# Identity-and-Access-Management-Architect Dumps

# Salesforce Certified Identity and Access Management Architect (SU23)

## https://www.certleader.com/Identity-and-Access-Management-Architect-dumps.html
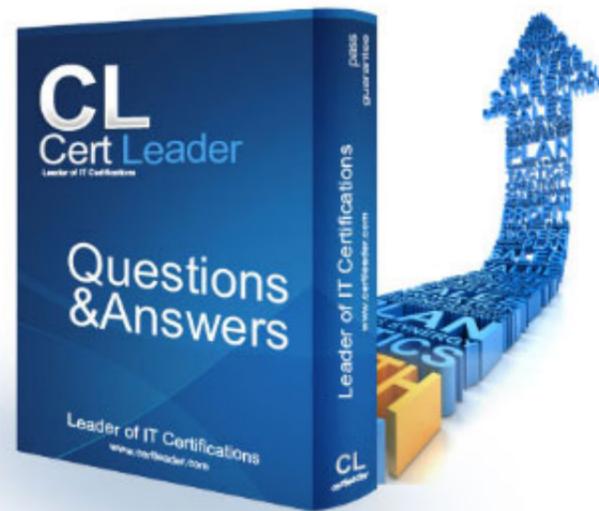
**NEW QUESTION 1**
Universal Containers is considering using Delegated Authentication as the sole means of Authenticating of Salesforce users. A Salesforce Architect has been brought in to assist with the implementation. What two risks Should the Architect point out? Choose 2 answers

A. Delegated Authentication is enabled or disabled for the entire Salesforce org.
B. UC will be required to develop and support a custom SOAP web service.
C. Salesforce users will be locked out of Salesforce if the web service goes down.
D. The web service must reside on a public cloud service, such as Heroku.

**Answer:** BC

**Explanation:**
The two risks that the architect should point out for using delegated authentication as the sole means of authenticating Salesforce users are:

≫ UC will be required to develop and support a custom SOAP web service. Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external service by making a SOAP callout to a web service that verifies the user's credentials. This feature requires UC to develop and support a custom SOAP web service that can accept and validate the user's username and password, and return a boolean value to indicate whether the authentication is successful or not. This could increase complexity and cost for UC, as they need to write custom code and maintain the web service.

≫ Salesforce users will be locked out of Salesforce if the web service goes down. Delegated authentication relies on the availability and performance of the external web service that handles the authentication requests from Salesforce. If the web service goes down or becomes slow, Salesforce users will not be able to log in or access Salesforce, as they will receive an error message or a timeout response. This could cause disruption and frustration for UC's business operations and user satisfaction.

The other options are not valid risks for using delegated authentication. Delegated authentication can be enabled or disabled for individual users or groups of users by using permission sets or profiles, not for the entire Salesforce org. The web service does not need to reside on a public cloud service, such as Heroku, as it can be hosted on any platform that supports SOAP services and can communicate with Salesforce. References: [Delegated Authentication], [Enable 'Delegated Authentication'], [Troubleshoot Delegated Authentication]

**NEW QUESTION 2**
Universal Containers (UC) wants to integrate a third-party Reward Calculation system with Salesforce to calculate Rewards. Rewards will be calculated on a schedule basis and update back into Salesforce. The integration between Salesforce and the Reward Calculation System needs to be secure. Which are two recommended practices for using OAuth flow in this scenario. choose 2 answers

A. OAuth Refresh Token FLow
B. OAuth Username-Password Flow
C. OAuth SAML Bearer Assertion FLow
D. OAuth JWT Bearer Token FLow

**Answer:** CD

**Explanation:**
OAuth is an open-standard protocol that allows a client app to access protected resources on a resource server, such as Salesforce API, by obtaining an access token from an authorization server. OAuth supports different types of flows, which are ways of obtaining an access token. For integrating a third-party Reward Calculation system with Salesforce securely, two recommended practices for using OAuth flow are:

≫ OAuth SAML Bearer Assertion Flow, which allows the client app to use a SAML assertion issued by a trusted identity provider to request an access token from Salesforce. This flow does not require the client app to store any credentials or secrets, and leverages the existing SSO infrastructure between Salesforce and the identity provider.

≫ OAuth JWT Bearer Token Flow, which allows the client app to use a JSON Web Token (JWT) signed by a private key to request an access token from Salesforce. This flow does not require any user interaction or consent, and uses a certificate to verify the identity of the client app.
Verified References: [OAuth 2.0 SAML Bearer Assertion Flow for Server-to-Server Integration], [OAuth 2.0 JWT Bearer Token Flow for Server-to-Server Integration]

**NEW QUESTION 3**
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 5alesforce contains an assertion ID previously used.

**Answer:** CD

**Explanation:**
A SAML SSO 'Replay Detected and Assertion Invalid' error occurs when Salesforce detects that the same assertion has been used more than once within the validity period. This can happen if the assertion ID is reused by the IdP or if the assertion is resent by the user. Another possible cause is that the time settings of the IdP and Salesforce are not synchronized, which can result in an assertion being valid for a shorter or longer period than expected. References: SAML Single Sign-On Settings, Troubleshoot SAML Single Sign-On

**NEW QUESTION 4**
Northern Trail Outfitters (NTO) utilizes a third-party cloud solution for an employee portal. NTO also owns Salesforce Service Cloud and would like employees to be able to login to Salesforce with their third-party portal credentials for a seamless experience. The third-party employee portal only supports OAuth.
What should an identity architect recommend to enable single sign-on (SSO) between the portal and Salesforce?

A. Configure SSO to use the third-party portal as an identity provider.
B. Create a custom external authentication provider.

C. Add the third-party portal as a connected app.
D. Configure Salesforce for Delegated Authentication.

**Answer:** A

**Explanation:**
Configuring SSO to use the third-party portal as an identity provider is the best option to enable SSO between the portal and Salesforce. The portal can use OAuth as the protocol to authenticate users and redirect them to Salesforce. The other options are either not feasible or not relevant for this use case. References: Single Sign-On for Desktop and Mobile Applications using SAML and OAuth, Single Sign-On with SAML on Force.com

**NEW QUESTION 5**
Which two roles of the systems are involved in an environment where salesforce users are enabled to access Google Apps from within salesforce through App launcher and connected App set up? Choose 2 answers

A. Google is the identity provider
B. Salesforce is the identity provider
C. Google is the service provider
D. Salesforce is the service provider

**Answer:** BC

**Explanation:**
In an environment where Salesforce users are enabled to access Google Apps from within Salesforce through App Launcher and Connected App setup, Google is the service provider and Salesforce is the identity provider. A service provider is an application that provides a service to users and relies on an identity provider for authentication3. A connected app is a service provider that integrates an application with Salesforce using APIs4. An identity provider is an application that authenticates users and provides information about them to service providers3. The App Launcher is a feature that allows users to access Salesforce, connected, and on-premises apps from one location5. In this scenario, Google Apps are connected apps that provide services to Salesforce users, such as Gmail, Google Drive, and Google Calendar. Salesforce is the identity provider that authenticates users and allows them to access Google Apps with their Salesforce credentials using single sign-on (SSO)6.
References: Identity Provider Overview, Connected Apps Overview, App Launcher, Single Sign-On for Desktop and Mobile Applications using SAML and OAuth

**NEW QUESTION 6**
Containers (UC) uses an internal system for recruiting and would like to have the candidates' info available in the Salesforce automatically when they are selected. UC decides to use OAuth to connect to Salesforce from the recruiting system and would like to do the authentication using digital certificates. Which two OAuth flows should be considered to meet the requirement? Choose 2 answers

A. JWT Bearer Token flow
B. Refresh Token flow
C. SAML Bearer Assertion flow
D. Web Service flow

**Answer:** AC

**Explanation:**
JWT Bearer Token flow and SAML Bearer Assertion flow are two OAuth flows that can be used to authenticate to Salesforce using digital certificates. JWT Bearer Token flow allows a connected app to request an access token from Salesforce by using a JSON Web Token (JWT) that is signed with a digital certificate. SAML Bearer Assertion flow allows a connected app to request an access token from Salesforce by using a SAML assertion that is signed with a digital certificate. These two flows can meet the requirement of UC to use OAuth and digital certificates to connect to Salesforce from the recruiting system.

**NEW QUESTION 7**
Which two considerations should be made when implementing Delegated Authentication? Choose 2 answers

A. The authentication web service can include custom attributes.
B. It can be used to authenticate API clients and mobile apps.
C. It requires trusted IP ranges at the User Profile level.
D. Salesforce servers receive but do not validate a user's credentials.
E. Just-in-time Provisioning can be configured for new users.

**Answer:** BE

**Explanation:**
Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external service of your choice1. When implementing delegated authentication, you should consider the following aspects2:

> The authentication web service can include custom attributes, such as user roles or permissions, in the response to Salesforce. These attributes can be used to update user records or trigger workflows in Salesforce2.

> Delegated authentication can be used to authenticate API clients and mobile apps that use the SOAP API or REST API login() methods. However, it does not support OAuth 2.0 flows or other authentication methods2.

> Delegated authentication does not require trusted IP ranges at the User Profile level. However, you can use them to restrict access to Salesforce from specific IP addresses or ranges2.

> Salesforce servers receive but do not validate a user's credentials. Instead, they pass the credentials to the external authentication service, which validates them and returns a response to Salesforce2.

> Just-in-time provisioning can be configured for new users who log in with delegated authentication. Thi
feature allows Salesforce to create or update user accounts based on the information provided by the external authentication service3.
References:

> Delegated Authentication

> Delegated Authentication Single Sign-On

> Just-in-Time Provisioning for Delegated Authentication

**NEW QUESTION 8**
Universal containers (UC) uses an internal company portal for their employees to collaborate. UC decides to use salesforce ideas and provide the ability for employees to post ideas from the company portal. They use SAML-BASED SSO to get into the company portal and would like to leverage it to access salesforce. Most of the users don't exist in salesforce and they would like the user records created in salesforce communities the first time they try to access salesforce. What recommendation should an architect make to meet this requirement?

A. Use on-the-fly provisioning
B. Use just-in-time provisioning
C. Use salesforce APIs to create users on the fly
D. Use Identity connect to sync users

**Answer:** B

**Explanation:**
Just-in-time provisioning is a feature that allows Salesforce to create user accounts automatically when users log in for the first time via an external identity provider. This way, UC can avoid creating user records manually or synchronizing them with another system. On-the-fly provisioning is not a valid term in Salesforce. Salesforce APIs can be used to create users programmatically, but they are not related to SSO. Identity Connect is a tool that can sync users between Salesforce and Active Directory, but it is not required for SSO.
References: Certification - Identity and Access Management Architect - Trailhead, [Just-in-Time Provisioning for SAML and OpenID Connect]

**NEW QUESTION 9**
Universal containers wants salesforce inbound Oauth-enabled integration clients to use SAML-BASED single Sign-on for authentication. What Oauth flow would be recommended in this scenario?

A. User-Agent Oauth flow
B. SAML assertion Oauth flow
C. User-Token Oauth flow
D. Web server Oauth flow

**Answer:** B

**Explanation:**
The SAML assertion OAuth flow allows a connected app to use a SAML assertion to request an OAuth access token to call Salesforce APIs. This flow provides an alternative for orgs that are currently using SAML to access Salesforce and want to access the web services API in the same way3. This flow can be used for inbound OAuth-enabled integration clients that want to use SAML-based single sign-on for authentication.
References: OAuth 2.0 SAML Bearer Assertion Flow for Previously Authorized Apps, Access Data with AP
Integration, Error 'Invalid assertion' in OAuth 2.0 SAML Bearer Flow

**NEW QUESTION 10**
A third-party app provider would like to have users provisioned via a service endpoint before users access their app from Salesforce.
What should an identity architect recommend to configure the requirement with limited changes to the third-party app?

