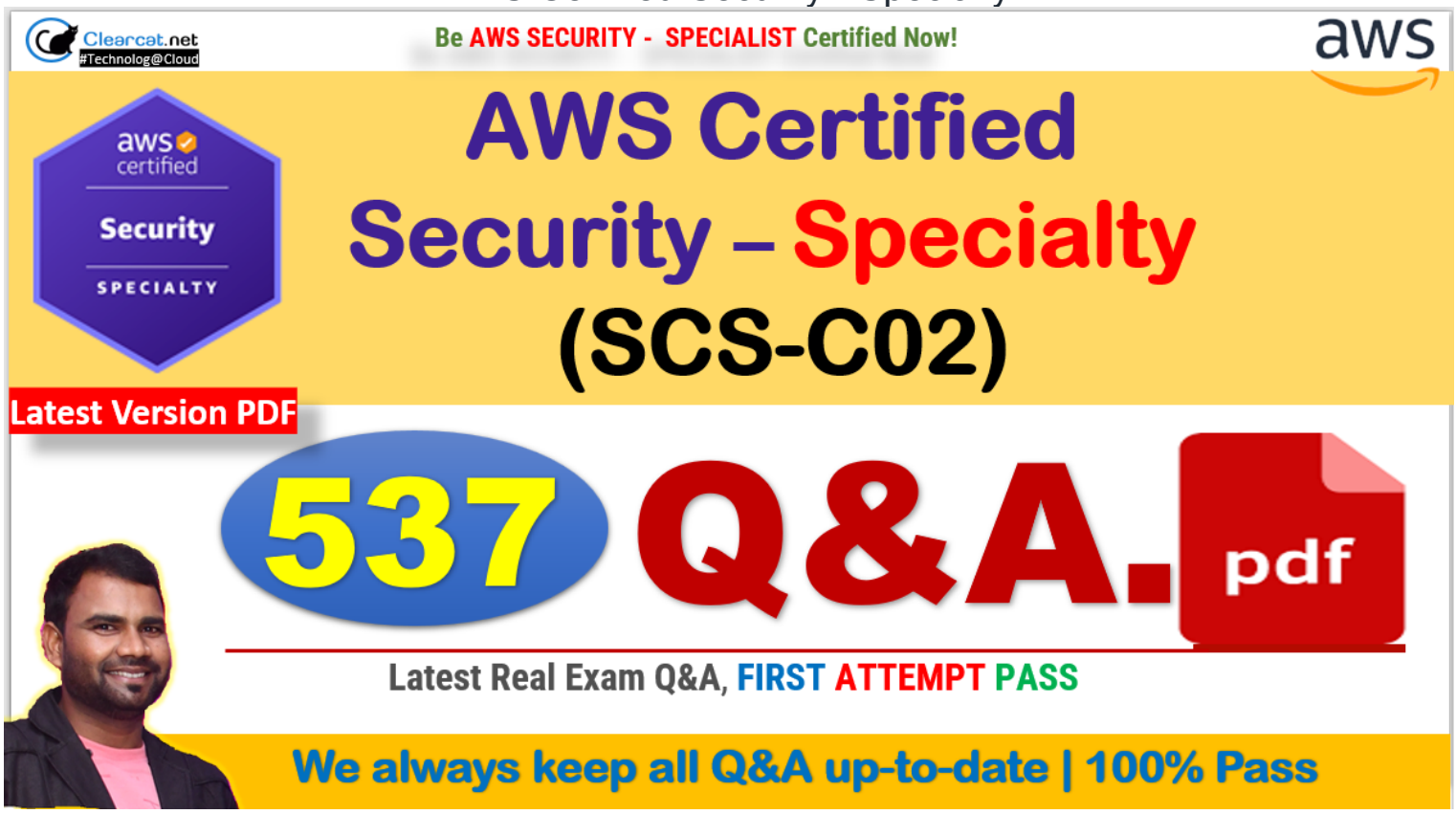
Amazon

Clearcat.Net | **FIRST ATTEMPT PASS** | **WWW.CLEARCATNET.COM**

AWS Certified Security - Specialty



Send us your request/inquiry at **clearcat.net@gmail.com** or connect us for Live Support any time for **any certification exam dumps pdf** Or for **most asked Interview Q&A PDFs** to ensure your success in first try!!

