1.

The Security team believes that a former employee may have gained unauthorized access to AWS resources sometime in the past 3 months by using an identified access key.

What approach would enable the Security team to find out what the former employee may have done within AWS?

A. Use the AWS CloudTrail console to search for user activity.

B. Use the Amazon CloudWatch Logs console to filter CloudTrail data by user.

C. Use AWS Config to see what actions were taken by the user.

D. Use Amazon Athena to query CloudTrail logs stored in Amazon S3.

A. Use the AWS CloudTrail event history to identify AWS API activity in the last 90 days for your IAM access key.

ref- https://aws.amazon.com/premiumsupport/knowledge-center/cloudtrail-search-for-activity/

Question #2

The Security Engineer implemented a new vault lock policy for 10TB of data and called initiate-vault-lock 12 hours ago.

The Audit team identified a typo that is allowing incorrect access to the vault.

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

A. Call the abort-vault-lock operation, fix the typo, and call the initiate-vault-lock again.

B. Copy the vault data to Amazon S3, delete the vault, and create a new vault with the data.

C. Update the policy, keeping the vault lock in place.

D. Update the policy and call initiate-vault-lock again to apply the new policy.

Correct is A

abort-vault-lock is a AWS-CLI S3 command

This command aborts the vault locking process if the vault lock is not in the Locked state

However, it returns an AccessDenied error if the vault is on Locked state,

InitiateVaultLock is a AWS-CLI S3 command

this command change the state of tha vault-lock to "InProgress"

CompleteVaultLock is a AWS-CLI S3 command

this command change the state of tha vault-lock to "Locked"

https://docs.aws.amazon.com/cli/latest/reference/glacier/abort-vault-lock.html

Question #3

A company wants to control access to its AWS resources by using identities and groups that are defined in its existing Microsoft Active Directory.

What must the company create in its AWS account to map permissions for AWS services to Active Directory user attributes?

A. AWS IAM groups

B. AWS IAM users

C. AWS IAM roles

D. AWS IAM access keys

Correct is C

Prerequisites to establish Federation Services in AWS

- You have a working AD directory and AD FS server.

- You have created an identity provider (IdP) in your AWS account using your XML file from your AD FS server. Remember the name of your IdP because you will use it later in this solution.

-You have created the appropriate IAM roles in your AWS account, which will be used for federated access.

https://aws.amazon.com/blogs/security/how-to-establish-federated-access-to-your-aws-resources-by-using-active-directory-user-attributes/

Question #4Topic 1

A company has contracted with a third party to audit several AWS accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.

Which of the following may be causing this problem? (Choose three.)

A. The external ID used by the Auditor is missing or incorrect.

B. The Auditor is using the incorrect password.

C. The Auditor has not been granted sts:AssumeRole for the role in the destination account.

D. The Amazon EC2 role used by the Auditor must be set to the destination account role.

E. The secret key used by the Auditor is missing or incorrect.

F. The role ARN used by the Auditor is missing or incorrect.

Correct is A, C and F

Using IAM to grant access to a Third-Party Account

1) Create a role to provide access to the require resources

1.1) Create a role policy that specifies the AWS Account ID to be accessed, "sts:AssumeRole" as

action, and "sts:ExternalID" as condition

1.2) Create a role using the role policy just created

1.3) Assign a resouce policy to the role. This will provide permission to access resource ARNs to

the auditor

2) Repeat steps 1 and 2 on all AWS accounts

3) The auditor connects to the AWS account AWS Security Token Service (STS). The auditor must

provide its ExternalID from step 1.2, the ARN of the role he is trying to assume from step 1.3,

sts:ExternalID

4) STS provide the auditor with temporary credentials that provides the role access from step 1

https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_roles\_create\_for-user\_externalid.html

https://aws.amazon.com/blogs/security/how-to-audit-cross-account-roles-using-aws-cloudtrail-and-amazon-cloudwatch-events/

Question #5Topic 1

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

Which of the following solutions will meet these requirements?

A. Offload SSL termination onto an SSL listener on a Classic Load Balancer, and use a TCP connection between the load balancer and the EC2 instances.

B. Route all traffic throughout a TCP listener on a Classic Load Balancer, and terminate the TLS connection on the EC2 instances.

C. Create an HTTPS listener using an Application Load Balancer, and route all of the communication through that load balancer.

D. Offload SSL termination onto an SSL listener using an Application Load Balancer, and re-spawn and SSL connection between the load balancer and the EC2 instances.

Agreed, B is correct.

Data must be encrypted in transit. That should imply end-to-end encryption. So TLS must be terminated at EC2 instance only.

Question #6Topic 1

An application is currently secured using network access control lists and security groups. Web servers are located in public subnets behind an Application Load

Balancer (ALB); application servers are located in private subnets.

