



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

Shared by Peterson on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Northern Trail Outfitters (NTO) is setting up Salesforce to authenticate users with an external identity provider. The NTO Salesforce Administrator is having trouble getting things setup.

What should an identity architect use to show which part of the login assertion is fading?

Options:

- A- SAML Metadata file importer
- B- Identity Provider Metadata download
- C- Connected App Manager
- D- Security Assertion Markup Language Validator

Answer:

D

Question 2

Question Type: MultipleChoice

Universal Containers (UC) currently uses Salesforce Sales Cloud and an external billing application. Both Salesforce and the billing application are accessed several times a day to manage customers. UC would like to configure single sign-on and leverage Salesforce as the identity provider. Additionally, UC would like the billing application to be accessible from Salesforce. A redirect is acceptable.

Which two Salesforce tools should an identity architect recommend to satisfy the requirements?

Choose 2 answers

Options:

- A- salesforce Canvas
- B- Identity Connect
- C- Connected Apps
- D- App Launcher

Answer:

A, D

Question 3

Question Type: MultipleChoice

Universal Container's (UC) is using Salesforce Experience Cloud site for its container wholesale business. The identity architect wants to an authentication provider for the new site.

Which two options should be utilized in creating an authentication provider?

Choose 2 answers

Options:

- A- A custom registration handler can be set.
- B- A custom error URL can be set.
- C- The default login user can be set.
- D- The default authentication provider certificate can be set.

Answer:

A, B

Question 4

Question Type: MultipleChoice

Northern Trail Outfitters (NTO) leverages Microsoft Active Directory (AD) for management of employee usernames, passwords, permissions, and asset access. NTO also owns a third-party single sign-on (SSO) solution. The third-party SSO solution is used for all corporate applications, including Salesforce.

NTO has asked an architect to explore Salesforce Identity Connect for automatic provisioning and deprovisioning of users in Salesforce.

What role does identity Connect play in the outlined requirements?

Options:

- A- Service Provider
- B- Single Sign-On
- C- Identity Provider
- D- User Management

Answer:

D

Question 5

Question Type: MultipleChoice

An identity architect is implementing a mobile-first Consumer Identity Access Management (CIAM) for external users. User authentication is the only requirement. The users email or mobile phone number should be supported as a username.

Which two licenses are needed to meet this requirement?

Choose 2 answers

Options:

- A- External Identity Licenses
- B- Identity Connect Licenses
- C- Email Verification Credits
- D- SMS verification Credits

Answer:

A, D

Question 6

Question Type: MultipleChoice

The executive sponsor for an organization has asked if Salesforce supports the ability to embed a login widget into its service providers in order to create a more seamless user experience.

What should be used and considered before recommending it as a solution on the Salesforce Platform?

Options:

- A-** OpenID Connect Web Server Flow. Determine if the service provider is secure enough to store the client secret on.
- B-** Embedded Login. Identify what level of UI customization will be required to make it match the service providers look and feel.
- C-** Salesforce REST apis. Ensure that Secure Sockets Layer (SSL) connection for the integration is used.
- D-** Embedded Login. Consider whether or not it relies on third party cookies which can cause browser compatibility issues.

Answer:

D

Question 7

Question Type: MultipleChoice

A global company has built an external application that uses data from its Salesforce org via an OAuth 2.0 authorization flow. Upon logout, the existing Salesforce OAuth token must be invalidated.

Which action will accomplish this?

Options:

- A-** Use a HTTP POST to request the refresh token for the current user.
- B-** Use a HTTP POST to the System for Cross-domain Identity Management (SCIM) endpoint, including the current OAuth token.
- C-** Use a HTTP POST to make a call to the revoke token endpoint.
- D-** Enable Single Logout with a secure logout URL.

Answer:

C

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>

