



Salesforce

IDENTITY-AND-ACCESS-MANAGEMENT- ARCHITECT Exam

Salesforce Identity and Access Management Architect

Product Questions: 247

Version: 15.0

Question: 1

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 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 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.

Answer: D

Explanation:

Question: 2

How should an Architect automatically redirect users to the login page of the external Identity provider when using an SP-Initiated SAML flow with Salesforce as a Service Provider?

- A. Use visualforce as the landing page for My Domain to redirect users to the Identity Provider login Page.
- B. Enable the Redirect to the Identity Provider setting under Authentication Services on the My domain Configuration.
- C. Remove the Login page from the list of Authentication Services on the My Domain configuration.
- D. Set the Identity Provider as default and enable the Redirect to the Identity Provider setting on the SAML Configuration.

Answer: C

Explanation:

Question: 3

Universal Containers (UC) has an e-commerce website where customers can buy products, make payments and manage their accounts. UC decides to build a Customer Community on Salesforce and wants to allow the customers to access the community from their accounts without logging in again. UC decides to implement an SP-initiated SSO using a SAML-compliant Idp. In this scenario where Salesforce is the Service Provider, which two activities must be performed in Salesforce to make SP-initiated SSO work? Choose 2 answers

- A. Configure SAML SSO settings.
- B. Create a Connected App.
- C. Configure Delegated Authentication.
- D. Set up My Domain.

Answer: AD

Explanation:

Question: 4

Universal Containers (UC) has a custom, internal-only, mobile billing application for users who are commonly out of the office. The app is configured as a connected App in Salesforce. Due to the nature of this app, UC would like to take the appropriate measures to properly secure access to the app. Which two are recommendations to make the UC? Choose 2 answers

- A. Disallow the use of Single Sign-on for any users of the mobile app.
- B. Require High Assurance sessions in order to use the Connected App.
- C. Set Login IP Ranges to the internal network for all of the app users Profiles.
- D. Use Google Authenticator as an additional part of the login process

Answer: B, D

Explanation:

Question: 5

What information does the 'Relaystate' parameter contain in sp-Initiated Single Sign-on?

- A. Reference to a URL redirect parameter at the identity provider.
- B. Reference to a URL redirect parameter at the service provider.
- C. Reference to the login address URL of the service provider.
- D. Reference to the login address URL of the identity Provider.

Answer: B

Explanation:

Question: 6

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

Answer: A, B, D

Explanation:

Question: 7

Universal Containers (UC) plans to use a SAML-based third-party IdP serving both of the Salesforce Partner Community and the corporate portal. UC partners will log in 65* to the corporate portal to access protected resources, including links to Salesforce resources. What would be the recommended way to configure the IdP so that seamless access can be achieved in this scenario?

- A. Set up the corporate portal as a Connected App in Salesforce and use the Web server OAuth flow.
- B. Configure SP-initiated SSO that passes the SAML token upon Salesforce resource access request.
- C. Set up the corporate portal as a Connected App in Salesforce and use the User Agent OAuth flow.
- D. Configure IdP-initiated SSO that passes the SAML token upon Salesforce resource access request.

Answer: D

Explanation:

Question: 8

Universal Containers (UC) wants to use Salesforce for sales orders and a legacy of system for order fulfillment. The legacy system must update the status of orders in 65* Salesforce in real time as they are fulfilled. UC decides to use OAuth for connecting the legacy system to Salesforce. What OAuth flow should be considered that doesn't require storing credentials, client secret or refresh tokens?

- A. Web Server flow
- B. JWT Bearer Token flow
- C. Username-Password flow
- D. User Agent flow

Answer: B

Explanation:

Question: 9

Universal Containers (UC) has a Customer Community that uses Facebook for of authentication. UC

would like to ensure that changes in the Facebook profile are reflected on the appropriate Customer Community user. How can this requirement be met?

- A. Use SAML Just-In-Time Provisioning between Facebook and Salesforce.
- B. Use information in the Signed Request that is received from Facebook.
- C. Develop a scheduled job that calls out to Facebook on a nightly basis.
- D. Use the updateUser() method on the Registration Handler class.

Answer: D

Explanation:

Question: 10

Universal Containers (UC) has five Salesforce orgs (UC1, UC2, UC3, UC4, UC5). Every user that is in UC2, UC3, UC4, and UC5 is also in UC1, however not all users have access to every org. Universal Containers would like to simplify the authentication process such that all Salesforce users need to remember one set of credentials. UC would like to achieve this with the least impact to cost and maintenance. What approach should an Architect recommend to UC?

- A. Purchase a third-party Identity Provider for all five Salesforce orgs to use and set up JIT user provisioning on all other orgs.
- B. Purchase a third-party Identity Provider for all five Salesforce orgs to use, but don't set up JIT user provisioning for other orgs.
- C. Configure UC1 as the Identity Provider to the other four Salesforce orgs and set up JIT user provisioning on all other orgs.
- D. Configure UC1 as the Identity Provider to the other four Salesforce orgs, but don't set up JIT user provisioning for other orgs.

Answer: B

Explanation:

Question: 11

Universal Containers (UC) wants to implement SAML SSO for their internal of Salesforce users using a third-party IdP. After some evaluation, UC decides NOT to set up My Domain for their Salesforce org. How does that decision impact their SSO implementation?

- A. IdP-initiated SSO will NOT work.
- B. Neither SP- nor IdP-initiated SSO will work.
- C. Either SP- or IdP-initiated SSO will work.
- D. SP-initiated SSO will NOT work

Answer: B

Explanation:

Question: 12
