Free Questions for SCS-C02 by dumpssheet

Shared by Johns on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

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.

Question 2

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.

To Get Premium Files for SCS-C02 Visit

https://www.p2pexams.com/products/scs-c02

For More Free Questions Visit

https://www.p2pexams.com/amazon/pdf/scs-c02