A. Use a connected app with user provisioning flow.
B. Create Canvas app in Salesforce for third-party app to provision users.
C. Redirect users to the third-party app for registration.
D. Use Salesforce identity with Security Assertion Markup Language (SAML) for provisioning users.

**Answer:** A

**Explanation:**
To have users provisioned via a service endpoint before users access their app from Salesforce, the identity architect should recommend using a connected app with user provisioning flow. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols. A user provisioning flow is a custom post-authentication process that can be used to create or update users in the external application using a service endpoint when users access the connected app from Salesforce. This approach can provide automatic user provisioning with limited changes to the third-party app. References: Connected Apps, User Provisioning for Connected Apps

**NEW QUESTION 10**
An Architect has configured a SAML-based SSO integration between Salesforce and an external Identity provider and is ready to test it. When the Architect attempts to log in to Salesforce using SSO, the Architect receives a SAML error. Which two optimal actions should the Architect take to troubleshoot the issue?

A. Ensure the Callback URL is correctly set in the Connected Apps settings.
B. Use a browser that has an add-on/extension that can inspect SAML.
C. Paste the SAML Assertion Validator in Salesforce.
D. Use the browser's Development tools to view the Salesforce page's markup.

**Answer:** BC

**Explanation:**
these are the optimal actions to troubleshoot a SAML error. According to the Salesforce documentation1, yo can use the following methods to debug a SAML error:
> Use a browser that has an add-on/extension that can inspect SAML. This will allow you to see the SAML request and response messages and identify any issues with the SAML assertion or the SAML response2.
> Paste the SAML Assertion Validator in Salesforce. This is a tool that helps you validate the last SAML operation on your organization and shows you any errors or warnings with the SAML assertion or the SAML response1.
Option A is incorrect because the Callback URL is not related to SAML SSO. The Callback URL is used for OAuth SSO, which is a different protocol3. Option D is incorrect because using the browser's Development tools to view the Salesforce page's markup will not help you debug a SAML error. The page's markup does not contain any information about the SAML request or response4.
References: 1: SAML Login Errors - Salesforce 2: How to Troubleshoot a Single Sign-On Error | Salesfo Ben 3: Identity Providers and Service Providers -

Salesforce 4: Single Sign-On - Salesforce

**NEW QUESTION 12**
Universal Containers (UC) is building a customer community and will allow customers to authenticate using Facebook credentials. The First time the user authenticating using Facebook, UC would like a customer account created automatically in their accounting system. The accounting system has a web service accessible to Salesforce for the creation of accounts. How can the Architect meet these requirements?

A. Create a custom application on Heroku that manages the sign-on process from Facebook.
B. Use JIT Provisioning to automatically create the account in the accounting system.
C. Add an Apex callout in the registration handler of the authorization provider.
D. Use OAuth JWT flow to pass the data from Salesforce to the Accounting System.

**Answer:** C

**Explanation:**
The best option for UC to meet the requirements is to add an Apex callout in the registration handler of the authorization provider. An authorization provider is a configuration in Salesforce that allows users to log in with an external authentication provider, such as Facebook. A registration handler is an Apex class that implements the Auth.RegistrationHandler interface and defines the logic for creating or updating a user account when a user logs in with an external authentication provider. An Apex callout is a method that invokes an external web service from Apex code. By adding an Apex callout in the registration handler, UC can create a customer account in their accounting system by calling the web service that is accessible to Salesforce. This option enables UC to automate the account creation process and integrate with their existing accounting system. The other options are not optimal for this scenario. Creating a custom application on Heroku that manages the sign-on process from Facebook would require UC to develop and maintain a separate application and infrastructure, which could increase complexity and cost. Using JIT provisioning to automatically create the account in the accounting system would require UC to configure Facebook as a SAML identity provider, which is not supported by Facebook. Using OAuth JWT flow to pass the data from Salesforce to the accounting system would require UC to obtain an OAuth token from the accounting system and use it to make API calls, which could introduce security and performance issues. References: [Authorization Providers],
[Create a Registration Handler Class], [Auth.RegistrationHandler Interface], [Apex Callouts], [Facebook as SAML Identity Provider], [OAuth 2.0 JWT Bearer Flow for Server-to-Server Integration]

**NEW QUESTION 17**
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 a Login Discovery page and provide a Login Discovery Handler Apex class.
B. Create a custom login page with an Apex controlle
C. The controller has logic to send and verify the identity.
D. Create an authentication provider and implement a self-registration handler class.
E. Create a custom login flow that uses an Apex controller to verify the phone numbers with the company's verification service.

**Answer:** A

**Explanation:**
To allow customers to use phone numbers to log in to their new digital portal, the identity architect should create a Login Discovery page and provide a Login Discovery Handler Apex class. A Login Discovery page is a custom page that allows users to enter their phone number or email address and receive a verification code via email or text. A Login Discovery Handler is a class that implements the Auth.LoginDiscoveryHandler interface and defines how to handle the user input and verification code. This approach can provide a passwordless login experience for the customers. References: Login Discovery, Create a Login Discovery Page

**NEW QUESTION 18**
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:** A

**Explanation:**
The Entity ID is the SAML SSO setting in Salesforce that provides the capability to differentiate Salesforce from other service providers. The Entity ID is a unique identifier for the service provider that is sent in the SAML request and response messages1. The identity provider uses the Entity ID to determine which service provider is requesting or receiving authentication information2. You can customize the Entity ID for your Salesforce org or Experience Cloud site in the SAML Single Sign-On Settings page3. References: 1: SAML SSO Flows 2: Federated Authentication Using SAML to Log in to Salesforce Org 3: Step 2: Create a SA Single Sign-On Setting in Salesforce

**NEW QUESTION 19**
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.

**Answer:** C

**Explanation:**
The underlying mechanisms that the UC Architect must ensure are part of the product are Just-in-Time (JIT) provisioning and deprovisioning. JIT provisioning is a process that creates or updates user accounts in Salesforce when users log in with SAML single sign-on (SSO)6. JIT deprovisioning is a process that disables or deletes user accounts in Salesforce when users are removed from the identity provider (IdP). Both of these processes enable automated provisioning and deprovisioning of users without requiring manual intervention or synchronization. The other options are not valid mechanisms for provisioning and deprovisioning. SOAP API is an application programming interface that allows developers to create, retrieve, update, or delete records in Salesforce. However, SOAP API does not support JIT provisioning or deprovisioning, and requires custom code to implement. Provisioning API is not a standard term for Salesforce, and there is no such API that supports both provisioning and deprovisioning.
References: Just-in-Time Provisioning for SAML, [Just-in-Time Deprovisioning], [SOAP API Developer

**NEW QUESTION 24**
Universal containers (UC) has built a custom based Two-factor Authentication (2fa) system for their existing on-premise applications. Thru are now implementing salesforce and would like to enable a Two-factor login process for it, as well. What is the recommended solution an architect should consider?

A. Replace the custom 2fa system with salesforce 2fa for on-premise application and salesforce.
B. Use the custom 2fa system for on-premise applications and native 2fa for salesforce.
C. Replace the custom 2fa system with an app exchange app that supports on-premise applications and salesforce.
D. Use custom login flows to connect to the existing custom 2fa system for use in salesforce.

**Answer:** D

**Explanation:**
Using custom login flows to connect to the existing custom 2fa system for use in salesforce is the recommended solution because it allows you to leverage your existing 2fa infrastructure and provide a consistent user experience across your applications. Custom login flows let you customize the authentication process by adding extra screens or logic before or after the standard login1. You can use Apex code to call your custom 2fa system and verify the user's identity2. This option also gives you more flexibility and control over the 2fa process than using native 2fa or an app exchange app3. References: 1: Customize User Authentication with Login Flows 2: Custom Login Flow Examples 3: Salesforce Multi-Factor Authentic

**NEW QUESTION 27**
Universal containers (UC) uses a legacy Employee portal for their employees to collaborate and post their ideas. UC decides to use salesforce ideas for voting and better tracking purposes. To avoid provisioning users on Salesforce, UC decides to push ideas posted on the Employee portal to salesforce through API. UC decides to use an API user using Oauth Username - password flow for the connection. How can the connection to salesforce be restricted only to the employee portal server?

A. Add the Employee portals IP address to the Trusted IP range for the connected App
B. Use a digital certificate signed by the employee portal Server.
C. Add the employee portals IP address to the login IP range on the user profile.
D. Use a dedicated profile for the user the Employee portal uses.

**Answer:** A

**Explanation:**
Adding the employee portal's IP address to the trusted IP range for the connected app is the best way to restrict the connection to Salesforce only to the employee portal server. This will ensure that only requests from the specified IP range will be accepted by Salesforce for that connected app. Option B is not a good choice because using a digital certificate signed by the employee portal server may not be supported by Salesforce for OAuth username-password flow. Option C is not a good choice because adding the employee portal's IP address to the login IP range on the user profile may not be sufficient, as it will still allow other users with the same profile to log in from that IP range. Option D is not a good choice because using a dedicated profile for the user that the employee portal uses may not be effective, as it will still allow other users with that profile to log in from any IP address. References: [Connected Apps], [OAuth 2.0 Username-Password Flow]

**NEW QUESTION 29**
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:** D

**Explanation:**
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, the identity architect should use Login Forensics. Login Forensics is a tool that analyzes login data and provides insights into user behavior and login patterns. Login Forensics can help identify anomalies, risks, and trends in user login activity. Login Forensics can also generate reports and dashboards to visualize the login data. References: Login Forensics, Analyze Login Data with Login Forensics

**NEW QUESTION 33**
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.

**Answer:** BCE

**Explanation:**

The three capabilities of delegated authentication are:

> It can connect to SOAP services. Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external service by making a SOAP callout to a web service that verifies the user's credentials. This feature enables Salesforce to integrate with existing identity stores or authentication methods that support SOAP services.

> It can be assigned by permission sets. Permission sets are collections of settings and permissions that give users access to various tools and functions in Salesforce. Permission sets can be used to assign delegated authentication to users by enabling the "Is Single Sign-on Enabled" permission. This permission allows users to log in with delegated authentication instead of their Salesforce username and password.

> It can connect to REST services. REST services are web services that use HTTP methods to access or manipulate resources on a server. REST services can be used for delegated authentication by creating a custom login page that makes a REST callout to an external service that verifies the user's credentials. This approach requires custom code and configuration, but it provides more flexibility and control over the authentication process.

The other options are not capabilities of delegated authentication. Delegated authentication cannot be assigned by custom permissions or profiles. Custom permissions are settings that can be used in Apex code or validation rules to check whether a user has access to a custom feature or functionality. Custom permissions cannot be used to enable delegated authentication for users. Profiles are collections of settings and permissions that determine what users can do in Salesforce. Profiles cannot be used to enable delegated authentication for users, as this feature is controlled by permission sets. References: [Delegated Authentication], [Permission Sets], [Enable 'Delegated Authentication'], [REST Services], [Custom Login Page for Delegated Authentication], [Custom Permissions], [Profiles]

## NEW QUESTION 34
A university is planning to set up an identity solution for its alumni. A third-party identity provider will be used for single sign-on Salesforce will be the system of records. Users are getting error messages when logging in.
Which Salesforce feature should be used to debug the issue?

