis Data Streams to process and store the findings, and SNS to send email alerts. Using EventBridge event pattern matching allows filtering findings based on properties like severity. Kinesis Data Streams can feed findings into OpenSearch Service. OpenSearch Dashboards or Amazon QuickSight can visualize the findings, while OpenSearch queries can provide analysis.

Option A is incorrect because GuardDuty integrates with EventBridge, not CloudWatch Alarms.
Option B is incorrect because GuardDuty integrates with EventBridge, not CloudTrail.
Option C is incorrect because Kinesis Data Firehose would not allow querying and analysis of findings - Kinesis Data Streams enables this with OpenSearch.

upvoted 1 times

Th3Dud3 1 month, 3 weeks ago

(C) - Kinesis Data *Streams* can't send to OpenSearch...

upvoted 2 times

Egle 2 months, 3 weeks ago

Selected Answer: C

correct

upvoted 1 times

kejam 2 months, 4 weeks ago

Selected Answer: C

https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_settingup.html#setup-sns

https://aws.amazon.com/blogs/big-data/audit-aws-service-events-with-amazon-eventbridge-and-amazon-kinesis-data-firehose/

https://aws.amazon.com/blogs/big-data/ingest-streaming-data-into-amazon-elasticsearch-service-within-the-privacy-of-your-vpc-with-amazon-kinesis-data-firehose/

upvoted 4 times

[Removed] 3 months ago

Selected Answer: C

C gets the job done

upvoted 1 times

oioi 3 months ago

Selected Answer: C

correct

upvoted 1 times

Question #102 *Topic 1*

A security engineer needs to implement a write-once-read-many (WORM) model for data that a company will store in Amazon S3 buckets. The company uses the S3 Standard storage class for all of its S3 buckets. The security engineer must ensure that objects cannot be overwritten or deleted by any user, including the AWS account root user.

Which solution will meet these requirements?

A. Create new S3 buckets with S3 Object Lock enabled in compliance mode. Place objects in the S3 buckets.

B. Use S3 Glacier Vault Lock to attach a Vault Lock policy to new S3 buckets. Wait 24 hours to complete the Vault Lock process. Place objects in the S3 buckets.

C. Create new S3 buckets with S3 Object Lock enabled in governance mode. Place objects in the S3 buckets.

D. Create new S3 buckets with S3 Object Lock enabled in governance mode. Add a legal hold to the S3 buckets. Place objects in the S3 buckets.

Correct Answer: *B*

Community vote distribution

A (100%)

Jamshif01 1 month ago

A
https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-configure.html

upvoted 1 times

confusedyeti69 2 months, 3 weeks ago

Selected Answer: A

In compliance mode, a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account. When an object is locked in compliance mode, its retention mode can't be changed, and its retention period can't be shortened. Compliance mode helps ensure that an object version can't be overwritten or deleted for the duration of the retention period.

In governance mode, users can't overwrite or delete an object version or alter its lock settings unless they have special permissions. With governance mode, you protect objects against being deleted by most users, but you can still grant some users permission to alter the retention settings or delete the objects if necessary. You can also use governance mode to test retention-period settings before creating a compliance-mode retention period.

upvoted 3 times

kejam 2 months, 4 weeks ago

Selected Answer: A

https://aws.amazon.com/s3/features/object-lock/

upvoted 2 times

Aamee 3 months ago

Selected Answer: A

Option A would work in this usecase.

upvoted 1 times

[Removed] 3 months ago

Selected Answer: A

A rings the most bells

upvoted 1 times

oioi 3 months ago

Selected Answer: A

coorect

upvoted 1 times

Question #103 *Topic 1*

A company needs complete encryption of the traffic between external users and an application. The company hosts the application on a fleet of Amazon EC2 instances that run in an Auto Scaling group behind an Application Load Balancer (ALB).

How can a security engineer meet these requirements?

A. Create a new Amazon-issued certificate in AWS Secrets Manager. Export the certificate from Secrets Manager. Import the certificate into the ALB and the EC2 instances.

B. Create a new Amazon-issued certificate in AWS Certificate Manager (ACM). Associate the certificate with the ALExport the certificate from ACM. Install the certificate on the EC2 instances.

C. Import a new third-party certificate into AWS Identity and Access Management (IAM). Export the certificate from IAM. Associate the certificate with the ALB and the EC2 instances.

D. Import a new third-party certificate into AWS Certificate Manager (ACM). Associate the certificate with the ALB. Install the certificate on the EC2 instances.

Correct Answer: *C*

Community vote distribution

D (83%) B (17%)

AgboolaKun Highly Voted 3 months ago

Selected Answer: D

Because of the wording of this question, I did not first know which of the options B and D is correct.

However, my conviction that you can't directly install Amazon-issued certificates on EC2 instances (refer to - https://repost.aws/knowledge-center/associate-acm-certificate-alb-nlb for more information) made me to study a few documentations to be sure D is the correct answer.

Please check the Accepted answer in the following thread - https://repost.aws/questions/QUIo7PWvZ3T6aFYCByhZ5f0A/load-certificate-on-alb-and-ec2

upvoted 7 times

vikasj1in Most Recent 1 month, 1 week ago

B.
To achieve complete encryption of the traffic between external users and an application hosted on Amazon EC2 instances behind an Application Load Balancer (ALB), you would typically use SSL/TLS encryption. AWS Certificate Manager (ACM) provides a managed service for provisioning and renewing SSL/TLS certificates.