Visit us **WWW.CLEARCATNET.com**

Like & subscribe us: **https://youtube.com/CLEARCATNET**

Follow us on: Facebook | Instagram | LinkedIn | reddit | Twitter | Quora | YouTube

Question: 1 **AWS Certified Security - Specialty: Actual Exam Q&A | CLEARCATNET**

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.

Answer: A

Explanation:

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

Reference:

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

Question: 2 **AWS Certified Security - Specialty: Actual Exam Q&A | CLEARCATNET**

A company is storing data in Amazon S3 Glacier. The security engineer implemented a new vault lock policy for 10TB of data and called initiate-vault-lock operation 12 hours ago. The audit team identified a typo in the policy that is allowing unintended access to the vault.
What is the MOST cost-effective way to correct this?

A. Call the abort-vault-lock operation. Update the policy. Call the initiate-vault-lock operation again.
B. Copy the vault data to a new S3 bucket. Delete the vault. Create a new vault with the data.
C. Update the policy to keep the vault lock in place.
D. Update the policy. Call initiate-vault-lock operation again to apply the new policy.

Answer: A

Explanation:

Initiate the lock by attaching a vault lock policy to your vault, which sets the lock to an in-progress state and returns a lock ID. While in the in-progress state, you have 24 hours to validate your vault lock policy before the lock ID expires.

Use the lock ID to complete the lock process. If the vault lock policy doesn't work as expected, you can abort the lock and restart from the beginning. For information on how to use the S3 Glacier API to lock a vault, see Locking a Vault by Using the Amazon S3 Glacier API.

Reference:

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

Question: 3 **SCSC02**

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

Answer: C

Explanation:

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.

Reference:

https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/

Question: 4

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.

Answer: ACF

Explanation:

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

Reference:

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: 5 **AWS Certified Security - Specialty: Actual Exam Q&A | CLEARCATNET**

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

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

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

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

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

Answer: B

Explanation:

B is correct , first it mentioned custom protocols and ALBs only support HTTP & HTTPS listeners, CLBs support TCP,SSL/TLS,HTTP & HTTPS listeners . Second , it says encryption in transit between hosts and EC2 which means end-end encryption and not terminating or off-loading the session on the laod balancer , so only answer that terminates Session on EC2 is B.

Question: 6 **SCSC02**

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.

Answer: BC

Explanation:

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

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

Reference:

https://d1.awsstatic.com/architecture-diagrams/ArchitectureDiagrams/web-application-architecture-on-aws-ra.pdf?did=wp_card&trk=wp_card

Question: 7

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.

Answer: C

Explanation:

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

Reference:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_about-scps.html

Question: 8 SCSC02

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

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

Answer: C

Explanation:

mechanisms for establishing a TLS-encrypted connection:

- STARTTLS:

Client starts an unencrypted connection to the SMTP server on ports 25, 587, 2587

After connection, the client starts TLS negotiation

- TLS Wrapper:

Client start an encrypted connection with the SMTP server on ports 465, 2465

Reference:

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

Question: 9 **AWS Certified Security - Specialty: Actual Exam Q&A | CLEARCATNET**

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:
Threat description: A malicious actor could upload sensitive data from Server X by configuring credentials for an AWS account (Account 2) they control and uploading data to an Amazon S3 bucket within their control.
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.

Answer: AB

Explanation:

You can not block vpc endpoint at security group, but can use cli to find vpc endpoint IP range and block that IPs in proxy configuration.

C could work but you don't want block vpc endpoint at subnet because it affects all instance in that subnet.

https://aws.amazon.com/premiumsupport/knowledge-center/connect-s3-vpc-endpoint/

Question: 10 **AWS Certified Security - Specialty: Actual Exam Q&A | CLEARCATNET**

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.

Answer: A

Explanation:

Just to answer those questions around "each object with a unique key"

Keep in mind that S3 applies envelop encryption, meaning that each object is NOT encrypted by your CMK directly. Instead each object is encrypted with a unique data key which is generated and also encrypted from your CMK

Question: 11 **SCSC02**

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.

