✓ 1. An IT company wants to review its security best-practices after an incident was reported where a new developer on the team was assigned full access to Amazon DynamoDB. The developer accidentally deleted a couple of tables from the production environment while building out a new feature. *1/1

Which is the MOST effective way to address this issue so that such incidents do not recur?

○ Remove full database access for all IAM users in the organization

● Use permissions boundary to control the maximum permissions employees can grant to the IAM principals ✓

○ The CTO should review the permissions for each new developer's IAM user so that such incidents don't recur

○ Only root user should have full database access in the organization

✓ 2. An organization wants to delegate access to a set of users from the development environment so that they can access some resources in the production environment which is managed under another AWS account. *1/1

As a solutions architect, which of the following steps would you recommend?

○ It is not possible to access cross-account resources

○ Both IAM roles and IAM users can be used interchangeably for cross-account access

● Create a new IAM role with the required permissions to access the resources in the production environment. The users can then assume this IAM role while accessing the resources from the production environment ✓

○ Create new IAM user credentials for the production environment and share these credentials with the set of users from the development environment

✓ 3. A new DevOps engineer has joined a large financial services company recently. As part of his onboarding, the IT department is conducting a review of the checklist for tasks related to AWS Identity and Access Management (AWS IAM). *1/1

As an AWS Certified Solutions Architect – Associate, which best practices would you recommend (Select two)?

☐ Use user credentials to provide access specific permissions for Amazon EC2 instances

☑ Configure AWS CloudTrail to log all AWS Identity and Access Management (AWS IAM) actions ✓

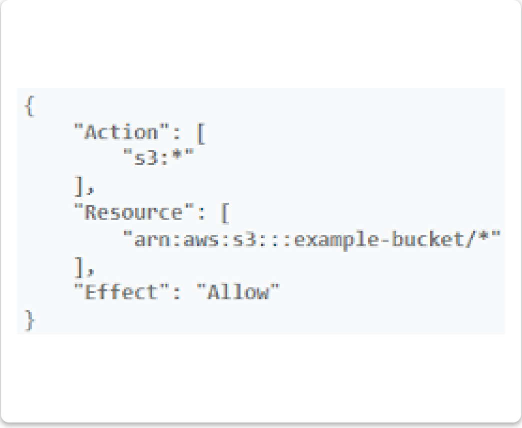
☑ Enable AWS Multi-Factor Authentication (AWS MFA) for privileged users ✓

☐ Grant maximum privileges to avoid assigning privileges again

☐ Create a minimum number of accounts and share these account credentials among employees

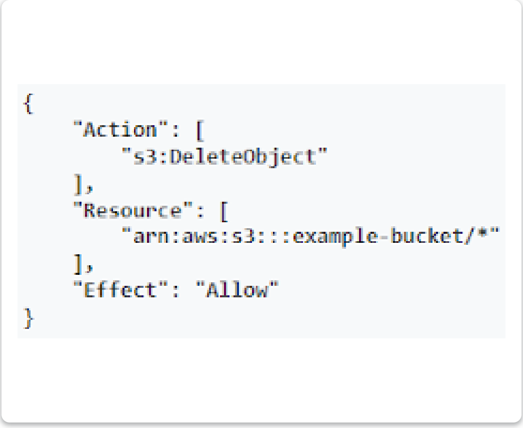
✓ 4. A development team requires permissions to list an Amazon S3 bucket and delete objects from that bucket. A systems administrator has created the following IAM policy to provide access to the bucket and applied that policy to the group. The group is not able to delete objects in the bucket. The company follows the principle of least privilege. *1/1

```
"Version": "2021-10-17",
"Statement": [
    {
        "Action": [
            "s3:ListBucket",
            "s3:DeleteObject"
        ],
        "Resource": [
            "arn:aws:s3:::example-bucket"
        ],
        "Effect": "Allow"
    }
]
```



