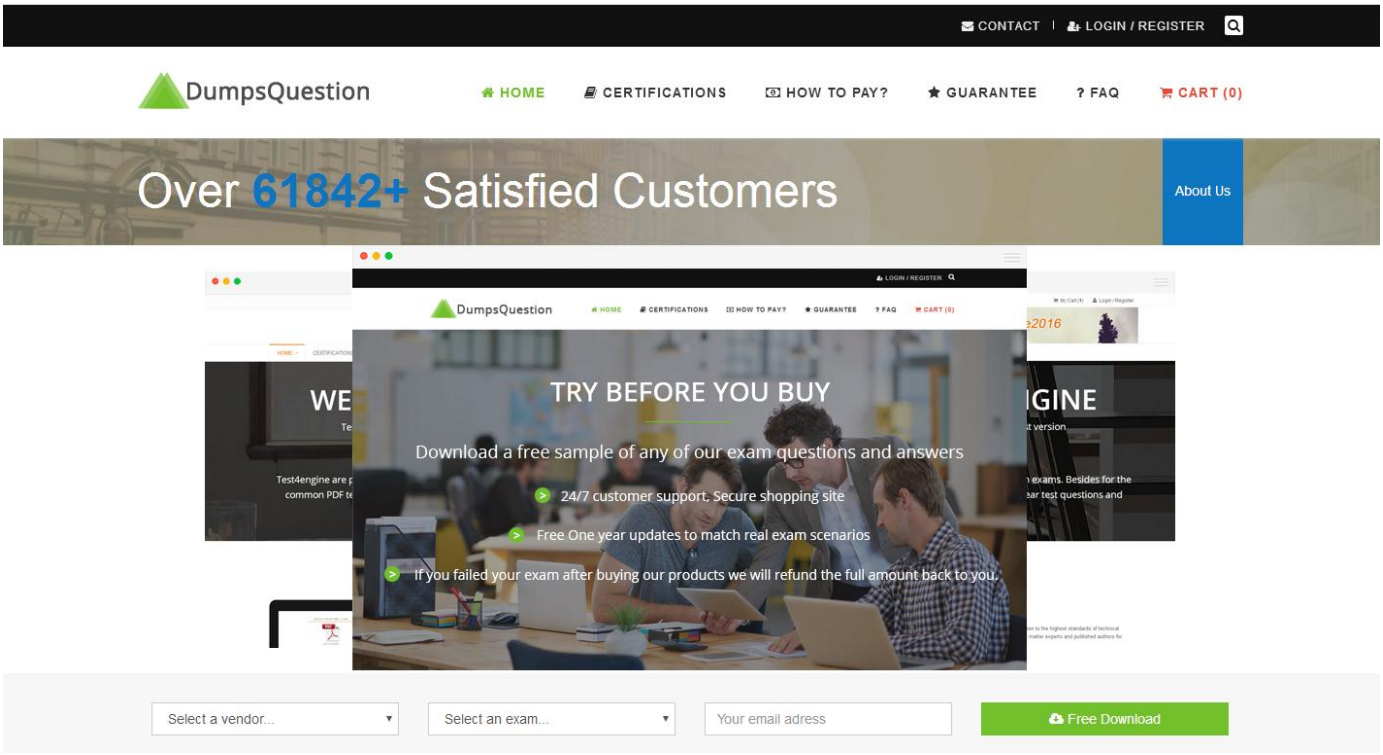
DumpsQuestion



What Clients Say About Us

Disclaimer Policy: The site does not guarantee the content of the comments. Because of the different time and the changes in the scope of the exam, it can produce different effect. Before you purchase the dump, please carefully read the product introduction from the page. In addition, please be advised the site will not be responsible for the content of the comments and contradictions between users.

"Good things should be shared together. I pass the HPE0-J75. The dumps is good for examination."

Honey

"Do not hesitate about the dumps. It is very good valid dumps. Yes, I am sure it is vald for this times. Worthy it."

Hardy

http://www.dumpsquestion.com

Professional Dump Collection & Excellent Exam Questions & Latest Questions

Exam : **Identity-and-Access-Management-Architect**

Title : Salesforce Certified Identity and Access Management Architect

Vendor : Salesforce

Version : DEMO

NO.1 Universal Containers is creating a mobile application that will be secured by Salesforce Identity using the QAuth 2.0 user-agent flow (this flow uses the QAuth 2.0 implicit grant type).
Which three QAuth concepts apply to this flow?
Choose 3 answers
A. Refresh Token
B. Client ID
C. Verification Code
D. Authorization Code
E. Scopus
Answer: A B E
Explanation:
Salesforce's user-agent flow implements the OAuth 2.0 implicit grant model for browser-based or mobile applications that obtain authorization through a browser. In that flow, the client uses a client ID and requests specific scopes. The user authorizes the app, and the resulting token is delivered through the browser-based redirect. In Salesforce identity examples, refresh-related behavior is often part of the mobile discussion, while an authorization code is not a characteristic of the implicit model. That is the key concept to remember:
implicit or user-agent flow is centered on browser-mediated authorization without a back-end code exchange.
So the valid concepts align with client identity and requested access, not with the server-side authorization- code step used in the web server flow. This is why options A, B, E work together as the correct solution.