Here's how the process works:

Create a new Amazon-issued certificate in ACM.
Associate the certificate with the ALB. This ensures that the ALB can terminate SSL/TLS connections on behalf of the EC2 instances.
Export the certificate from ACM.
Install the exported certificate on the EC2 instances. This ensures that the communication between the ALB and EC2 instances is also encrypted.
By using ACM, you benefit from the managed certificate service, automated certificate renewal, and easy integration with other AWS services like ALB. This approach ensures secure communication from external users to the ALB and between the ALB and EC2 instances.

upvoted 1 times

Daniel76 2 months, 1 week ago

Selected Answer: D

ACM should be used, so A and C are out.
Between B and D, B is out because Amazon-issued public cert cannot be installed on EC2 instances.
https://repost.aws/knowledge-center/associate-acm-certificate-alb-nlb

upvoted 1 times

azure4life 2 months, 2 weeks ago

Selected Answer: D

Option D is the correct solution.

To encrypt traffic between external users and the application behind the Application Load Balancer (ALB), a certificate should be imported into AWS Certificate Manager (ACM) and associated with the ALB. The same certificate should also be installed on the EC2 instances.

Option A is incorrect because Secrets Manager is used for storing secrets, not SSL/TLS certificates.

Option B is incorrect because Amazon-issued ACM certificates can only be used with Elastic Load Balancers and Amazon CloudFront. They cannot be exported and installed on EC2 instances.

Option C is incorrect because IAM does not support importing or managing SSL/TLS certificates.

Option D uses a third-party certificate imported into ACM, associated with the ALB, and installed on the EC2 instances. This provides complete encryption between the users and application.

upvoted 2 times

Oralinux 2 months, 2 weeks ago

Bad question; I think it should be B since AWS always tries to promote and use internal services and not go to third parties. We deploy SSL in ALB terminate and send non-SSL to EC2. In my opinion, the provided answers are incorrect.

upvoted 2 times

snowmaggedon 2 months, 4 weeks ago

CAN'T use an ACM cert on ec2 instance. D is the right answer.

upvoted 1 times

Aamee 3 months ago

Selected Answer: B

I think it's asking about the key difference btw creating Amazon based Cert versus creating/using 3rd party Certs.... specially on leveraging the feature of 'exporting the Cert' from ACM which looks valid in option B only whereas on other choices, it's not a good fit. I could be wrong but that's what makes me feel to go with option B here..

upvoted 1 times

[Removed] 3 months ago

Kind of a bad question here, so I can't really make a proper decision between B and D.. What certificate is being applied? ALB does not pass encrypted traffic to a target. NLB will do that.

you must deploy at least one SSL server certificate on your load balancer. The load balancer uses a server certificate to terminate the front-end connection and then decrypt requests from clients before sending them to the targets. You must also specify a security policy, which is used to negotiate secure connections between clients and the load balancer.

If you need to pass encrypted traffic to targets without the load balancer decrypting it, you can create a Network Load Balancer or Classic Load Balancer with a TCP listener on port 443. With a TCP listener, the load balancer passes encrypted traffic through to the targets without decrypting it.

