Free Questions for SCS-C02 by go4braindumps

Shared by Washington on 12-09-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company needs to follow security best practices to deploy resources from an AWS CloudFormation template. The CloudFormation template must be able to configure sensitive database credentials.

The company already uses AWS Key Management Service (AWS KMS) and AWS Secrets Manager.

Which solution will meet the requirements?

Options:

A- Use a dynamic reference in the CloudFormation template to reference the database credentials in Secrets Manager.

B- Use a parameter in the CloudFormation template to reference the database credentials. Encrypt the CloudFormation template by using AWS KMS.

C- Use a SecureString parameter in the CloudFormation template to reference the database credentials in Secrets Manager.

D- Use a SecureString parameter in the CloudFormation template to reference an encrypted value in AWS KMS

Answer:

A

Question 2

Question Type: MultipleChoice

A company uses Amazon Elastic Container Service (Amazon ECS) containers that have the Fargate launch type. The containers run web and mobile applications that are written in Java and Node.js. To meet network segmentation requirements, each of the company's business units deploys applications in its own dedicated AWS account.

Each business unit stores container images in an Amazon Elastic Container Registry (Amazon ECR) private registry in its own account.

A security engineer must recommend a solution to scan ECS containers and ECR registries for vulnerabilities in operating systems and programming language libraries.

The company's audit team must be able to identify potential vulnerabilities that exist in any of the accounts where applications are deployed.

Which solution will meet these requirements?

Options:

A- In each account, update the ECR registry to use Amazon Inspector instead of the default scanning service. Configure Amazon Inspector to forward
vulnerability findings to AWS Security Hub in a central security account. Provide access for the audit team to use Security Hub to review the findings.

B- In each account, configure AWS Config to monitor the configuration of the ECS containers and the ECR registry. Configure AWS

Config conformance packs for
vulnerability scanning. Create an AWS Config aggregator in a central account to collect configuration and compliance details from all accounts. Provide the
audit team with access to AWS Config in the account where the aggregator is configured.

C- In each account, configure AWS Audit Manager to scan the ECS containers and the ECR registry. Configure Audit Manager to forward vulnerability findings to
AWS Security Hub in a central security account. Provide access for the audit team to use Security Hub to review the findings.

D- In each account, configure Amazon GuardDuty to scan the ECS containers and the ECR registry. Configure GuardDuty to forward vulnerability findings to AWS Security Hub in a central security account. Provide access for the audit team to use Security Hub to review the findings.

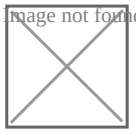
Answer:

B

Question 3

Question Type: MultipleChoice

A security engineer is designing an IAM policy to protect AWS API operations. The policy must enforce multi-factor authentication (MFA) for IAM users to access certain services in the AWS production account. Each session must remain valid for only 2 hours. The current version of the IAM policy is as follows:



Which combination of conditions must the security engineer add to the IAM policy to meet these requirements? (Select TWO.)

Options:

A- 'Bool ' : ' aws : Multi FactorAuthPresent': 'true' }

B- 'B001 ' : ' aws : MultiFactorAuthPresent': 'false' }

C- 'NumericLessThan' : { ' aws : Multi FactorAuthAge' : '7200'}

D- 'NumericGreaterThan' : { ' aws : MultiFactorAuthAge ' : '7200'

E- 'NumericLessThan' : { 'MaxSessionDuration ' : '7200'}

Answer:

A, C

Question 4

Question Type: MultipleChoice

A company wants to receive an email notification about critical findings in AWS Security Hub. The company does not have an existing architecture that supports this functionality.

Which solution will meet the requirement?

Options:

A- Create an AWS Lambda function to identify critical Security Hub findings. Create an Amazon Simple Notification Service (Amazon SNS) topic as the target of the Lambda function. Subscribe an email endpoint to the SNS topic to receive published messages.

B- Create an Amazon Kinesis Data Firehose delivery stream. Integrate the delivery stream with Amazon EventBridge. Create an EventBridge rule that has a filter to detect critical Security Hub findings. Configure the delivery stream to send the findings to an email address.

C- Create an Amazon EventBridge rule to detect critical Security Hub findings. Create an Amazon Simple Notification Service (Amazon SNS) topic as the target of the EventBridge rule. Subscribe an email endpoint to the SNS topic to receive published messages.

