



## **Salesforce**

### **Exam Questions Identity-and-Access-Management-Architect**

Salesforce Certified Identity and Access Management Architect (SU23)

### NEW QUESTION 1

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

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

**Answer:** BD

#### Explanation:

To use SAML SSO for accessing the Salesforce1 mobile app, the architect should recommend configuring the embedded web browser to use the My Domain URL and configuring the Salesforce1 app to use the My Domain URL4. Using the My Domain URL allows Salesforce to identify the identity provider and initiate the SSO process5. Using the existing SAML SSO flow along with user agent flow or web server flow is not necessary because Salesforce Mobile Applications only work with service provider initiated setups46. Therefore, option B and D are the correct answers.

References: Salesforce Mobile Application Single Sign-On overview, SAML SSO with Salesforce as the Service Provider, Single Sign-On

### NEW QUESTION 2

In a typical SSL setup involving a trusted party and trusting party, what consideration should an Architect take into account when using digital certificates?

- A. Use of self-signed certificate leads to lower maintenance for trusted party because multiple self-signed certs need to be maintained.
- B. Use of self-signed certificate leads to higher maintenance for trusted party because they have to act as the trusted CA
- C. Use of self-signed certificate leads to lower maintenance for trusting party because there is no trusted CA cert to maintain.
- D. Use of self-signed certificate leads to higher maintenance for trusting party because the cert needs to be added to their truststore.

**Answer:** D

#### Explanation:

D is correct because using a self-signed certificate leads to higher maintenance for the trusting party, which is the client or browser that connects to the server. The trusting party needs to add the self-signed certificate to their truststore, which is a repository of trusted certificates, in order to establish a secure connection with the server. Otherwise, the trusting party will see a warning message or an error when accessing the server.

A is incorrect because using a self-signed certificate leads to higher maintenance for the trusted party, not lower. The trusted party needs to maintain multiple self-signed certificates from different servers in their truststore.

B is incorrect because using a self-signed certificate does not make the trusted party act as the trusted CA (Certificate Authority). The trusted CA is the entity that issues and validates certificates for servers. The trusted party only needs to trust the CA's root certificate, which is usually pre-installed in their truststore.

C is incorrect because using a self-signed certificate leads to higher maintenance for the trusting party, not lower. The trusting party still needs to maintain a trusted CA cert in their truststore, which is the self-signed certificate itself.

References: 1: SSL Certificate Installation Instructions & Tutorials - DigiCert 2: How To Install an SSL Certificate from a Commercial ... - DigitalOcean 3: Setup SSL CSR Creation and SSL Certificate Installatio  
- DigiCert

### NEW QUESTION 3

Universal containers want to build a custom mobile app connecting to salesforce using Oauth, and would like to restrict the types of resources mobile users can access. What Oauth feature of Salesforce should be used to achieve the goal?

- A. Access Tokens
- B. Mobile pins
- C. Refresh Tokens
- D. Scopes

**Answer:** D

#### Explanation:

The OAuth feature of Salesforce that should be used to restrict the types of resources mobile users can access is scopes. Scopes are parameters that specify the level of access that the mobile app requests from Salesforce when it obtains an OAuth token. Scopes can be used to limit the access to certain resources or actions, such as API calls, full access, web access, or refresh token. By configuring scopes in the connected app settings, Universal Containers can control what the mobile app can do with the OAuth token and protect against unauthorized or excessive access.

References: [OAuth Scopes], [Connected Apps], [OAuth Authorization Flows]

### NEW QUESTION 4

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 5

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 6

Northern Trail Outfitters (NTO) uses Salesforce for Sales Opportunity Management. Okta was recently brought in to Just-in-Time (JIT) provision and authenticate NTO users to applications. Salesforce users also use Okta to authorize a Forecasting web application to access Salesforce records on their behalf.

Which two roles are being performed by Salesforce? Choose 2 answers

- A. SAML Identity Provider
- B. OAuth Client
- C. OAuth Resource Server
- D. SAML Service Provider

**Answer:** BD

#### Explanation:

Salesforce acts as an OAuth client when it uses Okta to authorize a Forecasting web application to access

Salesforce records on behalf of the user. Salesforce acts as a SAML service provider when it accepts SAML assertions from Okta to authenticate NTO users.

References: OAuth 2.0 Web Server Authentication Flow, SAML Single Sign-On Overview

#### NEW QUESTION 7

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 8

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

- A. Web server Oauth SSO flow.
- B. Identity-provider-initiated SSO
- C. Service-provider-initiated SSO
- D. Start URL on identity provider

**Answer:** C

**Explanation:**

Service-provider-initiated SSO is required to support deep linking, which is the ability to direct users to a specific page within Salesforce from a different app. With service-provider-initiated SSO, the user requests a resource from Salesforce (the service provider), which then redirects the user to the identity provider for authentication. After the user is authenticated, the identity provider sends a SAML response back to Salesforce, which then grants access to the requested resource. Web server OAuth SSO flow is used for OAuth 2.1 authentication, not SAML. Identity-provider-initiated SSO is when the user logs in to the identity provider first and then selects a service provider to access. Start URL on identity provider is not a type of authentication flow, but a parameter that can be used to specify the landing page after SSO. References: Certification - Identity and Access Management Architect - Trailhead, Deep Linking, Single Sign On Deep Linking - Salesforce Developer Community

**NEW QUESTION 9**

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 10**

Universal containers (UC) has implemented SAML SSO to enable seamless access across multiple applications. UC has regional salesforce orgs and wants it's users to be able to access them from their main Salesforce org seamless. Which action should an architect recommend?

- A. Configure the main salesforce org as an authentication provider.
- B. Configure the main salesforce org as the Identity provider.
- C. Configure the regional salesforce orgs as Identity Providers.
- D. Configure the main Salesforce org as a service provider.

**Answer:** B

**Explanation:**

The action that an architect should recommend to UC is to configure the main Salesforce org as the identity provider. An identity provider is an application that authenticates users and provides information about them to service providers. A service provider is an application that provides a service to users and relies on an identity provider for authentication. SAML (Security Assertion Markup Language) is an XML-based standard that allows identity providers and service providers to exchange authentication and authorization data. SSO (Single Sign-On) is a feature that allows users to access multiple applications with one login. In this scenario, the main Salesforce org is the identity provider that authenticates users using SAML and provides information about them to the regional Salesforce orgs. The regional Salesforce orgs are the service providers that provide services to users and rely on the main Salesforce org for authentication. This way, users can access the regional Salesforce orgs from the main Salesforce org seamlessly using SSO.

References: [Identity Provider Overview], [SAML Single Sign-On Overview], [Single Sign-On Overview], [Salesforce as an Identity Provider]

**NEW QUESTION 10**

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

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

**Answer:** B

**Explanation:**

When integrating a SP that supports both SAML and OIDC with Salesforce, the use case that is the determining factor when choosing OIDC or SAML is whether the SP needs to perform API calls back to Salesforce on behalf of the user after the user logs in to the service provider. OIDC is a protocol that allows users to authorize an external application to access Salesforce resources on their behalf. OIDC provides an access token that can be used to call Salesforce APIs. SAML is a protocol that allows users to authenticate and authorize with an external identity provider and access Salesforce resources. SAML does not provide an access token, but only a session ID that can be used for web-based access. Therefore, if the SP needs to perform API calls back to Salesforce, OIDC is the preferred choice over SAML. References: OpenID Connect, SAML, Authorize Apps with OAuth

**NEW QUESTION 12**

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 controller
- 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 17**

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

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

**Answer:** D

**Explanation:**

Setting the Identity Provider as default and enabling the Redirect to the Identity Provider setting on the SAML Configuration will automatically redirect users to the login page of the external Identity Provider when using an SP-Initiated SAML flow with Salesforce as a Service Provider<sup>1</sup>. Option A is incorrect because Visualforce is not a supported method for redirecting users to the Identity Provider login page<sup>2</sup>. Option B is incorrect because enabling the Redirect to the Identity Provider setting under Authentication Services on the My Domain Configuration will only redirect users to the Identity Provider login page when using an IdP-Initiated SAML flow<sup>3</sup>. Option C is incorrect because removing the Login page from the list of Authentication Services on the My Domain configuration will not affect the SP-Initiated SAML flow, and may cause other issues with authentication<sup>4</sup>.

References: SAML SSO Flows, Set up a Service Provider initiated login flow, Configure SAML single sign-on with an identity provider, SAML Identity Provider Configuration Settings

**NEW QUESTION 19**

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

Which two actions should an identity architect recommend to meet these requirements? Choose 2 answers

- A. Create a custom external authentication provider for Facebook.
- B. Configure a predefined authentication provider for Facebook.
- C. Create a custom external authentication provider for Twitter.
- D. Configure a predefined authentication provider for Twitter.