A. Apex Exception Email
B. View Setup Audit Trail
C. Debug Logs
D. Login History

**Answer:** D

## NEW QUESTION 37
A global company has built an external application that uses data from its Salesforce org via an OAuth 2.0 authorization flow. Upon logout, the existing Salesforce OAuth token must be invalidated.
Which action will accomplish this?

A. Use a HTTP POST to request the refresh token for the current user.
B. Use a HTTP POST to the System for Cross-domain Identity Management (SCIM) endpoint, including the current OAuth token.
C. Use a HTTP POST to make a call to the revoke token endpoint.
D. Enable Single Logout with a secure logout URL.

**Answer:** C

**Explanation:**
To invalidate an existing Salesforce OAuth token, the external application needs to make a HTTP POST request to the revoke token endpoint, passing the token as a parameter. This will revoke the access token and the refresh token if available. The other options are not relevant for this scenario. References: Revoke OAuth Tokens, OAuth 2.0 Token Revocation

## NEW QUESTION 42
A multinational industrial products manufacturer is planning to implement Salesforce CRM to manage their business. They have the following requirements:
* 1. They plan to implement Partner communities to provide access to their partner network .
* 2. They have operations in multiple countries and are planning to implement multiple Salesforce orgs.
* 3. Some of their partners do business in multiple countries and will need information from multiple Salesforce communities.
* 4. They would like to provide a single login for their partners.
How should an Identity Architect solution this requirement with limited custom development?

A. Create a partner login for the country of their operation and use SAML federation to provide access to other orgs.
B. Consolidate Partner related information in a single org and provide access through Salesforce community.
C. Allow partners to choose the Salesforce org they need information from and use login flows to authenticate access.
D. Register partners in one org and access information from other orgs using APIs.

**Answer:** A

**Explanation:**
SAML federation allows partners to log in to multiple Salesforce orgs with a single identity provider. The partner login can be created for the country of their operation and then federated to other orgs using SAML assertions. References: SAML Single Sign-On Overview, Federated Authentication Using SAML

## NEW QUESTION 46
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. Configure the Embedded Web Browser to use My Domain URL.
B. Configure the Salesforce1 App to use the MY Domain URL.
C. Use the existing SAML-SSO flow along with User Agent Flow.
D. Use the existing SAML SSO flow along with Web Server Flow.

**Answer:** BC

**Explanation:**

To ensure that SSO is used for accessing the Salesforce1 mobile app, UC should configure the Salesforce1 app to use the My Domain URL instead of the default login.salesforce.com URL. My Domain is a feature that allows UC to create a custom domain name for their Salesforce org that supports SSO with their identity provider. UC should also use the existing SAML-SSO flow along with User Agent Flow, which is an OAuth 2.1 flow that allows users to authenticate with their identity provider through an embedded browser within the mobile app. Verified References: [Configure SSO with Salesforce as a SAML Service Provider], [User-Agent Flow]

**NEW QUESTION 50**
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 fading?

A. SAML Metadata file importer
B. Identity Provider Metadata download
C. Connected App Manager
D. Security Assertion Markup Language Validator

**Answer:** D

**Explanation:**
Security Assertion Markup Language (SAML) Validator is a tool that allows administrators to test and troubleshoot SAML single sign-on configurations. It can show which part of the login assertion is failing and provide error messages and suggestions. SAML Metadata file importer and Identity Provider Metadata download are features that allow administrators to import or download metadata files for SAML configurations. Connected App Manager is a tool that allows administrators to manage connected apps in Salesforce. References: SAML Validator, SAML Single Sign-On Settings, Connected App Manager

**NEW QUESTION 54**
Universal Containers built a custom mobile app for their field reps to create orders in Salesforce. OAuth is used for authenticating mobile users. The app is built in such a way that when a user session expires after Initial login, a new access token is obtained automatically without forcing the user to log in again. While that improved the field reps' productivity, UC realized that they need a "logout" feature.
What should the logout function perform in this scenario, where user sessions are refreshed automatically?

A. Invoke the revocation URL and pass the refresh token.
B. Clear out the client Id to stop auto session refresh.
C. Invoke the revocation URL and pass the access token.
D. Clear out all the tokens to stop auto session refresh.

**Answer:** A

**Explanation:**
The refresh token is used to obtain a new access token when the previous one expires. To revoke the user session, the logout function should invoke the revocation URL and pass the refresh token as a parameter. This will invalidate both the refresh token and the access token, and prevent the user from accessing Salesforce without logging in again2.
References:
➢ Certification Exam Guide
➢ Revoke OAuth Tokens

**NEW QUESTION 58**
Universal Containers (UC) wants its users to access Salesforce and other SSO-enabled applications from a custom web page that UC magnets. UC wants its users to use the same set of credentials to access each of the applications. what SAML SSO flow should an Architect recommend for UC?

A. SP-Initiated with Deep Linking
B. SP-Initiated
C. IdP-Initiated
D. User-Agent

**Answer:** C

**Explanation:**
The SAML SSO flow that an architect should recommend for UC is IdP-initiated. IdP-initiated SSO is a process that allows users to start at the IdP site, such as UC's custom web page, and then be redirected to Salesforce or other SPs with a SAML assertion that contains information about the user's identity and attributes. This flow enables UC to provide a single point of entry for its users to access multiple applications with the same credentials, as they do not need to enter their username and password again for each application. This flow also simplifies the configuration and maintenance of SSO, as UC does not need to create or manage deep links or URLs for each application.
The other options are not valid SAML SSO flows for this scenario. SP-initiated with deep linking is a process that allows users to start at a specific resource on the SP site, such as a report or dashboard, and then be redirected to the IdP for authentication and back to the resource with a SAML assertion. This flow is not suitable for UC's scenario, as they want their users to start at their custom web page, not at a specific resource on Salesforce or other SPs. SP-initiated is a process that allows users to start at the SP site, such as Salesforce or other applications, and then be redirected to the IdP for authentication and back to the SP site with a SAML assertion. This flow is not suitable for UC's scenario, as they want their users to start at their custom web page, not at each application separately. User-agent is not a standard term for SAML SSO, but it could refer to user-agent flow, which is an OAuth authorization flow that allows users to obtain an access token from Salesforce by using a browser or web-view. This flow is not suitable for UC's scenario, as it does not use SAML or IdP for authentication. References: [SAML Single Sign-On], [IdP-Initiated Login], [SP-Initiated Login], [Deep Linking], [OAuth User-Agent Flow]

**NEW QUESTION 59**
Universal Containers (UC) is looking to build a Canvas app and wants to use the corresponding Connected App to control where the app is visible. Which two options are correct in regards to where the app can be made visible under the Connected App setting for the Canvas app? Choose 2 answers

A. As part of the body of a Salesforce Knowledge article.
B. In the mobile navigation menu on Salesforce for Android.
C. The sidebar of a Salesforce Console as a console component.

D. Included in the Call Control Tool that's part of Open CTI.

**Answer:** CD

**Explanation:**
The sidebar of a Salesforce Console as a console component and included in the Call Control Tool that's part of Open CTI are two options that are correct in regards to where the app can be made visible under the connected app settings for the Canvas app. A Canvas app is an external application that can be embedded within Salesforce using an iframe. A connected app is an application that integrates with Salesforce using APIs and uses OAuth as the authentication protocol. You can control where a Canvas app can be displayed in Salesforce by configuring the locations in the connected app settings. The sidebar of a Salesforce Console as a console component is a valid location for a Canvas app because it allows you to display the app as a collapsible panel on the side of any console app. Included in the Call Control Tool that's part of Open CTI is a valid location for a Canvas app because it allows you to display the app as part of the softphone panel that integrates with your telephony system. As part of the body of a Salesforce Knowledge article is not a valid location for a Canvas app because it is not supported by the connected app settings. In the mobile navigation menu on Salesforce for Android is not a valid location for a Canvas app because it is not supported by the connected app settings. References: : [Canvas Developer Guide] : [Connected Apps Overview] : [Add or Remove Components from Your Console Apps] : [Open CTI Developer Guide]

**NEW QUESTION 62**
What item should an Architect consider when designing a Delegated Authentication implementation?

A. The Web service should be secured with TLS using Salesforce trusted certificates.
B. The Web service should be able to accept one to four input method parameters.
C. The web service should use the Salesforce Federation ID to identify the user.
D. The Web service should implement a custom password decryption method.

**Answer:** A

**Explanation:**
The web service that is used for delegated authentication should be secured with TLS using Salesforce trusted certificates4. This ensures that the communication between Salesforce and the external authentication method is encrypted and authenticated. The other options are not relevant for designing a delegated authentication implementation. The web service does not need to accept one to four input method parameters, as it can accept any number of parameters as long as they are wrapped in a SOAP envelope5. The web service does not need to use the Salesforce Federation ID to identify the user, as it can use any identifier that is unique and consistent across systems6. The web service does not need to implement a custom password decryption method, as it can use any encryption or hashing algorithm that is supported by both systems7. References: Delegated Authentication, Enable 'Delegated Authentication', Delegated Authentication Flow in Salesforce, FAQs fo Delegated Authentication

**NEW QUESTION 63**
Northern Trail Outfitters (NTO) is planning to implement a community for its customers using Salesforce Experience Cloud. Customers are not able to self-register. NTO would like to have customers set their own passwords when provided access to the community.
Which two recommendations should an identity architect make to fulfill this requirement? Choose 2 answers

A. Add customers as contacts and add them to Experience Cloud site.
B. Enable Welcome emails while configuring the Experience Cloud site.
C. Allow Password reset using the API to update Experience Cloud site membership.
D. Use Login Flows to allow users to reset password in Experience Cloud site.

**Answer:** CD

**Explanation:**
Allowing password reset using the API and using login flows are two possible ways to enable customers to set their own passwords in Experience Cloud. The other options are not relevant for this requirement, as they do not address the password issue. References: Allow Password Reset Using the API, Use Login Flows to Allow Users to Reset Passwords in Experience Cloud Sites

