VCE & PDF
GeekCert.com

B2C-SOLUTION-ARCHITECT^{Q&As}

Salesforce Certified B2C Solution Architect

Pass Salesforce B2C-SOLUTION-ARCHITECT Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/b2c-solution-architect.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Salesforce Official Exam Center

🌣 **Instant Download** After Purchase

🌣 **100% Money Back** Guarantee

🌣 **365 Days** Free Update

🌣 **800,000+** Satisfied Customers

QUESTION 1

A company uses B2C Commerce, Experience Cloud, and Marketing Cloud. Now the company wants to enable Social
Login with Facebook, Google, and Twitter to increase their conversion rates. Currently, Customer Identity is in use and
two types of accounts are available: Individual accounts and household accounts.

Which consideration should a Solution Architect keep in mind when configuring seamless cross-cloud identity?

A. The Commerce Cloud to Service Cloud connector supports both person account and contact accounts out-of-the-
box.

B. Commerce Cloud will be the system of record for customer shopping data, including individual profile and
authentication credentials.

C. Full access (full) scope will request access to all accessible data that the third-party provides.

D. To create the external authenticated profile in Commerce Cloud, Service Cloud will need to invoke a remote OAuth2
authentication request to Commerce Cloud.

Correct Answer: B

Product Catalogs are a type of data extension that contain product information for generating product recommendations
using Einstein in Marketing Cloud. Product Catalogs can be configured natively to sync from B2C Commerce to
Marketing Cloud using a point and click configuration in the Marketing Cloud Business Manager. References:
https://help.salesforce.com/s/articleView?id=sf.mc_pb_product_catalog.htmandtype=5
https://developer.salesforce.com/docs/commerce/sfra/marketing-cloud/marketing-cloud-integration

QUESTION 2

A company uses Marketing Cloud, Experience Cloud, B2C Commerce, and Service Cloud. It is in the process of
defining the authoritative system for key data entities involved in B2C Journeys. The company has about 200,000
customers, each averaging 30 orders per year

Which option should be considered the authoritative record for consent and compliance preferences, as well as primary
person attributes such as name, address, birthday, phone, and email?

A. Marketing Cloud subscriber

B. B2C Commerce customer

C. Experience Cloud user

D. Service Cloud contact

Correct Answer: D

Service Cloud contact should be considered the authoritative record for consent and compliance preferences, as well as
primary person attributes such as name, address, birthday, phone, and email. Service Cloud contact is the core entity
that represents a person across multiple Salesforce clouds and can store and manage the customer\'s consent and
compliance preferences using features like Individual object, Data Protection and Privacy, and Consent Management.
The other systems can use Service Cloud contact as the master record and sync or update the customer data
accordingly.

QUESTION 3

A company needs to have specific fields encrypted in the user interface on the contact record in Service Cloud as well as on some fields in data extensions that exist only in the Marketing Cloud. The merchant believes that Salesforce Shield Encryption is a suitable solution.

Which two considerations are relevant for the merchant when determining an appropriate solution?

Choose 2 answers

A. With Shield, encrypted fields are not visible to the user, but there are no other feature impacts.

B. With Shield, encrypted fields cannot be used to filter or sort in Process Builder and Flow Builder.

C. Field-Level Encryption is also required on Marketing Cloud to encrypt the custom fields.

D. Shield encryption can be done on any standard or custom field on all field types, but cannot be set to encrypt those fields in Marketing Cloud.

Correct Answer: BD

Salesforce Shield Encryption is a feature that allows encrypting sensitive data at rest in Salesforce without compromising functionality or performance. Shield Encryption uses probabilistic encryption to protect data while preserving its format and length. Field-Level Encryption is a feature in Marketing Cloud that allows encrypting sensitive data at rest in Marketing Cloud using customer-managed keys. Field-Level Encryption uses deterministic encryption to protect data while preserving its format and length. When determining an appropriate solution for encrypting specific fields in Service Cloud as well as in data extensions in Marketing Cloud, the following considerations are relevant: With Shield, encrypted fields cannot be used to filter or sort in Process Builder and Flow Builder. Process Builder and Flow Builder are tools in Salesforce that allow creating automated workflows and processes based on certain criteria or conditions. However, Shield Encryption does not support filtering or sorting on encrypted fields in these tools, because probabilistic encryption does not allow exact matching or comparison of values. Shield encryption can be done on any standard or custom field on all field types, but cannot be set to encrypt those fields in Marketing Cloud. Shield Encryption supports encrypting any standard or custom field on any field type in Salesforce, such as text, email, phone, date, etc. However, Shield Encryption does not apply to Marketing Cloud fields or data extensions, because they are stored in a separate database from Salesforce. To encrypt fields in Marketing Cloud, Field- Level Encryption must be used. Option A is incorrect because with Shield, encrypted fields are visible to the user if they have the View Encrypted Data permission, but there are other feature impacts such as filtering, sorting, searching, etc. Option C is incorrect because Field-Level Encryption is not required on Marketing Cloud to encrypt the custom fields if they are already encrypted by Shield Encryption in Service Cloud. However, Field-Level Encryption can be used on Marketing Cloud if additional encryption or customer-managed keys are needed. References:
https://help.salesforce.com/s/articleView?id=sf.security_pe_overview.htmandtype=5
https://help.salesforce.com/s/articleView?id=sf.security_pe_considerations_general.htmandtype=5
https://help.salesforce.com/s/articleView?id=sf.mc_overview_field_level_encryption.htmandtype=5

QUESTION 4

A company currently uses B2C Commerce and Service Cloud for one of its storefronts. They are now considering implementing the \\'Order on Behalf of flow. Which consideration must a Solution Architect keep in mind while implementing the \\'Order on Behalf of flow?

