Exam Session - Cert Prep: AWS Security Specialty Certification

cloudacademy.com/quiz/exam/3758824/results

#1

You have been requested to review and document an existing IAM policy that has been attached via an IAM Role to an instance.{"Version": "2012-10-17","Statement": [{"Effect": "Allow","Action": ["ec2:AttachVolume","ec2:DetachVolume"],"Resource": ["arn:aws:ec2:us-west-1:123456789012:volume/*","arn:aws:ec2:us-west-1:123456789012:instance/*"],"Condition": {"ArnEquals": {"ec2:SourceInstanceARN": "arn:aws:ec2:us-west-1:123456789012:instance/i-0a57a24800d7d6ce9"}}}]}Which of the following statements are false regarding the policy? (select 2 answers)

✗

The policy allows EBS volumes to be attached to the EC2 instance i-0a57a24800d7d6ce9

✓

The policy disallows EBS volumes to be attached to the EC2 instance i-0a57a24800d7d6ce9

✓

The policy disallows the EC2 instance i-0a57a24800d7d6ce9 to detach volumes from other instances

✗

The policy allows the EC2 instance i-0a57a24800d7d6ce9 to detach volumes to other instances

Explanation

Answers “**The policy disallows EBS volumes to be attached to the EC2 instance i-0a57a24800d7d6ce9**” and “**The policy disallows the EC2 instance i-0a57a24800d7d6ce9 to detach volumes from other instances**” are the correct false answers . The quick approach to answer this question is to consider the Effect attribute which is set to Allow, meaning there are no explicit deny/disallows in the policy. The only other consideration within the question is the answer “The policy allows EBS volumes to be attached to the EC2 instance i-0a57a24800d7d6ce9”, here although the policy is implying that the permissions are granted only when the source instance id is i-0a57a24800d7d6ce9, the policy as a whole still allows this instance to attach EBS volumes to itself.

🔗

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_ec2_volumes-instance.html

#2

You are a security architect for a private school whose enrollment application runs on a fleet of EC2 instances in the US Ohio and US Oregon regions for disaster recovery purposes. The company uses Amazon Route53 for traffic routing and DNS management. You have been asked to set up a solution for logging the public DNS queries on Route53 so as to have visibility into these queries and to be able to analyze the data for any vulnerabilities. You need to set up a solution that will collect public DNS query information and log the data into a centralized place for further analysis. Which of the following logging solutions would allow you to log the public DNS query information from Amazon Route53 and store it in a centralized place for analysis?

✗

Enable AWS Macie and configure it to track and send the Route53 public DNS query information to Amazon CloudWatch Logs.

✗

Enable AWS Detective and configure it to track and send the Route53 public DNS query information to Amazon CloudWatch Logs.

✓

Create a CloudWatch Log Group, configure query logging to send the Route53 public DNS query information to Amazon CloudWatch Logs.

✗

Enable AWS CloudTrail logging for the AWS account which will automatically track and collect the public DNS query information from Route53. Configure an Amazon S3 bucket to receive the DNS query log information from CloudTrail.

Explanation

You can configure Amazon Route 53 to log information about the public DNS queries that Route 53 receives. You can log information regarding the domain or subdomain that was requested, date and time of the request, DNS record type (such as A or AAAA), Route 53 edge location that responded to the DNS query, DNS response code, such as NoError or ServFail. This information is logged after turning on query logging in Route53. Once you configure query logging, Route 53 will send logs to CloudWatch Logs groups. You can then use CloudWatch Logs tools to access the query logs.

The remaining choices are incorrect for the following reasons:

● AWS Macie is a service for the purpose of protecting sensitive data in AWS, not logging for Route53.

● Amazon Detective is primarily used to help identify the route cause of security issues. Amazon Detective analyzes events from multiple data sources such as VPC Flow Logs, AWS CloudTrail logs, and Amazon GuardDuty.

● The CloudTrail service monitors and records account API activity across all of your AWS resources. With CloudTrail, you can gain visibility into the API activity going on with Route53. CloudTrail does not give visibility into the public DNS queries in Route53.

🔗 https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/query-logs.html

#3

Key rotation is an important concept of key management. How does Key Management Service (KMS) implement key rotation?

✗

KMS supports manual Key Rotation only; you can create new keys any time you want and all data will be re-encrypted with the new key.

✗

Key rotation is the process of synchronizing keys between configured regions; KMS will synchronize key changes in near-real time once keys are changed.

✗

Key rotation is supported through the re-importing of new KMS keys; once you import a new key all data keys will be re-encrypted with the new KMS key.

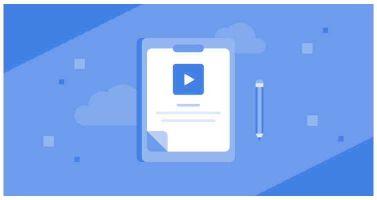
✓

KMS creates new cryptographic material for your KMS keys every rotation period, and uses the new keys for any upcoming encryption; it also maintains old keys to be able to decrypt data encrypted with those keys.

Explanation

When you enable *automatic key rotation* for a customer-managed KMS key, AWS KMS generates new cryptographic material for the KMS key every year. AWS KMS also saves the KMS key's older cryptographic material so it can be used to decrypt data that it has encrypted.

🔗/amazon-web-services/amazon-web-services-key-management-service-kms-course/key-management-service-basics.html
Covered in this lecture
Amazon Kinesis
Course:Designing Secure Applications and Architectures



5m

#4

Bearing in mind the shared responsibility model, who is responsible for modifying routing tables and NACLs in a VPC, to ensure that a RDS DB instance can be reached by other instances in the same VPC?

✓

The AWS account owner

✗

AWS Support desk

✗

AWS support technicians

✗

AWS VPC service administrators

Explanation

The account owner is in charge of configuring the routing tables for his/her VPC, as well as the network ACLs rules needed to make your DB instances accessible from all the instances of your VPC.

🔗http://aws.amazon.com/rds/faqs/

#5

What does the AWS best practice "designing for failure" mean?

✗

To develop cloud systems that never fail

✓

To design systems to anticipate failure and recover automatically

✗

To develop systems with single points of failure

✗

To back up your cloud environment with an on-premises environment

Explanation

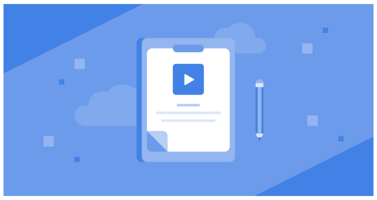
Designing for failure means assuming that what can go wrong will go wrong. Design your infrastructure to respond to potential outages of multiple kinds with an automated recovery process in place.

https://github.com/deep1224/AWS-Training-Docs/blob/master/AWS_Cloud_Best_Practices.pdf

Covered in this lecture

Terminology

Course:Solution Architect Associate - Introduction and High Level Overview



13m

#6

One of your clients has an Amazon VPC with multiple EC2 instances in both public and private subnets. They are unable to connect to one of the EC2 instances, which is their web server. The web server is in a public subnet. When they try to connect to the web server via SSH, they are getting the message 'Network Error: Connection timed out'. What is not a valid troubleshooting step in this case?

✗

Replace the Public IP address with an Elastic IP address.

✗

Check your security group rules.

✗

Check the route table for the subnet.

✓

Create multiple access control lists for the subnet.

Explanation

D is the correct response because it is not a correct troubleshooting action. While you can associate a network ACL with multiple subnets, a subnet can only be associated with one network ACL at a time. When you associate a network ACL with a subnet, the previous association is removed.

The other options are correct actions. The network ACLs must allow inbound and outbound traffic from your local IP address on the proper port. The default network ACL allows all inbound and outbound traffic. Check the route table for the subnet. You need a route that sends all traffic destined outside the VPC to the Internet gateway for the VPC. Check your security group rules. You need a security group rule that allows inbound traffic from your public IPv4 address on the proper port.

🔗

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html#TroubleshootingInstancesConnectionTimeout

#7

Your boss is looking to expand the customer base and has decided to create a customer demo environment to enable the sales team to demo to new customers during sales meetings. The Engineering team has attempted to create a new customer demo environment consisting of EC2 instances and encrypted EBS volumes using an existing CloudFormation template. After running the CloudFormation template, the encrypted EBS volumes are failing to be created for the instances. The team has contacted you to assist with troubleshooting the issue. Which of the following could be a potential cause of the failure?

✕

The IAM role associated with the EC2 instance does not have permission to access the encrypted EBS volume

✓

The KMS key associated with the EBS volume is disabled

✕

The customer master key associated with the EC2 instance is disabled

✕

The KMS key alias associated with the EBS volume is pending creation

Explanation

An EBS volume will fail to be created if the specified KMS key desired to encrypt the volume is invalid or disabled. The KMS key specified during the EBS volume creation must be valid and active in order for the EBS volume to be created.

The remaining choices are incorrect for the following reasons:

● An IAM role is an IAM identity that you can create in your account that has specific permissions. An IAM role is similar to an IAM user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. IAM roles are often created to grant one AWS service the ability to interact with another AWS service.

● KMS keys are used to encrypt data you store in AWS services. These keys are associated with AWS data services like S3, RDS, DynamoDB and EBS volumes to provide encryption of the data in those AWS services, not EC2 instances.

● An alias is a friendly name for an AWS KMS key. An alias pending creation would have no effect on the ability of an EBS volume to be created as it is just an alternate name for an existing AWS KMS key.

🔗https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-cloud-watch-events.html#create-fail-key

#8

Which of the following identity and access management solutions would allow users to sign in to an app with 3rd party providers while also allowing new users to register an account from the mobile application?

✕

Set up an identity pool in IAM and create roles for each social identity provider.

✓

Setup a user pool in AWS Cognito and add a social identity provider to the user pool.

✕

Set up a user directory in AWS Directory Service and add social identity providers to the user directory.

Explanation

With AWS Cognito, mobile app users can sign in through social identity providers (IdP) like Facebook, Google, Amazon, and Apple. This is facilitated by setting up a user pool with an app client and a user pool domain in AWS Cognito. After setting up the user pool and registering your application with a social Identity provider, you are then able to add your social identity provider to your user pool to facilitate login with that provider.

The remaining choices are incorrect for the following reasons:

● An identity pool is a feature of AWS Cognito, not IAM. Amazon Cognito identity pools provide temporary AWS credentials for users who are guests (unauthenticated) and for users who have been authenticated and received a token. An identity pool is a store of user identity data specific to your account.

● AWS Directory Service is a service primarily used for enabling your directory-aware workloads and AWS resources to use managed Microsoft Active Directory (AD) in AWS. Users set up in AWS Directory Service represent individual people or entities that have access to your directory.

● AWS Resource Access Manager (RAM) is primarily used to help you securely share your resources across AWS accounts, within your organization or organizational units (OUs) in AWS Organizations, and with IAM roles and IAM users for supported resource types. You create a resource share in AWS Resource Access Manager to add the resources you want to share and specify the permission for use of that resource type. This service is not used to set up sign-in with social identity providers.

🔗https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-social-idp.html

#9

A custom NAT instance that performs source/destination checks by default is launched in a VPC within a public subnet. All security groups, NACLs, and routing definitions are configured as expected. When a custom NAT instance is launched, which of the following must be done for the custom NAT instance to work?

✓

The source/destination checks should be disabled on the NAT instance.

✕

The NAT instance should be configured with a public IP address.

✕

The NAT instance should be configured with an elastic IP address.

✕

The NAT instance should be launched in a private subnet.