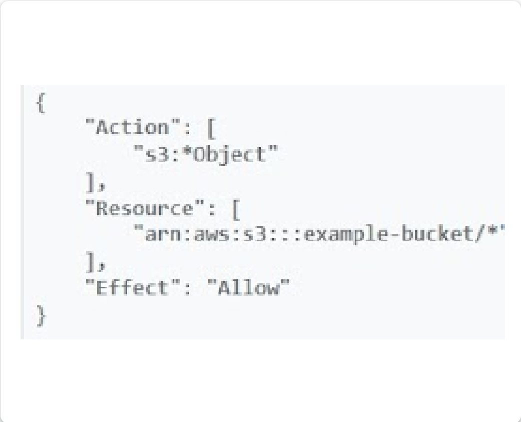
```
{
    "Action": [
        "s3:*"
    ],
    "Resource": [
        "arn:aws:s3:::example-bucket/*"
    ],
    "Effect": "Allow"
}
```

○ Option 1

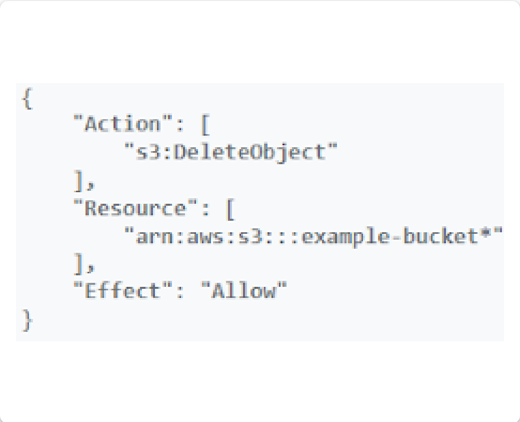


```
{
    "Action": [
        "s3:DeleteObject"
    ],
    "Resource": [
        "arn:aws:s3:::example-bucket/*"
    ],
    "Effect": "Allow"
}
```

● Option 2 ✓



```
{
    "Action": [
        "s3:*Object"
    ],
    "Resource": [
        "arn:aws:s3:::example-bucket/*'
    ],
    "Effect": "Allow"
}
```



```
{
    "Action": [
        "s3:DeleteObject"
    ],
    "Resource": [
        "arn:aws:s3:::example-bucket*"
    ],
    "Effect": "Allow"
}
```

○ Option 3 ○ Option 4

✓ 5. A developer needs to implement an AWS Lambda function in AWS account A that accesses an Amazon Simple Storage Service (Amazon S3) bucket in AWS account B. *1/1

As a Solutions Architect, which of the following will you recommend to meet this requirement?

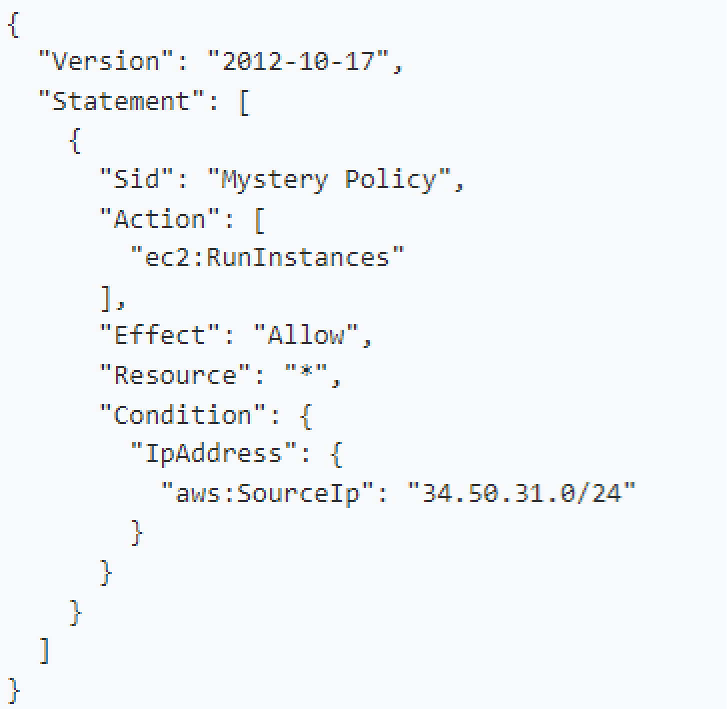
○ Create an IAM role for the AWS Lambda function that grants access to the Amazon S3 bucket. Set the IAM role as the Lambda function's execution role and that would give the AWS Lambda function cross-account access to the Amazon S3 bucket