**NEW QUESTION 67**
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:
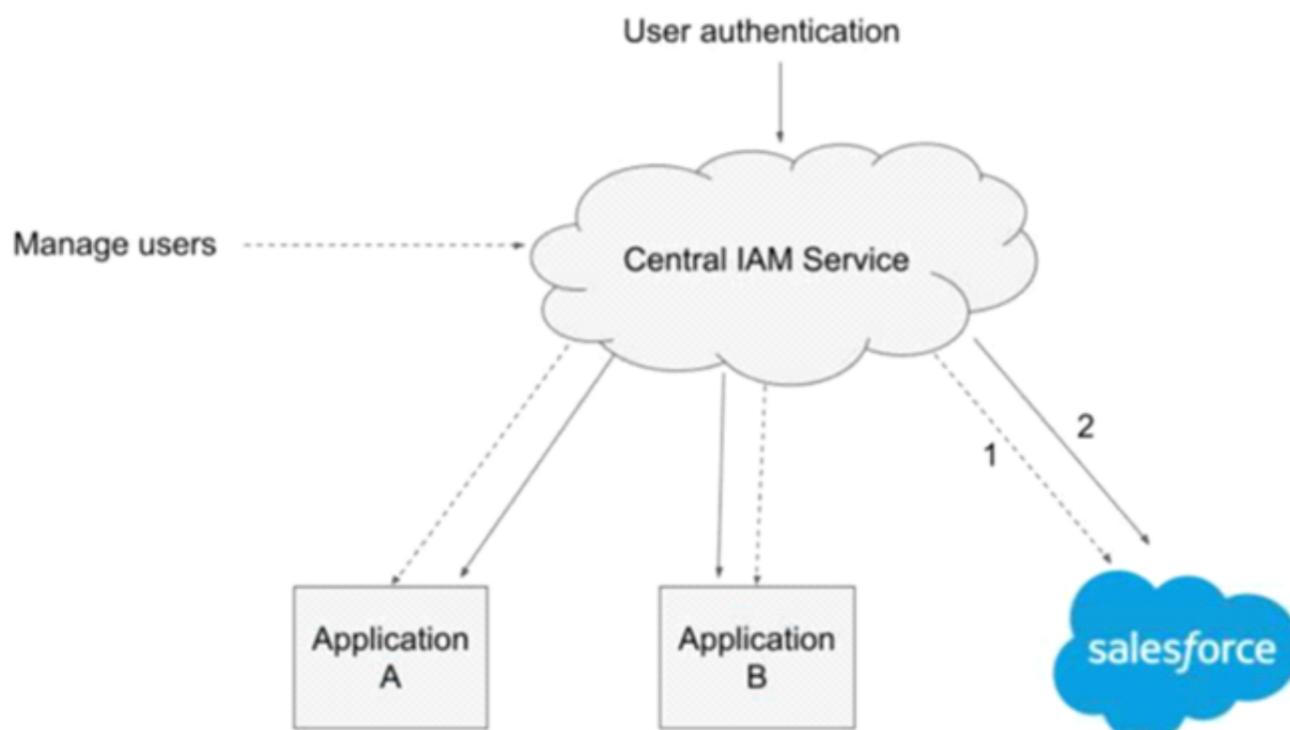
1 - Change of a user status in the central IAM Service triggers provisioning or deprovisioning in the integrated cloud applications.
2 - Security Assertion Markup Language single sign-on (SSO) is used to facilitate access for users authenticated at identity provider (Central IAM Service).
Which approach should an IAM architect implement on Salesforce Sales Cloud to meet the requirements?

A. A Configure Salesforce as a SAML Service Provider, and enable SCIM (System for Cross-Domain Identity Management) for provisioning and deprovisioning of users.
B. Configure Salesforce as a SAML service provider, and enable Just-in Time (JIT) provisioning and deprovisioning of users.
C. Configure central IAM Service as an authentication provider and extend registration handler to manage 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

**Explanation:**
To meet the requirements of using a central cloud-based IAM service for authentication and user management, the IAM architect should implement Salesforce Sales Cloud as a SAML service provider and enable SCIM for provisioning and deprovisioning of users. SAML is a protocol that allows users to authenticate and authorize with an external identity provider and access Salesforce resources. By configuring Salesforce as a SAML service provider, the IAM architect can use the central IAM service as an identity provider and enable single sign-on for users. SCIM is a standard that defines how to manage user identities across different systems. By enabling SCIM in Salesforce, the IAM architect can synchronize user data between the central IAM service and Salesforce and automate user provisioning and deprovisioning based on the changes made in the central IAM service. References: SAML Single Sign-On Settings, SCIM User Provisioning for Connected Apps

**NEW QUESTION 69**
Universal Containers (UC) has built a custom token-based Two-factor authentication (2FA) system for their existing on-premise applications. They are now implementing Salesforce and would like to enable a
Two-factor login process for it, as well. What is the recommended solution as Architect should consider?

A. Use the custom 2FA system for on-premise applications and native 2FA for Salesforce.
B. Replace the custom 2FA system with an AppExchange App that supports on premise application and salesforce.
C. Use Custom Login Flows to connect to the existing custom 2FA system for use in Salesforce.
D. Replace the custom 2FA system with Salesforce 2FA for on-premise applications and Salesforce.

**Answer:** D

**Explanation:**
The recommended solution for UC to enable a two-factor login process for Salesforce and their existing
on-premise applications is to replace the custom 2FA system with Salesforce 2FA for on-premise applications and Salesforce. Salesforce 2FA is a feature that requires users to verify their identity with a second factor, such as a verification code or a mobile app, after entering their username and password. Salesforce 2FA can be enabled for both Salesforce and on-premise applications by using one of the following methods:

➤ Use Salesforce Authenticator, a mobile app that generates verification codes or sends push notifications to users' devices.

➤ Use a third-party authenticator app, such as Google Authenticator or Microsoft Authenticator, that generates verification codes based on a shared secret key.

➤ Use a verification code sent by email or SMS to users' registered email address or phone number.

➤ Use a U2F security key, such as YubiKey, that plugs into users' devices and provides a physical token. By replacing the custom 2FA system with Salesforce 2FA, UC can benefit from the following advantages:

➤ Improved security and compliance by using a standard and proven 2FA solution that protects against
phishing, credential theft, and brute force attacks.

➤ Reduced complexity and cost by eliminating the need to maintain a custom 2FA system and integrating it with Salesforce.

➤ Enhanced user experience and convenience by providing multiple options for verifying identity and allowing users to remember trusted devices or browsers.
The other options are not recommended solutions for this scenario. Using the custom 2FA system for
on-premise applications and native 2FA for Salesforce would create inconsistency and confusion for users who have to use different methods of verification for different applications. Replacing the custom 2FA system with an AppExchange app that supports on-premise applications and Salesforce would require UC to find an app that meets their specific needs and pay for its license and maintenance. Using custom login flows to connect to the existing custom 2FA system for use in Salesforce would require UC to write custom code and logic to invoke the custom 2FA system from Salesforce, which could introduce security and performance issues. References: [Two-Factor Authentication], [Salesforce Authenticator], [Third-Party Authenticator Apps], [Verification Code via Email or SMS], [U2F Security Keys], [Custom Login Flows]

**NEW QUESTION 74**
Universal Containers (UC) has five Salesforce orgs (UC1, UC2, UC3, UC4, UC5). of Every user that is in UC2, UC3, UC4, and UC5 is also in UC1, however not all users 65* 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:** C

**Explanation:**
The best approach to simplify the authentication process and reduce cost and maintenance is to configure UC1 as the Identity Provider to the other four Salesforce orgs and set up JIT user provisioning on all other
orgs. This way, users can log in to any of the five orgs using their UC1 credentials, and their user accounts wil be automatically created or updated in the other orgs based on the information from UC11. This eliminates the need to purchase a third-party Identity Provider or manually provision users in advance. The other options are not optimal for this requirement because:

➤ Purchasing a third-party Identity Provider for all five Salesforce orgs would incur additional cost and maintenance, and would not leverage the existing user base in UC1.

➤ Not setting up JIT user provisioning for other orgs would require manually creating or updating user accounts in each org, which would be time-consuming and error-prone. References: Salesforce as an Identity Provider, Identity Providers and Service Providers, Just-in-Time Provisioning for SAML

**NEW QUESTION 77**
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.
Which two considerations should the architect keep in mind? Choose 2 answers

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:** AB

**Explanation:**
The AMR field in the Login History shows the authentication methods used at the IdP level, such as password, MFA, or SSO. Both OIDC and SAML are supported protocols for SSO, but the IdP must implement the AMR attribute and pass it to Salesforce. References: Secure Your Users' Identity, Salesforce Multi-Factor Authentication (MFA) and Single Sign-on (SSO)

**NEW QUESTION 78**
Universal containers (UC) has a mobile application that calls the salesforce REST API. In order to prevent users from having to enter their credentials everytime they use the app, UC has enabled the use of refresh Tokens as part of the salesforce connected App and updated their mobile app to take advantage of the refresh token. Even after enabling the refresh token, Users are still complaining that they have to enter their credentials once a day. What is the most likely cause of the issue?

A. The Oauth authorizations are being revoked by a nightly batch job.
B. The refresh token expiration policy is set incorrectly in salesforce
C. The app is requesting too many access Tokens in a 24-hour period
D. The users forget to check the box to remember their credentials.

**Answer:** B

**Explanation:**
The most likely cause of the issue is that the refresh token expiration policy is set incorrectly in Salesforce. A refresh token is a credential that allows a connected app to obtain a new access token when the previous one expires1. The refresh token expiration policy determines how long a refresh token is valid for2. If the policy is set to a short duration, such as 24 hours, the users have to enter their credentials once a day to get a new refresh token. To prevent this, the policy should be set to a longer duration, such as "Refresh token is valid until revoked" or "Refresh token expires after 90 days of inactivity"2.
References: OAuth 2.0 Refresh Token Flow, Manage OAuth Access Policies for a Connected App

**NEW QUESTION 79**
Universal Containers is implementing Salesforce Identity to broker authentication from its enterprise single sign-on (SSO) solution through Salesforce to third party applications using SAML.
What rote does Salesforce Identity play in its relationship with the enterprise SSO system?

A. Identity Provider (IdP)
B. Resource Server
C. Service Provider (SP)
D. Client Application

**Answer:** C

**Explanation:**
To broker authentication from its enterprise SSO solution through Salesforce to third party applications using SAML, Salesforce Identity plays the role of a Service Provider (SP). A SP is an entity that relies on an Identity Provider (IdP) to authenticate and authorize users. In this scenario, the enterprise SSO solution is the IdP, Salesforce is the SP, and the third party applications are the Resource Servers or Client Applications. The SP receives a SAML assertion from the IdP and uses it to obtain an access token from the Resource Server or Client Application. References: SAML Single Sign-On Settings, Authorize Apps with OAuth

**NEW QUESTION 81**
Universal Containers (UC) is using its production org as the identity provider for a new Experience Cloud site and the identity architect is deciding which login experience to use for the site. Which two page types are valid login page types for the site?
Choose 2 answers

A. Experience Builder Page
B. lightning Experience Page
C. Login Discovery Page
D. Embedded Login Page

**Answer:** CD

**Explanation:**
Login Discovery Page and Embedded Login Page are two valid login page types for Experience Cloud sites. Login Discovery Page allows users to choose their preferred login method, such as username/password, SSO, or social sign-on. Embedded Login Page allows users to log in from any site page without being redirected to a separate login page. References: Login Discovery Page, Embedded Login

**NEW QUESTION 86**
Universal Containers would like its customers to register and log in to a portal built on Salesforce Experience Cloud. Customers should be able to use their Facebook or LinkedIn credentials for ease of use.
Which three steps should an identity architect take to implement social sign-on? Choose 3 answers

A. Register both Facebook and LinkedIn as connected apps.

B. Create authentication providers for both Facebook and LinkedIn.
C. Check "Facebook" and "LinkedIn" under Login Page Setup.
D. Enable "Federated Single Sign-On Using SAML".
E. Update the default registration handlers to create and update users.

**Answer:** BCE

**Explanation:**
To implement social sign-on for customers to register and log in to a portal built on Salesforce Experience Cloud using their Facebook or LinkedIn credentials, the identity architect should take three steps:

≫ Create authentication providers for both Facebook and LinkedIn. Authentication providers are configurations that enable users to authenticate with an external identity provider and access Salesforce resources. Salesforce provides predefined authentication providers for some common identity providers, such as Facebook and LinkedIn, which can be easily configured with minimal customization.

≫ Check "Facebook" and "LinkedIn" under Login Page Setup. Login Page Setup is a setting that allows administrators to customize the login page for Experience Cloud sites. By checking "Facebook" and "LinkedIn", the identity architect can enable social sign-on buttons for these identity providers on the login page.