Explanation

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

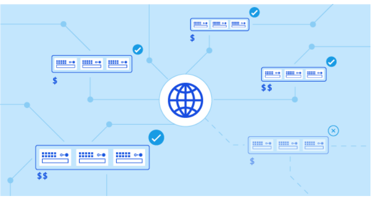
🔗

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html#EIP_Disable_SrcDestCheck

Covered in this lecture

Exam prep - Bastion Host versus NAT Gateway

Course:Designing Highly Available, Cost Efficient, Fault Tolerant, Scalable Systems for Solutions Architect Associate on AWS



10m

🔖

#10

You are a security architect for an eCommerce company. The main website you manage is a three-tier application consisting of a web server, application server, and database server running on EC2 instances. The application also uses multiple S3 buckets to manage different types of data; some need encryption of data at rest and some do not. Currently, the following S3 buckets exist: orderInformation QuarterlyFinancialReportsLogFilesSiteMedia You need to architect a solution for the management of KMS keys that will best control the blast radius around all of the customer-managed individual keys created and encrypt all data at rest. Which KMS management solution would be a good choice for your company to control the blast radius of the individual KMS keys?

✕

Create KMS allocation tags on the S3 buckets to classify the buckets according to data type and KMS key used.

✓

Define data classification levels for the keys and have at least one KMS key per level for the KMS keys.

✗

Utilize 1 KMS key across all of the buckets that need encryption at rest so as to minimize key management and neutralize the threat of having multiple keys.

✗

Enable auto rotation on all of the KMS keys in use to auto-delete after 1 year of inactivity to minimize key management and neutralize the threat of having an abundance of KMS keys

Explanation

With AWS KMS, you should define data classification levels and have at least one KMS key per level. You could define a KMS key for data classified as “Confidential,” and so on. This ensures that authorized users only have permissions for the key material that they require to complete their job and helps to manage the various KMS keys in use.

The remaining choices are incorrect for the following reasons:

● Amazon S3 offers the ability to tag S3 buckets for tracking purposes only. This feature is primarily used to track the storage cost or other criteria for individual projects or groups of projects, for your Amazon S3 buckets using cost allocation tags.

● Previously, you may have used the same key across different geographic regions, environments, or even applications. The best practice with AWS KMS is that you should define data classification levels and have at least one KMS key per level. For example, you could define a KMS key for data classified as “Confidential,” and so on. This ensures that authorized users only have permissions for the key material that they require to complete their job.

● When you enable automatic key rotation for a customer-managed key, AWS KMS generates new cryptographic material for the KMS key every year. AWS KMS will also save the KMS key's older cryptographic material so it can be used to decrypt data that the KMS key encrypted. AWS KMS does not delete any rotated key material until you delete the KMS key.

🔗https://docs.aws.amazon.com/whitepapers/latest/kms-best-practices/key-creation-and-management.html

#11

What does the Server-side encryption provide in Amazon S3?

✗

Server-side encryption doesn't exist for Amazon S3, but only for Amazon EC2.

✓

Server-side encryption protects data at rest using Amazon S3-managed encryption keys (SSE-S3).

✕

Server-side encryption allows you to upload files using an SSL endpoint for a secure transfer.

✕

Server-side encryption provides an encrypted virtual disk in the cloud.

Explanation

Server-side encryption is about protecting data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates.

🔗http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html

#12

Which of the following infrastructure security solutions will protect Amazon Route 53 from common infrastructure DDoS attacks such as SYN/ACK floods, UDP floods, reflection attacks and DNS query floods?

✕

Enable Amazon WAF for Amazon Route 53, enable the AWS managed rules group for DNS query floods in the WAF access control list.

✕

Set up Amazon Firewall for Amazon Route 53, enable the AWS managed rules group for DNS query floods in the WAF access control list.

✕

Configure Amazon DNS Manager for Amazon Route 53, set up a hosted zone for DNS query floods in the DNS Manager dashboard.

✓

Do nothing as this type of protection is already built into Amazon Route 53

Explanation

Always-on monitoring, anomaly detection, and mitigation against common infrastructure DDoS attacks such as SYN/ACK floods, UDP floods, and reflection attacks are built into both Route 53 and CloudFront**.** Route 53 is also already designed to withstand DNS query floods, which are real DNS requests that can continue for hours and attempt to exhaust DNS server resources. Route 53 uses shuffle sharding and anycast striping to spread DNS traffic across edge locations and help protect the availability of the service. No additional configuration is needed to get this protection.

The remaining choices are incorrect for the following reasons:

● Amazon WAF is a web application firewall designed to protect web applications against common security vulnerabilities, but can not be deployed to Amazon Route 53.

● You can use AWS Firewall Manager to simplify your administration and maintenance tasks across multiple accounts and resources for a variety of protections, including AWS WAF, AWS Shield Advanced, Amazon VPC security groups, AWS Network Firewall, and Amazon Route 53 Resolver DNS Firewall. It does not, however, handle the security piece.

● AWS DNS Management is a feature of Amazon Route 53. Amazon Route 53 traffic flow allows you to manage traffic globally through a variety of routing types, including Latency Based Routing, Geo DNS, Geo Proximity, and Weighted Round Robin.

🔗https://aws.amazon.com/blogs/security/how-to-protect-dynamic-web-applications-against-ddos-attacks-by-using-amazon-cloudfront-and-amazon-route-53/
#13

You are configuring EC2 Systems Manager. What policy should you assign to your EC2 instances so that they can communicate with the Systems Manager API?

✕

AmazonEC2RoleforSystemsManager

✓

AmazonEC2RoleforSSM

✕

AmazonEC2RoleforSystemsManagerAllCommands

✕

AmazonEC2RoleforSysMan

Explanation

The *AmazonEC2RoleforSSM* AWS Identity and Access Management (IAM) policy enables an EC2 instance to communicate with the Systems Manager (SSM) API. You must assign an IAM role with this policy when you create the new instance. You cannot assign a role to an instance that is already running.

🔗http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/mw-new-instance-console.html

#14

Your security team has been called in to perform the necessary configurations for a new application hosted on a fleet of EC2 instances before a rollout to production. The Database server's security group has been configured to only allow traffic from the Webserver and to block public internet accessibility keeping the Database server private. Now, the Webserver security needs to be configured in a way that supports anticipated traffic while minimizing the blast radius potential in the event of a large-scale attack. Following the principle of least privilege, which of the following security configurations provide the best way to configure the security of the Web Servers to allow for tight security and limit the blast surface of a potential attack?

✗

Add a Deny inbound rule for SSH on the Security Groups associated with the WebServers and add Allow inbound rules #200 and #300 to allow HTTP and HTTPS from source 0.0.0.0/0

✓

Create an Elastic Load Balancer and place the WebServers behind the Load Balancer. Attach a Security Group to the Load Balancer with inbound rules for HTTP and HTTPS allowlisting only ports 80 and 443

✗

Create an AWS WAF access control list with rules allowing traffic for HTTP and HTTPS from source 0.0.0.0/0. Associate the access control list with the WebServers to filter the traffic and protect the servers.

✗

Add an outbound rule to the Security Group associated with the EC2 instances allowing HTTP and HTTPS allowlisting only ports 80 and 443

Explanation

An Elastic Load Balancer is used to automatically route incoming application traffic to one or more EC2 instances in one or more availability zones. The ELB can help to maintain the availability and scalability of the system and assist in isolating your resources from malicious traffic directly. Placing your instances behind an ELB can prevent your servers from being directly exposed to the internet. This will help limit the blast radius of a potential attack by limiting the ability of an attacker to learn about and directly impact your application.

The remaining choices are incorrect for the following reasons:

- While limiting inbound SSH access to servers is a best practice, Security Groups are stateful and do not allow for allow and deny rules. Network Access Control List are stateless and allow for implicit allow and deny rules.
- Amazon WAF is a web application firewall designed to protect web applications against common security vulnerabilities. AWS WAF uses access control lists and rules to filter out specific traffic patterns. AWS WAF can only be deployed on Amazon CloudFront, API Gateway, AWS AppSync or an Application Load Balancer not EC2 instances.
- Outbound rules for Security Groups control the traffic flowing out of the severs. By default, a Security Group includes an outbound rule that allows all outbound traffic no additional rules are needed.

🔗https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/security-groups-and-network-access-control-lists-nacls-bp5.html
#15

You’re a security engineer for an insurance company. Your company’s platform consists of a Web/App server running on an EC2 instance and an RDS Microsoft SQL server database in a single VPC. The System Administration team has been monitoring the Web Server traffic and performance and has noticed an unusually high volume of requests hitting this server. After reviewing the alerts, your team suspects a possible DDoS attack. You need to discover a way to determine what IP addresses are accessing the EC2 instance and sending the requests. Which of the following solutions would allow you to examine the network traffic and identify the IP address sending the high volume of requests to determine if an active DDoS attack is in progress?

✓

Review the VPC Flow logs to examine the network traffic and zero in on the IP address in question

✗

Review the Network Access Control Log to view the network packet information and zero in on the IP address in question

✗

Review the CloudWatch Events Logs to view the traffic coming into the internet gateway and identify the IP address in question

✗

Review the Cloud Trail Activity Logs, filter by instance, and view all API activity for the EC2 instance in question to identify the IP address in question

Explanation

You can use VPC Flow Logs to gain visibility into the requests coming into your application. With VPC Flow Logs, you can capture information regarding the IP traffic that is going to and from the network interface of your VPC. Reviewing these logs can help you spot traffic anomalies and attack patterns that can signal an active DDoS attack. VPC Flow Logs once enabled, will be streamed to a log group in CloudWatch Logs for analysis.

The remaining choices are incorrect for the following reasons:

● Network Access Control Lists do not have their own log groups on AWS. Network Access Control Lists can be configured to block certain protocols or malicious IP addresses to assist in the remediation of an active DDoS attack.

● CloudWatch Events Logs are captured by CloudWatch Logs to store, monitor, and analyze CloudWatch Events in your AWS environment, not the network traffic. Whenever a CloudWatch Event happens, the log stream is created and the data is sent to CloudWatch Logs.

● The CloudTrail service monitors and records account API activity across all of your AWS resources. With CloudTrail, you can gain visibility into the activity going on with a specific EC2 instance by filtering by EC2 instance ID. This will allow you to view all API activity that has occurred on the EC2 instance in question and from what IP address the activity was performed. CloudTrail does not give visibility into the traffic coming in or out of your network interface.

https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/visibility.html

#16

With detailed monitoring enabled on an EC2 instance, how often is metric data sent to CloudWatch?

✗

Every 5 minutes

✓

Every minute

✗

Every 30 seconds

✗

Every 15 minutes

Explanation

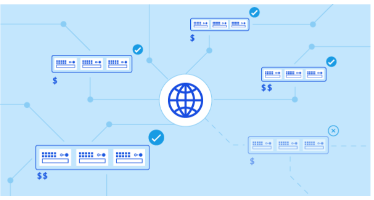
By default, Amazon EC2 metric data is automatically sent to CloudWatch in 5-minute periods. However, you can, enable detailed monitoring on an Amazon EC2 instance, which sends data to CloudWatch in 1-minute periods

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch.html

Covered in this lecture

Summary - Domain One

Course:Designing Highly Available, Cost Efficient, Fault Tolerant, Scalable Systems for Solutions Architect Associate on AWS



13m

#17

You are a security engineer at New World Bank. Your organization created a new online banking platform in AWS that is hosted on a fleet of EC2 instances. The software development team has created test, staging, and production environments for the new application. The team has been creating and managing encryption keys using the Key Management Service for all of the environments to provide encrypted data at rest. Now that the application is live, the encryption keys for the test and staging environments are no longer needed as these environments will be decommissioned. In order to avoid the management overhead and costs associated with maintaining the unused KMS keys, you need to delete the existing keys that are being stored in the KMS service. What is the safest process to delete the existing keys?

✗

Disable the KMS Keys

✗

Delete the KMS key material, leave the KMS key in place in case it is needed for the future

✗

Review the KMS Key Usage, delete the KMS key alias in case the KMS key is needed in the future

✓

Delete the KMS keys with a 30 day waiting period

Explanation

Deleting an AWS KMS key from AWS Key Management Service is destructive and potentially dangerous. It deletes the key material and all metadata associated with the KMS key and is irreversible. If you delete a KMS key, you can no longer decrypt the data that was encrypted with that KMS key, which means that the data becomes unrecoverable. The AWS KMS service will require you to set a waiting period of 7 – 30 days before a key is deleted. The default waiting period is 30 days.

