Answer Sheet

Q1)

You are planning on hosting a web application on AWS. You create an EC2 Instance in a public subnet.

This instance needs to connect to an EC2 Instance that will host an Oracle database.

Which of the following steps should be followed to ensure a secure setup is in place

- ✓ Create a database security group and ensure the web security group to allowed incoming access
- ✓ Place the EC2 Instance with the Oracle database in a separate private subnet
- Place the EC2 Instance with the Oracle database in the same public subnet as the Web server for faster communication.
- Ensure the database security group allows incoming traffic from 0.0.0.0/0

Q2)

An EC2 Instance hosts a Java based application that access a DynamoDB table. This EC2 Instance is currently serving production based users.

Which of the following is a secure way of ensuring that the EC2 Instance access the DynamoDB table

- Use IAM Access Groups with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- Use IAM Access Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- Use KMS keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- ✓ Use IAM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance

---

Q3)

An application running on EC2 instances processes sensitive information stored on Amazon S3. The information is accessed over the Internet.

The security team is concerned that the Internet connectivity to Amazon S3 is a security risk.

Which solution will resolve the security concern?

- Access the data through a NAT Gateway.
- Access the data through a VPN connection.
- Access the data through an Internet Gateway.
- ✓ Access the data through a VPC endpoint for Amazon S3

Q4)

Development teams in your organization use S3 buckets to store the log files for various application hosted in development environments in AWS.

The developers want to keep the logs for one month for troubleshooting purposes, and then purge the logs.

What feature will enable this requirement?

- Creating an IAM policy for the S3 bucket.
- ✓ Configuring lifecycle configuration rules on the S3 bucket.
- Adding a bucket policy on the S3 bucket.
- Enabling CORS on the S3 bucket.

Q5)

A company is using a Redshift cluster to store their data warehouse. There is a requirement from the Internal IT Security team to ensure that data gets encrypted for the Redshift database.

How can this be achieved?

- Use SSL/TLS for encrypting the data
- ✓ Use AWS KMS Customer Default master key
- Encrypt the EBS volumes of the underlying EC2 Instances
- Use S3 Encryption

Q6)

A company has resources hosted in their AWS Account. There is a requirement to monitor all API activity for all regions.

The audit needs to be applied for future regions as well.

Which of the following can be used to fulfil this requirement.

- Create a Cloudtrail for each region. Use Cloudformation to enable the trail for all future regions.
- ✓ Ensure one Cloudtrail trail is enabled for all regions.
- Ensure Cloudtrail for each region. Then enable for each future region.
- Create a Cloudtrail for each region. Use AWS Config to enable the trail for all future regions.

Q7)

A customer has an instance hosted in the AWS Public Cloud. The VPC and subnet used to host the Instance have been created with the default settings for the Network Access Control Lists.

They need to provide an IT Administrator secure access to the underlying instance.

How can this be accomplished.

- Ensure that the security group allows Outbound SSH traffic from the IT Administrator's Workstation
- ✓ Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation
- Ensure the Network Access Control Lists allow Outbound SSH traffic from the IT Administrator's Workstation
- Ensure the Network Access Control Lists allow Inbound SSH traffic from the IT Administrator's Workstation

---

Q8)

A company is planning to run a number of Admin related scripts using the AWS Lambda service. There is a need to understand if there are any errors encountered when the script run.

How can this be accomplished in the most effective manner.

- Use the AWS Config service to monitor for errors
- Use Cloudtrail to monitor for errors
- ✓ Use Cloudwatch metrics and logs to watch for errors
- Use the AWS Inspector service to monitor for errors

Q9)

A company hosts data in S3. There is now a mandate that going forward all data in the S3 bucket needs to encrypt at rest.

How can this be achieved?

- ✓ Enable server side encryption on the S3 bucket
- Use SSL certificates to encrypt the data
- Use AWS Access keys to encrypt the data
- Enable MFA on the S3 bucket

Q10)

You are responsible to deploying a critical application onto AWS. Part of the requirements for this application is to ensure that the controls set for this application met PCI compliance.

Also there is a need to monitor web application logs to identify any malicious activity.

