Salesforce Certified Identity and Access Management Architect

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:

A. 1, 4, 5, 2, 3

B. 4, 1, 5, 2, 3

C. 2, 1, 3, 4, 5

D. 4,5,2, 3, 1

Answer(s): B

---

2. Universal containers wants to implement single Sign-on for a salesforce org using an external identity provider and corporate identity store. What type of Authentication flow is required to support deep linking?

A. Web server Oauth SSO flow.

B. Identity-provider-initiated SSO

C. Service-provider-initiated SSO

D. Start URL on identity provider

Answer(s): C

---

3. A security architect is rolling out a new multi-factor authentication (MFA) mandate, where all employees must go through a secure authentication process before accessing Salesforce. There

are multiple Identity Providers (IdP) in place and the architect is considering how the "Authentication Method Reference" field (AMR) in the Login History can help.

A. AMR field shows the authentication methods used at IdP.

B. Both OIDC and Security Assertion Markup Language (SAML) are supported but AMR must be implemented at IdP.

C. High-assurance sessions must be configured under Session Security Level Policies.

D. Dependency on what is supported by OpenID Connect (OIDC) implementation at IdP.

Answer(s): A,B

---

4. Universal Containers (UC) wants to build a custom mobile app for their field reps to create orders in salesforce. After the first time the users log in, they must be able to access salesforce upon opening the mobile app without being prompted to log in again. What Oauth flows should be considered to support this requirement?

A. Web Server flow with a Refresh Token.

B. Mobile Agent flow with a Bearer Token.

C. User Agent flow with a Refresh Token.

D. SAML Assertion flow with a Bearer Token.

Answer(s): A,C

---

5. The CMO of an advertising company has invited an Identity and Access Management (IAM) specialist to discuss Salesforce out-of-box capabilities for configuring the company*s login and registration experience on Salesforce Experience Cloud.

A. Use Experience Builder to build branded Reset and Forgot Password pages.

B. Build custom pages for branding requirements in Experience Cloud.

C. Build custom site pages for reset and forgot password features.

D. Login & Registration pages can be branded in the Community Administration settings.

Answer(s): A,D

---

6. Northern Trail Outfitters (NTO) is planning to build a new customer service portal and wants to use passwordless login, allowing customers to login with a one-time passcode sent to them via email or SMS.

A. Each community comes with 10,000 Identity Verification Credits per month and only customers with more than 10,000 logins a month should estimate additional SMS verifications needed.

B. Identity Verification Credits are consumed with each SMS (text message) sent and should be estimated based on the number of login verification challenges for SMS verification users.

C. Identity Verification Credits are consumed with each verification sent and should be estimated based on the number of logins that will incur a verification challenge.

D. Identity Verification Credits are a direct add-on license based on the number of existing member-based or login-based Community licenses.

Answer(s): B

---

7. An architect needs to advise the team that manages the identity provider how to differentiate salesforce from other service providers. What SAML SSO setting in salesforce provides this capability?

A. Entity id

B. Issuer

C. Identity provider login URL

D. SAML identity location

Answer(s): A

---

8. Universal containers (UC) is building a mobile application that will make calls to the salesforce REST API.

A. Refresh token

B. API

C. full

D. Web

Answer(s): A,B

---

9. Universal Containers wants to secure its Salesforce APIs by using an existing Security Assertion Markup Language (SAML) configuration supports the company's single sign-on process to Salesforce, Which Salesforce OAuth authorization flow should be used?

A. OAuth 2.0 SAML Bearer Assertion Flow

B. A SAML Assertion Row

C. OAuth 2.0 User-Agent Flow

D. OAuth 2.0 JWT Bearer Flow

Answer(s): A

---

10. Which tool should be used to track login data, such as the average number of logins, who logged in more than the average number of times and who logged in during non-business hours?

A. Login Inspector

B. Login History

C. Login Report

D. Login Forensics

Answer(s): D

---

11. Universal Containers is budding a web application that will connect with the Salesforce API using JWT OAuth Flow.

A. The Use Digital Signature option in the connected app.

B. The "web" OAuth scope in the connected app,

C. The "api" OAuth scope in the connected app.

D. The "edair_api" OAuth scope m the connected app.

Answer(s): A,C

---

12. Northern Trail Outfitters (NTO) wants to give customers the ability to submit and manage issues with their purchases. It is important for to give its customers the ability to login with their Facebook and Twitter credentials.