How can edge security be enhanced to safeguard the Amazon EC2 instances against attack? (Choose two.)

A. Configure the application's EC2 instances to use NAT gateways for all inbound traffic.

B. Move the web servers to private subnets without public IP addresses.

C. Configure AWS WAF to provide DDoS attack protection for the ALB.

D. Require all inbound network traffic to route through a bastion host in the private subnet.

E. Require all inbound and outbound network traffic to route through an AWS Direct Connect connection.

Agreed. Correct is B and C

A is incorrect. Nat gateways is for outbound only trafffc

D is incorrect. Bastion host is mostly for incoming SSH/FTP connections and it must be placed on a public subnet

E is incorrect. AWS Direct connect is used to connect your on-premisse datacenter to AWS

Question #7Topic 1

A Security Administrator is restricting the capabilities of company root user accounts. The company uses AWS Organizations and has enabled it for all feature sets, including consolidated billing. The top-level account is used for billing and administrative purposes, not for operational AWS resource purposes.

How can the Administrator restrict usage of member root user accounts across the organization?

A. Disable the use of the root user account at the organizational root. Enable multi-factor authentication of the root user account for each organizational member account.

B. Configure IAM user policies to restrict root account capabilities for each Organizations member account.

C. Create an organizational unit (OU) in Organizations with a service control policy that controls usage of the root user. Add all operational accounts to the new OU.

D. Configure AWS CloudTrail to integrate with Amazon CloudWatch Logs and then create a metric filter for RootAccountUsage.

Correct is C

A is incorrect. organization root includes every user/group account in every account

B is incorrect. Correct, may be a Identity-based policy applied to the root user on each account

D is incorrect. This will not modify user's access or permission

Applying a "Control Policy" in your organization. A policy applied to:

1) root applies to all accounts in the organization

2) OU applies to all accounts in the OU and to any child OUs

3) account applies to one account only

Note- this requires that

Acquirements:

-all features are enabled for the organization in AWS Organizations

-Only service control policy (SCP) are supported

https://docs.aws.amazon.com/organizations/latest/userguide/orgs\_manage\_policies.html

Question #8Topic 1

A Systems Engineer has been tasked with configuring outbound mail through Simple Email Service (SES) and requires compliance with current TLS standards.

The mail application should be configured to connect to which of the following endpoints and corresponding ports?

A. email.us-east-1.amazonaws.com over port 8080

B. email-pop3.us-east-1.amazonaws.com over port 995

C. email-smtp.us-east-1.amazonaws.com over port 587

D. email-imap.us-east-1.amazonaws.com over port 993

C PORT 587

Question #9Topic 1

A threat assessment has identified a risk whereby an internal employee could exfiltrate sensitive data from production host running inside AWS (Account 1). The threat was documented as follows:

Server X has outbound internet access configured via a proxy server. Legitimate access to S3 is required so that the application can upload encrypted files to an

S3 bucket. Server X is currently using an IAM instance role. The proxy server is not able to inspect any of the server communication due to TLS encryption.

Which of the following options will mitigate the threat? (Choose two.)

A. Bypass the proxy and use an S3 VPC endpoint with a policy that whitelists only certain S3 buckets within Account 1.

B. Block outbound access to public S3 endpoints on the proxy server.

C. Configure Network ACLs on Server X to deny access to S3 endpoints.

D. Modify the S3 bucket policy for the legitimate bucket to allow access only from the public IP addresses associated with the application server.

E. Remove the IAM instance role from the application server and save API access keys in a trusted and encrypted application config file.

correction to my previous post.

Correct is A and B

in answer A we implement a private connection between ServerX and the S3 bucket

in answer B we block the existing public access between ServerX and the S3 bucket

Both should work. However, we are dealing from and internal employee. So correct answer should be resign and get another job.

Question #10Topic 1

A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of "Sensitive," "Confidential," and "Restricted." The security solution must meet all of the following requirements:

✑ Each object must be encrypted using a unique key.

✑ Items that are stored in the "Restricted" bucket require two-factor authentication for decryption.

✑ AWS KMS must automatically rotate encryption keys annually.

Which of the following meets these requirements?

A. Create a Customer Master Key (CMK) for each data classification type, and enable the rotation of it annually. For the "Restricted" CMK, define the MFA policy within the key policy. Use S3 SSE-KMS to encrypt the objects.

B. Create a CMK grant for each data classification type with EnableKeyRotation and MultiFactorAuthPresent set to true. S3 can then use the grants to encrypt each object with a unique CMK.

C. Create a CMK for each data classification type, and within the CMK policy, enable rotation of it annually, and define the MFA policy. S3 can then create DEK grants to uniquely encrypt each object within the S3 bucket.