Which of the following services can be used to fulfil this requirement. Choose 2 answers from the options given below

- Amazon AWS Config
- Amazon VPC Flow Logs
- ✓ Amazon Cloudwatch Logs
- ✓ Amazon Cloudtrail

Q11)

You need to have a cloud security device which would allow to generate encryption keys based on FIPS 140-2 Level 3.

Which of the following can be used for this purpose?

- ✓ AWS Cloud HSM
- AWS managed keys
- AWS Customer Keys
- AWS KMS

Q12)

A company has an existing AWS account and a set of critical resources hosted in that account.

The employee who was in-charge of the root account has left the company.

What must be now done to secure the account. Choose 3 answers from the options given below.

- ✓ Change the password for the root account
- ✓ Confirm MFA to a secure device
- ✓ Delete the access keys for the root account
- Change the password for all IAM users

Q13)

You have a set of application , database and web servers hosted in AWS. The web servers are placed behind an ELB. There are separate security groups for the application, database and web servers.

The network security groups have been defined accordingly.

There is an issue with the communication between the application and database servers.

In order to troubleshoot the issue between just the application and database server, what is the ideal set of MINIMAL steps you would take

- Check the Outbound security rules for the database security group Check the both the Inbound and Outbound security rules for the application security group
- Check the both the Inbound and Outbound security rules for the database security group Check the Inbound security rules for the application security group
- Check the Outbound security rules for the database security group Check the Inbound security rules for the application security group
- ✓ Check the Inbound security rules for the database security group Check the Outbound security rules for the application security group

---

Q14)

A company is planning on extending their on-premise AWS Infrastructure to the AWS Cloud. They need to have a solution that would give core benefits of traffic encryption and ensure latency is kept to a minimum.

Which of the following would help fulfil this requirement? Choose 2 answers from the options given below

- AWS NAT gateways
- AWS VPC Peering
- ✓ AWS VPN
- ✓ AWS Direct Connect

Q15)

How can you ensure that instance in an VPC does not use AWS DNS for routing DNS requests. You want to use your own managed DNS instance.

How can this be achieved?

- Change the route table for the VPC
- ✓ Create a new DHCP options set and replace the existing one.
- Change the existing DHCP options set
- Change the subnet configuration to allow DNS requests from the new DNS Server

---

Q16)

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet that was created with default ACL settings. The IT Security department has a suspicion that a DDos attack is coming from a suspecting IP.

How can you protect the subnets from this attack?

- ✓ Change the Inbound NACL to deny access from the suspecting IP
- Change the Outbound Security Groups to deny access from the suspecting IP
- Change the Inbound Security Groups to deny access from the suspecting IP
- Change the Outbound NACL to deny access from the suspecting IP

Q17)

You are designing a custom IAM policy that would allow uses to list buckets in S3 only if they are MFA authenticated.

Which of the following would best match this requirement?

- { "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Action": ["s3:ListAllMyBuckets", "s3:GetBucketLocation"], "Resource": "Resource": "arn:aws:s3:::*", "Condition": { "aws:MultiFactorAuthPresent":true } } }
- { "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Action": ["s3:ListAllMyBuckets", "s3:GetBucketLocation"], "Resource": "Resource": "arn:aws:s3:::*", "Condition": { "aws:MultiFactorAuthPresent":false } } }
- ✓ { "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Action": ["s3:ListAllMyBuckets", "s3:GetBucketLocation"], "Resource": "Resource": "arn:aws:s3:::*", "Condition": { "Bool": {"aws:MultiFactorAuthPresent": true} } } }
- { "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Action": ["s3:ListAllMyBuckets", "s3:GetBucketLocation"], "Resource": "Resource": "arn:aws:s3:::*", "Condition": { "Bool": {"aws:MultiFactorAuthPresent":false} } } }

Q18)

You are hosting a web site via website hosting on an S3 bucket http://demo.s3-website-us-east-1.amazonaws.com.

You have some web pages that use Javascript that access resources in another bucket which has web site hosting also enabled.

But when users access the web pages , they are getting a blocked Javascript error.How can you rectify this?

- Enable CRR for the bucket
- Enable MFA for the bucket
- Enable versioning for the bucket
- ✓ Enable CORS for the bucket

Q19)

You have a vendor that needs access to an AWS resource. You create an AWS user account.