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html

upvoted 2 times

oioi 3 months ago

Selected Answer: B

correct

upvoted 1 times

Question #104 *Topic 1*

A company has an organization with SCPs in AWS Organizations. The root SCP for the organization is as follows:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActions",
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Sid": "DenySES",
            "Effect": "Deny",
            "Action": "ses:*",
            "Resource": "*"
        }
    ]
}
```

The company's developers are members of a group that has an IAM policy that allows access to Amazon Simple Email Service (Amazon SES) by allowing ses:* actions. The account is a child to an OU that has an SCP that allows Amazon SES. The developers are receiving a not-authorized error when they try to access Amazon SES through the AWS Management Console.

Which change must a security engineer implement so that the developers can access Amazon SES?

A. Add a resource policy that allows each member of the group to access Amazon SES.

B. Add a resource policy that allows "Principal": {"AWS": "arn:aws:iam::account-number:group/Dev"}.

C. Remove the AWS Control Tower control (guardrail) that restricts access to Amazon SES.

D. Remove Amazon SES from the root SCP.

Correct Answer: *C*

Community vote distribution

D (100%)

awssecuritynewbie 1 week, 2 days ago

Selected Answer: D

pay attention to the question... it states it wants to allow the dev to use SES... it does not ask to "only" allow them. so it would make sure to remove the SCP because SCP is never overwritten.

upvoted 1 times

rahav 2 months ago

D is the correct one

upvoted 1 times

ykhan321 2 months, 1 week ago

Selected Answer: D

Why most of the answers are incorrect here.

upvoted 2 times

azure4life 2 months, 2 weeks ago

Selected Answer: D

Option D is the correct solution. The root SCP is denying access to Amazon SES across the organization. Even though the OU SCP and IAM policy allow SES access, the root SCP takes precedence and blocks it. Removing Amazon SES from the root SCP whitelist will resolve the issue and allow the developers to access SES based on the permissions granted in their IAM policy.

Option A is incorrect because resource policies apply at the service level, not for IAM users/groups.

Option B is also related to resource policies, not the issue with the SCP whitelist.

Option C mentions AWS Control Tower which is not referenced in the question. The SCP is set through AWS Organizations.

So the root cause is the root SCP denying access to SES, and it needs to be removed from that SCP to allow access that is permitted in the lower levels of permissions.

upvoted 2 times

Oralinux 2 months, 2 weeks ago

Answer D:
a resource policy attached directly to an AWS resource (such as Amazon SES) cannot override an SCP (Service Control Policy) set at the root level in AWS Organizations.

Service Control Policies (SCPs) at the root level act as "guardrails" and define the maximum permissions that accounts within the organization can have. They are evaluated before resource policies.

If an SCP denies access to a particular service, even a resource policy allowing access on the specific resource won't take effect. The SCP at the root level will override any resource policy attached to individual resources.

So, while a resource policy can be useful for granting permissions on a specific resource, it cannot be used to override the restrictions imposed by an SCP at a higher level in the organization's hierarchy. In this scenario, removing the restriction for Amazon SES from the root SCP would be the effective solution.

upvoted 1 times

Aamee 2 months, 3 weeks ago

Selected Answer: D

Leads me towards option D only cuz it seems like the denial of ses* actions explicitly defined under the SCP is probably blocking their authorization requests... not sure if Control Tower here makes any big difference..

upvoted 1 times

[Removed] 3 months ago

Selected Answer: D

The answer is D

upvoted 3 times

Question #105 *Topic 1*

A company hosts a public website on an Amazon EC2 instance. HTTPS traffic must be able to access the website. The company uses SSH for management of the web server.

The website is on the subnet 10.0.1.0/24. The management subnet is 192.168.100.0/24. A security engineer must create a security group for the EC2 instance.

Which combination of steps should the security engineer take to meet these requirements in the MOST secure manner? (Choose two.)

A. Allow port 22 from source 0.0.0.0/0.

B. Allow port 443 from source 0.0 0 0/0.

C. Allow port 22 from 192.168.100.0/24.

D. Allow port 22 from 10.0.1.0/24.

E. Allow port 443 from 10.0.1.0/24.

Correct Answer: *AE*

Community vote distribution

BC (100%)

rahav 2 months ago

Selected Answer: BC

BC is the correct

upvoted 1 times

tayman 2 months ago

Selected Answer: BC

BC 100%

upvoted 1 times

ykhan321 2 months, 1 week ago

Selected Answer: BC

Another wrong answer here. My head is spinning.

upvoted 1 times

Oralinux 2 months, 2 weeks ago

Answer: BC

upvoted 1 times

Aamee 3 months ago

Selected Answer: BC

Yup, agreed with B and C.

upvoted 4 times

[Removed] 3 months ago

Selected Answer: BC

Quite sure the subnet "10.0.1.0/24" is a distractor, so B and C are my vote.

upvoted 4 times

awssecuritynewbie 1 week, 2 days ago

yup it is a twister lol you are allowing the world to access your website so it has to be 0.0.0.0/0

upvoted 1 times

AgboolaKun 3 months ago

Agree. I almost fell for it until I read the question again and paid attention to "HTTPS traffic must be able to access the website". This means any (0.0.0.0/0) https traffic.

upvoted 2 times

oioi 3 months ago

Selected Answer: BC

correct

upvoted 2 times

Question #106 *Topic 1*

A security engineer wants to forward custom application-security logs from an Amazon EC2 instance to Amazon CloudWatch. The security engineer installs the CloudWatch agent on the EC2 instance and adds the path of the logs to the CloudWatch configuration file.

However, CloudWatch does not receive the logs. The security engineer verifies that the awslogs service is running on the EC2 instance.

What should the security engineer do next to resolve the issue?

A. Add AWS CloudTrail to the trust policy of the EC2 in stance. Send the custom logs to CloudTrail instead of CloudWatch.

B. Add Amazon S3 to the trust policy of the EC2 instance. Configure the application to write the custom logs to an S3 bucket that CloudWatch can use to ingest the logs.

C. Add Amazon Inspector to the trust policy of the EC2 instance. Use Amazon Inspector instead of the CloudWatch agent to collect the custom logs.

D. Attach the CloudWatchAgentServerPolicy AWS managed policy to the EC2 instance role.

Correct Answer: *A*

Community vote distribution

D (100%)

Jamshif01 1 month ago

D
All other answers are irrelevant

upvoted 1 times

rahav 2 months ago

Selected Answer: D

D for sure

upvoted 2 times

yorkicurke 2 months ago

Selected Answer: D

Uses of CloudWatchAgentServerPolicy ;
It allows the CloudWatch agent to publish metrics and logs to CloudWatch on behalf of the IAM role or user the policy is attached to.
It provides permissions for the agent to access and manage its own configuration files stored in S3.
The policy grants permissions across multiple AWS services like CloudWatch, S3, KMS etc. to allow end-to-end functionality of the monitoring agent.

upvoted 3 times

ykhan321 2 months, 1 week ago

Selected Answer: D

Only EC2 & Cloudwatch are in questions here.

upvoted 1 times

Oralinux 2 months, 2 weeks ago

Answer: D

upvoted 1 times

Aamee 3 months ago

Selected Answer: D

No doubt about D.

upvoted 3 times

[Removed] 3 months ago

Selected Answer: D

D is correcto

upvoted 3 times

oioi 3 months ago

Selected Answer: D

correct

upvoted 2 times

Question #107 *Topic 1*

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.

Correct Answer: *B*

Community vote distribution

C (100%)

vikasj1in 1 month, 1 week ago

C,
When you deploy a virtual security appliance inline in a subnet, you need to ensure that it can effectively route traffic between different subnets. The "Network Source/Destination check" is a feature in Amazon EC2 that controls whether source/destination checking is enabled or disabled on a network interface.

In this context, the virtual security appliance acts as a router, and the "Network Source/Destination check" should be disabled on its elastic network interface. When this check is disabled, the network interface can handle traffic that is not specifically destined for the instance it is attached to, allowing it to route traffic between different subnets.

upvoted 2 times

rahav 2 months ago

Selected Answer: C

C for sure

upvoted 1 times

Daniel76 2 months, 1 week ago

Selected Answer: C

Source/destination checking
You can enable or disable source/destination checks, which ensure that the instance is either the source or the destination of any traffic that it receives. Source/destination checks are enabled by default. You must disable source/destination checks if the instance runs services such as network address translation, routing, or firewalls.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

upvoted 2 times

azure4life 2 months, 2 weeks ago

Selected Answer: C

Option C is the correct solution.

To allow a virtual security appliance deployed inline to route traffic between subnets, the Network Source/Destination Check needs to be disabled on its elastic network interface. This enables the appliance to receive traffic that is not specifically addressed to itself.

Option A is incorrect because disabling network ACLs is not required for a virtual appliance deployment and would reduce security.

Option B mentions promiscuous mode which applies to physical network interfaces, not virtual ones in AWS.

Option D places the appliance in the public subnet which may help route internet traffic but does not address routing between private subnets. Disabling the Source/Destination Check is required to enable that routing functionality.

upvoted 3 times

Oralinux 2 months, 2 weeks ago

Answer: C

upvoted 1 times

kejam 2 months, 4 weeks ago

Selected Answer: C

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

upvoted 3 times

[Removed] 3 months ago

Selected Answer: C

C is correct

upvoted 3 times

oioi 3 months ago

Selected Answer: C

correct

upvoted 2 times

Question #108 *Topic 1*

A security engineer needs to create an Amazon S3 bucket policy to grant least privilege read access to IAM user accounts that are named User1, User2, and User3. These IAM user accounts are members of the AuthorizedPeople IAM group. The security engineer drafts the following S3 bucket policy:

```
{
    "Version": "2012-10-17",
    "Id": "AuthorizedPeoplePolicy",
    "Statement": [
        {
            "Sid": "Actions-Authorized-People",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::authorized-people-bucket/*"
        }
    ]
}
```

When the security engineer tries to add the policy to the S3 bucket, the following error message appears: "Missing required field Principal."

The security engineer is adding a Principal element to the policy. The addition must provide read access to only User1, User2, and User3.

Which solution meets these requirements?

A.
```
"Principal": {
    "AWS": [
        "arn:aws:iam::1234567890:user/User1",
        "arn:aws:iam::1234567890:user/User2",
        "arn:aws:iam::1234567890:user/User3"
    ]
}
```

B.
```
"Principal": {
    "AWS": [
        "arn:aws:iam::1234567890:root"
    ]
}
```

C.
```
"Principal": {
    "AWS": [
        "*"
    ]
}
```

D.
```
"Principal": {    "AWS": "arn:aws:iam::1234567890:group/AuthorizedPeople"
}
```

Correct Answer: *D*

Community vote distribution

A (94%) 6%

[Removed] Highly Voted 3 months ago

Selected Answer: A

Agree with AgboolaKun. What a lovely question

You can specify any of the following principals in a policy:
AWS account and root user
IAM roles
Role sessions
IAM users
Federated user sessions
AWS services
All principals

You cannot identify a user group as a principal in a policy (such as a resource-based policy) because groups relate to permissions, not authentication, and principals are authenticated IAM entities.

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_principal.html#Principal_specifying

upvoted 8 times

Raphaello Most Recent 6 days, 7 hours ago

Selected Answer: D

In AWS IAM, principals are authenticated IAM entities.
IAM entities are only IAM users and roles.

You cannot used IAM group as a principal in an IAM (resource) policy.

upvoted 1 times

Raphaello 6 days, 7 hours ago

Obviously error in selected answer.
Answer A is the correct one that is matching the provided explanation.

upvoted 1 times

Oralinux 2 months, 2 weeks ago

Answer A: " IAM user accounts that are named User1, User2, and User3. These IAM user accounts are members of the AuthorizedPeople IAM group"
we do not want to give read access to other accounts that are part of the AuthorizedPeople IAM group. => then only A satisfy this criteria

upvoted 2 times

Aamee 2 months, 3 weeks ago

Selected Answer: A

All others are not the valid choices since the Principal needs to be selected only for User1, User2 and User3 'only' explicitly... plus, groups can't be identified as a Principal anyways..

upvoted 4 times

AgboolaKun 3 months ago

Selected Answer: A

The correct answer is A - https://www.examtopics.com/discussions/amazon/view/60777-exam-aws-certified-security-specialty-topic-1-question-258/

upvoted 4 times

Question #109 *Topic 1*

A security engineer recently rotated all IAM access keys in an AWS account. The security engineer then configured AWS Config and enabled the following AWS Config managed rules: mfa-enabled-for-iam-console-access, iam-user-mfa-enabled, access-keys-rotated, and iam-user-unused-credentials-check.

The security engineer notices that all resources are displaying as noncompliant after the IAM GenerateCredentialReport API operation is invoked.

What could be the reason for the noncompliant status?

A. The IAM credential report was generated within the past 4 hours.

B. The security engineer does not have the GenerateCredentialReport permission.

C. The security engineer does not have the GetCredenlialReport permission.

D. The AWS Config rules have a MaximumExecutionFrequency value of 24 hours.

Correct Answer: *D*

Community vote distribution

A (93%) 7%

AgboolaKun Highly Voted 3 months ago

Selected Answer: A

The report was generated within the past 4 hours - https://repost.aws/knowledge-center/config-credential-report

upvoted 8 times

Raphaello Most Recent 5 days, 3 hours ago

Selected Answer: A

A.

You can generate a credential report as often as once every four hours
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

upvoted 1 times

awssecuritynewbie 1 week, 2 days ago

what a shit question btw! He has enabled a bunch of AWS configs, and then they are showing non-compliant. this can be anything really but yeah.

upvoted 1 times

vikasj1in 1 month, 1 week ago

Selected Answer: A

When these AWS Config rules are triggered, they rely on the latest IAM credential report to evaluate compliance. If the IAM credential report has been generated within the past 4 hours, it might not reflect the most recent changes, such as the rotation of access keys.

To address this, it's a good practice to ensure that the IAM credential report is generated and updated at regular intervals, and AWS Config rules are then evaluated against the most recent report. You can schedule the generation of the IAM credential report and the evaluation of AWS Config rules accordingly.

A &C are incorrect because the noncompliance is related to the timeliness of the IAM credential report rather than permissions. Option D is incorrect because the MaximumExecutionFrequency value doesn't affect the initial evaluation of the rules; it determines how often the rule is re-evaluated after its first evaluation.

upvoted 1 times

brpjp 1 month, 4 weeks ago

Answer D may be correct, on assumption that if maximumexecutionfrequency is 24 hours, then report is one day old rather than 4 hours mentioned on option A. Anyone can clarify my understanding.

upvoted 1 times

yorkicurke 2 months ago

Selected Answer: A

Explained in the following link;

https://repost.aws/knowledge-center/config-credential-report

upvoted 1 times

yorkicurke 2 months ago

oh shoot AgboolaKun already mentioned it. ok thumbs up for you AgboolaKun

upvoted 1 times

Aamee 3 months ago

Selected Answer: A

Agreed on A.

upvoted 1 times

[Removed] 3 months ago

Selected Answer: A

I agree with AgboolaKun. Read the link for some good insight

upvoted 1 times

oioi 3 months ago

Selected Answer: D

correct

upvoted 1 times

ykhan321 2 months, 1 week ago

Anything else besides correct?

upvoted 2 times

Question #110 *Topic 1*

A company is using AWS WAF to protect a customized public API service that is based on Amazon EC instances. The API uses an Application Load Balancer.