D. Create a CMK with unique imported key material for each data classification type, and rotate them annually. For the "Restricted" key material, define the MFA policy in the key policy. Use S3 SSE-KMS to encrypt the objects.

A is Correct

Question #11Topic 1

An organization wants to deploy a three-tier web application whereby the application servers run on Amazon EC2 instances. These EC2 instances need access to credentials that they will use to authenticate their SQL connections to an Amazon RDS DB instance. Also, AWS Lambda functions must issue queries to the RDS database by using the same database credentials.

The credentials must be stored so that the EC2 instances and the Lambda functions can access them. No other access is allowed. The access logs must record when the credentials were accessed and by whom.

What should the Security Engineer do to meet these requirements?

A. Store the database credentials in AWS Key Management Service (AWS KMS). Create an IAM role with access to AWS KMS by using the EC2 and Lambda service principals in the role's trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances. Set up Lambda to use the new role for execution.

B. Store the database credentials in AWS KMS. Create an IAM role with access to KMS by using the EC2 and Lambda service principals in the role's trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances and the Lambda function.

C. Store the database credentials in AWS Secrets Manager. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role's trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances and the Lambda function.

D. Store the database credentials in AWS Secrets Manager. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role's trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances. Set up Lambda to use the new role for execution.

D for sure correct . A & B are wrong because you do not store credentials in AWS-KMS . C is wrong because you do not attach EC2 instance profile to lamda function, you attach only to EC2 instance.

Question #12Topic 1

A company has a customer master key (CMK) with imported key materials. Company policy requires that all encryption keys must be rotated every year.

What can be done to implement the above policy?

A. Enable automatic key rotation annually for the CMK.

B. Use AWS Command Line interface to create an AWS Lambda function to rotate the existing CMK annually.

C. Import new key material to the existing CMK and manually rotate the CMK.

D. Create a new CMK, import new key material to it, and point the key alias to the new CMK.

D is correct for me

Question #13Topic 1

A water utility company uses a number of Amazon EC2 instances to manage updates to a fleet of 2,000 Internet of Things (IoT) field devices that monitor water quality. These devices each have unique access credentials.

An operational safety policy requires that access to specific credentials is independently auditable.

What is the MOST cost-effective way to manage the storage of credentials?

A. Use AWS Systems Manager to store the credentials as Secure Strings Parameters. Secure by using an AWS KMS key.

B. Use AWS Key Management System to store a master key, which is used to encrypt the credentials. The encrypted credentials are stored in an Amazon RDS instance.

C. Use AWS Secrets Manager to store the credentials.

D. Store the credentials in a JSON file on Amazon S3 with server-side encryption.

A is correct!

A secure string parameter is any sensitive data that needs to be stored and referenced in a secure manner. If you have data that you don't want users to alter or reference in plain text, such as passwords or license keys, create those parameters using the SecureString datatype. For the following scenarios-

You want to use data/parameters across AWS services without exposing the values as plain text in commands, functions, agent logs, or AWS CloudTrail logs.

You want to control who has access to sensitive data.

You want to be able to audit when sensitive data is accessed (AWS CloudTrail).

You want to encrypt your sensitive data and you want to bring your own encryption keys to manage access.

\*\*Most Cost-Effective Way\*\*

Question #14Topic 1

An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing.

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

A. Use an EC2 run command to confirm that the "awslogs" service is running on all instances.

B. Verify that the permissions used by the agent allow creation of log groups/streams and to put log events.

C. Check whether any application log entries were rejected because of invalid time stamps by reviewing /var/cwlogs/rejects.log.

D. Check that the trust relationship grants the service "cwlogs.amazonaws.com" permission to write objects to the Amazon S3 staging bucket.

E. Verify that the time zone on the application servers is in UTC.

A. INCORRECT: Service Manager has RunCommand, not EC2. Also, agent configuration files have been checked and found configured correctly.

B. CORRECT : permission used by agent creation of log groups/streams and to

C: CORRECT. Logging from specific instances is missing - here logging refers to application log files /var/cwlogs/rejects.log, not awslogs.

D. INCORRECT: No trust relation is required.

E. It has nothing to do with server's time zone

Question #15Topic 1

A Security Engineer must design a solution that enables the incident Response team to audit for changes to a user's IAM permissions in the case of a security incident.

How can this be accomplished?

A. Use AWS Config to review the IAM policy assigned to users before and after the incident.

B. Run the GenerateCredentialReport via the AWS CLI, and copy the output to Amazon S3 daily for auditing purposes.

C. Copy AWS CloudFormation templates to S3, and audit for changes from the template.

D. Use Amazon EC2 Systems Manager to deploy images, and review AWS CloudTrail logs for changes.

Agreed. Answer is A. However, this will require the admin to first create an AWS config rule to record the IAM use changes. AWS config will not record those changes by default. https://aws.amazon.com/blogs/security/how-to-record-and-govern-your-iam-resource-configurations-using-aws-config/

Question #16Topic 1

A company has complex connectivity rules governing ingress, egress, and communications between Amazon EC2 instances. The rules are so complex that they cannot be implemented within the limits of the maximum number of security groups and network access control lists (network ACLs).

