

IDENTITY-AND-ACCESS-MANAGEMENT-ARCHITECT^{Q&As}

Salesforce Certified Identity and Access Management Architect

Pass Salesforce IDENTITY-AND-ACCESS-MANAGEMENT-ARCHITECT Exam with 100% Guarantee

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

<https://www.leads4pass.com/identity-and-access-management-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 web service is developed that allows secure access to customer order status on the Salesforce Platform, The service connects to Salesforce through a connected app with the web server flow. The following are the required actions for the authorization flow:

1.
User Authenticates and Authorizes Access
2.
Request an Access Token
3.
Salesforce Grants an Access Token
4.
Request an Authorization Code
5.
Salesforce Grants Authorization Code

What is the correct sequence for the authorization flow?

- A. 1, 4, 5, 2, 3
- B. 4, 1, 5, 2, 3
- C. 2, 1, 3, 4, 5
- D. 4,5,2, 3, 1

Correct Answer: D

QUESTION 2

Under which scenario Web Server flow will be used?

- A. Used for web applications when server-side code needs to interact with APIS.
- B. Used for server-side components when page needs to be rendered.
- C. Used for mobile applications and testing legacy Integrations.
- D. Used for verifying Access protected resources.

Correct Answer: A

QUESTION 3

Universal containers (UC) has a classified information system that its call centre team uses only when they are working on a case with a record type of "classified". They are only allowed to access the system when they own an open "classified" case, and their access to the system is removed at all other times. They would like to implement SAML SSO with salesforce as the IDP, and automatically allow or deny the staff's access to the classified information system based on whether they currently own an open "classified" case record when they try to access the system using SSO. What is the recommended solution for automatically allowing or denying access to the classified information system based on the open "classified" case record criteria?

- A. Use a custom connected App handler using apex to dynamically allow access to the system based on whether the staff owns any open "classified" cases.
- B. Use apex trigger on case to dynamically assign permission sets that grant access when a user is assigned with an open "classified" case, and remove it when the case is closed.
- C. Use custom SAML jit provisioning to dynamically query the user's open "classified" cases when attempting to access the classified information system
- D. Use salesforce reports to identify users that currently owns open "classified" cases and should be granted access to the classified information system.

Correct Answer: A

QUESTION 4

Universal Containers has multiple Salesforce instances where users receive emails from different instances. Users should be logged into the correct Salesforce instance authenticated by their IdP when clicking on an email link to a Salesforce record. What should be enabled in Salesforce as a prerequisite?

- A. My Domain
- B. External Identity
- C. Identity Provider
- D. Multi-Factor Authentication

Correct Answer: A

QUESTION 5

Universal containers (UC) is setting up Delegated Authentication to allow employees to log in using their corporate credentials. UC's security team is concerned about the risk of exposing the corporate login service on the Internet and has asked that a reliable trust mechanism be put in place between the login service and salesforce. What mechanism should an architect put in place to enable a trusted connection between the login services and salesforce?

- A. Include client ID and client secret in the login header callout.
- B. Set up a proxy server for the login service in the DMZ.
- C. Require the use of Salesforce security Tokens on password.

D. Enforce mutual Authentication between systems using SSL.

Correct Answer: C

[Latest IDENTITY-AND-ACCESS-MANAGEMENT-ARCHITECT Dumps](#)

[IDENTITY-AND-ACCESS-MANAGEMENT-ARCHITECT Practice Test](#)

[IDENTITY-AND-ACCESS-MANAGEMENT-ARCHITECT Braindumps](#)