The AWS WAF web ACL is configured with an AWS Managed Rules rule group. After a software upgrade to the API and the client application, some types of requests are no longer working and are causing application stability issues. A security engineer discovers that AWS WAF logging is not turned on for the web ACL.

The security engineer needs to immediately return the application to service, resolve the issue, and ensure that logging is not turned off in the future. The security engineer turns on logging for the web ACL and specifies Amazon CloudWatch Logs as the destination.

Which additional set of steps should the security engineer take to meet the requirements?

A. Edit the rules in the web ACL to include rules with Count actions. Review the logs to determine which rule is blocking the request. Modify the IAM policy of all AWS WAF administrators so that they cannot remove the logging configuration for any AWS WAF web ACLs.

B. Edit the rules in the web ACL to include rules with Count actions. Review the logs to determine which rule is blocking the request. Modify the AWS WAF resource policy so that AWS WAF administrators cannot remove the logging configuration for any AWS WAF web ACLs.

C. Edit the rules in the web ACL to include rules with Count and Challenge actions. Review the logs to determine which rule is blocking the request. Modify the AWS WAF resource policy so that AWS WAF administrators cannot remove the logging configuration for any AWS WAF web ACLs.

D. Edit the rules in the web ACL to include rules with Count and Challenge actions. Review the logs to determine which rule is blocking the request. Modify the IAM policy of all AWS WAF administrators so that they cannot remove the logging configuration for any AWS WAF web ACLs.

Correct Answer: *B*

Community vote distribution

A (88%) 13%

lightrod 2 weeks, 4 days ago

Selected Answer: A

you should modify the resource policy as best practice

upvoted 1 times

vikasj1in 1 month, 1 week ago

B. A Count action allows rules to collect data about requests that match the conditions but does not block or allow the requests. After making this change, the SE can review the logs in CloudWatch Logs to determine which rule is blocking the specific requests causing the application stability issues. To ensure that logging is not turned off in the future, the security engineer should modify the AWS WAF resource policy. This modification should restrict AWS WAF administrators from removing the logging configuration for any AWS WAF web ACLs, adding an extra layer of protection against inadvertent changes.

C & D suggest including rules with Count and Challenge actions, which may not be necessary for the immediate resolution of the issue. Option A recommends modifying IAM policies, but modifying the AWS WAF resource policy is a more direct and suitable approach for preventing changes to logging configurations.

upvoted 1 times

yorkicurke 2 months ago

Selected Answer: A

As many have suggested of why i'ts unnecessary to go for 'challenge' so C&D -> OUT

As of why not picking B(resource-based) is because resource policy would only control access to that single web ACL.

The question asks to ensure logging is not turned off for any web ACLs[well that's what's implied], which modifying IAM policies globally achieves but modifying a single resource policy does not.

AWS documentation recommends applying least privilege permissions through IAM policies when managing access to resources across multiple accounts. This helps ensure permissions are restricted at the identity level rather than at the individual resource level.

upvoted 1 times

Aamee 3 months ago

Selected Answer: A

It's def. not B. Going with option A cuz of IAM policy capability in this use case rather than resource policies.

upvoted 3 times

[Removed] 3 months ago

Selected Answer: A

Challenge logs are not necessary here (CAPTCHA). We'll also want to restrict with IAM policies and NOT resource policies. Perhaps with SCPs as well. Answer is A

upvoted 2 times

WeepingMapIte 2 months, 1 week ago

Challenge:
Runs a silent background check on the client session to verify if it's a legitimate browser.
Doesn't involve any user interaction, keeping the experience seamless.
Less effective against sophisticated bots that can mimic browser behavior.

upvoted 1 times

oioi 3 months ago

Selected Answer: B

correct

upvoted 1 times

Question #111 *Topic 1*

A security engineer is creating an AWS Lambda function. The Lambda function needs to use a role that is named LambdaAuditRole to assume a role that is named AcmeAuditFactoryRole in a different AWS account.

When the code is processed, the following error message appears: "An error occurred (AccessDenied) when calling the AssumeRole operation."

Which combination of steps should the security engineer take to resolve this error? (Choose two.)

A. Ensure that LambdaAuditRole has the sts:AssumeRole permission for AcmeAuditFactoryRole.

B. Ensure that LambdaAuditRole has the AWSLambdaBasicExecutionRole managed policy attached.

C. Ensure that the trust policy for AcmeAuditFactoryRole allows the sts:AssumeRole action from LambdaAuditRole.

D. Ensure that the trust policy for LambdaAuditRole allows the sts:AssumeRole action from the lambda.amazonaws.com service.

E. Ensure that the sts:AssumeRole API call is being issued to the us-east-1 Region endpoint.

Correct Answer: *BC*

Community vote distribution

AC (100%)

kejam 2 months, 3 weeks ago

Selected Answer: AC

https://repost.aws/knowledge-center/lambda-function-assume-iam-role

upvoted 2 times

Aamee 3 months ago

Selected Answer: AC

makes the perfect logic.

upvoted 2 times

[Removed] 3 months ago

Selected Answer: AC

A and C seems right

upvoted 1 times

oioi 3 months ago

Selected Answer: AC

coorect

upvoted 1 times

Question #112 *Topic 1*

A company has AWS accounts in an organization in AWS Organizations. The organization includes a dedicated security account.

All AWS account activity across all member accounts must be logged and reported to the dedicated security account. The company must retain all the activity logs in a secure storage location within the dedicated security account for 2 years. No changes or deletions of the logs are allowed.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