The remaining choices are incorrect for the following reasons:

● Disabling the KMS key is a best practice and is a recommended alternative step to deleting a KMS key. Disabling the KMS key, however, decommissions key usage but does not stop the charges associated with the management of the KMS key.

● Deleting a KMS key deletes the key material and all metadata associated with the KMS key and is irreversible. After a KMS key is deleted, you can no longer decrypt the data that was encrypted under that KMS key, which means that data becomes unrecoverable. No KMS key is left behind after deleting.

● While reviewing past KMS key usage is a recommended best practice prior to deletion of a KMS key, deleting a KMS key Alias will not delete the KMS key itself. An alias is a friendly name for an AWS KMS key and deleting the alias allows you to change the alias for the KMS key.

🔗https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys.html

#18

Your organization has a new online bill payment system in AWS that is hosted on a fleet of EC2 instances. The application is a two-tier application with a web/app server running on an EC2 instance and a MySQL Database server running on Amazon RDS for transaction storage. Your organization has recently decided to take a centralized approach to user session management and will now store user-session information centrally in DynamoDB. You have been asked to set up an identity and access management solution that will allow the EC2 instance to access the DynamoDB table. Which of the following is a secure way of ensuring that the EC2 Instance can access the user session information from the DynamoDB table in a secure way?

✗

Set up AWS Single Sign-On (SSO) for the EC2 instance with permissions to interact with DynamoDB.

✗

Set up an IAM Group with the permissions to interact with DynamoDB and assign it to the EC2 Instance

✗

Create a KMS key with the permissions to interact with DynamoDB and associate it with the EC2 Instance

✓

Create an IAM Role with permissions to interact with DynamoDB and assign it to the EC2 Instance

Explanation

You can use AWS IAM to create a role to allow resources to interact with each other. Once a role is created and associated with the EC2 instance, an application running on an Amazon EC2 instance can assume to perform actions in your account including interacting with

DynamoDB tables. This role is assigned to the EC2 instance when it is launched. Applications running on that instance can retrieve temporary security credentials and perform actions that the role allows for DynamoDB.

The remaining choices are incorrect for the following reasons:

● AWS Single Sign-On is a service that allows you to centrally manage SSO access to all of your AWS accounts and cloud applications. AWS Single Sign-On helps you manage SSO access and user permissions across all your AWS accounts in AWS Organizations.

● An IAM user group is a collection of IAM users. User groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users. Groups are not used for the purpose of allowing one AWS service to interact with the other.

● KMS keys are used to encrypt data you store in AWS services. These keys are associated with AWS data services like S3, RDS, DynamoDB and EBS volumes to provide encryption of the data in those AWS services.

🔗https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

#19

You are a security engineer at a FinTech company. After a recent audit, it has been mandated that all financial statements containing personally identifiable information stored by the organization must be encrypted at rest. Currently, the finance team stores customer loan accounting statements and business financial records on an S3 bucket in the Ohio region. Which of the following solutions would provide the necessary encryption to protect the existing financial statement data at rest? (Choose two)

✕

Turn on encryption for the current S3 bucket and create a lifecycle rule to encrypt the existing objects in the current S3 bucket.

✓

Create a new S3 bucket, turn on encryption and upload the financial statements to the newly created bucket

✕

Create a new S3 bucket, turn on encryption, and set up cross-region replication to import all of the financial statements from the existing bucket to the new bucket.

✓

Turn on encryption for the current S3 bucket and create and run an S3 batch job to encrypt existing objects in the current S3 bucket.

Explanation

AWSS3 has a feature that can be configured during bucket creation to turn on encryption at the bucket level to provide server-side encryption for objects uploaded onto the S3 bucket. Once SSE is enabled, all objects uploaded into the S3 bucket will be encrypted and will require access to the encryption key in order to decrypt the data.

Whenturning on encryption for S3 buckets, existing objects in the bucket do not inherit the encryption setting. Only newly uploaded objects will inherit the encryption of the new configuration. Existing objects will remain unencrypted if they are not explicitly configured for encryption. One way to retroactively encrypt existing objects is to create an S3 batch job for your S3 bucket. The Copy operation can be used to copy existing unencrypted objects and write them back to the same bucket as encrypted objects.

The remaining choices are incorrect for the following reasons:

● Turning on encryption for the existing bucket will not affect the existing objects in the bucket. Only new objects uploaded after the configuration change will inherit the encryption. S3 lifecycle rules are not used to encrypt objects or import bulk objects to S3 buckets.

● Turning on encryption for the existing bucket will not affect the existing objects in the bucket. Only new objects uploaded after the configuration change will inherit the encryption. S3 cross region replication is primarily used to make copies of your S3 objects in a second AWS region, not bulk import objects to a new bucket.

🔗https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-copy-object.html

#20

Your CloudHSM high availability (HA) group has suffered a loss of communication between all its HA members. What method can you call to recover from this event without performing a manual recovery?

✕

HSMManager.recover()

✕

HSMManager.reinitialize()

✗

LunaSlotManager.recover()

✓

LunaSlotManager.reinitialize()

Explanation

In a high availability (HA) Cloud HSM environment, if there is a loss of all HA members (i.e., there is a complete loss of communication with all the members of your HA group), you can use the LunaSlotManager.reinitialize() method. With this instruction, you will not have to restart your applications. Alternately, you can restart your applications and use manual recovery.

🔗http://docs.aws.amazon.com/cloudhsm/latest/userguide/ha-best-practices.html#ha-config-recovery

#21

An AWS account owner is sharing his/her root credentials with multiple people who need access to the account. A hacker obtains the AWS account's root user credentials, accesses the AWS account, and deletes all of the account's stored data. This disrupts all sales related to the account. What steps could a system administrator have taken to prevent this type of unauthorized access, and minimize the risk if someone's credentials are stolen? (Choose 3 answers)

✗

Limit the root user's access to the account.

✓

Set up an MFA for each IAM user.

✓

Create an IAM user account for each person who needs access to the account.

✓

Create an IAM Administrator role, and avoid using root user credentials.

Explanation

You use an access key (an access key ID and secret access key) to make programmatic requests to AWS. However, do not use your AWS account root user access key. The access key for your AWS account root user gives full access to all your resources for all AWS services, including your billing information. You cannot reduce the permissions associated with your AWS account root user access key.

Therefore, protect your root user access key like you would your credit card numbers or any other sensitive secret.

🔗https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

#22

You are a security engineer for a streaming company that uses DataViews, a widely used 3rd party monitoring and logging tool, to monitor application performance. Your team has brought it to your attention that they have recently been alerted by the DataViews team that there has been a data breach and some AWS access key credentials in use by the program may have been compromised. You need to determine if any credentials in use by the DataViews program have been compromised and quickly remediate the issue. Which of the following solutions would provide the necessary steps to triage the access key usage and remediate the incident?

✕

Go into the Trusted Advisor security dashboard to determine if a security alert has been generated for the access key and use the KMS service to delete the compromised access keys. Use the KMS service to create a secure encrypted master key for use with the DataViews application going forward.

✓

Use the CloudTrail service to filter by access key to view all API requests made with the compromised keys and use the IAM service to disable the compromised keys. Create an IAM role for use with the DataViews application going forward.

✕

Use the AWS Config service to determine any configuration changes to the compromised access keys and use the system manager service to delete the compromised keys and generate a secure keypair for the DataViews application to use going forward.

✕

Go into the Inspector console to view any suspicious activity surrounding the compromised access key and trigger a lambda function to automatically delete the compromised keys. Create an IAM role for use with the DataViews application going forward.

Explanation

Explanation: The CloudTrail service monitors and records account activity across all of your AWS resources. With CloudTrail, you can gain visibility into the activity going on with a specific access key by filtering by the access key. This will allow you to quickly zero in on activity for a specific username or access key ID and determine any unusual usage of the compromised access key. The IAM service can then be utilized to disable then delete the compromised key and create a new role for the DataViews application. In line with the best practices set forth in the security pillar of the AWS Well-Architected framework, you should employ the use of roles when allowing applications to access AWS resources for enhanced security.

The remaining choices are incorrect for the following reasons:

● Under the upgraded support plan, Trusted Advisor will check popular code repositories for access key usage and for irregular EC2 usage indicative of a compromised access key. The KMS service, however, is used to create and manage encryption keys used in the process of providing data encryption for AWS data and storage services such as S3, RDS, and EBS not to generate access keys for use with 3rd party applications.

● AWS Config is primarily used to audit the configurations of your AWS resources. AWS Config can assist with security monitoring by alerting you to when security-related resources such as security groups and IAM credentials have had changes to the baseline configurations. AWS Config does not give visibility into the usage patterns of the resources in question but is used to audit configuration changes deviating from baseline configurations or defined compliance rules.

● AWS Inspector is a tool used primarily for the purpose of checking the network accessibility and security vulnerabilities of your EC2 instances and the security state of the applications running on those instances as opposed to specific access key usage. Inspector assessments check your infrastructure for Network reachability, CVE exposure, CIS benchmarks, and Amazon security best practices. Results from assessment runs are generated as findings with recommended steps for remediation.

🔗https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/identity-management.html
#23

Your team has reached out to you to design a secure way for your EC2 golden images that were created with EC2 Image Builder to be shared with the other environments that make up your AWS Organization. What is the best way to securely share the EC2 Images with the other environment accounts that make up the AWS Organization?

✗

Enable AWS Signer within the AWS Organization, create a signature for the EC2 images to allow them to be shared across all of the accounts in the AWS Organization.

✓

Enable sharing within the AWS Organization, create a resource share in AWS Resource Access Manager to share the images across the organization.

✗

Enable AWS Single Sign-On within the AWS Organization, grant SSO access to the EC2 images for all accounts in the AWS Organization

✗

Enable AWS Secrets Manager within the AWS Organization, create a secure secret to allow access to the EC2 images for all accounts in the AWS Organization

Explanation

AWS Resource Access Manager can be used to help you securely share the AWS resources that you create in one AWS account with other AWS accounts. If you have multiple AWS accounts, you can create a resource once and use AWS RAM to make that resource accessible to those other accounts. If your account is managed by AWS Organizations, then you can share resources with all of the other accounts in the organization. EC2 Image Builder integrates with AWS Resource Access Manager to allow you to securely share certain resources with any AWS account or through AWS Organizations. When you share a resource with another AWS account, you are granting access to principals in that account to the shared resource. Any policies and permissions that apply to the account you shared the resource with will also apply to the shared resource.

The remaining choices are incorrect for the following reasons:

● AWS Signer is used as a code signing service to ensure the trust and integrity of your code for AWS Lambda. AWS Signer is not used to share resources among AWS Organization accounts.

● AWS SSO is primarily used to grant access to your AWS accounts and any business applications that support SSO using SAML 2.0. AWS SSO is not used to share EC2 images among AWS Organization accounts.

● AWS Secrets Manager is designed to help you protect secrets needed to access your applications, services, and IT resources, not to share resources among Organization accounts.

🔗https://docs.aws.amazon.com/imagebuilder/latest/userguide/manage-shared-resources.html
#24

You have been charged with investigating cloud security options for your company in light of recent suspected threats. You are aware that certain AWS services can help mitigate DDoS attacks, and you are specifically looking for a service that provides protection from counterfeit requests (Layer 7) or SYN floods (Layer 4). Which services provide this protection? (Choose 2 answers)

✗
Route 53

✓
Amazon API Gateway

✓
CloudFront with AWS Shield

✗
VPC Security Groups

Explanation

Amazon API Gateway automatically protects your backend systems from distributed denial-of-service (DDoS) attacks, whether attacked with counterfeit requests (Layer 7) or SYN floods (Layer 3). Additional reading is available here (https://aws.amazon.com/api-gateway/faqs/).