**Answer:** BD

**Explanation:**

To give customers the ability to login with their Facebook and Twitter credentials, the identity architect should configure a predefined authentication provider for Facebook and a predefined authentication provider for Twitter. 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 Twitter, which can be easily configured with minimal customization. Creating a custom external authentication provider is not necessary for this scenario. References: Authentication Providers, Social Sign-On with Authentication Providers

**NEW QUESTION 23**

Universal containers (UC) has an e-commerce website while 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 for their accounts without logging in again. UC decides to implement ansp-Initiated SSO using a SAML-BASED complaint 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. Configure Delegated Authentication
- C. Create a connected App
- D. Set up my domain

**Answer:** AD

**Explanation:**

To enable SP-initiated SSO using a SAML-based identity provider, UC needs to configure SAML SSO settings in Salesforce and set up a custom domain using My Domain feature. This allows UC to specify the identity provider information, such as the issuer, entity ID, certificate, and SAML assertion attributes. Delegated authentication is a different mechanism that allows Salesforce to delegate the authentication process to an external web service. A connected app is not required for SP-initiated SSO, but it is used for IDP-initiated SSO or OAuth flows. References: Certification - Identity and Access Management Architect - Trailhead, [Set Up My Domain], [Configure SAML Settings for Single Sign-On]

**NEW QUESTION 27**

Northern Trail Outfitters would like to use a portal built on Salesforce Experience Cloud for customer self-service. Guests of the portal be able to self-register, but be unable to automatically be assigned to a contact record until verified. External Identity licenses have been purchased for the project.

After registered guests complete an onboarding process, a flow will create the appropriate account and contact records for the user.

Which three steps should an identity architect follow to implement the outlined requirements? Choose 3 answers

- A. Enable "Allow customers and partners to self-register".

- B. Select the "Configurable Self-Reg Page" option under Login & Registration.
- C. Set up an external login page and call Salesforce APIs for user creation.
- D. Customize the self-registration Apex handler to temporarily associate the user to a shared single contact record.
- E. Customize the self-registration Apex handler to create only the user record.

**Answer:** ABE

**Explanation:**

Enabling "Allow customers and partners to self-register" allows guests to create their own user accounts in the portal. Selecting the "Configurable Self-Reg Page" option allows the administrator to customize the self-registration page to capture the required fields. Customizing the self-registration Apex handler to create only the user record prevents the automatic creation of a contact record until verification. References: Enable Self-Registration, Customize Self-Registration

**NEW QUESTION 30**

Universal Containers (UC) has built a custom 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 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 login<sup>1</sup>. You can use Apex code to call your custom 2fa system and verify the user's identity<sup>2</sup>. This option also gives you more flexibility and control over the 2fa process than using native 2fa or an App Exchange app<sup>3</sup>. References: 1: Customize User Authentication with Login Flows 2: Custom Login Flow Examples 3: Salesforce Multi-Factor Authentication

**NEW QUESTION 34**

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 38**

An architect needs to set up a Facebook Authentication provider as login option for a Salesforce customer Community. What portion of the authentication provider setup associates a Facebook user with a Salesforce user?

- A. Consumer key and consumer secret
- B. Federation ID
- C. User info endpoint URL
- D. Apex registration handler

**Answer:** D

**Explanation:**

D is correct because the Apex registration handler is the portion of the authentication provider setup that associates a Facebook user with a Salesforce user when customers use their Facebook credentials to log in to the customer community. The Apex registration handler is an Apex class that handles the logic for creating or updating a user record based on the information received from Facebook. A is incorrect because the consumer key and consumer secret are portions of the authentication provider setup that identify and authenticate UC's customer community with Facebook, not associate a Facebook user with a Salesforce user. B is incorrect because the Federation ID is an attribute that can be used to identify a user in a SAML assertion when UC uses SAML-based SSO with Facebook, not when UC uses social sign-on with Facebook. C is incorrect because the user info endpoint URL is a portion of the authentication provider setup that specifies the URL to obtain the user information from Facebook, not associate a Facebook user with a Salesforce user. Verified References: [Apex Registration Handler], [Consumer Key and Secret], [Federation ID], [User Info Endpoint URL]

**NEW QUESTION 40**

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 44

Northern Trail Outfitters (NTO) uses the Customer 360 Platform implemented on Salesforce Experience Cloud. The development team in charge has learned of a contactless user feature, which can reduce the overhead of managing customers and partners by creating users without contact information. What is the potential impact to the architecture if NTO decides to implement this feature?

- A. Custom registration handler is needed to correctly assign External Identity or Community license for the newly registered contactless user.
- B. If contactless user is upgraded to Community license, the contact record is automatically created and linked to the user record, but not associated with an Account.
- C. Contactless user feature is available only with the External Identity license, which can restrict the Experience Cloud functionality available to the user.
- D. Passwordless authentication cannot be supported because the mobile phone receiving one-time password (OTP) needs to match the number on the contact record.

**Answer:** B

#### Explanation:

According to the Salesforce documentation<sup>3</sup>, contactless user feature allows creating users without contact information, such as email address or phone number. This reduces the overhead of managing customers and partners who don't need or want to provide their contact information. However, if a contactless user is upgraded to a Community license, a contact record is automatically created and linked to the user record, but not associated with an account. This can impact the architecture of NTO's Customer 360 Platform, as they may need to associate contacts with accounts for reporting or other purposes.

#### NEW QUESTION 48

An Identity and Access Management (IAM) architect is tasked with unifying multiple B2C Commerce sites and an Experience Cloud community with a single identity. The solution needs to support more than 1,000 logins per minute. What should the IAM do to fulfill this requirement?

- A. Configure both the community and the commerce sites as OAuth2 RPs (relying party) with an external identity provider.
- B. Configure community as a Security Assertion Markup Language (SAML) identity provider and enable Just-in-Time Provisioning to B2C Commerce.
- C. Create a default account for capturing all ecommerce contacts registered on the community because person Account is not supported for this case.
- D. Confirm performance considerations with Salesforce Customer Support due to high peaks.

**Answer:** A

#### Explanation:

According to the Salesforce documentation<sup>2</sup>, OAuth2 RPs (relying parties) are applications that use OAuth 2.0 for authentication and authorization with an external identity provider. This allows users to log in to multiple applications with a single identity provider account. The identity provider issues an access token to the relying party, which can be used to access protected resources on behalf of the user. This solution can support high volumes of logins per minute and unify multiple B2C Commerce sites and an Experience Cloud community with a single identity.

#### NEW QUESTION 53

A manufacturer wants to provide registration for an Internet of Things (IoT) device with limited display input or capabilities. Which Salesforce OAuth authorization flow should be used?

- A. OAuth 2.0 JWT Bearer Flow
- B. OAuth 2.0 Device Flow
- C. OAuth 2.0 User-Agent Flow
- D. OAuth 2.0 Asset Token Flow

**Answer:** B

#### Explanation:

The OAuth 2.0 Device Flow is a type of authorization flow that allows users to register an IoT device with limited display input or capabilities, such as a smart TV, a printer, or a smart speaker<sup>1</sup>. The device flow works as follows<sup>1</sup>:

- The device displays or reads out a verification code and a verification URL to the user.
- The user visits the verification URL on another device, such as a smartphone or a laptop, and enters the verification code.
- The user logs in to Salesforce and approves the device.
- The device polls Salesforce for an access token using the verification code.
- Salesforce returns an access token to the device, which can then access Salesforce APIs.

References:

- OAuth 2.0 Device Flow

#### NEW QUESTION 56

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 58

A public sector agency is setting up an identity solution for its citizens using a Community built on Experience Cloud and requires the new user registration functionality to capture first name, last name, and phone number. The phone number will be used for identity verification. Which feature should an identity architect recommend to meet the requirements?

- A. Integrate with social websites (Facebook, LinkedIn)
- B. Twitter
- C. Use an external Identity Provider
- D. Create a custom Lightning Web Component
- E. Use Login Discovery

**Answer:** D

#### Explanation:

Login Discovery allows the administrator to configure a custom login page that collects additional information from users, such as phone number, and use it for identity verification. Login Discovery can also be used to route users to different identity providers based on their input. References: Login Discovery, Customize Your Experience Cloud Site Login Process

#### NEW QUESTION 59

A technology enterprise is setting up an identity solution with an external vendors wellness application for its employees. The user attributes need to be returned to the wellness application in an ID token. Which authentication mechanism should an identity architect recommend to meet the requirements?