What mechanism will allow the company to implement all required network rules without incurring additional cost?

A. Configure AWS WAF rules to implement the required rules.

B. Use the operating system built-in, host-based firewall to implement the required rules.

C. Use a NAT gateway to control ingress and egress according to the requirements.

D. Launch an EC2-based firewall product from the AWS Marketplace, and implement the required rules in that product.

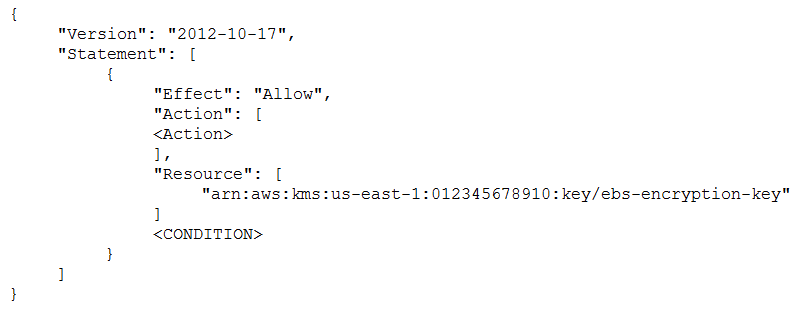
B = without incurring additional cost

Question #17Topic 1 (그림넣기)

An IAM user with fill EC2 permissions could bot start an Amazon EC2 instance after it was stopped for a maintenance task. Upon starting the instance, the instance state would change to "Pending", but after a few seconds, it would switch back to "Stopped".

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

The IAM user policy is as follows:



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

A. kms:GenerateDataKey

B. kms:Decrypt

C. kms:CreateGrant

D. "Condition": { "Bool": { "kms:ViaService": "ec2.us-west-2.amazonaws.com" } }

E. "Condition": { "Bool": { "kms:GrantIsForAWSResource": true } }

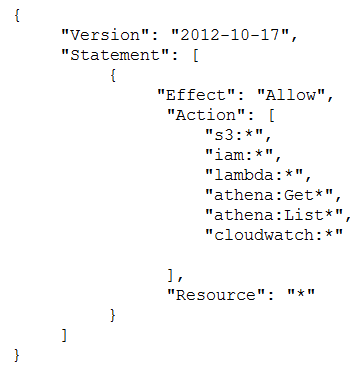
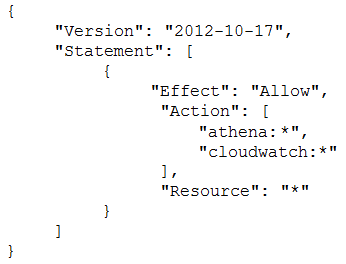
Question #18*Topic 1*

A Security Administrator has a website hosted in Amazon S3. The Administrator has been given the following requirements:  
✑ Users may access the website by using an Amazon CloudFront distribution.  
✑ Users may not access the website directly by using an Amazon S3 URL.  
Which configurations will support these requirements? (Choose two.)

* A. Associate an origin access identity with the CloudFront distribution.
* B. Implement a "Principal": "cloudfront.amazonaws.com" condition in the S3 bucket policy.
* C. Modify the S3 bucket permissions so that only the origin access identity can access the bucket contents.
* D. Implement security groups so that the S3 bucket can be accessed only by using the intended CloudFront distribution.
* E. Configure the S3 bucket policy so that it is accessible only through VPC endpoints, and place the CloudFront distribution into the specified VPC.

AC B: This does not restrict it just say this policy applies to cloudfront. Too little information to say if this is the answer ot not. D: S3 does not use security groups. E: No way to put Cloudfront into VPC.

Question #19*Topic 1*

A Security Engineer has created an Amazon CloudWatch event that invokes an AWS Lambda function daily. The Lambda function runs an Amazon Athena query that checks AWS CloudTrail logs in Amazon S3 to detect whether any IAM user accounts or credentials have been created in the past 30 days. The results of the  
Athena query are created in the same S3 bucket. The Engineer runs a test execution of the Lambda function via the AWS Console, and the function runs successfully.  
After several minutes, the Engineer finds that his Athena query has failed with the error message: "Insufficient Permissions". The IAM permissions of the Security  
Engineer and the Lambda function are shown below:  
  
Security Engineer -  
  
  
Lambda function execution role -  
  
What is causing the error?