AWS Shield Advanced includes intelligent DDoS attack detection and mitigation for not only for the network layer (layer 3) and transport layer (layer 4) attacks but also for application layer (layer 7) attacks.

NACLs do not provide DDoS mitigation. They are used to control ingress and egress into a subnet based on port and source IP range. Route 53 can protect against DNS based DDoS attacks but does not protect entire layers. Elastic Load Balancing can protect EC2 instances specifically, but not other AWS resources.

🔗http://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html

#25

A route table in VPC can be associated with multiple subnets, and a subnet can be associated with _______ at one time.

✓

one route table

✗

all route tables in a VPC

✗

two route tables

✗

five route tables

Explanation

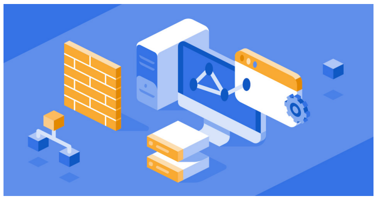
Every subnet in your VPC must be associated with exactly one route table at a time. However, the same route table can be associated with multiple subnets.

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html

Covered in this lecture

Summary

Course:AWS Virtual Private Cloud: Subnets and Routing



12m

#26

Which statement regarding VPC peering is correct?

✗

VPC-A can communicate with VPC-B through their peering connections with VPC-C.

✗

VPCs with overlapping CIDR block ranges can establish a peering connection.

✓

VPC-A and VPC-B have identical CIDR block ranges. VPC-C can establish peering connections with both VPC-A and VPC-B.

✗

VPCs with identical CIDR block ranges can establish a peering connection.

Explanation

The connectivity between the VPCs is implemented through the existing AWS network infrastructure, and so it is highly available with no bandwidth bottleneck. As peered connections operate as if they were part of the same network, there are restrictions when it comes to your CIDR block ranges that can be used.

Of the choices below, the only possible option is connecting two separate VPCs with identical CIDR blocks to the same separate VPC. The other choices, which involve duplicate or overlapping CIDR ranges, or daisy-chain connections between VPC peer connections, are not possible.

🔗https://docs.aws.amazon.com/vpc/latest/peering/peering-configurations-partial-access.html#one-to-two-vpcs-simple-hub

#27

Today while reviewing AWS Inspector findings, you notice a finding has been found for a common vulnerability and exposure (CVE) for a missing update. You now need to log the finding and coordinate the remediation of the issue right away. Going forward, you and the team would like to have a way to remediate these issues moving forward in an automated way. You need to create a solution that will allow you to automatically remediate AWS Inspector findings for EC2 instances when they occur. Which of the following infrastructure security solutions will allow you to have automatic remediation of the findings when they are detected by AWS Inspector?

✗

Create an AWS Audit Manager rule for AWS Inspector findings to trigger a Lambda function to remediate the issue whenever an AWS Inspector finding is discovered.

✗

Create a Cloudtrail alert for AWS Inspector findings to trigger a Lambda function to remediate the issue whenever an AWS Inspector finding is discovered.

✓

Create an SNS notification for AWS Inspector to publish findings to and trigger a Lambda function to remediate the issue whenever an AWS Inspector finding is published.

✗

Create an AWS Config Alert for AWS Inspector findings to trigger a Lambda function to remediate the issue whenever an AWS Inspector finding is discovered.

Explanation

Amazon Inspector automatically assesses resources for vulnerabilities and then produces a detailed list of security findings prioritized by level of severity. In order to set up automatic remediation for Amazon Inspector, you must first run an assessment and publish any security findings to an Amazon Simple Notification Service (SNS) topic. Then, you create an AWS Lambda function that is triggered by those notifications. Finally, the Lambda function examines the findings and then implements the appropriate remediation based on the type of issue.

The remaining choices are incorrect for the following reasons:

● AWS Audit Manager is used to assist you in auditing your AWS usage. This service can be used to evaluate controls to determine if they are operating as intended.

● The CloudTrail service monitors and records account activity across all of your AWS resources. WAlerts for the CloudTrail service are set up and triggered, however, through the CloudWatch service.

● AWS Config is primarily used to audit the configurations of your AWS resources. AWS Config audits your AWS resources based on defined compliance rules and then alerts on any configuration deviations or resources non-compliant with defined rules.

🔗https://aws.amazon.com/blogs/security/how-to-remediate-amazon-inspector-security-findings-automatically/
#28

The following IAM policy has been associated with the Business Intelligence team group: { "Version": "2012-10-17", "Statement": [{   "Effect": "Deny",   "Action": ["s3:GetObject",   "s3:ListBucket"   ],   "Resource": "arn:aws:s3:::Quarterly-Statements/*" }, {   "Effect": "Allow",   "Action": "s3:*",   "Resource": "arn:aws:s3:::Daily-Claims/*" }]}Based on the identity and access management policy attached to the Business Intelligence Team group, what could be the reason the users are unable to access the financial statements stored on the Quarterly-Statements S3 bucket?

✕

The policy resource specified for the Quarterly-Statements S3 bucket is formatted incorrectly.

✓

The policy denies listing and retrieving objects from the Quarterly-Statements S3 bucket.

✕

The policy denies listing and retrieving objects from the Quarterly-Statements and Daily Claims S3 buckets.

✕

The policy version specified is incorrect for the Quarterly-Statements S3 bucket.

Explanation

In an IAM JSON policy, the Effect element is used to specify if a policy allows or denies access to a principle. The Deny value will deny access to the principal for the actions specified in the Action element. This policy denies listing and retrieving objects from the Quarterly-Statements S3 bucket.

The remaining choices are incorrect for the following reasons:

● The policy Resource element should include a list of resources to which the actions apply. The format of the resource element for the specified S3 bucket is correct.

● The policy denies listing and retrieving objects from the Quarterly-Statements but allows all actions to the Daily-Claims S3 buckets.

● The policy version specifies the version of the policy language that you want to use. As a best practice, use the latest 2012-10-17 version. The policy version as listed in the version element is correct for the Quarterly-Statements S3 bucket.

🔗

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html#policies_resource-based

#29

Which of the following identity and access management solutions would allow users to log in to your company’s AWS-hosted application using existing Microsoft Active Directory credentials?

✕

Create a service control policy (SCP) for Microsoft Active Directory in AWS Organizations to allow users to sign in with their Microsoft Active Directory credentials.

✗

Create an identity pool in AWS Cognito and add Microsoft Active Directory to the pool as an identity provider to allow users to sign in with their existing Microsoft Active Directory credentials.

✓

Set up an AD Connector directory in AWS Directory to allow users to sign in with their existing Microsoft Active Directory credentials.

✗

Create a Microsoft Active Directory group in AWS Identity and Access Manager to allow users to sign in with their existing Microsoft Active Directory credentials.

Explanation

The AWS Directory Service will allow you to use Microsoft Active Directory (AD) with other AWS services. The AD Connector type directory specifically can be used when you need to allow your on-premises users to log in to AWS applications and services with their Active Directory credentials.

The remaining choices are incorrect for the following reasons:

● You would typically use service control policies to set permission guardrails across accounts in your AWS Organization. This will allow you to establish controls that all IAM users adhere to. A SCP is not used to set up sign in with Microsoft Active Directory.

● Amazon Cognito identity pools provide temporary AWS credentials for users who are guests (unauthenticated) and for users who have been authenticated and received a token. An identity pool is a store of user identity data specific to your account. User pools are for authentication (identify verification). With a user pool, your app users can sign in through the user pool or federate through a third-party identity provider (IdP) like Microsoft Active Directory. Identity pools are for authorization (access control). You can use identity pools to create unique identities for users and give them access to other AWS services.

● An IAM user group is a collection of IAM users. User groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users. Groups are not used for the purpose of extending your Microsoft Active Directory into AWS.

🔗https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html

#30

You have a Lambda function named ai-deep-thinker deployed into the us-west-1 region in your production AWS account 998877665544. You wish to restrict execution to members of the AI team within your organisation. To do so you are creating an IAM Policy with the following structure and attach it to the IAM AI-Team group : {"Version": "2012-10-17","Statement": [{"Action": ["TOKEN1"],"Effect": "Allow","Resource": TOKEN2}]} To complete the policy, which are the correct values that replace TOKEN1 and TOKEN2? (Choose 2 answers)

✗

TOKEN1 = arn:aws:lambda:us-west-1:998877665544:ai-deep-thinker

✓

TOKEN1 = lambda:InvokeFunction

✗

TOKEN1 = lambda:ExecuteFunction

✓

TOKEN2 = arn:aws:lambda:us-west-1:998877665544:ai-deep-thinker

Explanation

Answers "**TOKEN1 = lambda:InvokeFunction**" and "**TOKEN2 = arn:aws:lambda:us-west-1:998877665544:ai-deep-***" are correct. The action lambda:InvokeFunction should be used to control execution of a Lambda function. A Lambda ARN takes the form of arn:aws:lambda:<aws region>:<account number>:<function name>. Specifying a Lambda ARN in the policy will restrict invocation to that particular Lambda function.

🔗https://aws.amazon.com/blogs/compute/easy-authorization-of-aws-lambda-functions/

#31

You have been asked to tighten up the password policies in your organization after a serious security breach, so you need to consider every possible security measure. Which of the following is not an account password policy option for IAM users?

✓

Force IAM users to contact an account administrator when the user has entered his password incorrectly.

✕

A minimum password length.

✕

Allow all IAM users to change their own passwords.

✕

Require IAM users to change their password after a specified period of time.

Explanation

IAM users need passwords in order to access the AWS Management Console. (They do not need passwords if they will access AWS resources programmatically by using the CLI, AWS SDKs, or the APIs.)

You can use a password policy to do these things:

- Set a minimum password length.
- Require specific character types, including uppercase letters, lowercase letters, numbers, and non-alphanumeric characters. Be sure to remind your users that passwords are case sensitive.
- Allow all IAM users to change their own passwords.
- Require IAM users to change their password after a specified period of time (enable password expiration).
- Prevent IAM users from reusing previous passwords.
- Force IAM users to contact an account administrator when the user has allowed his or her password to expire.

🔗

http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_ManagingPasswordPolicies.html

#32

You are testing an EC2 instance store-backed instance, and it fails a status check. You’ve verified that associated applications are not running as expected. Upon checking the system logs, you see this entry: Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.120050727 (Red Hat 4.0.1-5)) #1 SMP Mon March 28 03:41:49 SAST 2017...Kernel command line: root=/dev/sda1 ro 4...Registering block device major 8...Kernel panic - not syncing: VFS: Unable to mount root fs on unknown-block(8,1) What is the most likely issue?

✕

A disconnected block device to the instance

✗

A missing GRUB configuration file

✗

A corrupted file system

✓

A hardware device failure

Explanation

When a VFS is unable to mount root fs on unknown-block on a store-backed instance, the most likely cause is hardware device failure. To fix this issue, AWS recommends that you terminate the instance and launch a new instance using a modern kernel.

🔗

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstances.html
#33

You are a security architect at a large Health insurance company. The company's corporate website is hosted on a cluster of EC2 instances. The production web server log files are stored on the server directly and the company has a requirement that the data has to be kept securely for at least a year for audit purposes. These log files are frequently causing the webserver to run out of storage space, so the team has decided to use Logrotate to rotate logs from the EC2 instance to S3 to improve the storage capabilities. After implementing the new solution, the team realized some log files were overwritten on the initial rollout of the solution. They have come to you to assist in creating a data protection solution that will allow for the protection of the log files in the event of data loss and a secure long-term storage solution that will enforce compliance needs.Which of the following solutions would add the appropriate protection to meet the requirements for the log files?

✓

Create an S3 bucket with versioning turned on with a lifecycle rule to Glacier; Employ Glacier vault lock

✗

Create an S3 bucket with cross-region replication to Glacier; Set up a Glacier access control list

✗

Create an S3 bucket and configure a backup plan for the bucket; Store completed backups in AWS Backup and turn on encryption for backups.