- A. OpenID Connect
- B. User Agent Flow
- C. JWT Bearer Token Flow
- D. Web Server Flow

**Answer:** A

#### Explanation:

OpenID Connect is an authentication protocol that allows a service provider to obtain user attributes in an ID token from an IdP. The other flows are OAuth 2.0 flows that are used for authorization, not authentication. References: Configure an Authentication Provider Using OpenID Connect, Integrate Service Providers as Connected Apps with OpenID Connect

#### NEW QUESTION 61

Universal Containers (UC) is rolling out its new Customer Identity and Access Management Solution built on top of its existing Salesforce instance. UC wants to allow customers to login using Facebook, Google, and other social sign-on providers. How should this functionality be enabled for UC, assuming all social sign-on providers support OpenID Connect?

- A. Configure an authentication provider and a registration handler for each social sign-on provider.
- B. Configure a single sign-on setting and a registration handler for each social sign-on provider.
- C. Configure an authentication provider and a Just-In-Time (JIT) handler for each social sign-on provider.
- D. Configure a single sign-on setting and a JIT handler for each social sign-on provider.

**Answer:** A

#### Explanation:

To allow customers to login using Facebook, Google, and other social sign-on providers, the identity architect should configure an authentication provider and a registration handler for each social sign-on provider. Authentication providers are configurations that enable users to authenticate with an external identity provider and access Salesforce resources. OpenID Connect is a protocol that allows users to sign in with an external identity provider, such as Facebook or Google, 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. A registration handler is a class that implements the Auth.RegistrationHandler interface and defines how to create or update users in Salesforce based on the information from the external identity provider. The registration handler can also be used to link the user's social identity with their Salesforce identity and prevent duplicate accounts. References: OpenID Connect Authentication Providers, Social Sign-On with OpenID Connect, Create a Custom Registration Handler

#### NEW QUESTION 64

Universal Containers (UC) is building a custom Innovation platform on their Salesforce instance. The Innovation platform will be written completely in Apex and Visualforce and will use custom objects to store the Data. UC would like all users to be able to access the system without having to log in with Salesforce credentials. UC will utilize a third-party idp using SAML SSO. What is the optimal Salesforce licence type for all of the UC employees?

- A. Identity Licence.
- B. Salesforce Licence.
- C. External Identity Licence.
- D. Salesforce Platform Licence.

**Answer:** D

#### Explanation:

The optimal Salesforce license type for all of the UC employees who will access the custom Innovation platform without logging in with Salesforce credentials is the Salesforce Platform license. The Salesforce Platform license allows users to access custom applications built on the Lightning Platform, such as Apex and Visualforce, and use standard objects such as accounts, contacts, reports, dashboards, and custom tabs. It also supports SSO with a third-party identity provider using SAML. Option A is not a good choice because the Identity license is designed for users who need to access Salesforce Identity features, such as identity provider, social sign-on, and user provisioning, but not for users who need to access custom applications. Option B is not a good choice because the Salesforce



license is designed for users who need full access to standard CRM and Lightning Platform features, such as leads, opportunities, campaigns, forecasts, and contracts, but it may be unnecessary or expensive for users who only need to access custom applications. Option C is not a good choice because the External Identity license is designed for users who are external to the organization, such as customers or partners, but not for users who are internal employees. References: Salesforce Help: User License Types, [Salesforce Help: Single Sign-On for Desktop and Mobile Applications using SAML and OAuth]

#### NEW QUESTION 65

Which two statements are capable of Identity Connect? Choose 2 answers

- A. Synchronization of Salesforce Permission Set Licence Assignments.
- B. Supports both Identity-Provider-Initiated and Service-Provider-Initiated SSO.
- C. Support multiple orgs connecting to multiple Active Directory servers.
- D. Automated user synchronization and de-activation.

**Answer: BD**

#### Explanation:

The two statements that are capabilities of Identity Connect are:

- It supports both identity-provider-initiated and service-provider-initiated SSO. Identity Connect is a desktop application that integrates Salesforce with Microsoft Active Directory (AD) and enables single sign-on (SSO) between the two systems. Identity Connect supports both identity-provider-initiated SSO, which is when the user starts at the AD site and then is redirected to Salesforce with a SAML assertion, and service-provider-initiated SSO, which is when the user starts at the Salesforce site and then is redirected to AD for authentication.
  - It enables automated user synchronization and deactivation. Identity Connect allows administrators to synchronize user accounts and attributes between AD and Salesforce, either manually or on a scheduled basis. Identity Connect also allows administrators to deactivate user accounts in Salesforce when they are disabled or deleted in AD, which helps maintain security and compliance.
- The other options are not capabilities of Identity Connect. Identity Connect does not support synchronization of Salesforce permission set license assignments, as these are not related to AD attributes. Identity Connect does not support multiple orgs connecting to multiple AD servers, as it can only connect one Salesforce org to one AD domain at a time. References: [Identity Connect], [Identity Connect Features], [Identity Connect User Synchronization], [Identity Connect Single Sign-On]

#### NEW QUESTION 70

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. Identity Provider Login URL.
- B. Issuer.
- C. Entity Id
- D. SAML Identity Location.

**Answer: C**

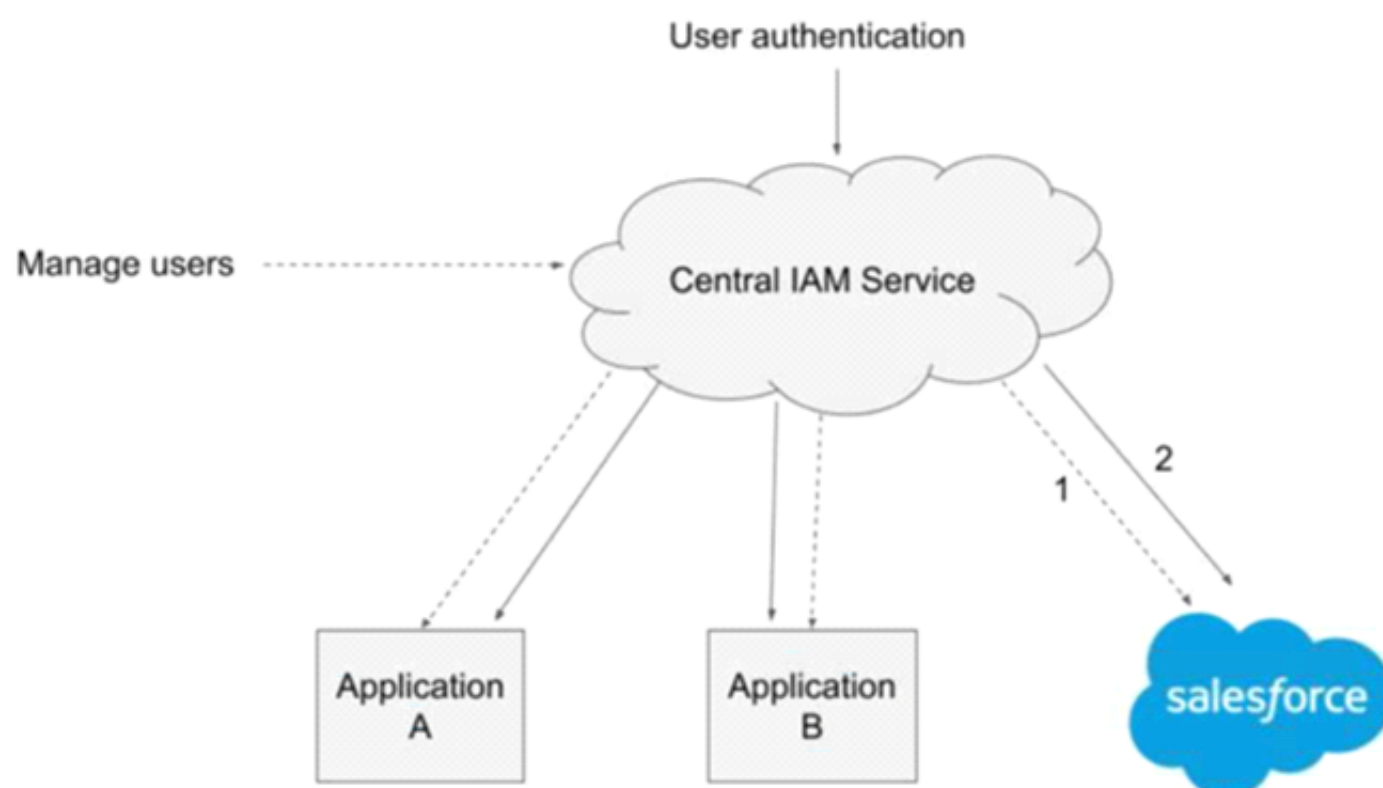
#### Explanation:

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 to the identity provider as part of the SSO request<sup>4</sup>. The identity provider uses the Entity Id to determine which service provider configuration to use and which SAML assertion to send back<sup>5</sup>. The other options are not valid SAML SSO settings for this purpose. The Identity Provider Login URL is the URL of the identity provider's SSO service that Salesforce redirects the user to for authentication<sup>4</sup>. The Issuer is the unique identifier for the identity provider that is sent by the identity provider as part of the SAML response<sup>4</sup>. The SAML Identity Location is the location of the user's identity in the SAML assertion, either in the Subject element or in an Attribute element<sup>4</sup>.