A. The Service Cloud Connector is not available for guests or anonymous storefront shoppers. Use Order on Behalf with registered B2C Commerce customer accounts.

B. The Service Cloud Connector enables data synchronization through SOAP services using Service Cloud and B2C Commerce. REST services are not available for such data synchronization needs.

C. The Service Cloud Connector does not require B2C Commerce to be registered as a remote site as long as the Service Cloud org and B2C Commerce realm are in the same geographic region.

D. The Service Cloud Connector can work with any valid Service Cloud user. There is no specific need for an Integration User with administrative rights.

Correct Answer: A

A is correct because the Service Cloud Connector only works with registered B2C Commerce customer accounts and does not support guests or anonymous storefront shoppers. The connector uses the customer ID to link the Service Cloud contact with the B2C Commerce customer profile. B is incorrect because the Service Cloud Connector supports both SOAP and REST services for data synchronization between Service Cloud and B2C Commerce. C is incorrect because the Service Cloud Connector requires B2C Commerce to be registered as a remote site in Service Cloud regardless of the geographic region. This is to allow outbound messages from Service Cloud to B2C Commerce. D is incorrect because the Service Cloud Connector requires a dedicated Integration User with administrative rights in both Service Cloud and B2C Commerce. This user is used to authenticate and authorize the data synchronization between the two systems. References: https://documentation.b2c.commercecloud.salesforce.com/DOC1/topic/com.demandware. dochelp/ServiceCloud/ServiceCloudConnectorOverview.html https://documentation.b2c.commercecloud.salesforce.com /DOC1/topic/com.demandware.dochelp/ServiceCloud/ServiceCloudConnectorDataSynchronization.html https://docume ntation.b2c.commercecloud.salesforce.com/DOC1/topic/com.demandware.dochelp/ServiceCloud/ServiceCloudConnect orSetup.html https://documentation.b2c.commercecloud.salesforce.com/DOC1/topic/com.demandware.dochelp/Service Cloud/ServiceCloudConnectorUserSetup.html

---

QUESTION 5

A university is considering using Experience Cloud so its students can interact with advisors who have Service Cloud licenses. The university would like to offer the easiest path for existing students to log in while still maintaining security.

They have an on- premises Active Directory identity provider and use Google Workspace (formerly known as G Suite) for student email addresses.

What should a Solution Architect recommend?

A. Implement Social Sign On with OpenId Connect and Google Workspace as Auth Provider.

B. Implement Active Directory and Salesforce Identity for SAML delegated Single Sign On.

C. Implement Aloha template for students to access email with Salesforce Authenticator app.

D. Implement OAuth 2.0 authentication protocol with Google Workspace as Service Provider.

Correct Answer: A

A is correct because implementing Social Sign On with OpenID Connect and Google Workspace as Auth Provider is a simple and secure way to allow existing students to log in to Experience Cloud using their Google Workspace credentials1. This also eliminates the need for creating and managing separate user accounts in Experience Cloud. B is incorrect because implementing Active Directory and Salesforce Identity for SAML delegated Single Sign On would require the university to set up and maintain a SAML identity provider and configure it with Salesforce Identity. This would be more complex and costly than using Social Sign On with Google Workspace2. C is incorrect because implementing Aloha template for students to access email with Salesforce Authenticator app would not meet the requirement of using the existing Google Workspace email addresses. Aloha template is a pre-built template for Experience Cloud that provides email functionality, but it does not integrate with Google Workspace3. Salesforce

Authenticator app is a mobile app that provides two-factor authentication, but it does not integrate with Google Workspace either. D is incorrect because implementing OAuth 2.0 authentication protocol with Google Workspace as Service Provider would not meet the requirement of using the easiest path for existing students to log in. OAuth 2.0 is a protocol that allows users to authorize third-party applications to access their data, but it does not provide authentication or single sign on functionality.

References:

1: https://help.salesforce.com/s/articleView?id=sf.networks_auth_provider_openid_connect.htmandtype=5

2: https://help.salesforce.com/s/articleView?id=sf.identity_provider_saml.htmandtype=5

3: https://help.salesforce.com/s/articleView?id=sf.networks_templates_aloha.htmandtype=5

4.

 https://help.salesforce.com/s/articleView?id=sf.security_authenticator_app.htmandtype=5

5.

 https://help.salesforce.com/s/articleView?id=sf.remoteaccess_oauth_web_server_flow.htmandtype=5

[B2C-SOLUTION-ARCHITECT PDF Dumps](#)   [B2C-SOLUTION-ARCHITECT Study Guide](#)   [B2C-SOLUTION-ARCHITECT Exam Questions](#)