✕

Create an S3 bucket and attach an EBS volume to the S3 bucket for persistent data; Store EBS snapshots in AWS Backup

Explanation

Amazon S3 has a versioning feature that can be enabled to protect your data from loss. You can use the S3 Versioning feature to preserve, retrieve, and restore every version of every object stored in your buckets. Versioning enabled buckets can help you recover objects from accidental deletion or overwrite. If you overwrite an object in the bucket, it results in a new object version in the bucket. This feature will help protect the log data from loss. Amazon S3 also has a lifecycle rule feature to help transition data between storage classes or expire them out of the S3 bucket. By setting up a lifecycle rule for the log files to be sent to Glacier, the long-term compliance needs of the log files can be met. Adding a Glacier vault lock allows you to deploy and enforce compliance controls for individual S3 Glacier vaults with a vault lock policy.

The remaining choices are incorrect for the following reasons:

● Amazon S3 replication can be used to automatically replicate S3 objects across different AWS Regions by using Amazon S3 Cross-Region Replication (CRR) or between buckets in the same AWS Region by using Amazon S3 Same-Region Replication (SRR), but doesn't help with longterm storage policies or encryption.

● AWS Backup enables you to centralize and automate data backups across AWS services. This service is used to create backup plans for Amazon EC2 instances, Amazon EBS volumes, Amazon RDS databases, Amazon DynamoDB tables, Amazon Neptune databases, Amazon DocumentDB databases, Amazon EFS file systems, Amazon FSx for Lustre file systems, Amazon FSx for Windows File Server file systems, and AWS Storage Gateway volumes, NOT S3 buckets.

● Amazon EBS volumes are only associated with EC2 instances and cannot be attached to S3 buckets. EBS volumes are used to provide persistent block-level storage for EC2 instances.

🔗https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html

#34

Which AWS service sends data to CloudWatch every minute by default?

✓

Amazon RDS

✗

Amazon EC2

✗

EC2 Autoscaling groups

✗

Amazon SNS

Explanation

Amazon RDS automatically sends metrics to CloudWatch every minute for each active database. You are not charged additionally for Amazon RDS metrics in CloudWatch.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/MonitoringOverview.html#monitoring-cloudwatch
Covered in this lecture
Amazon RDS Integrated Monitoring Tools
Course:Amazon RDS: Introduction to Monitoring

7m

#35

You use various AWS services and would like to minimize security breaches caused by accidental information disclosure. What are some valid strategies for achieving this goal? (Choose 2 answers)

✓

Use AWS permissions to manage access to resources for services such as Amazon S3.

✓

Use encryption to protect confidential data on Amazon EBS or RDS.

✗

Use data integrity checks on data stored in your Amazon EC2 instance.

✕

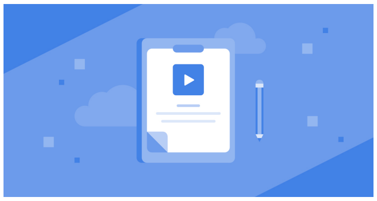
Use the object versioning functionality available on Amazon S3.

Explanation

Accidental information disclosure can be limited by designating data as confidential and limiting the number of users who can access it. Use AWS permissions to manage access to resources for services such as Amazon S3 to limit user access. Use encryption to protect confidential data on Amazon EBS or RDS. The other strategies would not protect against accidental information disclosure.

https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

Covered in this lecture
Summary - Domain Three
Course:Domain three - Summary - Designing Secure Application and Architectures



5m

#36

You’re in charge of a three-tier application running on EC2 instances with a DynamoDB database. Your team currently uses a third-party vulnerability management tool to provide actionable insight into your infrastructure’s security risks.Your third-party vulnerability tool has reported some EC2 instances that have not been patched to the correct version. You have been asked to come up with a solution that automates the process of patching managed nodes with both security-related and other types of updates.Which of the following infrastructure solutions would automate the process of patching managed nodes with both security-related and other types of updates?

✓

Use the patch manager feature of AWS Systems Manager to automate the process of patching instances with both system and security-related updates.

✕

Create a service action in AWS Service Catalog to automate the process of patching instances with both system and security-related updates.

✕

Use the service map feature in AWS X-Ray to schedule and automate the process of patching instances with both system and security-related updates.

✕

Create a job in AWS Batch to automate the process of patching instances with both system and security-related updates.

Explanation

AWS Systems Manager has a patch manager feature that can be used to automate the process of patching managed nodes with both security-related and other types of updates. You can use Patch Manager to apply patches for both operating systems and applications. Patch Manager provides options to scan your managed nodes and report compliance on a schedule, install available patches on a schedule, and patch or scan targets on demand.

The remaining choices are incorrect for the following reasons:

● AWS Service Catalog is primarily used to allow organizations to create and manage catalogs of IT services that are approved for use on AWS. AWS Service Catalog does not allow you to automate the process of patching instances with both system or security-related updates.

● AWS X-Ray is used to help developers analyze and debug production, distributed applications, such as those built using a microservices architecture. AWS X-Ray is not used to automate the process of patching instances with both system or security-related updates.

● AWS Batch can be utilized to help you to run batch computing workloads of any scale.AWS Batch is not used to automate the process of patching instances with both system or security-related updates.

🔗https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html
#37

The Cloud Operations team at your company has alerted you to an unusual amount of requests for the Webserver. Upon investigation, you determine that a security group associated with the server has a rule for SSH that allows connections from all sources (0.0.0.0/0) over Port Range 22. Allowing 0.0.0.0/0 over Port Range 22 introduces a security risk and it appears this server is under an SSH brute force attack. You and the team quickly move to resolve the immediate threat. Now, you need to design a solution that allows for visibility into similar attacks to allow for fast remediation of compromised instances going forward. Which of the following infrastructure security solutions would be a good choice for US Hardware to gain visibility into SSH brute force attacks on Linux instances going forward?

✓

Enable AWS GuardDuty for the AWS account, review the GuardDuty console for “UnauthorizedAccess:EC2/SSHBruteForce” findings.

✕

Enable AWS Detective and configure it to trigger a CloudWatch alarm and send the SSH traffic information to Amazon CloudWatch Logs when a “EC2/BruteForce” finding is discovered.

✕

Enable Macie on the EC2 instance and automatically run assessments daily; create a CloudWatch alert to trigger automatically in the event of an EC2 Brute Force assessment failure.

✕

Create an AWS Config rule to trigger a CloudWatch alarm whenever there is a configuration change on the EC2 instance security group allowing 0.0.0.0/0 over Port Range 22 for SSH.

Explanation

Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and resources for malicious activity and delivers detailed security findings for visibility and remediation to the GuardDuty console for further investigation. GuardDuty can monitor and detect for SSH brute force attacks. GuardDuty monitors VPC Flow Logs for suspicious activity and if an SSH brute force attack is suspected, a finding of type “UnauthorizedAccess:EC2/SSHBruteForce” is generated in the GuardDuty console. This finding informs you that an EC2 instance in your AWS environment was involved in a brute force attack aimed at obtaining passwords to SSH services on Linux-based systems. This can indicate unauthorized access to your AWS resources.

The remaining choices are incorrect for the following reasons:

● Amazon Detective is primarily used to help identify the route cause of security issues, but not for brute force attacks.

● AWS Macie is a service for the purpose of protecting sensitive data in AWS not logging for Route53. Macie can monitor S3 buckets in your account and alert you to sensitive data such as personally identifiable information.

- AWS Config is primarily used to audit the configurations of your AWS resources. AWS Config can assist with security monitoring by alerting you to when security-related resources such as EC2 instances, security groups, and IAM credentials have had changes to the baseline configurations. Getting alerted to the security group change allowing 0.0.0.0/0 over Port Range 22 for SSH may help prevent EC2/SSH BruteForce attacks but AWS Config will not alert you of an attack in progress.

🔗https://aws.amazon.com/premiumsupport/knowledge-center/identify-attacks-with-guardduty/

#38

The identity and access management solution your team has created should allow users to sign up for a new account and to sign in to your company's application through Okta. Which of the following identity and access management solutions would allow users to create new accounts and sign in to existing accounts with Okta, a SAML 2.0 identity provider?

✗

Create a connection in AWS Direct Connect, add Okta as a SAML provider to the new connection to allow users to sign in with Okta.

✓

Create a user pool in AWS Cognito, add Okta as a SAML provider to the user pool to allow users to sign in with Okta.

✗

Create a new configuration profile in AWS AppConfig, add Okta as a SAML provider to the configuration profile to allow users to sign in with Okta.

✗

Create a new subscription in AWS Data Exchange, add Okta as a SAML provider to the new subscription to allow users to sign in with Okta.

Explanation

With AWS Cognito, application users can sign in through SAML identity providers (IdP) like Okta. This is facilitated by setting up a user pool with an app client and a user pool domain in AWS Cognito. After setting up the user pool you are then able to add your SAML identity provider to your user pool to facilitate login with that provider.

The remaining choices are incorrect for the following reasons:

● AWS Direct Connect is primarily used to link your internal network to an AWS Direct Connect location over a standard Ethernet fiber-optic cable. AWS Direct Connect is not used to provide login with SAML 2.0 providers.

● AWS AppConfig can be used to create, manage, and quickly deploy application configurations. AWS AppConfig is not used to provide login with SAML 2.0 providers.

● AWS Data Exchange is used to find, subscribe to, and use third-party data in the cloud. AWS Data Exchange is not used to provide login with SAML 2.0 providers.

🔗https://aws.amazon.com/premiumsupport/knowledge-center/cognito-okta-saml-identity-provider/

#39

Your company uses an on-premises identity system such as Active Directory to authenticate users locally. You would like to implement a single sign-on (SSO) to grant the same users access into the AWS console without requiring them to authenticate again.What possible solution below can be used to provide this type of access?

✓

If your company's identity system is compatible with SAML 2.0, establish trust between your company's identity system and AWS

✗

If your company's identity system is compatible with Kerberos, establish trust between your company's identity system and AWS

✗

If your company's identity system is compatible with OpenID Connect (OIDC), establish trust between your company's identity system and AWS

✗

If your company's identity system is compatible with OAuth 2.0, establish trust between your company's identity system and AWS

Explanation

Answer “**If your company's identity system is compatible with SAML 2.0, establish trust between your company's identity system and AWS**” is correct. AWS supports identity federation with SAML 2.0 (Security Assertion Markup Language 2.0), an open standard that many identity providers (IdPs) use. This feature enables federated single sign-on (SSO), so users can log into the AWS Management Console or call the AWS API operations without you having to create an IAM user for everyone in your organization.

🔗https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html

#40

Your team has recently improved the security of its application infrastructure by setting up less permissive security groups and a Network Access Control List to be associated with your application VPC. After making the changes, traffic requests seem to be blocked and unable to make it to the website. VPC Flow logs are enabled for the VPC and logs are being sent to CloudWatch logs. As a part of the troubleshooting process, you and the team look to review the VPC flow logs for rejected traffic to try to identify the traffic that is being blocked. When you review the VPC Flow logs, however, you notice that no data is being generated for rejected traffic in the logs. Which of the following solutions could resolve this issue and get the blocked traffic in the logs? (Choose Two)

✓

Verify the VPC Flow log is configured to log all traffic to the CloudWatch Logs group

✗

Create a contributor insights rule to allow rejected traffic for the CloudWatch VPC log group to ensure you have visibility for rejected traffic in the CloudWatch Logs group.

✗

Create a response plan in AWS Incident Manager to set up logging for rejected VPC traffic to ensure you can log rejected traffic to CloudWatch Logs.

✓

Verify the VPC Flow log is configured to log rejected traffic to the CloudWatch Logs group.

Explanation

When creating a VPC flow log you can specify the type of traffic to capture in the CloudWatch Logs Group. In the Flow Log settings, you can choose to create a Flow log that captures all traffic, accepted traffic only, or rejected traffic only. To see rejected traffic, your VPC Flow log settings need to be configured to either capture all traffic or rejected traffic only.