References: Configure SSO with Salesforce as a SAML Service Provider, Set Up Single Sign-On for Your Internal Users

#### NEW QUESTION 75

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 80**

Universal containers (UC) wants to integrate a Web application with salesforce. The UC team has implemented the Oauth web-server Authentication flow for authentication process. Which two considerations should an architect point out to UC? Choose 2 answers

- A. The web application should be hosted on a secure server.
- B. The web server must be able to protect consumer privacy
- C. The flow involves passing the user credentials back and forth.
- D. The flow will not provide an Oauth refresh token back to the server.

**Answer:** AB

**Explanation:**

The web application should be hosted on a secure server and the web server must be able to protect consumer privacy are two considerations that an architect should point out to UC. To integrate an external web app with the Salesforce API, UC can use the OAuth 2.0 web server flow, which implements the OAuth 2.0 authorization code grant type<sup>4</sup>. With this flow, the server hosting the web app must be able to protect the connected app's identity, defined by the client ID and client secret<sup>4</sup>. The web application should be hosted on a secure server to ensure that the communication between the web app and Salesforce is encrypted and protected from unauthorized access or tampering<sup>6</sup>. The web server must be able to protect consumer privacy to comply with data protection laws and regulations, such as GDPR or CCPA . The web server should implement best practices for storing and handling user data, such as encryption, hashing, salting, and anonymization. The flow involves passing the user credentials back and forth is not a correct consideration, as the web server flow does not require the user credentials to be passed between the web app and Salesforce. Instead, it uses an authorization code that is exchanged for an access token and a refresh token<sup>4</sup>. The flow will not provide an OAuth refresh token back to the server is also not a correct consideration as the web server flow does provide a refresh token that can be used to obtain new access tokens without user interaction<sup>4</sup>. References: OAuth 2.0 Web Server Flow for Web App Integration, Secure Your Web Application, [General Data Protection Regulation (GDPR)], [California Consumer Privacy Act (CCPA)], [Data Protection Best Practices]

**NEW QUESTION 82**

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 <sup>65</sup>\* 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 will be automatically created or updated in the other orgs based on the information from UC1<sup>1</sup>. 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 86**

A global fitness equipment manufacturer is planning to sell fitness tracking devices and has the following requirements:

- 1) Customer purchases the device.
  - 2) Customer registers the device using their mobile app.
  - 3) A case should automatically be created in Salesforce and associated with the customer's account in cases where the device registers issues with tracking.
- Which OAuth flow should be used to meet these requirements?

- A. OAuth 2.0 Asset Token Flow
- B. OAuth 2.0 Username-Password Flow
- C. OAuth 2.0 User-Agent Flow
- D. OAuth 2.0 SAML Bearer Assertion Flow

**Answer:** A

**Explanation:**

OAuth 2.0 Asset Token Flow is the flow that allows customers to register their devices with Salesforce and get an access token that can be used to create cases. The other flows are not suitable for this use case.

References: OAuth Authorization Flows Trailblazer Community Documentation

**NEW QUESTION 91**

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 expires<sup>1</sup>. The refresh token expiration policy determines how long a refresh token is valid for<sup>2</sup>. 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"<sup>2</sup>.

References: OAuth 2.0 Refresh Token Flow, Manage OAuth Access Policies for a Connected App

**NEW QUESTION 93**

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

- A. OAuth 2.0 SAML Bearer Assertion Flow
- B. A SAML Assertion Row
- C. OAuth 2.0 User-Agent Flow
- D. OAuth 2.0 JWT Bearer Flow

**Answer:** A

**Explanation:**

OAuth 2.0 SAML Bearer Assertion Flow allows a client application to use a SAML assertion to request an access token from Salesforce. This flow can leverage the existing SAML configuration for single sign-on and secure the Salesforce APIs. References: OAuth 2.0 SAML Bearer Assertion Flow

**NEW QUESTION 97**

Universal containers (UC) has multiple salesforce orgs and would like to use a single identity provider to access all of their orgs. How should UC'S architect enable this behavior?

- A. Ensure that users have the same email value in their user records in all of UC's salesforce orgs.
- B. Ensure the same username is allowed in multiple orgs by contacting salesforce support.
- C. Ensure that users have the same Federation ID value in their user records in all of UC's salesforce orgs.
- D. Ensure that users have the same alias value in their user records in all of UC's salesforce orgs.

**Answer:** C

**Explanation:**

The best option for UC's architect to enable the behavior of using a single identity provider to access all of their Salesforce orgs is to ensure that users have the same Federation ID value in their user records in all of UC's Salesforce orgs. The Federation ID is a field on the user object that stores a unique identifier for each user that is consistent across multiple systems. The Federation ID is used by Salesforce to match the user with the SAML assertion that is sent by the identity provider during the single sign-on (SSO) process. By ensuring that users have the same Federation ID value in all of their Salesforce orgs, UC can enable users to log in with the same identity provider and credentials across multiple orgs. The other options are not valid ways to enable this behavior. Ensuring that users have the same email value in their user records in all of UC's Salesforce orgs does not guarantee that they can log in with SSO, as email is not used as a unique identifier by Salesforce. Ensuring the same username is allowed in multiple orgs by contacting Salesforce support is not possible, as username must be unique across all Salesforce orgs. Ensuring that users have the same alias value in their user records in all of UC's Salesforce orgs does not affect the SSO process, as alias is not used as a unique identifier by Salesforce. References: [Federation ID], [SAML SSO with Salesforce as the Service Provider], [Username], [Alias]

**NEW QUESTION 99**

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 the recommended best practices for using Oauth flows in this scenario? Choose 2 answers

- A. Oauth refresh token flow
- B. Oauth SAML bearer assertion flow
- C. Oauthjwt bearer token flow
- D. Oauth Username-password flow

**Answer:** AC

**Explanation:**

OAuth refresh token flow and OAuth JWT bearer token flow are the recommended best practices for using OAuth flows in this scenario. These flows are suitable for server-to-server integration scenarios where the client application needs to access Salesforce resources on behalf of a user. The OAuth refresh token flow allows the client application to obtain a long-lived refresh token that can be used to request new access tokens without requiring user interaction. The OAuth JWT



bearer token flow allows the client application to use a JSON Web Token (JWT) to assert its identity and request an access token. Both flows provide a secure and efficient way to integrate with Salesforce and the reward calculation system. OAuth SAML bearer assertion flow is not a recommended best practice for using OAuth flows in this scenario because it requires the client application to obtain a SAML assertion from an identity provider, which adds an extra layer of complexity and dependency. OAuth username-password flow is not a recommended best practice for using OAuth flows in this scenario because it requires the client application to store the user's credentials, which poses a security risk and does not support two-factor authentication. References: : [Which OAuth Flow to Use] : [Digging Deeper into OAuth 2.0 on Force.com] : [OAuth 2.0 JWT Bearer Token Flow] : [OAuth 2.0 SAML Bearer Assertion Flow] : [OAuth 2.0 Username-Password Flow]

#### NEW QUESTION 102

In an SP-Initiated SAML SSO setup where the user tries to access a resource on the Service Provider, What HTTP param should be used when submitting a SAML Request to the Idp to ensure the user is returned to the intended resource after authentication?

- A. RedirectURL
- B. RelayState
- C. DisplayState
- D. StartURL

**Answer:** B

#### Explanation:

The HTTP parameter that should be used when submitting a SAML request to the IdP to ensure the user is returned to the intended resource after authentication is RelayState. RelayState is an optional parameter that can be used to preserve some state information across the SSO process. For example, RelayState can be used to specify the URL of the resource that the user originally requested on the SP before being redirected to the IdP for authentication. After the IdP validates the user's identity and sends back a SAML response, it also sends back the RelayState parameter with the same value as it received from the SP. The SP then uses the RelayState value to redirect the user to the intended resource after validating the SAML response. The other options are not valid HTTP parameters for this purpose. RedirectURL, DisplayState, and StartURL are not standard SAML parameters and they are not supported by Salesforce as SP or IdP. References: [SAML SSO Flows], [RelayState Parameter]

#### NEW QUESTION 107

Containers (UC) uses a legacy Employee portal for their employees to collaborate. Employees access the portal from their company's internal website via SSO. It is set up to work with SiteMinder and Active Directory. The Employee portal has features to support posing ideas. UC decides to use Salesforce Ideas for voting and better tracking purposes. To avoid provisioning users on Salesforce, UC decides to integrate Employee portal ideas with Salesforce idea through the API. What is the role of Salesforce in the context of SSO, based on this scenario?