D- Create an Amazon EventBridge rule to detect critical Security Hub findings. Create an Amazon Simple Email Service (Amazon SES) topic as the target of the EventBridge rule. Use the Amazon SES API to format the message. Choose an email address to be the recipient of the message.

Answer:

C

Question 5

Question Type: MultipleChoice

A company has recently recovered from a security incident that required the restoration of Amazon EC2 instances from snapshots. The company uses an AWS Key

Management Service (AWS KMS) customer managed key to encrypt all Amazon Elastic Block Store (Amazon EBS) snapshots.

The company performs a gap analysis of its disaster recovery procedures and backup strategies. A security engineer needs to implement a solution so that the company can recover the EC2 instances if the AWS account is compromised and the EBS snapshots are deleted.

Which solution will meet this requirement?

Options:

A- Create a new Amazon S3 bucket. Use EBS lifecycle policies to move EBS snapshots to the new S3 bucket. Use lifecycle policies to move snapshots to the S3
Glacier Instant Retrieval storage class. Use S3 Object Lock to prevent deletion of the snapshots.

B- Use AWS Systems Manager to distribute a configuration that backs up all attached disks to Amazon S3.

C- Create a new AWS account that has limited privileges. Allow the new account to access the KMS key that encrypts the EBS snapshots. Copy the encrypted
snapshots to the new account on a recurring basis.

D- Use AWS Backup to copy EBS snapshots to Amazon S3. Use S3 Object Lock to prevent deletion of the snapshots.

Answer:

C

Question 6

Question Type: MultipleChoice

A security engineer is designing a cloud architecture to support an application. The application runs on Amazon EC2 instances and processes sensitive information, including credit card numbers.

The application will send the credit card numbers to a component that is running in an isolated environment. The component will encrypt, store, and decrypt the numbers.

The component then will issue tokens to replace the numbers in other parts of the application.

The component of the application that manages the tokenization process will be deployed on a separate set of EC2 instances. Other components of the application must not be able to store or access the credit card numbers.

Which solution will meet these requirements?

Options:

A- Use EC2 Dedicated Instances for the tokenization component of the application.

B- Place the EC2 instances that manage the tokenization process into a partition placement group.

C- Create a separate VPC. Deploy new EC2 instances into the separate VPC to support the data tokenization.

D- Deploy the tokenization code onto AWS Nitro Enclaves that are hosted on EC2 instances.

Answer:

D

Question 7

Question Type: **MultipleChoice**

To meet regulatory requirements, a Security Engineer needs to implement an IAM policy that restricts the use of AWS services to the us-east-1 Region.

What policy should the Engineer implement?

A.

Image not found or type unknown

B.

Image not found or type unknown

C.

Image not found or type unknown

D.

Image not found or type unknown

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

C

Explanation:

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_deny-requested-region.html

Question 8

Question Type: MultipleChoice

A security engineer wants to use Amazon Simple Notification Service (Amazon SNS) to send email alerts to a company's security team for Amazon GuardDuty findings

that have a High severity level. The security engineer also wants to deliver these findings to a visualization tool for further examination.

Which solution will meet these requirements?

Options:

A- Set up GuardDuty to send notifications to an Amazon CloudWatch alarm with two targets in CloudWatch. From CloudWatch, stream the findings through
Amazon Kinesis Data Streams into an Amazon OpenSearch Service domain as the first target for delivery. Use Amazon QuickSight to visualize the findings.
Use OpenSearch queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for the CloudWatch
alarm. Use event pattern matching with an Amazon EventBridge event rule to send only High severity findings in the alerts.

B- Set up GuardDuty to send notifications to AWS CloudTrail with two targets in CloudTrail. From CloudTrail, stream the findings through Amazon Kinesis Data
Firehose into an Amazon OpenSearch Service domain as the first target for delivery. Use OpenSearch Dashboards to visualize the findings. Use
OpenSearch queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for CloudTrail. Use event
pattern matching with a CloudTrail event rule to send only High severity findings in the alerts.

C- Set up GuardDuty to send notifications to Amazon EventBridge with two targets. From EventBridge, stream the findings through Amazon Kinesis Data
Firehose into an Amazon OpenSearch Service domain as the first target for delivery. Use OpenSearch Dashboards to visualize the findings. Use
OpenSearch queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for EventBridge. Use event
pattern matching with an EventBridge event rule to send only High severity findings in the alerts.