● Create an IAM role for the AWS Lambda function that grants access to the Amazon S3 bucket. Set the IAM role as the AWS Lambda function's execution role. Make sure that the bucket policy also grants access to the AWS Lambda function's execution role ✓

○ The Amazon S3 bucket owner should make the bucket public so that it can be accessed by the AWS Lambda function in the other AWS account

○ AWS Lambda cannot access resources across AWS accounts. Use Identity federation to work around this limitation of Lambda

✓ 6. What does this IAM policy do? * 1/1



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Mystery Policy",
      "Action": [
        "ec2:RunInstances"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "34.50.31.0/24"
        }
      }
    }
  ]
}
```

○ It allows starting an Amazon EC2 instance only when they have an Elastic IP within the 34.50.31.0/24 CIDR block

○ It allows starting an Amazon EC2 instance only when they have a Private IP within the 34.50.31.0/24 CIDR block

● It allows starting an Amazon EC2 instance only when the IP where the call originates is within the 34.50.31.0/24 CIDR block ✓

○ It allows starting an Amazon EC2 instance only when they have a Public IP within the 34.50.31.0/24 CIDR block

✓ 7. An IT company provides Amazon Simple Storage Service (Amazon S3) bucket access to specific users within the same account for completing project specific work. With changing business requirements, cross-account S3 access requests are also growing every month. The company is looking for a solution that can offer user level as well as account-level access permissions for the data stored in Amazon S3 buckets. *1/1

As a Solutions Architect, which of the following would you suggest as the MOST optimized way of controlling access for this use-case?

○ Use Security Groups

○ Use Access Control Lists (ACLs)

● Use Amazon S3 Bucket Policies ✓

○ Use Identity and Access Management (IAM) policies

✓ 8. A social photo-sharing web application is hosted on Amazon Elastic Compute Cloud (Amazon EC2) instances behind an Elastic Load Balancer. The app gives the users the ability to upload their photos and also shows a leaderboard on the homepage of the app. The uploaded photos are stored in Amazon Simple Storage Service (Amazon S3) and the leaderboard data is maintained in Amazon DynamoDB. The Amazon EC2 instances need to access both Amazon S3 and Amazon DynamoDB for these features. *1/1

As a solutions architect, which of the following solutions would you recommend as the MOST secure option?

○ Save the AWS credentials (access key Id and secret access token) in a configuration file within the application code on the Amazon EC2 instances. Amazon EC2 instances can use these credentials to access Amazon S3 and Amazon DynamoDB

● Attach the appropriate IAM role to the Amazon EC2 instance profile so that the instance can access Amazon S3 and Amazon DynamoDB ✓

○ Configure AWS CLI on the Amazon EC2 instances using a valid IAM user's credentials. The application code can then invoke shell scripts to access Amazon S3 and Amazon DynamoDB via AWS CLI

○ Encrypt the AWS credentials via a custom encryption library and save it in a secret directory on the Amazon EC2 instances. The application code can then safely decrypt the AWS credentials to make the API calls to Amazon S3 and Amazon DynamoDB

✓ 9. You have a team of developers in your company, and you would like to ensure they can quickly experiment with AWS Managed Policies by attaching them to their accounts, but you would like to prevent them from doing an escalation of privileges, by granting themselves the AdministratorAccess managed policy. How should you proceed? *1/1

● For each developer, define an IAM permission boundary that will restrict the managed policies they can attach to themselves ✓

○ Put the developers into an IAM group, and then define an IAM permission boundary on the group that will restrict the managed policies they can attach to themselves

○ Create a Service Control Policy (SCP) on your AWS account that restricts developers from attaching themselves the AdministratorAccess policy

○ Attach an IAM policy to your developers, that prevents them from attaching the AdministratorAccess policy

✓ 10. Consider the following policy associated with an IAM group containing several users.
Which of the following options is correct? *1/1