- A. Service Provider, because Salesforce is the application for managing ideas.
- B. Connected App, because Salesforce is connected with Employee portal via API.
- C. Identity Provider, because the API calls are authenticated by Salesforce.
- D. An independent system, because Salesforce is not part of the SSO setup.

**Answer:** D

#### Explanation:

D is correct because Salesforce is an independent system that is not part of the SSO setup between the Employee portal and Active Directory. Salesforce does not act as an IdP or an SP for the SSO, nor does it use a connected app to integrate with the Employee portal. Salesforce only exposes its API to allow the Employee portal to access its ideas feature.

A is incorrect because Salesforce is not a service provider for the SSO. The SSO is between the Employee portal and Active Directory, not between the Employee portal and Salesforce.

B is incorrect because Salesforce is not a connected app for the SSO. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect1. The Employee portal does not use any of these protocols to integrate with Salesforce, but only uses its API.

C is incorrect because Salesforce is not an identity provider for the SSO. The IdP is the system that authenticates users and issues tokens or assertions to allow access to other systems. In this scenario, the IdP is Active Directory, not Salesforce.

References: 1: Oauth Authorization flows in Salesforce - Apex Hours

#### NEW QUESTION 110

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-commerce 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 115



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

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

**Answer:** D

**Explanation:**

This is because without My Domain, Salesforce will not know in advance what Identity Provider (IdP) to use for SSO, since it does not even know yet what Organization the user is trying to log in to1. SP-initiated SSO is the scenario where the user starts with a Salesforce link (login page, deep link, Outlook Sync URL, etc.) and then gets redirected to the IdP for authentication2. Without My Domain, SP-initiated SSO requires that the user do an IdP-initiated SSO at least once first so that Salesforce can set a cookie in their browser identifying the IdP1. The other options are not correct for this question because:

- IdP-initiated SSO will work without My Domain, as long as the user starts SSO at the IdP and sends the identity information to Salesforce along with SAML protocol information that identifies the Organization and the IdP2.
- Neither SP- nor IdP-initiated SSO will not work is false, as explained above.
- Either SP- or IdP-initiated SSO will work is false, as explained above.

References: Considerations for setting up My Domain and SSO - Salesforce, SAML SSO with Salesforce as the Service Provider

**NEW QUESTION 120**

Universal Containers (UC) has a mobile application for its employees that uses data from Salesforce as well as uses Salesforce for Authentication purposes. UC wants its mobile users to only enter their credentials the first time they run the app. The application has been live for a little over 6 months, and all of the users who were part of the initial launch are complaining that they have to re-authenticate. UC has also recently changed the URI Scheme associated with the mobile app. What should the Architect at UC first investigate?Universal Containers (UC) has a mobile application for its employees that uses data from Salesforce as well as uses Salesforce for Authentication purposes. UC wants its mobile users to only enter their credentials the first time they run the app. The application has been live for a little over 6 months, and all of the users who were part of the initial launch are complaining that they have to re-authenticate. UC has also recently changed the URI Scheme associated with the mobile app. What should the Architect at UC first investigate?

- A. Check the Refresh Token policy defined in the Salesforce Connected App.
- B. Validate that the users are checking the box to remember their passwords.
- C. Verify that the Callback URL is correctly pointing to the new URI Scheme.
- D. Confirm that the access Token's Time-To-Live policy has been set appropriately.

**Answer:** A

**Explanation:**

The first thing that the architect at UC should investigate is the refresh token policy defined in the Salesforce connected app. A refresh token is a credential that allows an application to obtain new access tokens without requiring the user to re-authenticate. The refresh token policy determines how long a refresh token is valid and under what conditions it can be revoked. If the refresh token policy is set to expire after a certain period of time or after a change in IP address or device ID, then the users may have to re-authenticate after using the app for a while or from a different location or device. Option B is not a good choice because validating that the users are checking the box to remember their passwords may not be relevant, as the app uses SSO with a third-party identity provider and does not rely on Salesforce credentials. Option C is not a good choice because verifying that the callback URL is correctly pointing to the new URI scheme may not be necessary, as the callback URL is used for redirecting the user back to the app after authentication, but it does not affect how long the user can stay authenticated. Option D is not a good choice because confirming that the access token's time-to-live policy has been set appropriately may not be effective, as the access token's time-to-live policy determines how long an access token is valid before it needs to be refreshed by a refresh token, but it does not affect how long a refresh token is valid or when it can be revoked. References: [Connected Apps Developer Guide], [Digging Deeper into OAuth 2.0 on Force.com]

**NEW QUESTION 121**

Universal Containers allows employees to use a mobile device to access Salesforce for daily operations using a hybrid mobile app. This app uses Mobile software development kits (SDK), leverages refresh token to regenerate access token when required and is distributed as a private app. The chief security officer is rolling out an org wide compliance policy to enforce re-verification of devices if an employee has not logged in from that device in the last week.

Which connected app setting should be leveraged to comply with this policy change?

- A. Scope - Deny refresh\_token scope for this connected app.
- B. Refresh Token Policy - Expire the refresh token if it has not been used for 7 days.
- C. Session Policy - Set timeout value of the connected app to 7 days.
- D. Permitted User - Ask admins to maintain a list of users who are permitted based on last login date.

**Answer:** B

**Explanation:**

Refresh Token Policy - Expire the refresh token if it has not been used for 7 days is the connected app setting that should be leveraged to comply with the policy change. This setting ensures that users have to re-verify their devices if they have not logged in from that device in the last week. The other settings are either not relevant or not effective for this scenario. References: Connected App Basics, OAuth 2.0 Refresh Token Flow

**NEW QUESTION 125**

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 130**

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 135**

Universal containers(UC) has decided to build a new, highly sensitive application on Force.com platform. The security team at UC has decided that they want users to provide a fingerprint in addition to username/Password to authenticate to this application. How can an architect support fingerprint as a form of identification for salesforce Authentication?

- A. Use salesforce Two-factor Authentication with callouts to a third-party fingerprint scanning application.
- B. Use Delegated Authentication with callouts to a third-party fingerprint scanning application.
- C. Use an AppExchange product that does fingerprint scanning with native salesforce identity confirmation.
- D. Use custom login flows with callouts to a third-party fingerprint scanning application.

**Answer:** D

**Explanation:**

D is correct because using custom login flows with callouts to a third-party fingerprint scanning application allows UC to support fingerprints as a form of identification for Salesforce authentication. Custom login flows allow UC to implement custom logic and UI elements for authentication, such as calling an external web service that performs fingerprint scanning and verification. A is incorrect because using Salesforce two-factor authentication with callouts to a third-party fingerprint scanning application does not support fingerprints as a form of identification for Salesforce authentication. Salesforce two-factor authentication requires users to enter a verification code or use an app like Salesforce Authenticator, not a fingerprint. B is incorrect because using delegated authentication with callouts to a third-party fingerprint scanning application does not support fingerprints as a form of identification for Salesforce authentication. Delegated authentication requires users to enter their username and password, not a fingerprint. C is incorrect because using an AppExchange product that does fingerprint scanning with native Salesforce identity confirmation does not support fingerprints as a form of identification for Salesforce authentication. AppExchange products are third-party applications that integrate with Salesforce, not native Salesforce features. Verified References: [Custom Login Flows], [Two-Factor Authentication], [Delegated Authentication], [AppExchange]

**NEW QUESTION 140**

Universal containers (UC) would like to enable self - registration for their salesforce partner community users. UC wants to capture some custom data elements from the partner user, and based on these data elements, wants to assign the appropriate profile and account values. Which two actions should the architect recommend to UC? Choose 2 answers

- A. Modify the communitiesselfregcontroller to assign the profile and account.
- B. Modify the selfregistration trigger to assign profile and account.
- C. Configure registration for communities to use a custom visualforce page.
- D. Configure registration for communities to use a custom apex controller.