D- Set up GuardDuty to send notifications to Amazon EventBridge with two targets. From EventBridge, stream the findings through Amazon Kinesis Data

Streams into an Amazon OpenSearch Service domain as the first target for delivery. Use Amazon QuickSight to visualize the findings. Use OpenSearch
queries for further analysis. Deliver email alerts to the security team by configuring an SNS topic as a second target for EventBridge. Use event pattern
matching with an EventBridge event rule to send only High severity findings in the alerts.

Answer:

C

Question 9

Question Type: MultipleChoice

A company has AWS accounts in an organization in AWS Organizations. The organization includes a dedicated security account.

All AWS account activity across all member accounts must be logged and reported to the dedicated security account. The company must retain all the activity logs in a secure storage location within the dedicated security account for 2 years. No changes or deletions of the logs are allowed.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Select TWO.)

Options:

A- In the dedicated security account, create an Amazon S3 bucket. Configure S3 Object Lock in compliance mode and a retention period of 2 years on the S3 bucket. Set the bucket policy to allow the organization's management account to write to the S3 bucket.

B- In the dedicated security account, create an Amazon S3 bucket. Configure S3 Object Lock in compliance mode and a retention period of 2 years on the S3 bucket. Set the bucket policy to allow the organization's member accounts to write to the S3 bucket.

C- In the dedicated security account, create an Amazon S3 bucket that has an S3 Lifecycle configuration that expires objects after 2 years. Set the bucket policy to allow the organization's member accounts to write to the S3 bucket.

D- Create an AWS Cloud Trail trail for the organization. Configure logs to be delivered to the logging Amazon S3 bucket in the dedicated security account.

E- Turn on AWS CloudTrail in each account. Configure logs to be delivered to an Amazon S3 bucket that is created in the organization's management account. Forward the logs to the S3 bucket in the dedicated security account by using AWS Lambda and Amazon Kinesis Data Firehose.

Answer:

B, D

Explanation:

The correct answer is B and D. In the dedicated security account, create an Amazon S3 bucket. Configure S3 Object Lock in compliance mode and a retention period of 2 years on the S3 bucket. Set the bucket policy to allow the organization's member accounts to write to the S3 bucket. Create an AWS CloudTrail trail for the organization. Configure logs to be delivered to the logging Amazon S3 bucket in

the dedicated security account.

According to the AWS documentation, AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

To use CloudTrail with multiple AWS accounts and regions, you need to enable AWS Organizations with all features enabled. This allows you to centrally manage your accounts and apply policies across your organization. You can also use CloudTrail as a service principal for AWS Organizations, which lets you create an organization trail that applies to all accounts in your organization. An organization trail logs events for all AWS Regions and delivers the log files to an S3 bucket that you specify.

To create an organization trail, you need to use an administrator account, such as the organization's management account or a delegated administrator account. You can then configure the trail to deliver logs to an S3 bucket in the dedicated security account. This will ensure that all account activity across all member accounts and regions is logged and reported to the security account.

According to the AWS documentation, Amazon S3 is an object storage service that offers scalability, data availability, security, and performance. You can use S3 to store and retrieve any amount of data from anywhere on the web. You can also use S3 features such as lifecycle management, encryption, versioning, and replication to optimize your storage.

To use S3 with CloudTrail logs, you need to create an S3 bucket in the dedicated security account that will store the logs from the organization trail. You can then configure S3 Object Lock on the bucket to prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. You can also enable compliance mode on the bucket, which prevents any user, including the root user in your account, from deleting or modifying a locked object until it reaches its retention date.

To set a retention period of 2 years on the S3 bucket, you need to create a default retention configuration for the bucket that specifies a retention mode (either governance or compliance) and a retention period (either a number of days or a date). You can then set the

bucket policy to allow the organization's member accounts to write to the S3 bucket. This will ensure that all logs are retained in a secure storage location within the security account for 2 years and no changes or deletions are allowed.

Option A is incorrect because setting the bucket policy to allow the organization's management account to write to the S3 bucket is not sufficient, as it will not grant access to the other member accounts in the organization.

Option C is incorrect because using an S3 Lifecycle configuration that expires objects after 2 years is not secure, as it will allow users to delete or modify objects before they expire.