≫ Update the default registration handlers to create and update users. Registration handlers are classes that implement the Auth.RegistrationHandler interface and define how to create or update users in Salesforce based on the information from the external identity provider. The identity architect can update the default registration handlers to link the user's social identity with their Salesforce identity and prevent duplicate accounts. References: Authentication Providers, Social Sign-On with Authentication Providers, Login Page Setup, Create a Custom Registration Handler

**NEW QUESTION 90**
Universal Containers (UC) has an existing e-commerce platform and is implementing a new customer community. They do not want to force customers to register on both applications due to concern over the customers experience. It is expected that 25% of the e-commerce customers will utilize the customer community .
The e-commerce platform is capable of generating SAML responses and has an existing
REST-ful API capable of managing users. How should UC create the identities of its e-commerce users with the customer community?

A. Use SAML JIT in the Customer Community to create users when a user tries to login to the community from the e-commerce site.
B. Use the e-commerce REST API to create users when a user self-register on the customer community and use SAML to allow SSO.
C. Use a nightly batch ETL job to sync users between the Customer Community and the e-commerce platform and use SAML to allow SSO.
D. Use the standard Salesforce API to create users in the Community When a User is Created in the e-Commerce platform and use SAML to allow SSO.

**Answer:** A

**Explanation:**
The best option for UC to create the identities of its e-commerce users with the customer community is to use SAML JIT in the customer community to create users when a user tries to login to the community from the e-commerce site. SAML JIT (Just-in-Time) is a feature that allows Salesforce to create or update user accounts based on the information provided in a SAML assertion from an identity provider (IdP). This feature enables UC to avoid duplicating user registration on both applications and provide a seamless single sign-on (SSO) experience for its customers. The other options are not optimal for this scenario. Using the e-commerce REST API to create users when a user self-registers on the customer community would require the user to register twice, once on the e-commerce site and once on the customer community, which would degrade the customer experience. Using a nightly batch ETL job to sync users between the customer community and the e-c ommerce platform would introduce a delay in user creation and synchronization, which could cause errors or inconsistencies. Using the standard Salesforce API to create users in the community when a user is created in the e-commerce platform would require UC to write custom code and maintain API integration, which could increase complexity and cost. References: [Just-in-Time Provisioning for SAML], [Single Sign-On], [SAML SSO Flows]

**NEW QUESTION 94**
Northern Trail Outfitters manages application functional permissions centrally as Active Directory groups. The CRM_SuperlIser and CRM_Reportmg_SuperUser groups should respectively give the user the SuperUser and Reportmg_SuperUser permission set in Salesforce. Salesforce is the service provider to a Security Assertion Markup Language (SAML) identity provider.
Mow should an identity architect ensure the Active Directory groups are reflected correctly when a user accesses Salesforce?

A. Use the Apex Just-in-Time handler to query standard SAML attributes and set permission sets.
B. Use the Apex Just-in-Time handler to query custom SAML attributes and set permission sets.
C. Use a login flow to query custom SAML attributes and set permission sets.
D. Use a login flow to query standard SAML attributes and set permission sets.

**Answer:** B

**Explanation:**
Using the Apex Just-in-Time handler to query custom SAML attributes and set permission sets is the best way to ensure that the Active Directory groups are reflected correctly when a user accesses Salesforce. The Apex Just-in-Time handler is a custom class that can process the SAML response from the identity provider and assign permission sets based on the user's AD groups. The other options are either not feasible or not effective for this use case. References: Just-in-Time Provisioning for SAML, Apex Just-in-Time Handler

**NEW QUESTION 97**
Universal containers (UC) would like to enable SAML-BASED SSO for a salesforce partner community. UC has an existing ldap identity store and a third-party portal. They would like to use the existing portal as the primary site these users' access, but also want to allow seamless access to the partner community. What SSO flow should an architect recommend?

A. User-Agent
B. IDP-initiated
C. Sp-Initiated
D. Web server

**Answer:** B

**Explanation:**
IDP-initiated SSO flow is when the user starts at the identity provider (IDP) site and then is redirected to the service provider (SP) site with a SAML assertion. This flow is suitable for UC's scenario because they want to use their existing portal as the primary site and also enable seamless access to the partner community.

The IDP-initiated flow does not require the user to log in again at the SP site, which is Salesforce in this case.
References: SAML SSO Flows, Single Sign-On, Salesforce Community Single Sign-on (SSO)

## NEW QUESTION 102
Northern Trail Outfitters (NTO) uses Salesforce Experience Cloud sites (previously known as Customer Community) to provide a digital portal where customers can login using their Google account.
NTO would like to automatically create a case record for first time users logging into Salesforce Experience Cloud.
What should an Identity architect do to fulfill the requirement?

A. Configure an authentication provider for Social Login using Google and a custom registration handler.
B. Implement a Just-in-Time handler class that has logic to create cases upon first login.
C. Create an authentication provider for Social Login using Google and leverage standard registration handler.
D. Implement a login flow with a record create component for Case.

**Answer:** D

**Explanation:**
To automatically create a case record for first time users logging into Salesforce Experience Cloud using their Google account, the identity architect should implement a login flow with a record create component for Case. A login flow is a custom post-authentication process that can be used to add additional screens or logic after a user logs in to Salesforce. A record create component is a type of flow element that can be used to create a new record in Salesforce. By implementing a login flow with a record create component for Case, the identity architect can check if the user is logging in for the first time using their Google account and create a case record accordingly. References: Login Flows, Record Create Element

## NEW QUESTION 104
Universal Containers (UC) is implementing Salesforce and would like to establish SAML SSO for its users to log in. UC stores its corporate user identities in a Custom Database. The UC IT Manager has heard good things about Salesforce Identity Connect as an Idp, and would like to understand what limitations they may face if they decided to use Identity Connect in their current environment. What limitation Should an Architect inform the IT Manager about?

A. Identity Connect will not support user provisioning in UC's current environment.
B. Identity Connect will only support Idp-initiated SAML flows in UC's current environment.
C. Identity Connect will only support SP-initiated SAML flows in UC's current environment.
D. Identity connect is not compatible with UC's current identity environment.

**Answer:** A

**Explanation:**
Identity Connect will not support user provisioning in UC's current environment. Identity Connect is a tool that synchronizes user data between Active Directory and Salesforce, but it does not work with other identity sources such as a Custom Database5. Therefore, if UC wants to use Identity Connect as an Idp, they will not be able to provision users from their Custom Database to Salesforce.
Options B, C, and D are incorrect because Identity Connect does not have any limitations on the type of SAML flow or the compatibility with UC's current identity environment. Identity Connect supports both Idp-initiated and SP-initiated SAML flows6, and it can act as an Idp for any external service provider that supports SAML 2.07.
References: 5: Identity Connect - Salesforce 6: SAML SSO Flows - Salesforce 7: Salesforce Connect: Integration, Benefits, and Limitations

## NEW QUESTION 107
A global fitness equipment manufacturer uses Salesforce to manage its sales cycle. The manufacturer has a custom order fulfillment app that needs to request order data from Salesforce. The order fulfillment app needs to integrate with the Salesforce API using OAuth 2.0 protocol.
What should an identity architect use to fulfill this requirement?

A. Canvas App Integration
B. OAuth Tokens
C. Authentication Providers
D. Connected App and OAuth scopes

**Answer:** D

**Explanation:**
To integrate the order fulfillment app with the Salesforce API using OAuth 2.0 protocol, the identity architect should use a Connected App and OAuth scopes. A Connected App is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as OAuth 2.0. OAuth scopes are permissions that define the specific data that an external application can access or modify in Salesforce. To use OAuth 2.0 protocol, the identity architect needs to configure a Connected App in Salesforce and assign the appropriate OAuth scopes to it, such as "api" or "full". References: Connected Apps, OAuth Scopes

## NEW QUESTION 111
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:**
To enable SP-initiated SSO with Salesforce as the Service Provider, two steps are required in Salesforce:

≫ Option A is correct because configuring SAML SSO settings involves specifying the identity provider details, such as the entity ID, login URL, logout URL, and certificate2.

≫ Option D is correct because setting up My Domain enables you to use a custom domain name for your Salesforce org and allows you to use SAML as an authentication method3.

≫ Option B is incorrect because creating a connected app is not necessary for SP-initiated SSO using a SAML-compliant IdP. A connected app is used for OAuth-based authentication or OpenID Connect-based authentication4.

≫ Option C is incorrect because configuring delegated authentication is not related to SP-initiated SSO using a SAML-compliant IdP. Delegated authentication is a feature that allows Salesforce to delegate user authentication to an external service, such as LDAP or Active Directory5.
References: SAML-based single sign-on: Configuration and Limitations, Configure SAML single
sign-on with an identity provider, My Domain, Create a Connected App, Configure Salesforce for Delegated Authentication

**NEW QUESTION 115**
Universal Containers (UC) has implemented SAML-based Single Sign-On to provide seamless access to its Salesforce Orgs, financial system, and CPQ system. Below is the SSO implementation landscape.
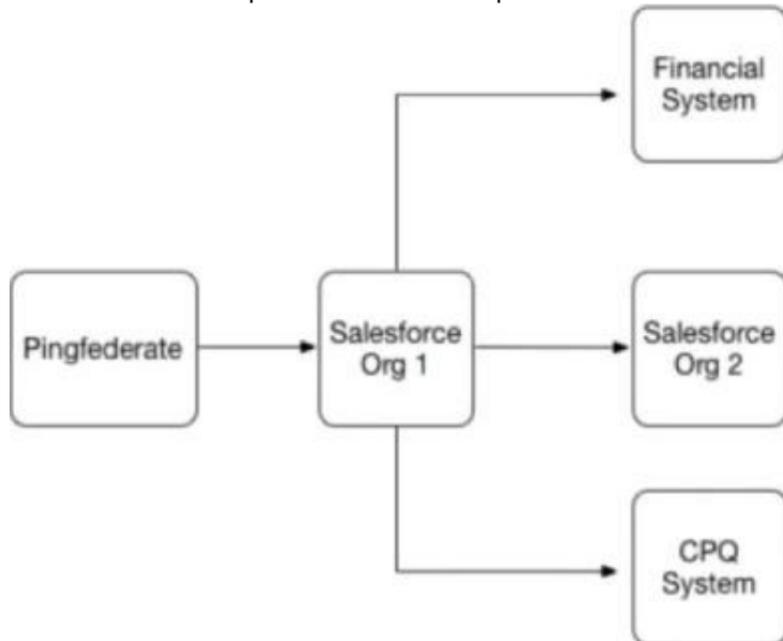


What role combination is represented by the systems in this scenario''

A. Financial System and CPQ System are the only Service Providers.
B. Salesforce Org1 and Salesforce Org2 are the only Service Providers.
C. Salesforce Org1 and Salesforce Org2 are acting as Identity Providers.
D. Salesforce Org1 and PingFederate are acting as Identity Providers.