The remaining choices are incorrect for the following reasons:

● You can use rules in Amazon CloudWatch Contributor Insights to gain security visibility into your VPC flow logs. The rules analyze flow logs in targeted groups in Amazon CloudWatch Logs and display the Top-N contributors for a given log field or combination of log fields. These rules are not set up to allow visibility for rejected traffic.

● AWS Incident Manager is a capability of AWS Systems Manager that enables you to create incident plans to allow for faster resolution of critical application availability and performance issues. Incident Manager helps you prepare for incidents with automated response plans so that issues can be resolved faster. Incident manager response plans are not used for the purpose of allowing visibility for rejected traffic.

🔗https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-cwl.html

#41

While troubleshooting a technical problem, a system administrator modified an EC2 instance's security group rules to allow SSH, and did not change the rule back to its original state. Going forward, you need to ensure a way to have visibility into security group rule changes and to be alerted when a change has occurred. Which monitoring solution would give you visibility into security group changes and alert you when a change to a security group has occurred?

✓

Create a rule in AWS Config to trigger whenever there is a change to a security group rule.

✕

Set up a CloudWatch alarm in the security section of the Trusted Advisor dashboard to trigger whenever there is a change to a Security Group Rule

✕

Install the Inspector agent on the EC2 instances, trigger an inspector assessment to run whenever there is a change to a Security Group Rule

✕

Set up an AWS Systems Manager alert to trigger whenever there is a change to a Security Group Rule

Explanation

You can use the AWS Config service to audit the configurations of your AWS resources. AWS Config can assist with security monitoring by alerting you to when security-related resources such as EC2 instances, security groups, and IAM credentials have had changes to the baseline configurations. AWS Config audits your AWS resources based on defined compliance rules then alerts on any configuration deviations or resources non-compliant to defined rules.

The remaining choices are incorrect for the following reasons:

● AWS Trusted Advisor is primarily used to provide recommendations that help you follow AWS best practices. Trusted Advisor does have a security section of the dashboard with a check for security groups. This Trusted Advisor check, however, checks the security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports as opposed to configuration changes.

● AWS Inspector is a tool used primarily for the purpose of checking the network accessibility and security vulnerabilities of your EC2 instances,

● AWS Systems Manager is primarily used as a unified user interface to view application and operational issues across your environment and manage them. You can use Systems Manager to automate operational tasks like stopping instances and remotely managing servers not managing configuration changes of resources.

🔗https://aws.amazon.com/blogs/security/how-to-monitor-aws-account-configuration-changes-and-api-calls-to-amazon-ec2-security-groups/
#42

You are an information security engineer at a large regional hospital. The hospital's patient portal application is hosted in AWS on an EC2 instance for the Web/App server that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default NACL settings. Based on traffic patterns, your team has reason to suspect that it is a malicious attack. You and the team need to determine a way to protect the subnets from specific IP addresses.Which of the following infrastructure security solutions would protect the subnets from the attack?

✓

Update the Inbound NACL rules to deny access from the specific IP addresses that you identify to block requests.

✕

Change the Inbound Security Groups to deny access from the specific IP address in question to block requests from that IP.

✕
Change the Outbound NACL to deny access from the specific IP address in question to block requests from that IP.

✕
Change the Outbound Security Groups to deny access from the specific IP address in question to block requests from that IP.

Explanation

A network access control list can be used as an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC. If you have identified Internet IP addresses or ranges that are unwanted or potentially abusive, you can block them from reaching your application with a deny rule.

The remaining choices are incorrect for the following reasons:

● A security group acts as a virtual firewall for your EC2 instances to control inbound and outbound traffic to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be assigned to a different set of security groups. In order to control traffic at the Subnet level, you would need to configure a NACL.

● The network ACL has outbound rules that allow outbound HTTP and HTTPS traffic out of the subnet. There's a corresponding inbound rule that enables responses to that outbound traffic.

🔗https://aws.amazon.com/blogs/security/how-to-help-prepare-for-ddos-attacks-by-reducing-your-attack-surface/
#43

You’ve built a mobile game app that reads daily game generated data files store in a S3 bucket created in the us-west-1 region. During the first full integration test of the application you observed an error in the apps log files “Action does not apply to any resource(s) in statement” during an attempt to read the daily game generated data files. All resources reside in the AWS account 123456789012. The configuration uses following AWS IAM Policy: {"Version": "2012-10-17","Statement": [{"Effect": "Allow","Action": ["s3:GetObject", "s3:GetObjectVersion"],"Resource": "arn:aws:s3:::gamedatafiles"}]} To remedy this issue, you do what:

✓

Change the Resource to arn:aws:s3:::gamedatafiles/*

✕

Change the Action to use s3:*

✕

Change the Resource to arn:aws:s3:us-west:123456789012:gamedatafiles

✕

Remove s3:GetObjectVersion from the Action array

Explanation

Answer "**Change the Resource to arn:aws:s3:::gamedatafiles/***" is correct. The Resource element specifies arn:aws:s3:::gamedatafiles/* for the GetObject, and s3:GetObjectVersion actions so that applications can read any objects in the gamedatafiles S3 bucket.

🔗https://aws.amazon.com/blogs/security/writing-iam-policies-how-to-grant-access-to-an-amazon-s3-bucket/

#44

In Amazon CloudFront, if you enable Logging, CloudFront records information about each ____________ and stores the files in the specified Amazon S3 bucket.

✕

edge location request for an object

✕

edge location request for a cache access

✕

end-user request for a cache access

✓

end-user request for an object

Explanation

In Amazon CloudFront, if you chose On for Logging, the Amazon S3 bucket that you want CloudFront to store access logs in, for example, myawslogbucket.s3.amazonaws.com. If you enable logging, CloudFront records information about each end-user request for an object and stores the files in the specified Amazon S3 bucket. You can enable or disable logging at any time.

http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html
Covered in this lecture
Course Summary
Course:How to Implement & Enable Logging Across AWS Services (Part 2 of 2)

5m

#45

An error has occurred in your company’s application and you are trying to retrace what happened. You come across this entry in the company’s CloudTrail logs. What events have happened, according to this log entry? (Choose 2 answers){ "eventVersion": "1.02", "userIdentity": { "type": "IAMUser", "principalId": "AIDACKCEVSQ6C2EXAMPLE", "arn": "arn:aws:iam::086441151436:user/AWSCloudTrail", "accountId": "086441151436", "accessKeyId": "AKIAI44QH8DHBEXAMPLE", "userName": "AWSCloudTrail", "sessionContext": {"attributes": { "mfaAuthenticated": "false", "creationDate": "2015-11-11T21:15:33Z" }}, "invokedBy": "internal.amazonaws.com" }, "eventTime": "2015-11-11T21:15:33Z", "eventSource": "kms.amazonaws.com", "eventName": "GenerateDataKey", "awsRegion": "us-west-2", "sourceIPAddress": "internal.amazonaws.com", "userAgent": "internal.amazonaws.com", "requestParameters": { "keyId": "arn:aws:kms:us-west-2:111122223333:alias/ExampleAliasForCloudTrailKMSkey", "encryptionContext": { "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-west-2:111122223333:trail/Default", "aws:s3:arn": "arn:aws:s3:::example-bucket-for-CT-logs/AWSLogs/111122223333/" }, "keySpec": "AES_256" }, "responseElements": null, "requestID": "581f1f11-88b9-11e5-9c9c-595a1fb59ac0", "eventID": "3cdb2457-c035-4890-93b6-181832b9e766", "readOnly": true, "resources": [{ "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab", "accountId": "111122223333" }], "eventType": "AwsServiceEvent", "recipientAccountId": "111122223333"}

✓

AWS KMS created a data key under a specific KMS key

✗

The public portion of the KMS key is arn:aws:kms:us-west-2:111122223333:alias/ExampleAliasForCloudTrailKMS key.

✓

CloudTrail called the AWS KMS GenerateDataKey API.

✗

The user’s pre-defined GenerateDataKey Java function was called by AWSCloudTrail.

Explanation

"resources": [{

"ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",

"accountId": "111122223333"

}]

indicates that AWS KMS created a data key under a specific KMS key.

"arn": "arn:aws:iam::086441151436:user/AWSCloudTrail"

[...]

"eventSource": "kms.amazonaws.com",

"eventName": "GenerateDataKey",

indicate that CloudTrail called the AWS KMS GenerateDataKey API.

🔗http://docs.aws.amazon.com/kms/latest/developerguide/services-cloudtrail.html

#46

Your application is most likely undergoing a Layer 7 HTTP Flood attack. The application is hosted in AWS as a 3 tier application running on a fleet of EC2 instances behind an application load balancer. Your team works to mitigate the threat in progress but you need to determine a way to automatically detect and mitigate these types of attacks in the future. Which of the following infrastructure security solutions would allow for automatic detection and mitigation of Layer 7 HTTP Flood Attacks in the future?

✗

Turn on AWS Config for the application load balancer, create a rule in AWS Config to track and automatically block requests from the offending source IP address.

✗

Enable AWS Shield on the application load balancer, turn on the managed rule group for "DDoS and HTTP floods" to automatically block requests from the offending source IP address.

✓

Enable AWS WAF on the application load balancer, set up a rate-based rule to automatically block requests from the offending source IP until the rate of requests falls below the set rate threshold.

✗

Update the listener on the application load balancer, add a rule for HTTPS over port 443 to automatically block any insecure requests coming into the application load balancer.

Explanation

AWS WAF is a web application firewall that lets you monitor the HTTP(S) requests that are forwarded to an Amazon CloudFront distribution, an Amazon API Gateway REST API, an Application Load Balancer, or an AWS AppSync GraphQL API. AWS WAF has a rate-based rule capability, which detects source IP addresses that make large numbers of HTTP requests within a 5-minute time span, and automatically blocks requests from the offending source IP until the rate of requests falls below a set threshold. A rate-based rule tracks the rate of requests for each originating IP address, and triggers the rule action on IPs with rates that go over a limit. You set the limit as the number of requests per 5-minute time span. You can use this type of rule to put a temporary block on requests from an IP address that's sending excessive requests.

The remaining choices are incorrect for the following reasons:

● AWS Config is primarily used to audit the configurations of your AWS resources. AWS Config does not have the capability to detect and block http requests but is used to audit configuration changes deviating from baseline configurations or defined compliance rules.

● AWS Shield is a managed DDoS service enabled by Amazon to protect applications running on AWS. Traffic will be blocked by AWS Shield during the remediation process of an active DDoS attack with no configuration needed by the end-user, but will not block for an HTTP Flood attack.

● Application Load Balancer HTTPS listeners are created to enable traffic encryption between your load balancer and clients initiating an SSL session. The listener checks for requests and enables the encryption as needed. Traffic is not blocked by the HTTPS listener.

https://aws.amazon.com/blogs/security/three-most-important-aws-waf-rate-based-rules/

#47

You are a security engineer at a healthcare company whose main business-critical application has 3 tiers and is running on a fleet of EC2 instances spread across the US Ohio and Oregon regions for high availability. The application must maintain HIPAA compliance and one of the mandates for maintaining certification is that the EBS volume data must be encrypted at rest. Under the new compliance requirements, the company has to have full control over the resources used to provide the encryption at rest. The company needs a solution that can allow them to generate and use their own encryption keys on their AWS resources. The solution needs to be compliant and allow the company to have explicit control over the key management process. Which of the following solutions would provide the necessary security to secure the EBS volume data at rest while allowing your company to have explicit control over the management of the encryption key creation and usage?

✗

Enable encryption with KMS managed keys

✗

Enable encryption withAWS certificate manager

✓

Enable encryption with Cloud HSM

✗

Install an ssl certificate on the EC2 instance to enable the appropriate encryption

Explanation

AWS CloudHSM is a cloud-based hardware security module that enables you to generate and use your own encryption keys on the AWS Cloud. This service can be utilized when a company needs to have explicit control over the key management process. With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs. The encryption keys that you generate and use with CloudHSM are accessible only by the HSM users that you specify. AWS has no visibility or access to your encryption keys.