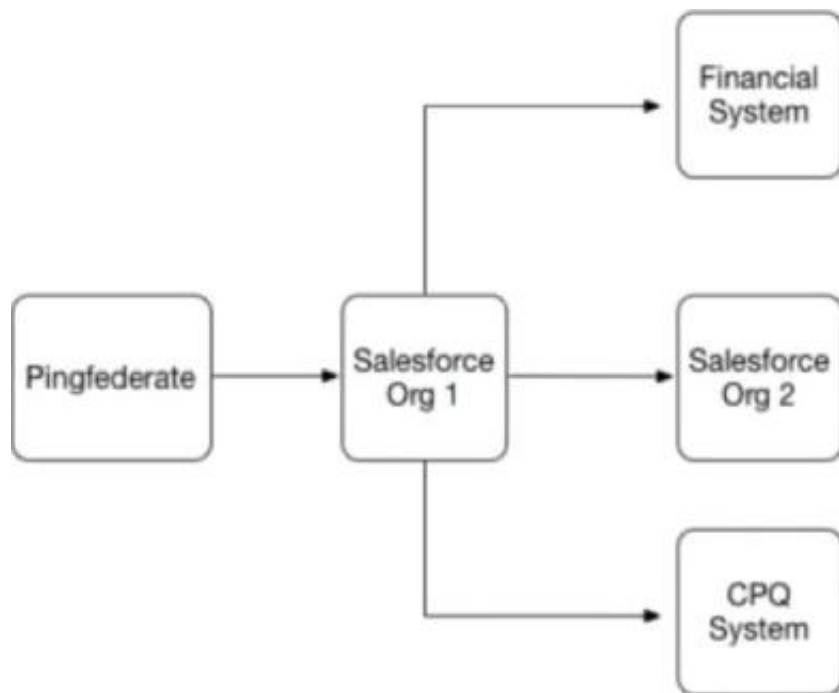
**Answer:** AC

**Explanation:**

To enable self-registration for their Salesforce partner community users, UC should modify the communities' self-registration controller to assign the profile and account based on the custom data elements from the partner user1. UC should also configure registration for communities to use a custom Visualforce page to capture the custom data elements from the partner user2. Therefore, option A and C are the correct answers. References: Salesforce Partner Community, Partner Community Registration Guide

**NEW QUESTION 142**

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 resource<sup>1</sup>. 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 System<sup>2</sup>. Therefore, the correct answer is B.

References:

- SAML web-based authentication guide
- SAML-based single sign-on: Configuration and Limitations

**NEW QUESTION 146**

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 147**

An identity architect is implementing a mobile-first Consumer Identity Access Management (CIAM) for external users. User authentication is the only requirement. The users email or mobile phone number should be supported as a username. Which two licenses are needed to meet this requirement? Choose 2 answers

- A. External Identity Licenses
- B. Identity Connect Licenses
- C. Email Verification Credits
- D. SMS verification Credits

**Answer: AD**

**Explanation:**

External Identity Licenses are required to enable external users to access Salesforce resources via a CIAM solution. Email Verification Credits and SMS Verification Credits are required to enable email or mobile phone number verification for user authentication. Identity Connect Licenses are not required for this scenario, as Identity Connect is a tool for synchronizing user data between Salesforce and Active Directory.

References: External Identity Implementation Guide, Identity Connect Implementation Guide



### NEW QUESTION 151

A client is planning to rollout multi-factor authentication (MFA) to its internal employees and wants to understand which authentication and verification methods meet the Salesforce criteria for secure authentication.

Which three functions meet the Salesforce criteria for secure mfa? Choose 3 answers

- A. username and password + SMS passcode
- B. Username and password + security key
- C. Third-party single sign-on with Mobile Authenticator app
- D. Certificate-based Authentication
- E. Lightning Login

**Answer:** BCE

#### Explanation:

Multi-factor authentication (MFA) is a security feature that requires users to verify their identity with two or more factors when they log in to Salesforce<sup>4</sup>. Salesforce supports several types of authentication and verification methods that meet the criteria for secure MFA, such as<sup>5</sup>:

- Username and password + security key: A security key is a physical device that plugs into a USB port or connects wirelessly to your computer or mobile device. It generates a unique code that you use to verify your identity when you log in to Salesforce<sup>5</sup>.
- Third-party single sign-on with Mobile Authenticator app: Single sign-on (SSO) is an authentication method that allows users to access multiple applications with one login and one set of credentials. A mobile authenticator app is an app that generates temporary codes or sends push notifications that you use to verify your identity when you log in to Salesforce via SSO<sup>5</sup>.
- Lightning Login: Lightning Login is an authentication method that allows users to log in to Salesforce without entering a password. Instead, users scan a QR code with their mobile device or click an email link that they receive when they try to log in. Then they use their fingerprint, face ID, or PIN to verify their identity on their mobile device<sup>5</sup>.

References:

- Multi-Factor Authentication
- Authentication and Verification Methods

### NEW QUESTION 156

Universal Containers wants to implement Single Sign-on for a Salesforce org using an external Identity Provider and corporate identity store. What type of authentication flow is required to support deep linking?

- A. Web Server OAuth SSO flow
- B. Service-Provider-Initiated SSO
- C. Identity-Provider-initiated SSO
- D. StartURL on Identity Provider

**Answer:** B

#### Explanation:

Single sign-on (SSO) is an authentication method that enables users to access multiple applications with one login and one set of credentials<sup>4</sup>. There are two types of SSO flows that can be used with Salesforce as the service provider (SP) and an external identity provider (IdP)<sup>5</sup>:

- Service-provider-initiated SSO: The user requests a resource from the SP, such as a Salesforce URL. The SP redirects the user to the IdP for authentication. The IdP authenticates the user and sends a SAML response to the SP. The SP validates the SAML response and grants access to the user<sup>5</sup>. This type of SSO flow supports deep linking, which means that the user can access a specific page within Salesforce without logging in again<sup>6</sup>.
- Identity-provider-initiated SSO: The user logs in to the IdP and selects an app from a list of available apps. The IdP sends a SAML response to the SP. The SP validates the SAML response and grants access to the user<sup>5</sup>. This type of SSO flow does not support deep linking, which means that the user can only access the default landing page of Salesforce<sup>6</sup>.

References:

- Single Sign-On
- SAML SSO Flows
- Deep Linking

### NEW QUESTION 160

Universal Containers (UC) has a Customer Community that uses Facebook for authentication. UC would like to ensure that changes in the Facebook profile are reflected on the appropriate Customer Community user. How can this requirement be met?

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

**Answer:** D

#### Explanation:

The update User() method on the Registration Handler class is used to update the Salesforce user record with information from the Facebook profile, such as name, email, and photo<sup>1</sup>. This method is invoked every time a user logs in to Salesforce using Facebook credentials<sup>2</sup>. The other options are not suitable for this requirement because:

- SAML Just-In-Time Provisioning is used to create or update users in Salesforce based on SAML assertions from an identity provider<sup>3</sup>. Facebook does not support SAML as an identity provider.
- The Signed Request is a parameter that contains information about the user who is logging in to Salesforce via Facebook. It does not contain the user's profile information, such as name, email, or photo.
- A scheduled job that calls out to Facebook on a nightly basis would not reflect the changes in the Facebook profile in real time, as the requirement states. It would also require storing the user's Facebook access token and making API calls to Facebook, which could be inefficient and insecure. References: Set Up Social Sign-On, Configure a Facebook Authentication Provider, SAML Just-in-Time Provisioning, [Facebook as a SAML Identity Provider], [Facebook Login for Apps - Signed Request], [Facebook Login for Apps - Access Tokens], [Facebook Graph API - User]



#### NEW QUESTION 165

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 companies' 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 querystring 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 166

Universal Containers (UC) uses Active Directory (AD) as their identity store for employees and must continue to do so for network access. UC is undergoing a major transformation program and moving all of their enterprise applications to cloud platforms including Salesforce, Workday, and SAP HANA. UC needs to implement an SSO solution for accessing all of the third-party cloud applications and the CIO is inclined to use Salesforce for all of their identity and access management needs.

Which two Salesforce license types does UC need for its employees' Choose 2 answers

- A. Company Community and Identity licenses
- B. Identity and Identity Connect licenses
- C. Chatter Only and Identity licenses
- D. Salesforce and Identity Connect licenses

**Answer:** BD

#### Explanation:

The two Salesforce license types that UC needs for its employees are Identity and Identity Connect licenses. According to the Salesforce documentation, "Identity licenses let your employees access any app that supports standards-based single sign-on (SSO). Identity Connect licenses let you integrate your Active Directory with Salesforce." Therefore, option B and D are the correct answers. References: [Identity Licenses]

#### NEW QUESTION 170

How should an identity architect automate provisioning and deprovisioning of users into Salesforce from an external system?

- A. Call SOAP API upsertQ on user object.
- B. Use Security Assertion Markup Language Just-in-Time (SAML JIT) on incoming SAML assertions.
- C. Run registration handler on incoming OAuth responses.
- D. Call OpenID Connect (OIDC)-userinfo endpoint with a valid access token.