NO.2 A global fitness equipment manufacturer is planning to sell fitness tracking devices and has the following requirements:
1) Customer purchases the device.
2) Customer registers the device using their mobile app.
3) A case should automatically be created in Salesforce and associated with the customers account in cases where the device registers issues with tracking.
Which OAuth flow should be used to meet these requirements?
A. OAuth 2.0 Asset Token Flow
B. OAuth 2.0 Device Flow
C. OAuth 2.0 SAVL Server Assertion Flow
D. OAuth 2.0 User-Agent Flow
Answer: A

NO.3 Universal Containers want users to be able to log in to the Salesforce mobile app with their Active Directory password. Employees are unable to use mobile VPN.
Which two options should an identity architect recommend to meet the requirement?
Choose 2 answers
A. Active Directory Password Since Plugin
B. Salesforce Trigger & Field on Contact Object
C. Salesforce Identity Connect
D. Configure Cloud Provider Load Balancer

Answer: A,C

NO.4 An organization has a central cloud-based Identity and Access Management (IAM) Service for authentication and user management, which must be utilized by all applications as follows:
1 - Change of a user status in the central IAM Service triggers provisioning or deprovisioning in the integrated cloud applications.
2 - Security Assertion Markup Language single sign-on (SSO) is used to facilitate access for users authenticated at identity provider (Central IAM Service).
Which approach should an IAM architect implement on Salesforce Sales Cloud to meet the requirements?
A. Configure Salesforce as a SAML Service Provider, and enable SCIM (System for CrossDomain Identity Management) for provisioning and deprovisioning of users.
B. Configure central IAM Service as an authentication provider and extend registration handler to manage provisioning and deprovisioning of users.
C. Configure Salesforce as a SAML service provider, and enable Just-In Time (JIT) provisioning and deprovisioning of users.
D. Deploy Identity Connect component and set up automated provisioning and deprovisioning of users, as well as SAML-based SSO.
Answer: A

NO.5 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 failing?
A. Security Assertion Markup Language Validator
B. Connected App Manager
C. SAML Metadata file importer
D. Identity Provider Metadata download
Answer: A
Explanation:
When SAML sign-on fails during setup, the fastest Salesforce-native diagnostic tool is the SAML Validator.
It breaks down the assertion and shows where validation fails, such as certificate issues, audience mismatches, subject formatting, missing attributes, or timestamp problems. That is much more useful than simply reviewing connected app settings or downloading metadata again, because the architect needs visibility into the actual assertion being posted to Salesforce. SAML integrations succeed or fail based on the signed XML and the trust configuration around it, so a validator that exposes the assertion details is the right troubleshooting instrument. In practice, this is the tool admins use to determine whether the issue sits in the identity provider output or in Salesforce configuration. This is why option A is the best answer in Salesforce terms.

NO.6 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?
A. Embedded Login. Identify what level of UI customization will be required to make it match the

service providers look and feel.

B. Salesforce REST APIs. Ensure that Secure Sockets Layer (SSL) connection for the integration is used.

C. OpenID Connect Web Server Flow. Determine if the service provider is secure enough to store the client secret on.

D. Embedded Login. Consider whether or not it relies on third party cookies which can cause browser compatibility issues.

Answer: D

Explanation:

Salesforce Embedded Login exists specifically to place a Salesforce-backed login experience inside another application or service provider, which makes it the right feature to consider for a seamless sign-in widget.

However, the architectural caveat is browser behavior. Embedded login can rely on third-party cookies, and modern browser privacy controls can affect how that experience behaves. That dependency is often the deciding consideration before recommending it. REST APIs and generic OAuth flows are part of the broader identity toolbox, but they don't answer the executive sponsor's question about embedding a login widget directly into another application. The recommendation should therefore focus on Embedded Login and on whether the target browser landscape will tolerate the cookie model it depends on. This is why option D is the best answer in Salesforce terms.

NO.7 Northern Trail Outfitters (NTO) wants its customers to use phone numbers to log in to their new digital portal, which was designed and built using Salesforce Experience Cloud. In order to access the portal, the user will need to do the following:

1. Enter a phone number and/or email address
2. Enter a verification code that is to be sent via email or text.

What is the recommended approach to fulfill this requirement?

A. create an authentication provider and implement a self-registration handler class.

B. Create a custom login page with an Apex controller. The controller has tips to send and verify the identity.

C. create a Login Discoverer page and provide a Login Discovery Handler Apex class.

D. Create a custom login flow that uses an Apex controller to verify the phone numbers with the company' s verification service.