A. Create a custom external authentication provider for Facebook.

B. Configure a predefined authentication provider for Facebook.

C. Create a custom external authentication provider for Twitter.

D. Configure a predefined authentication provider for Twitter.

Answer(s): B,D

---

13. A public sector agency is setting up an identity solution for its citizens using a Community built on Experience Cloud and requires the new user registration functionality to capture first name, last name, and phone number.

A. Integrate with social websites (Facebook, Linkedin. Twitter)

B. Use an external Identity Provider

C. Create a custom Lightning Web Component

D. Use Login Discovery

Answer(s): D

---

14. 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.

A. Identity Verification

B. Identity Connect

C. Identity Only

D. External Identity

Answer(s): C

---

15. Universal Containers (UC) implemented SSO to a third-party system for their Salesforce users to access the App Launcher. UC enabled "User Provisioning" on the Connected App so that changes to user accounts can be synched between Salesforce and the third-party system. However, UC quickly notices that changes to user roles in Salesforce are not getting synched to the third-party system. What is the most likely reason for this behavior?

A. User Provisioning for Connected Apps does not support role sync.

B. Required operation(s) was not mapped in User Provisioning Settings.

C. The Approval queue for User Provisioning Requests is unmonitored.

D. Salesforce roles have more than three levels in the role hierarchy.

Answer(s): B

---

16. Universal Containers (UC) has implemented a multi-org architecture in their company. Many users have licences across multiple orgs, and they are complaining about remembering which org and credentials are tied to which business process. Which two recommendations should the Architect make to address the Complaints?

A. Activate My Domain to Brand each org to the specific business use case.

B. Implement SP-Initiated Single Sign-on flows to allow deep linking.

C. Implement IdP-Initiated Single Sign-on flows to allow deep linking.

D. Implement Delegated Authentication from each org to the LDAP provider.

Answer(s): A,B

---

17. Universal Containers (UC) is using a custom application that will act as the Identity Provider and will generate SAML assertions used to log in to Salesforce. UC is considering including custom parameters in the SAML assertion. These attributes contain sensitive data and are needed to authenticate the users. The assertions are submitted to salesforce via a browser form post. The majority of the users will only be able to access Salesforce via UC's corporate network, but a subset of admins and executives would be allowed access from outside the corporate network on their mobile devices. Which two methods should an Architect consider to ensure that the sensitive data cannot be tampered with, nor accessible to anyone while in transit?

A. Use the Identity Provider's certificate to digitally sign and Salesforce's Certificate to encrypt the payload.

B. Use Salesforce's Certificate to digitally sign the SAML Assertion and a Mobile Device Management client on the users' mobile devices.

C. Use the Identity provider's certificate to digitally Sign and the Identity provider's certificate to encrypt the payload.

D. Use a custom login flow to retrieve sensitive data using an Apex callout without including the attributes in the assertion.

Answer(s): C,D

---

18. Universal containers (UC) would like to enable self - registration for their salesforce partner community users.

A. Modify the communitiesselfregcontroller to assign the profile and account.

B. Modify the selfregistration trigger to assign profile and account.

C. Configure registration for communities to use a custom visualforce page.

D. Configure registration for communities to use a custom apex controller.

Answer(s): A,C

---

19. Northern Trail Outfitters (NTO) is planning to roll out a partner portal for its distributors using Experience Cloud. NTO would like to use an external identity provider (idP) and for partners to register for access to the portal. Each partner should be allowed to register only once to avoid duplicate accounts with Salesforce.

A. On successful creation of Partners using Self Registration page in Experience Cloud, create identity in Ping.

B. Create a custom page m Experience Cloud to self register partner with Experience Cloud and Ping identity store.

C. Create a custom web page in the Portal and create users in the IdP and Experience Cloud using published APIs.

D. Allow partners to register through the IdP and create partner users in Salesforce through an API.

Answer(s): B

---

20. 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

Answer(s): B,D