* A. The Lambda function does not have permissions to start the Athena query execution.
* B. The Security Engineer does not have permissions to start the Athena query execution.
* C. The Athena service does not support invocation through Lambda.
* D. The Lambda function does not have permissions to access the CloudTrail S3 bucket.

D is Correct!

Question #20*Topic 1*

A company requires that IP packet data be inspected for invalid or malicious content.  
Which of the following approaches achieve this requirement? (Choose two.)

* A. Configure a proxy solution on Amazon EC2 and route all outbound VPC traffic through it. Perform inspection within proxy software on the EC2 instance.
* B. Configure the host-based agent on each EC2 instance within the VPC. Perform inspection within the host-based agent.
* C. Enable VPC Flow Logs for all subnets in the VPC. Perform inspection from the Flow Log data within Amazon CloudWatch Logs.
* D. Configure Elastic Load Balancing (ELB) access logs. Perform inspection from the log data within the ELB access log files.
* E. Configure the CloudWatch Logs agent on each EC2 instance within the VPC. Perform inspection from the log data within CloudWatch Logs.

Yes, A and B

Question #21*Topic 1*

An organization has a system in AWS that allows a large number of remote workers to submit data files. File sizes vary from a few kilobytes to several megabytes.  
A recent audit highlighted a concern that data files are not encrypted while in transit over untrusted networks.  
Which solution would remediate the audit finding while minimizing the effort required?

* A. Upload an SSL certificate to IAM, and configure Amazon CloudFront with the passphrase for the private key.
* B. Call KMS.Encrypt() in the client, passing in the data file contents, and call KMS.Decrypt() server-side.
* C. Use AWS Certificate Manager to provision a certificate on an Elastic Load Balancing in front of the web service's servers.
* D. Create a new VPC with an Amazon VPC VPN endpoint, and update the web service's DNS record.

A is incorrect. You can upload a SSL Certificate to a IAM. But when setting the cert up on cloundfront you will use the Cert path (a paraphrase if any will have to be provided bhy the client) https://aws.amazon.com/premiumsupport/knowledge-center/import-ssl-certificate-to-iam/ B is incorrect. This option will required a script or a change in the app code. KMS.Encrypt() is a function from the aws-sdk that can be used inside your code. KMS.Encrypt() and KMS.Dencrypt() are used on the client's side. C is correct. D may wotk but will required more effort than C

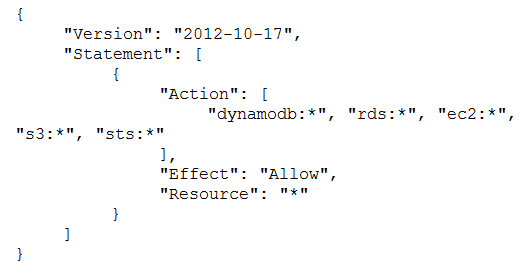
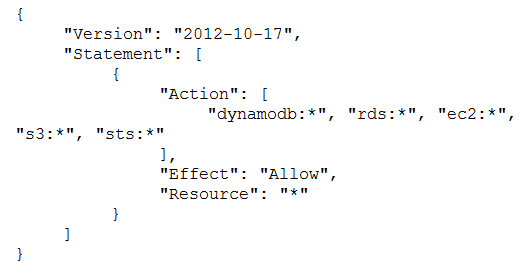
Question #22*Topic 1*

Which option for the use of the AWS Key Management Service (KMS) supports key management best practices that focus on minimizing the potential scope of data exposed by a possible future key compromise?

* A. Use KMS automatic key rotation to replace the master key, and use this new master key for future encryption operations without re-encrypting previously encrypted data.
* B. Generate a new Customer Master Key (CMK), re-encrypt all existing data with the new CMK, and use it for all future encryption operations.
* C. Change the CMK alias every 90 days, and update key-calling applications with the new key alias.
* D. Change the CMK permissions to ensure that individuals who can provision keys are not the same individuals who can use the keys.

A is the best answer I see here: https://aws.amazon.com/kms/faqs/ Q: Do I have to re-encrypt my data after keys in AWS KMS are rotated? If you choose to have AWS KMS automatically rotate keys, you don’t have to re-encrypt your data. AWS KMS automatically keeps previous versions of keys to use for decryption of data encrypted under an old version of a key. All new encryption requests against a key in AWS KMS are encrypted under the newest version of the key. If you manually rotate your imported or custom key store keys, you may have to re-encrypt your data depending on whether you decide to keep old versions of keys available.

A Security Engineer must enforce the use of only Amazon EC2, Amazon S3, Amazon RDS, Amazon DynamoDB, and AWS STS in specific accounts.  
What is a scalable and efficient approach to meet this requirement?