```
{
    "Version":"2012-10-17",
    "Id":"EC2TerminationPolicy",
    "Statement":[
        {
            "Effect":"Deny",
            "Action":"ec2:*",
            "Resource":"*",
            "Condition":{
                "StringNotEquals":{
                    "ec2:Region":"us-west-1"
                }
            }
        },
        {
            "Effect":"Allow",
            "Action":"ec2:TerminateInstances",
            "Resource":"*",
            "Condition":{
                "IpAddress":{
                    "aws:SourceIp":"10.200.200.0/24"
                }
            }
        }
    ]
}
```

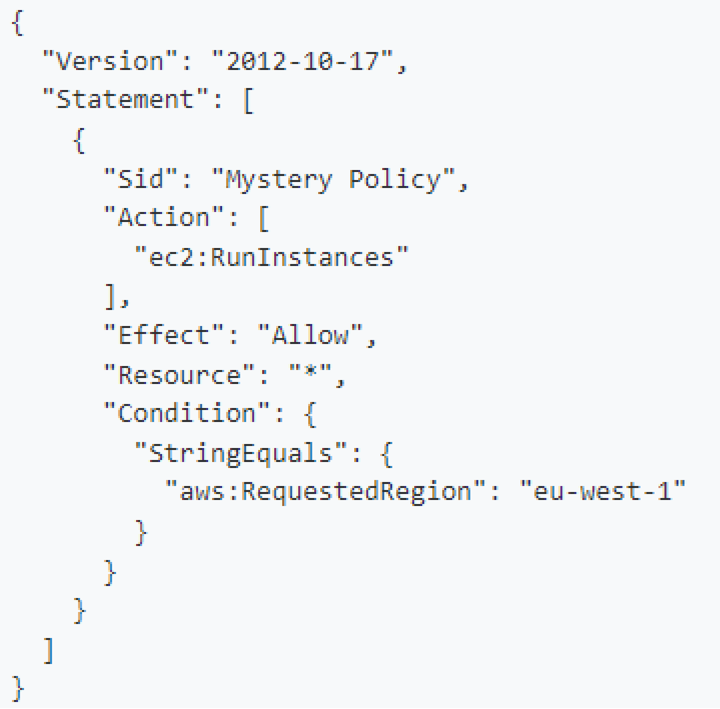
○ Users belonging to the IAM user group can terminate an Amazon EC2 instance belonging to any region except the us-west-1 region when the user's source IP is 10.200.200.200

● Users belonging to the IAM user group can terminate an Amazon EC2 instance in the us-west-1 region when the user's source IP is 10.200.200.200 ✓

○ Users belonging to the IAM user group cannot terminate an Amazon EC2 instance in the us-west-1 region when the user's source IP is 10.200.200.200

○ Users belonging to the IAM user group can terminate an Amazon EC2 instance in the us-west-1 region when the EC2 instance's IP address is 10.200.200.200

✓ 11. What does this IAM policy do? * 1/1



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Mystery Policy",
      "Action": [
        "ec2:RunInstances"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "eu-west-1"
        }
      }
    }
  ]
}
```

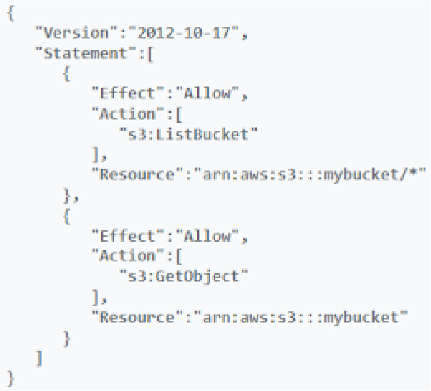
○ It allows running Amazon EC2 instances in any region when the API call is originating from the eu-west-1 region