You want to restrict access to the resource using a policy for just that user over a brief period.

Which of the following would be an ideal policy to use?

- A bucket ACL
- A Bucket Policy
- ✓ An Inline Policy
- An AWS Managed Policy

Q20)

Your company has a requirement to monitor all root user activity.

How can this best be achieved? Choose 2 answers from the options given below. Each answer forms part of the solution

- Use Cloudtrail API call
- ✓ Use a Lambda function
- Create a Cloudwatch Logs Rule
- ✓ Create a Cloudwatch Events Rule

Q21)

A company wants to have a secure way of generating, storing and managing cryptographic keys. But they want to have exclusive access for the keys.

Which of the following can be used for this purpose?

- ✓ Use Cloud HSM
- Use S3 Server Side encryption
- Use KMS and use an external key material
- Use KMS and the normal KMS encryption keys

Q22)

A company is hosting a website that must be accessible to users for HTTPS traffic. Also port 22 should be open for administrative purposes.

Which of the following security group configurations are the MOST secure but still functional to support these requirements?

Choose 2 answers from the options given below

- ✓ Port 22 coming from 10.0.0.0/16
- Port 22 coming from 0.0.0.0/0
- Port 443 coming from 10.0.0.0/16
- ✓ Port 443 coming from 0.0.0.0/0

Q23)

Your company has an EC2 Instance that is hosted in an AWS VPC.

There is a requirement to ensure that logs files from the EC2 Instance are stored accordingly.

The access should also be limited for the destination of the log files.

How can this be accomplished? Choose 2 answers from the options given below. Each answer forms part of the solution

- ✓ Create an IAM policy that gives the desired level of access to the Cloudwatch Log group
- Create an IAM policy that gives the desired level of access to the Cloudtrail trail
- ✓ Stream the log files to a separate Cloudwatch Log group
- Stream the log files to a separate Cloudtrail trail

Q24)

You have an Ec2 Instance in a private subnet which needs to access the KMS service.

Which of the following methods can help fulfil this requirement, keeping security in perspective

- Attach a VPN connection to the VPC
- Attach an Internet gateway to the subnet
- ✓ Use a VPC endpoint
- Use VPC Peering

Q25)

You have a web site that is sitting behind AWS Cloudfront.

You need to protect the web site against threats such as SQL injection and Cross site scripting attacks.

Which of the following service can help in such a scenario

- AWS Inspector
- ✓ AWS WAF

- AWS Trusted Advisor
- AWS Config

Q26)

Your company has a set of resources defined in the AWS Cloud.

Their IT audit department has requested to get a list of resources that have been defined across the account.

How can this be achieved in the easiest manner?

- Use Cloud Trail to get the list of all resources
- ✓ Use AWS Config to get the list of all resources
- Create a bash shell script with the AWS CLI. Query for all resources in all regions. Store the results in an S3 bucket.
- Create a powershell script using the AWS CLI. Query for all resources with the tag of production.

Q27)

A Lambda function reads metadata from an S3 object and stores the metadata in a DynamoDB table.

The function is triggered whenever an object is stored within the S3 bucket.

How should the Lambda function be given access to the DynamoDB table?

- ✓ Create an IAM service role with permissions to write to the DynamoDB table. Associate that role with the Lambda function.
- Create an IAM user with permissions to write to the DynamoDB table. Store an access key for that user in the Lambda environment variables.
- Create a resource policy that grants the Lambda function permissions to write to the DynamoDB table. Attach the policy to the DynamoDB table.
- Create a VPC endpoint for DynamoDB within a VPC. Configure the Lambda function to access resources in the VPC.

Q28)

Your company has defined privileged users for their AWS Account. These users are administrators for key resources defined in the company.

There is now a mandate to enhance the security authentication for these users. How can this be accomplished?

- Enable accidental deletion for these user accounts
- Enable versioning for these user accounts
- ✓ Enable MFA for these user accounts
- Disable root access for the users

Q29)

An application running on EC2 instances must use a username and password to access a database.

The developer has stored those secrets in the SSM Parameter Store with type SecureString using the default KMS CMK.

