



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.passapply.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



VCE & PDF

PassApply.com

<https://www.passapply.com/identity-and-access-management-architect.html>

2024 Latest passapply IDENTITY-AND-ACCESS-MANAGEMENT-ARCHITECT

PDF and VCE dumps Download

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

A service provider (SP) supports both Security Assertion Markup Language (SAML) and OpenID Connect (OIDC). When integrating this SP with Salesforce, which use case is the determining factor when choosing OIDC or SAML?

- A. OIDC is more secure than SAML and therefore is the obvious choice.
- B. The SP needs to perform API calls back to Salesforce on behalf of the user after the user logs in to the service provider.
- C. If the user has a session on Salesforce, you do not want them to be prompted for a username and password when they login to the SP.
- D. They are equivalent protocols and there is no real reason to choose one over the other.

Correct Answer: B

QUESTION 2

Universal Containers (UC) has built a custom time tracking app for its employee. UC wants to leverage Salesforce Identity to control access to the custom app.

At a minimum, which Salesforce license is required to support this requirement?

- A. Identity Verification
- B. Identity Connect
- C. Identity Only
- D. External Identity

Correct Answer: C

QUESTION 3

A company's external application is protected by Salesforce through OAuth. The identity architect for the project needs to limit the level of access to the data of the protected resource in a flexible way.

What should be done to improve security?

- A. Select "Admin approved users are pre-authorized" and assign specific profiles.
- B. Create custom scopes and assign to the connected app.
- C. Define a permission set that grants access to the app and assign to authorized users.
- D. Leverage external objects and data classification policies.



Correct Answer: B

QUESTION 4

The security team at Universal Containers (UC) has identified exporting reports as a high- risk action and would like to require users to be logged into Salesforce with their Active Directory (AD) credentials when doing so. For all other users of Salesforce, users should be allowed to use AD Credentials or Salesforce credentials. What solution should be recommended to prevent exporting reports except when logged in using AD credentials while maintaining the ability to view reports when logged in with Salesforce credentials?

- A. Use SAML Federated Authentication and block access to reports when accessed through a Standard Assurance session.
- B. Use SAML Federated Authentication and Custom SAML JIT Provisioning to dynamically and or remove a permission set that grants the Export Reports Permission.
- C. Use SAML federated Authentication, treat SAML Sessions as High Assurance, and raise the session level required for exporting reports.
- D. Use SAML federated Authentication with a Login Flow to dynamically add or remove a Permission Set that grants the Export Reports Permission.

Correct Answer: C

QUESTION 5

An insurance company has a connected app in its Salesforce environment that is used to integrate with a Google Workspace (formerly knot as G Suite).

An identity and access management (IAM) architect has been asked to implement automation to enable users, freeze/suspend users, disable users, and reactivate existing users in Google Workspace upon similar actions in Salesforce.

Which solution is recommended to meet this requirement?

- A. Configure user Provisioning for Connected Apps.
- B. Update the Security Assertion Markup Language Just-in-Time (SAML JIT; handler in Salesforce for user provisioning and de-provisioning.
- C. Build a custom REST endpoint in Salesforce that Google Workspace can poll against.
- D. Build an Apex trigger on the useriogin object to make asynchronous callouts to Google APIs.

Correct Answer: A

QUESTION 6

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?



- 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.

Correct Answer: A

QUESTION 7

Which three types of attacks would a 2-Factor Authentication solution help garden against?

- A. Key logging attacks
- B. Network perimeter attacks
- C. Phishing attacks
- D. Dictionary attacks
- E. Man-in-the-middle attacks

Correct Answer: ABD

QUESTION 8

Universal Containers (UC) has a classified information system that its call center team uses only when they are working on a case with a record type "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 eith 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 the access to the classified information system based on the open "classified" case record criteria?

- A. Use Salesforce reports to identify users that currently owns open "Classified" cases and should be granted access to the Classified information system.
- B. Use Apex trigger on case to dynamically assign permission Sets that Grant access when an 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 a Common Connected App Handler using Apex to dynamically allow access to the system based on whether the staff owns any open "Classified" Cases.

Correct Answer: D



QUESTION 9

Universal containers(UC) has implemented SAML-BASED single Sign-on for their salesforce application and is planning to provide access to salesforce on mobile devices using the salesforce1 mobile app. UC wants to ensure that single Sign-on is used for accessing the salesforce1 mobile app. Which two recommendations should the architect make?
Choose 2 answers

- A. Use the existing SAML SSO flow along with user agent flow.
- B. Configure the embedded Web browser to use my domain URL.
- C. Use the existing SAML SSO flow along with Web server flow
- D. Configure the salesforce1 app to use the my domain URL

Correct Answer: AD

QUESTION 10

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 subject element is missing from the assertion sent to salesforce.
- B. The certificate loaded into SSO configuration does not match the certificate used by the IdP.
- 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.

Correct Answer: AD

QUESTION 11

Universal Containers is creating a mobile application that will be secured by Salesforce Identity using the OAuth 2.0 user-agent flow (this flow uses the OAuth 2.0 implicit grant type).

Which three OAuth concepts apply to this flow?

Choose 3 answers

- A. Client ID
- B. Refresh Token
- C. Authorization Code



D. Verification Code

E. Scopes

Correct Answer: ABE

QUESTION 12

Universal containers (UC) has implemented SAML -based single Sign-on for their salesforce application. UC is using pingfederate as the Identity provider. To access salesforce, Users usually navigate to a bookmarked link to my domain URL. What type of single Sign-on is this?

A. Sp-Initiated

B. IDP-initiated with deep linking

C. IDP-initiated

D. Web server flow.

Correct Answer: A

QUESTION 13

A group of users try to access one of Universal Containers\' Connected Apps and receive the following error message: " Failed: Not approved for access." What is the most likely cause of this issue?

A. The Connected App settings "All users may self-authorize" is enabled.

B. The Salesforce Administrators have revoked the OAuth authorization.

C. The Users do not have the correct permission set assigned to them.

D. The User of High Assurance sessions are required for the Connected App.

Correct Answer: C

QUESTION 14

An Identity and Access Management (IAM) Architect is recommending Identity Connect to integrate Microsoft Active Directory (AD) with Salesforce for user provisioning, deprovisioning and single sign-on (SSO).

Which feature of Identity Connect is applicable for this scenano?

A. When Identity Connect is in place, if a user is deprovisioned in an on-premise AD, the user\'s Salesforce session Is revoked Immediately.

B. If the number of provisioned users exceeds Salesforce licence allowances, identity Connect will start disabling the existing Salesforce users in First-in, First-out (FIFO) fashion.

C. Identity Connect can be deployed as a managed package on salesforce org, leveraging High Availability of



Salesforce Platform out-of-the-box.

D. When configured, Identity Connect acts as an identity provider to both Active Directory and Salesforce, thus providing SSO as a default feature.

Correct Answer: A

QUESTION 15

What are three capabilities of Delegated Authentication? Choose 3 answers

- A. It can be assigned by Custom Permissions.
- B. It can connect to SOAP services.
- C. It can be assigned by Permission Sets.
- D. It can be assigned by Profiles.
- E. It can connect to REST services.

Correct Answer: BCE

[IDENTITY-AND-ACCESS-MANAGEMENT-ARCHITECT PDF Dumps](#) | [IDENTITY-AND-ACCESS-MANAGEMENT-ARCHITECT Study Guide](#) | [IDENTITY-AND-ACCESS-MANAGEMENT-ARCHITECT Braindumps](#)