A. In the dedicated security account, create an Amazon S3 bucket. Configure S3 Object Lock in compliance mode and a retention period of 2 years on the S3 bucket. Set the bucket policy to allow the organization's management account to write to the S3 bucket.

B. In the dedicated security account, create an Amazon S3 bucket. Configure S3 Object Lock in compliance mode and a retention period of 2 years on the S3 bucket. Set the bucket policy to allow the organization's member accounts to write to the S3 bucket.

C. In the dedicated security account, create an Amazon S3 bucket that has an S3 Lifecycle configuration that expires objects after 2 years. Set the bucket policy to allow the organization's member accounts to write to the S3 bucket.

D. Create an AWS CloudTrail trail for the organization. Configure logs to be delivered to the logging Amazon S3 bucket in the dedicated security account.

E. Turn on AWS CloudTrail in each account. Configure logs to be delivered to an Amazon S3 bucket that is created in the organization's management account. Forward the logs to the S3 bucket in the dedicated security account by using AWS Lambda and Amazon Kinesis Data Firehose.

Correct Answer: *CD*

Community vote distribution

BD (76%) AD (24%)

ahrentom Highly Voted 2 months, 4 weeks ago

Selected Answer: BD

I go with BD, because each Member Account has to write into the security Account S3 bucket, not only the Organization Management Account.
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-set-bucket-policy-for-multiple-accounts.html

upvoted 8 times

kejam 2 months, 3 weeks ago

Agreed. CloudTrail for Org requires the destination S3 bucket to allow writes from each member account. Object Lock is enabled to prevent the data from being overwritten/deleted.

upvoted 2 times

Ernestokoro Most Recent 1 month ago

The organization includes a dedicated security account= Member account while ALL OTHER =Management account. this means to me that granting the permission from the Management account reduces operational overhead than doing it at individual member accounts. Therefore I go with option AD.

upvoted 1 times

vikasj1in 1 month, 1 week ago

A, D
Option B covers the storage aspect by configuring a dedicated S3 bucket in the security account, allowing member accounts to write logs. S3 Object Lock in compliance mode ensures the retention requirements.

Option D complements this by configuring CloudTrail to capture the logs and deliver them to the dedicated S3 bucket directly.

Together, these options cover the log storage, retention, and collection requirements with the least operational overhead.

upvoted 1 times

WeepingMaplte 2 months ago

Selected Answer: AD

Enable Organization Trail: In the Management Console or CLI, activate an organization trail that logs all events from all member accounts.
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html

upvoted 1 times

jeff001 2 months, 1 week ago

Selected Answer: BD

Member account needs to write to S3.

upvoted 1 times

marco25 2 months, 3 weeks ago

Selected Answer: BD

trails across member accounts, needs permissions to the sender bucket

upvoted 4 times

Aamee 3 months ago

Selected Answer: AD

If I understand correctly, the reason why the option B can't be a correct one cuz the use case has asked about the logs which must not be deleted or changed which can't be met in option B if we opt for each member's accounts to be given with the full S3 logs access under an organization.

upvoted 1 times

ykhan321 2 months, 1 week ago

A has only one account and option B has all the aws accounts.

upvoted 1 times

confusedyeti69 2 months, 3 weeks ago

If following your logic, the management account can delete and change the logs too.
And the options also says to only give write access to S3 only.
It is not A because members need to write S3, not only management.

In compliance mode, a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html

upvoted 1 times

[Removed] 3 months ago

Selected Answer: AD

A and D are correct

upvoted 1 times

oioi 3 months ago

Selected Answer: AD

correct

upvoted 1 times

Question #113 *Topic 1*

A company is testing its incident response plan for compromised credentials. The company runs a database on an Amazon EC2 instance and stores the sensitive database credentials as a secret in AWS Secrets Manager. The secret has rotation configured with an AWS Lambda function that uses the generic rotation function template. The EC2 instance and the Lambda function are deployed in the same private subnet. The VPC has a Secrets Manager VPC endpoint.

A security engineer discovers that the secret cannot rotate. The security engineer determines that the VPC endpoint is working as intended. The Amazon CloudWatch logs contain the following error: "setSecret: Unable to log into database".

Which solution will resolve this error?

A. Use the AWS Management Console to edit the JSON structure of the secret in Secrets Manager so that the secret automatically conforms with the structure that the database requires.

B. Ensure that the security group that is attached to the Lambda function allows outbound connections to the EC2 instance. Ensure that the security group that is attached to the EC2 instance allows inbound connections from the security group that is attached to the Lambda function.

C. Use the Secrets Manager list-secrets command in the AWS CLI to list the secret. Identify the database credentials. Use the Secrets Manager rotate-secret command in the AWS CLI to force the immediate rotation of the secret.

D. Add an internet gateway to the VPC. Create a NAT gateway in a public subnet. Update the VPC route tables so that traffic from the Lambda function and traffic from the EC2 instance can reach the Secrets Manager public endpoint.

Correct Answer: *B*

Community vote distribution

B (100%)

Daniel76 2 months ago

Selected Answer: B

a) when you use the console to store a database secret, Secrets Manager automatically creates it in the correct JSON structure.
c) secret manager already configured as auto-rotation. also, secret id should have been known instead of listing secrets .
d) accessing secret manager via public is not recommended.

upvoted 1 times

yorkicurke 2 months ago

Selected Answer: B