Which combination of configuration steps will allow the application to access the secrets via the API? Select 2 answers from the options below

- Add the SSM service role as a trusted service to the EC2 instance role.
- ✓ Add permission to use the KMS key to decrypt to the EC2 instance role
- ✓ Add permission to read the SSM parameter to the EC2 instance role.
- Add permission to use the KMS key to decrypt to the SSM service role.
- Add the EC2 instance role as a trusted service to the SSM service role.

Q30) When you enable automatic key rotation for an existing CMK key where the backing key is managed by AWS, after how long is the key rotated?

- ✓ After 365 days
- After 128 days
- After 30 days
- After 3 years

Q31)

You have a 2 tier application hosted in AWS. It consists of a web server and database server (SQL Server) hosted on separate EC2 Instances.

You are devising the security groups for these EC2 Instances. The Web tier needs to be accessed by users across the Internet.

You have created a web security group(wg-123) and database security group(db-345).

Which combination of the following security group rules will allow the application to be secure and functional.

Choose 2 answers from the options given below.

- wg-123 - Allow port 1433 from wg-123
- ✓ db-345 - Allow port 1433 from wg-123
- ✓ wg-123 - Allow ports 80 and 443 from 0.0.0.0/0
- db-345 - Allow ports 1433 from 0.0.0.0/0

Q32) You are deivising a policy to allow users to have the ability to access objects in a bucket called appbucket.

You define the below custom bucket policy

{ "ID": "Policy1502987489630",

"Version": "2012-10-17",

"Statement": [

{

"Sid": "Stmt1502987487640",

"Action": [

"s3:GetObject",

"s3:GetObjectVersion"

],

"Effect": "Allow",

"Resource": "arn:aws:s3:::appbucket",

"Principal": "*"

}

]

}

But when you try to apply the policy you get the error

"Action does not apply to any resource(s) in statement.? What should be done to rectify the error

- Create the bucket "appbucket" and then apply the policy.
- ✓ Change the Resource section to "arn:aws:s3:::appbucket/*".
- Verify that the policy has the same name as the bucket name. If not, make it the same.
- Change the IAM permissions by applying PutBucketPolicy permissions.

Q33)

A company wants to have an Intrusion detection system available for their VPC in AWS. They want to have complete control over the system.

Which of the following would be ideal to implement?

- Use VPC Flow logs to detect the issues and flag them accordingly.
- ✓ Use a custom solution available in the AWS Marketplace
- Use AWS WAF to catch all intrusions occurring on the systems in the VPC
- Use AWS Cloudwatch to monitor all traffic

Q34)

Your IT Security department has mandated that all data on EBS volumes created for underlying EC2 Instances need to be encrypted.

Which of the following can help achieve this?

- IAM Access Key
- API Gateway with STS
- AWS Certificate Manager
- ✓ AWS KMS API

Q35)

You have an S3 bucket hosted in AWS. This is used to host promotional videos uploaded by yourself.

You need to provide access to users for a limited duration of time. How can this be achieved?

- Use IAM Roles with a timestamp to limit the access
- ✓ Use Pre-signed URL's
- Use versioning and enable a timestamp for each version
- Use IAM policies with a timestamp to limit the access

Q36)

Your company has mandated that all calls to the AWS KMS service be recorded.

How can this be achieved?

- Enable Cloudwatch logs
- Enable a trail in Cloudtrail
- Enable logging on the KMS service
- Use Cloudwatch metrics

Q37)

You want to get a list of vulnerabilities for an EC2 Instance as per the guidelines set by the Center of Internet Security.

How can you go about doing this?

- Use AWS Inspector
- Use AWS Trusted Advisor
- Enable AWS Guard Duty for the Instance
- Use AWS Macie

Q38)

You have an instance setup in a test environment in AWS. You installed the required application and the promoted the server to a production environment. Your IT Security team has advised that there maybe traffic flowing in from an unknown IP address to port 22.

How can this be mitigated immediately?

- Change the AMI for the instance
- Remove the rule for incoming traffic on port 22 for the Security Group
- Shutdown the instance
- Change the Instance type for the Instance

Q39)

Your company has defined a number of EC2 Instances over a period of 6 months.