**Answer:** B

**Explanation:**
In a SAML-based SSO scenario, the identity provider (IdP) is the system that performs authentication and passes the user's identity and authorization level to the service provider (SP), which trusts the IdP and authorizes the user to access the requested resource1. In this case, PingFederate is the IdP that authenticates users for UC and sends SAML assertions to the SPs. The SPs are the systems that rely on PingFederate for authentication and provide access to their services based on the SAML assertions. The SPs in this scenario are Salesforce Org1, Salesforce Org2, Financial System, and CPQ System2. Therefore, the correct answer is B.
References:

≫ SAML web-based authentication guide

≫ SAML-based single sign-on: Configuration and Limitations

**NEW QUESTION 116**
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:** CD

**Explanation:**
Using the identity provider's certificate to digitally sign and encrypt the payload, and using a custom login flow to retrieve sensitive data using an Apex callout without including the attributes in the assertion are two methods that can ensure that the sensitive data cannot be tampered with, nor accessible to anyone while in transit. Option A is not a good choice because using Salesforce's certificate to encrypt the payload may not work, as Salesforce does not support encrypted SAML assertions. Option B is not a good choice because using Salesforce's certificate to digitally sign the SAML assertion may not be necessary, as Salesforce does not validate digital signatures on SAML assertions. Also, using a mobile device management client on the users' mobile devices may not be relevant, as it does not affect how the sensitive data is transmitted between the identity provider and Salesforce.
References: [Single Sign-On Implementation Guide], [Customizing User Authentication with Login Flows]

**NEW QUESTION 120**
A global company is using the Salesforce Platform as an Identity Provider and needs to integrate a third-party application with its Experience Cloud customer

portal.
Which two features should be utilized to provide users with login and identity services for the third-party application?
Choose 2 answers

A. Use the App Launcher with single sign-on (SSO).
B. External a Data source with Named Principal identity type.
C. Use a connected app.
D. Use Delegated Authentication.

**Answer:** AC

**Explanation:**
Using the App Launcher with SSO and using a connected app are two features that can be utilized to provide users with login and identity services for the third-party application. The App Launcher allows users to access multiple apps from one location with SSO. The connected app allows users to authorize access to the third-party application using OAuth 2.0. The other options are either not relevant or not applicable for this use case. References: App Launcher, Connected Apps

**NEW QUESTION 121**
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. Setup Salesforce as an identity provider (IdP) for order Tracking.
B. Set up the Corporate Identity store as an identity provider (IdP) for Order Tracking,
C. Customize Order Tracking to initiate a REST call to validate users in Salesforce after login.
D. Setup Order Tracking as a Canvas app in Salesforce to POST IdP initiated SAML assertion.

**Answer:** AD

**Explanation:**
Single sign-on (SSO) is an authentication method that allows users to access multiple applications with one login and one set of credentials. SAML is an open standard for SSO that uses XML-based messages to exchange authentication and authorization information between an identity provider (IdP) and a service provider (SP). To fulfill the requirement, the following steps should be done:

≫ Setup Salesforce as an identity provider (IdP) for order tracking. An IdP is the system that performs authentication and passes the user's identity and authorization level to the SP, which trusts the IdP and authorizes the user to access the requested resource. To set up Salesforce as an IdP, you need to enable the Identity Provider feature, download the IdP certificate, and configure the SAML settings.

≫ Setup order tracking as a Canvas app in Salesforce to POST IdP initiated SAML assertion. A Canvas app is an application that can be embedded within a Salesforce page and interact with Salesforce data and APIs. To set up order tracking as a Canvas app, you need to create a connected app for order tracking in Salesforce, enable SAML and configure the SAML settings, such as the entity ID, ACS URL, and subject type. You also need to enable IdP initiated SAML assertion POST binding for the connected app, which allows Salesforce to initiate the SSO process by sending a SAML assertion to order tracking.
References:
≫ [SAML Single Sign-On]
≫ [Set Up Your Domain as an Identity Provider]
≫ [Canvas Apps]
≫ [Create a Connected App for Your Canvas App]
≫ [IdP Initiated SAML Assertion POST Binding]

**NEW QUESTION 125**
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:** AC

**Explanation:**
The OAuth 2.0 user-agent flow and the OAuth 2.0 web server flow are both suitable for building a custom mobile app that can access Salesforce data without prompting the user to log in again1. Both of these flows use a refresh token that can be used to obtain a new access token when the previous one expires2. The user-agent flow uses the Canvas JavaScript SDK to obtain an OAuth token by using the login function in the SDK2. The web server flow redirects the user to the Salesforce OAuth authorization endpoint and then obtains an OAuth access token by making a POST request to the Salesforce OAuth token endpoint2. The mobile agent flow and the SAML assertion flow are not valid OAuth flows for Salesforce3.
References: OAuth Authorization Flows, Mastering Salesforce Canvas Apps, Access Data with API Integration

**NEW QUESTION 126**
Northern Trail Outfitters recently acquired a company. Each company will retain its Identity Provider (IdP). Both companies rely extensively on Salesforce processes that send emails to users to take specific actions in Salesforce.
How should the combined companys' employees collaborate in a single Salesforce org, yet authenticate to the appropriate IdP?

A. Configure unique MyDomains for each company and have generated links use the appropriate MyDomam in the URL.
B. Have generated links append a querystnng parameter indicating the Id
C. The login service will redirect to the appropriate IdP.
D. Have generated links be prefixed with the appropriate IdP URL to invoke an IdP-initiated Security Assertion Markup Language flow when clicked.
E. Enable each IdP as a login option in the MyDomain Authentication Service setting

F. Users will then click on the appropriate IdP button.

**Answer:** D

**Explanation:**
To allow employees to collaborate in a single Salesforce org, yet authenticate to the appropriate IdP, the identity architect should enable each IdP as a login option in the MyDomain Authentication Service settings. Users will then click on the appropriate IdP button. MyDomain is a feature that allows administrators to customize the Salesforce login URL with a unique domain name. Authentication Service is a setting that allows administrators to enable different authentication options for users, such as social sign-on or single
sign-on with an external IdP. By enabling each IdP as a login option in the MyDomain Authentication Service settings, the identity architect can provide a user-friendly and secure way for employees to log in to Salesforce using their preferred IdP. References: MyDomain, Authentication Service

**NEW QUESTION 131**
Universal Containers (UC) wants its closed Won opportunities to be synced to a Data Warehouse in near real time. UC has implemented Outbound Message to enable near real-time data sync. UC wants to ensure that communication between Salesforce and Target System is Secure. What Certificate is sent along with the Outbound Message?

A. The CA-Signed Certificate from the Certificate and Key Management menu.
B. The default Client Certificate from the Develop--> API Menu.
C. The default Client Certificate or a Certificate from Certificate and Key Management menu.
D. The Self-Signed Certificates from the Certificate & Key Management menu.

**Answer:** A

**Explanation:**
The CA-Signed Certificate from the Certificate and Key Management menu is the certificate that is sent along with the outbound message. An outbound message is a SOAP message that is sent from Salesforce to an external endpoint when a workflow rule or approval process is triggered. To ensure that the communication between Salesforce and the target system is secure, the outbound message can be signed with a certificate that is generated or uploaded in the Certificate and Key Management menu. The certificate must be CA-Signed, which means that it is issued by a trusted certificate authority (CA) that verifies the identity of the sender. The other options are not valid certificates for this purpose. The default client certificate from the Develop–> API Menu is a self-signed certificate that is used for testing purposes only and does not provide adequate security. The default client certificate or a certificate from Certificate and Key Management menu is too vague and does not specify whether the certificate is CA-Signed or self-signed. The self-signed certificates from the Certificate & Key Management menu are certificates that are generated by Salesforce without any verification by a CA, and they are not recommended for production use.
References: [Outbound Messages], [Sign Outbound Messages with a Certificate], [CA-Signed Certificates], [Default Client Certificate], [Self-Signed Certificates]

**NEW QUESTION 132**
Universal containers (UC) has decided to use identity connect as it's identity provider. UC uses active directory(AD) and has a team that is very familiar and comfortable with managing ad groups. UC would like to use AD groups to help configure salesforce users. Which three actions can AD groups control through identity connect? Choose 3 answers

A. Public Group Assignment
B. Granting report folder access
C. Role Assignment
D. Custom permission assignment
E. Permission sets assignment

**Answer:** ACE

**Explanation:**
AD groups can control public group assignment, role assignment, and permission set assignment through Identity Connect. Identity Connect is a tool that integrates Microsoft Active Directory (AD) user accounts with Salesforce user records1. It allows Salesforce admins to leverage the existing user data and group memberships in AD to automate user provisioning and deprovisioning in Salesforce. Identity Connect can map AD groups to Salesforce public groups, roles, and permission sets, and assign them to users based on their group membership2. This way, AD groups can control the access level and visibility of users in Salesforce. AD groups cannot control granting report folder access or custom permission assignment through Identity Connect. These are not supported features of Identity Connect. Report folder access is controlled by the folder sharing settings in Salesforce. Custom permission assignment is controlled by the custom permission settings in Salesforce. References: Get to Know Identity Connect, Map Your Data, [Folder Sharing], [Custom Permissions]

**NEW QUESTION 133**
Universal Containers (UC) has Active Directory (AD) as their enterprise identity store and would like to use it for Salesforce user authentication. UC expects to synchronize user data between Salesforce and AD and Assign the appropriate Profile and Permission Sets based on AD group membership. What would be the optimal way to implement SSO?

A. Use Active Directory with Reverse Proxy as the Identity Provider.
B. Use Microsoft Access control Service as the Authentication provider.
C. Use Active Directory Federation Service (ADFS) as the Identity Provider.
D. Use Salesforce Identity Connect as the Identity Provider.

**Answer:** D

**Explanation:**
The optimal way to implement SSO with Active Directory as the enterprise identity store is to use Salesforce Identity Connect as the identity provider. Salesforce Identity Connect is a software that integrates Microsoft Active Directory with Salesforce and enables single sign-on (SSO) using SAML. It also allows user data synchronization between Active Directory and Salesforce and profile and permission set assignment based on Active Directory group membership. Option A is not a good choice because using Active Directory with reverse proxy as the identity provider may not be supported by Salesforce or may require additional configuration and customization. Option B is not a good choice because using Microsoft Access Control Service as the authentication provider may not be available, as Microsoft has retired this service in 2018. Option C is not a good choice because using Active Directory Federation Service (ADFS) as the identity provider may not allow user data synchronization or profile and permission set assignment based on Active Directory group membership, unless it is combined with another tool such as Salesforce Identity Connect.
References: Salesforce Identity Connect Implementation Guide, Single Sign-On Implementation Guide

**NEW QUESTION 137**
Northern Trail Outfitters (NTO) is launching a new sportswear brand on its existing consumer portal built on Salesforce Experience Cloud. As part of the launch, emails with promotional links will be sent to existing customers to log in and claim a discount. The marketing manager would like the portal dynamically branded so that users will be directed to the brand link they clicked on; otherwise, users will view a recognizable NTO-branded page.
The campaign is launching quickly, so there is no time to procure any additional licenses. However, the development team is available to apply any required changes to the portal.
Which approach should the identity architect recommend?

A. Create a full sandbox to replicate the portal site and update the branding accordingly.
B. Implement Experience ID in the code and extend the URLs and endpoints, as required.
C. Use Heroku to build the new brand site and embedded login to reuse identities.
D. Configure an additional community site on the same org that is dedicated for the new brand.

**Answer:** B

**Explanation:**
To dynamically brand the portal so that users will be directed to the brand link they clicked on, the identity architect should recommend implementing Experience ID in the code and extending the URLs and endpoints, as required. Experience ID is a parameter that can be used to identify different brands or experiences within a single Experience Cloud site (formerly known as Community). Dynamic branding is a feature that allows Experience Cloud sites to display different branding elements, such as logos, colors, or images, based on the Experience ID or other criteria. By implementing Experience ID in the code, the identity architect can provide a consistent and personalized brand experience for each user without creating multiple sites or sandboxes. References: Experience ID, Dynamic Branding for Experience Cloud Sites

**NEW QUESTION 139**
A technology enterprise is planning to implement single sign-on login for users. When users log in to the Salesforce User object custom field, data should be populated for new and existing users.
Which two steps should an identity architect recommend? Choose 2 answers

A. Implement Auth.SamlJitHandler Interface.
B. Create and update methods.
C. Implement RegistrationHandler Interface.
D. Implement SesslonManagement Class.