○ It allows running Amazon EC2 instances in the eu-west-1 region, when the API call is made from the eu-west-1 region

○ It allows running Amazon EC2 instances anywhere but in the eu-west-1 region

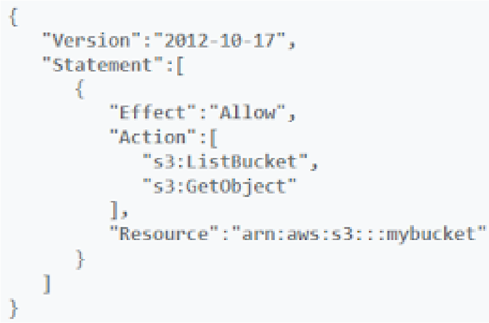
● It allows running Amazon EC2 instances only in the eu-west-1 region, and the API call can be made from anywhere in the world ✓

✓ 12. Which of the following IAM policies provides read-only access to the Amazon S3 bucket mybucket and its content? *1/1



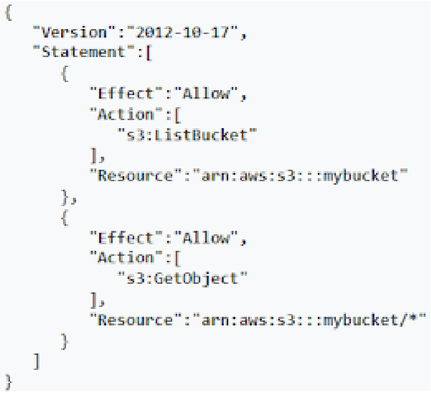
```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket"
         ],
         "Resource":"arn:aws:s3:::mybucket/*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":"arn:aws:s3:::mybucket"
      }
   ]
}
```

○ Option 1



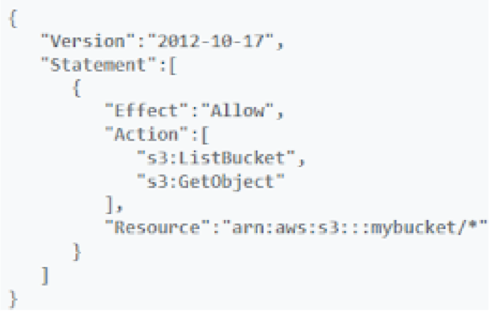
```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetObject"
         ],
         "Resource":"arn:aws:s3:::mybucket"
      }
   ]
}
```

○ Option 2



```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket"
         ],
         "Resource":"arn:aws:s3:::mybucket"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":"arn:aws:s3:::mybucket/*"
      }
   ]
}
```

● Option 3 ✓



```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetObject"
         ],
         "Resource":"arn:aws:s3:::mybucket/*"
      }
   ]
}
```

○ Option 4

✓ 13. A company runs a popular dating website on the AWS Cloud. As a Solutions Architect, you've designed the architecture of the website to follow a serverless pattern on the AWS Cloud using API Gateway and AWS Lambda. The backend uses an RDS PostgreSQL database. Currently, the application uses a username and password combination to connect the Lambda function to the RDS database. *1/1

You would like to improve the security at the authentication level by leveraging short-lived credentials. What will you choose? (Select two)

- ☑ Attach an AWS Identity and Access Management (IAM) role to AWS Lambda ✓
- □ Restrict the RDS database security group to the Lambda's security group
- ☑ Use IAM authentication from Lambda to RDS PostgreSQL ✓
- □ Embed a credential rotation logic in the AWS Lambda, retrieving them from SSM
- □ Deploy AWS Lambda in a VPC

✓ 14. You started a new job as a solutions architect at a company that has both AWS experts and people learning AWS. Recently, a developer misconfigured a newly created RDS database which resulted in a production outage. *1/1

How can you ensure that RDS specific best practices are incorporated into a reusable infrastructure template to be used by all your AWS users? (Select Two)