* A. Set up an AWS Organizations hierarchy, and replace the FullAWSAccess policy with the following Service Control Policy for the governed organization units: 
* B. Create multiple IAM users for the regulated accounts, and attach the following policy statement to restrict services as required: 
* C. Set up an Organizations hierarchy, replace the global FullAWSAccess with the following Service Control Policy at the top level: 
* D. Set up all users in the Active Directory for federated access to all accounts in the company. Associate Active Directory groups with IAM groups, and attach the following policy statement to restrict services as required: 

A is correct, as what is the questions Engineer can use only Amazon EC2, Amazon S3, Amazon RDS, Amazon DynamoDB, and AWS STS in specific accounts 1) policy should have "allow" for the above services. 2) and in specific accounts means it should be for governed organization units.

Question #24*Topic 1*

A company's database developer has just migrated an Amazon RDS database credential to be stored and managed by AWS Secrets Manager. The developer has also enabled rotation of the credential within the Secrets Manager console and set the rotation to change every 30 days.  
After a short period of time, a number of existing applications have failed with authentication errors.  
What is the MOST likely cause of the authentication errors?

* A. Migrating the credential to RDS requires that all access come through requests to the Secrets Manager.
* B. Enabling rotation in Secrets Manager causes the secret to rotate immediately and the applications are using the earlier credential.
* C. The Secrets Manager IAM policy does not allow access to the RDS database.
* D. The Secrets Manager IAM policy does not allow access for the applications.

Answer B. Because enabling the rotation, would immediately change the credentials, and that would cause the applications to fail if they uses the imbedded/old credentials.

Question #25*Topic 1*

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

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

Instances have outbound access to the internet. So the question is about ingress access. A is incorrect. It also requres -1, -1. -1 rule. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules-reference.html#sg-rules-other-instances B is incorrect. We need am ingress rule C is incorrect. D is correct.

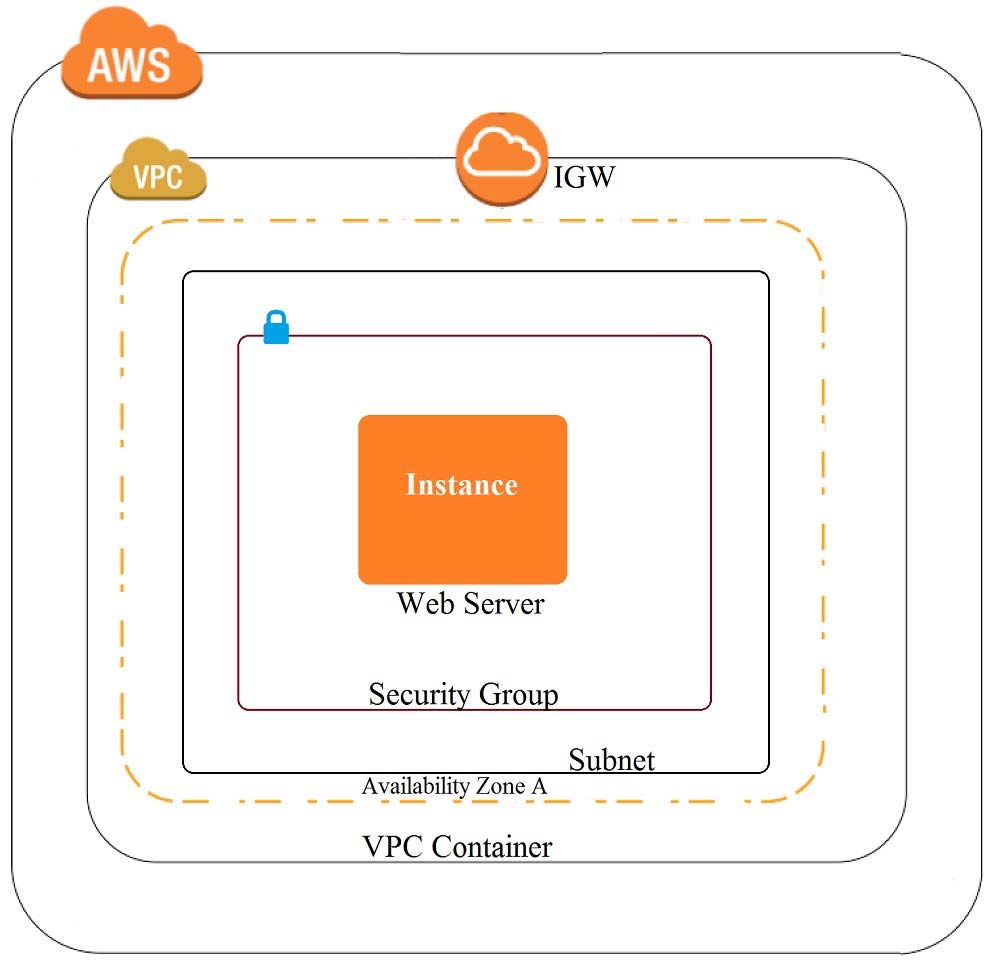
Question #26*Topic 1*

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

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

Answer is D WAF: AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. VPC Flow logs cannot get the URL: VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

Question #27*Topic 1*

A company recently experienced a DDoS attack that prevented its web server from serving content. The website is static and hosts only HTML, CSS, and PDF files that users download.  
Based on the architecture shown in the image, what is the BEST way to protect the site against future attacks while minimizing the ongoing operational overhead?  