Option E is incorrect because using Lambda and Kinesis Data Firehose to forward logs from one S3 bucket to another is not necessary, as CloudTrail can directly deliver logs to an S3 bucket in another account. It also introduces additional operational overhead and complexity.

Question 10

Question Type: MultipleChoice

An international company wants to combine AWS Security Hub findings across all the company's AWS Regions and from multiple accounts. In addition, the company

wants to create a centralized custom dashboard to correlate these findings with operational data for deeper analysis and insights. The company needs an analytics tool to search and visualize Security Hub findings.

Which combination of steps will meet these requirements? (Select THREE.)

Options:

A- Designate an AWS account as a delegated administrator for Security Hub. Publish events to Amazon CloudWatch from the delegated administrator account,
all member accounts, and required Regions that are enabled for Security Hub findings.

B- Designate an AWS account in an organization in AWS Organizations as a delegated administrator for Security Hub. Publish events to Amazon EventBridge
from the delegated administrator account, all member accounts, and required Regions that are enabled for Security Hub findings.

C- In each Region, create an Amazon EventBridge rule to deliver findings to an Amazon Kinesis data stream. Configure the Kinesis data streams to output the logs to a single Amazon S3 bucket.

D- In each Region, create an Amazon EventBridge rule to deliver findings to an Amazon Kinesis Data Firehose delivery stream. Configure the Kinesis Data Firehose delivery streams to deliver the logs to a single Amazon S3 bucket.

E- Use AWS Glue DataBrew to crawl the Amazon S3 bucket and build the schema. Use AWS Glue Data Catalog to query the data and create views to flatten nested attributes. Build Amazon QuickSight dashboards by using Amazon Athena.

F- Partition the Amazon S3 data. Use AWS Glue to crawl the S3 bucket and build the schema. Use Amazon Athena to query the data and create views to flatten nested attributes. Build Amazon QuickSight dashboards that use the Athena views.

Answer:

B, D, F

Explanation:

The correct answer is B, D, and F Designate an AWS account in an organization in AWS Organizations as a delegated administrator for Security Hub. Publish events to Amazon EventBridge from the delegated administrator account, all member accounts, and required Regions that are enabled for Security Hub findings. In each Region, create an Amazon EventBridge rule to deliver findings to an Amazon Kinesis Data Firehose delivery stream. Configure the Kinesis Data Firehose delivery streams to deliver the logs to a single Amazon S3 bucket. Partition the Amazon S3 data. Use AWS Glue to crawl the S3 bucket and build the schema. Use Amazon Athena to query the data and create views to flatten nested attributes. Build Amazon QuickSight dashboards that use the Athena views.

According to the AWS documentation, AWS Security Hub is a service that provides you with a comprehensive view of your security state across your AWS accounts, and helps you check your environment against security standards and best practices. You can use Security Hub to aggregate security findings from various sources, such as AWS services, partner products, or your own applications.

To use Security Hub with multiple AWS accounts and Regions, you need to enable AWS Organizations with all features enabled. This allows you to centrally manage your accounts and apply policies across your organization. You can also use Security Hub as a service principal for AWS Organizations, which lets you designate a delegated administrator account for Security Hub. The delegated administrator account can enable Security Hub automatically in all existing and future accounts in your organization, and can view and manage findings from all accounts.

According to the AWS documentation, Amazon EventBridge is a serverless event bus that makes it easy to connect applications using data from your own applications, integrated software as a service (SaaS) applications, and AWS services. You can use EventBridge to create rules that match events from various sources and route them to targets for processing.

To use EventBridge with Security Hub findings, you need to enable Security Hub as an event source in EventBridge. This will allow you to publish events from Security Hub to EventBridge in the same Region. You can then create EventBridge rules that match Security Hub findings based on criteria such as severity, type, or resource. You can also specify targets for your rules, such as Lambda functions, SNS topics, or Kinesis Data Firehose delivery streams.

According to the AWS documentation, Amazon Kinesis Data Firehose is a fully managed service that delivers real-time streaming data to destinations such as Amazon S3, Amazon Redshift, Amazon Elasticsearch Service (Amazon ES), and Splunk. You can use Kinesis Data Firehose to transform and enrich your data before delivering it to your destination.