- ☑ Attach an IAM policy to interns preventing them from creating an RDS database ✓
- □ Create a Lambda function which sends emails when it finds misconfigured RDS databases
- □ Store your recommendations in a custom Trusted Advisor rule
- ☑ Use CloudFormation to manage RDS databases ✓

✓ 15. A DevOps engineer at an IT company was recently added to the admin group of the company's AWS account.
The **AdministratorAccess** managed policy is attached to this group.
Can you identify the AWS tasks that the DevOps engineer CANNOT perform even though he has full Administrator privileges (Select two)? *1/1

☐ Delete an S3 bucket from the production environment

☐ Delete the IAM user for his manager

☐ Change the password for his own IAM user account

☑ Configure an Amazon S3 bucket to enable MFA (Multi Factor Authentication) delete ✓

☑ Close the company's AWS account ✓

✓ 16. A team has around 200 users, each of these having an IAM user account in AWS. Currently, they all have read access to an Amazon S3 bucket. The team wants 50 among them to have write and read access to the buckets. *1/1

How can you provide these users access in the least possible time, with minimal changes?

○ Create a policy and assign it manually to the 50 users

○ Create an AWS Multi-Factor Authentication (AWS MFA) user with read / write access and link 50 IAM with AWS MFA

○ Update the Amazon S3 bucket policy

● Create a group, attach the policy to the group and place the users in the group ✓

✓ 17. A company has moved its business critical data to Amazon Elastic File System (Amazon EFS) which will be accessed by multiple Amazon EC2 instances. *1/1

As an AWS Certified Solutions Architect - Associate, which of the following would you recommend to exercise access control such that only the permitted Amazon EC2 instances can read from the Amazon EFS file system? (Select two)

☑ Set up the IAM policy root credentials to control and configure the clients accessing the Amazon EFS file system ✓

□ Use Amazon GuardDuty to curb unwanted access to Amazon EFS file system

□ Use network access control list (network ACL) to control the network traffic to and from your Amazon EC2 instance

☑ Use an IAM policy to control access for clients who can mount your file system with the required permissions ✓

□ Use VPC security groups to control the network traffic to and from your file system

✓ 18. An application running on an Amazon EC2 instance needs to access a Amazon DynamoDB table in the same AWS account. * 1/1

Which of the following solutions should a solutions architect configure for the necessary permissions?

○ Set up an IAM user with the appropriate permissions to allow access to the Amazon DynamoDB table. Store the access credentials in the local storage and read them from within the application code directly

○ Set up an IAM user with the appropriate permissions to allow access to the Amazon DynamoDB table. Store the access credentials in an Amazon S3 bucket and read them from within the application code directly

○ Set up an IAM service role with the appropriate permissions to allow access to the Amazon DynamoDB table. Add the Amazon EC2 instance to the trust relationship policy document so that the instance can assume the role

● Set up an IAM service role with the appropriate permissions to allow access to the Amazon DynamoDB table. Configure an instance profile to assign this IAM role to the Amazon EC2 instance ✓

✗ 19. A company is implementing a new business application. The application runs on two Amazon EC2 instances and uses an Amazon S3 bucket for document storage. A solutions architect needs to ensure that the EC2 instances can access the S3 bucket. What should the solutions architect do to meet this requirement? *0/1

○ Create an IAM role that grants access to the S3 bucket. Attach the role to the EC2 instances.

● Create an IAM policy that grants access to the S3 bucket. Attach the policy to the EC2 instances. ✗