The remaining choices are incorrect for the following reasons:

● The KMS service is able to allow you to create and manage encryption keys, but are managed by AWS and do not provide for explicit control over the key management process.

● AWS Certificate Manager is primarily used to provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks.

●An SSL certificate is a digital certificate that authenticates a website's identity and enables an encrypted connection. SSL stands for Secure Sockets Layer, a security protocol that creates an encrypted link between a web server and a web browser. Organizations add SSL certificates to their websites to secure online transactions and keep customer information private and secure not to configure encryption at rest.

🔗https://aws.amazon.com/cloudhsm/

#48

While building your environment on AWS you decide to use Key Management Service to help you manage encryption of data volumes. As part of your architecture you design a disaster recovery environment in a second region.What should you anticipate in your architecture regarding the use of KMS in this environment?

✕

KMS is not highly available by default; you have to make sure you span KMS across at least two availability zones to avoid single points of failure.

✓

KMS keys can operate on a multi-region scope, but AWS recommends region-specific keys for most cases.

✕

KMS is a global service, your architecture must account for regularly migrating encryption keys across regions to allow disaster recovery environment to decrypt volumes.

✕

KMS is highly available within the region; to make it span across multiple regions you have to connect primary and DR environments with a Direct Connect line.

Explanation

KMS has been a regional service for many years, and while can complicate the design of multi-region architecture, there are security benefits to the regional limitations.

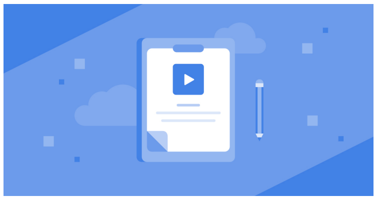
KMS has a multi-region key option, but region-specific keys cannot be converted to multi-region AND there are significantly more security issues to consider with using a multi-region key. The benefit it offers customers also expands the risk if the key is compromised or deleted, so something to keep in mind. AWS mentions it here:

You cannot convert an existing single-Region key to a multi-Region key. This design ensures that all data protected with existing single-Region keys maintain the same data residency and data sovereignty properties.

For most data security needs, the Regional isolation and fault tolerance of Regional resources make standard AWS KMS single-Region keys a best-fit solution. However, when you need to encrypt or sign data in client-side applications across multiple Regions, multi-Region keys might be the solution.

🔗/amazon-web-services/amazon-web-services-key-management-service-kms-course/key-management-service-basics.html

Covered in this lecture
Encryption Summary
Course:Designing Secure Applications and Architectures



10m

#49

Which other AWS service can you use to enable greater security of your CloudTrail log files?

✓

AWS Key Management Service (KMS)

✕

Amazon S3

✕

Amazon Simple Notification Service (SNS)

✕

Amazon CloudWatch

Explanation

The use of AWS KMS is an optional element of CloudTrail, but it allows additional encryption to be added to your Log files when stored on S3 http://docs.aws.amazon.com/kms/latest/developerguide/services-cloudtrail.html

Covered in this lecture
How does AWS CloudTrail work?
Course:AWS CloudTrail: An Introduction

6m

#50

You are a lead security engineer at a healthcare company. The Software Development team created a test environment to test out new features for HIPAA compliance. The team tested with production data and as such has been using customer-created encryption keys managed by the KMS service to encrypt the data on the EBS volumes associated with the test servers. After testing, the encryption keys for the test environment were no longer needed and were deleted when the test environment was terminated. Unfortunately, one of the KMS keys used to secure the test EBS volumes is also in use to encrypt the production EBS volume for a reporting application server used by the Finance department. Now that the KMS key has been deleted, which of the following solutions would allow for the data on the EBS volume to be decrypted for the reporting application?

✗

Create a new customer key using the KMS service and attach it to the existing EBS volume

✗

Use AWS Backup to recover the existing customer KMS key

✓

You cannot decrypt the data that was encrypted under the KMS customer key, and the data is not recoverable

✗

Make a request to AWS Support to recover the deleted customer KMS key

Explanation

After a KMS key is deleted, you can no longer decrypt the data that was encrypted under that KMS key, which means that the data becomes unrecoverable. You should delete a KMS key only when you are sure that you don't need to use it anymore.

The remaining choices are incorrect for the following reasons:

● Creating a new KMS key and associating that key with the existing EBS volume will not allow for the recovery of the encrypted data on the EBS volume. Once a KMS key is deleted it is irreversible.

● AWS Backup enables you to centralize and automate data backups across AWS services. This service is used to create backup plans for Amazon EC2 instances, Amazon EBS volumes, Amazon RDS databases, Amazon DynamoDB tables, Amazon Neptune databases, Amazon DocumentDB databases, Amazon EFS file systems, Amazon FSx for Lustre file systems, Amazon FSx for Windows File Server file systems, and AWS Storage Gateway volumes, not KMS keys.

● Deleting an AWS KMS key from AWS Key Management Service is destructive and potentially dangerous. It deletes the key material and all metadata associated with the KMS key and is irreversible. If you delete a KMS key, you can no longer decrypt the data that was encrypted with that KMS key, which means that the data becomes unrecoverable. AWS support cannot recover deleted KMS keys.

🔗https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys.html

#51

Which activity is performed by a CloudWatch alarm?

✗

Notifying an ELB to terminate an instance

✓

Sending notifications to a user using SNS

✗

Notifying an ELB to stop distributing traffic

✗

Generating metrics aggregates

Explanation

The CloudWatch alarms watch a single metric over a period of time and perform actions specified by the user when the metric crosses the threshold. It can perform actions, such as notifying SNS, sending message to Auto Scaling policy, etc.

🔗 http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/AlarmThatSendsEmail.html

#52

You can use AWS Trusted Advisor to monitor the configuration of your Amazon S3 buckets and ensure that ____ is enabled, which can be useful for performing security audits and tracking usage patterns in S3.

✗

restricted permissions

✓

bucket logging

✗

IAM user tracking

✗

CloudTrail sync

Explanation

AWS Trusted Advisor's S3 Bucket Logging Check monitors the logging configuration of Amazon S3 buckets. When server access logging is enabled, detailed access logs are delivered hourly to a bucket that you choose. An access log record contains details about each request, such as the request type, the resources specified in the request, and the time and date the request was processed. By default, bucket logging is not enabled; you should enable logging if you want to perform security audits or learn more about users and usage patterns.

🔗https://aws.amazon.com/premiumsupport/trustedadvisor/best-practices/

#53

Consider the following IAM Policy which is currently used by your custom Lambda function to write only messages to an SNS topic named funtimes: {"Version": "2012-10-17","Statement": [{"Effect": "Allow","Action": ["sns:*"],"Resource": "*"}]} You have a requirement to implement the rule of least privilege, and therefore need to refine the IAM policy above. What 2 edits do you perform on this policy? (Choose 2 answers)

✓

Update the existing Action array element from “sns:*” to “sns:Publish”

✓

Update the Resource attribute to: “arn:aws:sns:us-west-1:123456789012:funtimes”

✕

Add an additional entry “sns:Publish” to the Action array

✕

Change the Effect from Allow to Deny

Explanation

Answers ‘**Update the existing Action array element from “sns:*” to “sns:Publish”’** and ‘**Update the Resource attribute to: “arn:aws:sns:us-west-1:123456789012:funtimes”’** are correct. To establish the principle of least privilege the given answers lock the permissions down the most to just those required as per the stated requirements

https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege

#54

You are an information security manager for a music streaming company. Your company's application consists of: EC2 instances, including one running third-party tool SplunkS3 buckets that store music S3 buckets that store CloudTrail logs, encrypted with a KMS keyOne of your security engineers is attempting to review application log files (stored in S3) using Splunk which is currently installed and hosted on an Amazon EC2 instance. The security engineer is unable to access the logs in the S3 bucket via Splunk and receives an access denied error message. Which of the following solutions would resolve the access denied error message?

✕

Check that the KMS key associated with the S3 bucket is not disabled

✓

Check that the role the EC2 instance profile uses grants permission to decrypt objects using the KMS key and gives access to the S3 bucket and objects

✕

Check the KMS key policy and ensure the KMS administrator policy for the security engineer allows the engineer to perform the decrypt operation

✗

Check that the IAM role the security engineer uses for Splunk grants permission to decrypt objects using the KMS key

Explanation

An IAM role is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. You can use roles to delegate access to users, applications like Splunk, or services that don't normally have access to your AWS resources. IAM roles can be used to allow applications to use AWS resources when you do not want to embed AWS keys within the app. In order for Splunk to access the logs in the S3 bucket, the EC2 instance it is running on must have permission both to access the S3 bucket and have permission to decrypt objects using the KMS key.

The remaining choices are incorrect for the following reasons:

● A disabled KMS key will prevent the log files from being able to be decrypted but this would be due to an invalid key, not access denied permissions error.

● The KMS key policy must allow the requesting IAM identity to have the ability to perform the decryption operation in order to be able to use the KMS key to decrypt the objects in the S3 bucket. Granting the security engineer this access would only allow the IAM identity associated with the security engineer the appropriate access and not the Splunk application.

● The IAM role the security engineer uses for Splunk does need to have permissions to decrypt objects using the KMS key however, the role also will need to have access to the S3 bucket where the objects are being stored in order to successfully access the log files.

🔗https://docs.aws.amazon.com/kms/latest/APIReference/CommonErrors.html

#55

You've taken over management of your company's AWS cloud environment. You know very little about the environment and have been provided very little documentation. You have been given access to the environment and begin a discovery and documentation process. You begin by looking at the route table. Without seeing the specific route table, what information do you know it contains about the subnets in the VPC? (Choose 2 answers)

✓

Subnets that direct traffic to an Internet Gateway are public.

✗

The subnets region is indicated.

✗

The subnets availability zone is indicated.

✓

Subnets that do not direct traffic to an Internet Gateway are private.

Explanation

A route table contains a set of rules, called *routes*, that are used to determine where network traffic is directed.

Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table. When you add an Internet gateway, an egress-only Internet gateway, a virtual private gateway, a NAT device, a peering connection, or a VPC endpoint in your VPC, you must update the route table for any subnet that uses these gateways or connections.

🔗http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html

#56

In your AWS CloudHSM setup, you have combined three HSMs into a high availability cluster in a single VPC. Each HSM is configured within a separate subnet in a separate availability zone. Two of the HSMs go offline.When two of the HSMs go offline, will the service be maintained?

✓

Yes, because a single HSM can maintain service in this configuration.

✗

No, because all the three HSMs need to be online to maintain service.

✗

No, because you need at least two HSMs online to maintain service.

✗

Yes, but only if the HSMs are using RAID technology.

Explanation

When you implement CloudHSM, you will begin by creating a cluster. This cluster is simply a grouping of different HSMs which will act as a single unit when configured and deployed. Having multiple HSMs provides an element of high availability as you are able to select multiple different subnets, one from each availability zone that your VPC operates in, to deploy an HSM into.

Any requests to your CloudHSM cluster are then automatically load-balanced between the HSMs in the cluster, and if one HSM fails, AWS will automatically deploy another one within your cluster. As a result, running a VPC is a prerequisite of implementing your cluster.

🔗/course/get-started-with-aws-cloudhsm/cloudhsm-operations/
#57

What is Envelope Encryption in the context of Key Management Service (KMS)?

✕

It is the practice of encrypting the Master Key when exported from KMS to be used in another region or system.

✓

Two-tier hierarchy system to encrypt data with data key and then encrypt data key with master key.

✕

It is the practice of encrypting the Master Key when exported from on-premises appliance to be imported in KMS.

✕

It is the practice of encrypting data objects using Customer Master Key managed by KMS.

