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 Cloud Trail console to search for user activity.
B. Use the Amazon Cloud Watch Logs console to filter Cloud Trail 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.

2. 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.

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

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: Assume Role 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.

5. 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.