To use Kinesis Data Firehose with Security Hub findings, you need to create a Kinesis Data Firehose delivery stream in each Region where you have enabled Security Hub. You can then configure the delivery stream to receive events from EventBridge as a source, and deliver the logs to a single S3 bucket as a destination. You can also enable data transformation or compression on the delivery stream if needed.

According to the AWS documentation, Amazon S3 is an object storage service that offers scalability, data availability, security, and performance. You can use S3 to store and retrieve any amount of data from anywhere on the web. You can also use S3 features such as lifecycle management, encryption, versioning, and replication to optimize your storage.

To use S3 with Security Hub findings, you need to create an S3 bucket that will store the logs from Kinesis Data Firehose delivery streams. You can then partition the data in the bucket by using prefixes such as account ID or Region. This will improve the performance and cost-effectiveness of querying the data.

According to the AWS documentation, AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy to prepare and load your data for analytics. You can use Glue to crawl your data sources, identify data formats, and suggest schemas and transformations. You can also use Glue Data Catalog as a central metadata repository for your data assets.

To use Glue with Security Hub findings, you need to create a Glue crawler that will crawl the S3 bucket and build the schema for the data. The crawler will create tables in the Glue Data Catalog that you can query using standard SQL.

According to the AWS documentation, Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run. You can use Athena with Glue Data Catalog as a metadata store for your tables.

To use Athena with Security Hub findings, you need to create views in Athena that will flatten nested attributes in the data. For example, you can create views that extract fields such as account ID, Region, resource type, resource ID, finding type, finding title, and finding description from the JSON data. You can then query the views using SQL and join them with other tables if needed.

According to the AWS documentation, Amazon QuickSight is a fast, cloud-powered business intelligence service that makes it easy to deliver insights to everyone in your organization. You can use QuickSight to create and publish interactive dashboards that include machine learning insights. You can also use QuickSight to connect to various data sources, such as Athena, S3, or RDS.

To use QuickSight with Security Hub findings, you need to create QuickSight dashboards that use the Athena views as data sources. You can then visualize and analyze the findings using charts, graphs, maps, or tables. You can also apply filters, calculations, or aggregations to the data. You can then share the dashboards with your users or embed them in your applications.

Question 11

Question Type: **MultipleChoice**

A security engineer needs to run an AWS CloudFormation script. The CloudFormation script builds AWS infrastructure to support a stack that includes web servers and a MySQL database. The stack has been deployed in pre-production environments and is ready for production.

The production script must comply with the principle of least privilege. Additionally, separation of duties must exist between the security engineer's IAM account and CloudFormation.

Which solution will meet these requirements?

Options:

A- Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stack. Attach the policy to a new
IAM role. Modify the security engineer's IAM permissions to be able to pass the new role to CloudFormation.

B- Create an IAM policy that allows ec2:* and rds:* permissions. Attach the policy to a new IAM role. Modify the security engineer's IAM permissions to be able to
assume the new role.

C- Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stack. Modify the security
engineer's IAM permissions to be able to run the CloudFormation script.

D- Create an IAM policy that allows ec2:* and rds:* permissions. Attach the policy to a new IAM role. Use the IAM policy simulator to confirm that the policy allows the AWS API calls that are necessary to build the stack. Modify the security engineer's IAM permissions to be able to pass the new role to CloudFormation.

Answer:

A

Explanation:

The correct answer is A) Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stack. Attach the policy to a new IAM role. Modify the security engineer's IAM permissions to be able to pass the new role to CloudFormation.

According to the AWS documentation, IAM Access Analyzer is a service that helps you identify the resources in your organization and accounts, such as Amazon S3 buckets or IAM roles, that are shared with an external entity. You can also use IAM Access Analyzer to generate fine-grained policies that grant least privilege access based on access activity and access attempts.

To use IAM Access Analyzer policy generation, you need to enable IAM Access Analyzer in your account or organization. You can then use the IAM console or the AWS CLI to generate a policy for a resource based on its access activity or access attempts. You can review and edit the generated policy before applying it to the resource.

To use IAM Access Analyzer policy generation with CloudFormation, you can follow these steps:

Run the CloudFormation script in a pre-production environment and monitor its access activity or access attempts using IAM Access Analyzer.

Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stack. The policy will include only the permissions that are necessary for the script to function.

Attach the policy to a new IAM role that has a trust relationship with CloudFormation. This will allow CloudFormation to assume the role and execute the script.