**Answer:** AB

**Explanation:**
To populate data for new and existing users in the Salesforce User object custom field when they log in using SSO, the identity architect should implement the Auth.SamlJitHandler interface and create and update methods. The Auth.SamlJitHandler interface is an interface that defines how to handle SAML assertions for Just-in-Time (JIT) provisioning. JIT provisioning is a feature that allows Salesforce to create or update user records on the fly when users log in through an external identity provider. The create and update methods are methods in the Auth.SamlJitHandler interface that define how to create or update users in Salesforce based on the information from the SAML assertion. References: Auth.SamlJitHandler Interface, Just-in-Time Provisioning for SAML and OpenID Connect

**NEW QUESTION 143**
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:**
The recommended way to configure the IdP for seamless access is to use IdP-initiated SSO that passes the SAML token upon Salesforce resource access request. This means that the user logs in to the corporate portal first, and then clicks a link to access a Salesforce resource. The IdP sends a SAML response to Salesforce with the user's identity and other attributes. Salesforce verifies the SAML response and logs in the user to the appropriate Salesforce org and community12. This way, the user does not have to log in again to Salesforce or enter any credentials3. References: 1: SAML SSO with Salesforce as the Service Provider 2: Set Up Single Sign-On for Your Internal Users Unit | Salesforce - Trailhead 3: What is IdP-Initiated Single Sign-On? – OneLogin

**NEW QUESTION 144**
An architect has successfully configured SAML-BASED SSO for universal containers. SSO has been working for 3 months when Universal containers manually adds a batch of new users to salesforce. The new users receive an error from salesforce when trying to use SSO. Existing users are still able to successfully use SSO to access salesforce. What is the probable cause of this behaviour?

A. The administrator forgot to reset the new user's salesforce password.
B. The Federation ID field on the new user records is not correctly set
C. The my domain capability is not enabled on the new user's profile.
D. The new users do not have the SSO permission enabled on their profiles.

**Answer:** B

**Explanation:**
The Federation ID field on the new user records is not correctly set is the probable cause of this behavior. The Federation ID is an additional field contained in the Salesforce interface that allows admins to pick whatever username or username format they want to pass to Salesforce from their user directory for single sign-on. This field does not appear on the user page layout editor or on the user record page by default, and it must be populated with a unique value that matches the identity provider's assertion for each user. If the Federation ID is missing or incorrect, the SSO will fail. The administrator does not need to reset the new user's Salesforce password, as SSO bypasses the password authentication. The My Domain capability is not enabled on the new user's profile, but on the org level, so it does not affect individual users. The new users do not have the SSO permission enabled on their profiles is not a valid option, as there is no such permission in

Salesforce.
References: Certification - Identity and Access Management Architect - Trailhead, Federation ID field on Us detail page is not visible, What is the purpose of Salesforce SSO by federation ID?

**NEW QUESTION 149**
Northern Trail Outfitters (NTO) has a number of employees who do NOT need access Salesforce objects. Trie employees should sign in to a custom Benefits web app using their Salesforce credentials.
Which license should the identity architect recommend to fulfill this requirement?

A. Identity Only License
B. External Identity License
C. Identity Verification Credits Add-on License
D. Identity Connect License

**Answer:** A

**Explanation:**
To allow employees to sign in to a custom Benefits web app using their Salesforce credentials, the identity architect should recommend the Identity Only License. The Identity Only License is a license type that enables users to access external applications that are integrated with Salesforce using single sign-on (SSO) or delegated authentication, but not access Salesforce objects or data. The other license types are not relevant for this scenario. References: Identity Only License, User Licenses

**NEW QUESTION 150**
Universal containers (UC) wants to implement a partner community. As part of their implementation, UC would like to modify both the Forgot password and change password experience with custom branding for their partner community users. Which 2 actions should an architect recommend to UC? Choose 2 answers

A. Build a community builder page for the change password experience and Custom Visualforce page for the Forgot password experience.
B. Build a custom visualforce page for both the change password and Forgot password experiences.
C. Build a custom visualforce page for the change password experience and a community builder page for the Forgot password experience.
D. Build a community builder page for both the change password and Forgot password experiences.

**Answer:** BC

**Explanation:**
The two actions that an architect should recommend to UC are to build a custom Visualforce page for both the change password and forgot password experiences and to build a custom Visualforce page for the change password experience and a community builder page for the forgot password experience. A custom Visualforce page is a page that uses Visualforce markup and Apex code to create a custom user interface. A community builder page is a page that uses the Community Builder tool to create a custom user interface with drag-and-drop components. Both types of pages can be used to modify the look and feel of the password management features for partner community users. However, using a custom Visualforce page for both features requires more coding and customization, while using a community builder page for the forgot password feature allows more flexibility and configuration options.
References: [Visualforce Pages], [Community Builder Pages], [Customize Password Management Features]

**NEW QUESTION 155**
Universal Containers is implementing a new Experience Cloud site and the identity architect wants to use dynamic branding features as of the login process.
Which two options should the identity architect recommend to support dynamic branding for the site? Choose 2 answers

A. To use dynamic branding, the community must be built with the Visuaiforce + Salesforce Tabs template.
B. To use dynamic branding, the community must be built with the Customer Account Portal template.
C. An experience ID (expid) or placeholder parameter must be used in the URL to represent the brand.
D. An external content management system (CMS) must be used for dynamic branding on Experience Cloud sites.

**Answer:** BC

**Explanation:**
Dynamic branding is a feature that allows Experience Cloud sites to display different branding elements, such as logos, colors, or images, based on the user's profile or preferences. To use dynamic branding, the community must be built with the Customer Account Portal template, which supports this feature. An experience ID (expid) or placeholder parameter must be used in the URL to represent the brand and trigger the dynamic branding logic.
References: Dynamic Branding for Experience Cloud Sites, Create a Customer Account Portal

**NEW QUESTION 159**
Universal containers (UC) does my domain enable in the context of a SAML SSO configuration? Choose 2 answers

A. Resource deep linking
B. App launcher
C. SSO from salesforce1 mobile app.
D. Login forensics

**Answer:** AC

**Explanation:**
Enabling My Domain in the context of a SAML SSO configuration enables resource deep linking and SSO from Salesforce1 mobile app. Resource deep linking allows users to access specific records or pages after logging in with SSO5. SSO from Salesforce1 mobile app requires using the My Domain URL as the login server4. Enabling My Domain does not affect the app launcher or login forensics features. Therefore, option A and C are the correct answers. References: Salesforce Mobile Application Single Sign-On overview, SAML SSO with Salesforce as the Service Provider, Single Sign-On, Considerations for setting up My Domain and SSO

**NEW QUESTION 163**
The CIO of universal containers(UC) wants to start taking advantage of the refresh token capability for the UC applications that utilize Oauth 2.0. UC has listed an

architect to analyze all of the applications that use Oauth flows to. See where refresh Tokens can be applied. Which two OAuth flows should the architect consider in their evaluation? Choose 2 answers

A. Web server
B. Jwt bearer token
C. User-Agent
D. Username-password

**Answer:** AC

**Explanation:**
The two OAuth flows that support refresh tokens are Web server and User-Agent. According to the Salesforce documentation2, "The web server authentication flow and user-agent flow both provide a refresh token that can be used to get a new access token." Therefore, option A and C are the correct answers.
References: Salesforce Documentation

**NEW QUESTION 165**
Universal Containers (UC) uses middleware to integrate multiple systems with Salesforce. UC has a strict, new requirement that usernames and passwords cannot be stored in any UC system. How can UC's middleware authenticate to Salesforce while adhering to this requirement?

A. Create a Connected App that supports the JWT Bearer Token OAuth Flow.
B. Create a Connected App that supports the Refresh Token OAuth Flow
C. Create a Connected App that supports the Web Server OAuth Flow.
D. Create a Connected App that supports the User-Agent OAuth Flow.

**Answer:** A

**Explanation:**
A is correct because creating a connected app that supports the JWT Bearer Token OAuth Flow allows the middleware to authenticate to Salesforce without storing usernames and passwords. The JWT Bearer Token OAuth Flow uses a certificate and a private key to sign a JSON Web Token (JWT) that contains information about the user identity and requested access. The middleware sends the JWT to Salesforce, which verifies it using the certificate and grants an access token2.
B is incorrect because creating a connected app that supports the Refresh Token OAuth Flow requires storing usernames and passwords in the middleware. The Refresh Token OAuth Flow uses a username-password authentication flow to obtain an access token and a refresh token. The middleware can use the refresh token to obtain new access tokens without user interaction, but it still needs to store the username and password for the initial authentication3.
C is incorrect because creating a connected app that supports the Web Server OAuth Flow requires user interaction to authenticate to Salesforce. The Web Server OAuth Flow redirects the user to a Salesforce login page, where they enter their credentials and grant access to the middleware. The middleware then receives an authorization code that it can exchange for an access token and a refresh token4.
D is incorrect because creating a connected app that supports the User-Agent OAuth Flow also requires user interaction to authenticate to Salesforce. The User-Agent OAuth Flow is similar to the Web Server OAuth Flow, except that it does not return a refresh token. The middleware can only use the access token until it expires5.
References: 2: Accessing Salesforce with JWT OAuth Flow 3: OAuth Authorization Flows - Salesforce 4: OAuth Authorization Flows - Salesforce 5: OAuth Authorization Flows - Salesforce

**NEW QUESTION 169**
A financial enterprise is planning to set up a user authentication mechanism to login to the Salesforce system. Due to regulatory requirements, the CIO of the company wants user administration, including passwords and authentication requests, to be managed by an external system that is only accessible via a SOAP webservice.
Which authentication mechanism should an identity architect recommend to meet the requirements?

A. OAuth Web-Server Flow
B. Identity Connect
C. Delegated Authentication
D. Just-in-Time Provisioning

**Answer:** C

**Explanation:**
Delegated Authentication is an authentication mechanism that allows Salesforce to delegate the authentication process to an external system via a SOAP webservice. The external system can manage the user administration, passwords, and authentication requests. The other options are either not suitable or not supported for this use case. References: Delegated Authentication, FAQs for Delegated Authentication

**NEW QUESTION 171**
Universal Containers (UC) has implemented SSO according to the diagram below. uses SAML while Salesforce Org 1 uses OAuth 2.0. Users usually start their day by first attempting to log into Salesforce Org 2 and then later in the day, they will log into either the Financial System or CPQ system depending upon their job position. Which two systems are acting as Identity Providers?

A. Financial System
B. Pingfederate
C. Salesforce Org 2
D. Salesforce Org 1

**Answer:** BD

**Explanation:**
These are the systems that are acting as identity providers (IdPs) in the SSO scenario. An IdP is a trusted provider that enables a customer to use single sign-on (SSO) to access other websites5. In this case, Pingfederate and Salesforce Org 1 are the IdPs that authenticate the users and issue SAML assertions or OAuth tokens to the service providers (SPs). The SPs are the websites that host apps and rely on the IdPs for authentication5. In this case, Salesforce Org 2, Financial System, and CPQ System are the SPs that receive the SAML assertions or OAuth tokens from the IdPs and grant access to the users.
Option A is incorrect because Financial System is not an IdP, but an SP. It does not authenticate the users, but receives SAML assertions from Pingfederate.
Option C is incorrect because Salesforce Org 2 is not an IdP, but an SP. It does not authenticate the users, but receives OAuth tokens from Salesforce Org 1.