They want to know if any of the security groups allow unrestricted access to a resource.

What is the best option to accomplish this requirement?

- Use the AWS CLI to query the security groups and then filter for the rules which have unrestricted access
- Use AWS Config to see which security groups have compromised access.
- Use AWS Inspector to inspect all the security Groups
- Use the AWS Trusted Advisor to see which security groups have compromised access.

Q40)

A company is using CloudTrail to log all AWS API activity for all regions in all of its accounts. The CISO has asked that additional steps be taken to protect the integrity of the log files.

What combination of steps will protect the log files from intentional or unintentional alteration? Choose 2 answers from the options given below

- Create a Security Group that blocks all traffic except calls from the CloudTrail service. Associate the security group with all the Cloud Trail destination S3 buckets.
- Use Systems Manager Configuration Compliance to continually monitor the access policies of S3 buckets containing Cloud Trail logs.
- Enable Cloud Trail log file integrity validation
- Write a Lambda function that queries the Trusted Advisor Cloud Trail checks. Run the function every 10 minutes.
- Create an S3 bucket in a dedicated log account and grant the other accounts write only access. Deliver all log files from every account to this S3 bucket.

Q41)

You have just received an email from AWS Support stating that your AWS account might have been compromised.

Which of the following steps would you look to carry out immediately. Choose 3 answers from the options below.

- Keep all resources running to avoid disruption
- Rotate all IAM access keys
- Change the root account password.
- Change the password for all IAM users.

Q42)

Your IT Security team has advised to carry out a penetration test on the resources in their company's AWS Account.

This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?

- Submit a request to AWS Support
- Turn on VPC Flow Logs and carry out the penetration test
- Turn on Cloud trail and carry out the penetration test
- Use a custom AWS Marketplace solution for conducting the penetration test

---

Q43)

Your company is planning on hosting an internal network in AWS. They want machines in the VPC to authenticate using private certificates.

They want to minimize the work and maintenance in working with certificates. What is the ideal way to fulfil this requirement.

- Consider using AWS Access keys to generate the certificates
- ✅ Consider using AWS Certificate Manager
- Consider using Windows Server 2016 Certificate Manager
- Consider using AWS Trusted Advisor for managing the certificates

---

Q44)

You have enabled Cloudtrail logs for your company's AWS account.

In addition, the IT Security department has mentioned that the logs need to be encrypted.

How can this be achieved?

- Enable Server side encryption for the trail
- ✅ There is no need to do anything since the logs will already be encrypted
- Enable SSL certificates for the Cloudtrail logs
- Enable Server side encryption for the destination S3 bucket

---

Q45)

You have just recently set up a web and database tier in a VPC and hosted the application.

When testing the application , you are not able to reach the home page for the app. You have verified the security groups.

What can help you diagnose the issue.

- Use AWS WAF to analyze the traffic
- ✅ Use VPC Flow logs to diagnose the traffic
- Use the AWS Trusted Advisor to se what can be done.
- Use AWS Guard Duty to analyze the traffic

Q46)

A security team is creating a response plan in the event an employee executes unauthorized actions on AWS infrastructure.

They want to include steps to determine if the employee's IAM permissions changed as part of the incident.

What steps should the team document in the plan?

- Use Trusted Advisor to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.
- Use CloudTrail to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.
- Use Macie to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.
- ✅ Use AWS Config to examine the employee's IAM permissions prior to the incident and compare them to the employee's current IAM permissions.

Q47)

A security team must present a daily briefing to the CISO that includes a report of which of the company's thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day's report.

How can the security team fulfill these requirements?

- Use Trusted Advisor to generate the report of out of compliance instances/ servers. Use Systems Manger Patch Manger to install the missing patches.
- Use Systems Manger Patch Manger to generate the report of out of compliance instances/ servers. Redeploy all out of compliance instances/servers using an AMI with the latest patches.
- ✅ Use Systems Manger Patch Manger to generate the report of out of compliance instances/ servers. Use Systems Manager Patch Manger to install the missing patches.
- Use Amazon QuickSight and Cloud Trail to generate the report of out of compliance instances/servers. Redeploy all out of compliance instances/servers using an AMI with the latest patches.

