



**Free Questions for Identity-and-Access-Management-Architect
by certsdeals**

Shared by Marsh on 27-07-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Universal Containers wants to secure its Salesforce APIs by using an existing Security Assertion Markup Language (SAML) configuration supports the company's single sign-on process to Salesforce,

Which Salesforce OAuth authorization flow should be used?

Options:

- A- OAuth 2.0 SAML Bearer Assertion Flow
- B- A SAML Assertion Row
- C- OAuth 2.0 User-Agent Flow
- D- OAuth 2.0 JWT Bearer Flow

Answer:

B

Question 2

Question Type: MultipleChoice

An identity architect's client has a homegrown identity provider (IdP). Salesforce is used as the service provider (SP). The head of IT is worried that during a SP initiated single sign-on (SSO), the Security Assertion Markup Language (SAML) request content will be altered.

What should the identity architect recommend to make sure that there is additional trust between the SP and the IdP?

Options:

- A-** Ensure that there is an HTTPS connection between IDP and SP.
- B-** Ensure that on the SSO settings page, the 'Request Signing Certificate' field has a self-signed certificate.
- C-** Ensure that the Issuer and Assertion Consumer service (ACS) URL is property configured between SP and IDP.
- D-** Encrypt the SAML Request using certification authority (CA) signed certificate and decrypt on IdP.

Answer:

D

Question 3

Question Type: MultipleChoice

A public sector agency is setting up an identity solution for its citizens using a Community built on Experience Cloud and requires the new user registration functionality to capture first name, last name, and phone number. The phone number will be used for identity verification.

Which feature should an identity architect recommend to meet the requirements?

Options:

- A- Integrate with social websites (Facebook, LinkedIn, Twitter)
- B- Use an external Identity Provider
- C- Create a custom Lightning Web Component
- D- Use Login Discovery

Answer:

D

Question 4

Question Type: MultipleChoice

Northern Trail Outfitters would like to use a portal built on Salesforce Experience Cloud for customer self-service. Guests of the portal be able to self-register, but be unable to automatically be assigned to a contact record until verified. External Identity licenses have been purchased for the project.

After registered guests complete an onboarding process, a flow will create the appropriate account and contact records for the user.

Which three steps should an identity architect follow to implement the outlined requirements?

Choose 3 answers

Options:

- A-** Enable 'Allow customers and partners to self-register'.
- B-** Select the 'Configurable Self-Reg Page' option under Login & Registration.
- C-** Set up an external login page and call Salesforce APIs for user creation.
- D-** Customize the self-registration Apex handler to temporarily associate the user to a shared single contact record.
- E-** Customize the self-registration Apex handler to create only the user record.

Answer:

A, B, E

Question 5

Question Type: MultipleChoice

Northern Trail Outfitters (NTO) believes a specific user account may have been compromised. NTO inactivated the user account and needs U perform a forensic analysis and identify signals that could indicate a breach has occurred.

What should NTO's first step be in gathering signals that could indicate account compromise?

Options:

- A- Review the User record and evaluate the login and transaction history.
- B- Download the Setup Audit Trail and review all recent activities performed by the user.
- C- Download the Identity Provider Event Log and evaluate the details of activities performed by the user.
- D- Download the Login History and evaluate the details of logins performed by the user.

Answer:

D

Question 6

Question Type: MultipleChoice

When designing a multi-branded Customer Identity and Access Management solution on the Salesforce Platform, how should an identity architect ensure a specific brand experience in Salesforce is presented?

Options:

- A-** The Experience ID, which can be included in OAuth/Open ID flows and Security Assertion Markup Language (SAML) flows as a URL parameter.
- B-** Provide a brand picker that the end user can use to select its sub-brand when they arrive on salesforce.
- C-** Add a custom parameter to the service provider's OAuth/SAML call and implement logic on its login page to apply branding based on the parameters value.
- D-** The Audience ID, which can be set in a shared cookie.

Answer:

A

Question 7

Question Type: MultipleChoice

Northern Trail Outfitters (NTO) has an off-boarding process where a terminated employee is first disabled in the Lightweight Directory Act Protocol (LDAP) directory, then requests are sent to the various application support teams to finish user deactivations. A terminated employee recently was able to login to NTO's Salesforce instance 24 hours after termination, even though the user was disabled in the corporate LDAP directory.

What should an identity architect recommend to prevent this from happening in the future?

Options:

- A-** Create a Just-in-Time provisioning registration handler to ensure users are deactivated in Salesforce as they are disabled in LDAP.
- B-** Configure an authentication provider to delegate authentication to the LDAP directory.
- C-** use a login flow to make a callout to the LDAP directory before authenticating the user to Salesforce.
- D-** Setup an identity provider (IdP) to authenticate users using LDAP, set up single sign-on to Salesforce and disable Login Form authentication.

Answer:

B

To Get Premium Files for Identity-and-Access-Management-Architect Visit

<https://www.p2pexams.com/products/identity-and-access-management-architect>

For More Free Questions Visit

<https://www.p2pexams.com/salesforce/pdf/identity-and-access-management-architect>