References: 5: Identity Providers and Service Providers - Salesforce 6: Salesforce as Service Provider an Identity Provider for SSO

**NEW QUESTION 172**
customer service representatives at Universal containers (UC) are complaining that whenever they click on links to case records and are asked to login with SAML SSO, they are being redirected to the salesforce home tab and not the specific case record. What item should an architect advise the identity team at UC to investigate first?

A. My domain is configured and active within salesforce.
B. The salesforce SSO settings are using http post
C. The identity provider is correctly preserving the Relay state
D. The users have the correct Federation ID within salesforce.

**Answer:** C

**Explanation:**
The identity provider must correctly preserve the Relay state in order to redirect the user to the specific case record after login with SAML SSO. According to the Salesforce documentation3, "The RelayState parameter is used by SAML to indicate where the user should be redirected after they've been authenticated by the identity provider." Therefore, option C is the correct answer. References: Salesforce Documentation

**NEW QUESTION 177**
Universal Containers (UC) is building a custom employee hut) application on Amazon Web Services (AWS) and would like to store their users' credentials there. Users will also need access to Salesforce for internal operations. UC has tasked an identity architect with evaluating Afferent solutions for authentication and authorization between AWS and Salesforce.
How should an identity architect configure AWS to authenticate and authorize Salesforce users?

A. Configure the custom employee app as a connected app.
B. Configure AWS as an OpenID Connect Provider.
C. Create a custom external authentication provider.
D. Develop a custom Auth server in AWS.

**Answer:** B

**Explanation:**
To authenticate and authorize Salesforce users with AWS, the identity architect should configure AWS as an OpenID Connect Provider. OpenID Connect is a protocol that allows users to sign in with an external identity provider, such as AWS, and access Salesforce resources. To enable this, the identity architect needs to configure an OpenID Connect Authentication Provider in Salesforce and link it to a connected app. The other options are not relevant for this scenario. References: OpenID Connect Authentication Providers, Social Sign-On with OpenID Connect

**NEW QUESTION 182**
Which two things should be done to ensure end users can only use single sign-on (SSO) to login in to Salesforce?
Choose 2 answers

A. Enable My Domain and select "Prevent login from https://login.salesforce.com".
B. Request Salesforce Support to enable delegated authentication.
C. Once SSO is enabled, users are only able to login using Salesforce credentials.
D. Assign user "is Single Sign-on Enabled" permission via profile or permission set.

**Answer:** AD

**Explanation:**
To ensure end users can only use single sign-on (SSO) to log in to Salesforce, two things should be done:

➤ Enable My Domain and select "Prevent login from https://login.salesforce.com". My Domain is a feature that allows administrators to customize the Salesforce login URL with a unique domain name. By preventing login from the standard login URL, administrators can enforce SSO and restrict users from logging in with their Salesforce credentials.

➤ Assign user "is Single Sign-on Enabled" permission via profile or permission set. This permission allows users to log in to Salesforce using SSO. Users who do not have this permission will not be able to access Salesforce even if they have valid Salesforce credentials. References: My Domain, User Permissions for Single Sign-On

**NEW QUESTION 184**
Universal containers (UC) employees have salesforce access from restricted ip ranges only, to protect against unauthorized access. UC wants to rollout the salesforce1 mobile app and make it accessible from any location.
Which two options should an architect recommend? Choose 2 answers

A. Relax the ip restriction in the connect app settings for the salesforce1 mobile app
B. Use login flow to bypass ip range restriction for the mobile app.
C. Relax the ip restriction with a second factor in the connect app settings for salesforce1 mobile app
D. Remove existing restrictions on ip ranges for all types of user access.

**Answer:** AC

**Explanation:**
Relaxing the IP restriction in the connected app settings for the Salesforce1 mobile app and relaxing the IP restriction with a second factor in the connected app settings for Salesforce1 mobile app are two options that an architect should recommend. These options allow UC employees to access the Salesforce1 mobile app from any location, while still maintaining some level of security. Relaxing the IP restriction means that users can log in to the connected app from outside the trusted IP ranges defined in their profiles1. Adding a second factor means that users need to provide an additional verification method, such as a verification code or a security key, to access the app2. Using a login flow to bypass IP range restriction for the mobile app is not a recommended option because it can create a complex and inconsistent user experience3. Removing existing restrictions on IP ranges for all types of user access is not a recommended option because it can expose UC's data and applications to unauthorized access4. References: 1: Restrict Access to Trusted IP Ranges for a Connected App 2: Require Multi-Factor

Authentication for Connected Apps 3: [Custom Login Flows] 4: [Restrict Login Access by IP Address]

**NEW QUESTION 188**
Universal Containers (UC) operates in Asia, Europe and North America regions. There is one Salesforce org for each region. UC is implementing Customer 360 in Salesforce and has procured External Identity and Customer Community licenses in all orgs.
Customers of UC use Community to track orders and create inquiries. Customers also tend to move across regions frequently.
What should an identity architect recommend to optimize license usage and reduce maintenance overhead?

A. Merge three orgs into one instance of Salesforc
B. This will no longer require maintaining three separate copies of the same customer.
C. Delete contact/ account records and deactivate user if user moves from a specific region; Sync will no longer be required.
D. Contacts are required since Community access needs to be enable
E. Maintenance is a necessary overhead that must be handled via data integration.
F. Enable Contactless User in all orgs and downgrade users from Experience Cloud license to External Identity license once users have moved out of that region.

**Answer:** D

**Explanation:**
To optimize license usage and reduce maintenance overhead for customers who use Community to track orders and create inquiries and tend to move across regions frequently, the identity architect should recommend enabling Contactless User in all orgs and downgrade users from Experience Cloud license to External Identity license once users have moved out of that region. Contactless User is a feature that allows users to access Experience Cloud sites without having a contact record associated with them. External Identity is a license type that enables users to access Experience Cloud sites using social sign-on or single sign-on, but not access Salesforce objects or data. By enabling Contactless User and downgrading users from Experience Cloud license to External Identity license, the identity architect can reduce the number of contacts and licenses needed for each region and avoid data duplication and synchronization issues. References: Contactless User, External Identity License, User Licenses

**NEW QUESTION 192**
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.

**Answer:** A

**Explanation:**
The web server flow is used for web applications when server-side code needs to interact with APIs. This flow implements the OAuth 2.0 authorization code grant type, which allows the web app to obtain an access token and a refresh token from Salesforce after the user grants permission1. The web app can then use the access token to call the Salesforce APIs and use the refresh token to obtain a new access token when the previous one expires2. The other options are not valid scenarios for using the web server flow. The web server flow is not used for server-side components when page needs to be rendered, as this does not involve API calls. The web server flow is not used for mobile applications and testing legacy integrations, as these scenarios are better suited for other OAuth flows, such as the user-agent flow or the password flow3. The web server flow is not used for verifying access protected resources, as this is a general purpose of OAuth, not a specific scenario for the web server flow. References: OAuth 2.0 Web Server Flow for Web App Integration, Mastering Salesforc Canvas Apps, OAuth Authorization Flows

**NEW QUESTION 193**
architect is troubleshooting some SAML-based SSO errors during testing. The Architect confirmed that all of the Salesforce SSO settings are correct. Which two issues outside of the Salesforce SSO settings are most likely contributing to the SSO errors the Architect is encountering? Choose 2 Answers

A. The Identity Provider is also used to SSO into five other applications.
B. The clock on the Identity Provider server is twenty minutes behind Salesforce.
C. The Issuer Certificate from the Identity Provider expired two weeks ago.
D. The default language for the Identity Provider and Salesforce are Different.

**Answer:** BC

**Explanation:**
The two issues outside of the Salesforce SSO settings that are most likely contributing to the SSO errors are the clock on the identity provider server being twenty minutes behind Salesforce and the issuer certificate from the identity provider expiring two weeks ago. These issues can cause SAML assertion errors, which prevent the user from logging in with SSO. A SAML assertion is an XML document that contains information about the user's identity and attributes, and it is signed by the identity provider and sent to Salesforce as part of the SSO process4. If the clock on the identity provider server is not synchronized with Salesforce, the SAML assertion may be rejected as invalid or expired, as it has a time limit for validity5. If the issuer certificate from the identity provider is expired, the SAML assertion may not be verified by Salesforce, as it relies on the certificate to validate the signature6. The other options are not likely issues that cause SSO errors. The identity provider being used to SSO into five other applications does not affect its ability to SSO into Salesforce, as long as it supports multiple service providers and has a separate configuration for each one7. The default language for the identity provider and Salesforce being different does not affect the SSO process, as it does not impact the SAML assertion or its validation.
References: SAML Login Errors, Troubleshoot SAML Assertion Errors, SAML SSO with Salesforce as th Service Provider, Single Sign-On, [How to Troubleshoot a Single Sign-On Error]

**NEW QUESTION 195**
Universal Containers (UC) is building an integration between Salesforce and a legacy web application using the canvas framework. The security for UC has determined that a signed request from Salesforce is not an adequate authentication solution for the Third-Party app. Which two options should the Architect consider for authenticating the third-party app using the canvas framework? Choose 2 Answers

A. Utilize the SAML Single Sign-on flow to allow the third-party to authenticate itself against UC's IdP.
B. Utilize Authorization Providers to allow the third-party application to authenticate itself against Salesforce as the Idp.
C. Utilize Canvas OAuth flow to allow the third-party application to authenticate itself against Salesforce as the Idp.
D. Create a registration handler Apex class to allow the third-party application to authenticate itself against Salesforce as the Idp.

**Answer:** AC

**Explanation:**
The Canvas framework supports OAuth 2.0 for authorization1. There are two OAuth flows that can be used to authenticate the third-party app using the canvas framework: User-Agent OAuth Flow and Web Server OAuth Flow2. The User-Agent OAuth Flow uses the Canvas JavaScript SDK to obtain an OAuth token by using the login function in the SDK2. The Web Server OAuth Flow redirects the user to the Salesforce OAuth authorization endpoint and then obtains an OAuth access token by making a POST request to the Salesforce OAuth token endpoint2. Both of these flows allow the third-party app to authenticate itself against Salesforce as the IdP. The SAML Single Sign-on flow can also be used to allow the third-party app to authenticate itself against UC's IdP, which is another option for authentication3.
References: OAuth Authorization, Mastering Salesforce Canvas Apps, Integrate third-party applications vi Canvas App

**NEW QUESTION 200**
Universal Containers is budding a web application that will connect with the Salesforce API using JWT OAuth Flow.
Which two settings need to be configured in the connect app to support this requirement? Choose 2 answers

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:** AC

**Explanation:**
JWT OAuth Flow is a protocol that allows a client app to obtain an access token from Salesforce by using a JSON Web Token (JWT) instead of an authorization code. The JWT contains information about the client app and the user who wants to access Salesforce. To use this flow, the client app needs to have a connected app configured in Salesforce. The connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols. To support JWT OAuth Flow, two settings need to be configured in the connected app:

➤ The Use Digital Signature option, which enables the connected app to verify the signature of the JWT using a certificate.

➤ The "api" OAuth scope, which allows the connected app to access Salesforce APIs on behalf of the user.
References: JWT OAuth Flow, Connected Apps, OAuth Scopes

**NEW QUESTION 202**
......

# Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

**100% Pass Your Identity-and-Access-Management-Architect Exam with Our Prep Materials Via below:**

https://www.certleader.com/Identity-and-Access-Management-Architect-dumps.html