Hate questions like these which rather then testing your knoweledge of technologies trick you into these weired worded questions.

the statement 'Ensure that the security group that is attached to the Lambda function allows outbound' threw me off as Lambda does not have SGs.

But then through some internet digging came accross the fact that when a Lambda function needs to access resources inside a Virtual Private Cloud (VPC), it does so using ENI which resides in a subnet of the VPC and can have a security group associated with it. The security group acts as a virtual firewall for the ENI.

upvoted 3 times

confusedyeti69 2 months, 3 weeks ago

Why would the lambda need access to the EC2? The question is unclear about the exact job of the lambda. It is worded as if the lambda job is to change the creds in secrets manager only.

upvoted 2 times

JPSWS 2 months, 1 week ago

The DB runs on the EC2 that's why the Lambda needs access to it to set the new credentials

upvoted 2 times

Aamee 3 months ago

Selected Answer: B

B is the only one that logically seems right. All others are distracters except option C. But option C describes the solution of this problem as a one time thing whereas, it's been asked to provide a permanent solution for this use case. That's why B looks much more secured and valid option among all others.

upvoted 4 times

[Removed] 3 months ago

Selected Answer: B

I'll vote B. The rest are distractors but feel free to correct me if I'm wrong.

upvoted 2 times

oioi 3 months ago

Selected Answer: B

correct

upvoted 2 times

Question #114 *Topic 1*

A company deploys a set of standard IAM roles in AWS accounts. The IAM roles are based on job functions within the company. To balance operational efficiency and security, a security engineer implemented AWS Organizations SCPs to restrict access to critical security services in all company accounts.

All of the company's accounts and OUs within AWS Organizations have a default FullAWSAccess SCP that is attached. The security engineer needs to ensure that no one can disable Amazon GuardDuty and AWS Security Hub. The security engineer also must not override other permissions that are granted by IAM policies that are defined in the accounts.

Which SCP should the security engineer attach to the root of the organization to meet these requirements?

A.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "securityhub:DisableSecurityHub"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

B.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "*",y
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "NotAction": [
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "securityhub:DisableSecurityHub"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

C.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "NotAction":[
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "securityhub:DisableSecurityHub"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

D.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "securityhub:DisableSecurityHub"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Correct Answer: *B*

Community vote distribution

A (75%) D (25%)

ahrentom 2 months, 4 weeks ago

Selected Answer: A

A is correct, key word in SCP is to Deny, because it overwrites the FullAccessSCP Alow statement.

upvoted 3 times

AgboolaKun 3 months ago

Selected Answer: A

A is correct. The NotAction element cannot be used in this case.

You only need an explicit DENY here since all accounts and OUs already have a default FullAWSAccess SCP but you don't want them to be able to disable Amazon GuardDuty and AWS Security Hub.

upvoted 3 times

Sab31 1 month, 3 weeks ago

Kindly correct me if I am wrong. When we attach a new SCP the default FullAWSAccess SCP is detached from the OU. isn't that right?

upvoted 1 times

Aamee 3 months ago

Selected Answer: D

Probably going with D but still not 100% sure how is it going to work that way... would appreciate if someone could help in understanding this question..

upvoted 2 times

LeoD 2 months, 3 weeks ago

SCPs do not support NotAction with effect Allow.

upvoted 2 times

Aamee 2 months, 3 weeks ago

Ah ok, got it...thnx so much... in this way, probably looks like all other options are invalid except option A since on all others they've used 'NotAction' attribute with Allow directly and indirectly which won't work..

upvoted 2 times

[Removed] 3 months ago

A. OU level will still have access to other services outside of Guardduty and Security Hub due to the OU level policy. D could work but is not necessary

upvoted 1 times

Question #115 *Topic 1*

A company needs to follow security best practices to deploy resources from an AWS CloudFormation template. The CloudFormation template must be able to configure sensitive database credentials.

The company already uses AWS Key Management Service (AWS KMS) and AWS Secrets Manager.

Which solution will meet the requirements?

A. Use a dynamic reference in the CloudFormation template to reference the database credentials in Secrets Manager.

B. Use a parameter in the CloudFormation template to reference the database credentials. Encrypt the CloudFormation template by using AWS KMS.

C. Use a SecureString parameter in the CloudFormation template to reference the database credentials in Secrets Manager.

D. Use a SecureString parameter in the CloudFormation template to reference an encrypted value in AWS KMS.

Correct Answer: *C*

Community vote distribution

A (100%)

Aamee Highly Voted 2 months, 2 weeks ago

Since this is the last question here so maybe I can post it here. I've passed this exam with a score of 926. Only few of the questions were not from this exam material but else, everything came from here. Would like to thanks to all of you who helped in answering my queries and got my concept clarified!... Man_Kind, Agboola and others, you guys simply rock, thanks once again so much! :)

upvoted 9 times

giancesarini2023 2 months ago

@Aamee, do you think there is a question from 1 to 50? I'm only studying from 50 to 115.

upvoted 2 times

nn67 Most Recent 2 weeks, 6 days ago

A
keyword dynamic reference

upvoted 2 times

Pmktechno 3 weeks, 3 days ago

Yesterday I took this exam (Feb 1st) single question also wasn't came from this set of questions. Please wait examtopics team should be update soon new set of questions.

