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.

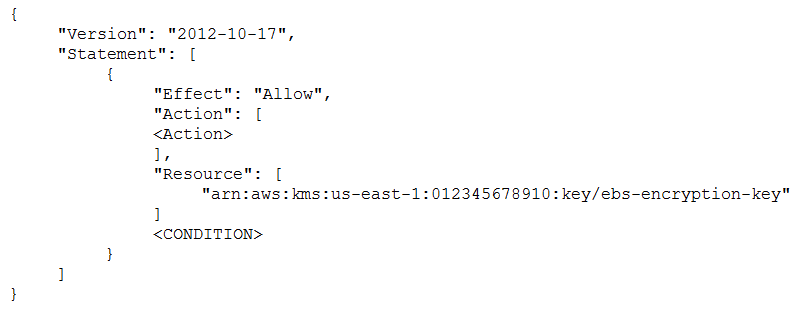
B = without incurring additional cost

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 } }