Explanation

Enveloper Encryption is a two-tier or multi-tier of encryption, it is the system by which data is encrypted using Data Keys and then those Keys are encrypted with Key Encryption Key. The same process could be applied multiple times if needed to encrypt the Key Encryption Key with another KEK, etc.

🔗/amazon-web-services/amazon-web-services-key-management-service-kms-course/key-management-service-basics.html
Covered in this lecture
Components of KMS
Course:How to Use KMS Key Encryption to Protect Your Data

11m

#58

When sending CloudTrail Logs to a CloudWatch Logs Group, which two CloudWatch APIs are called? (Choose 2 answers)

✓

CreateLogStream

✓

PutLogEvents

✗

PutMetricData

✗

DescribeAlarms

Explanation

1. When a log file is created by CloudTrail it is sent to your selected S3 bucket and your chosen CloudWatch Log Group (assuming your Trail has been configured for this feature)

2. To allow CloudTrail to deliver these logs to CloudWatch, CloudTrail must have the correct permissions, and these are gained by assuming a Role with the relevant permissions needed to run two CloudWatch APIs

    1. **CreateLogStream:** This enables CloudTrail to create a CloudWatch Logs log stream in the log group

    2. **PutLogEvents:** This allows CloudTrail to deliver CloudTrail events to the CloudWatch Logs log stream

3. CloudTrail then delivers logs to CloudWatch Logs.

http://docs.aws.amazon.com/awscloudtrail/latest/userguide/send-cloudtrail-events-to-cloudwatch-logs.html

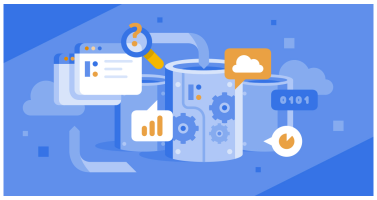
Covered in this lecture

Course Summary

Course:How to Implement & Enable Logging Across AWS Services (Part 1 of 2)

7m

#59



Which use cases would be best served by an S3 bucket ACL? (Choose 2 answers)

✗

Hosting databases

✓

Enabling bucket logging

✗

Ensuring PCI compliant data

✓

Making a bucket world readable for static web hosting

Explanation

S3 bucket access control lists are a legacy access control mechanism, created before IAM existed. S3 bucket ACLs are best used for a limited set of use cases.

http://docs.aws.amazon.com/AmazonS3/latest/dev/S3_ACLs_UsingACLs.html

#60

Your CTO has asked you to set up the manager account of a Cloud HSM environment. How do you install the SSH key that will be used to authenticate the manager account when logging in to a CloudHSM appliance?

✓

The public key is installed on the HSM appliance during provisioning

✗

The private key is installed on the HSM appliance during provisioning.

✗

The public key is copied to each HSM appliance during provisioning.

✗

The private key is supplied to AWS before HSM appliance provisioning.

Explanation

AWS CloudHSM uses an SSH key pair to authenticate the manager account when logging in to the appliance. The public key is installed on the HSM appliance during provisioning, while the private key must be available to any instance you use to connect to the HSM appliance. You can generate the key pair on any machine, but you need to copy the private key to any instances that will be used to connect to the HSM appliance.

🔗http://docs.aws.amazon.com/cloudhsm/latest/userguide/generate_ssh_key.html
#61

You've previously configured two IAM policies, Policy1 and Policy2. Policy 1 has a source IP restriction for 192.168.10.11 and allows access to S3 bucket xyz-bucket. Policy 2 has a date after May 1, 2018 restriction and denies access to the S3 bucket xyz-bucket. A user is attempting to access the S3 bucket xyz-bucket from IP address 192.168.10.11 on May 2, 2018. Which statement is correct regarding this scenario?

✕
The user will be granted access due to an explicit allow rule

✓
The user will not be granted access due to an explicit deny rule

✕
The user will not be granted access due to a default deny rule

✕
The user will be granted access due to a default allow rule

Explanation

Answer "**The user will not be granted access due to an explicit deny rule**" is correct. The distinction between a request being denied by default and an explicit deny in a policy is important. By default, a request is denied, but this can be overridden by an allow. In contrast, if a policy explicitly denies a request, that deny can't be overridden.

🔗https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html#AccessPolicyLanguage_Interplay
#62

This month, your company hired a 3rd party company to ensure the compliance of the organization’s data to HIPAA standards in preparation for an upcoming audit. The 3rd party company will be reviewing controls for both on-premise and cloud resources and as a result, they will need access to the S3 buckets accessing the financial statements and billing reports. You have been called in to create the necessary permissions to allow access to the S3 buckets. Upon editing the existing policy on the buckets using the console, you are getting the error: “Invalid principal in policy”Which of the following could be a cause for the error message? (Choose Two)

✗

The S3 ARN specified is incorrectly formatted

✓

The IAM user or role specified has been deleted

✗

The Principle S3 Bucket name specified is incorrect

✓

The value for Principal is an unsupported type

Explanation

You receive the "Error: Invalid principal in policy" message when the value of a Principal in your bucket policy is not valid. The Principal element in a resource-based JSON policy is used to specify the principal or who or what is allowed or denied access to a resource. To resolve this error, confirm your bucket policy uses supported values for a Principal element, the Principal value is formatted correctly and If the Principal is an AWS Identity and Access Management (IAM) user or role, then confirm that the user or role wasn't deleted.

The remaining choices are incorrect for the following reasons:

● Amazon S3 is a resource in the JSON policy. The Resource element specifies the object or objects that the statement covers. Statements must include either a Resource or a NotResource element. You specify a resource using an ARN. If the S3 ARN was incorrectly formatted or the S3 Bucket name specified is incorrect the invalid principal error message would not be generated.

🔗https://aws.amazon.com/premiumsupport/knowledge-center/s3-invalid-principal-in-policy-error/
#63

Which of the following infrastructure security solutions will provide a dedicated, secure link from your company network to Amazon’s and allow for the migration of local application data to Amazon S3?

✗
Set up the AWS Application Migration Service to establish a secure, dedicated connection to Amazon, upload the data to Amazon S3.

✗
Enable AWS Snowball to establish a secure, dedicated connection to Amazon, upload the data to AWS Snowball for transfer to Amazon S3.

✓
Create a Direct Connect connection to provide a dedicated, secure link from the company network to Amazon’s and allow for the migration of application data to Amazon S3.

✗
Create a task in AWS DataSync to establish a secure, dedicated connection to Amazon, upload the data to Amazon S3.

Explanation

AWS Direct Connect can be used to link your internal network to an AWS Direct Connect location over a standard Ethernet fiber-optic cable. With this connection, you can create virtual interfaces directly to securely access public AWS services like Amazon S3 to upload your data while bypassing internet service providers in your network path. An AWS Direct Connect location provides access to AWS in the region with which it is associated.

The remaining choices are incorrect for the following reasons:

● AWS Application Migration Service allows you to migrate your virtual, physical, or cloud-based servers to AWS. With this service you can install the AWS Replication Agent on your source servers and AWS Application Migration Service will replicate the entire server including the operating system, applications, data and configurations. This service is not used to establish a secure, dedicated connection to Amazon and upload the data to Amazon S3.

● AWS Snowball is a petabyte-scale data transport service that uses secure physical devices to transfer large amounts of data into and out of the AWS Cloud. While AWS Snowball can be used to move large volumes of data over to AWS, it does this by use of an appliance and is not used to establish a secure, dedicated connection to Amazon.

● AWS DataSync is primarily used as an online data transfer service that automates, and accelerates moving data between on-premises storage systems and AWS Storage services, as well as between AWS Storage services. AWS DataSync is not used to establish a secure, dedicated connection to Amazon and upload the data to Amazon S3.

🔗https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

#64

You are a security engineer at a FinTech company that has just updated its application architecture to incorporate a multi-regional architecture for disaster recovery purposes. Currently, the wealth management application resides on a cluster of EC2 instances that have been replicated in the US Virginia and US Northern California regions. Now that the application has moved to a multi-regional architecture, you need to set up a way to have centralized logging of API activity across all of the AWS resources in both regions. Which of the following logging solutions would allow for centralized logging while capturing the necessary API activity for all of the resources in both regions?

✗

Turn on AWS Config for both regions to track and log API activity for all resources to CloudWatch Logs.

✗

Create a CloudTrail trail in both regions and send the CloudTrail information to a single S3 bucket.

✗

Enable AWS Control Tower for both regions to track API activity, and configure Control Tower to send API information to CloudWatch Logs.

✓

Create a single CloudTrail trail for both regions and send the CloudTrail information to a single S3 bucket.

Explanation

The remaining choices are incorrect for the following reasons:

- AWS Config is primarily used to audit the configurations of your AWS resources. AWS Config can assist with security monitoring by alerting you to when security-related resources such as security groups and IAM credentials have had changes to the baseline configurations. AWS Config does not give visibility into the API activity of the resources in question but is used to audit configuration changes deviating from baseline configurations or defined compliance rules.
- AWS CloudTrail is the service that can track API activity for your AWS resources. CloudTrail logs events from all regions in your account. When logging information for both regions, 2 separate CloudTrail trails per region are not required.
- AWS Control Tower is primarily used to provide a way to easily set up and govern a secure, multi-account AWS environment. AWS Control Tower does not track API activity for AWS resources but will help automate the setup of your multi-account AWS environment. The setup employs blueprints, which capture AWS best practices for configuring AWS security and management services to govern your environment.

🔗https://docs.aws.amazon.com/awscloudtrail/latest/userguide/receive-cloudtrail-log-files-from-multiple-regions.html
#65

You are a security architect for a company running a three-tier web application running on a cluster of EC2 instances spread across multiple availability zones in the US Virginia region.The application also has a Microsoft SQL Server backend RDS database used for calculating and storing rate information. The Webserver makes frequent read requests to the database to retrieve rate information for the application. Currently, the application has database credentials embedded into the application. A new security mandate is requiring that this design is done away with and that all passwords can no longer be exposed in the application code. You need to architect a solution that will allow the Web Server to access the database server without passing the exposed passwords directly. The new solution must prevent the use of embedded passwords and allow for automatic password rotation of the database password every 30 days. Which of the following solutions would allow the Web Server to access the database while allowing for automatic rotation of the database password?

✕

Set up an IAM Role for the EC2 instance, enable IAM role rotation every 30 days

✕

Associate a KMS Key with the RDS database, enable automatic key rotation every 30 days

✓

Set up AWS Secrets Manager for the RDS database password, enable secret rotation every 30 days.

✕

Create an RDS Database instance identifier for the EC2 instance to connect to prevent the need to exchange the database password, set up AWS Systems Manager to automatically create a new database alias every 30 days.

Explanation

AWS Secrets Manager can be used to help you protect secrets needed to access your applications, services, and IT resources. The service enables you to rotate, manage, and retrieve database credentials, API keys, and other secrets. Users and applications retrieve secrets with a call to Secrets Manager APIs, which eliminates the need to hardcode sensitive information in plain text. Secrets Manager offers secret rotation with built-in integration for Amazon RDS, Amazon Redshift, and Amazon DocumentDB.

The remaining choices are incorrect for the following reasons:

● An IAM role is an IAM identity that you can create in your account that has specific permissions. IAM roles can be used to allow applications to use AWS resources when you do not want to embed AWS keys within the app. IAM roles cannot be rotated every 30 days.

● AWS KMS keys are used to provide encryption at rest for AWS data services like Amazon RDS. When automatic rotation is enabled, Amazon will rotate the KMS keys once a year. These KMS keys are not used for database authentication only to protect the RDS data at rest.

● An RDS database instance identifier is a customer-supplied name that uniquely identifies the DB instance when interacting with the Amazon RDS API and AWS CLI commands. The DB instance identifier must be unique in an AWS Region. Each DB instance has a DB instance identifier and these identifiers do not facilitate secure connectivity from EC2 to RDS databases. There is no rotation for database instance identifiers.

https://aws.amazon.com/secrets-manager/