* A. Move all the files to an Amazon S3 bucket. Have the web server serve the files from the S3 bucket.
* B. Launch a second Amazon EC2 instance in a new subnet. Launch an Application Load Balancer in front of both instances.
* C. Launch an Application Load Balancer in front of the EC2 instance. Create an Amazon CloudFront distribution in front of the Application Load Balancer.
* D. Move all the files to an Amazon S3 bucket. Create a CloudFront distribution in front of the bucket and terminate the web server.

D.. what is the BEST way to protect the site against future attacks.. With Cloudfront

Question #28*Topic 1*

The Information Technology department has stopped using Classic Load Balancers and switched to Application Load Balancers to save costs. After the switch, some users on older devices are no longer able to connect to the website.  
What is causing this situation?

* A. Application Load Balancers do not support older web browsers.
* B. The Perfect Forward Secrecy settings are not configured correctly.
* C. The intermediate certificate is installed within the Application Load Balancer.
* D. The cipher suites on the Application Load Balancers are blocking connections.

Answer should be D. Classic load balancers support some of the legacy cipher suites. Given that some of the users are having problems could mean that legacy cipher suites have been deprecated in ALBs.

Question #29*Topic 1*

A security team is responsible for reviewing AWS API call activity in the cloud environment for security violations. These events must be recorded and retained in a centralized location for both current and future AWS regions.  
What is the SIMPLEST way to meet these requirements?

* A. Enable AWS Trusted Advisor security checks in the AWS Console, and report all security incidents for all regions.
* B. Enable AWS CloudTrail by creating individual trails for each region, and specify a single Amazon S3 bucket to receive log files for later analysis.
* C. Enable AWS CloudTrail by creating a new trail and applying the trail to all regions. Specify a single Amazon S3 bucket as the storage location.
* D. Enable Amazon CloudWatch logging for all AWS services across all regions, and aggregate them to a single Amazon S3 bucket for later analysis.

The referenced link does not prove req that futre regions must be taken into account. With C future regions req is satisfied.

Question #30*Topic 1*

A Security Administrator is performing a log analysis as a result of a suspected AWS account compromise. The Administrator wants to analyze suspicious AWS  
CloudTrail log files but is overwhelmed by the volume of audit logs being generated.  
What approach enables the Administrator to search through the logs MOST efficiently?

* A. Implement a "write-only" CloudTrail event filter to detect any modifications to the AWS account resources.
* B. Configure Amazon Macie to classify and discover sensitive data in the Amazon S3 bucket that contains the CloudTrail audit logs.
* C. Configure Amazon Athena to read from the CloudTrail S3 bucket and query the logs to examine account activities.
* D. Enable Amazon S3 event notifications to trigger an AWS Lambda function that sends an email alarm when there are new CloudTrail API entries.

C is the correct answer since it asks how to search the logs most efficiently and the only way to search and analyze huge logs is using Athena queries on S3. A is wrong because you can create a trail with write-only managment and data events upon creation of the trail and this has nothing to do with searching exisitng huge number of logs in an efficient way.

Question #31*Topic 1*

During a recent security audit, it was discovered that multiple teams in a large organization have placed restricted data in multiple Amazon S3 buckets, and the data may have been exposed. The auditor has requested that the organization identify all possible objects that contain personally identifiable information (PII) and then determine whether this information has been accessed.  
What solution will allow the Security team to complete this request?

* A. Using Amazon Athena, query the impacted S3 buckets by using the PII query identifier function. Then, create a new Amazon CloudWatch metric for Amazon S3 object access to alert when the objects are accessed.
* B. Enable Amazon Macie on the S3 buckets that were impacted, then perform data classification. For identified objects that contain PII, use the research function for auditing AWS CloudTrail logs and S3 bucket logs for GET operations.
* C. Enable Amazon GuardDuty and enable the PII rule set on the S3 buckets that were impacted, then perform data classification. Using the PII findings report from GuardDuty, query the S3 bucket logs by using Athena for GET operations.
* D. Enable Amazon Inspector on the S3 buckets that were impacted, then perform data classification. For identified objects that contain PII, query the S3 bucket logs by using Athena for GET operations.