Answer: D

Explanation:

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: 12 **AWS Certified Security - Specialty: Actual Exam Q&A | CLEARCATNET**

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.

Answer: D

Explanation:

"You might prefer to rotate keys manually so you can control the rotation frequency. It's also a good solution for CMKs that are not eligible for automatic key rotation, such as asymmetric CMKs, CMKs in custom key stores and CMKs with imported key material.

Because the new CMK is a different resource from the current CMK, it has a different key ID and ARN. When you change CMKs, you need to update references to the CMK ID or ARN in your applications. Aliases, which associate a friendly name with a CMK, make this process easier. Use an alias to refer to a CMK in your applications. Then, when you want to change the CMK that the application uses, change the target CMK of the alias.

To update the target CMK of an alias, use UpdateAlias operation in the AWS KMS API. " - https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html#rotate-keys-manually

Question: 13 **SCSC02**

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?

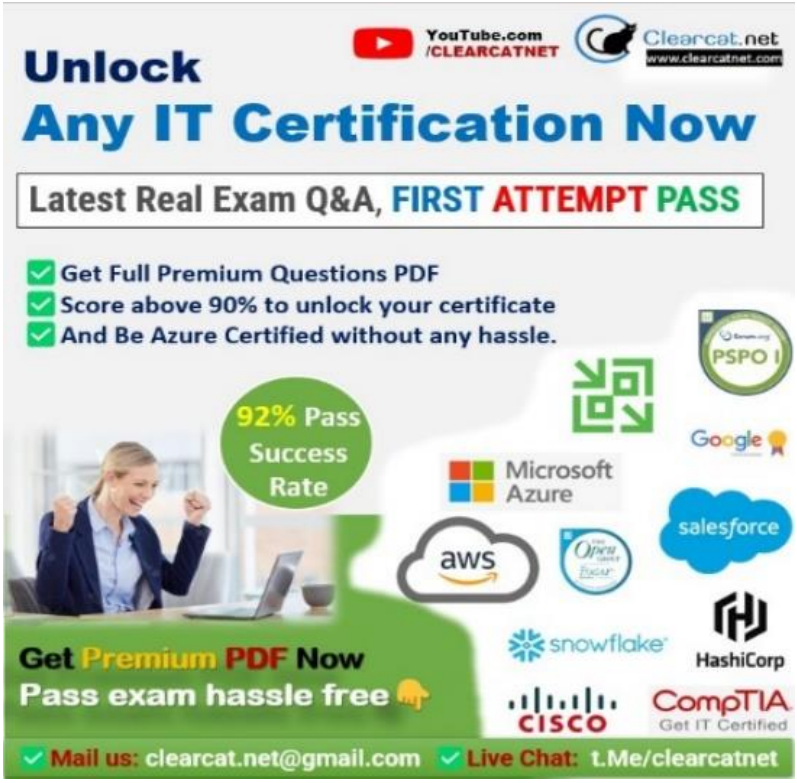
A. Use AWS Systems Manager to store the credentials as Secure Strings Parameters. Secure by using an AWS KMS key.
B. Use AWS Key Management System to store a master key, which is used to encrypt the credentials. The encrypted credentials are stored in an Amazon RDS instance.
C. Use AWS Secrets Manager to store the credentials.
D. Store the credentials in a JSON file on Amazon S3 with server-side encryption.

Thank you for Trying our Free Sample Questions

But We Recommend try our premium exam material (Full Premium PDF) dumps in PDF Format to certain your success in First Attempt Only.

VISIT US NOW TO DOWNLOAD PDF INSTANTLY

https://www.clearcatnet.com/Papers



Send us your request/inquiry at clearcat.net@gmail.com or connect us for Live Support any time for **any certification exam dumps pdf** Or for **most asked Interview Q&A PDFs** to ensure your success in first try!!

Get any exam latest real exam questions PDF Now-

- **Visit us** - www.clearcatnet.com
- **Mail us**- clearcat.net@gmail.com
- **Live Support**- https://t.me/clearcatnet

YouTube.com /CLEARCATNET

t.Me /CLEARCATNET