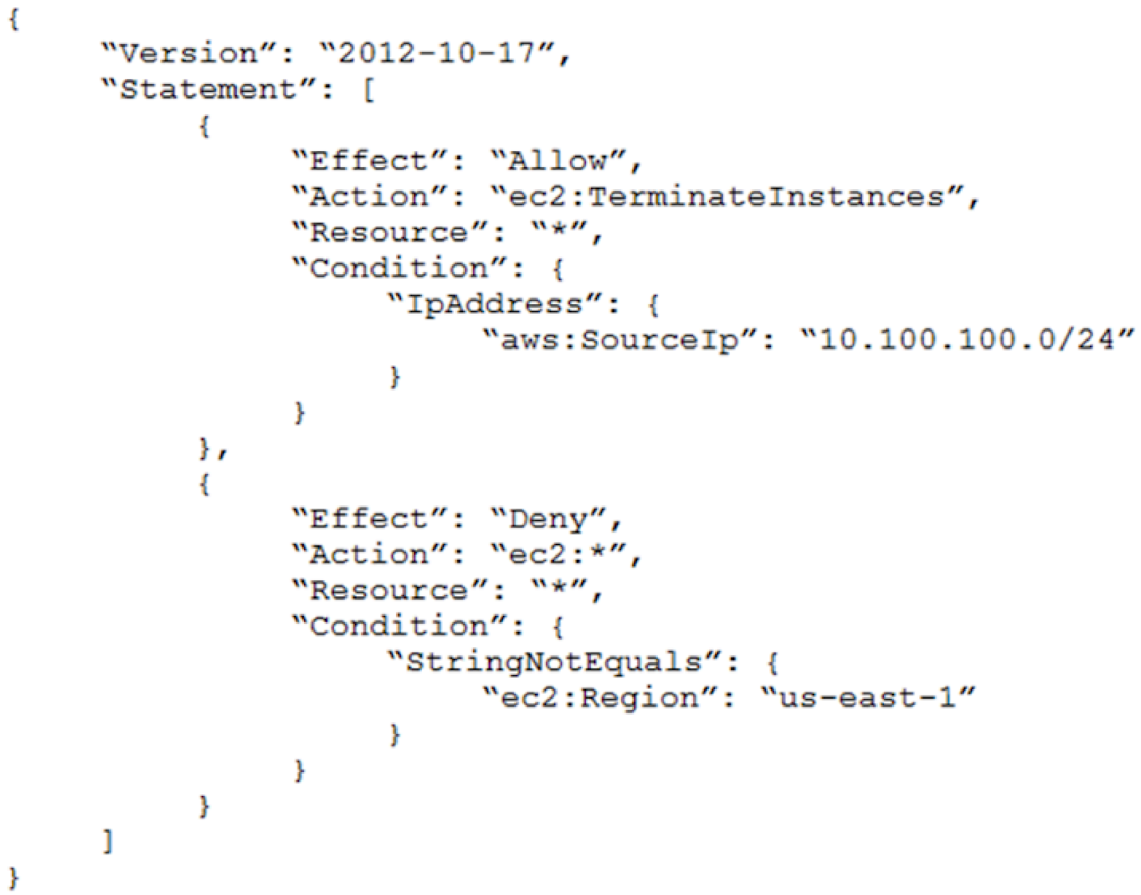
○ Create an IAM group that grants access to the S3 bucket. Attach the group to the EC2 instances.

○ Create an IAM user that grants access to the S3 bucket. Attach the user account to the EC2 instances.

Correct answer

● Create an IAM role that grants access to the S3 bucket. Attach the role to the EC2 instances.

✓ 20. An Amazon EC2 administrator created the following policy associated with an IAM group containing several users. What is the effect of this policy? *1/1



```
{
     “Version”: “2012-10-17”,
     “Statement”: [
          {
               “Effect”: “Allow”,
               “Action”: “ec2:TerminateInstances”,
               “Resource”: “*”,
               “Condition”: {
                    “IpAddress”: {
                         “aws:SourceIp”: “10.100.100.0/24”
                    }
               }
          },
          {
               “Effect”: “Deny”,
               “Action”: “ec2:*”,
               “Resource”: “*”,
               “Condition”: {
                    “StringNotEquals”: {
                         “ec2:Region”: “us-east-1”
                    }
               }
          }
     ]
}
```

○ Users can terminate an EC2 instance in any AWS Region except us-east-1.

○ Users can terminate an EC2 instance with the IP address 10.100.100.1 in the us-east-1 Region.

● Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254. ✓

○ Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.