**Answer:** C

#### Explanation:

To automate provisioning and deprovisioning of users into Salesforce from an external system, the identity architect should run a registration handler on incoming OAuth responses. A registration handler is a class that implements the Auth.RegistrationHandler interface and defines how to create or update users in Salesforce based on the information from an external identity provider. OAuth is a protocol that allows users to authorize an external application to access Salesforce resources on their behalf. By running a registration handler on incoming OAuth responses, the identity architect can automate user provisioning and deprovisioning based on the OAuth attributes. References: Registration Handler, Authorize Apps with OAuth

#### NEW QUESTION 173

A division of a Northern Trail Outfitters (NTO) purchased Salesforce. NTO uses a third party identity provider (IdP) to validate user credentials against its corporate Lightweight Directory Access Protocol (LDAP) directory. NTO wants to help employees remember as passwords as possible.

What should an identity architect recommend?

- A. Setup Salesforce as a Service Provider to the existing IdP.
- B. Setup Salesforce as an IdP to authenticate against the LDAP directory.
- C. Use Salesforce connect to synchronize LDAP passwords to Salesforce.
- D. Setup Salesforce as an Authentication Provider to the existing IdP.

**Answer:** A

#### Explanation:

To help employees remember fewer passwords, an identity architect should recommend setting up Salesforce as a service provider (SP) to the existing IdP. A SP is the system that relies on the IdP for authentication and provides access to its services based on the SAML assertions from the IdP. To set up Salesforce as a SP, you need to create a connected app for Salesforce in the IdP, enable SAML and configure the SAML settings, such as the entity ID, ACS URL, and subject type. You also need to enable SSO for your Salesforce org, upload the IdP certificate, and configure the SSO settings, such as the issuer, identity type, and service provider initiated request binding.

References:

➤ [SAML Single Sign-On]

- [Set Up Salesforce as a Service Provider]
- [Enable Single Sign-On for Your Org]

#### NEW QUESTION 175

Universal containers (UC) has decided to use identity connect as its 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 records<sup>1</sup>. 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 membership<sup>2</sup>. 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 180

Northern Trail Outfitters would like to automatically create new employee users in Salesforce with an appropriate profile that maps to its Active Directory Department.  
How should an identity architect implement this requirement?

- A. Use the createUser method in the Just-in-Time (JIT) provisioning registration handler to assign the appropriate profile.
- B. Use the updateUser method in the Just-in-Time (JIT) provisioning registration handler to assign the appropriate profile.
- C. Use a login flow to collect Security Assertion Markup Language attributes and assign the appropriate profile during Just-In-Time (JIT) provisioning.
- D. Make a callout during the login flow to query department from Active Directory to assign the appropriate profile.

**Answer:** B

#### Explanation:

To automatically create new employee users in Salesforce with an appropriate profile that maps to their Active Directory Department, the identity architect should use the updateUser method in the Just-in-Time (JIT) provisioning registration handler to assign the appropriate profile. 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, such as Active Directory. The updateUser method is a method in the Auth.RegistrationHandler interface that defines how to update an existing user in Salesforce based on the information from the external identity provider. The identity architect can use this method to assign the appropriate profile to the user based on their department attribute. References: Just-in-Time Provisioning for SAML and OpenID Connect, Create a Custom Registration Handler

#### NEW QUESTION 184

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 SessionManagement 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 186

Universal Containers is creating a mobile application that will be secured by Salesforce Identity using the OAuth 2.0 user-agent flow. Application users will authenticate using username and password. They should not be forced to approve API access in the mobile app or reauthenticate for 3 months.  
Which two connected app options need to be configured to fulfill this use case?  
Choose 2 answers

- A. Set Permitted Users to "Admin approved users are pre-authorized".
- B. Set Permitted Users to "All users may self-authorize".
- C. Set the Session Timeout value to 3 months.
- D. Set the Refresh Token Policy to expire refresh token after 3 months.

**Answer:** BD

#### Explanation:

To fulfill the use case of creating a mobile application that will be secured by Salesforce Identity using the OAuth 2.0 user-agent flow, where users will authenticate using username and password and not be forced to approve API access or reauthenticate for 3 months, the identity architect should configure two connected app options:

- Set Permitted Users to “All users may self-authorize”. Permitted Users is a setting that controls how users can access a connected app. By setting it to “All users may self-authorize”, the identity architect can allow users to access the connected app without requiring administrator approval or API access confirmation.
- Set the Refresh Token Policy to expire refresh token after 3 months. Refresh Token Policy is a setting that controls how long a refresh token can be used to obtain a new access token without requiring user authentication. By setting it to expire refresh token after 3 months, the identity architect can allow users to access the connected app for 3 months without reauthenticating, as long as they use the app at least once every 90 days. References: Connected Apps, OAuth 2.0 User-Agent Flow

#### NEW QUESTION 191

Universal Containers want users to be able to log in to the Salesforce mobile app with their Active Directory password. Employees are unable to use mobile VPN. Which two options should an identity architect recommend to meet the requirement? Choose 2 answers

- A. Active Directory Password Sync Plugin
- B. Configure Cloud Provider Load Balancer
- C. Salesforce Trigger & Field on Contact Object
- D. Salesforce Identity Connect

**Answer:** AD

#### Explanation:

Active Directory Password Sync Plugin allows users to log in to Salesforce with their Active Directory password without using a VPN. Salesforce Identity Connect synchronizes users and groups between Active Directory and Salesforce and enables single sign-on. References: Active Directory Password Sync Plugin, Salesforce Identity Connect

#### NEW QUESTION 192

An identity architect has been asked to recommend a solution that allows administrators to configure personalized alert messages to users before they land on the Experience Cloud site (formerly known as Community) homepage. What is recommended to fulfill this requirement with the least amount of customization?

- A. Customize the registration handler Apex class to create a routing logic navigating to different home pages based on the user profile.
- B. Use Login Flows to add a screen that shows personalized alerts.
- C. Build a Lightning web Component (LWC) for a homepage that shows custom alerts.
- D. Create custom metadata that stores user alerts and use a LWC to display alerts.

**Answer:** B

#### Explanation:

Login Flows are custom post-authentication processes that can be used to add additional screens or logic after a user logs in to Salesforce. Login Flows can be used to show personalized alert messages to users based on their profile or other criteria before they land on the Experience Cloud site homepage. Login Flows require minimal customization and can be configured using Visual Workflow or Apex. References: Login Flows, Customizing User Authentication with Login Flows

#### NEW QUESTION 196

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 197

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

- A. Use Salesforce reports to identify users that currently own open "Classified" cases and should be granted access to the Classified information system.
- B. Use Apex trigger on case to dynamically assign permission Sets that Grant access when a user is assigned with an open "Classified" case, and remove it when the case is closed.
- C. Use Custom SAML JIT Provisioning to dynamically query the user's open "Classified" cases when attempting to access the classified information system.
- D. Use a Common Connected App Handler using Apex to dynamically allow access to the system based on whether the staff owns any open "Classified" Cases.

**Answer:** C



**Explanation:**

Custom SAML JIT Provisioning allows Salesforce to dynamically create or update user records in the classified information system based on the SAML assertion sent by Salesforce as the IdP. This way, the staff can access the system only when they have an open “Classified” case, and their access is revoked when they don’t. Option A is incorrect because Salesforce reports are not a reliable way to grant or revoke access to the system, as they are not updated in real time and may not reflect the current status of the cases. Option B is incorrect because Apex triggers can only assign or remove permission sets within Salesforce, not in an external system. Option D is incorrect because a Common Connected App Handler using Apex is used to customize the behavior of a connected app, not to control access to an external system based on user attributes. References: Custom SAML JIT Provisioning, Create a Custom Connected App Handler

**NEW QUESTION 199**

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 203**

A real estate company wants to provide its customers a digital space to design their interior decoration options. To simplify the registration to gain access to the community site (built in Experience Cloud), the CTO has requested that the IT/Development team provide the option for customers to use their existing social-media credentials to register and access.

The IT lead has approached the Salesforce Identity and Access Management (IAM) architect for technical direction on implementing the social sign-on (for Facebook, Twitter, and a new provider that supports standard OpenID Connect (OIDC)).

Which two recommendations should the Salesforce IAM architect make to the IT Lead? Choose 2 answers

- A. Use declarative registration handler process builder/flow to create, update users and contacts.
- B. Authentication provider configuration is required each social sign-on providers; and enable Authentication providers in community.
- C. For supporting OIDC it is necessary to enable Security Assertion Markup Language (SAML) with Just-in-Time provisioning (JIT) and OAuth 2.0.
- D. Apex coding skills are needed for registration handler to create and update users.

**Answer:** BD

**Explanation:**

Authentication provider configuration and Apex coding skills are two recommendations that the Salesforce IAM architect should make to the IT Lead.