upvoted 2 times

brpjp 1 month, 1 week ago

Hello, I passed exam with 956 score. Thank you all for contributing and correcting the answers.

upvoted 1 times

alexleely 4 weeks, 1 day ago

when did you take the exam?

upvoted 1 times

Aamee 3 months ago

Selected Answer: A

Yup, for sure it should be A. Here's the summary:

"Updating a secret in Secrets Manager doesn't automatically update the secret in CloudFormation. In order for CloudFormation to update a secretsmanager dynamic reference, you must perform a stack update that updates the resource containing the dynamic reference, either by updating the resource property that contains the secretsmanager dynamic reference, or updating another of the resource's properties."

upvoted 1 times

[Removed] 3 months ago

Selected Answer: A

A. See below

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/dynamic-references.html#dynamic-references-secretsmanager

upvoted 4 times

oioi 3 months ago

Selected Answer: A

correct
upvoted 1 times

Question #116 *Topic 1*

An international company wants to combine AWS Security Hub findings across all the company's AWS Regions and from multiple accounts. In addition, the company wants to create a centralized custom dashboard to correlate these findings with operational data for deeper analysis and insights. The company needs an analytics tool to search and visualize Security Hub findings.

Which combination of steps will meet these requirements? (Chose three.)

A. Designate an AWS account as a delegated administrator for Security Hub. Publish events to Amazon CloudWatch from the delegated administrator account, all member accounts, and required Regions that are enabled for Security Hub findings.

B. Designate an AWS account in an organization in AWS Organizations as a delegated administrator for Security Hub. Publish events to Amazon EventBridge from the delegated administrator account, all member accounts, and required Regions that are enabled for Security Hub findings.

C. In each Region, create an Amazon EventBridge rule to deliver findings to an Amazon Kinesis data stream. Configure the Kinesis data streams to output the logs to a single Amazon S3 bucket.

D. In each Region, create an Amazon EventBridge rule to deliver findings to an Amazon Kinesis Data Firehose delivery stream. Configure the Kinesis Data Firehose delivery streams to deliver the logs to a single Amazon S3 bucket.

E. Use AWS Glue DataBrew to crawl the Amazon S3 bucket and build the schema. Use AWS Glue Data Catalog to query the data and create views to flatten nested attributes. Build Amazon QuickSight dashboards by using Amazon Athena.

F. Partition the Amazon S3 data. Use AWS Glue to crawl the S3 bucket and build the schema. Use Amazon Athena to query the data and create views to flatten nested attributes. Build Amazon QuickSight dashboards that use the Athena views.

Correct Answer: *BDE*

Community vote distribution

BDF (100%)

nublit 3 days, 16 hours ago

Selected Answer: BDF

BDF are the best options
upvoted 1 times

awssecuritynewbie 1 week, 2 days ago

Selected Answer: BDF

BDF for sure,
upvoted 1 times

sarcactus 1 week, 3 days ago

Selected Answer: BDF

BDF
Also agree with previous comment.
upvoted 1 times

MikeRach 1 week, 5 days ago

BDF
The steps are literally provided in this Doc https://aws.amazon.com/blogs/architecture/visualize-aws-security-hub-findings-using-analytics-and-business-intelligence-tools/
upvoted 1 times

Question #117 *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 parameters. Use these resulting values to make API/CLI calls.

C. Implement federated API/CLI access using SAML 2.0, then configure the identity provider to enforce multi-factor authentication.

D. 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. Add sts:AssumeRole to NotAction in the policy.

Correct Answer: *C*

Community vote distribution

B (100%)

nublit 3 days, 16 hours ago

Selected Answer: B

B for sure

upvoted 1 times

awssecuritynewbie 1 week, 2 days ago

Selected Answer: B

B for sure they required to enable CLI

upvoted 1 times

sarcactus 1 week, 3 days ago

Selected Answer: B

I agree with MikeRach comment.

upvoted 2 times

MikeRach 1 week, 6 days ago

B
https://www.examtopics.com/discussions/amazon/view/47596-exam-aws-certified-security-specialty-topic-1-question-225/

upvoted 1 times

Question #118 *Topic 1*

A company is developing a mechanism that will help data scientists use Amazon SageMaker to read, process, and output data to an Amazon S3 bucket. Data scientists will have access to a dedicated S3 prefix for each of their projects. The company will implement bucket policies that use the dedicated S3 prefixes to restrict access to the S3 objects. The projects can last up to 60 days.

The company's security team mandates that data cannot remain in the S3 bucket after the end of the projects that use the data.

Which solution will meet these requirements MOST cost-effectively?

A. Create an AWS Lambda function to identify and delete objects in the S3 bucket that have not been accessed for 60 days. Create an Amazon EventBridge scheduled rule that runs every day to invoke the Lambda function.

B. Create a new S3 bucket. Configure the new S3 bucket to use S3 Intelligent-Tiering. Copy the objects to the new S3 bucket.

C. Create an S3 Lifecycle configuration for each S3 bucket prefix for each project. Set the S3 Lifecycle configurations to expire objects after 60 days.

D. Create an AWS Lambda function to delete objects that have not been accessed for 60 days. Create an S3 event notification for S3 Intelligent-Tiering automatic archival events to invoke the Lambda function.

Correct Answer: *B*

Community vote distribution

C (100%)

nublit 3 days, 16 hours ago

Selected Answer: C

C for sure

upvoted 1 times

sarcactus 1 week ago

Selected Answer: C

C is the correct one.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-configuration-examples.html#lifecycle-config-conceptual-ex3

upvoted 1 times

anasbakla 1 week, 1 day ago

C is the answer

upvoted 2 times

anasbakla 1 week, 1 day ago

Me too

upvoted 1 times

awssecuritynewbie 1 week, 2 days ago

Selected Answer: C

C makes sense you need to remove the data after 60 day so lifecycle will do that.

upvoted 1 times

jabilrn 1 week, 5 days ago

C for me

upvoted 1 times