**QUESTION 79**

A new employee has joined a company as a deployment engineer.

The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources.

A solutions architect wants the deployment engineer to perform job activities while following the principle of least privilege.

Which steps should the solutions architect do in conjunction to reach this goal? (Select TWO)

1. Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.
2. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.
3. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the Administrate/Access IAM policy attached.
4. Create a new IAM User for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.
5. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using Dial IAM role.

**Answer:** DE

**Explanation:**

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html>

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html>

**QUESTION 117**

A company wants to move from many standalone AWS accounts to a consolidated, multi-account architecture.

The company plans to create many new AWS accounts for different business units.

The company needs to authenticate access to these AWS accounts by using a centralized corporate directory service.

Which combination of actions should a solutions architect recommend to meet these requirements? (Select TWO)

1. Create a new organization in AWS Organizations with all features turned on.

Create the new AWS accounts in the organization.

1. Set up an Amazon Cognito identity pool.

Configure AWS Single Sign-On to accept Amazon Cognito authentication.

1. Configure a service control policy (SCP) to manage the AWS accounts.

Add AWS Single Sign-On to AWS Directory Service.

1. Create a new organization in AWS Organizations.

Configure the organization's authentication mechanism to use AWS Directory Service directly.

1. Set up AWS Single Sign-On (AWS SSO) in the organization.

Configure AWS SSO and integrate it with the company's corporate directory service.

**Answer:** BC

**Explanation:**

SCPs affect only IAM users and roles that are managed by accounts that are part of the organization. SCPs don't affect resource-based policies directly. They also don't affect users or roles from accounts outside the organization. For example, consider an Amazon S3 bucket that's owned by account A in an organization. The bucket policy (a resource-based policy) grants access to users from account B outside the organization. Account A has an SCP attached. That SCP doesn't apply to those outside users in account B. The SCP applies only to users that are managed by account A in the organization.

An SCP restricts permissions for IAM users and roles in member accounts, including the member account's root user. Any account has only those permissions permitted by every parent above it. If a permission is blocked at any level above the account, either implicitly (by not being included in an Allow policy statement) or explicitly (by being included in a Deny policy statement), a user or role in the affected account can't use that permission, even if the account administrator attaches the AdministratorAccess IAM policy with \*/\* permissions to the user.

Reference:

<https://aws.amazon.com/cognito/>

<https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html>

**QUESTION 130**

A company is running a popular social media website.

The website gives users the ability to upload images to share with other users.

The company wants to make sure that the images do not contain inappropriate content.

The company needs a solution that minimizes development effort.

What should a solutions architect do to meet these requirements?

1. Use Amazon Comprehend to detect inappropriate content.

Use human review for lowconfidence predictions.

1. Use Amazon Rekognition to detect inappropriate content.

Use human review for low-confidence predictions.

1. Use Amazon SageMaker to detect inappropriate content.

Use ground truth to label lowconfidence predictions.

1. Use AWS Fargate to deploy a custom machine learning model to detect inappropriate content. Use ground truth to label low-confidence predictions.

**Answer:** B

**QUESTION 142**

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?

1. Create an IAM role that grants access to the S3 bucket.

Attach the role to the EC2 instances.

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

1. Create an IAM group that grants access to the S3 bucket. Attach the group to the EC2 instances.
2. Create an IAM user that grants access to the S3 bucket.

Attach the user account to the EC2 instances.

**Answer:** A

**QUESTION 201**

A company uses AWS Organizations to create dedicated AWS accounts for each business unit to manage each business unit's account independently upon request.

The root email recipient missed a notification that was sent to the root user email address of one account.

The company wants to ensure that all future notifications are not missed.

Future notifications must be limited to account administrators.

Which solution will meet these requirements?

1. Configure the company's email server to forward notification email messages that are sent to the AWS account root user email address to all users in the organization.

1. Configure all AWS account root user email addresses as distribution lists that go to a few administrators who can respond to alerts. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.
2. Configure all AWS account root user email messages to be sent to one administrator who is responsible for monitoring alerts and forwarding those alerts to the appropriate groups.
3. Configure all existing AWS accounts and all newly created accounts to use the same root user email address.

Configure AWS account alternate contacts in the AWS Organizations console or programmatically.

**Answer:** D

**QUESTION 156**

An Amazon EC2 administrator created the following policy associated with an IAM group containing several users.



What is the effect of this policy?

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

1. Users can terminate an EC2 instance with the IP address 10 100 100 1 in the us-east-1 Region.
2. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is

10.100.100.254

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

10.100 100 254

**Answer:** C

**Explanation:** as the policy prevents anyone from doing any EC2 action on any region except us-east-1 and allows only users with source ip 10.100.100.0/24 to terminate instances. So user with source ip 10.100.100.254 can terminate instances in us-east-1 region.