Q48)

Your development team has started using AWS resources for development purposes. The AWS account has just been created.

Your IT Security team is worried about possible leakage of AWS keys.

What is the first level of measure that should be taken to protect the AWS account.

- Create IAM Roles
- Create IAM Groups
- ✅ Delete the AWS keys for the root account
- Restrict access using IAM policies

Q49) Which of the following is not a best practice for carrying out a security audit?

- Conduct an audit if you ever suspect that an unauthorized person might have accessed your account
- Conduct an audit if application instances have been added to your account
- ✓ Conduct an audit on a yearly basis
- Whenever there are changes in your organization

Q50) Which of the following is used as a secure way to log into an EC2 Linux Instance?

- AWS Access keys
- ✓ Key pairs
- IAM User name and password
- AWS SDK keys

Q51)

A windows machine in one VPC needs to join the AD domain in another VPC. VPC Peering has been established. But the domain join is not working.

What is the other step that needs to be followed to ensure that the AD domain join can work as intended

- ✓ Ensure the security groups for the AD hosted subnet has the right rule for relevant subnets
- Change the VPC peering connection to a Direct Connect connection
- Change the VPC peering connection to a VPN connection
- Ensure that the AD is placed in a public subnet

Q52)

You need to have a requirement o store objects in an S3 bucket with a key that is automatically managed and rotated.

Which of the following can be used for this purpose?

- AWS Customer Keys
- ✓ AWS S3 Server side encryption
- AWS KMS
- AWS Cloud HSM

Q53)

A company stores critical data in an S3 bucket. There is a requirement to ensure that an extra level of security is added to the S3 bucket. In addition , it should be ensured that objects are available in a secondary region if the primary one goes down.

Which of the following can help fulfil these requirements? Choose 2 answers from the options given below

- ✓ For the Bucket policy add a condition for { "Null": { "aws:MultiFactorAuthAge": true }}
- Enable bucket versioning and enable Master Pays
- ✓ Enable bucket versioning and also enable CRR
- Enable the Bucket ACL and add a condition for { "Null": { "aws:MultiFactorAuthAge": true }}

Q54)

Your company manages thousands of EC2 Instances. There is a mandate to ensure that all servers don't have any critical security flaws.

Which of the following can be done to ensure this? Choose 2 answers from the options given below.

- Use AWS Inspector to patch the servers
- ✓ Use AWS Inspector to ensure that the servers have no critical flaws.
- Use AWS Config to ensure that the servers have no critical flaws.
- ✓ Use AWS SSM to patch the servers

Q55)

You need to inspect the running processes on an EC2 Instance that may have a security issue. How can you achieve this in the easiest way possible.

Also you need to ensure that the process does not interfere with the continuous running of the instance.

- ✓ Use the SSM Run command to send the list of running processes information to an S3 bucket.
- Use AWS Cloudwatch to record the processes running on the server
- Use AWS Cloudtrail to record the processes running on the server to an S3 bucket.
- Use AWS Config to see the changed process information on the server

---

Q56)

A company has a large set of keys defined in AWS KMS. Their developers frequently use the keys for the applications being developed.

What is one of the ways that can be used to reduce the cost of accessing the keys in the AWS KMS service.

- Create an alias of the key
- Use Data key caching
- Enable rotation of the keys
- Use the right key policy

Q57)

You are trying to use the AWS Systems Manager run command on a set of Instances. The run command is not working on a set of Instances.

What can you do to diagnose the issue? Choose 2 answers from the options given below

- Ensure the security groups allow outbound communication for the Instance
- Ensure the right AMI is used for the Instance
- Check the /var/log/amazon/ssm/errors.log file
- Ensure that the SSM agent is running on the target machine

Q58)

You are working for a company and been allocated the task for ensuring that there is a federated authentication mechanism setup between AWS and their On-premise Active Directory.

Which of the following are important steps that need to be covered in this process? Choose 2 answers from the options given below.

- Configure AWS as the relying party in Active Directory Federation services
- Configure AWS as the relying party in Active Directory
- Ensure the right match is in place for On-premise AD Groups and IAM Groups.
- Ensure the right match is in place for On-premise AD Groups and IAM Roles.