Answer: C

Explanation:

For a portal that wants users to enter a phone number or email address first and then receive a one-time verification code, Salesforce's recommended pattern is a Login Discovery page backed by a Login Discovery handler. This supports identifier-first authentication and lets the org decide how to route or verify the user once the identifier is known. Building a custom login page and controller can work, but it bypasses the purpose-built experience Salesforce provides for this exact passwordless entry pattern. Authentication providers and login flows solve different phases of the login journey. The architectural advantage of Login Discovery is that it cleanly supports phone-or-email identification before the platform or handler triggers the verification step. This is why option C is the best answer in Salesforce terms.

NO.8 An identity professional working on a project to integrate a third-party application with Salesforce, is tasked with evaluating OAuth options. The project requires fine-grained access control

and the ability to obtain long-lived access tokens.
Which OAuth flow would best full fill the project requirements?
A. Client Credentials flow
B. Authorization Code flow
C. Implicit flow
D. Username-password grant
Answer: B
Explanation:
For fine-grained delegated access and long-lived sessions, the Authorization Code flow is the strongest mainstream OAuth choice. It supports user consent, server-side token exchange, and refresh-token issuance in the patterns Salesforce documents for confidential applications. Client Credentials is for app-to-app integration without a user context, and Implicit/User-Agent is less suitable for strong control and durable token management. Username-password is a special-case flow that trades off security and user experience.
The reason this matters architecturally is that the authorization code pattern separates user authentication from token exchange and allows the client to keep secrets securely on the server side. That is why it remains the preferred model for robust delegated access to protected Salesforce resources. This is why option B is the best answer in Salesforce terms.

NO.9 A global company ' s Salesforce Identity Architect is reviewing its Salesforce production org login history and is seeing some intermittent Security Assertion Markup Language (SAML SSO) " Replay Detected " and " Assertion Invalid " login errors.
Which two issues would cause these errors?
Choose 2 answers
A. The certificate loaded into SSO configuration does not match the certificate used by the IdP.
B. The subject element is missing from the assertion sent to Salesforce.
C. The current time setting of the company ' s identity provider (IdP) and Salesforce platform is out of sync by more than eight minutes.
D. The assertion sent to Salesforce contains an assertion ID previously used.
Answer: B D
Explanation:
Salesforce treats SAML assertions as short-lived, unique security artifacts. Two classic reasons for "Replay Detected" or "Assertion Invalid" errors are a reused assertion ID and an assertion structure problem such as a missing subject. A replay error occurs when Salesforce sees an assertion identifier that was already used. An invalid-assertion error can also occur when required elements are missing or malformed. Time skew and certificate mismatches can cause SSO failures too, but the question specifically points to replay and assertion validity symptoms that align most directly with assertion uniqueness and required content. This reflects a core SAML security principle: assertions must be complete, signed correctly, timely, and never reused. This is why options B, D work together as the correct solution.

NO.10 Northern Trail Outfitters (NTO) uses Salesforce for Sales Opportunity Management. Okta was recently brought in to Just-in-Time (JIT) provision and authenticate NTO users to applications. Salesforce users also use Okta to authorize a Forecasting web application to access Salesforce records on their behalf.

Which two roles are being performed by Salesforce?
Choose 2 answers
A. OAuth Resource Server
B. SAML Service Provider
C. OAuth Client
D. SAML Identity Provider
Answer: B C
Explanation:
In this design, Salesforce plays two separate identity roles. Because Okta authenticates the workforce and sends users into Salesforce via federation, Salesforce is acting as the SAML service provider. At the same time, when the forecasting web application asks users to authorize access to Salesforce records, Salesforce is the OAuth resource owner's platform and the external application is the client. From Salesforce's perspective in that authorization exchange, it participates as the OAuth authorization platform and the ecosystem around it treats Salesforce as the protected resource. The important exam distinction is that one platform can play different identity roles in different flows. Here, Salesforce accepts a SAML assertion for login and also participates in an OAuth pattern for delegated data access. This is why options B, C work together as the correct solution.

NO.11 Universal Containers (UC) uses Salesforce for its customer service agents. UC has a proprietary system for order tracking which supports Security Assertion Markup Language (SAML) based single sign-on. The VP of customer service wants to ensure only active Salesforce users should be able to access the order tracking system which is only visible within Salesforce.
What should be done to fulfill the requirement?
Choose 2 answers
A. Set up the Corporate Identity store as an identity provider (IdP) for Order Tracking.
B. Customize Order Tracking to initiate a REST call to validate users in Salesforce after login.
C. Setup Salesforce as an identity provider (IdP) for Order Tracking.
D. Setup Order Tracking as a Canvas app in Salesforce to POST IdP initiated SAML assertion.
Answer: C D
Explanation:
If the order-tracking application supports SAML SSO and should only be accessible to active Salesforce users from inside Salesforce, the clean approach is to make Salesforce the identity provider and expose the app through Salesforce as a Canvas-style embedded experience or equivalent app launch pattern. Using Salesforce as the IdP ensures that only valid Salesforce users can obtain the SAML identity needed to enter the external system. A separate corporate identity store or a custom REST validation step introduces more moving parts than needed. The architectural goal is to let Salesforce govern access to the application that is surfaced from within Salesforce. That points to Salesforce-led federation and an in-platform application entry point. This is why options C, D work together as the correct solution.