Authentication providers are used to configure social sign-on providers, such as Facebook, Twitter, and any OpenID Connect compliant provider. Apex coding skills are needed for registration handlers, which are custom classes that create and update users based on social sign-on data. References: Authentication Providers, Registration Handlers

**NEW QUESTION 207**

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

Which three OAuth concepts apply to this flow? Choose 3 answers

- A. Client ID
- B. Refresh Token
- C. Authorization Code
- D. Verification Code
- E. Scopes

**Answer:** AE

**Explanation:**

The OAuth 2.0 user-agent flow uses the OAuth 2.0 implicit grant type, which does not require an authorization code or a refresh token. The client ID and scopes are required to identify the connected app and request the appropriate permissions from the user. References: OAuth Authorization Flows, OAuth with Salesforce Demystified

**NEW QUESTION 209**

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 212

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 token<sup>2</sup>.

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 authentication<sup>3</sup>.

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 token<sup>4</sup>.

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 expires<sup>5</sup>.

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 214

An Enterprise is using a Lightweight Directory Access Protocol (LDAP) server as the only point for user authentication with a username/password. Salesforce delegated authentication is configured to integrate Salesforce under single sign-on (SSO). How can end users change their password?

- A. Users once logged in, can go to the Change Password screen in Salesforce.
- B. Users can click on the "Forgot your Password" link on the Salesforce.com login page.
- C. Users can request the Salesforce Admin to reset their password.
- D. Users can change it on the enterprise LDAP authentication portal.

**Answer:** C

#### Explanation:

Users can request the Salesforce Admin to reset their password if they are using delegated authentication with LDAP. The other options are not applicable for this scenario, as the password is managed by the LDAP server, not by Salesforce. References: Delegated Authentication, FAQs for Delegated Authentication

#### NEW QUESTION 217

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 220

Universal Containers (UC) is setting up delegated authentication to allow employees to log in using their corporate credentials. UC's security team is concerned about the risks of exposing the corporate login service on the internet and has asked that a reliable trust mechanism be put in place between the login service and Salesforce.

What mechanism should an Architect put in place to enable a trusted connection between the login service and Salesforce?

- A. Require the use of Salesforce security tokens on passwords.
- B. Enforce mutual authentication between systems using SSL.
- C. Include Client Id and Client Secret in the login header callout.
- D. Set up a proxy service for the login service in the DMZ.

**Answer:** B

#### Explanation:

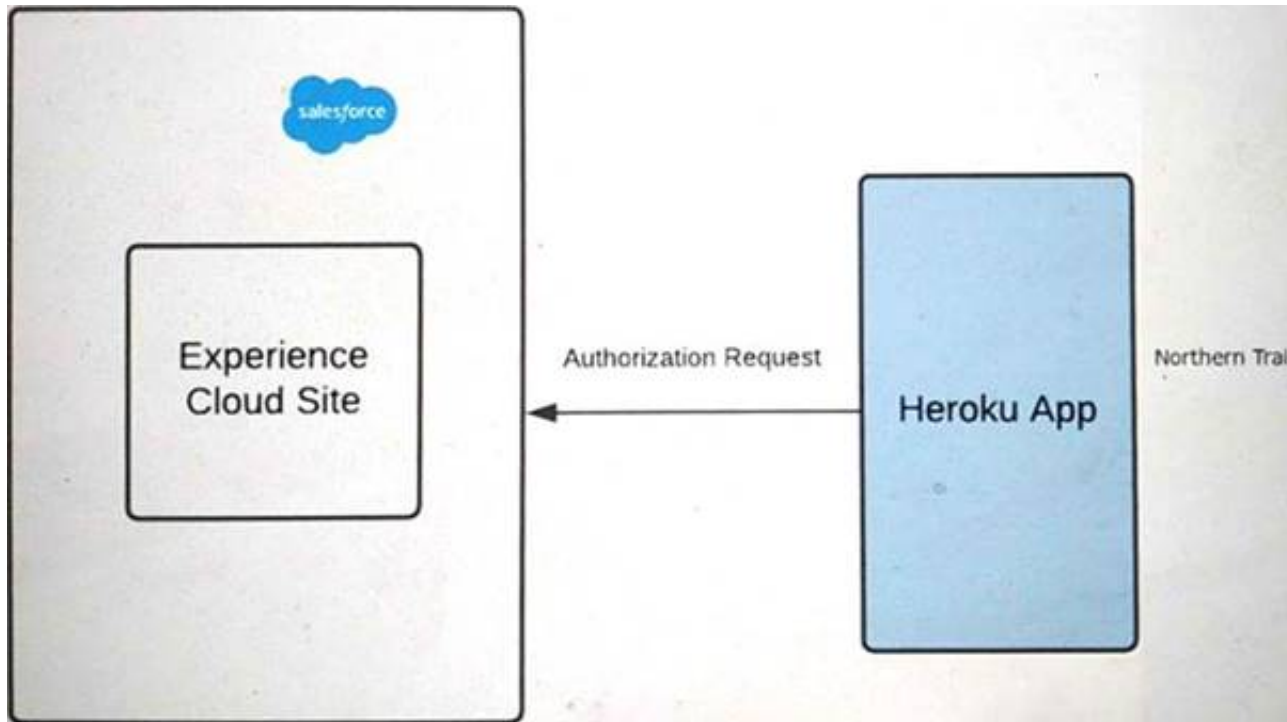
To enable a trusted connection between the login service and Salesforce, an architect should enforce mutual authentication between systems using SSL. Mutual

authentication, also known as two-way SSL or client certificate authentication, is a process in which both parties in a communication exchange certificates to verify their identities<sup>7</sup>. This mechanism ensures that only authorized systems can access each other's resources and prevents unauthorized access or spoofing attacks<sup>8</sup>. To use mutual authentication with delegated authentication you need to do the following steps<sup>9</sup>:

- Generate a self-signed certificate in Salesforce and download it.
- Import the certificate into your login service's truststore.
- Configure your login service to require client certificates for incoming requests.
- Generate a certificate for your login service and export it.
- Import the certificate into Salesforce's certificate and key management tool.
- Enable mutual authentication for your login service's endpoint URL in Salesforce. References:
- Mutual Authentication
- Mutual Authentication Overview
- Set Up Mutual Authentication

#### NEW QUESTION 221

Refer to the exhibit.



Outfitters (NTO) is using Experience Cloud as an Identity for its application on Heroku. The application on Heroku should be able to handle two brands, Northern Trail Shoes and Northern Trail Shirts.

A user should select either of the two brands in Heroku before logging into the community. The app then performs Authorization using OAuth2.0 with the Salesforce Experience Cloud site.

NTO wants to make sure it renders login page images dynamically based on the user's brand preference selected in Heroku before Authorization. what should an identity architect do to fulfill the above requirements?

- A. For each brand create different communities and redirect users to the appropriate community using a custom Login controller written in Apex.
- B. Create multiple login screens using Experience Builder and use Login Flows at runtime to route to different login screens.
- C. Authorize third-party service by sending authorization requests to the community-url/services/oauth2/authorize/cookie\_value.
- D. Authorize third-party service by sending authorization requests to thecommunity-url/services/oauth2/authonze/expid\_value.

**Answer:** D

#### Explanation:

OAuth 2.0 is an open standard for authorization that allows a third-party application to obtain limited access to a protected resource on behalf of a user. To authorize a third-party service using OAuth 2.0 with the Salesforce Experience Cloud site, the identity architect should do the following steps:

- Create a connected app for the third-party service in Salesforce. A connected app is an application that integrates with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect. To create a connected app, you need to provide the basic information, such as the app name, logo URL, contact email, and API name. You also need to enable OAuth and configure the OAuth settings, such as the callback URL, the scopes, and the policies.
- Authorize the third-party service by sending authorization requests to the community-url/services/oauth2/authorize/expid\_value. This is a special endpoint that allows you to specify an experience ID (expid) as a query parameter in the authorization request. The experience ID is a unique identifier for each experience (community or site) in Salesforce. By using this endpoint, you can dynamically render the login page images based on the user's brand preference selected in the third-party service before authorization.

References:

- OAuth 2.0
- OAuth 2.0 Web Server Authentication Flow
- Connected Apps
- Create a Connected App
- Experience ID
- Authorize Apps with OAuth

#### NEW QUESTION 226

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### Identity-and-Access-Management-Architect Practice Exam Features:

- \* Identity-and-Access-Management-Architect Questions and Answers Updated Frequently
- \* Identity-and-Access-Management-Architect Practice Questions Verified by Expert Senior Certified Staff
- \* Identity-and-Access-Management-Architect Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* Identity-and-Access-Management-Architect Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The Identity-and-Access-Management-Architect Practice Test Here](#)**