Modify the security engineer's IAM permissions to be able to pass the new role to CloudFormation. This will allow the security engineer to launch the stack using the role.

Run the CloudFormation script in the production environment using the new role.

This solution will meet the requirements of least privilege and separation of duties, as it will limit the permissions of both CloudFormation and the security engineer to only what is needed for running and managing the stack.

Option B is incorrect because creating an IAM policy that allows ec2:* and rds:* permissions is not following the principle of least privilege, as it will grant more permissions than necessary for running and managing the stack. Moreover, modifying the security engineer's IAM permissions to be able to assume the new role is not ensuring separation of duties, as it will allow the security engineer to bypass CloudFormation and directly access the resources.

Option C is incorrect because modifying the security engineer's IAM permissions to be able to run the CloudFormation script is not ensuring separation of duties, as it will allow the security engineer to execute the script without using CloudFormation.

Option D is incorrect because creating an IAM policy that allows ec2:* and rds:* permissions is not following the principle of least privilege, as it will grant more permissions than necessary for running and managing the stack. Using the IAM policy simulator to confirm that the policy allows the AWS API calls that are necessary to build the stack is not sufficient, as it will not generate a fine-grained policy based on access activity or access attempts.

Question 12

Question Type: MultipleChoice

A company is expanding its group of stores. On the day that each new store opens, the company wants to launch a customized web application for that store. Each store's application will have a non-production environment and a production environment. Each environment will be deployed in a separate AWS account. The company uses AWS Organizations and has an OU that is used only for

these accounts.

The company distributes most of the development work to third-party development teams. A security engineer needs to ensure that each team follows the company's

deployment plan for AWS resources. The security engineer also must limit access to the deployment plan to only the developers who need access. The security engineer already has created an AWS CloudFormation template that implements the deployment plan.

What should the security engineer do next to meet the requirements in the MOST secure way?

Options:

A- Create an AWS Service Catalog portfolio in the organization's management account. Upload the CloudFormation template. Add the template to the
portfolio's product list. Share the portfolio with the OIJ.

B- Use the CloudFormation CLI to create a module from the CloudFormation template. Register the module as a private extension in the CloudFormation
registry. Publish the extension. In the OU, create an SCP that allows access to the extension.

C- Create an AWS Service Catalog portfolio in the organization's management account. Upload the CloudFormation template. Add the template to the
portfolio's product list. Create an IAM role that has a trust policy that allows cross-account access to the portfolio for users in the OU accounts. Attach the
AWSServiceCatalogEndUserFullAccess managed policy to the role.

D- Use the CloudFormation CLI to create a module from the CloudFormation template. Register the module as a private extension in the

CloudFormation
registry. Publish the extension. Share the extension with the OU

Answer:

A

Explanation:

The correct answer is A. Create an AWS Service Catalog portfolio in the organization's management account. Upload the CloudFormation template. Add the template to the portfolio's product list. Share the portfolio with the OU.

According to the AWS documentation, AWS Service Catalog is a service that allows you to create and manage catalogs of IT services that are approved for use on AWS. You can use Service Catalog to centrally manage commonly deployed IT services and help achieve consistent governance and compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

To use Service Catalog with multiple AWS accounts, you need to enable AWS Organizations with all features enabled. This allows you to centrally manage your accounts and apply policies across your organization. You can also use Service Catalog as a service principal for AWS Organizations, which lets you share your portfolios with organizational units (OUs) or accounts in your organization.

To create a Service Catalog portfolio, you need to use an administrator account, such as the organization's management account. You can upload your CloudFormation template as a product in your portfolio, and define constraints and tags for it. You can then share your portfolio with the OU that contains the accounts for the web applications. This will allow the developers in those accounts to launch products from the shared portfolio using the Service Catalog end user console.

Option B is incorrect because CloudFormation modules are reusable components that encapsulate one or more resources and their configurations. They are not meant to be used as templates for deploying entire stacks of resources. Moreover, sharing a module with an OU does not grant access to launch stacks from it.

Option C is incorrect because creating an IAM role that has a trust policy that allows cross-account access to the portfolio is not secure. It would allow any user in the OU accounts to assume the role and access the portfolio, regardless of their job function or access requirements.

Option D is incorrect because sharing a module with an OU does not grant access to launch stacks from it. It also does not limit access to the deployment plan to only the developers who need access.