Answer is Macie Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved

Question #32*Topic 1*

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

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

The answer should be B. We can achieve this using AWS Config. https://docs.aws.amazon.com/config/latest/developerguide/cloudtrail-enabled.html <https://docs.aws.amazon.com/config/latest/developerguide/iam-root-access-key-check.html>

Question #33*Topic 1*

An application has a requirement to be resilient across not only Availability Zones within the application's primary region but also be available within another region altogether.  
Which of the following supports this requirement for AWS resources that are encrypted by AWS KMS?

* A. Copy the application's AWS KMS CMK from the source region to the target region so that it can be used to decrypt the resource after it is copied to the target region.
* B. Configure AWS KMS to automatically synchronize the CMK between regions so that it can be used to decrypt the resource in the target region.
* C. Use AWS services that replicate data across regions, and re-wrap the data encryption key created in the source region by using the CMK in the target region so that the target region's CMK can decrypt the database encryption key.
* D. Configure the target region's AWS service to communicate with the source region's AWS KMS so that it can decrypt the resource in the target region.

C is Correct

Question #34*Topic 1*

An organization policy states that all encryption keys must be automatically rotated every 12 months.  
Which AWS Key Management Service (KMS) key type should be used to meet this requirement?

* A. AWS managed Customer Master Key (CMK)
* B. Customer managed CMK with AWS generated key material
* C. Customer managed CMK with imported key material
* D. AWS managed data key

Corect answer is sure B . A is wrong since AWS KMS managed CMK is rotated every 3 years by AWs and you cannot change this. for AWS Customer managed CMK with back end keys managed by AWS , it is auto rotation every 12 months , and for AWS customer managed CMKS with imported keys , it must be manual process.So B is 100% right

Question #35*Topic 1*

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

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

AWS Artifact is a repository for compliance documents. I would go for B, C, E.

Question #36*Topic 1*

A Security Administrator is configuring an Amazon S3 bucket and must meet the following security requirements:  
✑ Encryption in transit  
✑ Encryption at rest  
✑ Logging of all object retrievals in AWS CloudTrail  
Which of the following meet these security requirements? (Choose three.)

* A. Specify "aws:SecureTransport": "true" within a condition in the S3 bucket policy.
* B. Enable a security group for the S3 bucket that allows port 443, but not port 80.
* C. Set up default encryption for the S3 bucket.
* D. Enable Amazon CloudWatch Logs for the AWS account.
* E. Enable API logging of data events for all S3 objects.
* F. Enable S3 object versioning for the S3 bucket.

Encryption in transit ->Specify "aws:SecureTransport": "true" within a condition in the S3 bucket policy. Encryption at rest -> Set up default encryption for the S3 bucket. Logging of all object retrievals in AWS CloudTrail --> Enable API logging of data events for all S3 objects. A,C,E

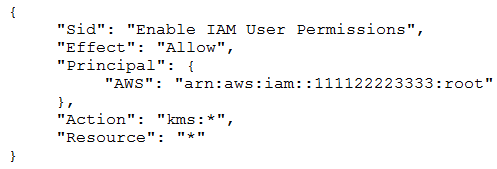
Question #37*Topic 1*

What is the function of the following AWS Key Management Service (KMS) key policy attached to a customer master key (CMK)?  


* A. The Amazon WorkMail and Amazon SES services have delegated KMS encrypt and delegated KMS encrypt and decrypt permissions to the ExampleUser principal in the 111122223333 account.
* B. The ExampleUser principal can transparently encrypt and decrypt email exchanges specifically between ExampleUser and AWS.
* C. The CMK is to be used for encrypting and decrypting only when the principal is ExampleUser and the request comes from WorkMail or SES in the specified region.
* D. The key policy allows WorkMail or SES to encrypt or decrypt on behalf of the user for any CMK in the account.

C should be correct! - kms:ViaService - Condition key limits use of an AWS KMS customer master key (CMK) to requests from specified AWS services. The kms:ViaService condition key is valid for all AWS KMS operations except: CreateKey, GenerateRandom, ListAliases, ListKeys, ListRetirableGrants, RetireGrant.

Question #38*Topic 1*

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

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

D should be correct . "AWS" : "arn:aws:iam:111122223333:root", " this allows IAM to further delegate permission" check reinvent video <https://www.youtube.com/watch?v=X1eZjXQ55ec>

Question #39*Topic 1*

A Software Engineer wrote a customized reporting service that will run on a fleet of Amazon EC2 instances. The company security policy states that application logs for the reporting service must be centrally collected.  
What is the MOST efficient way to meet these requirements?

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

D is correct You can set your application to send logs and cloudwatch to receive them using the cloudwatrch agent. A Lambda is not necessary <https://aws.amazon.com/blogs/devops/new-how-to-better-monitor-your-custom-application-metrics-using-amazon-cloudwatch-agent/>

Question #40*Topic 1*

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

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

B is correct as per the following link https://aws.amazon.com/artifact/